Cisco Security Manager 4.24 ユーザーガイド

初版：2021 年 11 月 22 日

最終更新：2021 年 6 月 7 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（ **www.cisco.com/jp/go/safety_warning/** ）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

第 I 部 : **Security Manager の基本的な使用方法** 81

第 1 章 **Getting Started With Cisco Security Manager** 1

製品の概要 1

Cisco Security Manager の主な利点 2

Security Manager のポリシー フィーチャ セット 5

Security Manager アプリケーションの概要 8

デバイス モニタリングの概要 9

Security Manager での IPv6 サポート 11

Cisco Security Manager サーバーでの IPv6 の設定 11

IPv6 ポリシーの設定 12

Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 14

Security Manager へのログインおよび終了 14

ユーザの権限について 15

Cisco Security Management Suite サーバへのログイン 16

Security Manager クライアントへのログインおよび終了 17

Configuration Manager の使用方法 - 概要 18

Configuration Manager の概要 19

デバイス ビューの概要 20

ポリシー ビューの概要 22

マップ ビューの概要 23

セキュリティ ポリシー設定のタスク フロー 24

ポリシーおよびポリシー オブジェクトの概要 25

ワークフローおよびアクティビティの概要 26

Workflow モードの作業 27
Workflow 以外のモードの作業 28
Workflow モードの比較 29
JumpStart を使用した Security Manager の理解 32
Security Manager の初期設定の実行 32
電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 34
ワークフロー モードの変更 36
Security Manager インターフェイスの基本機能について 38
Configuration Manager のメニュー バー リファレンス 38
[File] メニュー（Configuration Manager） 39
[Edit] メニュー（Configuration Manager） 40
[View] メニュー（Configuration Manager） 41
[Policy] メニュー（Configuration Manager） 42
[Map] メニュー（Configuration Manager） 43
[Manage] メニュー（Configuration Manager） 45
[Tools] メニュー（Configuration Manager） 46
[Activities] メニュー（Configuration Manager） 48
Tickets Menu（Configuration Manager） 48
[Launch] メニュー（Configuration Manager） 49
[Help] メニュー（Configuration Manager） 51
ツールバー リファレンス（Configuration Manager） 51
グローバル検索の使用 55
セレクタの使用 60
セレクタ内の項目のフィルタリング 60
[Create Filter] ダイアログボックス 62
ウィザードの使用 63
テーブルの使用 64
テーブルのフィルタリング 64
テーブル カラムおよびカラム見出しの機能 66
テキスト フィールドの使用方法 66
テキストの ASCII 制限について 66

テキスト ボックス内のテキストの検索 67
テキスト ボックス内のナビゲート 67
Cisco Security Manager でのファイルまたはディレクトリの選択または指定 67
ユーザ インターフェイスに問題がある場合のトラブルシューティング 69
オンライン ヘルプの利用方法 70

第 2 章 デバイスを管理するための準備 71
デバイスの通信要件について 71
SSL（HTTPS）の設定 73
PIX ファイアウォール、ASA、および FWSM デバイスでの SSL（HTTPS）の設定 74
Cisco IOS ルータでの SSL の設定 75
SSH の設定 77
SSH の重要な行末端ルール 77
認証のテスト 78
Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定 79
非 SSH 接続の禁止（任意） 80
AUS または Configuration Engine の設定 81
PIX ファイアウォールおよび ASA デバイスでの AUS の設定 81
Cisco ASA デバイスでのライセンスの設定 83
Cisco IOS デバイスでのライセンスの設定 84
IPS デバイスの初期化 85

第 3 章 デバイス インベントリの管理 87
デバイス インベントリについて 87
デバイス ビューについて 87
デバイス名およびデバイスと見なされる要素について 90
デバイス クレデンシャルについて 91
デバイス プロパティについて 93
デバイス インベントリへのデバイスの追加 94
デバイスクラスタの使用 97

ネットワークからのデバイスの追加 100
[Device Information] ページ - [Add Device from Network] 103
[Service Module Credentials] ダイアログボックス 108
[IPS Module Discovery] ダイアログボックス 110
設定ファイルからのデバイスの追加 112
[Device Information] ページ - [Configuration File] 113
手動定義によるデバイスの追加 116
[Device Information] ページ - [New Device] 118
インベントリ ファイルからのデバイスの追加 122
[Device Information] ページ - [Add Device from File] 125
デバイス インベントリの使用 129
Auto Update Server または Configuration Engine の追加、編集、または削除 130
[Server Properties] ダイアログボックス 132
[Available Servers] ダイアログボックス 134
インターフェイス モジュールの追加または変更 135
デバイス プロパティの表示または変更 136
[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ 137
[Device Credentials] ページ 143
[Device Groups] ページ 148
[グループ情報（Group Information）] ページ 149
[ライセンス情報（License Information）] ページ 152
ポリシー オブジェクト オーバーライドのページ 154
重要なデバイス プロパティの変更 155
Security Manager の機能セットを変更しないイメージ バージョン変更 155
Security Manager の機能セットを変更する変更 157
デバイスに含まれている要素の表示 160
デバイスの複製 160
Security Manager インベントリからのデバイスの削除 162
[Device Delete Validation] ダイアログボックス 163
デバイス グループの使用 164
デバイスのグループ化について 164

[Edit Device Groups] ダイアログボックス 166
デバイス グループ タイプの作成 167
デバイス グループの作成 168
デバイス グループまたはグループ タイプの削除 169
デバイス グループに対するデバイスの追加と削除 169
[デバイスステータスビュー（Device Status View）] の使用 170

第 4 章 アクティビティの管理 177
アクティビティについて 177
アクティビティの利点 179
アクティビティの承認 179
アクティビティとロッキング 180
アクティビティと複数のユーザ 181
アクティビティ/チケットの状態について 181
アクティビティ/チケットの操作 185
Workflow モードでのアクティビティ機能へのアクセス 186
Workflow 以外のモードでのチケット機能へのアクセス 188
アクティビティ/チケット マネージャ ウィンドウ 189
アクティビティ/チケットの作成 193
[必要なアクティビティ/チケットへの応答（Responding to the Activity/Ticket Required）] ダイアログボックス 195
アクティビティ/チケットを開く 195
アクティビティ/チケットを閉じる 196
変更レポートの表示 197
チケット管理が無効になっている Workflow 以外のモードでの変更レポートの選択 200
アクティビティ/チケットの検証 200
承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） 202
アクティビティの承認または拒否（Workflow モード） 203
アクティビティ/チケットの破棄 205
アクティビティ/チケットのステータスおよび履歴の表示 207

第 5 章 ポリシーの管理 209

ポリシーについて 209

設定ベースのポリシーとルールベースのポリシー 210

サービスポリシーとプラットフォーム固有のポリシー 211

ローカルポリシーと共有ポリシー 211

ルールの継承について 213

継承と割り当て 216

ポリシー管理とオブジェクト 217

ポリシーのロックについて 217

ロックとポリシーについて 219

ロックと VPN トポロジについて 220

ロックとオブジェクトについて 220

ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ 221

ポリシーの検出 223

Security Manager にすでに存在するデバイス上のポリシーの検出 227

[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス 231

ポリシー検出タスクのステータスの表示 237

[Discovery Status] ダイアログボックス 238

[Policy Discovery Status] ページ 240

ポリシー検出に関する FAQ 243

デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 247

ポリシー ステータス アイコン 248

基本的なポリシー管理の実行 248

デバイス ビューにおけるローカル ポリシーの設定 249

デバイス間でのポリシーのコピー 251

ポリシーの割り当て解除 255

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 256

ポリシー バナーの使用 258

デバイス ビューおよび Site-to-Site VPN Manager におけるポリシー ショートカット メニュー コマンド 260

ローカル ポリシーの共有 262
選択したデバイスの複数のポリシーの共有 263
ポリシーの共有解除 265
デバイスまたは VPN トポロジへの共有ポリシーの割り当て 266
共有ポリシーへのローカル ルールの追加 267
ルールの継承または継承の解除 269
共有ポリシーのクローニング（コピー） 270
共有ポリシー名の変更 270
デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更 271
デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 272
ポリシー ビューにおける共有ポリシーの管理 273
ポリシー ビューのセレクタ 275
ポリシー ビュー - 共有ポリシー セレクタのオプション 277
新しい共有ポリシーの作成 278
ポリシー ビューにおけるポリシー割り当ての変更 279
共有ポリシーの削除 280
ポリシーバンドルの管理 281
新規ポリシーバンドルの作成 282
ポリシーバンドルの複製 283
ポリシーバンドルの名前変更 284
ポリシーバンドルのデバイスへの割り当て 284

第 6 章 ポリシー オブジェクトの管理 287
ポリシーのオブジェクトの選択 288
Policy Object Manager 290
ポリシーオブジェクト マネージャー: ドッキング解除とドッキング 296
Policy Object Manager のショートカットメニュー 297
ポリシー オブジェクトの操作：基本手順 298
ポリシー オブジェクトの作成 299
オブジェクトの編集 303

カテゴリ オブジェクトの使用 304
オブジェクトのクローニング（複製） 305
オブジェクトの詳細の表示 305
オブジェクト使用状況レポートの生成 306
オブジェクトの削除 308
オブジェクト オーバーライドの管理 309
個々のデバイスのポリシー オブジェクト オーバーライドについて 310
ポリシー オブジェクトの上書きの許可 311
単一デバイスのオブジェクト オーバーライドの作成または編集 312
複数デバイスのオブジェクト オーバーライドの一括での作成または編集 313
デバイスレベルのオブジェクト オーバーライドの削除 315
Cisco Security Manager のオーバーライド可能なオブジェクト 316
ポリシー オブジェクトのインポートおよびエクスポート 318
AAA サーバおよびサーバ グループ オブジェクトについて 323
サポートされる AAA サーバ タイプ 324
ASA、PIX、および FWSM デバイスでのその他の AAA サポート 325
定義済みの AAA 認証サーバ グループ 328
デフォルトの AAA サーバ グループおよび IOS デバイス 329
AAA サーバ オブジェクトの作成 330
[Add AAA Server]/[Edit AAA Server] ダイアログボックス 331
[AAA Server] ダイアログボックス - RADIUS 設定 334
[AAA Server] ダイアログボックス - TACACS+ 設定 337
[AAA Server] ダイアログボックス - Kerberos 設定 338
[AAA Server] ダイアログボックス - LDAP 設定 339
[AAA Server] ダイアログボックス - NT 設定 343
[AAA Server] ダイアログボックス - SDI 設定 344
[AAA Server] ダイアログボックス - HTTP-FORM 設定 345
[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス 347
[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス 348
[Add Map Value]/[Edit Map Value] ダイアログボックス 349
AAA サーバ グループ オブジェクトの作成 349

[AAA Server Group] ダイアログボックス 351
アクセス コントロール リスト オブジェクトの作成 356
拡張アクセス コントロール リスト オブジェクトの作成 357
標準アクセス コントロール リスト オブジェクトの作成 360
Web アクセス コントロール リスト オブジェクトの作成 361
統合アクセス制御リストオブジェクトの作成 363
[Add Access List]/[Edit Access List] ダイアログボックス 365
[Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス 367
[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス 370
[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス 372
[Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）] ダイアログボックス 375
時間範囲オブジェクトの設定 379
[Recurring Ranges] ダイアログボックス 381
インターフェイス ロール オブジェクトについて 381
インターフェイス ロール オブジェクトの作成 383
[Interface Role] ダイアログボックス 384
ポリシー定義中のインターフェイスの指定 386
単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 387
インターフェイスとインターフェイス ロール間の名前の競合の処理 388
マップ オブジェクトについて 388
ネットワーク/ホストオブジェクトについて 391
連続および不連続ネットワーク マスク（IPv4 アドレスに対応） 393
ネットワーク/ホストオブジェクトの作成 394
[Add Network/Host]/[Edit Network/Host] ダイアログボックス 395
未指定ネットワーク/ホストオブジェクトの使用 400
ポリシー定義中の IP アドレスの指定 401
VM 属性ポリシー 403
VM 属性エージェントと vCenter 間の通信 404

属性エージェントの状態 404
vCenter 仮想マシンの設定に関するガイドライン 405
VM 属性ポリシーの設定 406
プールオブジェクトについて 407
[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス 407
[IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックス 409
[MACアドレスプールの追加または編集（Add or Edit MAC Address Pool）] ダイアログボックス 410
[NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックス 411
[DHCPv6プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス 413
SAML ID プロバイダの構成 415
SAML アイデンティティ プロバイダーの追加または編集 415
サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 418
ポート リスト オブジェクトの設定 420
サービス オブジェクトの設定 422
ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 426
ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 427
サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 429

第 7 章 **FlexConfig の管理** 431
FlexConfig ポリシーとポリシー オブジェクトについて 432
FlexConfig ポリシー オブジェクトにおける CLI コマンドの使用 433
スクリプト言語命令の使用 434
スクリプト言語の例 1：ループ 434
スクリプト言語の例 2：2 次元配列でのループ 434
例 3：If/Else ステートメントを使用したループ 435
FlexConfig オブジェクトの変数について 436
FlexConfig ポリシー オブジェクトの変数の例 437
FlexConfig システム変数 438
定義済みの FlexConfig ポリシー オブジェクト 454

FlexConfig ポリシーとポリシー オブジェクトの設定 461
FlexConfig の作成シナリオ 461
FlexConfig ポリシー オブジェクトの作成 465
[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス 467
[Create Text Object] ダイアログボックス 469
[Add Text Object]/[Edit Text Object] ダイアログボックス 470
[FlexConfig Undefined Variables] ダイアログボックス 471
[Property Selector] ダイアログボックス 472
FlexConfig ポリシーの編集 473
[FlexConfig Policy] ページ 475
[Values Assignment] ダイアログボックス 476
[FlexConfig Preview] ダイアログボックス 478
FlexConfig のトラブルシューティング 478

第 8 章 展開の管理 481
展開について 481
展開プロセスの概要 482
Workflow 以外のモードでの展開 484
Workflow 以外のモードでの展開タスク フロー 484
Workflow 以外のモードでのジョブの状態 485
Workflow モードでの展開 486
Workflow モードでの展開タスク フロー 486
Workflow モードでのジョブの状態 487
展開ジョブの承認 489
展開ジョブと複数のユーザ 489
展開ジョブまたは展開スケジュールにデバイスを含める操作 489
展開方法について 490
デバイスへの直接展開 491
中間サーバを使用したデバイスへの展開 492
ファイルへの展開 493
アウトオブバンド変更の処理方法について 494

デバイス OS バージョン不一致の処理 495
Deployment Manager および Configuration Archive の概要 497
Deployment Manager でできること 498
[Deployment Manager] ウィンドウ 499
[Deployment Workflow Commentary] ダイアログボックス 505
[Deployment Schedules] タブ、Deployment Manager 505
[Configuration Archive] ウィンドウ 509
展開および Configuration Archive の使用 511
ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 512
展開ジョブを正常に完了するためのヒント 513
Workflow 以外のモードでの設定の展開 515
[Edit Deploy Method] ダイアログボックス 518
警告 - [Partial VPN Deployment] ダイアログボックス 519
[Deployment Status Details] ダイアログボックス 520
Workflow モードでの設定の展開 523
展開ジョブの作成および編集 524
展開ジョブの送信 528
展開ジョブの承認と拒否 529
Workflow モードでの展開ジョブの展開 530
展開ジョブの廃棄 531
Auto Update Server または CNS Configuration Engine を使用した設定の展開 532
Token Management Server への設定の展開 534
設定のプレビュー 535
アウトオブバンド変更の検出および分析 537
アウトオブバンド変更検出の例外 540
アウトオブバンド変更検出の例外 541
[OOB (Out of Band) Changes] ダイアログボックス 541
OOB 再同期Tool 543
デバイスへの設定の再展開 547
展開ジョブの中断 549
展開スケジュールの作成または編集 550

[Schedule] ダイアログボックス 551
[Add Other Devices] ダイアログボックス 553
展開スケジュールの一時停止または再開 554
デバイスの設定バージョンの Configuration Archive への追加 555
アーカイブされた設定バージョンの表示および比較 555
[Configuration Version Viewer] 556
展開トランスクリプトの表示 558
設定のロールバック 560
設定のロールバックについて 560
マルチ コンテキスト モードのデバイスのロールバックについて 562
フェールオーバー デバイスのロールバックについて 562
Catalyst 6500/7600 デバイスのロールバックについて 563
IPS および IOS IPS のロールバックについて 564
ロールバック後、競合を発生させる可能性があるコマンド 566
ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド 567
Deployment Manager を使用したデバイスへの設定のロールバック 568
ロールバックを使用したアーカイブ済み設定の展開 569
ファイルへの展開時のロールバックの実行 571

第 9 章 デバイス通信および展開のトラブルシューティング 573
デバイス接続のテスト 573
[Device Connectivity Test] ダイアログボックス 575
デバイス通信設定および証明書の管理 576
複数証明書認証のサポート 577
HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 578
デバイス検出時にセキュリティ証明書が拒否される 579
デバイス検出中の無効な証明書のエラー 580
SSH 接続の問題のトラブルシューティング 581
デバイス通信障害のトラブルシューティング 581
デバイス セレクタ内の赤い X マークの解決 583
展開のトラブルシューティング 584

Security Manager のデバイス メッセージへの応答方法の変更 585
ASA 8.3+ デバイスのメモリ違反展開エラー 587
未参照のオブジェクトを削除しようとしたときのエラー 587
展開後に Security Manager がデバイスと通信できない 588
ルーティング プロセスを組み込む VPN の更新 589
ルータ ポリシーおよび VPN ポリシーを使用した展開方式の混合 589
ルータへの展開の失敗 591
Catalyst スイッチおよびサービス モジュールへの展開の失敗 592
Security Manager でマルチ コンテキストの FWSM に設定を展開する方法の変更 594
AUS により管理されるデバイスへの展開が失敗する 595
Configuration Engine により管理されるデバイスのセットアップのトラブルシューティング 595

第 10 章 **Cisco Security Manager サーバーの管理** 599
Security Manager サーバの管理および運用の概要 599
Security Manager サーバのクラスタの管理 600
Security Manager サーバ クラスタの管理 601
Security Manager サーバの分割 601
Cisco Security Manager サーバー間での共有ポリシーの同期 603
デバイス インベントリのエクスポート 605
Security Manager クライアントからのデバイス インベントリのエクスポート 605
インベントリのインポートまたはエクスポートでサポートされている CSV 形式 609
コマンドラインからのデバイス インベントリのエクスポート 611
共有ポリシーのエクスポート 612
ポリシーまたはデバイスのインポート 615
Security Manager のライセンス ファイルのインストール 618
証明書信頼管理 620
監査レポートの使用 622
監査レポートについて 623
監査レポートの生成 623
[Audit Report] ウィンドウの使用 624

監査ログ エントリのパージ 627
別のユーザの作業の引き継ぎ 628
管理ユーザまたは他のユーザのパスワード変更 628
Security Manager データベースのバックアップおよび復元 629
サーバ データベースのバックアップ 629
サーバ データベースの復元 632
Cisco Technical Assistance Center 用データの生成 633
Cisco Technical Assistance Center 用の診断ファイルの作成 633
展開ステータス レポートまたは検出ステータス レポートの生成 636
Cisco Technical Assistance Center 用の差分データベース バックアップの生成 637

第 11 章 **Security Manager の管理設定値の設定** 641
[API設定（API Settings）] ページ 642
[自動リンク設定（AutoL-ink Settings）] ページ 643
[ACLヒットカウント設定（ACL Hit Count Settings）] ページ 644
[CCO設定（CCO Settings）] ページ 645
[Configuration Archive] ページ 649
[CS-MARS] ページ 650
[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス 652
[CSM Mobile] ページ 653
[Customize Desktop] ページ 654
[Debug Options] ページ 656
[Deployment] ページ 658
[Device Communication] ページ 668
[Add Certificate] ダイアログボックス 672
[Device Groups] ページ 673
[Discovery] ページ 674
[Event Management] ページ 677
Syslog リレーサーバーのトラブルシューティング 685
IP によるデバイス管理 685
[CPU スロットリング ポリシー] ダイアログボックス 686

[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス 688
[Health and Performance Monitor] ページ 690
[Report Manager] ページ 692
[Identity Settings] ページ 693
[Image Manager] ページ 695
[IPインテリジェンス設定（IP Intelligence Settings）] ページ 696
[イベント通知設定（Eventing Notification Settings）] ページ 701
[IPS Updates] ページ 705
[Edit Update Server Settings] ダイアログボックス 712
[Edit Auto Update Settings] ダイアログボックス 715
[シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックス 716
[ISE設定（ISE Settings）] ページ 718
Licensing ページ 719
[CSM] タブ、[Licensing] ページ 720
[IPS] タブ、[Licensing] ページ 720
ライセンスを更新または再展開する IPS デバイスの確認 724
IPS ライセンス ファイルの選択 725
[License Update Status Details] ダイアログボックス 725
[Logs] ページ 726
[Policy Management] ページ 729
[Policy Objects] ページ 732
[プロセスモニタリングの設定（Process Monitoring Settings）] ページ 733
[シングルサインオンの設定（Single Sign-on Configuration）] ページ 735
[Rule Expiration] ページ 736
[Server Security] ページ 737
[Take Over User Session] ページ 739
[チケット管理（Ticket Management）] ページ 740
[Token Management] ページ 742
[VPN Policy Defaults] ページ 743
[Workflow] ページ 745

[ウォール設定（Wall Settings）] ページ 747

第 II 部： ファイアウォール サービスおよび NAT 753

第 12 章 ファイアウォール サービスの概要 755

ファイアウォール サービスの概要 755

ファイアウォール ルールの処理順序について 757

NAT がファイアウォール ルールに与える影響について 758

Security Manager によって保持される ACL 名 759

ACL 命名ルール 761

ユーザー定義の ACL ポリシーの名前付けの競合の解決 763

ポリシー間での ACL 名前競合の解決 763

ルール テーブルの管理 763

ルール テーブルの使用 764

ルールの追加および削除 766

ルールの編集 767

ルール テーブルの [Address] セルの追加または編集 769

ルールテーブルの [ユーザー（User）] セルの追加または編集 771

ルール テーブルの [Services] セルの追加または編集 772

ルール テーブルの [Interfaces] セルまたは [Zones] セルの追加または編集 773

ルール テーブルの [Category] セルの編集 774

ルール テーブルの [Description] セルの編集 774

ルール テーブルのセルの内容の表示 774

ルール テーブルの項目の検索と置換 777

[Find and Replace] ダイアログボックス 778

ルールの移動とルール順序の重要性 781

ルールのイネーブル化とディセーブル化 782

セクションを使用したルール テーブルの編成 783

[Add Rule Section]/[Edit Rule Section] ダイアログボックス 784

ルールの結合 785

[Combine Rules Selection Summary] ダイアログボックス 787

Rule Combiner 結果の解釈 789
Rule Combiner 結果の例 791
IPv4 ルールから統合ルールへの変換 792
ポリシー クエリー レポートの生成 793
[Querying Device or Policy] ダイアログボックス 795
ポリシー クエリー結果の解釈 799
[Policy Query Result] の例 801
ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化 802
検出中のオブジェクト グループの展開 806

第 13 章 ID 認証ファイアウォール ポリシーの管理 809
ID 認証ファイアウォールポリシーの概要 809
ユーザー ID の取得 810
ID 認証ファイアウォール ポリシーの要件 811
ID 認証サービスを提供するためのファイアウォールの設定 816
ID 認証ファイアウォール ポリシーの設定 817
ID 認証ファイアウォール サービスのイネーブル化 818
Active Directory サーバおよびエージェントの識別 818
アイデンティティ オプションの設定 828
アイデンティティ ユーザ グループ オブジェクトの作成 833
ポリシーでのアイデンティティ ユーザの選択 835
アイデンティティ ベースのファイアウォール ルールの設定 836
カットスルー プロキシの設定 839
ユーザ統計の収集 842
アイデンティティ ベースのルールを使用した VPN トラフィックのフィルタリング 843
アイデンティティ ファイアウォール ポリシーの監視 844

第 14 章 Trustsec ファイアウォールポリシーの管理 845
TrustSec ファイアウォールポリシーの概要 845
Cisco TrustSec の SGT および SXP サポートについて 846
Cisco TrustSec ソリューションのロール 847

セキュリティ グループ ポリシーの適用 848
送信者および受信者のロールについて 851
ASA と Cisco TrustSec を統合するための前提条件 852
TrustSec ファイアウォールポリシーの構成 853
Cisco TrustSec サービスの設定 854
Security Exchange Protocol（SXP）の設定 854
SXP 接続ピアの定義 859
セキュリティ グループ オブジェクトの作成 863
ポリシーでのセキュリティグループの選択 865
TrustSec ベースのファイアウォールルールの設定 866
TrustSec ファイアウォールポリシーのモニタリング 867

第 15 章 ファイアウォール AAA ルールの管理 869
AAA ルールについて 869
ユーザの認証方法について 871
ASA、PIX、および FWSM デバイスの AAA ルールの設定 873
IOS デバイスの AAA ルールの設定 877
[AAA Rules] ページ 880
[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス 885
[Edit AAA Option] ダイアログボックス 893
[AuthProxy] ダイアログボックス 893
[Edit Server Group] ダイアログボックス 894
AAA ファイアウォール設定ポリシー 894
[AAA Firewall] 設定ページの [Advanced Setting] タブ 895
[Interactive Authentication Configuration] ダイアログボックス 900
[Clear Connection Configuration] ダイアログボックス 901
[AAA Firewall] ページの [MAC-Exempt List] タブ 902
[Firewall AAA MAC Exempt Setting] ダイアログボックス 904
[AAA] ページ 905
Firewall AAA IOS Timeout Value Setting 908

第 16 章 ファイアウォール アクセス ルールの管理 913
アクセス ルールについて 913
グローバル アクセス ルールについて 915
デバイス固有のアクセス ルールの動作について 917
アクセス ルールのアドレス要件およびルールの展開方法について 918
アクセス ルールの設定 920
[Access Rules] ページ 924
[Add Access Rule]/[Edit Access Rule] ダイアログボックス 930
[Advanced]/[Edit Options] ダイアログボックス 936
[Hit Count Selection Summary] ダイアログボックス 939
アクセス ルールの有効期限の設定 942
アクセス コントロール ポリシー設定の指定 943
[Access Control Settings] ページ 944
[Firewall ACL Setting] ダイアログボックス 947
自動競合検出の使用 950
自動競合検出について 950
自動競合検出のユーザー インターフェイスについて 952
競合の解決 957
ヒットカウントの詳細の表示 960
[サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ 963
ルールのインポート 966
Import Rules ウィザード - [Enter Parameters] ページ 967
Import Rules ウィザード - [Status] ページ 969
Import Rules ウィザード - [Preview] ページ 970
インポートされたルールの例 971
展開中のアクセス ルールの自動最適化 973
[アクセスルールの追加（Add Access Rule）] ダイアログでのデフォルトのカスタマイズ 975

第 17 章 ファイアウォール インスペクション ルールの管理 977
インスペクション ルールについて 977

インスペクション ルールのインターフェイスの選択 979
検査するプロトコルの選択 980
インスペクション ルールのアクセス ルール要件について 981
IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 982
インスペクション ルールの設定 983
[Inspection Rules] ページ 986
Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード 991
[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 994
[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ 998
[Configure DNS] ダイアログボックス 1000
[Configure SMTP] ダイアログボックス 1001
[Configure ESMTP] ダイアログボックス 1001
[Configure Fragments] ダイアログボックス 1002
[Configure IMAP]/[Configure POP3] ダイアログボックス 1002
[Configure RPC] ダイアログボックス 1003
[Custom Protocol] ダイアログボックス 1004
[Configure] ダイアログボックス 1004
インスペクションのプロトコルおよびマップの設定 1004
インスペクション ポリシーのクラス マップの設定 1011
DCE/RPC マップの設定 1013
DCE/RPC クラスとポリシーマップの [一致条件（とアクション）の追加（Add Match Condition (and Action)）]/[一致条件（とアクション）の編集（Edit Match Condition (and Action)）] ダイアログボックス 1015
DNS マップの設定 1017
DNS マップの [Protocol Conformance] タブ 1020
DNS マップの [Filtering] タブ 1021
[DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ 1022

DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1023

ESMTP マップの設定 1027

ESMTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1029

FTP マップの設定 1031

FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1033

GTP マップの設定 1036

[Add Country Network Codes]/[Edit Country Network Codes] ダイアログボックス 1040

[Add Permit Response]/[Edit Permit Response] ダイアログボックス 1040

[GTP Map Timeouts] ダイアログボックス 1040

GTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1041

H.323 マップの設定 1044

[Add HSI Group]/[Edit HSI Group] ダイアログボックス 1047

[Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス 1048

H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1049

ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 1051

HTTP マップの [General] タブ 1053

HTTP マップの [Entity Length] タブ 1055

HTTP マップの [RFC Request Method] タブ 1056

HTTP マップの [Extension Request Method] タブ 1058

HTTP マップの [Port Misuse] タブ 1059

HTTP マップの [Transfer Encoding] タブ 1060

ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定 1062

HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1064

ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定 1069

IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1071

IOS デバイスの IM マップの設定 1073
IP オプション マップの設定 1075
IPv6 マップの設定 1079
IPv6 ポリシーマップの [マッチ条件とアクションの追加または編集（Add/Edit Match Condition and Action] ダイアログボックス 1081
IPsec パススルー マップの設定 1084
NetBIOS マップの設定 1086
ScanSafe マップの設定 1087
SIP マップの設定 1089
SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1091
Skinny マップの設定 1095
Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1098
SNMP マップの設定 1099
SCTP マップの設定 1100
SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス 1102
Diameter マップの設定 1103
Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス 1106
カスタム AVP の作成と追加 1109
TLS プロキシオブジェクトの作成と追加 1112
LISP マップの設定 1116
M3UA マップの設定 1118
M3UA プロトコル準拠 1119
M3UA インスペクションの制限事項 1119
M3UA ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス 1122
正規表現グループの設定 1125
正規表現の追加/編集 1126
正規表現の作成に使用されるメタ文字 1127

IOS デバイスのインスペクション ルールの設定 1129

第 18 章 ファイアウォール Web フィルタ ルールの管理 1135

Web フィルタ ルールについて 1135

ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 1136

[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） 1138

[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログ ボックス 1141

[Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス 1145

[Edit Web Filter Options] ダイアログボックス 1147

IOS デバイス用の Web フィルタルールの設定 1148

[Web Filter Rules] ページ（IOS） 1150

[IOS Web Filter Rule and Applet Scanner] ダイアログボックス 1152

[IOS Web Filter Exclusive Domain Name] ダイアログボックス 1154

Web フィルタ サーバの設定 1155

Web Filter 設定ページ 1156

[Web Filter Server Configuration] ダイアログボックス 1160

第 19 章 ファイアウォールの Botnet Traffic Filter ルールの管理 1163

Botnet Traffic Filter について 1163

ボットネット トラフィック フィルタの設定のタスク フロー 1165

ダイナミック データベースの設定 1167

スタティック データベースへのエントリの追加 1168

DNS スヌーピングのイネーブル化 1169

ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 1170

[Botnet Traffic Filter Rules] ページ 1174

[動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ 1175

[Traffic Classification] タブ 1176

BTF イネーブル化ルール エディタ 1178

BTF 廃棄ルール エディタ 1179

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ 1181

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス 1182

第 20 章 ScanSafe Web Security の使用 1185

ScanSafe Web セキュリティの設定 1187

ScanSafe Web Security ページ 1189

[Add Default User Group]/[Edit Default User Group] ダイアログボックス 1191

[ScanSafe Web Security Settings] ページ 1192

第 21 章 ゾーンベースのファイアウォール ルールの管理 1195

ゾーンベースのファイアウォール ルールについて 1197

Self ゾーン 1200

ゾーンベースのファイアウォールポリシーでの VPN の使用 1201

ゾーンと VRF 対応ファイアウォール 1202

ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について 1203

ゾーンベースのファイアウォール ルールの Services と Protocols の関係について 1207

ゾーンベースのファイアウォール ルールに対する一般的な推奨事項 1208

ゾーンベースのファイアウォールルールの開発と適用 1209

ゾーンベースのファイアウォールルールの追加 1210

ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 1213

ゾーンベースのファイアウォール ポリシーのクラス マップの設定 1217

ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス 1220

ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス 1221

H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1222

HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1222

IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1226

SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1226
SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1228
Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1232
ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1232
N2H2 および Websense クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス 1233
インスペクション パラメータ マップの設定 1234
プロトコル情報パラメータ マップの設定 1237
プロトコル情報パラメータの [Add DNS Server]/[Edit DNS Server] ダイアログボックス 1238
ゾーンベースのファイアウォール ポリシーのポリシー マップの設定 1239
ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス 1240
ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 1242
ローカル Web フィルタ パラメータ マップの設定 1245
N2H2 または WebSense パラメータ マップの設定 1246
[Add External Filter]/[Edit External Filter] ダイアログボックス 1249
Trend パラメータ マップの設定 1250
URL フィルタ パラメータ マップの設定 1251
URL フィルタ パラメータの [Add URL Domain Name]/[Edit URL Domain Name] ダイアログボックス 1255
URLF Glob パラメータ マップの設定 1255
Web フィルタ マップの設定 1258
デフォルトのドロップ動作の変更 1260
ゾーンベースのファイアウォール ルールの設定 1261
[Zone Based Firewall] ページ 1262
[Zone Based Firewall] ページ - [Content Filter] タブ 1265
[Add Zone]/[Edit Zone] ダイアログボックス 1267
ゾーンベースのルールと設定のトラブルシューティング 1267

[Zone-based Firewall Rules] ページ 1272
ゾーンベースのファイアウォール ルールの追加と編集 1276
ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス 1281
[Protocol Selector] ダイアログボックス 1283
[Configure Protocol] ダイアログボックス 1284

第 22 章 トラフィック ゾーンの管理 1287
ゾーンを使用する理由 1287
ECMP ルーティング 1289
トラフィックゾーンについて 1290
トラフィック ゾーンの前提条件 1292
トラフィック ゾーンのガイドライン 1293
トラフィックゾーンの設定 1295

第 23 章 トランスペアレント ファイアウォール ルールの管理 1297
トランスペアレント ファイアウォール ルールの設定 1297
[Transparent Rules] ページ 1300
[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス 1302
[Edit Transparent EtherType] ダイアログボックス 1305
[トランスペアレントマスクの編集（Edit Transparent Mask）] ダイアログボックス 1305

第 24 章 ネットワーク アドレス変換の設定 1307
ネットワーク アドレス変換について 1307
アドレス変換のタイプ 1309
ASA 8.3 以降のデバイスでの「簡易」NAT について 1311
Cisco IOS ルータにおける NAT ポリシー 1313
[NAT] ページ - [Interface Specification] 1313
[NAT] ページ - [Static Rules] 1314
[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス 1316
[NAT] ページ - [Dynamic Rules] 1319
[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス 1321

[NAT] ページ - [Timeouts] 1323
セキュリティ デバイスの NAT ポリシー 1326
トランスペアレント モードの NAT 1326
[CGNATマップ（CGNAT Map）] ページ 1327
[グローバルオプション（Global Options）] ページ 1328
[Translation Options] ページ 1329
PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 1331
アドレス プール 1331
[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA 1333
[Translation Exemptions (NAT 0 ACL)] 1334
[Dynamic Rules] タブ 1337
[Policy Dynamic Rules] タブ 1340
[Static Rules] タブ 1342
[General] タブ 1349
ASA 8.3+ デバイスでの NAT の設定 1352
[Translation Rules]：ASA 8.3+ 1352
Per-Session NAT ルール: ASA 9.0（1）+ 1371

第 III 部： VPN の設定 1377

第 25 章 サイト間 VPN の管理：基本 1379
VPN トポロジについて 1380
ハブアンドスポーク VPN トポロジ 1380
ポイントツーポイント VPN トポロジ 1382
完全メッシュ VPN トポロジ 1382
暗黙的にサポートされるトポロジ 1384
IPsec テクノロジーおよびポリシーについて 1384
サイト間 VPN の必須ポリシーおよびオプションのポリシーについて 1385
サイト間 VPN ポリシーの概要 1388
IKEv2 のサイト間 VPN での複数ピアクリプトマップの設定 1389
各 IPsec テクノロジーでサポートされるデバイスについて 1392

管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み 1394
VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 1395
デバイスのオーバーライドを使用した VPN ポリシーのカスタマイズ 1398
VRF 対応 IPsec について 1398
VRF 対応 IPsec 1 ボックス ソリューション 1399
VRF 対応 IPsec 2 ボックス ソリューション 1400
Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化 1402
サイト間 VPN トポロジおよびポリシーへのアクセス 1403
[Site-to-Site VPN Manager] ウィンドウ 1404
デバイス ビューにおける VPN トポロジの設定 1405
サイト間 VPN ディスカバリ 1406
VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ 1406
VPN ディスカバリの前提条件 1408
VPN ディスカバリ ルール 1408
サイト間 VPN の検出 1411
検出された、複数のスポーク定義を持つ VPN の定義または修復 1413
サイト間 VPN の再検出 1415
VPN トポロジの作成または編集 1416
VPN トポロジの名前および IPsec テクノロジーの定義 1420
VPN トポロジのデバイスの選択 1422
エンドポイントおよび保護対象ネットワークの定義 1424
VPN インターフェイス エンドポイントの設定 1427
ダイヤル バックアップの設定 1432
[Dial Backup Settings] ダイアログボックス 1434
VPNSM または VPN SPA/VSPA エンドポイントの設定 1436
エンドポイントの保護対象ネットワークの特定 1441
VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 1443
VRF 対応 IPsec の設定 1445
クリプトマップの設定 1448

VPN トポロジにおけるハイ アベイラビリティの設定 1450
GET VPN グループ暗号化の定義 1453
[Add Certificate Filter] ダイアログボックス 1458
[Add New Security Association]/[Edit Security Association] ダイアログボックス 1459
GET VPN ピアの定義 1461
新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て 1463
[VPNトポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）] 1464
エクストラネット VPN の作成または編集 1469
VPN トポロジの削除 1475

第 26 章 **IKE および IPsec ポリシーの設定** 1477
IKE および IPsec 設定の概要 1478
IKE バージョン 1 と 2 の比較 1481
IKE について 1482
使用する暗号化アルゴリズムの決定 1483
使用するハッシュ アルゴリズムの決定 1484
使用する Diffie-Hellman 係数グループの決定 1485
使用する認証方式の決定 1486
IKE プロポーザルの設定 1488
[IKEv1 Proposal] ポリシー オブジェクトの設定 1490
[IKEv2 Proposal] ポリシー オブジェクトの設定 1494
IPsec プロポーザルについて 1499
サイト間 VPN の IPsec プロポーザルについて 1500
クリプト マップについて 1500
トランスフォーム セットの概要 1501
逆ルート注入について 1503
サイト間 VPN での IPsec プロポーザルの設定 1504
サイト間 VPN におけるデバイスの IKE バージョンの選択 1509
IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 1510
VPN グローバル設定 1517

VPN グローバルアドレス割り当て設定の設定 1518
VPN グローバル ISAKMP/IPsec 設定 1520
VPN グローバル IKEv2 設定 1526
VPN での NAT について 1530
VPN グローバル NAT 設定 1532
VPN グローバル一般設定 1534
サイト間 VPN での IKEv1 事前共有キー ポリシーについて 1538
IKEv1 事前共有キー ポリシーの設定 1540
Public Key Infrastructure ポリシーについて 1544
PKI 登録を正常に行うための前提条件 1546
サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 1549
サイト間 VPN での複数の IKEv1 CA サーバの定義 1550
リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 1552
[PKI Enrollment] ダイアログボックス 1554
[PKI Enrollment] ダイアログボックス - [CA Information] タブ 1556
[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ 1561
[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ 1565
[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ 1566
サイト間 VPN での IKEv2 認証の設定 1567
[IKEv2 Authentication] ポリシー 1570
[IKEv2 Authentication (Override)] ダイアログボックス 1572

第 27 章 **GRE および DM VPN** 1575
[GRE Modes] ページについて 1575
GRE およびダイナミック GRE VPN 1576
GRE について 1577
GRE を使用した IPsec トンネリングの利点 1577
Security Manager における GRE の実装 1578
GRE を正常に設定するための前提条件 1578
動的にアドレス指定されるスポークの GRE 設定について 1580
IPsec GRE VPN の設定 1581

GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定 1582
ダイナミック マルチポイント VPN（DMVPN） 1586
DMVPN について 1587
DMVPN トポロジでのスポーク間接続のイネーブル化 1588
DMVPN を使用した GRE の利点 1589
DMVPN の設定 1589
DMVPN の [GRE Modes] の設定 1590
大規模 DMVPN の設定 1595
大規模 DMVPN でのサーバ ロード バランシングの設定 1596
[Edit Load Balancing Parameters] ダイアログボックス 1597

第 28 章 **Easy VPN** 1599
Easy VPN について 1599
Easy VPN とダイヤル バックアップ 1600
ハイ アベイラビリティ Easy VPN 1601
Easy VPN とダイナミック仮想トンネル インターフェイス 1601
Easy VPN コンフィギュレーション モード 1602
Easy VPN および IKE 拡張認証（Xauth） 1603
Easy VPN の設定の概要 1605
Easy VPN 設定に関する重要事項 1606
Easy VPN のクライアント接続特性の設定 1607
クレデンシャル ポリシー オブジェクトの設定 1610
Easy VPN での IPsec プロポーザルの設定 1611
Easy VPN に対するダイナミック VTI の設定 1614
Easy VPN における Connection Profile ポリシーの設定 1616
Easy VPN における User Group ポリシーの設定 1617

第 29 章 **Group Encrypted Transport（GET）VPN** 1619
Group Encrypted Transport（GET）VPN について 1619
GET VPN 登録プロセスについて 1623
キーの再生成転送メカニズムの選択 1625

協調キー サーバを使用した冗長性の設定 1627
登録の失敗時にも保護するためのフェールクローズの設定 1628
GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて 1631
時間ベースのアンチリプレイについて 1633
GET VPN の設定 1634
RSA キーの生成と同期 1636
GET VPN の IKE プロポーザルの設定 1638
GET VPN のグローバル設定 1640
GET VPN キー サーバの設定 1642
[Add Key Server]、[Add Group Member] ダイアログボックス 1643
[Edit Key Server] ダイアログボックス 1644
GET VPN グループ メンバーの設定 1645
[Edit Group Member] ダイアログボックス 1646
パッシブ モードを使用した GET VPN への移行 1649
GET VPN 設定のトラブルシューティング 1652

第 30 章 リモート アクセス VPN の管理の基礎 1655
リモート アクセス VPN について 1655
リモート アクセス IPSec VPN について 1656
リモート アクセス SSL VPN について 1657
リモート アクセス SSL VPN の例 1658
SSL VPN アクセスのモード 1659
SSL VPN サポート ファイルの概要と管理 1660
SSL VPN を設定するための前提条件 1663
SSL VPN の制限 1664
各リモート アクセス VPN テクノロジーでサポートされるデバイスについて 1665
リモート アクセス VPN ポリシーの概要 1666
リモート アクセス VPN ポリシーの検出 1669
Remote Access VPN Configuration ウィザードの使用 1671
Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス） 1672

SSL VPN Configuration ウィザード：[Access] ページ（ASA） 1675
SSL VPN Configuration ウィザード：[Connection Profile] ページ（ASA） 1676
Create Group Policy ウィザードによるユーザ グループの作成 1680
Create Group Policy ウィザード：[Full Tunnel] ページ 1682
Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ 1686
Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） 1688
Remote Access VPN Configuration ウィザード：[IPSec VPN Connection Profile] ページ（ASA） 1692
Remote Access VPN Configuration ウィザード：[IPSec Settings] ページ（ASA） 1694
Remote Access VPN Configuration ウィザード：[Defaults] ページ 1695
Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス） 1697
SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） 1699
SSL VPN Configuration ウィザード：[Portal Page Customization] ページ（IOS） 1702
Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） 1703

第 31 章 **ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理 1705**
ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要 1706
グループのロードバランシングについて（ASA） 1710
グループのロードバランスポリシーの設定（ASA） 1711
接続プロファイルの設定（ASA、PIX 7.0+） 1713
[Connection Profiles] ページ 1715
リモートアクセス VPN マルチコンテキスト モードでサポートされる CLI - 接続プロファイル 1717
[General] タブ（[Connection Profiles]） 1718
[AAA] タブ（[Connection Profiles]） 1721
[Secondary AAA] タブ（[Connection Profiles]） 1727
[IPSec] タブ（[Connection Profiles]） 1730
[SSL] タブ（[Connection Profiles]） 1734
リモート アクセス VPN のグループ ポリシーの設定 1740

グループ ポリシーについて（ASA） 1741
グループ ポリシーの作成（ASA、PIX 7.0+） 1743
SSL VPN サーバー検証（ASA）について 1745
信頼できるプール設定の設定（ASA） 1746
Trustpool Manager の使用 1748
[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス 1751
IPSec VPN ポリシーの使用 1753
Certificate to Connection Profile Map ポリシーの設定（ASA） 1754
証明書/接続プロファイル マップ ルールの設定（ASA） 1755
[Map Rule] ダイアログボックス（上半分のテーブル） 1757
[Map Rule] ダイアログボックス（下半分のテーブル） 1758
リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス） 1759
[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス） 1761
SSL および IKEv2 IPSec VPN ポリシーの使用 1764
SSL VPN アクセス ポリシーについて（ASA） 1765
[SSL VPN Access Policy] ページ 1766
Access ポリシーの設定 1772
他の SSL VPN 設定の定義（ASA） 1774
SSL VPN パフォーマンス設定の定義（ASA） 1776
SSL VPN コンテンツ書き換えルールの定義（ASA） 1778
SSL VPN エンコーディング ルールの設定（ASA） 1780
SSL VPN プロキシおよびプロキシ バイパスの設定（ASA） 1782
SSL VPN ブラウザ プラグインの設定（ASA） 1787
SSL VPN AnyConnect クライアント設定について 1789
SSL VPN AnyConnect クライアント設定の定義（ASA） 1792
SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） 1796
SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA） 1799
AnyConnect カスタム属性（ASA）の設定 1801
SSL VPN の高度な設定の定義（ASA） 1803
SSL VPN サーバー検証の設定（ASA） 1805

SSL VPN 共有ライセンスの設定（ASA 8.2+） 1806
共有ライセンス クライアントとしての ASA デバイスの設定 1809
共有ライセンス サーバとしての ASA デバイスの設定 1810
クライアントレス SSL VPN ポータルのカスタマイズ 1811
SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 1811
ASA デバイスの SSL VPN Web ページのローカライズ 1815
ASA デバイスの独自 SSL VPN ログイン ページの作成 1817
ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 1818
SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 1820
ASA デバイスの SSL VPN スマート トンネルの設定 1821
WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化 1825

第 32 章 **リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス） 1827**
ダイナミック アクセス ポリシーについて 1827
ダイナミック アクセス ポリシーの設定 1829
DAP 属性について 1831
DAP 属性の設定 1836
ASA デバイスでの Cisco Secure Desktop ポリシーの設定 1838
[Dynamic Access] ページ（ASA） 1840
[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス 1842
[Main] タブ 1844
[論理的な操作（Logical Operators）] タブ 1884
[Advanced Expressions] タブ 1887
[Cisco Secure Desktop Manager Policy Editor] ダイアログボックス 1888

第 33 章 **IOS および PIX 6.3 デバイスでのリモートアクセス VPN の管理 1891**
IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要 1892
リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス） 1893
IPsec Proposal Editor（IOS、PIX 6.3 デバイス） 1895

[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス 1898
リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） 1900
リモートアクセス VPN での高可用性の設定（IOS） 1904
ユーザ グループ ポリシーの設定 1906
SSL VPN ポリシーの設定（IOS） 1908
[SSL VPN Context Editor] ダイアログボックス（IOS） 1910
[General] タブ 1911
Cisco Secure Desktop 設定オブジェクトの作成 1913

第 34 章 リモート アクセス VPN 用のポリシー オブジェクトの設定 1917
[ASA Group Policies] ダイアログボックス 1918
ASA ポリシーグループのオーバーライド 1923
リモートアクセス VPN マルチコンテキスト モードでサポートされる CLI - グループポリシー 1923
ASA グループ ポリシーのクライアント設定 1925
ASA グループ ポリシーのクライアント ファイアウォール属性 1926
ASA グループ ポリシーのハードウェア クライアント属性 1928
ASA グループ ポリシーの IPSec 設定 1930
[Add Client Access Rules]/[Edit Client Access Rules] ダイアログボックス 1932
ASA グループ ポリシーの SSL VPN クライアントレス設定 1933
[VDIサーバーの追加または編集（Add or Edit VDI Server）] ダイアログボックス 1938
ASA グループ ポリシーの SSL VPN フル クライアント設定 1945
ASA グループ ポリシーの SSL VPN 設定 1954
[Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックス 1957
ASA グループポリシーのブラウザ プロキシ設定 1961
ASA グループ ポリシーの DNS/WINS 設定 1963
ASA グループ ポリシーのスプリット トンネリング設定 1965
ASA グループ ポリシーの接続設定 1967
[Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス 1969
[Add File Object]/[Edit File Object] ダイアログボックス 1972

[ファイルオブジェクト—ファイルを選択（File Object — Choose a file）] ダイアログボックス 1975

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス 1977

[Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックス 1979

[Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス 1980

[Add Bookmarks]/[Edit Bookmarks] ダイアログボックス 1982

[ブックマークエントリの追加（Add Bookmark Entry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス 1984

[Add Post Parameter]/[Edit Post Parameter] ダイアログボックス 1988

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス 1992

[SSL VPN Customization] ダイアログボックス - [Title Panel] 1996

[SSL VPN Customization] ダイアログボックス - [Language] 1997

[Add Language]/[Edit Language] ダイアログボックス 1999

[SSL VPN Customization] ダイアログボックス - [Logon Form] 2000

[SSL VPN Customization] ダイアログボックス - [Informational Panel] 2001

[SSL VPN Customization] ダイアログボックス - [Copyright Panel] 2002

[SSL VPN Customization] ダイアログボックス - [Full Customization] 2003

[SSL VPN Customization] ダイアログボックス - [Toolbar] 2004

[SSL VPN Customization] ダイアログボックス - [Applications] 2005

[SSL VPN Customization] ダイアログボックス - [Custom Panes] 2006

[Add Column]/[Edit Column] ダイアログボックス 2007

[Add Custom Pane]/[Edit Custom Pane] ダイアログボックス 2008

[SSL VPN Customization] ダイアログボックス - [Home Page] 2009

[SSL VPN Customization] ダイアログボックス - [Logout Page] 2010

[Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス 2011

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス 2013

[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス 2015

[スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス 2017

[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス 2019

[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス 2020
[Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス 2022
[Add User Group]/[Edit User Group] ダイアログボックス 2024
[User Group] ダイアログボックス - 一般設定 2027
[User Group] ダイアログボックス - DNS/WINS 設定 2028
[User Group] ダイアログボックス - スプリット トンネリング 2029
[User Group] ダイアログボックス - IOS クライアント設定 2030
[User Group] ダイアログボックス - IOS Xauth オプション 2032
[User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新 2034
[Add Client Update]/[Edit Client Update] ダイアログボックス 2034
[User Group] ダイアログボックス - PIX の詳細オプション 2035
[User Group] ダイアログボックス - クライアントレス設定 2036
[User Group] ダイアログボックス - シン クライアント設定 2038
[User Group] ダイアログボックス - SSL VPN フル トンネル設定 2039
[User Group] ダイアログボックス - SSL VPN スプリット トンネリング 2042
[User Group] ダイアログボックス - ブラウザ プロキシ設定 2043
[User Group] ダイアログボックス - SSL VPN 接続設定 2045
[Add WINS Server List]/[Edit WINS Server List] ダイアログボックス 2045
[Add WINS Server]/[Edit WINS Server] ダイアログボックス 2047

第 35 章 マップ ビューの使用 2049
マップとマップ ビューについて 2049
マップ ビューのメイン ページについて 2050
マップ ツールバー 2052
ナビゲーション ウィンドウの使用方法 2053
マップのコンテキスト メニュー 2053
[Managed Device Node] コンテキスト メニュー 2054
[Multiple Selected Nodes] コンテキスト メニュー 2055
[VPN Connection] コンテキスト メニュー 2056

[Layer 3 Link] コンテキスト メニュー 2056
[Map Object] コンテキスト メニュー 2056
[Map Background] コンテキスト メニュー 2057
マップのアクセス権 2057
マップの操作 [英語] 2058
新しいマップまたはデフォルト マップの作成 2059
マップを開く 2060
マップの保存 2060
マップの削除 2061
マップのエクスポート 2061
マップ要素の配置 2061
マップのパン、中央への配置、およびズーム 2062
マップ要素の選択 2063
マップ ノードの検索 2063
リンクされたマップの使用方法 2064
マップの背景プロパティの設定 2064
マップでのネットワークの表示 2065
マップ要素について 2065
マップでの管理対象デバイスの表示 2067
Catalyst スイッチ、ファイアウォール、および適応型セキュリティ アプライアンスの包含関係の表示 2068
ネットワーク トポロジを表すマップ オブジェクトの使用方法 2069
[Add Map Object] および [Node Properties] ダイアログボックス 2070
[Select Policy Object] ダイアログボックス 2071
[Interface Properties] ダイアログボックス 2072
マップにおけるレイヤ 3 リンクの追加と管理 2072
[Select Interfaces] および [Link Properties] ダイアログボックス 2073
[Add Link] ダイアログボックス 2074
マップ ビューにおける VPN の管理 2074
マップにおける既存 VPN の表示 2074
マップ ビューにおける VPN トポロジの作成 2075

マップからの VPN ポリシーまたはピアの編集 2076
マップ ビューにおけるデバイス ポリシーの管理 2076
マップ ビューにおける基本的なポリシー管理の実行 2076
マップ ビューにおけるファイアウォール ポリシーの管理 2077
マップ ビューにおけるファイアウォール設定の管理 2078

第 IV 部 : IPS の設定 2081

第 36 章 IPS 設定を開始する前に 2083
IPS ネットワーク検知について 2084
ネットワーク トラフィックのキャプチャ 2085
センサーの適切な展開 2086
IPS の調整 2087
IPS 設定の概要 2088
許可ホストの識別 2091
SNMP の設定 2092
汎用 SNMP 設定オプション 2095
SNMPv3 ユーザータブ 2096
[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス 2097
[SNMP Trap Configuration] タブ 2098
[Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス 2100
ユーザ アカウントとパスワードの要件の管理 2101
IPS ユーザーロールについて 2102
管理対象と管理対象外の IPS パスワードについて 2103
IPS パスワードの検出および展開方法について 2104
IPS ユーザ アカウントの設定 2105
ユーザの追加またはユーザログイン情報の編集ダイアログボックス 2107
ユーザ パスワード要件の設定 2108
IPS デバイスの AAA アクセス コントロールの設定 2109
NTP サーバの識別 2112

DNS サーバの識別 2113
HTTP プロキシ サーバの識別 2114
IPS SSHv2 の既知のホストキー 2115
[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス 2115
IPS SSHv1 フォールバック設定の指定 2116
外部製品インターフェイスの設定 2117
[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス 2118
[Add Posture ACL]/[Modify Posture ACL] ダイアログボックス 2120
IPS ロギング ポリシーの設定 2121
IPS ヘルスモニター 2122
IPS セキュリティ設定の指定 2125

第 37 章 IPS デバイスインターフェイスの管理 2127
インターフェイスについて 2127
インターフェイス モードについて 2129
無差別モード 2129
インライン インターフェイス モード 2130
インライン VLAN ペア モード 2130
VLAN グループ モード 2131
VLAN グループの展開 2133
インターフェイスの設定 2133
IPS インターフェイス ポリシーについて 2134
IPS インターフェイス設定のサマリーの表示 2137
物理インターフェイスの設定 2139
[Modify Physical Interface Map] ダイアログボックス 2140
バイパス モードの設定 2142
CDP モードの設定 2143
インライン インターフェイス ペアの設定 2144
インライン VLAN ペアの設定 2145
VLAN グループの設定 2147

第 38 章 仮想センサーの設定 2151

仮想センサーについて 2151

仮想化の利点および制約事項 2153

インライン TCP セッション トラッキング モード 2154

ノーマライザ モードについて 2155

仮想センサーへのインターフェイスの割り当て 2155

デバイスに対する仮想センサーの識別 2156

仮想センサーの定義 2157

仮想センサー ダイアログボックス 2159

仮想センサーのポリシーの編集 2162

仮想センサーの削除 2162

第 39 章 IPS シグニチャの定義 2165

シグニチャについて 2165

シグネチャの詳細情報の取得 2167

シグニチャ継承について 2168

IPS シグネチャの削除 2168

シグニチャの設定 2169

[Signatures] ページ 2169

シグネチャ脅威プロファイルの適用 2177

シグネチャのショートカット メニュー 2179

[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス 2181

[Edit Fidelity] ダイアログボックス 2182

シグネチャ更新レベルの表示 2183

シグニチャのイネーブル化とディセーブル化 2184

シグネチャの編集 2185

[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス 2186

カスタム シグニチャの追加 2191

エンジンのオプション 2192

シグニチャのクローニング 2195

カスタム署名の正規表現 2195
シグニチャ パラメータの編集（シグニチャの調整） 2196
[Edit Signature Parameters] ダイアログボックス 2198
Meta エンジン シグネチャのコンポーネント リストの編集 2205
[Obsoletes] ダイアログボックス 2207
シグニチャの設定値の設定 2207

第 40 章 イベント アクション ルールの設定 2211
IPS イベント アクション プロセスについて 2212
IPS イベント アクションについて 2213
イベント アクション フィルタの設定 2216
イベント アクション フィルタ ルールの管理に関するヒント 2218
[Event Action Filters] ページ 2219
[Add Filter Item]/[Edit Filter Item] ダイアログボックス 2222
イベント アクション オーバーライドの設定 2227
[イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス 2229
リスク評価ポリシーオブジェクトの構成 2230
[リスク レーティングの追加または編集] ダイアログボックス 2232
IPS イベント アクション ネットワーク情報の設定 2233
ターゲットの価値レーティングの設定 2234
[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックス 2235
パッシブ OS フィンガープリントについて 2236
OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） 2238
[Add OS Map]/[Edit OS Map] ダイアログボックス 2241
イベント アクションの設定 2242

第 41 章 IPS 異常検出の管理 2247
異常検出について 2247
ワーム ウイルス 2248
異常検出モード 2249

異常検出ゾーン 2250
異常検出をオフにする場合について 2250
異常検出シグニチャの設定 2251
異常検出の設定 2253
異常検出の学習受け入れモードの設定 2256
異常検出しきい値とヒストグラムについて 2258
異常検出しきい値とヒストグラムの設定 2259
[Add Dest Port Map]/[Modify Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス 2261
[Histogram] ダイアログボックス 2263

第 42 章 グローバル相関の設定 2265
グローバル相関について 2265
レピュテーションについて 2267
ネットワーク参加について 2268
グローバル相関の要件および制限 2269
グローバル相関インスペクションおよびレピュテーションの設定 2271
ネットワーク参加の設定 2272

第 43 章 Attack Response Controller でのブロッキングとレート制限の設定 2275
IPS ブロッキングについて 2275
ブロック適用のストラテジ 2278
レート制限について 2279
ルータおよびスイッチ ブロッキング デバイスについて 2279
メインブロッキングセンサーについて 2281
IPS のブロッキングおよびレート制限の設定 2282
[Blocking] ページ 2285
[General] タブ、IPS ブロッキング ポリシー 2288
[Add User Profile]/[Modify User Profile] ダイアログボックス 2291
[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス 2291

[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス 2293
[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス 2295
[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス 2296
[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス 2297

第 44 章 **IPS センサーの管理 2299**
IPS ライセンスの管理 2299
IPS ライセンス ファイルの更新 2299
IPS ライセンス ファイルの再展開 2301
IPS ライセンス ファイル更新の自動化 2301
IPS 更新の管理 2302
IPS 更新サーバの設定 2303
IPS 更新の確認とダウンロード 2304
IPS 更新の自動化 2305
IPS 更新の手動適用 2307
IPS 証明書の管理 2310
IPS センサーのリブート 2313

第 45 章 **IOS IPS ルータの設定 2315**
Cisco IOS IPS について 2315
IPS サブシステムおよび IOS IPS リビジョンのサポートについて 2316
ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャン 2316
ルータ設定ファイルおよびシグニチャ イベント アクション プロセッサ（SEAP） 2317
Cisco IOS IPS の制限事項および制約事項 2317
Cisco IOS IPS 設定の概要 2318
Cisco IOS IPS ルータでの最初の準備 2320
Cisco IOS IPS のシグニチャ カテゴリの選択 2321
Cisco IOS IPS の一般的な設定値の設定 2322
IOS IPS インターフェイス ルールの設定 2325

[IPS Rule] ダイアログボックス 2326
ペアのダイアログボックス 2327

第 V 部： PIX/ASA/FWSM デバイスの設定 2329

第 46 章 ファイアウォール デバイスの管理 2331
ファイアウォールデバイスのタイプ 2331
ファイアウォールのデフォルト設定 2333
ファイアウォール デバイスのインターフェイスの設定 2333
デバイス インターフェイスについて 2334
ルーテッド モードおよびトランスペアレント モードのインターフェイス 2336
シングルおよびマルチ コンテキストのインターフェイス 2337
非対称ルーティング グループについて 2337
ASA 5505 のポートおよびインターフェイスについて 2338
サブインターフェイスの設定（PIX/ASA） 2339
冗長インターフェイスの設定 2341
EtherChannel の設定 2343
VNI インターフェイスの設定 2350
トンネルインターフェイスの設定 2360
通常の IPSec VPN トンネルの確立 2363
トンネルインターフェイス向け IPSec ポリシーの設定 2364
VLAN インターフェイスの設定 2368
デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 2373
[Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3） 2375
[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） 2380
[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：Cisco Firepower 9000（[全般（General）] タブと [詳細（Advanced）] タブ） 2394
ASA 5505 でのハードウェア ポートの設定 2429
[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス 2432
高度なインターフェイス設定（PIX/ASA/FWSM） 2440
同じセキュリティ レベルを持つインターフェイス間のトラフィックのイネーブル化 2442

PPPoE ユーザ リストの管理 2443
VPDN グループの管理 2444
VXLAN 2446
VXLAN ポリシーの設定 2446

第 47 章 ファイアウォール デバイスでのブリッジング ポリシーの設定 2449
ファイアウォール デバイスでのブリッジングについて 2449
FWSM 3.1 のブリッジング サポート 2452
[ARP Table] ページ 2453
[Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス 2454
[ARP Inspection] ページ 2455
[Add/Edit ARP Inspection] ダイアログボックス 2456
IPv6 ネイバー キャッシュの管理 2457
[MAC Address Table] ページ 2458
[Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックス 2459
[MAC Learning] ページ 2460
[Add MAC Learning]/[Edit MAC Learning] ダイアログボックス 2461
[Management IP] ページ 2461
[Management IPv6] ページ（ASA 5505） 2462

第 48 章 ファイアウォール デバイスでのデバイス管理ポリシーの設定 2467
セキュリティ デバイスでの AAA について 2467
AAA の準備 2468
ローカル データベース 2470
デバイス管理用の AAA 2471
ネットワーク アクセス用の AAA 2471
VPN アクセス用の AAA 2471
[AAA] の [Authentication] タブの設定 2472
[Authorization] タブ 2475
[Accounting] タブ 2476
バナーの設定 2478

[Boot Image/Configuration] の指定 2479
[Images] ダイアログボックス 2480
CLI プロンプトの設定 2481
デバイス クロックの設定 2483
FIPS の有効化/無効化 2485
Cisco Success Network の有効化 2486
Umbrella グローバルポリシーの設定 2487
デバイス クレデンシャルの設定 2488
マウント ポイントの管理 2491
[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス 2492
IP クライアント 2494
[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックス 2494
アプリケーション エージェント 2495

第 49 章 ファイアウォール デバイスでのデバイス アクセスの設定 2497
コンソール タイムアウトの設定 2497
[HTTP] ページ 2498
[HTTP Configuration] ダイアログボックス 2501
ICMP の設定 2502
[Add ICMP]/[Edit ICMP] ダイアログボックス 2503
管理アクセスの設定 2504
管理セッションクォータの制限の設定 2505
セキュア シェル アクセスの設定 2506
[Add SSH Host]/[Edit SSH Host] ダイアログボックス 2507
SSL 設定：[基本（Basic）] タブと [詳細（Advanced）] タブ 2508
参照 ID 2514
[参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックス 2514
SNMP の設定 2516
SNMP の用語 2517

SNMP バージョン 3 2517
[SNMP] ページ 2519
[SNMP Trap Configuration] ダイアログボックス 2522
[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス 2527
[SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス 2529
[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス 2531
[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス 2533
[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス 2537
[Telnet] ページ 2537
[Telnet Configuration] ダイアログボックス 2538

第 50 章 フェールオーバーの設定 2541
フェールオーバーについて 2542
アクティブ/アクティブ フェールオーバー 2544
ステートフル フェールオーバー 2546
基本的なフェールオーバー設定 2547
フェールオーバー グループ 2 へのセキュリティコンテキストの追加 2550
アクティブ/スタンバイ フェールオーバー設定の追加手順 2552
ファイルまたは PKCS12 データへの証明書のエクスポート 2552
スタンバイ デバイスへの証明書のインポート 2553
フェールオーバー ポリシー 2553
[Failover] ページ（PIX 6.3） 2554
[Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3） 2556
[Failover] ページ（FWSM） 2557
[Advanced Settings] ダイアログボックス 2562
[Failover] ページ（ASA/PIX 7.0 以降） 2565
[Settings] ダイアログボックス 2570

[Failover] ページ（セキュリティ コンテキスト） 2578

[Bootstrap Configuration for LAN Failover] ダイアログボックス 2579

第 51 章 ホスト名、リソース、ユーザ アカウントおよび SLA の設定 2581

[Hostname] ページ 2581

マルチコンテキスト FWSM でのリソース管理 2582

[Resources] ページ 2584

[Add Resource]/[Edit Resource] ダイアログボックス 2584

ユーザ アカウントの設定 2588

[Add User Account]/[Edit User Account] ダイアログボックス 2589

接続を維持するためのサービス レベル契約（SLA）のモニタリング 2591

サービス レベル契約の作成 2591

SLA モニタ オブジェクトの設定 2593

第 52 章 ファイアウォール デバイスでのサーバ アクセスの設定 2597

[AUS] ページ 2597

[Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス 2601

[DHCP Relay] ページ 2602

[Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス 2604

[Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス 2605

[DHCPリレーIPv6（DHCP Relay IPv6）] ページ 2606

[DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）]/[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックス 2608

[DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）]/[DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックス 2609

DHCP サーバーの設定 2610

[DHCP Server] ページ 2611

[Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス 2613

[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス 2614

[DNS] ページ 2616

[Add DNS Server Group] ダイアログボックス 2618

[Add DNS Server] ダイアログボックス 2619

DDNS の設定 2620

[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス 2621

[DDNS Update Methods] ダイアログボックス 2622

[NTP] ページ 2624

[NTP Server Configuration] ダイアログボックス 2625

[SMTP Server] ページ 2627

[TFTP Server] ページ 2627

第 53 章 **Firepower 2100 シリーズ デバイスでの FXOS サーバーアクセス設定の構成 2629**

[HTTPS] ページ 2629

[HTTPSの追加（Add HTTPS）]/[HTTPSの編集（Edit HTTPS）] ダイアログボックス 2630

SSH ページ（SSH Page） 2631

[SSHホストの追加（Add SSH Host）]/[SSHホストの編集（Edit SSH Host）] ダイアログボックス 2632

[SNMP] ページ 2633

[SNMPの追加（Add SNMP）]/[SNMPの編集（Edit SNMP）] ダイアログボッス 2634

第 54 章 **ファイアウォール デバイスでのロギング ポリシーの設定 2635**

[NetFlow] ページ 2635

[Add Collector]/[Edit Collector] ダイアログボックス（NetFlow） 2637

組み込まれている Event Manager 2638

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス 2640

[Syslog 設定の追加（Add Syslog Configuration）]/[Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックス 2644

アクション構成の追加および編集ダイアログボックス 2645
[E-Mail Setup] ページ 2645
[Add Email Recipient]/[Edit Email Recipient] ダイアログボックス 2646
[Event Lists] ページ 2647
セージ クラスおよび関連するメッセージ ID 番号 2647
[Add Event List]/[Edit Event List] ダイアログボックス 2649
[Add/Edit Syslog Class] ダイアログボックス 2650
[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス 2650
[Logging Filters] ページ 2651
[Edit Logging Filters] ダイアログボックス 2653
ロギング設定の設定 2655
[Logging Setup] ページ 2656
レート制限レベルの設定 2658
[Rate Limit] ページ 2659
[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス 2660
[Add/Edit Rate Limited Syslog Message] ダイアログボックス 2661
Syslog サーバ設定の設定 2662
Syslog リレー構成 2664
[Server Setup] ページ 2664
ログ レベル 2667
[Add/Edit Syslog Message] ダイアログボックス 2668
Syslog サーバの定義 2669
[Syslog Servers] ページ 2671
[Add/Edit Syslog Server] ダイアログボックス 2672

第 55 章 ファイアウォール デバイスでのマルチキャスト ポリシーの設定 2675
PIM および IGMP のイネーブル化 2675
IGMP の設定 2676
[IGMP] ページ - [Protocol] タブ 2678
[Configure IGMP Parameters] ダイアログボックス 2679
[IGMP] ページ - [Access Group] タブ 2680

[Configure IGMP Access Group Parameters] ダイアログボックス 2681
[IGMP] ページ - [Static Group] タブ 2682
[Configure IGMP Static Group Parameters] ダイアログボックス 2682
[IGMP] ページ - [Join Group] タブ 2683
[Configure IGMP Join Group Parameters] ダイアログボックス 2684
マルチキャスト ルートの設定 2684
[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックス 2685
マルチキャスト境界フィルタの設定 2686
[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックス 2687
[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス 2687
PIM の設定 2688
[PIM] ページ - [Protocol] タブ 2689
[Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックス 2690
[PIM] ページ - [Neighbor Filter] タブ 2691
[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックス 2691
[PIM] ページ - [Bidirectional Neighbor Filter] タブ 2692
[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックス 2693
[PIM] ページ - [Rendezvous Points] タブ 2694
[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス 2695
[PIM] ページ - [Route Tree] タブ 2697
[PIM] ページ - [Request Filter] タブ 2698
[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス 2700
PIM ページ - ブートストラップ ルータ タブ 2701
[ブートストラップルータの追加/編集（Add/Edit Bootstrap Router）] ダイアログボックス 2702

第 56 章 ファイアウォール デバイスでのルーティング ポリシーの設定 2703
[No Proxy ARP] の設定 2703
BGP の設定 2704
BGP について 2706

[General] タブ 2709
[IPv4ファミリ（IPv4 Family）] タブ 2711
IPv4 Family - [全般（General）] タブ 2713
[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス 2715
[Add Filter]/[Edit Filter] ダイアログボックス 2717
[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス 2718
[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス 2728
[Add Redistribution]/[Edit Redistribution] ダイアログボックス 2729
[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス 2730
[IPv6ファミリ（IPv6 Family）] タブ 2732
[IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ 2733
[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス 2735
[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス 2737
[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス 2747
[Add Redistribution]/[Edit Redistribution] ダイアログボックス 2748
[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス 2749
EIGRP の設定 2751
EIGRP について 2753
EIGRP 詳細ダイアログボックス 2754
[Setup] タブ 2757
[フィルタルール（Filter Rules）] タブ 2760
[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックス 2761
[Neighbors] タブ 2762
[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス 2763
[Redistribution] タブ 2764
[EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックス 2766
[サマリーアドレス（Summary Address）] タブ 2768
[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックス 2769

[Interfaces] タブ 2770
[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックス 2771
ISIS の設定 2772
ISIS について 2773
[General] タブ 2773
[IPv4ファミリ（IPv4 Family）] タブ 2776
[IPv4ファミリ（IPv4 Family）] タブ：[全般（General）]タブ 2777
[IPv4ファミリ（IPv4 Family）] タブ：[SPF] タブ 2780
IPv4 ファミリータブ：再配布タブ 2781
[IPv6ファミリ（IPv6 Family）] タブ 2782
[IPv6ファミリ（IPv6 Family）] タブ：[全般（General）]タブ 2784
[IPv6ファミリ（IPv6 Family）] タブ：[SPF] タブ 2785
IPv6 ファミリータブ：再配布タブ 2786
IPv6 Familyタブ：サマリープレフィックス 2787
[Authentication] タブ 2788
リンクステートパケット タブ 2789
[サマリーアドレス（Summary Address）] タブ 2792
[ネットワーク エンティティ タイトル（Network Entity Title）] タブ 2793
[Interface] タブ 2794
[インターフェイス（Interface）] タブ：[全般（General）] タブ 2796
[インターフェイス（Interface）] タブ：[認証（Authentication）] タブ 2798
[インターフェイス（Interface）] タブ：[Helloパディング（Hello Padding）] タブ 2799
[インターフェイス（Interface）] タブ：[LSP設定（LSP Settings）] タブ 2801
[インターフェイス（Interface）] タブ：[メトリック（Metrics）] タブ 2801
[パッシブインターフェイス（Passive Interfaces）] タブ 2802
BFD ルーティングの設定 2803
BFD について 2803
BFD 非同期モードおよびエコー機能 2803
BFD セッション確立 2804
BFD タイマー ネゴシエーション 2806

BFD 障害検出 2807
BFD 導入シナリオ 2807
BFD テンプレートの作成 2808
[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックス 2810
[BFDインターフェイスの追加/編集（Add/Edit BFD Interface）] ダイアログボックス 2811
OSPF の設定 2812
OSPF について 2813
[General] タブ 2814
[OSPF Advanced] ダイアログボックス 2816
[Area] タブ 2823
[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス 2824
[Range] タブ 2826
[エリア範囲ネットワークの追加/編集（Add/Edit Area Range Network）] ダイアログボックス 2827
[Neighbors] タブ 2828
[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックス 2829
[Redistribution] タブ 2829
[Redistribution] ダイアログボックス 2831
[Virtual Link] タブ 2833
[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス 2834
[Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス 2837
[Filtering] タブ 2837
[Add Filtering]/[Edit Filtering] ダイアログボックス 2838
[フィルタルール（Filter Rule）] タブ 2840
[フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス 2841
[サマリーアドレス（Summary Address）] タブ 2842
[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス 2843
[Interface] タブ 2844
[Add Interface]/[Edit Interface] ダイアログボックス 2846
キーチェーンの設定 2849

キーのライフタイム 2850
キーチェーンの追加/編集 2850
OSPFv3 の設定 2853
OSPFv3 について 2854
[プロセス（Process）] タブ 2856
[OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス 2857
[エリア（Area）] タブ（OSPFv3） 2863
Add/Edit Redistribution Dialog Box（OSPFv3） 2869
[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3） 2871
[OSPFv3インターフェイス（OSPFv3 Interface）] タブ 2872
[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3） 2872
[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3） 2877
RIP の設定 2879
PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ 2881
[Add RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)]/[Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)] ダイアログボックス 2882
PIX/ASA 7.2 以降の RIP ページ 2883
[RIP] - [Setup] タブ 2884
RIP の [再配布（Redistribution）] タブ 2886
[RIP] - [Filtering] タブ 2888
[RIP] - [Interface] タブ 2890
スタティック ルートの設定 2891
[Add Static Route]/[Edit Static Route] ダイアログボックス 2893
[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス 2895
ASA ルーティング ポリシーのポリシーオブジェクトの設定 2896
ルートマップオブジェクトについて 2897
[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス 2901

[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス 2913

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス 2917

[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス 2919

[プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス 2920

[IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス 2923

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス 2924

[パス エントリとして追加または編集] ダイアログボックス 2926

[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス 2926

[コミュニティ リスト エントリの追加または編集] ダイアログボックス 2928

第 57 章 ファイアウォール デバイスのセキュリティ ポリシーの設定 2931

[一般（General）] ページ 2931

フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 2933

[Add/Edit General Security Configuration] ダイアログボックス 2934

タイムアウトの設定 2935

第 58 章 ファイアウォール デバイスでのサービス ポリシールールの設定 2941

サービス ポリシールールについて 2941

TCP ステート バイパスについて 2943

[Priority Queues] ページ 2944

[Priority Queue Configuration] ダイアログボックス 2945

[サービスポリシールール（Service Policy Rules）] ページ 2946

Insert/Edit Service Policy (MPC) Rule ウィザード 2948

手順 1：サービス ポリシーの設定 2948

手順 2：トラフィック クラスの設定 2949

手順 3：MPC アクションの設定 2950
ASA デバイスでの IPS モジュールについて 2961
ASA CX について 2963
ASA CX 認証プロキシの設定 2964
トラフィック フロー オブジェクトの設定 2965
デフォルト インスペクション トラフィック 2969
TCP マップの設定 2971
[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックス 2976

第 59 章 ファイアウォール デバイスでのセキュリティ コンテキストの設定 2979
マルチ コンテキスト モードのイネーブル化とディセーブル化 2980
マルチ セキュリティ コンテキストを設定するためのチェックリスト 2981
セキュリティ コンテキストの管理 2984
[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） 2986
[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） 2988
[Allocate Interfaces] ダイアログボックス（PIX/ASA だけ） 2991

第 60 章 ユーザー設定 2995
ファイアウォールデバイスでの展開設定の構成 2995
ファイアウォールデバイスでのトランザクション コミットの設定の構成 2996

第 VI 部： ルータおよびスイッチ デバイスの設定 2999

第 61 章 ルータの管理 3001
IOS ソフトウェア Release 12.1 および 12.2 を実行するルータの設定 3003
ルータ ポリシーの検出 3004

第 62 章 ルータインターフェイスの設定 3005
Cisco IOS ルータでの基本的なインターフェイス設定 3006
使用可能なインターフェイス タイプ 3006
基本的なルータ インターフェイス設定の定義 3009

Cisco IOS ルータ インターフェイスの削除 3011
[Router Interfaces] ページ 3012
[Create Router Interface] ダイアログボックス 3014
[Interface Auto Name Generator] ダイアログボックス 3020
Cisco IOS ルータでの高度なインターフェイス設定 3021
ヘルパー アドレスについて 3022
[Advanced Interface Settings] ページ 3024
[Advanced Interface Settings] ダイアログボックス 3025
Cisco IOS ルータでの IPS モジュール インターフェイス設定 3032
[IPS Module Interface Settings] ページ 3033
[IPS Monitoring Information] ダイアログボックス 3035
Cisco IOS ルータでの CEF インターフェイス設定 3036
[CEF Interface Settings] ページ 3037
[CEF Interface Settings] ダイアログボックス 3039
Cisco IOS ルータ上のダイヤラ インターフェイス 3040
ダイヤラ プロファイルの定義 3040
BRI インターフェイス プロパティの定義 3042
[Dialer Policy] ページ 3044
[Dialer Profile] ダイアログボックス 3045
[Dialer Physical Interface] ダイアログボックス 3046
Cisco IOS ルータでの ADSL 3049
サポートされる ADSL 動作モード 3050
ADSL 設定の定義 3051
[ADSL] ポリシー ページ 3053
[ADSL Settings] ダイアログボックス 3054
Cisco IOS ルータでの SHDSL 3057
SHDSL コントローラの定義 3058
[SHDSL] ポリシー ページ 3059
[SHDSL Controller] ダイアログボックス 3061
[Controller Auto Name Generator] ダイアログボックス 3064
Cisco IOS ルータでの PVC 3065

仮想パスおよび仮想チャネルについて 3066
ATM サービス クラスについて 3067
ATM 管理プロトコルについて 3068
ILMI について 3069
OAM について 3070
ATM PVC の定義 3071
ATM PVC での OAM 管理の定義 3074
[PVC] ポリシー ページ 3075
[PVC] ダイアログボックス 3077
[PVC] ダイアログボックス - [Settings] タブ 3079
[PVC] ダイアログボックス - [QoS] タブ 3082
[PVC] ダイアログボックス - [Protocol] タブ 3086
[Define Mapping] ダイアログボックス 3087
[PVC Advanced Settings] ダイアログボックス 3088
[PVC Advanced Settings] ダイアログボックス - [OAM] タブ 3089
[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ 3092
Cisco IOS ルータでの PPP 3094
マルチリンク PPP（MLP）について 3095
PPP 接続の定義 3096
マルチリンク PPP バンドルの定義 3099
[PPP/MLP] ポリシー ページ 3100
[PPP] ダイアログボックス 3102
[PPP] ダイアログボックス - [PPP] タブ 3104
[PPP] ダイアログボックス - [MLP] タブ 3107

第 63 章 ルータ デバイス管理 3113
Cisco IOS ルータにおける AAA 3114
サポートされる認可タイプ 3115
サポートされるアカウンティング タイプ 3115
方式リストについて 3116
AAA サービスの定義 3117

[AAA] ポリシー ページ 3119
[AAA] ページ - [Authentication] タブ 3120
[AAA] ページ - [Authorization] タブ 3121
[Command Authorization] ダイアログボックス 3123
[AAA] ページ - [Accounting] タブ 3124
[Command Accounting] ダイアログボックス 3127
Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル 3129
アカウントおよびクレデンシャル ポリシーの定義 3130
[アカウントおよびログイン情報ポリシー（Accounts and Credentials Policy）] ページ 3132
[User Account] ダイアログボックス 3134
Cisco IOS ルータにおけるブリッジング 3135
ブリッジ グループ仮想インターフェイス 3136
ブリッジ グループの定義 3137
[Bridging] ポリシー ページ 3139
[Bridge Group] ダイアログボックス 3140
Cisco IOS ルータにおけるタイム ゾーン設定 3141
タイム ゾーンと DST 設定の定義 3141
[Clock] ポリシー ページ 3142
Cisco IOS ルータにおける CPU 使用率設定 3145
CPU 使用率設定の定義 3145
[CPU] ポリシー ページ 3146
Cisco IOS ルータにおける HTTP と HTTPS 3149
HTTP ポリシーの定義 3149
[HTTP] ポリシー ページ 3152
[HTTP] ページ - [Setup] タブ 3152
[HTTP] ページ - [AAA] タブ 3154
[Command Authorization Override] ダイアログボックス 3156
Cisco IOS ルータにおける回線アクセス 3157
コンソール ポートの設定パラメータの定義 3158
コンソール ポートの AAA 設定の定義 3159
VTY 回線の設定パラメータの定義 3161

VTY 回線の AAA 設定の定義 3164
[Console] ポリシー ページ 3165
[Console] ページ - [Setup] タブ 3166
[Console] ページ - [Authentication] タブ 3168
[Console] ページ - [Authorization] タブ 3170
[Console] ページ - [Accounting] タブ 3172
[VTY] ポリシー ページ 3177
[VTY Line] ダイアログボックス 3178
[VTY Line] ダイアログボックス - [Setup] タブ 3179
[VTY Line] ダイアログボックス - [Authentication] タブ 3182
[VTY Line] ダイアログボックス - [Authorization] タブ 3184
[VTY Line] ダイアログボックス - [Accounting] タブ 3186
[Command Authorization] ダイアログボックス - [Line Access] 3191
[Command Accounting] ダイアログボックス - [Line Access] 3192
Cisco IOS ルータにおける任意の SSH 設定 3194
任意の SSH 設定の定義 3194
[Secure Shell] ポリシー ページ 3196
Cisco IOS ルータの SNMP 3198
SNMP エージェントのプロパティの定義 3199
SNMP トラップの有効化 3200
[SNMP] ポリシー ページ 3201
[Permission] ダイアログボックス 3203
[Trap Receiver] ダイアログボックス 3204
[SNMP Traps] ダイアログボックス 3206
Cisco IOS ルータにおける DNS 3208
DNS ポリシーの定義 3209
[DNS] ポリシー ページ 3210
[IP Host] ダイアログボックス 3211
Cisco IOS ルータにおけるホスト名とドメイン名 3212
ホスト名ポリシーの定義 3212
[Hostname] ポリシー ページ 3213

Cisco IOS ルータにおけるメモリ設定 3214
ルータのメモリ設定の定義 3214
[Memory] ポリシー ページ 3215
Cisco IOS ルータにおけるセキュア デバイス プロビジョニング 3217
ブートストラップ設定の内容 3218
セキュア デバイス プロビジョニングのワークフロー 3219
セキュア デバイス プロビジョニング ポリシーの定義 3219
管理イントロデューサの AAA サーバ グループの設定 3221
[Secure Device Provisioning] ポリシー ページ 3222
Cisco IOS ルータにおける DHCP 3224
DHCP データベース エージェントについて 3225
DHCP リレーエージェントについて 3226
DHCP Option 82 について 3226
Secured ARP について 3227
DHCP ポリシーの定義 3228
DHCP アドレス プールの定義 3229
[DHCP] ポリシー ページ 3230
[DHCP Database] ダイアログボックス 3233
[IP Pool] ダイアログボックス 3234
Cisco IOS ルータにおける NTP 3237
NTP サーバの定義 3237
[NTP Policy] ページ 3239
[NTP Server] ダイアログボックス 3241

第 64 章 アイデンティティ ポリシーの設定 3243
Cisco IOS ルータでの 802.1x 3244
802.1x デバイス ロールについて 3245
802.1x インターフェイス認可状態 3245
802.1x でサポートされるトポロジ 3246
802.1x ポリシーの定義 3247
[802.1x] ポリシー ページ 3249

Cisco IOS ルータでのネットワーク アドミッション コントロール 3252
NAC をサポートするルータ プラットフォーム 3253
NAC コンポーネントについて 3254
NAC システム フローについて 3254
NAC 設定パラメータの定義 3255
NAC インターフェイス パラメータの定義 3257
NAC アイデンティティ パラメータの定義 3258
[Network Admission Control Policy] ページ 3260
[Network Admission Control] ページ - [Setup] タブ 3261
[Network Admission Control] ページ - [Interfaces] タブ 3263
[NAC Interface Configuration] ダイアログボックス 3264
[Network Admission Control] ページ - [Identities] タブ 3265
[NAC Identity Profile] ダイアログボックス 3266
[NAC Identity Action] ダイアログボックス 3267

第 65 章 ロギング ポリシーの設定 3269
Cisco IOS ルータにおけるロギング 3269
Syslog ロギングの設定パラメータの定義 3270
Syslog サーバの定義 3272
ログ メッセージの重大度について 3273
Cisco IOS ルータにおける NetFlow 3274
NetFlow パラメータの定義 3275
Syslog ロギングの設定ポリシーのページ 3278
Syslog サーバ ポリシーのページ 3282
[Syslog Server] ダイアログボックス 3283
NetFlow ポリシー ページ 3284
NetFlow インターフェイス設定の追加および編集 3287

第 66 章 Quality of Service の設定 3289
Cisco IOS ルータにおける Quality of Service 3289
uality of Service と CEF 3290

マッチング パラメータについて 3291
マーキング パラメータについて 3291
キューイング パラメータについて 3293
テール ドロップと WRED 3294
低遅延キューイング 3295
デフォルト クラス キューイング 3295
ポリシング パラメータとシェーピング パラメータについて 3296
トークン バケット メカニズムについて 3297
コントロール プレーン ポリシングについて 3299
QoS ポリシーの定義 3300
インターフェイスでの QoS の定義 3301
コントロール プレーンでの QoS の定義 3303
QoS クラスのマッチング パラメータの定義 3305
QoS クラスのマーキング パラメータの定義 3307
QoS クラスのキューイング パラメータの定義 3308
QoS クラスのポリシング パラメータの定義 3309
QoS クラスのシェーピング パラメータの定義 3311
サービス品質ポリシーページ 3312
[QoS Policy] ダイアログボックス 3314
[QoS Class] ダイアログボックス 3316
[QoS Class] ダイアログボックス - [Matching] タブ 3318
[Edit ACLs] ダイアログボックス - QoS クラス 3320
[QoS Class] ダイアログボックス - [Marking] タブ 3321
[QoS Class] ダイアログボックス - [Queuing and Congestion Avoidance] タブ 3322
[QoS Class] ダイアログボックス - [Policing] タブ 3325
[QoS Class] ダイアログボックス - [Shaping] タブ 3327

第 67 章 ルーティング ポリシーの設定 3331
Cisco IOS ルータにおける BGP ルーティング 3331
BGP ルートの定義 3332
BGP へのルートの再配布 3334

[BGP] ルーティング ポリシー ページ 3335
[BGP] ページ - [Setup] タブ 3336
[Neighbors] ダイアログボックス 3337
[BGP] ページ - [Redistribution] タブ 3338
[BGP Redistribution Mapping] ダイアログボックス 3339
Cisco IOS ルータにおける EIGRP ルーティング 3340
EIGRP ルートの定義 3342
EIGRP インターフェイスのプロパティの定義 3343
EIGRP へのルートの再配布 3345
[EIGRP] ルーティング ポリシー ページ 3346
[EIGRP] ページ : [セットアップ（Setup）] タブ 3347
[EIGRPのセットアップ（EIGRP Setup）] ダイアログボックス 3348
[EIGRP] ページ : [インターフェイス（Interfaces）] タブ 3349
[EIGRP Interface] ダイアログボックス 3350
[EIGRP] ページ - [Redistribution] タブ 3351
[EIGRP再配布マッピング（EIGRP Redistribution Mapping）] ダイアログボックス 3353
Cisco IOS ルータにおける OSPF ルーティング 3355
OSPF プロセス設定の定義 3355
OSPF エリア設定の定義 3356
OSPF へのルートの再配布 3358
OSPF 再配布マッピングの定義 3358
OSPF 最大プレフィックス値の定義 3360
OSPF インターフェイス設定の定義 3361
インターフェイス コストについて 3363
インターフェイス プライオリティについて 3363
MTU 不一致検出のディセーブル化 3364
LSA フラッディングのブロック 3365
OSPF タイマー設定について 3365
OSPF ネットワーク タイプについて 3366
OSPF インターフェイス認証について 3367
[OSPF Interface] ポリシー ページ 3368

[OSPF Interface] ダイアログボックス 3370
[OSPF Process] ポリシー ページ 3374
[OSPF Process] ページ - [Setup] タブ 3375
[OSPF Setup] ダイアログボックス 3376
[Edit Interfaces] ダイアログボックス - OSPF 受動インターフェイス 3377
[OSPF Process] ページ - [Area] タブ 3377
[OSPF Area] ダイアログボックス 3378
[OSPF Process] ページ - [Redistribution] タブ 3379
[OSPF Redistribution Mapping] ダイアログボックス 3381
[OSPF Max Prefix Mapping] ダイアログボックス 3383
Cisco IOS ルータにおける RIP ルーティング 3384
RIP 設定パラメータの定義 3385
RIP インターフェイス認証設定の定義 3386
RIP へのルートの再配布 3387
[RIP] ルーティング ポリシー ページ 3388
[RIP] ページ - [Setup] タブ 3389
[RIP] ページ - [Authentication] タブ 3390
[RIP Authentication] ダイアログボックス 3391
[RIP] ページ - [Redistribution] タブ 3392
[RIP Redistribution Mapping] ダイアログボックス 3393
Cisco IOS ルータにおけるスタティック ルーティング 3394
スタティック ルートの定義 3395
[Static Routing] ポリシー ページ 3396
[Static Routing] ダイアログボックス 3398

第 68 章 **Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理 3401**
Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出 3402
Catalyst サマリー情報の表示 3403
Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 3404
インターフェイス 3406
Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集 3407

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除 3409
[Interfaces/VLANs] ページ - [Interfaces] タブ 3410
[Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード 3412
[Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード 3417
[Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード 3420
[Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード 3426
[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス 3431
[Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード 3433
VLANs 3436
VLAN の作成または編集 3436
VLAN の削除 3438
[Interfaces/VLANs] ページ - [VLANs] タブ 3438
[Create VLAN]/[Edit VLAN] ダイアログボックス 3440
[Access Port Selector] ダイアログボックス 3442
[Trunk Port Selector] ダイアログボックス 3443
VLAN グループ 3444
VLAN グループの作成または編集 3444
VLAN グループの削除 3446
[Interfaces/VLANs] ページ - [VLAN Groups] タブ 3446
[Create VLAN Group]/[Edit VLAN Group] ダイアログボックス 3447
[Service Module Slot Selector] ダイアログボックス 3448
[VLAN Selector] ダイアログボックス 3449
VLAN ACL（VACL） 3450
VACL の作成または編集 3451
VACL の削除 3453
[VLAN Access Lists] ページ 3454
[Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス 3456
[Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス 3457
IDSM 設定 3459
EtherChannel VLAN 定義の作成または編集 3460
EtherChannel VLAN 定義の削除 3462

データ ポート VLAN 定義の作成または編集 3463
データ ポート VLAN 定義の削除 3464
[IDSM Settings] ページ 3465
[Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス 3467
[Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス 3468

第 VII 部： モニタリング、レポート、および診断 3471

第 69 章 イベントの表示 3473
Event Viewer 機能の概要 3473
履歴ビュー 3474
リアルタイム ビュー 3475
ビューとフィルタ 3475
ポリシーのナビゲーション 3476
Event Viewer のアクセス コントロールについて 3477
Event Viewer のスコープおよび制限 3478
詳細に解析される Syslog 3479
Event Viewer の概要 3481
Event Viewer の [File] メニュー 3484
Event Viewer の [View] メニュー 3485
ビューリスト 3487
[Event Monitoring] ウィンドウ 3489
イベント テーブル ツールバー 3491
イベント テーブルのカラム 3494
時間スライダ 3504
[Event Details] ペイン 3505
イベント管理の準備 3506
時間の同期 3506
イベント管理のための ASA と FWSM デバイスの設定 3506
イベント管理のための IPS デバイスの設定 3508

Event Manager サービスの管理 3509
Event Manager サービスの開始、停止、および設定 3509
Event Manager サービスのモニタリング 3511
モニタするデバイスの選択 3514
イベント データ ストア用のディスク スペースの使用率のモニタリング 3516
イベント データ ストアのアーカイブまたはバックアップと復元 3516
イベントビューアの使用 3518
イベント ビューの使用方法 3518
ビューを開く 3519
ビューのフローティングと配置 3519
イベント テーブルの表示のカスタマイズ 3520
送信元/宛先 IP アドレスとホスト オブジェクト名間の切り替え 3521
ビューの色ルールの設定 3522
カスタム ビューの作成 3523
カスタム ビューの名前または説明の編集 3524
リアルタイム ビューと履歴ビュー間の切り替え 3524
ビューの保存 3525
カスタム ビューの削除 3525
イベントのフィルタリングおよびクエリー 3526
イベントの時間範囲の選択 3526
フィルタリングと時間スライダの使用方法 3527
イベント テーブルのリフレッシュ 3528
カラムベース フィルタの作成 3528
特定のイベントの値に基づいたフィルタリング 3531
テキスト文字列に対するフィルタリング 3532
フィルタのクリア 3533
特定のイベントに対する操作の実行 3534
イベント コンテキスト（右クリック）メニュー 3534
IPS シグネチャ クイック チューン ダイアログボックス 3538
単一のイベントの詳細の参照 3539
イベント レコードのコピー 3540

ファイルへのイベントの保存 3540
Event Viewer からの Security Manager ポリシーの検索 3541
Looking Up Events for a Cisco Security Manager Policy 3543
アクセスルールのイベントの表示 3543
IPS シグニチャのイベントの表示 3545
HPM デバイスとサイト間 VPN のイベントの表示 3546
イベント分析の例 3547
ヘルプ デスク：サーバへのユーザ アクセスがファイアウォールでブロックされている 3547
ボットネット アクティビティのモニタリングと軽減 3550
対処可能なイベントであることを示す syslog メッセージについて 3550
Security Manager の Event Viewer を使用したボットネットのモニタリング 3551
Security Manager の Report Manager を使用したボットネットのモニタリング 3553
Adaptive Security Device Manager（ASDM）を使用したボットネット アクティビティのモニタリング 3554
ボットネット トラフィックの軽減 3555
イベント テーブルからの false positive IPS イベントの削除 3557

第 70 章 レポートの管理 3561
レポート管理について 3561
Security Manager で使用可能なレポートのタイプについて 3562
Report Manager レポート用のデバイスの準備 3564
Report Manager データ集約について 3565
Report Manager のアクセス コントロールについて 3567
Report Manager の概要 3568
Report Manager のメニュー 3571
Report Manager のレポート リストについて 3572
レポート設定ペインについて 3573
生成済みレポート ペインおよびツールバーについて 3575
Report Manager の事前定義システム レポートについて 3578
ファイアウォール トラフィック レポートについて 3578
ファイアウォール サマリー ボットネット レポートについて 3579

VPN 上位レポートについて 3580
全般 VPN レポートについて 3581
IPS 上位レポートについて 3583
全般 IPS レポートについて 3585
Report Manager でのレポートの使用 3585
レポートの起動と生成 3586
カスタム レポートの作成 3588
レポート設定の編集 3589
レポートデータへのドリルダウン 3593
レポートの印刷 3595
レポートのエクスポート 3596
レポートのデフォルト設定値の設定 3598
レポート ウィンドウの配置 3599
レポートの保存 3600
レポートの名前変更 3601
レポート ウィンドウの終了 3601
レポートの削除 3602
カスタム レポートの管理 3602
レポートのスケジュール設定 3603
レポート スケジュールの表示 3603
レポート スケジュールの設定 3604
スケジューリングされたレポートの結果の表示 3605
レポート スケジュールのイネーブル化およびディセーブル化 3606
レポート スケジュールの削除 3607
Report Manager のトラブルシューティング 3607

第 71 章 ヘルスとパフォーマンスのモニタリング 3611
Health and Performance Monitor の概要 3611
トレンド情報 3612
マルチコンテキストのモニタリング 3613
HPM アクセス制御 3614

正常性とパフォーマンスのモニタリングの準備 3615
Health and Performance Monitor の起動 3616
監視対象デバイスの管理 3616
HPM ウィンドウ 3617
テーブル列の操作 3619
テーブル列の表示と非表示 3620
列ベースのフィルタリング 3632
リストフィルターフィールドの使用 3635
デバイスのモニタリング 3637
デバイスビューの管理 3637
ビュー：開閉 3639
ビュー：水平または垂直方向に並べて表示 3640
ビュー：フローティングとドッキング 3641
ビュー：カスタム 3641
[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ 3642
モニタリングビュー：デバイスまたは VPN サマリー 3644
モニタリングビュー：デバイスまたは VPN ステータスリスト 3645
モニタリングビュー：デバイスまたは VPN の詳細 3646
モニタリングビュー：VPN、RA および S2S 3649
HPM データのエクスポート 3650
アラートと通知 3651
HPM ウィンドウ：アラートディスプレイ 3652
アラート：設定 3654
アラート設定：IPS 3656
アラート設定：ファイアウォール 3658
アラート設定：VPN 3660
アラート：表示 3663
アラート：確認応答とクリア 3664
アラート：履歴 3665
SNMP トラップ転送通知 3666
[SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックス 3668

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックス 3669

第 72 章 外部モニタリング、トラブルシューティング、および診断ツールの使用方法 3673

ダッシュボードの概要 3674

CSM Mobile 3692

インベントリ ステータスの表示 3694

[Inventory Status] ウィンドウ 3695

デバイス マネージャの起動 3697

デバイス マネージャのトラブルシューティング 3699

デバイス マネージャからのアクセス ルールの検索 3701

ASDM からアクセス ルールへのナビゲート 3702

SDM からアクセス ルールへのナビゲート 3704

Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 3705

ASA CX モジュールおよび FirePOWER モジュールの検出 3707

PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有 3708

Packet Tracer を使用した ASA または PIX の設定の分析 3709

ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析 3713

ping を使用した設定の分析 3714

TraceRoute を使用した設定の分析 3716

NS ルックアップを使用した設定の分析 3718

Packet Capture Wizard の使用 3718

IPインテリジェンス（IP Intelligence） 3723

CS-MARS と Security Manager の統合 3727

CS-MARS と Security Manager を統合するためのチェックリスト 3728

CS-MARS ポリシー クエリーに応答するための Security Manager サーバの設定 3729

Security Manager での CS-MARS サーバの登録 3730

デバイスの CS-MARS コントローラの検出または変更 3731

CS-MARS クエリーのトラブルシューティングに関するヒント 3732

Security Manager ポリシーの CS-MARS イベントの検索 3734

アクセス ルールの CS-MARS イベントの表示 3735

IPS シグニチャの CS-MARS イベントの表示 3738
CS-MARS イベントからの Security Manager ポリシーの検索 3740
ポリシー検索に対してサポートされるシステム ログ メッセージ 3741
CS-MARS での NetFlow イベント レポート 3743

第 VIII 部： イメージ管理 3747

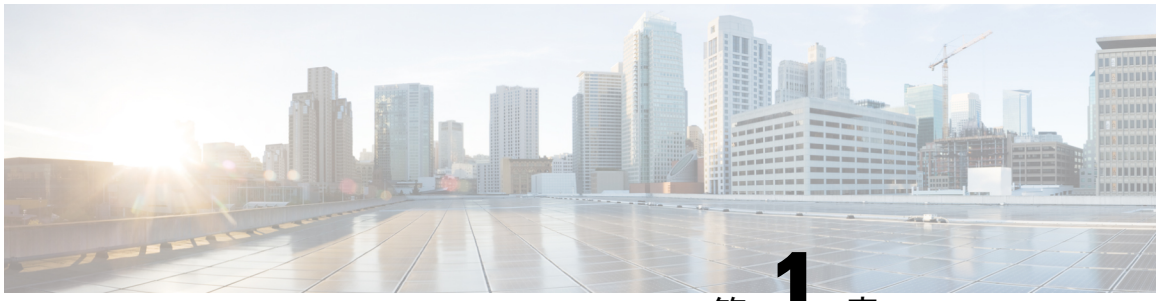
第 73 章 Image Manager の使用 3749
イメージ マネージャの使用開始 3749
Image Manager のサポートされるプラットフォームおよびバージョン 3750
Image Manager によってサポートされるデバイス設定 3753
マルチコンテキスト ASA のイメージ管理 3754
Image Manager でサポートされるイメージタイプ 3754
Image Manager での管理設定 3756
Image Manager 用のデバイスのブートストラップ 3758
イメージの操作 3759
すべてのイメージの表示 3760
イメージのリポジトリへのダウンロード 3762
バンドルの操作 3764
バンドルの作成 3765
バンドル別のイメージの表示 3766
バンドルの名前変更 3766
バンドルの削除 3767
バンドルからのイメージの削除 3767
デバイスの使用 3767
デバイス インベントリの表示 3768
デバイス上のイメージの管理 3770
デバイスメモリの表示 3771
イメージのインストール場所の設定 3772
Image Manager を使用したデバイスでのイメージの更新について 3773
デバイスで提案されたイメージの更新を検証する 3777

Image Installation ウィザードを使用してデバイスにイメージをインストールする 3780
バンドルされたイメージをデバイスにインストールする 3786
互換性のあるイメージのデバイスへのインストール 3786
選択したデバイスにイメージをインストールする 3788
ジョブの操作 3789
イメージインストールジョブの概要の表示 3789
インストールジョブの表示 3790
イメージインストールジョブの中止 3791
失敗したイメージインストールジョブの再試行 3791
展開されたジョブをロールバックする 3792
イメージインストールジョブの承認ワークフロー 3793
イメージ管理のトラブルシューティング 3794

第 部

Security Manager の基本的な使用方法

- Getting Started With Cisco Security Manager （1 ページ）
- デバイスを管理するための準備 （71 ページ）
- デバイス インベントリの管理 （87 ページ）
- アクティビティの管理 （177 ページ）
- ポリシーの管理 （209 ページ）
- ポリシー オブジェクトの管理 （287 ページ）
- FlexConfig の管理 （431 ページ）
- 展開の管理 （481 ページ）
- デバイス通信および展開のトラブルシューティング （573 ページ）
- Cisco Security Manager サーバーの管理 （599 ページ）
- Security Manager の管理設定値の設定 （641 ページ）



第 1 章

Getting Started With Cisco Security Manager

- 製品の概要　（1 ページ）
- Security Manager へのログインおよび終了　（14 ページ）
- Configuration Manager の使用方法 - 概要　（18 ページ）
- JumpStart を使用した Security Manager の理解　（32 ページ）
- Security Manager の初期設定の実行　（32 ページ）
- Security Manager インターフェイスの基本機能について　（38 ページ）
- オンライン ヘルプの利用方法　（70 ページ）

製品の概要

（注）　バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および次のデバイスを含む Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

- Cisco Catalyst 6500 および 7600 シリーズ ファイアウォール サービス モジュール（EOL8184）
- Cisco Catalyst 6500 シリーズ Intrusion Detection System サービスモジュール 2（EOL8843）
- Cisco Intrusion Prevention System：IPS 4200、4300、および 4500 シリーズ センサー（EOL9916）
- Cisco SR 500 シリーズ Secure Router（EOL7687、EOL7657）
- PIX ファイアウォール（EOL）

注意 バージョン 4.18 以降、Cisco Security Manager では、ASA 5512、ASA 5506、ASA 5506H、および ASA 5506W モデルの ASA 9.10(1) 以降の SFR はサポートされないため、Image Manager を介して 9.10(1) にアップグレードすると、既存の SFR 設定が失われます。

Cisco Security Manager（Security Manager）を使用すると、シスコ セキュリティ デバイスのセキュリティ ポリシーを管理できます。Cisco Security Manager では、複数の ASA セキュリティ アプライアンス間でのファイアウォール、およびVPN（サイト間、リモートアクセス、および SSL）サービスの統合的なプロビジョニングがサポートされています。

Cisco Security Manager でサポートされるデバイスおよび OS バージョンの一覧については、Cisco.com で Cisco Security Manager のサポート対象デバイスとソフトウェアバージョン [英語] を参照してください。

Security Manager では、インターフェイス、ルーティング、ID、QoS、ロギングなど、さまざまなプラットフォーム固有の設定のプロビジョニングもサポートしています。

Security Manager は、数台のデバイスで構成される小規模ネットワークから、数千台のデバイスで構成される大規模ネットワークまで、広範囲のネットワークを効率的に管理します。共有可能なオブジェクトおよびポリシーの持つ豊富なフィーチャセットと、デバイスのグループ化機能により、スケーラビリティが実現されます。

Security Manager では、さまざまなタスク フローと使用例に基づいて最適化された、複数の設定ビューをサポートしています。

ここでは、Security Manager の概要について説明します。

- Cisco Security Manager の主な利点　（2 ページ）
- Security Manager のポリシー フィーチャ セット　（5 ページ）
- Security Manager アプリケーションの概要　（8 ページ）
- デバイス モニタリングの概要　（9 ページ）
- Security Manager での IPv6 サポート　（11 ページ）

Cisco Security Manager の主な利点

Security Manager を使用する主な利点は、次のとおりです。

- **スケーラブルなネットワーク管理**：小規模ネットワーク、または数千台のデバイスで構成される大規模ネットワークのセキュリティポリシーとデバイス設定を集中管理します。ポリシーおよび設定は、定義したあとに、必要に応じて個別のデバイス、デバイスのグループ、または企業内のすべてのデバイスに割り当てます。
- **異なるプラットフォームにまたがる複数のセキュリティテクノロジーのプロビジョニング**：ルータ、セキュリティアプライアンス、Catalyst デバイスとサービスモジュール、およびIPSデバイス上のVPN、ファイアウォール、およびIPSテクノロジーを管理します。

- **プラットフォーム固有の設定およびポリシーのプロビジョニング**：特定のデバイスタイプでのプラットフォーム固有の設定を管理します。たとえば、ルータでのルーティング、802.1x、EzSDD、ネットワーク アドミッション コントロールや、ファイアウォール デバイスでのデバイス アクセス セキュリティ、DHCP、AAA、マルチキャストなどがあります。
- **VPN ウィザード**：異なる VPN デバイスタイプにわたってポイントツーポイント VPN、ハブアンドスポーク VPN、完全メッシュ、およびエクストラネット サイト間 VPN をすばやく簡単に設定します。ASA、IOS、および PIX デバイスでリモート アクセス IPsec および SSL VPN をすばやく簡単に設定します。
- **複数の管理ビュー**：デバイスビュー、ポリシービュー、およびマップビューを使用することにより、ニーズに最も適した環境でセキュリティを管理できます。
- **再利用可能なポリシーオブジェクト**：ネットワークアドレス、デバイス設定、VPN パラメータなどを表す、再利用可能なオブジェクトを作成します。作成後は、手動で値を入力する代わりに、このオブジェクトを使用します。
- **デバイスのグループ化機能**：組織構造を表すデバイスグループを作成します。グループ内のすべてのデバイスを同時に管理します。
- **ポリシー継承**：必須ポリシーおよび組織の下層に適用するポリシーを一元的に指定します。
- **ロールベースの管理**：複数のオペレータに対する適切なアクセスコントロールが可能です。
- **ワークフロー**：（任意）ネットワークオペレータとセキュリティオペレータの間で責務分担と作業負荷分散が可能となり、変更管理の承認とトラッキングメカニズムを実現します。
- **チケット管理**：チケット ID をポリシーの変更に関連付け、それらの変更に関するコメントを簡単に追加および更新し、Security Manager から外部の変更管理システムにすばやく移動します。
- **単一で一貫性のあるユーザインターフェイスによる共通ファイアウォール機能の管理**：すべてのプラットフォーム（ルータ、PIX、ASA、および FWSM）に対応した単一のルールテーブル。
- **イメージ管理**：ASA デバイス用の完全なイメージ管理。イメージリポジトリのダウンロードと保守、イメージの評価、アップグレードの影響の分析、信頼性が高く安定したデバイスアップグレードの準備と計画、十分なフォールバックと回復メカニズムの確保によって、デバイスのイメージアップグレードのすべての段階を容易にします。
- **ファイアウォールポリシーのインテリジェントな分析**：競合検出機能を使用して、他のルールと重複または競合するルールを分析およびレポートします。ACL ヒット カウント機能により、パケットが特定のルールに一致したか、または特定のルールがトリガーされたかどうかがリアルタイムでチェックされます。

- **ルールテーブルの高度な編集**：インライン編集、ルールのカット、コピー、およびペースト機能とルールテーブル内でのルールの順序変更。
- **デバイスからのファイアウォールポリシー検出**：デバイス上に存在するポリシーを Security Manager にインポートし、あとで管理することができます。
- **柔軟性のある展開オプション**：デバイスに設定を直接展開する方法と設定ファイルに展開する方法をサポートします。Auto-Update Server（AUS）、Configuration Engine、または Token Management Server（TMS）を使用して、展開することもできます。
- **ロールバック**：必要に応じて以前の設定にロールバックすることができます。
- **FlexConfig（テンプレートマネージャ）**：デバイスで使用可能な機能を管理するためのインテリジェントな CLI configlet エディタ。ただし、Security Manager では、ネイティブにはサポートしていません。
- **統合されたデバイスモニタリングとレポート**：IPS、ASA、および FWSM デバイスでイベントをモニターし、関連する設定ポリシーにこれらのイベントを関連付けて、セキュリティレポートと使用状況レポートを作成するための機能。これらの機能には、次のスタンドアロン Security Manager アプリケーションが含まれます。
  - **Event Viewer**：Event Viewer は、ASA および FWSM デバイス、ならびにセキュリティコンテキストからのシステムログ（syslog）イベント、ならびに IPS デバイスおよび仮想センサーからの SDEE イベントを対象にネットワークをモニターします。Event Viewer は、これらのイベントを収集し、収集したイベントを表示し、グループ化し、その詳細をほぼリアルタイムで調べるためのインターフェイスを備えています。
  - **Report Manager**：Report Manager を使用すると、ASA および IPS デバイス、および ASA がホストするリモートアクセス IPsec および SSL VPN に関するさまざまなネットワーク使用状況とセキュリティ情報を収集、表示、およびエクスポートできます。これらのレポートは、上位の送信元、宛先、攻撃者、攻撃対象などのセキュリティデータと、上位の帯域幅、期間、スループットユーザなどのセキュリティ情報を集計します。データは、時間、日、および月の期間で利用できます。（Report Manager は、Event Manager サービスによってモニターされるデバイスから収集される情報を集約します。このため、デバイスに関するレポートを表示するには、Event Viewer で該当デバイスをモニタリングしている必要があります）

（注） Event Viewer は FWSM を処理しますが、Report Manager は FWSM イベントについては報告しません。

- **Health and Performance Monitor**：Health and Performance Monitor（HPM）は、モニター対象の ASA デバイス、IPS デバイス、および ASA がホストする VPN サービスを、正常性およびパフォーマンスデータについて定期的にポーリングします。これらのデータには、メモリ使用量、インターフェイスステータス、ドロップされたパケット、トンネルステータスなど、重大な問題、および重大ではない問題が含まれます。この情報は、アラートの生

成と電子メール通知に使用され、時間単位、日単位、および週単位で利用可能な集計データに基づいて傾向を表示します。

（注） Health and Performance Monitor は、FWSM デバイスをモニターしません。

- **ダッシュボード**：ダッシュボードは、IPS と FW タスクをより便利にする Cisco Security Manager で設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要 （3674 ページ）を参照してください。

追加機能を使用すると、Cisco Security Monitoring, Analysis and Response System（CS-MARS）、Cisco Performance Monitor、および ASDM（Security Manager に含まれる機能の読み取り専用バージョン）などのデバイスマネージャを含め、関連の深い他のアプリケーションを使用して、Security Manager からデバイスをモニターできます。

Security Manager のポリシー フィーチャ セット

Security Manager には、主に次のような設定ポリシーのフィーチャ セットが用意されています。

ファイアウォール サービス

IOS ルータ、ASA/PIX デバイス、Catalyst ファイアウォール サービス モジュール（FWSM）など、複数のプラットフォームにまたがるファイアウォールポリシーの設定および管理です。次の機能が含まれています。

- アクセス コントロール ルール：IPv4 と IPv6 の両方のトラフィックに関するアクセス コントロール リストを使用して、インターフェイス上のトラフィックを許可または拒否する。
- ボットネット トラフィック フィルタ ルール：（ASA のみ）。既知のマルウェアサイトに基づいてトラフィックをフィルタ処理し、必要に応じて脅威レベルに基づいてトラフィックをドロップします。
- インスペクション ルール：アプリケーション レイヤ プロトコルのセッション情報に基づいて、TCP パケットおよび UDP パケットをフィルタリングする。
- AAA/認証プロキシ ルール：HTTP、HTTPS、FTP、または Telnet のセッションを経由してネットワークにログインする、またはインターネットにアクセスするユーザの認証と認可に基づいて、トラフィックをフィルタリングする。
- Web フィルタリング ルール：Websense などの URL フィルタリング ソフトウェアを使用して、特定の Web サイトへのアクセスを拒否する。

- ScanSafe Web セキュリティ：（ルータのみ）。コンテンツスキャンおよびマルウェア保護サービスのために、HTTP/HTTPS トラフィックを ScanSafe Web セキュリティセンターにリダイレクトします。
- トランスペアレント ファイアウォール ルール：トランスペアレントなインターフェイスまたはブリッジングされたインターフェイス上で、レイヤ 2 トラフィックをフィルタリングする。
- ゾーンベースのファイアウォール ルール：個々のインターフェイスではなく、ゾーンに基づいて、アクセル ルール、インスペクション ルール、および Web フィルタリング ルールを設定する。

詳細については、ファイアウォール サービスの概要 （755 ページ）を参照してください。

サイト間 VPN

IPsec サイト間 VPN のセットアップと設定です。IOS ルータ、PIX/ASA デバイス、Catalyst VPN サービス モジュールなど、複数のデバイス タイプが単一の VPN に参加できます。サポートされる VPN トポロジは、次のとおりです。

- ポイントツーポイント
- ハブアンドスポーク
- 完全メッシュ
- エクストラネット（管理対象外デバイスへのポイントツーポイント接続）

サポートされる IPsec テクノロジーは、次のとおりです。

- 通常の IPsec
- GRE
- GRE ダイナミック IP
- DMVPN
- Easy VPN
- GET VPN

詳細については、サイト間 VPN の管理：基本 （1379 ページ）を参照してください。

リモートアクセス VPN

サーバと、Cisco VPN Client または AnyConnect クライアント ソフトウェアが稼働しているモバイル リモート ワークステーション間の IPsec および SSL VPN のセットアップと設定です。詳細については、リモート アクセス VPN の管理の基礎 （1655 ページ）を参照してください。

侵入防御システム（IPS）管理

Cisco IPS センサー（アプライアンスとサービス モジュール）および IOS IPS デバイス（IPS 対応イメージ搭載の Cisco IOS ルータと Cisco サービス統合型ルータ）の管理および設定です。

詳細については、IPS 設定の概要 （2088 ページ）および Cisco IOS IPS 設定の概要 （2318 ページ）を参照してください。

ファイアウォール デバイス（PIX/ASA/FWSM）固有の機能

プラットフォーム固有の高度な機能の設定、および PIX/ASA デバイスと Catalyst FWSM の設定です。これらの機能は、セキュリティ プロファイルを管理するときに付加価値を提供し、次のものを含みます。

- インターフェイス コンフィギュレーション
- ID 認証ファイアウォール設定
- デバイス管理設定
- セキュリティ
- ルーティング
- マルチキャスト
- ログ
- NAT
- ブリッジング
- フェールオーバー
- セキュリティ コンテキスト

詳細については、ファイアウォール デバイスの管理 （2331 ページ）を参照してください。

IOS ルータ固有の機能

プラットフォーム固有の高度な機能の設定、および IOS ルータの設定です。これらの機能は、セキュリティ プロファイルを管理するときに付加価値を提供し、次のものを含みます。

- インターフェイス コンフィギュレーション
- ルーティング
- NAT
- 802.1x
- NAC
- QoS
- ダイヤラ インターフェイス
- セキュア デバイス プロビジョニング

詳細については、ルータの管理 （3001 ページ）を参照してください。

Catalyst 6500/7600 デバイスおよび Catalyst スイッチ固有の機能

VLAN、ネットワーク接続、およびサービス モジュールの機能の設定と、Catalyst 6500/7600 デバイスおよびその他の Catalyst スイッチの設定です。

詳細については、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理 （3401 ページ）を参照してください。

FlexConfig

FlexConfig ポリシーおよびポリシー オブジェクトを使用すると、デバイスでは使用できるが、Security Manager でネイティブにサポートされていない機能をプロビジョニングできます。このポリシーやオブジェクトによって、一連の CLI コマンドを手動で指定し、Cisco Security Manager のプロビジョニング メカニズムを使用して、デバイスにコマンドを展開できます。Security Manager で生成されたコマンドの前後にこれらのコマンドを追加すると、セキュリティ ポリシーをプロビジョニングできます。

詳細については、FlexConfig の管理 （431 ページ）を参照してください。

Security Manager アプリケーションの概要

Cisco Security Manager クライアントには、6 つの主要アプリケーションとモバイルデバイス用に設計された 1 つのアプリケーションがあります。

- **Configuration Manager**：これがプライマリアプリケーションです。Configuration Manager を使用して、デバイス インベントリの管理、ローカル ポリシーと共有ポリシーの作成と編集、VPN 設定の管理、およびデバイスへのポリシーの展開を行います。Configuration Manager は最大のアプリケーションであり、ほとんどのマニュアルでこのアプリケーションが扱われています。手順でアプリケーションが明確に言及されていない場合は、手順では Configuration Manager を使用しています。Configuration Manager の概要については、Configuration Manager の使用方法 - 概要 （18 ページ）を参照してください。
- **イベントビューア**：これはイベント モニタリング アプリケーションで、Cisco Security Manager にイベントを送信するよう設定した IPS、ASA、および FWSM デバイスから生成されたイベントを表示および分析できます。Event Viewer の使用については、イベントの表示 （3473 ページ）を参照してください。
- **Report Manager**：これはレポートアプリケーションで、デバイスに関する集約された情報および VPN 統計情報のレポートを表示および作成できます。多くの情報は、Event Viewer で使用可能なイベントから取得されますが、一部の VPN 統計情報は、デバイスと直接通信することで取得されます。Report Manager の使用方法については、レポートの管理 （3561 ページ）を参照してください。
- **Health & Performance Monitor**：HPM アプリケーションを使用すると、デバイスのステータスとトラフィック情報をネットワークレベルで可視化することで、ASA（ASA-SM を含む）デバイス、IPS デバイス、VPN サービスの主要な正常性データとパフォーマンスデータを監視できます。この機能を使用して、主要なネットワークとデバイスのメトリックを監視することで、ネットワーク内のデバイスの誤動作やボトルネックをすばやく検出して解決できます。このアプリケーションの詳細については、ヘルスとパフォーマンスのモニタリング （3611 ページ）を参照してください。

- **Image Manager**：Image Manager アプリケーションでは、ASA デバイス用の完全なイメージ管理が提供されるため、イメージの更新のダウンロード、評価、分析、準備、および計画が容易になります。また、イメージの可用性、互換性、デバイスへの影響を評価し、デバイス更新のスケジュール、グループ化、および変更管理が提供されます。さらに、Image Manager には、イメージリポジトリを維持するための機能と、ASA デバイスでのイメージ更新の安定したフォールバックや回復メカニズムを保証するための機能が含まれています。Image Manager の使用方法については、Image Manager の使用 （3749 ページ）を参照してください。
- **ダッシュボード**：ダッシュボードは、Cisco Security Manager で設定可能な起動ポイントで、IPS および FW タスクをより便利なタスクにできます。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要 （3674 ページ）を参照してください。

これらのアプリケーションはすべて、Windows のスタートメニューまたはデスクトップアイコンから直接開くことができます。または、アプリケーションの [起動（Launch）] メニューから開くことができます。アプリケーションを開く方法については、Security Manager へのログインおよび終了 （14 ページ）を参照してください。

Cisco Security Manager クライアントには、モバイルデバイス用に特別に設計された追加のアプリケーションである CSM Mobile があります。

- **CSM Mobile**：CSM Mobile では、モバイルデバイスから Device Health Summary 情報にアクセスできます。この方法で入手できる情報は、Device Health Summary ウィジェットで入手可能な情報と同じ、HPM によって生成される現在の重大度が低いまたは中程度のアクティブなアラートになります。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。CSM Mobile の詳細については、CSM Mobile （3692 ページ）を参照してください。Device Health Summary 情報の詳細については、ダッシュボードの概要 （3674 ページ）を参照してください。CSM Mobile の有効化または無効化については、[CSM Mobile] ページ （653 ページ）を参照してください。

デバイス モニタリングの概要

Security Manager には、デバイスをモニタするための機能がいくつか備わっています。

- **イベントビューア**：この統合ツールを使用すると、ASA、FWSM、および IPS デバイスでイベントを表示し、関連する設定ポリシーにそのイベントを関連付けることができます。これは、問題の特定、設定のトラブルシューティング、および設定の修正と再展開を行う場合に役立ちます。詳細については、イベントの表示 （3473 ページ）を参照してください。
- **Report Manager**：これはレポートアプリケーションで、デバイスに関する集約された情報および VPN 統計情報のレポートを表示および作成できます。多くの情報は、Event Viewer で使用可能なイベントから取得されますが、一部の VPN 統計情報は、デバイスと直接通

信することで取得されます。Report Manager の使用方法については、レポートの管理 （3561 ページ）を参照してください。

Security Manager で使用可能なレポートのすべてのタイプについては、Security Manager で使用可能なレポートのタイプについて （3562 ページ）を参照してください。

- **Health & Performance Monitor**：HPM アプリケーションを使用すると、ASA（ASA-SM を含む）デバイスの主要な正常性データとパフォーマンスデータを監視できます。このアプリケーションの詳細については、ヘルスとパフォーマンスのモニタリング （3611 ページ）を参照してください。
- **ダッシュボード**：ダッシュボードは、Cisco Security Manager で設定可能な起動ポイントで、IPS および FW タスクをより便利なタスクにできます。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要 （3674 ページ）を参照してください。
- **パケット トレーサ**：このツールを使用すると、特定のタイプのパケットが ASA デバイスを通過するのを許可されているかテストできます。詳細については、Packet Tracer を使用した ASA または PIX の設定の分析 （3709 ページ）を参照してください。
- **ping、トレース ルート、および NS ルックアップ**：管理対象デバイスで ping とトレースルートを使用して、デバイスと特定の宛先の間にルートが存在するかどうかを確認できます。NS ルックアップを使用すると、アドレスを DNS 名に解決できます。詳細については、ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析 （3713 ページ）を参照してください。
- **Cisco Prime Security Manager（PRSM）の統合**：Configuration Manager アプリケーションから PRSM を「クロス起動」できます。PRSM アプリケーションは、ASA CX デバイスの設定と管理に使用されます。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。
- **デバイス マネージャの統合**：Cisco Security Manager には、Adaptive Security Device Manager（ASDM）など、さまざまなデバイス マネージャの読み取り専用コピーが含まれています。これらのツールを使用すると、デバイス ステータスの表示はできますが、デバイス設定の変更はできません。詳細については、デバイス マネージャの起動 （3697 ページ）を参照してください。
- **Cisco Security Monitoring, Analysis and Response System（CS-MARS）の統合**：CS-MARS アプリケーションを使用する場合は、Cisco Security Manager と統合して、CS-MARS のイベントを Cisco Security Manager で表示したり、逆にイベントに関連する Cisco Security Manager ポリシーを CS-MARS で表示できます。詳細については、CS-MARS と Security Manager の統合 （3727 ページ）を参照してください。

Security Manager での IPv6 サポート

Security Manager では、より多くの IPv6 設定、モニタリング、およびレポートのサポートを提供しています。

バージョン 4.12 以降、Security Manager は、IPv6 アドレスまたは IPv4 アドレスを介した Security Manager サーバーから管理対象デバイスへの通信をサポートします。この機能は、ファイアウォールデバイス、つまり、OS タイプが ASA または FWSM のデバイスでのみ使用できます。IPv6 アドレスを介した通信を有効にするには、最初に Security Manager サーバーで IPv6 アドレスを有効にする必要があります。詳細については、Cisco Security Manager サーバーでの IPv6 の設定 （11 ページ）を参照してください。

（注） Security Manager サーバーと Security Manager クライアント間の通信は、IPv4 アドレスのみを介して行われます。サーバーからクライアントへの通信では、IPv6 アドレスはサポートされていません。また、認証に ACS サーバーを使用する場合、ACS には IPv4 アドレスが必要です。ACS サーバーへの IPv6 通信はサポートされていません。Auto Update Server（AUS）は IPv6 アドレスをサポートしていません。

4.12 以前のバージョンで、IPv6 アドレスをサポートするデバイスを Security Manager で管理するには、デバイスの管理アドレスを IPv4 アドレスとして設定する必要があります。ポリシー検出と展開など、デバイスと Security Manager 間のすべての通信で IPv4 トランスポートが使用されます。サポートされるデバイスで IPv6 ポリシーが表示されない場合は、デバイスポリシーを再検出します。必要に応じて、インベントリからそのデバイスを削除して、再度追加します。

Cisco Security Manager サーバーでの IPv6 の設定

次の手順に従って、IPv6 アドレスを介してデバイスと通信するように Security Manager サーバーで IPv6 を設定します。

ステップ 1 Security Manager サーバーで、**[スタート（Start）] > [コントロールパネル（Control panel）] > [ネットワークとインターネット（Network and Internet）] > [ネットワーク接続（Network Connections）]** に移動します。

ステップ 2 使用可能なネットワーク接続をクリックして、[イーサネットのステータス（Ethernet Status）] ウィンドウを開きます。[プロパティ（Properties）] をクリックします。 [イーサネットのプロパティ（Ethernet Properties）] ウィンドウが表示されます。

ステップ 3 [ネットワーク（Networking）] タブで、[インターネットプロトコルバージョン6（TCP/IPv6）（Internet Protocol Version 6 (TCP/IPv6)）] チェックボックスをオンにし、[プロパティ（Properties）] をクリックします。[インターネットプロトコルバージョン 6（TCP/IPv6）のプロパティ（Internet Protocol Version 6 (TCP/IPv6) Properties）] ウィンドウが表示されます。

ステップ 4 IPv6 静的アドレスと DNS サーバーを設定し、[OK] をクリックします。

（注） Security Manager サーバーのホスト名を、IPv4 アドレスのみに解決されるように設定する必要があります。サーバーのホスト名が IPv6 アドレスに解決されないようにしてください。

IPv6 ポリシーの設定

通常、次のタイプのデバイスで IPv6 ポリシーを設定できます。さらに、IPS、ASA、および FWSM デバイスによって生成された IPv6 アラートをモニタできます。その他のタイプのデバイスでは、FlexConfig ポリシーを使用して IPv6 設定を行います。IPv6 デバイスサポートに関する具体的な情報については、Cisco.com でCisco Security Manager のサポート対象デバイスとソフトウェアバージョン [英語] を参照してください。

- **ASA**：ルータモードで実行されている場合はリリース 7.0 以降、トランスペアレントモードで実行されている場合はリリース 8.2 以降。1 つのセキュリティ コンテキスト デバイスと複数のセキュリティ コンテキスト デバイスの両方がサポートされます。
- **FWSM**：ルータモードで実行されている場合はリリース 3.1 以降。トランスペアレントモードではサポートされません。1 つのセキュリティ コンテキスト デバイスと複数のセキュリティ コンテキスト デバイスの両方がサポートされます。
- **IPS**：リリース 6.1 以降。

次に、IPv6 アドレッシングをサポートする Security Manager 機能の要約を示します。

- **ポリシーオブジェクト**：次のポリシーオブジェクトで IPv6 アドレスがサポートされます。
  - ネットワーク/ホスト。 ネットワーク/ホストオブジェクトについて （391 ページ）を参照してください。
  - サービス。このオブジェクトには、IPv6 ポリシーとのみ使用できる、ICMP6 および DHCPv6 用の定義済みサービスが含まれています。他のサービスは、IPv4 と IPv6 の両方に適用されます。サービス オブジェクトの詳細については、 サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
- **ファイアウォール サービスポリシー**：次のファイアウォール サービス ポリシーとツールでは IPv6 設定がサポートされます。
  - AAA ルール。ファイアウォール AAA ルールの管理 （869 ページ）を参照してください。
  - アクセスルール。 アクセス ルールの設定 （920 ページ）を参照してください。
  - インスペクションルール。ファイアウォール インスペクション ルールの管理 （977 ページ）を参照してください。

    [設定（Settings）] > [アクセス制御（Access Control）]。 アクセス コントロール ポリシー設定の指定 （943 ページ）を参照してください。
  - Tools:

[Hit Count]。 ヒットカウントの詳細の表示 （960 ページ）を参照してください。

[Find and Replace]。 ルールテーブルの項目の検索と置換 （777 ページ）を参照してください。

- **ASA および FWSM ポリシー**：次の ASA および FWSM ポリシーでは IPv6 設定がサポートされます。
  - （ASA 7.0 以降のルーテッドモード、ASA 8.2 以降のトランスペアレントモード、FWSM 3.1 以降のルーテッドモード）。インターフェイス：[インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [IPv6] タブ。 IPv6 インターフェイスの設定（ASA/FWSM） （2409 ページ）を参照してください。
  - （ASA のみ）。**[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [IPv6 ネイバーキャッシュ（IPv6 Neighbor Cache）]**。 IPv6 ネイバー キャッシュの管理 （2457 ページ）を参照してください。
  - （ASA 5505 8.2/8.3 のみ）。**[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理IPv6（Management IPv6）]**。 [Management IPv6] ページ（ASA 5505） （2462 ページ）を参照してください。
  - （ASA 8.4.2 以降のみ）。**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS]**。 [DNS] ページ （2616 ページ）を参照してください。
- **FlexConfig ポリシー**：デバイスで IPv6 ACL を識別するために使用できる 2 つのファイアウォールシステム変数があります。詳細については、 FlexConfig システム変数 （438 ページ）を参照してください。

これらの変数を使用する定義済みの FlexConfig ポリシー オブジェクト（ASA_add_IPv6_ACE）もあります。

- **イベントビューア**：IPv6 アドレスが含まれているイベントがサポートされ、アドレスは、IPv4 アドレスと同じ列（[送信元（Source）]、[宛先（Destination）]、および [IPLog アドレス（IPLog Address）]（IPS アラートの場合））に表示されます。ただし、Security Manager サーバへのイベントの送信に IPv4 を使用するようデバイスを設定する必要があります。すべてのイベント通信で IPv4 トランスポートが使用されます。Event Viewer の詳細については、 イベントの表示 （3473 ページ）を参照してください。
- **ダッシュボード**：ダッシュボードでは、IP アドレスを使用するすべてのウィジェットで IPv6 アドレスがサポートされます。ただし、Cisco Security Manager における他の場合と同様に、Cisco Security Manager サーバーへのイベントの送信時に IPv4 を使用するようデバイスを設定する必要があります。すべてのイベント通信で IPv4 トランスポートが使用されます。ダッシュボードの詳細については、 ダッシュボードの概要（3674 ページ）を参照してください。
- **Report Manager**：レポートには、イベント管理によって収集された IPv6 イベントの統計情報が含まれています。Report Manager の詳細については、 レポートの管理 （3561 ページ）を参照してください。

Cisco Security Manager 4.4 でのポリシーオブジェクトの変更

以前は分離していた IPv4 要素と IPv6 要素を統合するために、Security Manager 4.4 のいくつかのポリシーとポリシーオブジェクトに一定の変更が加えられました。これらの変更の中で最も重要なのは、ネットワーク/ホストオブジェクト（それ自体はネットワーク/ホストオブジェクトとネットワーク/ホスト IPv6 オブジェクトの統合を表す）に対する変更です。

- 新しいネットワーク/ホストオブジェクト「All-IPv4-Addresses」によって、IPv4「any」ネットワーク ポリシー オブジェクトは置き換えられます。以前のバージョンから Security Manager 4.4 にアップグレードすると、IPv4「any」ネットワーク ポリシー オブジェクトへのすべての参照が「All-IPv4-Addresses」に変更されます。
- 新しいネットワーク/ホストオブジェクト「All-IPv6-Addresses」によって、IPv6「any」ネットワーク ポリシー オブジェクトは置き換えられます。以前のバージョンから Security Manager 4.4 にアップグレードすると、IPv6「any」ネットワーク ポリシー オブジェクトへのすべての参照が「All-IPv6-Addresses」に変更されます。
- 新しいネットワーク/ホストオブジェクト「All-Addresses」には、以前のバージョンの Security Manager に対応するポリシーオブジェクトがありません。これは新しいグローバルな「any」ポリシーオブジェクトであり、すべての IPv4 および IPv6 アドレス範囲を含みます。

その他の関連する変更には、アクセスルール、検査ルールといったデバイス固有のポリシーの IPv4 バージョンと IPv6 バージョンの統合が含まれます。

さらに、ポリシーとオブジェクトを編集するとき、IPv4、IPv6、または混合モード（IPv4 と IPv6 の両方）のエントリは、ダイアログボックスなどの要素で自動的にフィルタリングされます（これらのエントリの 1 つ以上が要素に該当しません）。

関連項目

- Policy Object Manager （290 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

Security Manager へのログインおよび終了

Security Manager には、次の 2 つの主要インターフェイスがあります。

- Cisco Security Management Suite ホームページ：このインターフェイスは、Security Manager クライアントをインストールする場合およびサーバを管理する場合に使用します。Resource Manager Essentials（RME）など、インストール済みの他の CiscoWorks アプリケーションにアクセスすることもできます。
- Security Manager クライアント：これらのインターフェイスは、ほとんどの Security Manager タスクを実行する場合に使用します。6 つのクライアントアプリケーション（Configuration Manager、Event Viewer、Report Manager、Health & Performance Monitor、Image Manager またはダッシュボード）のいずれかに直接記録できます。

ここでは、これらのインターフェイスにログインする方法およびインターフェイスを終了する方法について説明します。

• ユーザの権限について （15 ページ）
• Cisco Security Management Suite サーバへのログイン （16 ページ）
• Security Manager クライアントへのログインおよび終了 （17 ページ）

ユーザの権限について

ユーザがログインする前に、Cisco Security Manager によってユーザ名とパスワードが認証されます。認証されると、Security Manager によってアプリケーション内のユーザのロールが確立されます。このロールによって、実行が認可されるタスクまたは操作のセットである権限（特権とも呼ばれる）が定義されます。特定のタスクまたはデバイスに対して認可されなかった場合は、関連するメニュー項目、目次内の項目、およびボタンが非表示またはディセーブルになります。加えて、選択した情報を表示したり、選択した操作を実行したりするための権限がないことを伝えるメッセージが表示されます。

Security Manager の認証と認可は、CiscoWorks サーバと Cisco Secure Access Control Server（ACS）のどちらかによって管理されます。デフォルトでは CiscoWorks で認証および認可を管理しますが、Security Manager を設定すれば Cisco Secure ACS セットアップを使用できます。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

ACS を使用する場合は、すべての ACS サーバが利用不能な状態になると Security Manager でタスクを実行できません。ログイン済みの場合は、ACS による認可が必要なタスクを実行しようとすると、（変更を保存する間もなく）システムから突然ログアウトされることがあります。この場合、認可を実行できないためにログオフされたことを示すメッセージが表示されます。Security Manager と ACS の統合の設定方法については、「Integrating Security Manager with Cisco Secure ACS」を参照してください。

ユーザ権限および AAA 設定の詳細については、『Installation Guide for Cisco Security Manager』を参照してください。

Event Viewer および Report Manager アプリケーションでの認可制御の詳細については、次の項を参照してください。

• Event Viewer のアクセス コントロールについて （3477 ページ）
• Report Manager のアクセス コントロールについて （3567 ページ）

Cisco Security Management Suite サーバへのログイン

Security Manager クライアントをインストールしてサーバを管理するには、Cisco Security Management Suite ホームページおよび CiscoWorks Common Services を使用します。RME など、インストール済みの他の CiscoWorks アプリケーションにアクセスすることもできます。

（注） Common Services の [ソフトウェアセンター（Software Center）] > [ソフトウェアの更新（Software Update）] 機能は、Cisco Security Manager ではサポートされていません。

ステップ 1 Web ブラウザで、次の URL のいずれかを開きます。*SecManServer* は、Security Manager がインストールされているコンピュータの名前です。いずれかの [セキュリティアラート（Security Alert）] ウィンドウで [はい（Yes）] をクリックします。

- SSL を使用していない場合は、http://*SecManServer*:1741 を開きます。
- SSL を使用している場合は、https://*SecManServer*:443 を開きます。

Cisco Security Management Suite のログイン画面が表示されます。ページ上で、JavaScript と cookie がイネーブルになっていることと、サポートされているバージョンの Web ブラウザを実行していることを確認します。Security Manager を実行するためのブラウザの設定方法については、『Installation Guide for Cisco Security Manager』を参照してください。

ステップ 2 ユーザ名とパスワードを使用して、Cisco Security Management Suite サーバにログインします。初めてサーバーをインストールする場合は、ユーザー名 **admin** と、製品のインストール中に定義されたパスワードを使用してログインできます。

ステップ 3 Cisco Security Management Suite ホームページで、少なくとも次の機能にアクセスします。製品のインストール内容によっては、他の機能も使用できる場合があります。

- [Cisco Security Manager Client Installer]：この項目をクリックして、Security Manager クライアントをインストールします。このクライアントが、製品を使用する際の主要なインターフェイスとなります。
- Server Administration：この項目をクリックすると、CiscoWorks Common Services Server のページが開きます。CiscoWorks Common Services は、サーバを管理する基盤ソフトウェアです。このソフトウェアを使用して、サーバの保守とトラブルシューティングやローカルユーザ定義などのバックエンドサーバ機能を設定して管理します。
- CiscoWorks リンク（ページ右上）：このリンクをクリックすると、CiscoWorks Common Services のホームページが開きます。

ステップ 4 アプリケーションを終了するには、画面右上隅にある [ログアウト（Logout）] をクリックします。ホームページと Security Manager クライアントの両方を同時に開いている場合は、ブラウザ接続を終了しても Security Manager クライアントが終了しません。

次のタスク

（注） PCI コンプライアンスに対応するために、TLS 1.0 は CSM サーバーで無効になっています。そのため、CSM サーバーは TLS 1.0 クライアントの接続を許可しません。この変更は、CSM サーバーからデバイスへの通信には適用されません。既存の CSM サーバーからデバイスへの通信は、引き続きサポートされます。

Security Manager クライアントへのログインおよび終了

Security Manager クライアントを使用して、ほとんどの Security Manager タスクを実行します。

ヒント Security Manager クライアント アプリケーションを十分に活用できる管理者特権が付与された Windows ユーザ アカウントを使用してワークステーションにログインする必要があります。より低い特権を使用してアプリケーションを操作しようとすると、一部の機能が正しく機能しない場合があります。

はじめる前に

コンピュータにクライアントをインストールします。クライアントをインストールするには、Security Manager サーバーにログインし（Cisco Security Management Suite サーバへのログイン（16 ページ）を参照）、[Cisco Security Managerクライアントインストーラ（Cisco Security Manager Client Installer）] をクリックしてインストールウィザードの指示に従ってください。

ステップ 1 [開始（Start）]>[すべてのプログラム（All Programs）]>[Cisco Security Managerクライアント（Cisco Security Manager Client）] メニューから、次のいずれかのアプリケーションを選択します。

- 設定マネージャ（Configuration Manager）
- イベントビューア
- Report Manager
- Health and Performance Monitor
- Image Manager
- ダッシュボード

ヒント クライアントがワークステーションにインストールされているのに [Start] メニューに表示されない場合は、別のユーザがクライアントをインストールした可能性があります。クライアント ステーションのすべてのユーザに対して、Security Manager クライアントが [Start] メニューに表示されるようにするには、Cisco Security Manager クライアント フォルダを Documents and Settings\<user>\Start Menu\Programs\Cisco Security Manager から Documents and Settings\All Users\Start Menu\Programs\Cisco Security Manager にコピーします。

ステップ 2 アプリケーションのログインウィンドウで、ログインするサーバーを選択して、Security Manager のユーザー名とパスワードを入力します。[ログイン（Login）] をクリックします。

クライアントがサーバにログインし、次の条件に基づいて選択したアプリケーションが開きます。これらの条件はアプリケーション単位であることに注意してください。たとえば、あるワークステーションで Configuration Manager を開いている場合に、別のワークステーションから Event Viewer を開いても、Event Viewer から Configuration Manager を開始しないかぎり、Configuration Manager セッションは影響を受けません。

- Workflow モードと Workflow 以外のモードの両方で、単一のワークステーションからは同じサーバにログインできず、同じユーザアカウントを使用して複数のアクティブセッションを使用することはできません。すでにログインしていることが通知され、既存の開いているアプリケーションを再使用するよう求められます。
- 両方の Workflow モードで、同じ（または別の）ユーザ名を使用して同じワークステーションから異なるサーバにログインできます。
- Workflow 以外のモードでは、特定のサーバでユーザ名が別のワークステーションにログインしている場合は、他のワークステーションのクライアントは自動的にログアウトされ、保存されていない変更はすべて失われます。そのため、ユーザアカウントを共有しないでください。別のワークステーションから同じサーバにログインする必要がある場合は、アクティブクライアントを終了する前に忘れずに変更を保存してください。
- Workflow モードでは、異なるワークステーションだけから、同じユーザアカウントを使用して複数回ログインできます。ただし、複数のクライアントで同時に Configuration Manager で同じアクティビティを開くことはできません。別のアクティビティを開く必要があります。アクティビティは、Event Viewer または Report Manager の使用時には適用されません。

ヒント クライアントは、アイドル状態が 120 分間続くと自動的に閉じます。アイドルタイムアウトを変更するには、Configuration Manager で [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [デスクトップのカスタマイズ（Customize Desktop）] を選択して、必要なタイムアウト期間を入力します。この機能をディセーブルにして、クライアントが自動的に閉じないようにすることもできます。すべてのアプリケーションが同じタイムアウト設定を使用し、あるアプリケーションでの作業によって、その他すべてのアプリケーションのタイマーがリセットされます。

ステップ 3 アプリケーションを終了するには、[ファイル（File）] > [終了（Exit）] の順に選択します。

Configuration Manager の使用方法 - 概要

ここでは、Configuration Manager で使用できるさまざまなビューの概要、ポリシーを定義してデバイスに展開するための基本タスク フロー、およびいくつかの基本概念について説明します。

- Configuration Manager の概要 （19 ページ）
- セキュリティ ポリシー設定のタスク フロー （24 ページ）

• ポリシーおよびポリシー オブジェクトの概要 （25 ページ）
• ワークフローおよびアクティビティの概要 （26 ページ）

Configuration Manager の概要

Configuration Managerアプリケーションには、デバイス ビュー、ポリシー ビュー、およびマップ ビューという3つのビューがあり、これらのビューによってデバイスおよびポリシーを管理できます。ツールバーのボタンまたは [View] メニューを使用すると、必要に応じてこれらのビュー間を切り替えることができます。

- デバイス ビュー：デバイス中心のビューを表示します。このビューでは、個々のデバイスのポリシーを設定します。詳細については、 デバイス ビューの概要 （20 ページ）を参照してください。
- ポリシー ビュー：ポリシー中心のビューを表示します。このビューでは、デバイスに依存しない共有ポリシーを作成し、1 つ以上のデバイスに割り当てることができます。詳細については、 ポリシー ビューの概要 （22 ページ）を参照してください。
- マップ ビュー：ネットワークを視覚的に表示します。これは、主にサイト間 VPN を視覚的に表示して設定する場合に役立ちます。詳細については、 マップ ビューの概要 （23 ページ）を参照してください。

各ビューを使用すると、Configuration Manager の機能に異なる方法でアクセスできます。操作できる内容と操作方法は、選択したビューによって決まります。デバイス ビューおよびポリシー ビューでは、左側に2つのセレクタ、右側に作業領域が表示されます。それぞれのビューで上部のセレクタから項目を選択すると、下部のセレクタで選択できる項目が決まります。下部のセレクタから項目を選択すると、作業領域に表示される内容が決まります。この設計により、目的のネットワークの詳細まですばやく簡単にドリルダウンして表示または編集できます。

メインのビュー以外にも、サイト間 VPN やポリシー オブジェクトなどの他の項目を設定するとき、またはデバイスをモニタするときに使用するツールがいくつかあります。通常、これらのツールは [Manage] メニューから使用できますが、一部は [Policy]、[Activities]、[Tools]、または [Launch] メニューから使用できます。関連するボタンがツールバーに用意されているツールもあります。これらのツールは別のウィンドウで開くため、現在使用しているメイン ビューの位置を見失うことはありません。

ユーザ インターフェイスの基本機能に関する参照情報については、次の項を参照してください。

- Configuration Manager のメニュー バー リファレンス （38 ページ）
- ツールバー リファレンス（Configuration Manager） （51 ページ）
- セレクタの使用 （60 ページ）
- ウィザードの使用 （63 ページ）
- ルール テーブルの使用 （764 ページ）

• テキスト フィールドの使用方法 （66 ページ）
• オンライン ヘルプの利用方法 （70 ページ）

デバイス ビューの概要

Configuration Manager のデバイス ビューを使用すると、Security Manager インベントリにデバイスを追加して、デバイス ポリシー、プロパティ、インターフェイスなどを集中管理できます。次の図に、デバイス ビューの機能領域を示します。

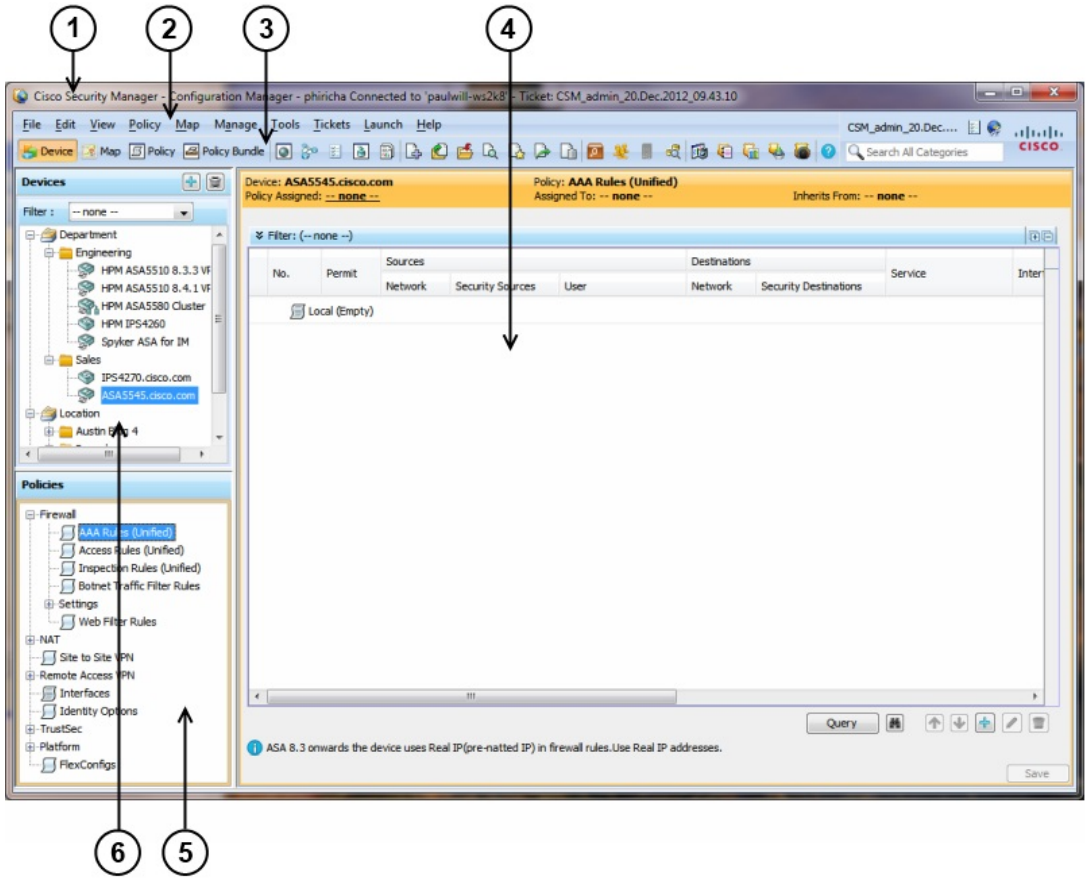
これはデバイス中心のビューであり、すべての管理対象デバイスを表示したり、特定のデバイスを選択してそのプロパティの表示や設定とポリシーの定義を行うことができます。

（注） Security Manager には、Security Manager インベントリ内のデバイスのステータスを表示する機能もあります。デバイスステータスビューにアクセスするには、[表示（View）] > [デバイスステータスビュー（Device Status View）] を選択するか、デバイスセレクタでフォルダノードの 1 つを選択します。詳細については、[デバイスステータスビュー（Device Status View）] の使用 （170 ページ）を参照してください。

デバイス ビューでは、個々のデバイスのローカルにセキュリティ ポリシーを定義できます。続けて、グローバルに使用できるようにポリシーを共有すれば、他のデバイスに割り当てることができます。

詳細については、デバイス ビューについて （87 ページ）を参照してください。

図 *1* : デバイス ビューの概要



1	タイトル バー	2	メニュー バー（Configuration Manager のメニュー バー リファレンス （38 ページ）を参照）
3	ツールバー（ツールバー リファレンス（Configuration Manager） （51 ページ）を参照）	4	作業領域
5	ポリシー セレクタ	6	デバイス セレクタ（セレクタの使用 （60 ページ）を参照）

タイトル バーには Security Manager の次の情報が表示されます。

- ログイン名
- 接続先の Security Manager サーバの名前
- 開いているアクティビティの名前（Workflow モードがイネーブルの場合）

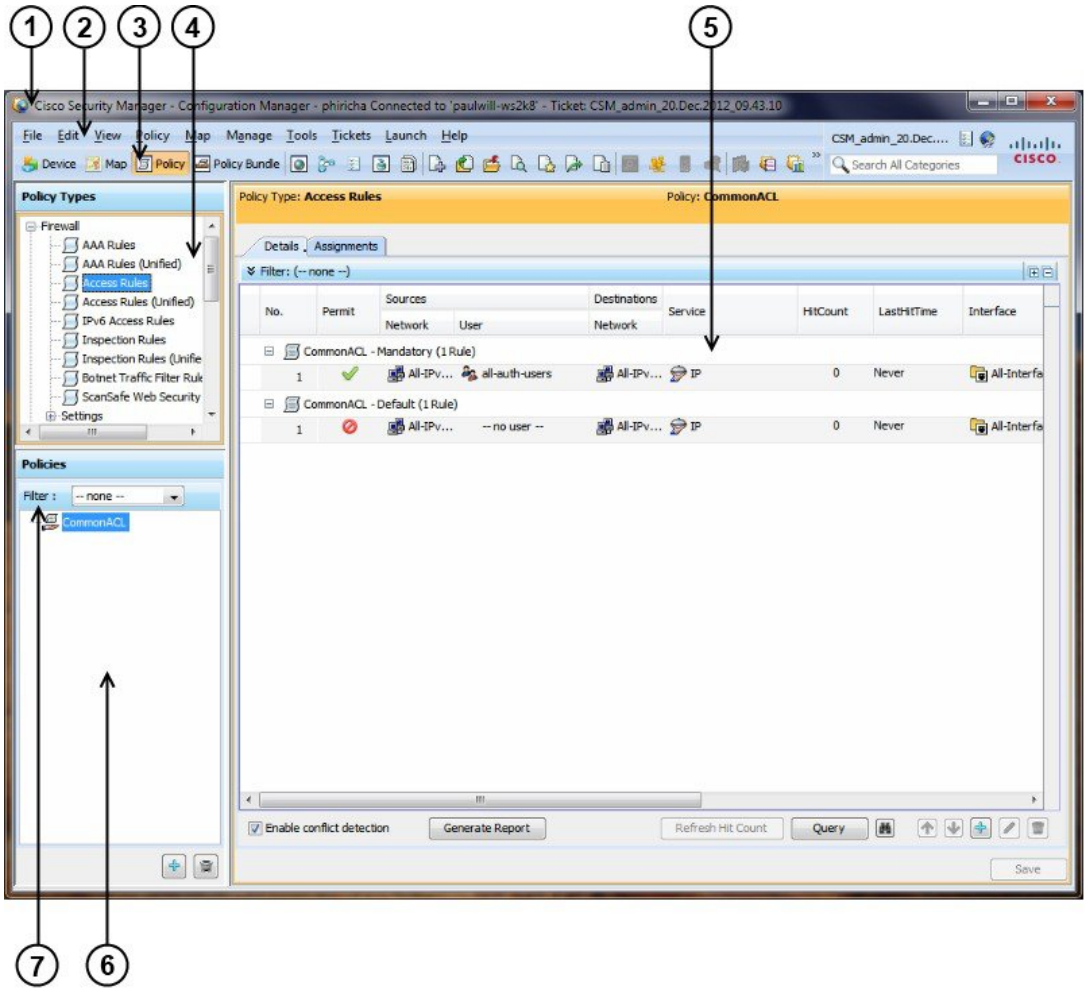
ポリシー ビューの概要

Configuration Manager のポリシー ビューを使用すると、複数のデバイス間で共有できる、再利用可能なポリシーを作成および管理できます。次の図に、ポリシー ビューの機能領域を示します。

これはポリシー中心のビューです。このビューには、Security Manager でサポートされている、共有可能なポリシー タイプがすべて表示されます。特定のポリシー タイプを選択して、そのタイプの共有ポリシーを作成、表示、または変更できます。各共有ポリシーが割り当てられているデバイスを確認し、必要に応じて割り当てを変更することもできます。

詳細については、ポリシー ビューにおける共有ポリシーの管理 （273 ページ）を参照してください。

図 *2:* ポリシー ビューの概要



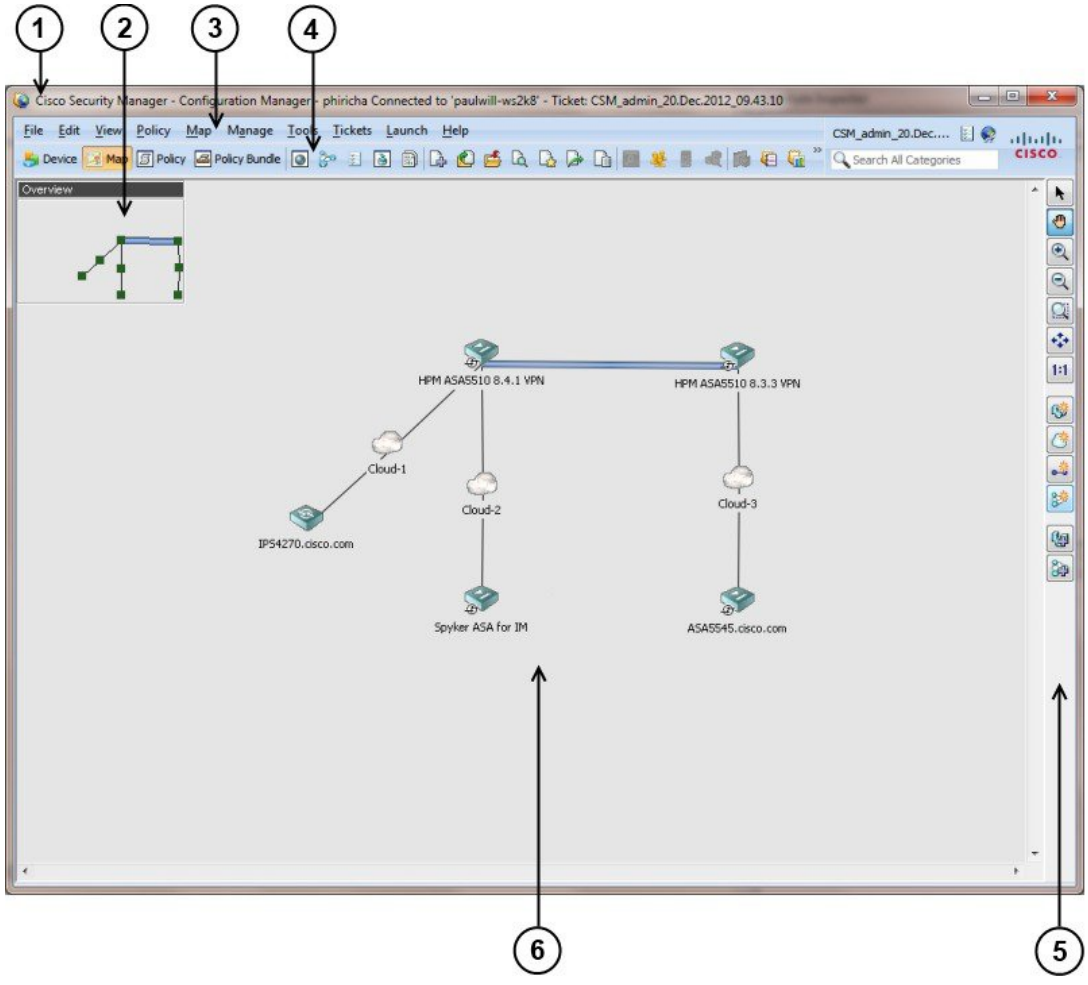
1	タイトル バー	2	メニューバー（Configuration Manager のメニュー バー リファレンス （38 ページ）を参照）

3	ツールバー（ツールバー リファレンス（Configuration Manager） （51 ページ）を参照）	4	ポリシー タイプ セレクタ（セレクタの使用（60 ページ）を参照）
5	作業領域	6	共有ポリシー セレクタ
7	ポリシー フィルタ		

マップ ビューの概要

Configuration Manager のマップ ビューを使用すると、ネットワークのカスタマイズされた視覚的なトポロジ マップを作成できます。このトポロジ マップ内で、デバイス間の接続を表示したり、VPN およびアクセス コントロール設定を簡単に行ったりできます。次の図は、マップ ビューの機能領域を示しています。

図 *3:* マップ ビューの概要



1	タイトル バー	2	ナビゲーション ウィンドウ

3	メニュー バー（[Map] メニュー（Configuration Manager） （43 ページ）を参照）	4	ツールバー（ツールバー リファレンス（Configuration Manager） （51 ページ）を参照）
5	マップ ツールバー（マップ ツールバー （2052 ページ）を参照）	6	マップ

セキュリティ ポリシー設定のタスク フロー

デバイスのセキュリティ ポリシーを設定する場合、基本となるユーザ タスク フローは、Security Manager インベントリへのデバイスの追加、ポリシーの定義、およびデバイスへのポリシーの展開です。これらのタスクは Configuration Manager で実行します。次に、一般的なユーザ タスク フローの手順を簡単に説明します。

ステップ 1 **管理するデバイスを準備します。**

Security Manager デバイス インベントリにデバイスを追加して管理する前に、デバイスで最小限の設定を行い、Security Manager がデバイスに接続できるようにする必要があります。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。

ステップ 2 **Security Manager デバイス インベントリにデバイスを追加します。**

Security Manager でデバイスを管理するには、まず Security Manager インベントリにそのデバイスを追加する必要があります。Security Manager にはデバイスを追加するいくつかの方式が用意されています。方式には、ネットワーク経由（ライブ デバイス）、別の Security Manager サーバまたは CiscoWorks Common Services Device Credential Repository（DCR）からエクスポートされたインベントリ ファイル経由、Cisco Security Monitoring, Analysis and Response System（CS-MARS）形式のインベントリ ファイル経由、またはデバイス設定ファイル経由があります。Security Manager でデバイスを作成すると、ネットワークにはまだ存在しないが、配置する予定のあるデバイスを追加することもできます。

デバイスを追加した場合は、そのデバイスのインターフェイスと、すでに設定されている特定のポリシーも検出できます。検出された情報は Security Manager データベースに登録され、それ以降も Security Manager によって継続的に管理できます。

詳細については、デバイス インベントリの管理 （87 ページ）を参照してください。

ステップ 3 **セキュリティ ポリシーを定義します。**

デバイスの追加が完了すると、必要なセキュリティ ポリシーを定義できます。個々のデバイスのポリシーの定義には、デバイス ビューを使用できます。任意の数のデバイスで共有できる、再利用可能なポリシーの作成および管理には、ポリシー ビューを使用できます。共有ポリシーに変更を加えると、そのポリシーが割り当てられているすべてのデバイスに変更が適用されます。

ポリシー定義を簡素化して時間を短縮するために、ポリシー オブジェクトを使用できます。これは、特定の値に名前を付けて再利用可能としたオブジェクトです。オブジェクトを定義すると、複数のポリシーからそのオブジェクトを参照できるため、ポリシーごとに値を個別に定義する必要がなくなります。

（注） Workflowモードを使用している場合は、アクティビティを作成してからポリシーを定義する必要があります。詳細については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。

ステップ 4 ポリシー定義を送信して展開します。

ポリシー定義はユーザの専用ビュー内で行われます。ユーザが定義を送信するまで、定義はデータベースに登録されず、他のSecurity Managerユーザがその定義を確認することもできません。ポリシー定義を送信する場合は、その整合性が検証されます。エラーまたは警告があればそれらが表示され、ポリシーをデバイスに展開する前に対処しておく必要のある問題が通知されます。

Security Managerではポリシー定義に従ってCLIコマンドが生成され、すばやく簡単に定義をデバイスに展開できます。セキュアな接続を経由してネットワーク内のライブデバイス（動的にアドレス指定されたデバイスを含む）に直接展開するか、またはファイルに展開していつでもデバイスに転送できます。

Workflow 以外のモードでは、1 回のアクションで変更の送信と展開を実行できます。Workflow モードでは、最初にアクティビティを送信してから、変更を展開する展開ジョブを作成します。

詳細については、展開の管理 （481 ページ）を参照してください。

ポリシーおよびポリシー オブジェクトの概要

ポリシーとは、ネットワークの特定の設定項目を定義した一連のルールまたはパラメータのことです。Configuration Manager では、デバイスに必要なセキュリティ機能を指定するポリシーを定義します。定義されたポリシーは、関連デバイスに展開可能なCLIコマンドに変換されます。

Security Manager を使用すると、ローカル ポリシーおよび共有ポリシーを設定できます。

- **ローカル ポリシー**は、設定したデバイス限定のポリシーです。このポリシーを設定すると、デバイスに自動的に割り当てられます（適用されます）。未設定ポリシー（デフォルト設定を変更していないポリシー）は、割り当て済みまたは設定済みとは見なされません。ポリシーを削除するには、その割り当てを解除します。
- **共有ポリシー**は、名前が付けられた再利用可能なポリシーであり、一度に複数のデバイスに割り当てることができます。共有ポリシーを変更すると、変更したポリシーが割り当てられているすべてのデバイスに変更が反映されます。このため、デバイスごとに変更を行う必要がありません。

インベントリにデバイスを追加すると、そのデバイスに設定されている既存のポリシーを検出できるようになります。Security Manager はデバイス設定を Security Manager ポリシーに変換し、関連するローカル ポリシーに値を読み込んでデバイスにポリシーを割り当てます。**ポリシー検出**を使用することにより、Security Manager の観点で既存の設定を作成し直す必要がなくなります。CLIを使用して設定を変更した場合は、インベントリにポリシーを追加したあとに再検出することもできます。

多くの場合、ポリシーを作成するときに**ポリシーオブジェクト**を使用できます。ポリシーオブジェクトとは、関連する値のセットを再利用可能な形で定義したものです。（場合によって

は、ポリシーオブジェクトを使用する必要があります。）たとえば、ネットワークの一連の IP アドレスが含まれる、MyNetwork というネットワークオブジェクトを定義できます。これらのアドレスを必要とするポリシーを設定するときは、常に MyNetwork ネットワーク オブジェクトを参照するだけで済み、毎回手動でアドレスを入力する必要がありません。さらに、集中管理する場所でポリシーオブジェクトを変更でき、この変更は、オブジェクトを参照しているすべてのポリシーに反映されます。

詳細については、ポリシーの管理（209ページ）およびポリシーオブジェクトの管理（287ページ）を参照してください。

ワークフローおよびアクティビティの概要

柔軟性のあるセキュアなポリシー管理を提供する一方、組織が変更制御プロセスを実行できるようにするために、Security Manager には、Configuration Manager に密接に関連する 3 つの機能が用意されています。

- [Workflowモード（Workflow Mode）]/[Workflow以外のモード（Non-Workflow Mode）]：Configuration Manager には、Workflow モードおよび Workflow 以外のモード（デフォルト）の 2 つの動作モードがあり、さまざまな組織の作業環境に対応できます。
  - [Workflowモード（Workflow Mode）]：Workflow モードは、セキュリティポリシーを定義するユーザーと管理するユーザーで責務を分担している組織のためのモードです。明示的にアクティビティを作成し、そのコンテキスト内ですべてのポリシー設定を行うことにより、正式な変更追跡と管理のシステムが導入されます。単一のアクティビティには論理的に関連するポリシー変更だけを追加するために、ユーザは複数のアクティビティを作成できます。チェックなしで設定変更が行われないように、個別のアプルーバを必要とするように Workflow モードを設定できます。承認後、ユーザは別の展開ジョブを定義して、ポリシー変更をデバイスにプッシュします。詳細については、Workflow モードの作業 （27 ページ）を参照してください。
  - [Workflow以外のモード（Non-Workflow Mode）]：Workflow 以外のモードでは、アクティビティを明示的には作成しません。ログインすると、Configuration Manager はアクティビティを作成するか、または以前に使用したアクティビティが送信されていない場合はそのアクティビティを開きます。ポリシーを定義して保存すれば、1 回の手順でポリシーを送信して展開できます。詳細については、Workflow 以外のモードの作業 （28 ページ）を参照してください。

モードの選択の詳細については、ワークフロー モードの変更 （36 ページ）を参照してください。

- [アクティビティまたは設定セッション（Activities or Configuration Sessions）]：アクティビティ（Workflow 以外のモードでは設定セッション）は、基本的に Security Manager データベースの専用ビューです。Configuration Manager では、アクティビティを使用して、ポリシーおよびポリシー割り当てに対して行われる変更を制御します。インベントリにデバイスを追加しても、アクティビティは含まれません。ただし、（マルチコンテキストのファイアウォールデバイスの）セキュリティ コンテキストまたは（IPS デバイスの）仮想センサーを定義するポリシーを検出する場合は除きます。アクティビティからポリシー変更を

分離すると、「処理中の作業」を誤ってアクティブデバイスの設定に送信することを防ぐのに役立ちます。アクティビティおよび設定セッションの詳細については、アクティビティについて （177 ページ）およびアクティビティ/チケットの操作 （185 ページ）を参照してください。

- [チケット管理（Ticket Management）]：チケット管理により、チケット ID を Security Manager で行われたポリシー設定の変更に関連付けることができます。チケット管理は、Workflow モードが有効になっているかどうかに応じて、アクティビティまたは設定セッションと連動して機能します。Workflow モードが有効になっている場合は、チケット管理を有効にして、オプションでチケット ID を特定のアクティビティに関連付けることもできます。Workflow モードが有効になっていない場合、チケット管理を使用すると、すべての変更をチケットの一部として実行する必要があり、それらの変更を展開する前にチケットを送信する必要があります。この点で、ワークフローが無効な場合のチケット管理は、ワークフローが有効な場合のアクティビティの機能によく似ています。ただし、送信されたチケットの承認は必要ありません。

さまざまな動作モードの比較については、Workflow モードの比較 （29 ページ）を参照してください。

Workflow モードの作業

Workflow モードは、正式な変更追跡と管理のシステムを導入する高度な動作モードです。このモードは、ポリシーを定義する責務とデバイスにポリシーを展開する責務を、セキュリティ オペレータとネットワーク オペレータの間で分担している組織に適しています。たとえば、あるセキュリティ オペレータはデバイスでセキュリティ ポリシーの定義を担当し、別のセキュリティ オペレータはポリシー定義の承認を担当、およびネットワーク オペレータは承認された設定をデバイスに展開することを担当する場合があります。このように責務を分離すると、展開したデバイス設定の整合性を維持できます。

Workflowモードはアプルーバの有無に関係なく使用できます。アプルーバを設定してWorkflowモードを使用する場合、ユーザが実行したデバイス管理およびポリシー設定の変更は、別のユーザによる確認および承認を経て関連デバイスに展開されます。アプルーバを設定しないでWorkflowモードを使用する場合は、1人のユーザがデバイスおよびポリシー設定の変更を作成して承認できるため、変更プロセスが簡素化されます。

（注） Workflow モードは、チケット管理が有効か無効かに関係なく、同じように機能します。Workflow モードでチケット管理を有効にすると、アクティビティで使用する [チケット（Ticket）] フィールドが有効になります。チケット ID の入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように[チケット（Ticket）]フィールドを設定できます。詳細については、「チケット管理」を参照してください。

Workflow モードの有効化または無効化、またはチケット管理の有効化または無効化については、ワークフロー モードの変更 （36 ページ）を参照してください。

ワークフロー モードで、次の手順を実行します。

- ユーザは、Configuration Manager でポリシー設定を定義または変更する前にアクティビティを作成する必要があります。アクティビティは、基本的には設定変更を行うためのプロポーザルです。アクティビティ内で行われた変更は、適切な権限を持つユーザがアクティビティを承認したあとにだけ適用されます。アクティビティは、別のユーザーに送信して確認および承認することも、現在のユーザーが承認することもできます。アクティビティを作成、送信、および承認するプロセスの詳細については、アクティビティの管理 （177 ページ）を参照してください。
- アクティビティを承認したあとは、設定変更を関連デバイスに展開する必要があります。このとき、ユーザーは展開ジョブを作成します。展開ジョブには、設定の展開先デバイスおよび使用する展開方法を定義します。展開ジョブは、別のユーザーに送信して確認および承認することも、現在のユーザーが承認することもできます。展開プリファレンスは、ジョブ承認の有無に関係なく設定できます。詳細については、展開の管理 （481 ページ）を参照してください。

Workflow 以外のモードの作業

組織によっては、VPN ポリシーとファイアウォール ポリシーを定義および管理する場合に、ユーザ間で責務を分担しない場合があります。これらの組織は、Workflow 以外のモードで作業できます。Workflow 以外のモードを使用する場合は、アクティビティを明示的には作成しません。ログインしたときに、Configuration Manager によってアクティビティ（別名を設定セッションと呼びます）が作成されるか、または以前のログイン時に使用していたアクティビティが開きます（Security Manager をログアウトすると、設定セッションは自動的に閉じます）。このアクティビティはユーザに対して透過的であり、特に管理する必要はありません。設定変更をデータベースに送信した場合、これは Workflow モードにおけるアクティビティの送信および承認に相当します。また、設定変更を送信して展開すると、展開ジョブも作成されます。アクティビティと同様、展開ジョブも透過的であり、管理の必要はありません。

Workflow 以外のモードを使用している場合、同じユーザ名とパスワードを持つ複数のユーザが、同時に Security Manager にログインすることはできません。作業中に、同じユーザ名とパスワードを持つ別のユーザがログインすると、セッションが終了するため再度ログインする必要があります。

Workflow 以外のモードのチケット管理

組織が変更管理システムを使用している場合、Security Manager は、設定に加えられた変更をチケット ID に関連付けることができます。設定を変更する前に、チケットを開いて、チケットに関連付けられた変更を展開できるようにする前に、チケットを送信する必要があります。チケットは必要に応じて開いたり閉じたりでき、チケットに関連する変更が不要になった場合はチケットを破棄できます。チケット ID の入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように[チケット（Ticket）]フィールドを設定できます。詳細については、「チケット管理」を参照してください。

チケット管理が有効になっている Workflow 以外のモードは、Security Manager のデフォルトモードです。Workflow モードの有効化または無効化、またはチケット管理の有効化または無効化については、ワークフロー モードの変更 （36 ページ）を参照してください。

Workflow モードの比較

次の表に、Workflow モード間の違いを示します。

（注） Workflow モードは、チケット管理が有効か無効かに関係なく、同じように機能します。Workflow モードでチケット管理を有効にすると、アクティビティで使用する [チケット（Ticket）] フィールドが有効になります。チケット ID の入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように [チケット（Ticket）] フィールドを設定できます。詳細については、「チケット管理」を参照してください。

表 *1 : Configuration Manager* での *Workflow* モードと *Workflow* 以外のモードの比較

質問	チケット管理が有効になっている Workflow 以外のモード	チケット管理が無効になっている Workflow 以外のモード	Workflow モード
Security Manager のデフォルトモードはどれですか。	デフォルト	非デフォルト	非デフォルト。
現在選択されているモードを確認するにはどうすればよいですか。	**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [ワークフロー（Workflow）]** を選択します。[Workflow の有効化（Enable Workflow）] チェックボックスがオンになっている場合、Workflow モードです。 **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [チケット管理（Ticket Management）]** を選択します。[チケットの有効化（Enable Ticketing）] チェックボックスをオンにすると、チケット管理が有効になります。		
設定を変更するためにアクティビティを明示的に作成する必要がありますか。	設定を変更する前に、明示的にチケットを作成する必要があります。Configuration Manager は、そのチケットに関連付けられたアクティビティを自動的に作成します。	いいえ。ログイン時に Configuration Manager によってアクティビティが自動的に作成されるか、またはログアウト前に以前のセッションを送信しなかった場合はそのセッションが開きます。	はい。
デバイスに設定を展開するために展開ジョブを明示的に作成する必要がありますか。	いいえ。設定変更を展開すると、Configuration Manager によって展開ジョブが作成されます。	いいえ。設定変更を展開すると、Configuration Manager によって展開ジョブが作成されます。	はい。

質問	チケット管理が有効になっている Workflow 以外のモード	チケット管理が無効になっている Workflow 以外のモード	Workflow モード
設定変更をデバイスに展開するにはどうすればよいですか。	次のいずれかを実行します。 • **[ファイル（File）] > [展開（Deploy）]** を選択します。 • **[管理（Manage）] > [展開（Deployments）]** を選択して、[展開ジョブ（Deployment Jobs）] タブで [展開（Deploy）] をクリックします。	次のいずれかを実行します。 • [メイン（Main）] ツールバーで**[変更の送信と展開（Submit and Deploy Changes）]** ボタンをクリックします。 • **[ファイル（File）] > [送信と展開（Submit and Deploy）]** を選択します。 • **[管理（Manage）] > [展開（Deployments）]** を選択して、[展開ジョブ（Deployment Jobs）] タブで [展開（Deploy）] をクリックします。	**[管理（Manage）] > [展開（Deployments）]** を選択して、展開ジョブを作成します。
設定変更用の CLI コマンドはどの段階で生成されますか。	展開の開始時。	展開の開始時。	展開ジョブの作成時。

質問	チケット管理が有効になっている Workflow 以外のモード	チケット管理が無効になっている Workflow 以外のモード	Workflow モード
現在の変更を削除するにはどうすればよいですか。	**[チケット（Tickets）] > [チケットの破棄（Discard Ticket）]** を選択して、現在開いているチケットを破棄するか、Ticket Manager でチケットを選択して [破棄（Discard）] をクリックします。 デバイスの展開をすでに開始している場合は、Deployment Manager でジョブを選択して [中止（Abort）] をクリックし、展開を中止します。	**[ファイル（File）] > [破棄（Discard）]** の順に選択します。 デバイスの展開をすでに開始している場合は、Deployment Manager でジョブを選択して [中止（Abort）] をクリックし、展開を中止します。	**[アクティビティ（Activities）] > [アクティビティの破棄（Discard Activity）]** の順に選択して現在開いているアクティビティを破棄するか、または Activity Manager でアクティビティを選択して [破棄（Discard）] をクリックします。 展開ジョブを作成済みの場合は、Deployment Manager でジョブを選択して [破棄（Discard）] をクリックします。ジョブを展開済みの場合は、[中止（Abort）] を選択するとジョブを中断できます。
複数のユーザが同時に Security Manager にログインできますか。	はい。各ユーザーは異なるチケットを開き、設定変更ができます。一人のユーザーが複数回ログインできますが、ユーザーは別のチケットを開く必要があります。	はい。ただし、各ユーザのユーザ名が異なる場合だけです。同じユーザ名のユーザが Security Manager にログインすると、最初のユーザは自動的にログアウトされます。	はい。各ユーザは異なるアクティビティを開き、設定変更を行うことができます。単一のユーザが複数回ログインできますが、ユーザは別個のアクティビティを開く必要があります。
別のユーザが設定しているデバイスを設定するとどうなりますか。	デバイスがロックされていることを示すメッセージが表示されます。アクティビティとロッキング （180 ページ） を参照してください。		

JumpStart を使用した Security Manager の理解

JumpStart は Security Manager を紹介する手引きです。製品の使用にかかわる主な概念の説明が記載されています。Security Manager の機能を試しに使用する場合は、JumpStart を使用してください。

JumpStart は、Security Manager を初めて起動したときに自動的に開きます。Security Manager の使用中に JumpStart を起動するには、Configuration Manager のメインメニューから **[ヘルプ（Help）] > [JumpStart]** の順に選択します。

JumpStart には、次のナビゲーション機能があります。

- コンテンツ テーブル。常に右上隅に表示されます。ページを開くにはエントリをクリックします。
- ページ内のリンク。JumpStart 内の詳細情報およびオンライン ヘルプ内の関連情報にドリルダウンできます。

Security Manager の初期設定の実行

Security Manager をインストールしたら、いくつかの設定手順を実行してインストールを完了します。初期設定するほとんどの機能にはデフォルト設定がありますが、機能をよく理解して、デフォルト設定が組織に最適な設定かどうかを判断する必要があります。

次に、初期設定が必要な機能のリストを示します。示されている詳細情報の参照先も参照してください。これらの機能は任意の順序で設定できます。また、まだ使用する必要のない機能の設定は、後回しにすることもできます。

- SMTP サーバおよびデフォルト電子メール アドレスを設定します。Security Manager では、システム内で行われたさまざまなアクションに対して、電子メール通知を送信できます。たとえば、展開ジョブによるネットワーク デバイスの再設定が完了すると、電子メールを受信します。電子メール通知が動作するためには、SMTP サーバを設定する必要があります。

SMTP サーバーおよびデフォルト電子メールアドレスの設定の詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）を参照してください。

- ユーザ アカウントを作成します。ユーザが製品を使用する場合は、Security Manager にログインする必要があります。ただし、別のユーザがすでに使用しているアカウントを使用してログインすると、最初のユーザは自動的に切断されます。したがって、ユーザごとに一意のアカウントを設定する必要があります。Security Manager サーバにローカルなアカウントを作成することも、ACS システムを使用してユーザ認証を管理することもできます。詳細については、*Cisco Security Manager インストレーションガイド* [英語] を参照してください。
- デフォルトの展開を設定します。ユーザは、デバイスに設定を展開するときに、設定の展開方法および Security Manager で異常を処理する方法を選択できます。ただし、システム

デフォルト設定を選択する方が、組織の推奨事項への準拠は容易になります。展開のデフォルト値を設定するには、Configuration Manager で [ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [展開（Deployment）] を選択して [展開（Deployment）] 設定ページを開きます（[Deployment] ページ （658 ページ）を参照）。

特に重要なのは、次の展開設定です。

- • デフォルトの展開方式：デバイスまたは転送サーバに設定の展開を直接書き込むか、または Security Manager サーバの指定したディレクトリに設定ファイルを書き込むかどうか。デフォルトでは、デバイスの設定が行われると、その設定はデバイスまたは転送サーバに直接展開されます。ただし、設定ファイルを展開する独自の方法があるときは、デフォルトの展開方式として [File] を選択する必要がある場合があります。展開方式の詳細については、展開方法について （490 ページ）を参照してください。

  • アウトオブバンド変更の検出時：Security Manager ではなく CLI を使用してデバイスの設定変更が行われたとき、そのことを Security Manager で検出した場合の対処方法。デフォルトでは、警告が発行されて展開が続行し、CLI を介して行われた変更が上書きされます。ただし、この動作は、単に変更チェックをスキップする（つまり、Security Manager は変更を上書きするが警告は行わない）か、または展開をキャンセルしてデバイスを現在の状態にしておくように変更できます。アウトオブバンド変更を処理する方法の詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

  • エラー時のダウンロード許可：軽微な設定エラーが検出された場合に、展開の継続を許可するかどうか。デフォルトでは、軽微なエラーが検出された場合は展開を許可しません。

- ワークフローモードを選択します。デフォルトのモードは、チケット管理が有効になっている Workflow 以外のモードです。Workflow 以外のモードでは、設定を作成および展開するときのユーザの自由度が高くなります。ただし、ネットワーク管理に対してトランザクション指向の強い方法を必要とする組織で、別々のユーザがポリシーの作成、承認、および展開を実行する場合は、Workflow モードをイネーブルにすると独自の手順を実行できます。Workflow モードを使用する場合は、必要な作業を分担するためのユーザ アカウントを定義するとき、ユーザ権限を正しく設定します。使用できるワークフロータイプの詳細については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。ワークフロー モードを変更する方法の詳細については、ワークフロー モードの変更 （36 ページ）を参照してください。

ヒント Workflow 以外のモードでチケット管理を無効にすると、ほとんどのアクティビティ管理タスクを自動化できます。

- デフォルトのデバイス通信を設定します。デバイスのタイプに基づいてデバイスにアクセスする場合、Security Manager は最も一般的に利用される方式を使用します。たとえば、Security Manager が Catalyst スイッチに接続する場合、デフォルトでは SSH を使用します。

デフォルトのプロトコルが大部分のデバイスで動作する場合は、プロトコルを変更する必要はありません。デフォルト以外のプロトコルを使用するデバイスの場合は、個々のデバイスのデバイス プロパティでプロトコルを変更できます。ただし、Security Manager のデフォルトではないプロトコルを常に使用する場合（たとえば、ルータに Token Management Server（TMS）を使用する場合など）、デフォルト設定を変更する必要があります。デフォルトの通信設定を変更するには、Configuration Manager で [ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します。[Device Connection Settings] グループで、デバイスのタイプごとに最適なプロトコルを選択します。デフォルトの接続タイムアウトおよび再試行の設定を変更することもできます。デバイスの通信設定の詳細については、[Device Communication] ページ （668 ページ）を参照してください。

- Security Manager で管理するルータ ポリシーおよびファイアウォール ポリシーのタイプを選択します。Security Manager で IPS デバイスを管理すると、必然的に設定全体を管理することになります。ただし、ルータおよびファイアウォール デバイス（ASA、PIX、および FWSM）の場合は、Security Manager で管理するポリシーのタイプを選択できます。その他の部分のデバイス設定は、他のツール（デバイスの CLI を含む）を使用して管理できます。デフォルトでは、すべてのセキュリティ関連のポリシーが管理対象です。管理するポリシーを変更するには、Configuration Manager で [ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [ポリシー管理（Policy Management）] の順に選択します。これらの設定を変更する方法および変更の前後に実行する作業の詳細については、ルータおよびファイアウォールデバイスのポリシー管理のカスタマイズ （221 ページ）を参照してください。
- ファイアウォール イベントおよび IPS イベントの管理に Event Viewer を使用するかどうかを決定します。デバイスから Syslog イベントを収集するためのディスクと場所、および Syslog 通信に使用するポート番号を設定できます。イベント管理に Security Manager を使用しない場合は、この機能をオフにできます（デフォルトではイネーブル）。設定オプションの詳細については、[Event Management] ページ （677 ページ）を参照してください。
- Cisco Security Monitoring, Analysis and Response System（CS-MARS）と通信するために Security Manager を設定します。CS-MARS を使用してネットワークをモニタする場合は、サーバを識別して Security Manager に登録すると、Security Manager から CS-MARS イベント情報にアクセスできます。この相互通信を設定する方法の詳細については、CS-MARS と Security Manager を統合するためのチェックリスト （3728 ページ）を参照してください。

電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定

Security Manager では、展開ジョブの完了、アクティビティの承認、または ACL ルールの期限切れなど、さまざまなタイプのイベントの発生時に電子メール通知を送信できます。電子メール通知をイネーブルにするには、Security Manager で電子メールの送信に使用できる SMTP サーバを設定する必要があります。その後、次の設定ページで電子メールアドレスおよび通知の設定を行うことができます（Configuration Manager で [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] の順に選択し、コンテンツテーブルからページを選択します）。

- [Workflow] ページ：展開ジョブとアクティビティ用のデフォルト電子メールアドレスおよび通知設定の場合。展開ジョブおよびアクティビティを管理する場合にデフォルト値を上書きできます。
- [Rules Expiration] ページ：ACL ルールの期限切れに対するデフォルト電子メール アドレスおよび通知設定の場合。ルールが期限切れになるのは、有効期限を設定した場合だけです。
- [IPS Updates] ページ：IPS Update のアベイラビリティを通知する電子メール アドレスの場合。
- [サーバーセキュリティ（Server Security）] ページ：ローカルユーザアカウントを設定するときに（[ローカルユーザ設定（Local User Setup）] をクリック）、ユーザの電子メールアドレスを指定する場合。このアドレスは、展開ジョブの完了などを通知する場合のデフォルト ターゲットとして使用されます。
- [Event Management] ページ：拡張データ ストレージの場所を設定する場合は、少なくとも 1 つの電子メールアドレスを指定する必要があります。電子メールアドレスは、拡張保管場所の使用で問題が発生した場合に通知を受信します。また、Syslog リレーサービスを使用している場合は、syslog リレーサービスが CPU スロットリングを出入りするときに通知される電子メールアドレスを設定できます。

ヒント ユーザ認可に ACS を使用している場合は、ACS 統合手順で、SMTP サーバーおよびシステム管理者の電子メールアドレスを設定済みである必要があります（『Installation Guide for Cisco Security Manager』を参照）。すべての ACS サーバが利用不能な状態になると、Security Manager はこのアドレスに通知を送信します。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

ステップ 1 Security Manager サーバで CiscoWorks Common Services にアクセスします。

- Security Manager クライアントを使用中の場合、最も簡単にアクセスするには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] の順に選択し、コンテンツテーブルから [サーバーセキュリティ（Server Security）] を選択して、そのページのいずれかのボタンをクリックします（[ローカルユーザ設定（Local User Setup）] など）。
- Web ブラウザを使用して Security Manager サーバーのホームページ（https://*servername*/CSCOnm/servlet/login/login.jsp）にログインし、[サーバー管理（Server Administration）] をクリックします。

ステップ 2 [サーバー（Server）] > [管理（Admin）] の順にクリックして、コンテンツテーブルから [システム設定（System Preferences）] を選択します。

ステップ 3 [System Preferences] ページで、Security Manager が使用できる SMTP サーバのホスト名または IP アドレスを入力します。SMTP サーバが電子メール メッセージを送信する場合に、ユーザ認証は必要ありません。

また、CiscoWorks が電子メールの送信に使用できる電子メール アドレスを入力します。このアドレスは、Security Manager から送信される通知用に設定した電子メール アドレスと同じである必要はありません。ACS を使用して認可を行っている場合は、すべての ACS サーバが利用不能な状態になると、Security Manager はこのアドレスに電子メール メッセージを送信します。このメッセージにより、早急な対応を必要とする問題に対して警告を出すことができます。管理者は、ACS に関連しないイベントについて、Common Services から電子メール メッセージを受け取る場合もあります。

ステップ 4 [Apply] をクリックして変更内容を保存します。

ワークフロー モードの変更

適切な管理者権限がある場合は、Security Manager で実行されるワークフロー モードを変更できます。ワークフローモードを変更すると、ユーザには大きな影響があります。変更を行う場合は、次の点を考慮してください。

- ワークフロー モードを変更すると、同じサーバを使用しているすべての Security Manager ユーザに対して、変更が有効となります。
- Workflow モードから Workflow 以外のモードに変更する場合は、編集可能状態（Edit、Edit Open、Submit、または Submit Open）にあるアクティビティをすべて承認または廃棄し、生成済みのジョブをすべて展開、拒否、廃棄、または中断して、デバイスのロックを解放する必要があります。エラー状態にあるジョブに対しては、何も行う必要はありません。
- Workflow 以外のモードでチケット管理を無効にする前に、編集可能な状態（[編集（Edit）] または [編集オープン（Edit Open）]）になっているすべてのチケットを送信または破棄する必要があります。
- Workflow モードから Workflow 以外のモードに変更したあとに、以前のバージョンのデータベースを復元した場合は、復元されたデータベースに編集可能状態（Edit、Edit Open、Submit、または Submit Open）のアクティビティが存在すると、Security Manager は自動的に Workflow モードに切り替わります。編集可能なアクティビティを承認または削除してから、Workflow モードを再度オフにします。
- Workflow 以外のモードから Workflow モードに変更した場合、または Workflow 以外のモードでチケット管理を有効にした場合、現在の設定セッションは Edit_Open 状態のアクティビティ/チケットとして一覧に表示されるため、これらのアクティビティ/チケットは明示的に管理する必要があります。
- チケット管理が有効または無効になっている場合、Cisco Security Manager にログインしている他のユーザーはすべてログアウトされます。

ワークフローモードの説明については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。

ステップ 1 Configuration Manager で **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** の順に選択し、目次から [ワークフロー（Workflow）] を選択して [ワークフロー（Workflow）] ページを開きます（[Workflow] ページ （745 ページ）を参照）。

ステップ 2 [Workflow Control] グループでワークフローモード設定を行います。[Enable Workflow] をオンにして Workflow モードを使用する場合は、次のオプションを選択することもできます。

- [Require Activity Approval]：ポリシー変更をデータベースにコミットする前に、アクティビティの明示的な承認を実行します。
- [送信者がアクティビティを承認可能（Submitter can Approve Activity）]：送信者は、送信ロールと承認ロールを分離する代わりに、自分のアクティビティも承認できます（有効になっている場合）。
- [Require Deployment Approval]：展開ジョブを実行する前に、ジョブの明示的な承認を実行します。
- [送信者が展開ジョブを承認可能（Submitter can Approve Deployment Job）]：有効にすると、送信者は自分が送信した展開ジョブを承認できます。

ステップ 3 電子メール通知設定を行います。ここで設定するのは、電子メール送信者（つまり Security Manager）、アプルーバ、および展開ジョブの完了時に通知が必要な別のユーザまたは電子メール エイリアスのデフォルト電子メール アドレスです。

ジョブ ステータスの通知を送信するときにジョブ展開者を含めたり、展開ジョブのステータスが変更された場合に電子メール通知を送信するように設定することもできます。

ステップ 4 [保存（Save）] をクリックして、変更を保存および適用します。

ステップ 5 目次から [ワークフロー（Workflow）] を選択して、[チケット管理（Ticket Management）] ページを開きます（[Token Management] ページ （742 ページ）を参照）。

ステップ 6 [チケット管理（Ticket Management）] 設定を設定します。[チケットの有効化（Enable Ticketing）] を選択すると、次のオプションも選択できます。

（注） これらのフィールドの詳細については、[Token Management] ページ （742 ページ）を参照してください。

- [チケットシステムURL（Ticket System URL）]：チケット ID と外部チケット管理システム間のリンクを提供します。
- [チケット履歴（Ticket History）]：チケットに関連する情報を保持する期間を指定します。

ステップ 7 [保存（Save）] をクリックして、変更を保存および適用します。

Security Manager インターフェイスの基本機能について

ここでは、メニュー コマンドの説明、ツールバーのボタン、およびユーザ インターフェイスの共通要素の使用方法など、基本的なインターフェイス機能について説明します。説明されている機能の多くは、Configuration Manager だけで使用されます。

- Configuration Manager のメニュー バー リファレンス （38 ページ）
- ツールバー リファレンス（Configuration Manager） （51 ページ）
- セレクタの使用 （60 ページ）
- ウィザードの使用 （63 ページ）
- テーブルの使用 （64 ページ）
- テキスト フィールドの使用方法 （66 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）
- ユーザ インターフェイスに問題がある場合のトラブルシューティング （69 ページ）

Configuration Manager のメニュー バー リファレンス

Configuration Manager のメニュー バーには、Security Manager を使用するためのコマンドを含むメニューがあります。コマンドは、実行中のタスクに応じて利用不能な状態になる場合があります。

ここでは、メニュー バーに含まれるメニュー項目について説明します。

- [File] メニュー（Configuration Manager） （39 ページ）
- [Edit] メニュー（Configuration Manager） （40 ページ）
- [View] メニュー（Configuration Manager） （41 ページ）
- [Policy] メニュー（Configuration Manager） （42 ページ）
- [Map] メニュー（Configuration Manager） （43 ページ）
- [Manage] メニュー（Configuration Manager） （45 ページ）
- [Tools] メニュー（Configuration Manager） （46 ページ）
- [Launch] メニュー（Configuration Manager） （49 ページ）
- [Activities] メニュー（Configuration Manager） （48 ページ）
- Tickets Menu（Configuration Manager） （48 ページ）
- [Help] メニュー（Configuration Manager） （51 ページ）

[File] メニュー（Configuration Manager）

次の表に、Configuration Manager の [File] メニューのコマンドを示します。メニュー項目は、ワークフロー モードによって異なります。

表 2 : [File] メニュー（*Configuration Manager*）

コマンド	説明
新規デバイス（New Device）	新しいデバイスを追加するウィザードを開始します。デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。
Clone Device	既存のデバイスを複製してデバイスを作成します。デバイスの複製 （160 ページ）を参照してください
デバイスの削除	デバイスを削除します。Security Manager インベントリからのデバイスの削除 （162 ページ）を参照してください。
保存	アクティブなページで行われた変更を保存します。ただし、Security Manager データベースには変更を送信しません。
インポート	別の Security Manager サーバからエクスポートされたポリシーとデバイスをインポートします。ポリシーまたはデバイスのインポート （615 ページ）を参照してください。
エクスポート	ポリシーまたはデバイスをエクスポートして、別の Security Manager サーバにインポートできるようにします。デバイスのエクスポートはポリシー情報を含んでいるか、CiscoWorks Common Services Device Credential Repository（DCR）または Cisco Security Monitoring, Analysis and Response System（CS-MARS）にインポートできる単純な CSV ファイルです。Security Manager クライアントからのデバイス インベントリのエクスポート （605 ページ）および共有ポリシーのエクスポート （612 ページ）を参照してください。
変更の表示 （Workflow 以外のモードのみ）	現在の設定セッションのアクティビティ変更レポート（PDF 形式）を開きます。 Workflow モードで現在のアクティビティの変更を確認するには、**[アクティビティ（Activities）] > [変更の表示（View Changes）]** の順に選択します。
検証（Validate） （Workflow 以外のモードのみ）	保存済みの変更を検証します。アクティビティ/チケットの検証 （200 ページ）を参照してください。 Workflow モードで現在のアクティビティを検証するには、**[アクティビティ（Activities）] > [アクティビティの検証（Validate Activity）]** の順に選択します。

コマンド	説明
送信 （Workflow 以外のモードのみ）	Security Manager データベースに最後に送信したあとに行われた変更をすべて送信します。 Workflow モードで現在のアクティビティを検証するには、**[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）]** の順に選択します。
Submit and Deploy （Workflow 以外のモードのみ）	Security Manager データベースに最後に送信したあとに行われた変更をすべて送信し、最後に展開したあとに行われた変更をすべて展開します。 展開について （481 ページ）を参照してください。 Workflow モードでは、アクティビティが承認され、デバイスへの変更を展開する展開ジョブを作成する必要があります。
[展開（Deploy）] （Workflow 以外のモードのみ）	最後の展開よりあとに行われた変更をすべて展開します。 展開について （481 ページ）を参照してください。 Workflow モードでは、アクティビティが承認され、デバイスへの変更を展開する展開ジョブを作成する必要があります。
廃棄 （Workflow 以外のモードのみ）	最後の送信よりあとの設定変更をすべて廃棄します。 Workflow モードで現在のアクティビティを検証するには、**[アクティビティ（Activities）] > [アクティビティの破棄（Discard Activity）]** の順に選択します。
Edit Device Groups	デバイス グループを編集します。 デバイス グループの使用 （164 ページ）を参照してください。
New Device Group	デバイス グループを追加します。 デバイス グループの作成 （168 ページ）を参照してください。
グループへのデバイスの追加	グループにデバイスを追加します。 デバイス グループに対するデバイスの追加と削除 （169 ページ）を参照してください。
印刷（Print）	アクティブなページを印刷します。 印刷できるのは一部のページだけです。[Print] コマンドが使用不能になっている場合は、アクティブなページを印刷できません。
終了（Exit）	Security Manager を終了します。

[Edit] メニュー（Configuration Manager）

次の表に、Configuration Manager の [Edit] メニューのコマンドを示します。通常、これらのコマンドを使用できるのは、ポリシー内のテーブルを操作している場合、およびルールテーブルに関する作業を行っている場合だけです（ルール テーブルの使用 （764 ページ）を参照）。

表 3 : [Edit] メニュー（Configuration Manager）

コマンド	説明
切り取り（Cut）	ルール テーブルで選択した行をカットして、クリップボードに保存します。
コピー（Copy）	ルール テーブルで選択した行をコピーして、クリップボードに保存します。
貼り付け	ルール テーブルで選択した行のあとに、クリップボードからルール テーブルの行をペーストします。
行を追加（Add Row）	アクティブなテーブルに行を追加します。
Edit Row	選択したテーブル行を編集します。
Delete Row	選択したテーブル行を削除します。
Move Row Up Move Row Down	選択した行をルール テーブル内で上下に移動します。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。
[グローバル検索（Global Search）]	[グローバル検索（Global Search）] ウィンドウが開きます。詳細については、グローバル検索の使用 （55 ページ）を参照してください。

[View] メニュー（Configuration Manager）

Configuration Manager の [View] メニューには、ユーザ インターフェイス内をナビゲートするか、ツールバーを変更するためのコマンドがあります。

表 4 : [View] メニュー

メニュー コマンド	説明
デバイス ビュー	デバイス ビューを開きます。デバイス ビューの概要 （20 ページ）を参照してください。
デバイスステータスビュー（Device Status View）	[デバイスステータスビュー（Device Status View）] ウィンドウを開きます。[デバイスステータスビュー（Device Status View）] の使用 （170 ページ）を参照してください。
Map View	マップ ビューを開きます。マップ ビューの概要 （23 ページ）を参照してください。
Policy View	ポリシー ビューを開きます。ポリシー ビューの概要 （22 ページ）を参照してください。

メニュー コマンド	説明
ポリシーバンドルビュー（Policy Bundle View）	ポリシーバンドルビューを開きます。 ポリシーバンドルの管理 を参照してください。
Customized Toolbar	ツールバーで一部のオプションのボタンを追加または削除できます。ツールバーに表示できるすべてのボタンについては、ツールバー リファレンス（Configuration Manager） （51 ページ）を参照してください。

[Policy] メニュー（Configuration Manager）

Configuration Manager の [Policy] メニューには、ポリシーを管理するためのコマンドがあります。

表 5 : [Policy] メニュー（*Configuration Manager*）

メニュー コマンド	説明
Share Policy	アクティブなローカル ポリシーを共有ポリシーとして保存します。 ローカル ポリシーの共有 （262 ページ）を参照してください。
Unshare Policy	アクティブな共有ポリシーをローカル ポリシーとして保存します。 ポリシーの共有解除 （265 ページ）を参照してください。
Assign Shared Policy	デバイスに共有ポリシーを割り当てます。 デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）を参照してください。
Unassign Policy	選択したデバイスから現在のポリシーの割り当てを解除します。 ポリシーの割り当て解除 （255 ページ）を参照してください。
Copy Policies Between Devices	デバイス間でポリシーをコピーします。デバイス間でのポリシーのコピー （251 ページ）を参照してください
Share Device Polices	ローカル デバイス ポリシーを共有できるようにします。 ローカル ポリシーの共有 （262 ページ）を参照してください。
Edit Policy Assignments	デバイスに対する共有ポリシーの割り当てを編集します。 ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。
ポリシーの複製	新しい名前でポリシーのコピーを作成します。共有ポリシーのクローニング（コピー） （270 ページ）を参照してください。
Rename Policy	共有ポリシー名の変更 （270 ページ）

メニュー コマンド	説明
Add Local Rules	デバイスの共有ポリシーにローカル ルールを追加します。このコマンドを使用するには、ルールベースの共有ポリシーを選択する必要があります。
Inherit Rules	ポリシーの継承を編集します。ルールの継承または継承の解除（269 ページ）を参照してください。
Discover Policies on Device	デバイス上のポリシーを検出します。ポリシーの検出 （223 ページ）を参照してください。
Discover VPN Policies	Discover VPN Policies ウィザードを開きます。サイト間 VPN ディスカバリ （1406 ページ） を参照してください。

[Map] メニュー（Configuration Manager）

Configuration Manager の [Map] メニューには、マップ ビューを使用するためのコマンドがあります。このメニューのコマンドを使用できるのは、マップ ビューが開いている場合だけです。詳細については、マップ ビューの使用 （2049 ページ）を参照してください。

表 *6 : [Map] メニュー（Configuration Manager）*

メニュー コマンド	説明
New Map	マップを作成します。新しいマップまたはデフォルト マップの作成（2059 ページ）を参照してください。
Open Map	保存済みのマップまたはデフォルト マップを開きます。マップを開く （2060 ページ）を参照してください。
Show Devices On Map	アクティブなマップ上に表示する管理対象デバイスを選択します。マップでの管理対象デバイスの表示 （2067ページ）を参照してください。
Show VPNs On Map	アクティブなマップ上に表示する VPN を選択します。マップにおける既存 VPN の表示 （2074 ページ）を参照してください。
Add Map Object	開いたマップ上にマップ オブジェクトを作成します。ネットワーク トポロジを表すマップ オブジェクトの使用方法 （2069ページ）を参照してください。
Add Link	開いたマップ上にレイヤ 3 リンクを作成します。マップにおけるレイヤ 3 リンクの追加と管理 （2072 ページ）を参照してください。
Find Map Node	開いたマップ上のノードを検索します。マップ ノードの検索 （2063 ページ）を参照してください。

メニュー コマンド	説明
Save Map	開いたマップを保存します。マップの保存 （2060 ページ）を参照してください。
Save Map As	開いたマップに新しい名前を付けて保存します。マップの保存 （2060 ページ）を参照してください。
拡大（Zoom In）	マップをズームインします。マップのパン、中央への配置、およびズーム （2062 ページ）を参照してください。
縮小（Zoom Out）	マップをズームアウトします。マップのパン、中央への配置、およびズーム （2062 ページ）を参照してください。
ウィンドウに合わせる	開いたマップをズームしてマップ全体を表示します。マップのパン、中央への配置、およびズーム （2062 ページ）を参照してください。
Display Actual Size	開いたマップをズームして実際のサイズを表示します。マップのパン、中央への配置、およびズーム （2062 ページ）を参照してください。
Refresh Map	更新されたネットワーク データを使用して、開いたマップをリフレッシュします。新しいマップまたはデフォルト マップの作成 （2059 ページ）を参照してください。
Export Map	開いたマップをファイルにエクスポートします。マップのエクスポート （2061 ページ）を参照してください。
マップの削除	選択したマップをリストから削除します。マップの削除 （2061 ページ）を参照してください。
マップのプロパティ	開いたマップのプロパティを表示または編集します。マップの背景プロパティの設定 （2064 ページ）を参照してください。
Show/Hide Navigation Window	開いたマップのナビゲーション ウィンドウの表示/非表示を切り替えます。ナビゲーション ウィンドウの使用方法 （2053 ページ）を参照してください。
Undock/Dock Map View	マップのウィンドウを切り離して、マップを開いたままで他の機能を使用できるようにします。すでにウィンドウが切り離されている場合は、[Dock Map View] コマンドを選択すると、Security Manager のメイン ウィンドウに再度固定されます。マップ ビューのメイン ページについて （2050 ページ） を参照してください。

[Manage] メニュー（Configuration Manager）

Configuration Manager の [Manage] メニューには、Security Manager のメイン インターフェイスとは独立したウィンドウで実行されるツールを起動するコマンドがあります。このメニューを使用すると、現在使用中のページを閉じることなく、さまざまな機能にアクセスできます。

表 7 : *[Manage] メニュー（Configuration Manager）*

メニュー コマンド	説明
ポリシー オブジェクト	Policy Object Manager を開きます。このツールでは、使用可能なすべてのオブジェクトを、オブジェクト タイプに従ってグループ化して表示できます。また、オブジェクトを作成、コピー、編集、および削除できるほか、使用状況レポートを生成できます。使用状況レポートには、選択したオブジェクトが、他の Security Manager オブジェクトおよびポリシーからどのように使用されているかが記述されます。詳細については、Policy Object Manager （290 ページ）を参照してください。
Site-to-Site VPNs	Site-to-Site VPN Manager を開きます。このツールでは、サイト間 VPN を設定できます。サイト間 VPN の管理：基本 （1379 ページ）を参照してください。
アクティビティ（Workflow モード限定）	Activity Manager を開きます。このツールでは、アクティビティを作成および管理できます。アクティビティ/チケット マネージャ ウィンドウ （189 ページ）を参照してください。
展開（Deployments）	Deployment Manager を開きます。このツールでは、設定の展開および展開ジョブの管理を実行できます。展開の管理 （481 ページ）を参照してください
設定アーカイブ（Configuration Archive）	デバイス設定のアーカイブされたバージョンを格納し、設定の表示と比較、およびある設定から別の設定へのロールバックを実行できます。[Configuration Archive] ウィンドウ （509 ページ）を参照してください。
Policy Discovery Status	[Policy Discovery Status] ウィンドウを開きます。このウィンドウでは、ポリシー検出およびデバイス インポートのステータスを確認できます。ポリシー検出タスクのステータスの表示 （237 ページ）を参照してください。
IPS	デバイスの通信に必要な IPS デバイス証明書を管理します。
Audit Report	監査レポートページに設定されたパラメータに従って、監査レポートを生成します。[Audit Report] ウィンドウの使用 （624 ページ）を参照してください。

メニュー コマンド	説明
Change Reports （Workflow 以外のモードのみ）	デバイスに対する変更、共有ポリシー、および以前の設定セッションのポリシー オブジェクトに関するレポートを生成できます。変更レポートの表示 （197 ページ）を参照してください。 現在の設定セッション中に行われた変更を表示するには、[ファイル（**File**）] > **[変更の表示（View Changes）]** を選択します。]

[Tools] メニュー（Configuration Manager）

に

[Device Properties] ウィンドウを開きます。このウィンドウには、デバイス、クレデンシャル、デバイスの割り当て先グループ、およびポリシー オブジェクトの上書きに関する一般情報が表示されます。詳細については、デバイス プロパティについて （93 ページ）を参照してください。

Configuration Manager の [ols] メニューには、Security Manager のメインインターフェイスとは独立したウィンドウで実行されるツールを起動するコマンドがあります。このメニューを使用すると、現在使用中のページを閉じることなく、さまざまな機能にアクセスできます。

表 *8 : [Tools] メニュー（Configuration Manager）*

メニュー コマンド	説明
デバイス プロパティ	
Detect Out of Band Changes	デバイスを分析して、最後に Security Manager が設定を展開してから設定が変更されたかどうかを判別します。この情報を使用して、重要な設定変更が失われないようにできます。アウトオブバンド変更の検出および分析 （537 ページ）を参照してください。
Packet Capture Wizard	ASA デバイスでパケットの取り込みを設定できる Packet Capture Wizard を開きます。
Ping, TraceRoute and NSLookup	これらのトラブルシューティング コマンドを使用できる ping、TraceRoute、および NSLookup ツールを開きます。ping と TraceRoute は管理対象デバイスで稼働しますが、NSLookup はクライアント ワークステーションで稼働します。ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析 （3713 ページ）を参照してください。

メニュー コマンド	説明
IPインテリジェンス（IP Intelligence）	IP インテリジェンスツールを開きます。ここから、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS 情報など、IPv4 アドレスに関するさまざまな情報にアクセスできます。IP インテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence）（3723 ページ）を参照してください。 IP インテリジェンス機能を使用する前に、[IP インテリジェンス設定（IP Intelligence Settings）] ページでこれらの機能を有効にして設定する必要があります([IPインテリジェンス設定（IP Intelligence Settings）] ページ（696 ページ）を参照)。
壁面	同じ Security Manager サーバーにログインしているすべてのユーザにメッセージを送信できる [ウォール（Wall）] ウィンドウを開きます。ただし、最初に、[ウォール設定（Wall Settings）] ページで有効にする必要があります。[ウォール設定（Wall Settings）] ページ（747 ページ）を参照してください。
Show Containment	デバイスのセキュリティ コンテキストまたはサービス モジュールを表示します。 デバイスに含まれている要素の表示 （160 ページ）を参照してください。
インベントリ ステータス	すべてのデバイスのデバイス概要情報を表示します。 インベントリ ステータスの表示 （3694 ページ）を参照してください。
Catalyst Summary Info	選択した Catalyst スイッチ上で Security Manager が検出したすべてのサービス モジュール、ポート、および VLAN を含む、システム情報の概要を表示します。 Catalyst サマリー情報の表示 （3403 ページ）を参照してください。
Apply IPS Update	IPS イメージおよびシグニチャの更新を手動で適用します。 IPS 更新の手動適用 （2307 ページ）を参照してください。
Preview Configuration	特定のデバイスの提示された変更、最後に展開された設定、または現在実行中の設定を表示します。 設定のプレビュー （535 ページ）を参照してください。
バックアップ	CiscoWorks Common Services を使用して、Security Manager データベースをバックアップします。Security Manager データベースのバックアップおよび復元 （629 ページ）を参照してください。
Security Manager Diagnostics	Technical Assistance Center（TAC）からの要求に応じて送信するトラブルシューティング情報を収集します。Cisco Technical Assistance Center 用の診断ファイルの作成 （633 ページ）を参照してください。 ヒント Cisco Security Manager バージョン 4.7 以降では、既存の [一般的な診断（General Diagnostics）] の代わりに [ライト診断（Light Diagnostics）] を選択できます。

メニュー コマンド	説明
Security Manager Administration	Security Manager の機能を制御する、システム全体の設定を行います。

[Activities] メニュー（Configuration Manager）

Configuration Manager の [Activities] メニューには、アクティビティを管理するためのコマンドがあります。このメニューは、Workflow モードがイネーブルの場合だけ表示されます。これらのコマンドの詳細については、Workflow モードでのアクティビティ機能へのアクセス （186 ページ）を参照してください。

表 *9 : [Activities]* メニュー（*Configuration Manager*）

メニューコマンド	説明
New Activity	新しいアクティビティを作成します。アクティビティ/チケットの作成 （193 ページ）を参照してください。
Open Activity	アクティビティを開きます。アクティビティ/チケットを開く （195 ページ）を参照してください。
Close Activity	開いているアクティビティを閉じます。アクティビティ/チケットを閉じる （196 ページ）を参照してください。
変更の表示	アクティビティ変更レポート（PDF 形式）を開きます。変更レポートの表示 （197 ページ）を参照してください。
Validate Activity	開いているアクティビティを検証します。アクティビティ/チケットの検証 （200 ページ）を参照してください。
Submit Activity	開いているアクティビティを送信します。承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） （202 ページ）を参照してください。
Approve Activity	開いているアクティビティを承認します。アクティビティの承認または拒否（Workflow モード） （203 ページ）を参照してください。
Reject Activity	開いているアクティビティを拒否します。アクティビティの承認または拒否（Workflow モード） （203 ページ）を参照してください。
Discard Activity	開いているアクティビティを廃棄します。アクティビティ/チケットの破棄 （205 ページ） を参照してください。

Tickets Menu（Configuration Manager）

Configuration Manager の [チケット（Tickets）] メニューには、チケットを管理するためのコマンドが含まれています。Workflow 以外のモードでチケット管理が有効になっている場合にの

み表示されます。これらのコマンドの詳細については、 Workflow モードでのアクティビティ機能へのアクセス （186 ページ）を参照してください。

表 *10 : Tickets Menu*（*Configuration Manager*）

メニュー コマンド	説明
新しいチケット（New Ticket）	新しいチケットを作成します。アクティビティ/チケットの作成 （193 ページ）を参照してください。
チケットを開く（Open Ticket）	チケットを開きます。 アクティビティ/チケットを開く（195 ページ）を参照してください。
チケットを閉じる（Close Ticket）	オープンチケットを閉じます。アクティビティ/チケットを閉じる （196 ページ）を参照してください。
変更の表示	チケット変更レポート（PDF 形式）を開きます。 変更レポートの表示 （197 ページ）を参照してください。
チケットの検証（Validate Ticket）	オープンチケットを検証します。アクティビティ/チケットの検証 （200 ページ）を参照してください。
チケットの送信（Submit Ticket）	オープンチケットを送信します。アクティビティ/チケットの状態について （181 ページ）を参照してください。
チケットを破棄（Discard Ticket）	オープンチケットを破棄します。アクティビティ/チケットの検証 （200 ページ） を参照してください。

[Launch] メニュー（Configuration Manager）

[Launch] メニューには、他のアプリケーションを起動するコマンドがあります。

表 *11 : [Launch] メニュー*（*Configuration Manager*）

メニューコマンド	説明
Device Manager	PIX セキュリティ アプライアンス、Firewall Services Module（FWSM; ファイアウォール サービス モジュール）、IPS センサー、IOS ルータ、および Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスなど、サポート対象のすべてのデバイスに関するデバイスマネージャを起動します。デバイス マネージャには、いくつかのモニタリング機能および診断機能があります。この機能を使用すると、デバイスで実行されているサービスに関する情報、およびシステム全体のヘルスのスナップショットを取得できます。 デバイスマネージャの起動 （3697ページ）を参照してください。

メニューコマンド	説明
Prime Security Manager	ASA CX デバイスの管理に使用される Cisco Prime Security Manager（PRSM）アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。
FireSight Management Center	FirePOWER モジュールの管理に使用される FireSIGHT Management Center アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。
ダッシュボード	ダッシュボードが開きます。このダッシュボードは、IPS と FW タスクをより便利にする Security Manager で設定可能な起動点です。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成したり、すべてのダッシュボードをカスタマイズしたりすることができます。ダッシュボードを使用することによって、Security Manager の他のいくつかの領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などの多くのタクスを 1 箇所で実行できます。ダッシュボードの詳細については、ダッシュボードの概要 （3674 ページ）を参照してください。
イベントビューア	Event Viewer を開きます。このツールでは、デバイスイベントを表示および分析できます。詳細については、イベントの表示 （3473 ページ）を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用してイベントビューアが開きます。別のユーザーアカウントを使用してイベントビューアを開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。
Report Manager	セキュリティ レポートと使用状況レポートを生成して分析できる Report Manager を開きます。詳細については、レポートの管理 （3561 ページ）を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用して Report Manager が開きます。別のユーザーアカウントを使用して Report Manager を開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。
Image Manager	ASA デバイスのイメージを管理できる Image Manager を開きます。詳細については、Image Manager の使用 （3749 ページ）を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用して Image Manager が開きます。別のユーザーアカウントを使用して Image Manager を開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。

メニューコマンド	説明
Health and Performance Monitor	Health and Performance Monitor（HPM）を開きます。ここでは、ネットワーク全体のデバイスステータスとトラフィック情報を表示したり、デバイス固有のアラートを表示して確認したりできます。詳細については、ヘルスとパフォーマンスのモニタリング （3611 ページ）を参照してください。 すでに別の Security Manager アプリケーションにログインしている場合は、同じユーザーアカウントを使用して HPM が開きます。別のユーザーアカウントを使用して HPM を開くには、Windows のスタートメニューまたはデスクトップアイコンからアプリケーションを開きます。

[Help] メニュー（Configuration Manager）

Configuration Manager の [Help] メニューには、製品マニュアルおよびトレーニングにアクセスするためのコマンドがあります。詳細については、オンライン ヘルプの利用方法 （70 ページ）を参照してください。

表 *12 : [Help]* メニュー（*Configuration Manager*）

メニュー コマンド	説明
ヘルプ トピック（Help Topics）	オンライン ヘルプ システムを開きます。
Help About This Page	アクティブなページのオンライン ヘルプを開きます。
JumpStart	JumpStart を開きます。
Security Manager Online	Cisco.com の Security Manager Web ページを開きます。
About Configuration Manager	Configuration Manager に関する情報を表示します。

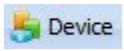
ツールバー リファレンス（Configuration Manager）

メインツールバーには、Configuration Manager のアクションを実行するボタンがあります。

メインツールバーに表示されるボタンは、Workflow/チケット管理モードが有効かどうか、およびツールバーをカスタマイズした方法によって異なります。選択すると、ツールバーに含まれているいくつかのボタンを選択できます。多数のボタンは永続的にツールバーに存在し、削除できません。

次の表に、すべてのボタンを示します。

表 *13 : Configuration Manager* ツールバー

ボタン	説明
	デバイス ビューを開きます。 詳細については、デバイス ビューについて （87 ページ）を参照してください。
	マップ ビューを開きます。 詳細については、マップ ビューの使用 （2049 ページ）を参照してください。
	ポリシー ビューを開きます。 詳細については、ポリシー ビューにおける共有ポリシーの管理 （273 ページ）を参照してください。
	ポリシーバンドルウィンドウを開きます。 詳細については、ポリシーバンドルの管理 （281 ページ）を参照してください。
	Policy Object Manager を開きます。 詳細については、ポリシー オブジェクトの管理 （287 ページ）を参照してください。
	Site-to-Site VPN Manager を開きます。 詳細については、サイト間 VPN の管理：基本 （1379 ページ）を参照してください。
	Deployment Manager を開きます。 詳細については、展開の管理 （481 ページ）を参照してください。
	Audit Report を開きます。 詳細については、監査レポートについて （623 ページ）を参照してください。
	（チケット管理が無効になっている Workflow 以外モードのみ。）変更を送信および展開します。 詳細については、展開の管理 （481 ページ）を参照してください。
	現在選択されているデバイスで定義されている設定ポリシーを検出します。 詳細については、ポリシーの検出 （223 ページ）を参照してください。

ボタン	説明
	現在選択されているデバイスのアウトオブバンド変更（Security Manager の外部のデバイスに対して行った変更）を検出します。 詳細については、アウトオブバンド変更の検出および分析 （537 ページ）を参照してください。
	IP インテリジェンスツールを開きます。ここから、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS 情報など、IPv4 アドレスに関するさまざまな情報にアクセスできます。IP インテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence） （3723 ページ）を参照してください。 IP インテリジェンス機能を使用する前に、[IP インテリジェンス設定（IP Intelligence Settings）] ページでこれらの機能を有効にして設定する必要があります（[IPインテリジェンス設定（IP Intelligence Settings）] ページ （696 ページ）を参照）。
	同じ Security Manager サーバーにログインしているすべてのユーザにメッセージを送信できる [ウォール（Wall）] ウィンドウを開きます。ただし、最初に、[ウォール設定（Wall Settings）] ページで有効にする必要があります。 詳細については、[Workflow] ページ （745 ページ）を参照してください。
	選択した Catalyst スイッチ上で Security Manager が検出したすべてのサービス モジュール、ポート、および VLAN を含む、システム情報の概要を表示します。 詳細については、Catalyst サマリー情報の表示 （3403 ページ）を参照してください。
	現在選択されているデバイスの設定をプレビューします。 詳細については、設定のプレビュー （535 ページ）を参照してください。
	Security Manager の機能を制御する、システム全体の設定を行います。詳細については、Security Manager の管理設定値の設定 （641 ページ）を参照してください。
	現在選択されているデバイスのデバイス マネージャを開きます。 詳細については、デバイス マネージャの起動 （3697 ページ）を参照してください。
	ASA CX デバイスの管理に使用される Cisco Prime Security Manager（PRSM）アプリケーションを起動します。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。

ボタン	説明
	FirePOWER モジュールの管理に使用される FireSIGHT Management Center アプリケーションを起動します。詳細については、 Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。
	ダッシュボード アプリケーションを開きます。 詳細については、ダッシュボードの概要 （3674 ページ）を参照してください。
	Event Viewer アプリケーションを開きます。 詳細については、イベントの表示 （3473 ページ）を参照してください。
	Report Manager アプリケーションを開きます。 詳細については、レポートの管理 （3561 ページ）を参照してください。
	Image Manager アプリケーションを開きます。 詳細については、Image Manager の使用 （3749 ページ）を参照してください。
	ヘルスとパフォーマンスのモニターアプリケーションを開きます。 詳細については、ヘルスとパフォーマンスのモニタリング （3611 ページ）を参照してください。
	現在のページのオンライン ヘルプを開きます。 詳細については、 オンライン ヘルプの利用方法 （70 ページ）を参照してください。
（注） チケット管理が無効になっている場合、Workflow 以外のモードでは次のボタンを使用できません。	
	Workflow モードで [Activity Manager] ウィンドウを開くか、または Workflow 以外モードでチケット管理が有効になっている場合は、[Ticket Manager] ウィンドウを開きます。これらのウィンドウを使用して、アクティビティ/チケットを作成および管理できます。詳細については、アクティビティ/チケット マネージャ ウィンドウ （189 ページ）を参照してください。 [アクティビティ（activity）] ボタン、およびこれらのボタンが有効になる条件の詳細については、 Workflow モードでのアクティビティ機能へのアクセス （186 ページ）を参照してください。 [チケット（ticket）] ボタン、およびこれらのボタンが有効になる条件の詳細については、 Workflow 以外のモードでのチケット機能へのアクセス （188 ページ）を参照してください。
	新しいアクティビティ/チケットを作成します。

ボタン	説明
	アクティビティ/チケットを開きます。
	アクティビティ/チケットが開いている間に行われた変更をすべて保存して閉じます。
	アクティビティ/チケットで行われたすべての変更を評価し、PDF 形式の変更レポートを別のウィンドウ内に生成します。詳細については、変更レポートの表示 （197 ページ）を参照してください。
	現在のアクティビティ/チケット内で変更されたポリシーの整合性を検証します。
	（承認者のWorkflow モードのみ。) アクティビティ承認者がいる Workflow モードを使用している場合、承認のためにアクティビティを送信します。 （チケット管理が有効になっている Workflow 以外モードのみ。）チケットを送信します。チケットを送信すると、提案された変更がデータベースに保存されます。チケットに関連付けられたデバイスはロック解除されるため、ポリシー定義に含めたり、他のチケットで変更したりできます。チケットは、[編集（Edit）]状態または[編集オープン（Edit Open）]状態にある場合に送信できます。
	（Workflowモード限定）アクティビティ内で提案された変更を承認します。
	（Workflowモード限定）アクティビティ内で提案された変更を拒否します。
	選択したアクティビティ/チケットを破棄します。

グローバル検索の使用

Security Manager には、関心のある情報を簡単に見つけて操作するためのグローバル検索機能が用意されています。グローバル検索機能を使用すると、特定の検索文字列を含むデバイス、ポリシーオブジェクト、ポリシー、およびチケットを検索できます。検索の範囲は、デバイス、ポリシーオブジェクト、ポリシー、またはチケットのみに制限できます。

（注） 検索は、コミットされたデータを使用してのみ実行されます。データベースにまだ送信されていない変更は、検索結果に含まれません。

ワイルドカード照合

検索文字列では、次のワイルドカード文字の使用がサポートされています。

- **アスタリスク（*）**：0 個以上の文字と一致します

- **疑問符（?）**は、任意の 1 文字に一致します

セマンティック検索

入力された検索文字列が IP アドレスの場合、Security Manager はセマンティック検索を実行します。たとえば、検索文字列に「192.168.0.0/16」と入力すると、そのサブネットに一致するアイテムに加え、そのサブネットに属する、またはそのサブネットが属する特定のホストまたは他のサブネットが返されます。

グローバル検索範囲

グローバル検索は、すべてではなく、一連のポリシーおよびポリシーオブジェクト内でのみサポートされます。サポートされているポリシーとポリシーオブジェクトは、お客様導入事例で最も頻繁に使用されるポリシーとオブジェクトです。サポートされているポリシーとポリシーオブジェクトは次のとおりです。

- デバイス：すべてのデバイス
- ポリシーオブジェクト：
  - AAA サーバグループ
  - AAAサーバ
  - アクセス コントロール リスト
  - As Path Policies
  - ASA グループポリシー
  - BFD テンプレート（BFD Template）
  - カテゴリ
  - Cisco Secure Desktop（ルータ）
  - コミュニティリストポリシー
  - 資格情報
  - DHCPv6 プール
  - ファイルオブジェクト
  - FlexConfig
  - アイデンティティ ユーザー グループ
  - IKE プロポーザル
  - Interface Roles
  - IPsec トランスフォームセット
  - LDAP 属性マップ

- ネットワーク/ホスト（IPv4 および IPv6）
- PKI 登録
- ポリシーリストポリシー
- Port Forwarding List
- プレフィックス リスト ポリシー
- ルートリストポリシー
- サービス
- シングルサインオンサーバー
- SLA モニター
- SSL VPN ブックマーク
- SSL VPN カスタマイズ
- SSL VPN ゲートウェイ
- SSL VPN スマートトンネル自動サインオンリスト
- SSL VPN スマートトンネル
- テキスト オブジェクト
- 時間範囲
- トラフィック フロー
- ユーザー グループ
- WINS サーバーリスト

- ポリシー：
  - AAA ルール
  - アクセル ルール
  - IPv6 アクセスルール
  - インスペクション ルール
  - 変換ルール
  - Web フィルタ ルール
  - ゾーンベースのファイアウォールルール
- チケット
  - 設定マネージャ（Configuration Manager）

- Image Manager

グローバル検索の実行

グローバル検索を実行するには、次のいずれかを実行します。

- [編集（Edit）]>[グローバル検索（Global Search）] を選択するか、Ctrl+F を押して [グローバル検索（Global Search）] ウィンドウを開きます。[検索（search）] フィールドの左側にあるドロップダウンリストで検索の範囲を選択し、[検索（search）] フィールドに検索文字列を入力して、[検索（Search）] をクリックします。

（注） 現在 [ルールテーブル（rule table）]を表示している場合、**Ctrl+F** を押すと、[グローバル検索（Global Search）] ウィンドウではなく、[検索と置換（Find and Replace）] ダイアログボックスが開きます。検索と置換機能の代わりに、他の方法のいずれかを使用して、グローバル検索機能にアクセスします。

- [設定マネージャ（Configuration Manager）] ウィンドウの右上隅にある [検索（search）] フィールドを使用し、[検索（Search)] アイコンをクリックして検索の範囲を選択し、 [検索（search）] フィールドに検索文字列を入力して、**Enter** キーを押します。

[グローバル検索（Global Search）] ウィンドウには、検索条件に一致する結果が表示されます。カテゴリセレクタツリーから目的のデータタイプを選択して、そのカテゴリの結果を表示します。

検索結果への対応

検索から返されたアイテムに対して、次のアクションを実行できます。

- **データのエクスポート（すべて）**：選択したカテゴリの検索結果をCSV形式でエクスポートできます。[グローバル検索（Global Search）] ウィンドウのカテゴリセレクタツリーから目的のデータタイプを選択して、そのカテゴリの結果を表示し、検索結果の上にあるツールバーの [エクスポート（Export）] をクリックして、そのデータのテーブルを CSV 形式でエクスポートします。
- **印刷（すべて）**：選択したカテゴリの検索結果を印刷できます。[グローバル検索（Global Search）] ウィンドウのカテゴリセレクタツリーから目的のデータタイプを選択して、そのカテゴリの結果を表示し、検索結果の上にあるツールバーの [印刷（Print）] をクリックして、そのデータのテーブルを印刷します。
- **デバイスプロパティ（デバイス）**：検索結果で返されたデバイスのデバイスプロパティを表示できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のデバイスグループを選択して、そのカテゴリの結果を表示します。[結果（results] テーブルでデバイスを選択して強調表示し、デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。選択したデバイスの [デバイスプロパティ（Device Properties）] ダイアログ ボックスが表示されます。詳細については、デバイスプロパティの表示または変更 （136 ページ）を参照してください。

- **移動（ポリシー）**：検索結果からポリシーに移動できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシータイプを選択して、そのポリシータイプの結果を表示します。[結果（results] テーブルでアイテムを選択して強調表示し、アイテムを右クリックして、[移動（Go To）] を選択します。選択したアイテムに関連するポリシーが表示されます。
- **フィルタ（ポリシー）**：標準のテーブルフィルタを使用して検索結果をフィルタ処理できます。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
- **表示（ポリシーオブジェクト）**：検索結果のオブジェクトのポリシーオブジェクトの詳細を表示できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシーオブジェクトタイプを選択して、そのオブジェクトタイプの結果を表示します。[結果（results）] テーブルでオブジェクトを選択して強調表示し、検索結果の上にあるツールバーで [表示（View）] をクリックします（または、オブジェクトを右クリックして [表示（View）] を選択します)。選択したポリシーオブジェクトに関連する [編集（Edit）] ダイアログボックスが読み取り専用モードで表示されます。
- **編集（ポリシーオブジェクト）**：検索結果からポリシーオブジェクトを編集できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシーオブジェクトタイプを選択して、そのオブジェクトタイプの結果を表示します。[結果（results）] テーブルでオブジェクトを選択して強調表示し、検索結果の上にあるツールバーで [編集（Edit）] をクリックします（または、オブジェクトを右クリックして [編集（Edit）] を選択します)。選択したポリシーオブジェクトに関連する [編集（Edit）] ダイアログボックスが表示されます。

（注） チケットまたはアクティビティが現在開かれていない場合、ポリシーオブジェクトを編集する前に、チケットまたはアクティビティを作成するか、既存のものを開くように求められます。

- **使用状況の検索（ポリシーオブジェクト）**：検索結果で、オブジェクトを使用しているポリシー、オブジェクト、VPN、およびデバイスを見つけることができます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のポリシーオブジェクトタイプを選択して、そのオブジェクトタイプの結果を表示します。[結果（results）] テーブルでオブジェクトを選択して強調表示し、検索結果の上にあるツールバーで [使用状況の検索（Find Usage）] をクリックします（または、オブジェクトを右クリックして [使用状況の検索（Find Usage）] を選択します)。選択したポリシーオブジェクトの [オブジェクトの使用状況（Object Usage）] ダイアログボックスが表示されます。詳細については、オブジェクト使用状況レポートの生成 （306 ページ）を参照してください。
- **チケットの表示（チケット）**：検索結果で返されたチケットの [チケットマネージャ（Ticket Manager）] ウィンドウに移動できます。[グローバル検索（Global Search）] ウィンドウのカテゴリ セレクタ ツリーから目的のチケットグループを選択して、そのカテゴリの結果を表示します。表示するチケットの [結果（results）] テーブルの [チケット（Ticket）] 列をクリックします。選択したチケットが強調表示された状態で、[チケットマネージャ

（Ticket Manager）] ウィンドウが表示されます。詳細については、アクティビティ/チケット マネージャ ウィンドウ （189 ページ）を参照してください。

セレクタの使用

セレクタは、ユーザインターフェイスのさまざまな場所に表示されます。たとえば、デバイス ビューのデバイスセレクタなどがあります（図 1-1 を参照）。これらのツリー構造を使用すると、アクションを実行する（デバイスなどの）項目を選択できます。セレクタには、実行しているタスクに応じていくつかのタイプの項目が表示されます。

セレクタの項目は、フォルダの階層に表示されます。セレクタ内の項目を参照するには、フォルダを展開および縮小します。フォルダには、他のフォルダ、項目、またはフォルダと項目の組み合わせを格納できます。フォルダを展開および縮小するには、フォルダの横にある [+] または [-] をクリックします。

項目を選択するには、その項目をクリックします。（デバイスセレクタなどで）複数の項目に対してアクションを実行できる場合は、Ctrl を押しながら項目をクリックして 1 つ 1 つ項目を選択するか、または Shift を押しながら項目範囲の最初と最後の項目をクリックして、範囲内の項目をすべて選択できます。多くのセレクタでは自動選択をサポートしています。つまり、文字を 1 文字入力すると、その文字で始まる次のフォルダまたは項目がセレクタ内で選択されます。

項目を右クリックすると、その項目で使用できるコマンドが表示されます。右クリック メニューのコマンドには固有のコマンドもあり、その場合は通常のメニューに表示されません。

多くの場合、ダイアログボックスに表示されるデバイス セレクタは、[Available Devices] および [Selected Devices] の 2 つのペインに分割されています。これらのダイアログボックスでは、使用可能デバイスのリストでデバイスを選択し、[>>] をクリックして選択済みリストにデバイスを移動して、デバイスを実際に選択する必要があります。デバイスの選択を解除するには、選択済みデバイス リストでデバイスを選択し、[<<] をクリックします。

セレクタに多数の項目が含まれている場合は、項目をフィルタリングして一部の項目を表示できます。詳細については、セレクタ内の項目のフィルタリング （60 ページ）を参照してください。

セレクタ内の項目のフィルタリング

セレクタに含まれる項目の一部を表示するには、指定した基準に一致する項目だけを表示するフィルタを作成します。セレクタごとに、ユーザ 1 人につき最大 10 個のフィルタを作成できます。そのあとにフィルタをもう 1 個作成すると、最も古いフィルタが新しいフィルタで置き換えられます。作成したフィルタの重複チェックは行われません。フィルタは手動では削除できません。

フィルタ リストは、フィルタリング可能なすべてのセレクタの上部に表示されます。このリストから、次の動作を行うことができます。

- 以前作成したフィルタを選択する。
- [なし（None）] を選択して、フィルタを適用せずにツリーを表示する。

- [フィルタの作成（Create Filter）] を選択してフィルタを作成する。

各フィルタには、複数のフィルタ ルールを含めることができます。各フィルタ ルールには、ルールタイプ、基準、および値を指定します。セレクタに表示されるときに、項目が一部または全部のフィルタ ルールに一致する必要があるかどうかを選択します。

フィルタを作成してフィルタリングできるフィールドは、フィルタに表示される項目のタイプによって異なります。ただし、一般的な手順は、どのセレクタの場合でも同じです。

テーブルのフィルタリングの詳細については、テーブルのフィルタリング （64 ページ）を参照してください。

ヒント セレクタをフィルタリングすると、そのセレクタが含まれる別のウィンドウを開いたとき、セレクタにフィルタが適用されている場合があります。たとえば、デバイス ビューでデバイス セレクタにフィルタを適用すると、New Device ウィザードを開いた場合に、セレクタにフィルタが適用されています。セレクタで項目が見つからない場合は、[Filter] フィールドをオンにして、フィルタが適用されているかどうかを確認してください。

ステップ 1 [セレクタフィルタ（selector filter）] フィールドから [フィルタの作成（Create Filter）] を選択して、[フィルタの作成（Create Filter）] ダイアログボックスを開きます。

ステップ 2 次のオプション ボタンのいずれかを選択して、一致基準を決定します。次の選択項目があります。

- [Match Any of the Following]：フィルタ基準の間に OR 関係を作成します。基準のいずれかに一致するポリシーがフィルタに追加されます。
- [Match All of the Following]：フィルタ基準の間に AND 関係を作成します。すべての基準に一致するポリシーだけがフィルタに追加されます。

ステップ 3 次のように、3 つの基準を入力してフィルタ ルールを設定します。

- 最初のリストから、フィルタリングするタイプを選択します（*Name* など）。
- 次のリストから、フィルタの動作基準を選択します（*contains* など）。
- 最後のフィールドで、フィルタする値を入力または選択します（*Cisco* など）。

ステップ 4 [追加（Add）] をクリックします。

ヒント フィルタルールを作成するときに誤りがあった場合は、ルールを選択して [削除（Remove）] をクリックし、ルールを削除してください。

ステップ 5 必要なフィルタ ルールをさらに追加します。作業が完了したら [OK] をクリックします。

新しいフィルタ基準に従ってセレクタがフィルタリングされ、新しいフィルタがフィルタ リストに追加されます。

[Create Filter] ダイアログボックス

セレクタまたはテーブル内のサブセット項目をフィルタリングおよび表示するには、[Create Filter] ダイアログボックスを使用します。フィルタを作成すると、大きなリストを表示する場合に項目の検索が容易になります。

フィルタリングの詳細については、次の項を参照してください。

- セレクタ内の項目のフィルタリング （60 ページ）
- テーブルのフィルタリング （64 ページ）

ナビゲーション パス

次のいずれかを実行します。

- セレクタツリーの [フィルタ（Filter）] フィールドから [フィルタの作成（Create Filter）] を選択します。
- テーブルの上にある [フィルタ（Filter）] フィールドから [高度なフィルタ（Advanced Filter）] を選択します。

フィールド リファレンス

表 *14 : [Create Filter]* ダイアログボックス

要素	説明
Match All of the Following	このオプションを選択すると、定義したフィルタリング基準間に AND 関係が作成されます。項目がリストに表示されるには、その項目がフィルタのすべてのルールに一致する必要があります。 たとえば、次の基準を定義する場合があります。 • 名前に OSPF が含まれる • 名前に West が含まれる [OK] をクリックすると、フィルタが Name contains OSPF および Name contains West と定義されます。

要素	説明
Match Any of the Following	このオプションを選択すると、定義したフィルタリング基準間に OR 関係が作成されます。項目がリストに表示されるには、その項目がフィルタのルールのいずれか1つに一致する必要があります。 たとえば、次の基準を定義する場合があります。 • 名前に OSPF が含まれる • 名前に RIP が含まれる [OK] をクリックすると、フィルタが Name contains OSPF または Name contains RIP と定義されます。
Filter Type （最初のフィールド）	フィルタリングするプロパティのタイプ。テーブルのカラム見出しに相当します。特定のリストでは、フィルタリングするオプションが1つだけの場合もあります（たとえば、フィルタリングできるのが項目の名前だけの場合など）。
Filter Operator （2 番めのフィールド）	フィルタ タイプとフィルタ値の関係。使用できるオプションは選択したタイプによって異なります。
Filter Value （3 番めのフィールド）	フィルタリングする値。選択したタイプに応じて、このフィールドにはテキスト文字列を入力するか、またはリストから値を選択します。
Filter Content Area [追加（Add）] ボタン [Remove] ボタン	各基準に対して選択したフィルタ タイプ、演算子、および値。 • 基準を追加するには、この領域の上にあるフィールドで基準を作成し、[追加（Add）] をクリックします。 • 基準を削除するには、基準を選択し、[削除（Remove）] をクリックします。

ウィザードの使用

Security Managerを使用して実行できるタスクには、ウィザード形式のタスクもあります。ウィザードは、タスクを実行できる一連のダイアログボックス（または手順）のことです。ウィザードのタイトルバーには、現在の手順の番号およびそのウィザードに含まれる手順の合計数が表示されます。

次のボタンは、各ウィザードに共通です。

- [戻る（Back）]：前のダイアログボックスに戻ります。ウィザードの前の手順で定義した設定を確認および変更できます。

- [次へ（Next）]：次のダイアログボックスに進みます。 このボタンを使用できない場合は、現在のダイアログボックスで、次に進むための必須の設定を定義する必要があります。必須の設定には、アスタリスク（*）のマークが付いています。
- [終了（Finish）]：ウィザードを終了して、定義した設定を保存します。 このボタンが使用可能な場合は、いつでもウィザードを終了できます。このボタンを使用できない場合は、定義する設定が残っています。
- [キャンセル（Cancel）]：設定を保存しないでウィザードを閉じます。
- [ヘルプ（Help）]：ウィザードのオンラインヘルプを開きます。

テーブルの使用

Security Manager の多くのポリシーでは、テーブルを使用します。少数ですが、ルール テーブルと呼ばれる特別なタイプのテーブルを使用するポリシーもあります。標準テーブルと比較すると、ルール テーブルには追加機能が用意されています。詳細については、ルール テーブルの使用 （764 ページ）を参照してください。

標準テーブルの基本機能は、次のとおりです。

- テーブル フィルタ：行をフィルタリングして表示し、大きいテーブルで項目を検索しやすくします。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
- テーブルのカラム見出し：カラムによるソート、カラムの移動、カラムの表示/非表示の切り替えを実行できます。詳細については、テーブル カラムおよびカラム見出しの機能（66 ページ）を参照してください。
- テーブルのボタン：テーブルの下にあるボタンは、次の手順を実行する場合に使用します。
  - [Add Row] ボタン（[+] アイコン）：テーブルに項目を追加するには、このボタンをクリックします。
  - [Edit Row] ボタン（鉛筆アイコン）：プロパティを編集するには、行を選択してこのボタンをクリックします。
  - [Delete Row] ボタン（ゴミ箱アイコン）：テーブルから行を削除するには、行を選択してこのボタンをクリックします。

テーブルのフィルタリング

テーブル内の項目をフィルタリングすると、特定の基準を満たすサブセットを表示できます。テーブルをフィルタリングしてもテーブルの内容は変更されず、現在関心のあるエントリだけに注目できます。この機能は、テーブルに数百ものエントリがある場合に有効です。

テーブルをフィルタリングするには、テーブルの上にある [Filter] フィールドを使用します。これらのコントロールを使用すると、次の作業を実行できます。

- 簡単なフィルタリングを実行するには、フィルタリングする列の名前を選択し、検索する関係（「begins with」など）を選択して、目的のテキスト文字列を入力（場合によっては事前定義されたオプションのいずれかを選択）してから [適用（Apply）] をクリックします。

もう 1 回基準を選択して [Apply] をクリックすると、結果をフィルタリングできます。フィルタがまとめられ、すべての基準を満たす結果が表示されます。たとえば、最初に「Service begins with IP」と入力して [適用（Apply）] をクリックしたあと、「Source contains 10.100.10.10」と入力して [適用（Apply）] をクリックしたとします。結果のテーブルには、サービスが IP かつ送信元に 10.100.10.10 が含まれるすべての行が表示されます（他の IP アドレスが含まれる場合もあります）。

- 高度なフィルタリングを実行するには、左端のメニュー（列の見出しを含むメニュー）から [高度なフィルタ（Advanced Filter）] を選択します。この操作によって [Create Filter] ダイアログボックスが開きます。このダイアログボックスを使用すると、通常のフィルタコントロールを使用する場合と同様に、複数のフィルタ基準を作成できます。ただし、[次のいずれかと一致（Match Any of the Following）] を選択し、分割して論理和を取った基準のリストを作成することもできます。つまり、「サービスの IP または送信元アドレスが 10.100.10.10 であるすべての行を表示する」ことを指定できます。
  - 基準を追加するには、基準を入力して [追加（Add）] をクリックします。
  - 基準を削除するには、不要な基準を選択して [削除（Remove）] をクリックします。

簡単な方式を使用してテーブルをフィルタリングする場合も、[Advanced Filter] を選択すると、必要に応じて既存のフィルタを変更したり、基準を追加または削除できます。ダイアログボックスには、現在テーブルに適用されているフィルタ基準がすべて表示されます。

- 現在のフィルタは、フィルタ制御領域の [Filter] ラベルの横に表示されます。フィルタを削除してすべての行を表示するには、[クリア（Clear）] をクリックします。
- 適用するすべてのフィルタは、[Advanced Filter] エントリの下の左端のメニューに保持されます。フィルタを適用するには、リストからフィルタを選択します。ただし、このリストに登録できるエントリは最大 10 エントリです。11 番めのフィルタを作成すると、最も古いフィルタがリストから削除されます。フィルタを選択して基準を追加する場合は、新しいフィルタの作成ではなくフィルタの変更になります。リストに表示されているフィルタは削除できません。

ヒント 別のデバイスを選択するか、ログアウトしてから再度ログインした場合でも、特定のタイプのテーブルに対して同じフィルタが維持されます。たとえば、あるデバイスの [アクセスルール（Access Rules）] テーブルをフィルタリングすると、他のデバイスも同じ方法でフィルタリングされます。フィルタをクリアすると、すべてのデバイスの同じタイプのテーブルのフィルタもクリアされます。フィルタは他のユーザの表示内容には影響しません。

テーブル カラムおよびカラム見出しの機能

テーブルにはカラムがあり、それぞれのカラムの見出し行にはカラム見出しがあります。これらのカラムおよびその見出しには、次のような機能があります。

- カラムの表示/非表示：テーブルの見出し行を右クリックしてコンテキスト メニューを開き、[Show Columns] を選択します。このメニューを使用すると、表示されるカラムを選択できます。カラムの表示または非表示は、テーブルに定義された項目の内容には影響せず、表示だけに影響します。

デフォルトでは、一部のポリシーのテーブルには、使用可能な一部のカラムだけが表示されます。

- [詳細の表示（Show Details）]/[サマリーの表示（Show Summary）]：テーブルの見出し行を右クリックしてコンテキストメニューを開き、[詳細の表示（Show Details）] または [サマリーの表示（Show Summary）] のいずれかを選択します。この切り替えメニューを使用すると、テーブルに詳細情報を表示するか概要情報を表示するかを選択できます。
- カラムの移動：カラム見出しをクリックしてドラッグし、新しい位置にカラムを移動します。
- カラムのサイズ変更：カラム見出しディバイダをクリックして（カーソルが矢印に変化したら）、ディバイダをドラッグしてカラムのサイズを変更します。
- カラム見出しによるソート：カラム見出しをクリックして、そのカラムの内容でテーブルをソートします。同じカラム見出しを再度クリックすると、ソート順序が逆になります。ソートされたカラムには、見出しの横に矢印が表示されます。

テキスト フィールドの使用方法

テキストフィールドには、そのフィールドの目的に応じて、1行を入力する場合または複数行を入力する場合があります。複数のテキスト行を入力できるテキストフィールドには、フィールドの使い勝手を向上させる機能がいくつか備わっています。ここでは、テキストフィールドの制限および機能に付いて説明します。

- テキストの ASCII 制限について （66 ページ）
- テキスト ボックス内のテキストの検索 （67 ページ）
- テキスト ボックス内のナビゲート （67 ページ）

テキストの ASCII 制限について

通常、デバイスではテキストがASCII文字に制限されています。デバイス設定ファイルで、コマンドの生成に使用されるSecurity Managerのテキスト フィールドにASCII文字以外の文字を入力すると、その文字が原因で設定ファイルがデバイスにロードされなくなる可能性があります。たとえば、FWSMのインターフェイスの説明にASCII文字以外の文字があると、デバイ

スを再起動したときに、そのデバイスのスタートアップ コンフィギュレーションがロードされないことがあります。

デバイス設定に ASCII 文字以外、英語以外の言語を入力できるのは、SSL VPN ブックマークおよび SSL VPN カスタマイゼーションのポリシー オブジェクトだけです。これらのポリシー オブジェクトは、ASA デバイスでブラウザベースのクライアントレス SSL VPN の設定に使用されます。これらのオブジェクトのローカル言語をサポートする方法の詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。

テキスト ボックス内のテキストの検索

複数行テキスト フィールド内のテキストを検索するには、[Find] ダイアログボックスを使用します。

ステップ 1 複数行テキスト フィールドをクリックします。

ステップ 2 Ctrl+F を押します。[Find] ダイアログボックスが開きます。

ステップ 3 検索するテキストを [Find what] フィールドに入力します。

ステップ 4 検索の方向を指定するには、[方向（Direction）] フィールドで [上（Up）] または [下（Down）] のいずれかを選択します。

ステップ 5 入力したテキストの大文字と小文字を区別するには、[大文字と小文字を区別（Match Case）] チェックボックスをオンにします。

ステップ 6 [検索（Find）] をクリックします。次に出現する検索テキストが、テキスト フィールド内で強調表示されます。

テキスト ボックス内のナビゲート

複数行テキスト フィールドで特定の行にナビゲートするには、[Goto line] ダイアログボックスを使用します。

ステップ 1 複数行テキスト フィールドをクリックします。

ステップ 2 Ctrl+G を押します。[Goto line] ダイアログボックスが開きます。

ステップ 3 [Line number] フィールドに行番号を入力します。

ステップ 4 [OK] をクリック入力した行番号までテキスト フィールドがスクロールします。

Cisco Security Manager でのファイルまたはディレクトリの選択または指定

Cisco Security Manager は標準的なファイル システム ブラウザを使用しており、ディレクトリまたはファイルを選択したり、ファイルを指定できます。

次のファイル操作を実行するときに、クライアント ファイル システムとサーバーファイルシステムを選択できます。

- Security Manager のライセンス ファイルのインストール
- デバイス インベントリ ファイルのインポート/エクスポート
- 共有ポリシーのインポート/エクスポート
- 次のファイル オブジェクトの作成
  - Cisco Secure Desktop Package
  - Plug-In：ブラウザ プラグイン ファイル用。
  - AnyConnect Profile
  - AnyConnect Image
  - Hostscan Image

他のすべてのファイル操作については、Security Manager サーバーでのみファイルを作成または選択できます。サーバーにマウントされたドライブは使用できず、クライアントシステムも使用できません。

ヒント　Security Manager クライアントでファイル操作を許可するかどうかは、[ツール（Tools）] > [Security Manager 管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。

通常、ファイルを作成または選択するには、[参照（Browse）] ボタンをクリックして、実行するアクションに関連するタイトルのダイアログボックスを開きます（たとえば、設定ファイルの選択時は [ファイルの選択（Choose Files）]）。[Browse] ボタンは、製品全体でさまざまなダイアログボックスに表示されます。

目的のフォルダにナビゲートするには、このダイアログボックスの左側にあるフォルダ ツリーを使用します。

- クライアント側のファイルのブラウズがイネーブルのとき、クライアント側のブラウズをサポートしている機能（上記を参照）を実行する場合は、インポートまたはエクスポートするシステムに対応したタブを選択します。
- ファイルを選択する場合は、フォルダ ツリーでファイルを検索し、右側のペインで選択します。複数のファイルを選択できるアクションを実行している場合は、Ctrl を押しながらクリックしてファイルを個別に選択するか、または Shift を押しながらクリックしてファイルの範囲を選択します。ファイル タイプを選択して、アクションに適用されるファイルだけを表示することが必要な場合もあります。
- ファイルを指定（作成）する場合は、ファイルを作成するフォルダにナビゲートし、ファイル名を入力して、適切なファイル タイプを選択します。

（注） パスとファイル名は、英語のアルファベット文字に制限されます。日本語文字はサポートされません。Windows 日本語 OS システムでファイルを選択する場合は、通常のファイル区切り文字 \ がサポートされますが、これは円記号（U+00A5）として表示されることがあることに注意する必要があります。

ユーザインターフェイスに問題がある場合のトラブルシューティング

次のヒントを参照すると、ユーザインターフェイスに関する一般的な問題が発生した場合に、その問題の解決に役立つ場合があります。

- **インターフェイスがフリーズしたように見える**：Security Manager のダイアログボックスから他のアプリケーション（電子メールのチェックなど）に移動して Security Manager に戻ったときに、クリックしてもまったく応答がない場合があります。インターフェイスがフリーズしているように見えます。

これは、開いたダイアログボックスの上に別の Security Manager ウィンドウが重なっていることが原因の場合があります。このダイアログボックスを閉じるまで、アプリケーションの他のウィンドウは使用できません。隠れているダイアログボックスを見つけるには、Alt を押しながら Tab を押します。この操作によって、現在開いているすべてのウィンドウのアイコンが表示された Windows のパネルが開きます。Alt を押したまま Tab を何回か押し、適切なアイコンが見つかるまでアイコンを順に選択します（アイコンは Security Manager のアイコンではなく、一般的な Java のアイコンになっている場合があります）。Tab キーを使用してアイコンを順に選択するのではなく、マウスを使用して目的のアイコンをクリックすることもできます。

- **ボタンをクリックすると、テキストおよびリストの要素が見つからないという Java のエラーが発生する**：Security Manager クライアントの実行中に Windows のカラースキームを変更した場合は、クライアントを閉じて再起動する必要があります。再起動しないと、クライアントの動作を予測できなくなります。

カラースキームを変更していないのに、これらの問題が発生する場合も、アプリケーションを閉じて再起動する操作を試してください。

- **画面に対してダイアログボックスが大きすぎる**：実際には、多くのラップトップで対応している最適な画面解像度より、Security Manager クライアントの最小画面解像度の方が大きくなります（画面解像度の要件については、『Installation Guide for Cisco Security Manager』でクライアントのシステム要件を参照してください）。非常に大きなダイアログボックスもあるため、クライアントをラップトップで実行している場合は、ダイアログボックスが大きすぎて画面に収まりきらないことがあります。

通常は、ダイアログボックスの位置を変更すれば、[OK]、[Cancel]、および [Help] の各ボタンにアクセスできます。ただし、これらのボタンも画面に表示されない場合は、次の方法で同じアクションを実行できます。

- [OK]：フィールド内のカーソルをダイアログボックスの下部付近に置き、Tab を押してフィールド間を移動します。通常は、画面外の最初のフィールドが [OK] ボタンです。カーソルの強調表示が画面外に移動したら、Enter を押します。

復帰を使用できないフィールド（一般的には [Name] フィールドなど）にカーソルを置き、Enter を押すこともできます。多くの場合、これは [OK] のクリックに相当します。

- [キャンセル（Cancel）]：ウィンドウのタイトルバーの右側にある [X] をクリックします。
- [ヘルプ（Help）]：F1 を押します。

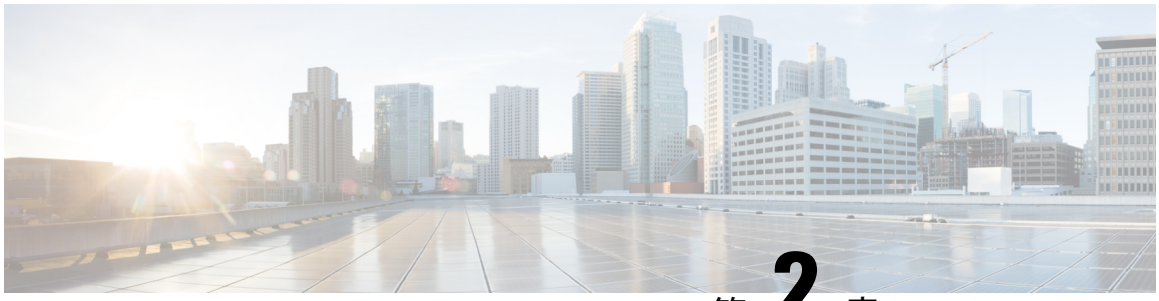
オンライン ヘルプの利用方法

Security Manager のオンライン ヘルプにアクセスするには、次のいずれかを実行します。

- Security Manager オンラインヘルプのメインページを開くには、[ヘルプ（Help）] > [ヘルプトピック（Help Topics）] の順に選択します。
- アクティブなページの状況依存オンラインヘルプを開くには、[ヘルプ（Help）] > [このページについてのヘルプ（Help About This Page）] の順に選択するか、またはツールバーで [?] をクリックします。
- ダイアログボックスの状況依存オンラインヘルプを開くには、ダイアログボックスの [ヘルプ（Help）] をクリックします。

ヒント オンライン ヘルプがブロックされずに開くようにするには、コンピュータでアクティブコンテンツの実行を許可するように Internet Explorer を設定する必要があります。Internet Explorer で、[ツール（Tools）] > [インターネット オプション（Internet Options）] を選択し、[詳細設定（Advanced）] タブを選択します。[セキュリティ（Security）] セクションまでスクロールして、[マイコンピュータのファイルでのアクティブコンテンツの実行を許可する（Allow active content to run in files on My Computer）] を選択します。[OK] をクリックして変更を保存します。Internet Explorer および Firefox の各ブラウザでの設定要件の一覧については、『Installation Guide for Cisco Security Manager』を参照してください。

オンラインヘルプページは、ユーザー認証なしで表示されます。ヘルプページは直接 URL アクセスで開きますが、それらは静的コンテンツページに過ぎず、Cisco Security Manager 内で機能します。



第 2 章

デバイスを管理するための準備

Security Manager を使用してデバイスの管理を開始する前に、最低限の設定を行ってデバイスを準備する必要があります。次の各項では、さまざまなトランスポートプロトコルまたはデバイスタイプに必要な基本的なデバイス構成について説明します。

- デバイスの通信要件について （71 ページ）
- SSL（HTTPS）の設定 （73 ページ）
- SSH の設定 （77 ページ）
- AUS または Configuration Engine の設定 （81 ページ）
- Cisco ASA デバイスでのライセンスの設定 （83 ページ）
- Cisco IOS デバイスでのライセンスの設定 （84 ページ）
- IPS デバイスの初期化 （85 ページ）

デバイスの通信要件について

Security Manager には、デバイスを管理するための多くの方法が用意されています。最も簡単なのは、Security Manager からデバイスに直接接続する方法です。Security Manager がデバイスにアクセスするのは、インベントリまたはポリシーのディスカバリ中、設定の展開中、または Security Manager でデバイス接続を要求するアクション（接続のテストなど）が行われた場合などです。

オフラインの方法を使用して、Security Manager インベントリにデバイスを追加したり、デバイスに設定変更を展開したりできるため、Security Manager で使用するためにデバイス通信設定を行うかどうかは任意に選択できます。ただし、通常は、オフラインまたはカスタマイズした設定展開ツールを実装するために、デバイスで基本的なデバイス通信設定を行う必要があります。

Security Manager では、特定のタイプのデバイスがデフォルトで使用するトランスポート プロトコルを設定する一方で、別のプロトコルに応答するように設定されたデバイスではそのデフォルトのプロトコルを変更できます。Security Manager は、そのタイプのデバイスで最もよく使用されるプロトコルがデフォルトのプロトコルとして設定されます。あるタイプのデバイスに対するデフォルトのデバイス通信設定を変更するには、[ツール（Tools）]>[Security Manager 管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します（詳細については、[Device Communication] ページ

（668 ページ）を参照してください）。特定のデバイスに対するトランスポート設定を変更するには、デバイス プロパティの表示または変更 （136 ページ）の説明に従って、そのデバイス プロパティを変更します。

Security Manager では、次のトランスポート プロトコルを使用できます。

- SSL（HTTPS）：Secure Socket Layer は HTTPS 接続であり、PIX ファイアウォール、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）、および Firewall Services Module（FWSM; ファイアウォール サービス モジュール）で使用される唯一のトランスポート プロトコルです。また、SSL は、Cisco IOS ソフトウェアリリース 12.3 以降を実行しているルータおよび IPS デバイスのデフォルトプロトコルです。

Cisco IOS ルータでトランスポート プロトコルとして SSL を使用する場合、ルータで SSH も設定する必要があります。Security Manager は、SSH 接続を使用して、SSL 展開中にインタラクティブ コマンド展開を処理します。

Cisco Security Manager は、Transport Layer Security（TLS）およびセキュアソケットレイヤ（SSL）プロトコルに OpenSSL を使用していました。バージョン 4.13 以降、Cisco Security Manager は OpenSSL バージョン 1.0.2 を Cisco SSL バージョン 6.x に置き換えました。Cisco SSL は、完全な FIPS 検証による FIPS 準拠を可能にし、高速で費用対効果の高い接続を実現します。Cisco SSL のコモンクライテリアモードにより、コンプライアンスが容易になります。OpenSSL と比較して、Cisco SSL は機能が進んでいます。Cisco SSL の製品セキュリティベースライン（PSB）要件により、ログイン情報とキーの管理、暗号化標準規格、スプーフィング対策機能、整合性と改ざん防止といったセキュリティの重要な側面が保証され、セッション、データ、ストリームの管理と運用が保護対象となります。

SSL の設定方法の詳細については、SSL（HTTPS）の設定 （73 ページ）を参照してください。

- SSH：セキュア シェルは、Catalyst スイッチおよび Catalyst 6500/7600 デバイスのデフォルトのトランスポート プロトコルです。また、Cisco IOS ルータでも SSH を使用できます。

SSH の設定方法の詳細については、SSH の設定 （77 ページ）を参照してください。

- Telnet：Telnet は、Cisco IOS ソフトウェア Release 12.1 および 12.2 を実行しているルータのデフォルト プロトコルです。また、Catalyst スイッチ、Catalyst 6500/7600 デバイス、および、Cisco IOS ソフトウェア Release 12.3 以降を実行しているルータでも Telnet を使用できます。Telnet の設定方法の詳細については、Cisco IOS ソフトウェアのマニュアルを参照してください。
- HTTP：IPS デバイスでは、HTTPS（SSL）の代わりに HTTP を使用できます。いずれのデバイス タイプでも、HTTP はデフォルト プロトコルではありません。
- SQL Anywhere：バージョン 4.20 まで、Security Manager は SQL Anywhere バージョン 12.x をデータベースとして使用していました。バージョン 4.21 以降、Security Manager は Sybase SQL Anywhere バージョン 17.0.10.5855 を使用しています。
- TMS：Token Management Server は、Security Manager でトランスポート プロトコルと同様に処理されますが、実際のトランスポート プロトコルではありません。TMS をルータのトランスポート プロトコルとして設定することにより、設定を TMS に展開するように

Security Manager に指示します。TMS から設定を eToken にダウンロードし、その eToken をルータの USB バスにプラグインして、設定を更新できます。TMS は、Cisco IOS ソフトウェア 12.3 以降を実行している特定のルータでのみ使用可能です。

設定を TMS に展開してルータにダウンロードする方法の詳細については、Token Management Server への設定の展開 （534 ページ）を参照してください。

また、Security Manager は、間接的な方法を使用して設定をデバイスに展開し、展開を管理するサーバ上の設定をデバイスにステージングすることもできます。さらに、これらの間接的な方法を使用すると、デバイスでダイナミック IP アドレスを使用することもできます。これらの方法はトランスポート プロトコルとしてではなく、デバイスの補助トランスポート プロトコルとして扱われます。次の間接的な方法を使用できます。

- AUS（Auto Update Server）：デバイスを Security Manager に追加するときに、Security Manager を管理している AUS サーバを選択できます。AUS は、PIX ファイアウォールおよび ASA デバイスで使用できます。

AUS サーバを使用するようにデバイスを設定する方法の詳細については、AUS または Configuration Engine の設定 （81 ページ）を参照してください。

- Configuration Engine：ルータを Security Manager に追加するときに、Security Manager を管理している Configuration Engine を選択できます。

Configuration Engine サーバを使用するようにデバイスを設定する方法の詳細については、AUS または Configuration Engine の設定 （81 ページ）を参照してください。

AUS サーバまたは Configuration Engine サーバを使用するデバイスを Security Manager に追加する方法の詳細については、次の項を参照してください。

- デバイス インベントリへのデバイスの追加 （94 ページ）
- Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）

SSL（HTTPS）の設定

多くのデバイスでは、デバイスとの通信に Secure Socket Layer（SSL）プロトコルを使用できます。これは HTTPS とも呼ばれます。このプロトコルを使用して設定を展開すると、Security Manager では設定ファイルが暗号化されてからデバイスに送信されます。

ここでは、デバイスで SSL を設定する方法について説明します。

- PIX ファイアウォール、ASA、および FWSM デバイスでの SSL（HTTPS）の設定 （74 ページ）
- Cisco IOS ルータでの SSL の設定 （75 ページ）

PIXファイアウォール、ASA、およびFWSMデバイスでのSSL（HTTPS）の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、PIX ファイアウォール、ASA、および FWSM デバイスでデバイス管理用のトランスポート プロトコルとして SSL を使用する前に実行する必要のあるタスクについて説明します。

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
hostname# config terminal
```

プロンプトに応答します。次にいくつかのヒントを示します。

- インタラクティブプロンプトを使用して事前設定するかを確認するプロンプトが表示されたら、**y** を入力します。
- 現在のイネーブル パスワードを入力します。
- タイム ゾーン、年、月、日、および時間を指定します。
- デバイスが次の場合は、それぞれ次の操作を実行します。
  - 新規のデバイス：ネットワーク インターフェイス IP アドレスと、デバイスの内部 IP アドレスに適用するネットワーク マスクを指定します。
  - 既存のデバイス：インターフェイス IP アドレスおよびマスクが正しいことを確認します。
- デバイスが次の場合は、それぞれ次の操作を実行します。
  - 新規のデバイス：ホスト名およびドメイン名を指定します。
  - 既存のデバイス：ホスト名およびドメイン名が正しいことを確認します。
- PIX Device Manager を実行するホストの IP アドレスの入力を要求された場合、Security Manager サーバの IP アドレスを指定します。
- 前述の変更をフラッシュに書き込むかどうかを確認するプロンプトが表示されたら、**yes** を入力します。

ステップ 2 ASA を設定している場合、ASA がサーバーとして機能するときに使用する SSL/TLS プロトコルのバージョンを指定します。バージョン 4.8 以降、Cisco Security Manager はすべての SSL/TLS プロトコルバージョンをサポートしています。最新の認定バージョンは TLS 1.2 です。

例：

```
hostname(config)# ssl server-version any
```

ステップ 3 HTTP サーバーをイネーブルにします。

例：

```
hostname(config)# http server enable
```

ステップ 4 デバイスとの HTTP 接続を開始することを認可されたホストまたはネットワークを指定します。

例：

```
hostname(config)# http
 ip_address
 [netmask
] [if_name
```

ステップ 5 現在の設定がフラッシュ メモリに保存されます。

例：

```
hostname(config)# write memory
```

ここで、

- ip_address：Cisco Security Manager サーバーの IP アドレス。
- netmask：IP アドレスのネットワークマスク。
- if_name：デバイスのインターフェイス名（デフォルトは **inside**）。このインターフェイスから Cisco Security Manager が HTTP 接続を開始します。

Cisco IOS ルータでの SSL の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、IOS デバイス、および IPS をサポートしますが、拡張機能はサポートしません。

ここでは、Cisco IOS ルータでデバイス管理用のトランスポート プロトコルとして SSL を使用する前に実行する必要のあるタスクについて説明します。

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
hostname# config terminal
```

ステップ 2 デバイスが新規の場合は、ホスト名とドメイン名を設定します。

例：

```
router(config)# hostname
 name

hostname(config)# ip domain-name
 your_domain
```

ステップ 3 レベル 15 の権限を設定します。SSL では、Cisco IOS ルータにログインするためにレベル 15 の権限が必要です。

例：

```
hostname(config)# username
 username
 privilege 15 password 0
 password
```

ステップ 4 ローカル認可または AAA 認可のどちらかをイネーブルにします。

- ローカル認可：認可に AAA を使用しているが、ローカル認可を使用する場合は、次のコマンドを使用して、ログイン時の AAA 認可および AAA 認証をディセーブルにします。list-name は、認可方式のリストに名前を付け、設定したユーザー名を使用してローカル認可をイネーブルにするために使用する文字列です。

例：

```
hostname(config)# no aaa authorization network
 list-name

hostname(config)# no aaa authentication login
 list-name
hostname(config)#ip http authentication local
```

ip http authentication local コマンドを入力しない場合、デフォルトのイネーブルパスワードが認証に使用されます。

- AAA 認可：次のコマンドを使用して、AAA 認証および認可をイネーブルにします。最後の 2 つのコマンドが必要になるのは、複数の AAA リストが定義されている場合だけです。list-name は、認可方式のリストに名前を付けるために使用される文字列です。これらのコマンドによって、HTTPS プロトコルを使用してデバイスに接続しようとするユーザが認証されます。

例：

```
hostname(config)#ip http authentication aaa

hostname(config)#ip http authentication aaa login-authentication
 list-name
hostname(config)# ip http authentication aaa exec-authorization
 list-name
```

ステップ 5 HTTPS サーバーをイネーブルにします。

例：

```
hostname(config)# ip http secure-server
```

ステップ 6 コンフィギュレーション モードを終了し、EXEC モードに戻ります。

例：

```
hostname(config)# exit
```

ステップ 7 デバイスで SSL が設定されていることを確認します。デバイスは「イネーブル」ステータスで応答する必要があります。

例：

```
hostname# show ip http server secure status
```

SSH の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、拡張機能はサポートしていません。

Secure Shell（SSH; セキュア シェル）プロトコルを使用して、Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスと通信できます。このプロトコルにより、セキュアでないチャネルでも強固な認証と安全な通信を確保できます。Security Manager は、SSH バージョン 1.5 と 2 の両方をサポートしています。デバイスに接続されると、Security Manager はどのバージョンを使用するかを決定し、そのバージョンを使用して通信を行います。

ここでは、サポートされているデバイスで SSH を設定する方法について説明します。

- SSH の重要な行末端ルール （77 ページ）
- 認証のテスト （78 ページ）
- Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定（79 ページ）
- 非 SSH 接続の禁止（任意） （80 ページ）

SSH の重要な行末端ルール

システム障害を防止するため、SSH では次の行末端ルールに従う必要があります。

- バナーメッセージの行を「#」、「#」、「>」、または「>」で終了しないでください。システムで、バナーメッセージの最後に「#」記号または「>」記号が必要となる場合は、必ずその後に 2 つのスペースを入れてください。

- 「Username:」または「Password:」だけを含むバナーメッセージ行を使用しないでください。
- 「>」または「#」で終わるようにデバイスユーザEXECモードプロンプトをカスタマイズしないてください。

認証のテスト

SSHを設定する前に、SSHなしで認証をテストして、デバイスを認証できることを確認する必要があります。ローカルのユーザ名とパスワードを使用して認証することも、TACACS+ またはRADIUS を実行している認証、許可、アカウンティング（AAA）サーバを使用して認証することもできます。

ここでは、ローカルまたはAAA サーバのユーザ名とパスワードを使用して、SSH なしで認証をテストする方法について説明します。

ステップ1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ2 AAA ステートメントがない場合はローカルのユーザ名とパスワードを使用するように指定します。Cisco IOS ルータで、VTY 行で **aaa new-model** コマンドの代わりに **login local** コマンドを使用できます。

例：

```
hostname(config)#aaa new-model
```

ステップ3 （任意）デバイスのローカル データベース内にユーザ アカウントを設定します。

例：

```
hostname(config)# username
 name
 password 0
 password
```

ステップ4 コンフィギュレーション モードを終了し、EXEC モードに戻ります。

例：

```
hostname(config)# exit
```

ステップ5 設定の変更を保存します。

例：

```
hostname(config)# write memory
```

Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSMおよび IPS をサポートしますが、拡張機能はサポートしません。

ここでは、Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定に必要なタスクについて説明します。

ヒント Security Manager は SSH 接続を使用して SSL 展開中にインタラクティブ コマンド展開を処理するため、Cisco IOS ルータで SSH を設定する必要があります。

関連項目

- SSH の重要な行末端ルール （77 ページ）
- 認証のテスト （78 ページ）
- 非 SSH 接続の禁止（任意） （80 ページ）

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ 2 デバイスが新規の場合は、ホスト名とドメイン名を設定します。

例：

```
router(config)# hostname
 name

hostname(config)# ip domain-name
 your_domain
```

ステップ 3 SSH セッションの RSA キーペアを生成します。デバイスにより係数のサイズの入力を要求されたら、1024 を入力することを推奨します。

例：

```
hostname(config)# crypto key generate rsa
```

ステップ 4 （任意）タイムアウト間隔（分）と再試行回数を設定します。

例：

```
hostname(config)# ip ssh timeout
 time
hostname(config)# ip ssh authentication-retries
 n
```

ステップ 5 コンフィギュレーション モードを終了し、EXEC モードに戻ります。

例：

```
hostname(config)# exit
```

ステップ 6 設定の変更を保存します。

例：

```
hostname# write memory
```

非 SSH 接続の禁止（任意）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、IOS デバイス、および IPS をサポートしますが、拡張機能はサポートしません。

SSH の設定後は、SSH 接続だけを使用するように Cisco IOS ルータ、Catalyst スイッチ、およびCatalyst 6500/7600 デバイスを設定できます。

関連項目

- SSH の重要な行末端ルール （77 ページ）
- 認証のテスト （78 ページ）
- Cisco IOS ルータ、Catalyst スイッチ、および Catalyst 6500/7600 デバイスでの SSH の設定（79 ページ）

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ 2 Telnet アクセス用のルータを設定します。使用できる最初と最後の行番号を指定します（数字の範囲は 0 ～ 1180 で、最後の番号の方が最初の番号よりも大きくなっている必要があります）。

例：

```
hostname(config)# line vty
 first_line last_line
```

ステップ 3 非 SSH 接続（Telnet など）を禁止します。

例：

```
hostname(config-line)# transport input ssh
```

ステップ 4 コンフィギュレーション モードを終了します。

例：

```
hostname(config-line)# end
```

ステップ 5 設定の変更を保存します。

例：

```
hostname# write memory
```

AUS または Configuration Engine の設定

多くのデバイスでは、中間トランスポート サーバを使用して、設定の更新をデバイスにステージングできます。また、このトランスポート サーバを使用すると、静的IPアドレスではなく、（DHCP サーバを使用して）動的に割り当てられた IP アドレスを使用するデバイスを管理することもできます。トランスポート サーバを使用して設定を展開すると、Security Manager が設定をサーバに展開し、デバイスがサーバから設定を取得します。AUSプロトコルを実行する Auto Update Server を使用することも、CNS プロトコルを実行する Cisco Configuration Engine を使用することもできます。

ここでは、デバイスで AUS または CNS を設定する方法について説明します。

• PIX ファイアウォールおよび ASA デバイスでの AUS の設定 （81 ページ）

PIX ファイアウォールおよび ASA デバイスでの AUS の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

設定およびイメージの更新のために AUS プロトコルを使用して Auto Update Server または CNS Configuration Engine に接続するように、PIX ファイアウォールおよび ASA デバイスを設定できます。Configuration Engine を使用する場合、デバイスは Auto Update Server と同じ AUS プロトコルを使用するため、設定は同じです。AUS/CE 展開の処理に関するエンドツーエンドの説明については、Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）を参照してください。

設定の更新のために AUS/CE サーバに接続する必要があることをデバイスが認識できるように、最初に AUS 設定を行う必要があります。最初の展開後は、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] ポリシーを使用して、これらの設定を変更できます。

ここでは、PIX ファイアウォールおよび ASA デバイスでデバイス管理用のトランスポート プロトコルとして AUS または CNS を使用する前に実行する必要のあるタスクについて説明します。

ステップ 1 コンフィギュレーション モードを入力します。

例：

```
router# config terminal
```

ステップ 2 AUS に接続します。Security Manager にログインできるユーザ名とパスワードを指定します。通常、ポート番号は 443 です。

例：

```
hostname(config)# auto-update server https://
username:password@AUSserver_IP_address:port
 /autoupdate/AutoUpdateServlet
```

ステップ 3 AUS のポーリング期間を指定します。

例：

```
hostname(config)# auto-update poll-period
 poll_period
 [retry_count
 ] [retry_period
 ]
```

ここで、

- *poll_period*：2 つの更新の間のポーリング間隔。デフォルトは 720 分（12 時間）です。
- *retry_count*：（任意）サーバー接続試行が失敗した場合に再試行する回数。デフォルトは 0 です。

ステップ 4 指定した固有のデバイス ID を使用して自身を識別するようにデバイスを設定します。

例：

```
hostname(config)# auto-update device-id
 [ hardware-serial | hostname |
ipaddress
 [if_name
 ] |  mac-address
 [if_name
 ] | string
 text
 ]
```

ここで、

- *if_name*：デバイスインターフェイス名（デフォルトは **inside**）。
- *text*：固有の文字列名。

ステップ 5 設定の変更を保存します。

例：

```
hostname# write memory
```

Cisco ASA デバイスでのライセンスの設定

Cisco ASA ソフトウェアを実行するデバイスには、機能のライセンスごとに製品アクティベーション キーが必要です。ボットネット トラフィック フィルタなど、一部のライセンスはオプションであり、使用期間があります。あるモデルでは標準でも、他のモデルではオプションになる機能もあります。たとえば、フェールオーバーのライセンスは、5505 モデルおよび 5510 モデルではオプションになりますが、その他すべてのモデルでは標準です。

Security Manager を使用して ASA ライセンスをインストールおよびアクティブ化できません。代わりに、Adaptive Security Device Manager（ASDM）を使用します。[設定（Configuration）] > [デバイス管理（Device Management）] > [ライセンス（Licensing）] > [アクティベーション キー（Activation Key）] を選択してアクティベーションキーを入力し、このページのオンライン ヘルプの説明に従います。[Activation Key] ページには、すべての機能のライセンスのステータスも表示されます。ASDM オンライン ヘルプには、ASA ライセンスに関する広範な情報が含まれます。

Security Manager から設定を展開する場合、デバイスには、設定に含まれるすべての機能に対してアクティブなライセンスが必要です。そうでない場合は、展開エラーが表示されます。ほとんどの場合、デバイス上にあるアクティブなライセンスに基づいた、ユーザによる機能の設定を Security Manager が妨げることはありません。たとえば、デバイスのボットネット ライセンスがディセーブルである場合でも、そのデバイスのボットネット トラフィック フィルタリングを設定することはできます。

例外は、5505 モデルおよび 5510 モデル上のフェールオーバー ライセンスです。デバイス上にアクティブなフェールオーバー ライセンスがあるかどうかを示すように設定が可能なデバイス プロパティがあります。ライセンスはフェールオーバーをサポートします。（デバイス ビューで）デバイスをダブルクリックして [Device Properties] ページを開き、このプロパティを設定できます。このオプションは [General] タブ（[デバイスのプロパティ（Device Properties）]：[全般（General）]ページ （137 ページ）を参照）にあります。デバイス上のポリシーを検出する場合、たとえば、[Add Device From Network] オプションまたは [Add Device from File]（設定ファイルではなくインベントリ ファイルから）オプションを使用してデバイスをインベントリに追加するときなど、Security Manager は、フェールオーバー ライセンスのステータスを判断し、プロパティを適切に設定します。プロパティが正しく維持されていることを確認する必要があります。プロパティが選択されても、デバイスに非アクティブのフェールオーバー ライセンスがある場合は、展開に失敗します。

ヒント [New Device] オプションまたは [Configuration File] オプションを使用してデバイスを追加する場合は、License Supports Failover プロパティは、デバイス プロパティに設定されるのを待つ代わりに、デバイスの追加時に設定できます。

Cisco IOS デバイスでのライセンスの設定

Cisco IOS ソフトウェアを実行するデバイスには、さまざまな機能（セキュリティ機能など）のライセンス ファイルが必要です。これらのライセンス（securityk9 パッケージなど）がデバイスにインストールされていない場合、Security Manager は、特定のライセンス レベルを必要とするコマンドを設定できません。この場合、ライセンスされていないデバイスにポリシーを展開しようとすると、展開が失敗します。

Security Manager を使用して、IPS ライセンスを展開および管理できますが、それ以外のタイプのライセンスは展開および管理できません。コマンドライン インターフェイスを使用して、デバイスで直接これらのライセンスを設定するか、Cisco License Manager を使用します。次に、ライセンスを設定するための一般的なプロセスを示します。ライセンスの設定方法の詳細については、Cisco.com の『Cisco IOS Software Activation Command Guide』および『Cisco IOS Software Activation Command Reference』を参照してください。

1. 使用する機能に必要なライセンスを取得します。または、一部のデバイスに付属の評価版ライセンスを使用できます。**show license all** コマンドを使用すると、使用可能なライセンスが表示されます。
2. 購入したライセンスをデバイス上のフラッシュ ストレージにコピーするか、TFTP サーバに配置します。たとえば、ライセンスを TFTP サーバーに配置し、**copy tftp flash0:** コマンドを使用してファイルを flash0 ストレージエリアにコピーします。
3. **license install** コマンドを使用して、購入した各ライセンスをインストールします。次に例を示します。

license install flash0:uc-base-CISCO2951-FHH1216P06Z.xml

一部のライセンスでは、ライセンス契約書を読んで合意するように要求されます。

評価ライセンスを使用する場合は、**license boot** コマンドを使用してライセンスを有効にしてから、デバイスをリロードします。エンドユーザ ライセンス契約書に合意しないと、Security Manager はデバイスに設定を展開できません。

- **show version**、**show license feature**、および **show license all** コマンドを使用して、インストールされたライセンスを確認できます。

IPS デバイスの初期化

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

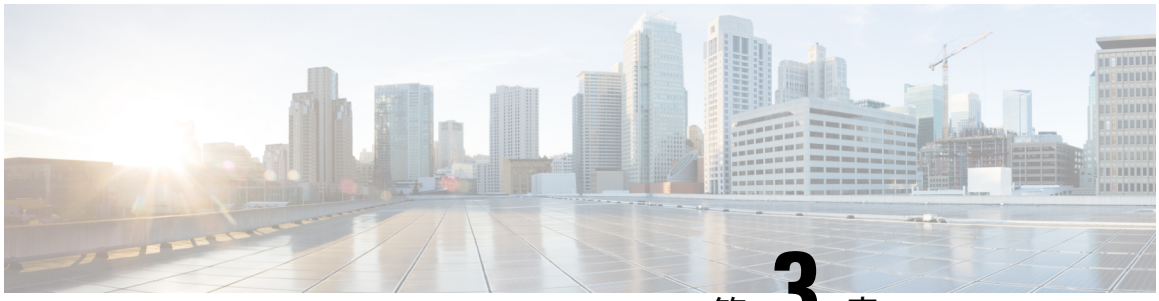
IPS デバイスを初期化するには、次の設定を行う必要があります。次の設定はネットワーク設定であり、IPS デバイスの管理者権限を持つユーザだけが設定できます。

- センサー名
- IP アドレス
- ネットマスク
- デフォルト ルート（Default route）
- TLS/SSL の有効化（デバイスで Web サーバの TLS/SSL をイネーブルにするため）
- Web サーバのポート
- デフォルト ポートの使用

これらの設定は、IPS デバイスで使用されているプラットフォームに応じて、Intrusion Prevention System Device Manager（IDM）またはコマンドラインセッションで **setup** コマンドを使用して設定します。サポートされている IPS プラットフォームのリストについては、次の URL で、サポートされているデバイスおよびソフトウェアバージョンの情報を参照してください：
http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html

これらの設定の詳細については、IPS デバイスの技術マニュアルを参照してください。

（注） IOS IPS デバイスの使用準備に関する詳細については、Cisco IOS IPS ルータでの最初の準備 （2320 ページ）を参照してください。



第 3 章

デバイス インベントリの管理

次の項では、デバイス インベントリを管理する方法について説明します。

- デバイス インベントリについて （87 ページ）
- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイス インベントリの使用 （129 ページ）
- デバイス グループの使用 （164 ページ）
- [デバイスステータスビュー（Device Status View）] の使用 （170 ページ）

デバイス インベントリについて

Security Manager は、管理対象のデバイスのインベントリを保持します。インベントリにはデバイスを特定してログインするために必要な情報が格納されており、ログインしたデバイスにポリシーを展開できます。次の項では、デバイスインベントリに関連する一般概念について説明します。

- デバイス ビューについて （87 ページ）
- デバイス名およびデバイスと見なされる要素について （90 ページ）
- デバイス クレデンシャルについて （91 ページ）
- デバイス プロパティについて （93 ページ）

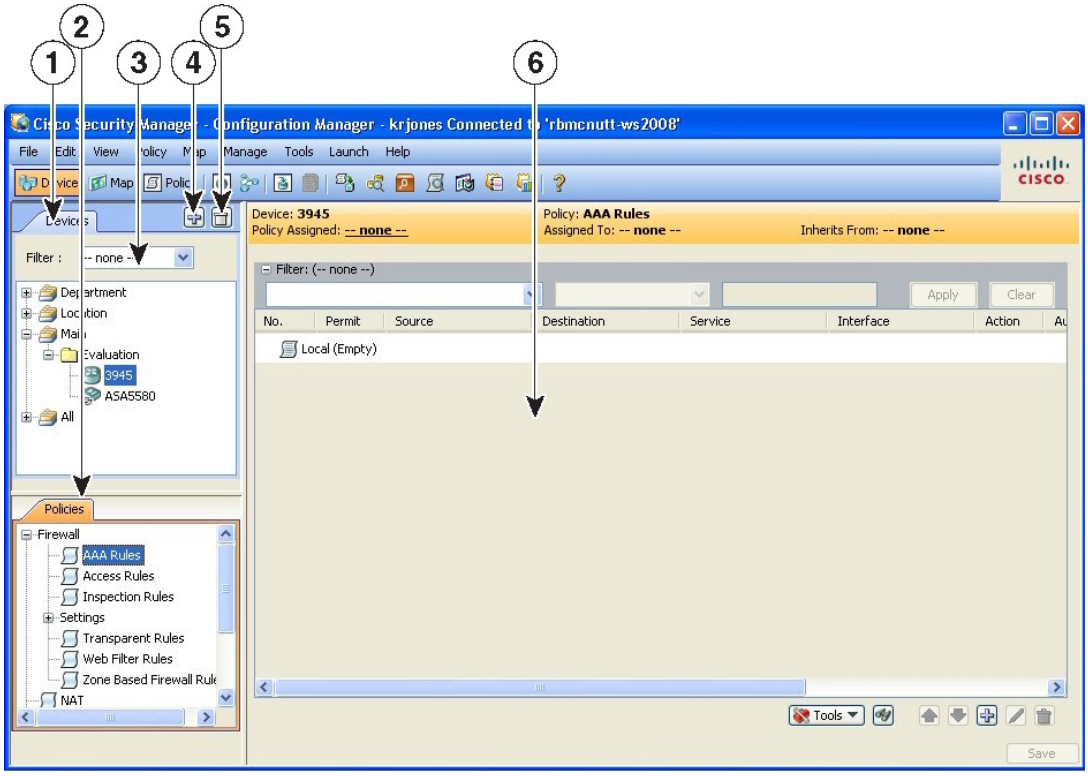
デバイス ビューについて

[Device View] ボタンを押すと、[Devices] ページが開きます。ここでは、Security Manager インベントリに対するデバイスの追加と削除、デバイスのポリシー、プロパティ、およびインターフェイスの一元管理を行うことができます。

これはデバイス中心のビューであり、すべての管理対象デバイスを表示したり、特定のデバイスを選択してそのプロパティの表示や設定とポリシーの定義を行うことができます。特定のデバイスにセキュリティ ポリシーをローカルに定義できます。その後、そのポリシーを共有して、他のデバイスにグローバルに割り当てることができます。

[Devices] ページには、ペインが 2 つあります。左ペインには要素が 2 つあり、左上にデバイス セレクタ、左下にポリシーセレクタが配置されています。右ペインはメインのコンテンツ領域です。次の図に、[Devices] ページを示します。

図 *4 : [Devices]* ページ



デバイスセレクタ（1、3、4、5）：次の要素が含まれています。

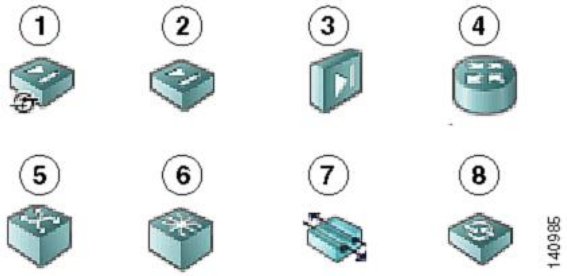
- [Add]/[Delete] ボタン（4、5）：Security Manager インベントリに対してデバイスの追加と削除を行うことができます。
- [Filter] フィールド（3）：独自に定義したフィルタリング基準に基づいて、デバイスのサブセットを表示できます。詳細については、セレクタ内の項目のフィルタリング （60 ページ）を参照してください。
- [Device] ツリー：システムに存在するデバイス グループおよびデバイスを一覧表示します。各デバイス タイプが、アイコンで表されます。アイコンについては、図 5 : デバイスのアイコン を参照してください。

マウスのポインタをデバイスの上に置くと、デバイスに関する詳細情報がポップアップ ウィンドウに表示されます。情報は、デバイスプロパティの概要です（[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ （137 ページ）を参照）。

（注） バージョン 4.8 以降、Security Manager は、Auto Update Server（AUS）を使用してアップグレードされたデバイスの更新されたバージョン情報を表示します。この機能を有効にするには、AUS ユーザーインターフェイスで Security Manager の詳細情報を設定する必要があります。デバイスにマウスのカーソルを合わせると、AUS がデバイスバージョンを正常に更新した場合、次のメッセージが表示されます。

「State Description: Version update is successfully completed by Auto Update Server. Check if any other configuration changes are required in Security Manager.」（状態の説明：Auto Update Server によるバージョンの更新が正常に完了しました。Security Manager で他の設定変更が必要かどうかを確認してください）

図 *5:* デバイスのアイコン



1	Adaptive Security Appliance（ASA）	5	Catalyst スイッチ
2	PIX ファイアウォール	6	Catalyst 7600 シリーズ ルータ
3	Catalyst セキュリティ サービス モジュール：Firewall Services Module（FWSM; ファイアウォール サービス モジュール）および ASA-SM	7	VPN 3000 コンセントレータ
4	Cisco IOS ルータ	8	侵入防御システム（IPS）

- ショートカット メニュー オプション：デバイスまたはデバイス グループを右クリックすると、そのデバイスまたはグループに関連するコマンドのメニューが表示されます。これらのコマンドは、通常のメニューで使用できるコマンドへのショートカットです。

ポリシーセレクタ（2）：次の要素が含まれています。

- ポリシー グループ：選択されたデバイス タイプでサポートされているポリシー グループを一覧表示します。表示されるポリシー グループは、次の 4 つの要因によって決まります。
  - デバイス セレクタで選択されているデバイスのタイプ。
  - デバイスで実行されているオペレーティング システム。

- 生成した設定に使用できるコマンドを決定するために選択したターゲットのオペレーティング システム バージョン。
- サポートされているサービス モジュールがデバイスに含まれているかどうか。

詳細については、ポリシーについて （209 ページ）を参照してください。

- ショートカット メニュー オプション：ポリシーを右クリックすると、そのポリシーに関連するコマンドのメニューが表示されます。これらのコマンドは、通常のメニューで使用できるコマンドへのショートカットです。

[コンテンツ（Contents）] ペイン（6）：メインのコンテンツ領域。

この領域に表示される情報は、デバイス セレクタから選択しているデバイスおよびポリシー セレクタから選択しているオプションによって異なります。

デバイス名およびデバイスと見なされる要素について

Security Manager では、従来のデバイスの管理のほか、あるタイプのセキュリティ デバイスに定義できる仮想デバイスも管理できます。このような仮想デバイスは、デバイス インベントリでは独立したデバイスとして扱われ、デバイス セレクタには独立したエントリとして表示されます。仮想デバイスは実際にはホストとなる物理デバイス上にあるため、展開など多くのアクションにはホスト デバイスだけでなく仮想デバイスも含める必要があります。

物理デバイスはすべて、デバイス セレクタに表示されます。また、デバイス セレクタに表示されるタイプの仮想デバイスでもあります。

- セキュリティ コンテキスト：PIX ファイアウォール、FWSM デバイス、ASA デバイスにセキュリティ コンテキストを定義できます。セキュリティ コンテキストは、仮想ファイアウォールとして機能します。デフォルトでは、セキュリティコンテキストは、*host-display-name_context-name* という命名ルールに基づいてデバイスセレクタに表示されます。*host-display-name* はコンテキストが定義されているデバイスの表示名で、*context-name* はセキュリティコンテキストの名前です。たとえば、firewall12 というデバイスにある admin セキュリティ コンテキストの場合は firewall12_admin となります。

ヒント [検出設定（Discovery settings）] ページ（[Discovery] ページ （674 ページ）を参照）の [セキュリティコンテキスト名を生成するときにデバイス名を先頭に追加する（Prepend Device Name when Generating Security Context Names）] プロパティを使用して、表示名をコンテキスト名に追加するかどうかを制御できます。ただし、表示名を追加しないと、コンテキストをホストしているデバイスを特定するのが容易ではなく、コンテキスト名がホスト デバイスでソートされません（コンテキスト名が、ホスト デバイスに付加されるフォルダに表示されません）。表示名を追加しないと、複数のコンテキストが同じ名前でインベントリに追加されている場合には、Security Manager がコンテキスト名に数値のサフィックスを追加します（たとえば、admin_01、admin_02）。このような数値は、ホスト デバイスとは関連がありません。

- 仮想センサー：IPS デバイスに仮想センサーを定義できます。仮想センサーは、*host-display-name_virtual-sensor-name* という命名ルールでデバイスセレクタに表示されます。この命名ルールを制御するための検出設定はありません。

ヒント　デバイスのプロパティでは、仮想センサー、セキュリティコンテキスト、または他のデバイスのタイプの表示名をいつでも変更できます。

仮想デバイスの命名ルールのほか、さまざまなタイプのデバイス名間の関係についても理解する必要があります。

- 表示名：表示名は、単にデバイス セレクタの Security Manager 内に表示される名前です。実際にデバイスに定義されている名前に関連している必要はありません。デバイスをインベントリに追加する際、入力した DNS 名または IP アドレスに基づいて表示名が提案されますが、任意の命名ルールを使用できます。
- DNS 名：デバイスに定義する DNS 名は、Security Manager サーバ向けの DNS サーバによって解決可能である必要があります。
- IP アドレス：デバイスに定義する IP アドレスは、そのデバイスの管理 IP アドレスである必要があります。
- ホスト名：デバイスを検出すると、デバイスプロパティに表示されるホスト名プロパティがデバイスの設定から取得されます。設定ファイルを使用してデバイスを追加する場合に、ファイルにホスト名コマンドが含まれていないと、設定ファイルの名前が初期ホスト名となります。

ただし、デバイスでホスト名を変更しても、ホスト名デバイスプロパティは更新されません。デバイス プラットフォーム ポリシー領域に [Hostname] ポリシーがあり、この [Hostname] ポリシーによってデバイスに定義されるホスト名が決まります。

デバイス クレデンシャルについて

Security Manager では、デバイスにログインする際にクレデンシャルが必要になります。デバイス クレデンシャルは次の 2 つのタイミングで提供できます。

- 手動またはネットワーク検出からデバイスを追加するとき。詳細については、次の項を参照してください。
  - ネットワークからのデバイスの追加　（100 ページ）
  - 手動定義によるデバイスの追加　（116 ページ）
- デバイス プロパティを編集するとき。詳細については、デバイス プロパティの表示または変更　（136 ページ）を参照してください。

次のデバイス クレデンシャルを指定できます。

- プライマリ クレデンシャル：SSH または Telnet を使用してデバイスにログインするためのユーザ名およびパスワード。デバイス通信には、この情報が必要です。
- HTTP クレデンシャル：HTTP 接続または HTTPS 接続を許可するデバイスもあれば、その接続を必要とするデバイス（IPS デバイスなど）もあります。デフォルトでは、Security Manager は HTTP/HTTPS アクセスにプライマリ クレデンシャルを使用しますが、一意の HTTP/HTTPS クレデンシャルを設定できます。
- Rx-Boot モード：（任意）Cisco ルータの中にはフラッシュ メモリから実行されるように設計されているものがあり、フラッシュの最初のファイルからだけ起動されます。つまり、フラッシュ イメージをアップグレードするには、フラッシュ内のイメージ以外のイメージを実行する必要があります。そのイメージが、Rx-Boot と呼ばれるサイズを小さくしたコマンド セット イメージ（ROM ベースのイメージ）です。
- SNMP クレデンシャル：（任意）簡易ネットワーク管理プロトコル（SNMP）を使用すると、ネットワーク デバイス間で管理情報を容易に交換できます。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

（注） PIX、ASA、およびFWSMデバイスでは、ユーザ名を4文字以上にする必要があります。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェアバージョン 9.6(1) 以降を実行している ASA デバイスの場合、最大 127 文字のパスワードを入力できます。

デバイス ベースのクレデンシャルを使用するのではなく、Security Manager にログインするときに使用するクレデンシャルを使用するように、Security Manager を設定できます。その後、AAA サーバーのアカウンティング機能を使用して、ユーザーによる設定変更を追跡することができます。ユーザ ログイン クレデンシャルが適しているのは、次の基準に従って、ご使用の環境が設定されている場合だけです。

- 変更の監査に TACACS+ または RADIUS を使用します。ユーザ ログイン クレデンシャルが、このようなアカウンティング レコードに反映されます。デバイス クレデンシャルを使用した場合は、Security Manager でのすべての変更が、どのユーザがその変更を加えたかに関係なく、同じアカウントによるものとなります。
- ユーザ アカウントは AAA サーバに設定されており、設定変更を実行するために必要なデバイス レベルのアクセス権が付与されています。
- 認可に AAA サーバを使用するように Security Manager および管理対象デバイスを設定します。AAA を使用するように Cisco Security Manager を設定する方法の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。
- ワンタイム パスワードは使用しません。

ネットワーク設定でユーザー ログイン クレデンシャルをサポートしている場合は、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択して、そのクレデンシャルを使用するようにSecurity Managerを設定できます。コンテンツテーブルから [デ

バイス通信（Device Communication）] を選択し、[デバイスへの接続方法（Connect to Device Using）] フィールドで [Security Managerのユーザーログイン資格情報（Security Manager User Login Credentials）] を選択します。デフォルトでは、すべてのデバイス アクセスにデバイス クレデンシャルが使用されます。

関連項目

- [Device Credentials] ページ （143 ページ）
- デバイス インベントリへのデバイスの追加 （94 ページ）
- [Device Communication] ページ （668 ページ）

デバイス プロパティについて

デバイスを Security Manager に追加するときには、デバイス プロパティを定義します。デバイス プロパティは、デバイス、クレデンシャル、デバイスが割り当てられているグループ、およびポリシー オーバーライドに関する一般的な情報です。デバイス アイデンティティやプライマリ クレデンシャルなど一部のデバイス プロパティ情報はデバイスを追加するときに指定する必要がありますが、[Device Properties] ダイアログボックスからプロパティを追加または編集できます。

デバイス プロパティを表示するには、デバイス セレクタで次のどちらかを実行します。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

[Device Properties] ダイアログボックスには、ペインが 2 つあります。左ペインにはコンテンツ テーブルがあり、次の項目が含まれています。

- [General]：デバイス アイデンティティ、デバイスで実行されているオペレーティング システム、およびデバイス通信設定など、デバイスに関する一般的な情報が含まれています。
- [Credentials]：デバイス プライマリ クレデンシャル（ユーザ名、パスワード、およびイネーブル パスワード）、SNMP クレデンシャル、Rx-Boot モード クレデンシャル、および HTTP クレデンシャルが含まれています。
- [Device Groups]：デバイスが割り当てられているグループが含まれています。
- [クラスタ情報（Cluster Information）]：クラスタ グループの詳細情報が含まれています（存在する場合）。
- [ライセンス情報（License Information）]：FPR-3100 シリーズ デバイスのライセンス ステータス、ライセンスの有効期限、およびライセンスの取得日に関する情報が含まれています。

（注） ライセンス情報パネルは、CSM 4.24 の FPR-3100 シリーズデバイスに対してのみ表示されます。

- [Policy Object Overrides]：再利用可能なポリシー オブジェクトのグローバル設定のうち、このデバイス用に上書きできるものが含まれています。

コンテンツ テーブルで項目を選択すると、対応する情報が右ペインに表示されます。

注記

- Security Manager は、[Device Properties] ページに表示される DNS ホスト名が、デバイスに設定したホスト名と同じであるとは想定していません。
- デバイスを Security Manager に追加するときには、管理 IP アドレスまたは DNS ホスト名を入力する必要があります。設定ファイルから検出するときには管理インターフェイスを特定できず、そのため管理 IP アドレスも特定できないため、設定ファイルに記載されたホスト名が DNS ホスト名として使用されます。設定ファイルの CLI にホスト名が見当たらない場合は、設定ファイル名が DNS ホスト名として使用されます。
- ネットワークからデバイスを検出するときには、[Device Properties] ページの DNS ホスト名が、デバイスに設定されたホスト名で更新されません。このため、デバイスの DNS ホスト名を指定する場合は、デバイスを Security Manager または [Device Properties] ページに追加するときに手動でそのホスト名を指定する必要があります。

デバイス プロパティの詳細については、デバイス プロパティの表示または変更 （136ページ）を参照してください。

デバイス インベントリへのデバイスの追加

デバイスを Security Manager に追加するときには、DNS 名や IP アドレスなど、デバイスの識別情報を指定します。この情報は、デバイス検出時に追加されます。ポリシー検出を開始して、デバイスに関連付けられた既存のネットワーク設定を取り込むこともできます。ポリシー検出の詳細については、ポリシーの検出 （223ページ）を参照してください。追加したデバイスは、Security Manager デバイス インベントリに表示されます。

New Device ウィザードに従うと、デバイスをインベントリに追加するプロセスを実行できます。多種多様な追加元からデバイスを追加できます。ウィザードに至るパスは、使用する方法によって大きく異なります。

（注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェアサポートは提供されません。

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）]>[新規デバイス（New Device）] を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。

（注） デバイスを追加するには、他の方法もあります。デバイスインベントリだけではなく、割り当てられたポリシーおよびポリシーオブジェクトも含む .dev ファイルを別の Security Manager サーバーからエクスポートした場合、[ファイル（File）]>[インポート（Import）] コマンドを使用して、ファイルをインポートできます。詳細については、ポリシーまたはデバイスのインポート （615 ページ）を参照してください。

デバイスおよびサービス モジュールの追加に関するヒント

- PIX ファイアウォール、FWSM デバイス、および ASA デバイスがフェールオーバーに対応するように設定されている場合、アクティブ装置だけを Security Manager に追加します。デバイスに管理 IP アドレスを設定し、その IP アドレスを検出に使用するようにします。フェールオーバー対応のサービスモジュール（FWSM または ASA-SM）が複数含まれている Catalyst スイッチを検出するときは、画面の指示に従って、フェールオーバーモジュールに対して [モジュールを検出しない（Do Not Discover Module）] を選択します。Security Manager は、プライマリまたはセカンダリのどちらのフェールオーバー サービス モジュールが追加されたにかかわらず、常にアクティブな管理コンテキストを管理します。
- Security Manager は、ASA 設定ガイドで定義されている CLI ブートストラップを使用して ASA クラスタを 1 つのクラスタとして設定した後、ASA クラスタを管理できます（http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html [英語] を参照）。クラスタのすべてのメンバーには、ブートストラッププロセスの際に個別の IP アドレスが割り当てられます。クラスタを Security Manager に追加するときは、メインクラスタの IP アドレスを使用してクラスタを検出します。メインクラスタの IP アドレスは、そのクラスタの固定アドレスであり、常に現在の制御ユニットに属します。これは制御ユニットの個別の IP アドレスではありません。クラスタの詳細については、デバイスクラスタの使用 （97 ページ）を参照してください。
- サービス モジュールは、独立したデバイスとして扱われます。ほとんどのモジュールでは、ホスト デバイスとは別にサービス モジュールを追加する必要があります。ただし、Security Manager では Catalyst 6500 デバイスの FWSM モジュールまたは IDSM モジュールを自動的に検出できるため、親デバイスを追加するだけで十分です。（ASA-SM は、親デバイスの検出中に検出できません。ASA-SM を個別に追加する必要があります）この唯一の例外は、HTTPS（SSL）にデフォルト以外のポートを使用するように FWSM モジュールまたは IDSM モジュールを設定する場合です。この場合、モジュールを個別に追加する必要があります。
- セキュリティ コンテキストが複数ある ASA-SM または FWSM を追加するときには（これらはマルチ コンテキスト モードで動作しています）、それぞれの管理 IP アドレスを使用してセキュリティ コンテキストを個別に追加しないでください。その代わりに、管理コンテキストの管理アドレスを使用してデバイスを追加します（これにより、個々のコンテキストも追加されます）。次に、 Security Manager でマルチ コンテキストの FWSM に設定

を展開する方法の変更 （594 ページ）の説明に従って、マルチ コンテキスト デバイスに設定をシリアルに展開するように Security Manager を設定します。

- Security Manager ライセンスに定義されているデバイス制限を超えてデバイスを追加することはできません。たとえば、50 台のデバイスのライセンスを保有し、インベントリに 45 台のデバイスがある場合、セキュリティ コンテンツが 6 個あるマルチ コンテキスト ASA を追加しようとすると、デバイスの追加と検出が失敗します。

次の項では、デバイスを追加するさまざまな方法について説明します。

- [ネットワークからのデバイスの追加（Add Device from Network）]：ネットワークで現在アクティブなデバイスを追加するには、 ネットワークからのデバイスの追加 （100 ページ）を参照してください。Security Manager は、デバイスに直接かつ安全に接続し、その識別情報およびプロパティを検出します。
  - **長所**：デバイスに関する最小限の情報を指定すればよく、Security Manager がデバイスから直接詳細な情報を取得して正確性を保ちます。
  - **短所**：追加できるデバイスは一度に 1 つだけです。ダイナミック IP アドレスが付与されているデバイスを追加するには、デバイスの現在の IP アドレスを特定し、そのアドレスを使用してデバイスを追加し、デバイスを管理している Configuration Engine を特定するように Security Manager でデバイスプロパティを更新する必要があります。
- [構成ファイルからの追加（Add from Configuration File）]：デバイス構成ファイルのコピーを使用してデバイスを追加するには、設定ファイルからのデバイスの追加 （112 ページ）を参照してください。
  - **長所**：一度に複数のデバイスを追加できます。
  - **短所**：この方法では、Catalyst 6500/7600 デバイスおよび IPS デバイスを追加できません。設定ファイルをいくつかまとめて追加するときには、そのどちらのファイルも同じデバイス タイプである必要があります。

また、デバイスとの接続を必要とするポリシーを正常に検出できません。たとえば、ポリシーがデバイスに存在するファイルを指している場合、構成ファイルを使用してデバイスを追加すると、Security Manager がデバイスから参照先のファイルを取得できないため、Security Manager 設定に **no** 形式のコマンドが含まれることになります。たとえば、Web VPN の **svc image** コマンドが無効になることがあります。

- [新規デバイスの追加（Add New Device）]：ネットワークにまだ存在しないデバイスを追加して Security Manager でそのデバイスを事前プロビジョニングできるようにするには、手動定義によるデバイスの追加 （116 ページ）を参照してください。デバイス ハードウェアを設置する前に、システムでデバイスを作成し、ポリシーをデバイスに割り当て、設定ファイルを生成できます。
  - **長所**：ネットワークにまだ存在しないデバイスを事前プロビジョニングできます。
  - **短所**：他の方法よりも詳細な情報を指定する必要があります。Catalyst 6500 デバイス、または IPS モジュールが含まれているルータを作成する場合、[ポリシー（Policy）]>

[デバイス上のポリシーを検出する（Discover Policies on Device）] を選択して、そのモジュールを検出する必要があります。

- [ファイルからのデバイスの追加（Add Device from File）]：カンマ区切り値（CSV）形式のインベントリファイルからデバイスを追加するには、インベントリ ファイルからのデバイスの追加 （122 ページ）を参照してください。
  - **長所**：タイプの異なる複数のデバイスを一度に追加できます。CiscoWorks Common Services、Cisco Security Monitoring, Analysis and Response System（CS-MARS）、その他の Security Manager サーバなど、他のネットワーク管理アプリケーションのインベントリ リストを再利用できます。別の Security Manager サーバからエクスポートされたファイルを使用する場合は、ポリシーを検出するせずに任意でデバイスを追加できます。これは、オフライン デバイスまたはスタンバイ デバイスを追加する場合に便利です。
  - **短所**：この方法では、インベントリですでに定義されているデバイスのプロパティを更新できません。また、100 を超えるデバイスを一度にインポートしようとすると、ポリシー検出が失敗することがあり、それより少ない数でも失敗する可能性があります。IPS デバイスの場合には、ポリシー検出の失敗を避けるため、5 台以上の IPS デバイスを一度に追加しないでください。

デバイスクラスタの使用

クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。クラスタリングは、9.0(1) 以降を実行している ASA 5580 および 5585 デバイス、および 9.1(4) 以降を実行している ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X デバイスでサポートされています。

Security Manager は、ASA 設定ガイドで定義されている CLI ブートストラップを使用して ASA クラスタを 1 つのクラスタとして設定した後、ASA クラスタを管理できます（http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html [英語] を参照）。

クラスタのすべてのメンバーには、ブートストラッププロセスの際に個別の IP アドレスが割り当てられます。クラスタを Security Manager に追加するときは、メインクラスタの IP アドレスを使用してクラスタを検出します。メインクラスタの IP アドレスは、そのクラスタの固定アドレスであり、常に現在の制御ユニットに属します。これは制御ユニットの個別の IP アドレスではありません。

（注） 必要な CLI ブートストラップを実行した後にデバイスを再検出しても、スタンドアロンデバイスを Security Manager のクラスタに変換することはできません。最初に Security Managerからデバイスを削除する必要があります。次に、必要なCLIブートストラップを実行した後で、クラスタを新しいデバイスとして Security Manager に追加できます。

Security Manager ではクラスタは単一のデバイスとして表されます。クラスタが Security Manager に追加されたら、クラスタインターフェイスやセキュリティポリシーなどのクラスタ設定の構成を完了することができます。

（注） クラスタリングには、設定に関する特定の要件および制限があります。要件、設定の推奨事項、およびパフォーマンス情報の詳細については、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html にある ASA のドキュメントを参照してください。

ASA クラスタでサポートされない機能

これらの機能は、クラスタリングがイネーブルのときは設定できず、コマンドは拒否されます。

- ユニファイド コミュニケーション
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 次のアプリケーション インスペクション：
  - CTIQBE
  - GTP
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SIP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- ボットネット トラフィック フィルタ
- Auto Update Server

- DHCP クライアント、サーバ、リレー、およびプロキシ
- VPN ロード バランシング
- フェールオーバー
- ASA CX モジュール

中央集中型機能

次の機能は、制御ユニット上だけでサポートされます。クラスタの場合もスケーリングされません。たとえば、8 ユニット（5585-X と SSP-60）から成るクラスタがあるとします。Other VPN ライセンスでは、1 台の ASA 5585-X と SSP-60 に対して許可される IPSec トンネルの最大数は 10,000 です。8 ユニット クラスタ全体で使用できるトンネル数は 10,000 までです。この機能はスケーリングしません。

（注） 中央集中型機能のトラフィックは、メンバーユニットから制御ユニットに、クラスタ制御リンクを介して転送されます。クラスタ制御リンク用に十分な帯域幅を確保するには、ASA ドキュメントの「クラスタ制御リンクのサイジング」を参照してください。再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ユニット以外のユニットに転送されることがあります。この場合は、トラフィックが制御ユニットに送り返されます。中央集中型機能については、制御ユニットで障害が発生するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

- サイト間 VPN
- 次のアプリケーション インスペクション：
  - DCERPC
  - NetBios
  - PPTP
  - RADIUS
  - RSH
  - SUNRPC
  - TFTP
  - XDMCP
- ダイナミック ルーティング（スパンド EtherChannel モードのみ）
- マルチキャスト ルーティング（個別インターフェイス モードのみ）
- スタティック ルート モニタリング

- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス

個々のユニットに適用される機能

これらの機能は、クラスタ全体ではなく、個々の ASA ユニットに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは、各ユニットに対して個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。8 ユニットから成るクラスタがあり、トラフィックが均等に分散している場合は、適合レートは実際にクラスタのレートの 8 倍になります。
- 脅威検出：脅威検出は、各ユニットに対して個別に機能します。たとえば、上位統計情報は、ユニット別です。たとえば、ポート スキャン検出が機能しないのは、スキャン トラフィックが全ユニット間で分散されるので、1 つのユニットがすべてのトラフィックを読み取ることはないからです。
- リソース管理：マルチ コンテキスト モードでのリソース管理は、ローカル使用状況に基づいて各ユニットに個別に適用されます。
- IPS モジュール：IPS モジュール間でのコンフィギュレーションの同期や状態の共有は行われません。IPS シグニチャによっては、IPS が複数の接続にわたって状態を保持することが必要になります。たとえば、ポート スキャン シグニチャが使用されるのは、同じ人物が同じサーバーへの多数の接続を、それぞれ異なるポートを使用して開いていることを IPS モジュールが検出した場合です。クラスタリングでは、これらの接続は複数の ASA デバイス間で分散されます。これらのデバイスそれぞれに専用の IPS モジュールがあります。これらの IPS モジュールはステート情報を共有しないので、結果としてのポート スキャンをクラスタが検出できない場合があります。

関連項目

- [グループ情報（Group Information）] ページ （149 ページ）

ネットワークからのデバイスの追加

デバイスをインベントリに追加する最も簡単で最も信頼性の高い方法の 1 つに、ネットワークでアクティブであるデバイスを特定するというものがあります。デバイスの IP アドレス（または DNS ホスト名）およびデバイスへのログインに必要なクレデンシャルを提供すると、

Security Manager では必要な情報の多くをデバイスから直接取得して、情報の精度を確保できます。

はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス グループの使用 （164 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

ステップ 1 デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

ステップ 2 [方式を選択（Choose Method）] ページで、[ネットワークからのデバイスの追加（Add Device from Network）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます。

ステップ 3 [Device Information] ページで、少なくとも次のフィールドに値を入力します。すべてのフィールドの詳細については、[Device Information] ページ - [Add Device from Network] （103 ページ）を参照してください。

- ホスト名と DNS 名、または IP アドレス（あるいはその両方）を入力します。
- 表示名を入力します。この名前は Security Manager のデバイス セレクタに表示されます。
- 正しいオペレーティング システムとバージョンを選択します。Catalyst スイッチまたは 7600 ルータを設定している場合は、[IOS - Catalyst Switch/7600] を選択し、それ以外の IOS エントリは選択しません。
- Security Manager に定義されているデフォルトとは異なるプロトコルを使用するようにデバイスが設定されている場合には、デバイスにログインするのに使用するトランスポート プロトコルを選択します。デフォルトは、[Device Communication] 管理ページに設定されています（[Device Communication] ページ （668 ページ）を参照）。

[次へ（Next）] をクリックします。

ステップ 4 [Device Credentials] ページで、デバイスへのログインに必要なユーザ名およびパスワードを入力します。少なくともプライマリ デバイス クレデンシャルを入力します。これは、従来のユーザ EXEC モードと特権 EXEC モードのパスワードです。

クレデンシャルの各種タイプについては、[Device Credentials] ページ （143 ページ）を参照してください。

ヒント [Device Credentials] ページで [Next] または [Finished] をクリックすると、Security Manager はデバイスに接続できるかどうかをテストします。テストが正常に完了しないかぎり、デバイスは追加できません。詳細については、デバイス接続のテスト （573 ページ）を参照してください。

ステップ 5 （任意）[次へ（Next）] をクリックして [デバイスのグルーピング（Device Grouping）] ページを開き、インポートしたデバイスの追加先となるデバイスグループを選択します（[Device Groups] ページ （148 ページ）を参照）。

ステップ 6 [終了（Finish）] をクリックします。Security Manager が [Discovery Status] ダイアログボックスを開きます。ここでは、デバイス検出およびポリシー分析のステータスを参照できます（[Discovery Status] ダイアログボックス （238 ページ）を参照）。

ヒント デバイスの追加中にポリシーを検出している場合は、提示されているメッセージをよくお読みください。これらのメッセージには、次に実行する手順に関する重要な推奨事項が含まれている場合があります。Security Manager が設定の所有権を引き継ぐことができるように、検出した設定をファイルにすぐに展開することを推奨します。展開方法の詳細については、展開方法について（490 ページ）を参照してください。

ステップ 7 モジュールが含まれているデバイスを追加し、Security Manager がそのタイプのデバイスでモジュールの検出をサポートしている場合、デバイスシャーシの検出が完了したときに通知され、デバイスのモジュールを検出するかどうかを確認されます。[はい（Yes）] をクリックすると、次の情報の入力を要求されます。

- Catalyst 6500 サービス モジュール：[Service Module Credentials] ダイアログボックスが開き、シャーシに含まれているモジュールに基づいて次の情報の入力が要求されます。詳細については、[Service Module Credentials] ダイアログボックス （108 ページ）を参照してください。
  - FWSM：管理 IP アドレス（推奨する）、ユーザ名とパスワード、および実行する検出のタイプ。FWSM がフェールオーバーペアの 2 番めのデバイスである場合は、フェールオーバーモジュールの [モジュールを検出しない（Do Not Discover Module）] を選択します。（Security Manager は、プライマリまたはセカンダリのどちらのフェールオーバー サービスモジュールが追加されたにかかわらず、常にアクティブな管理コンテキストを管理します）。
  - IDSM：ユーザ名とパスワード、および実行する検出のタイプ。
  - ASA-SM：Catalyst 6500 で、シャーシ経由での ASA サービス モジュールの検出はサポートされません。ASA-SM は、ASA-SM の管理 IP アドレスを使用して直接追加する必要があります。

    （注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェア サポートは提供されません。

- IPS ルータ モジュール：実行する検出のタイプ、管理 IP アドレス、ユーザ名とパスワード、およびその他の SSL 接続情報。詳細については、[IPS Module Discovery] ダイアログボックス （110 ページ）を参照してください。

Security Manager で管理しないモジュールの検出をスキップできます。

[OK] をクリック [Discovery Status] ダイアログボックスに戻り、サービス モジュールの検出の経過を表示できます。完了したらウィンドウを閉じます。デバイスがインベントリ リストに追加されます。リストに掲載するすべてのデバイスのアクティビティ（たとえば、ASA デバイスに定義されている個々のセキュリティ コンテキスト）を送信する必要がある場合には、メッセージにその説明が示されます。

ステップ 8 デバイスセレクタでデバイスを選択して Auto Update Server または Configuration Engine によって管理されているデバイスを追加した場合は、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選

択します。[Auto Update] または [Configuration Engine] 設定で、デバイスで使用するサーバを選択します。サーバがリストにない場合は追加できます。詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）を参照してください。

[Device Information] ページ - [Add Device from Network]

ネットワークからデバイスを追加する場合は、New Device ウィザードの [デバイス情報（Device Information）] ページを使用して、デバイスの識別情報を指定します。

（注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。

ナビゲーション パス

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。

関連項目

- デバイス ビューについて （87 ページ）
- ネットワークからのデバイスの追加 （100 ページ）
- [Device Credentials] ページ （143 ページ）
- [Device Groups] ページ （148 ページ）
- ポリシーの検出 （223 ページ）
- [Device Communication] ページ （668 ページ）

フィールド リファレンス

表 *15* : ネットワークからデバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ

要素	説明
ID	

要素	説明
IP タイプ（IP Type）	デバイスの IP アドレスをスタティックにする（デバイスで定義する）か、またはダイナミックにする（DHCP サーバから取得する）かを指定します。選択した IP タイプによって、表示されるフィールドが異なります。 スタティック IP アドレスを持つデバイスだけを追加できます。 （DHCP サーバから提供される）ダイナミック アドレスを使用するデバイスを追加するには、デバイスの現在の IP アドレスを特定し、そのアドレスを使用します。デバイスを追加したあと、そのプロパティで [IP Type] を [Dynamic] に変更し、デバイスを管理している AUS または Configuration Engine を特定します。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。IPv6 アドレスは 128 ビットの一意のアドレスです。IPv6 アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは、IPv6 アドレスではサポートされません。
ホストネーム	デバイスの DNS ホスト名。IP アドレスが不明な場合に、DNS ホスト名を入力します。 （注） DNS ホスト名と IP アドレスのどちらか一方、または両方を入力する必要があります。
ドメイン名	デバイスの DNS ドメイン名。
IP Address	デバイスの管理 IP アドレス。IP アドレスは、10.64.3.8 というように、ドット付きの 4 つの数字列でなければなりません。 （注） IP アドレスと DNS ホスト名のどちらか一方、または両方を入力する必要があります。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。デバイスがデュアルスタックで設定されている場合、Security Manager は、Security Manager に追加されたデバイスの IP アドレスに基づいてデバイスと通信します。IPv6 アドレスは 128 ビットの一意のアドレスです。
表示名	Security Manager のデバイス セレクタに表示する名前。ホスト名または IP アドレスを入力した場合は、そのホスト名または IP アドレスがこのフィールドに自動的に入力されますが、変更することもできます。 最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。 （注） 2 つのデバイスに同じ表示名を設定することはできません。

要素	説明
OS タイプ	デバイスで実行されているオペレーティング システムのファミリ。慎重に正しいタイプを選択する必要があります。選択内容が、Security Manager がデバイスにログインし、デバイスの設定を取得する方法に影響を与えるためです。次のオプションがあります。 • [IOS 12.3+]：Cisco IOS ソフトウェアリリース 12.3 以降を実行している Cisco ルータの場合。Catalyst 6500/7600 または他の Catalyst デバイスの場合には選択しないでください。 ヒント Aggregation Services Router（ASR; アグリゲーション サービス ルータ）の場合は、バージョン 12.2 を実行中であっても、このオプションを選択します。ASR IOS リリースは、上位のリリースとして扱われます。 • [IOS - Catalystスイッチ/7600（IOS - Catalyst Switch/7600）]：すべての Catalyst スイッチおよび 7600 デバイスの場合。 • [ASA]：すべての ASA デバイスの場合。 • [FWSM]：すべての FWSM デバイスの場合。 • [IPS]：IPS ソフトウェアを実行しているすべてのデバイスの場合。 • [PIX]：すべての PIX デバイスの場合。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。この機能は、オペレーティング システムのタイプが ASA または FWSM であるデバイスでのみ使用できます。
トランスポート プロトコル（Transport Protocol）	デバイスに接続するときに Security Manager で使用するプロトコル。デバイスに設定され、かつクレデンシャルを提供できるプロトコルを選択します。各デバイス タイプにはデフォルト プロトコルがあり、通常この方法がそれぞれのデバイスで使用されます。

要素	説明
システムコンテキスト	マルチ コンテキスト モードで実行されている PIX ファイアウォール 7 デバイス、ASA デバイス、または FWSM デバイスのシステム実行スペースを検出するかどうかを指定します。複数のセキュリティ コンテキストをホストするデバイスを検出している場合は、このチェックボックスをオンにするかどうかが、Security Manager でデバイスを設定する方法に重要な意味を持ちます。デバイスで検出される対象も、[セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）] チェックボックスをオンにするかどうかによって異なります。 • [システムコンテキスト（System Context）] と [セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）] のどちらもオン：これが推奨する選択です。Security Manager は、デバイスに定義されているシステム実行スペースおよびすべてのセキュリティ コンテキストを検出して、デバイス セレクタに一覧表示します。[Discovery] ページ（[Discovery] ページ （674 ページ）を参照）に設定されたデフォルトの命名ルールを変更していないかぎり、基本表示名はシステム実行スペースを表したもの（たとえば、10.10.11.24）であり、セキュリティ コンテキストはノードではコンテキスト名をデバイス名に付加したもの（たとえば、10.10.11.24_admin）として表されます。 • [システムコンテキスト（System Context）] はオン、[セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）] はオフ：システム実行スペースが検出されて、デバイスセレクタに追加されます。あとでセキュリティ コンテキストのポリシーを検出できます。この方法は、インベントリを検出するユーザ グループと、さらにもう 1 つポリシーを検出するグループがある場合に適しています。 • どちらのチェックボックスもオフ：管理コンテキストだけが検出されて、デバイス セレクタに追加されます。他のセキュリティ コンテキストは検出できず、管理もできません。
デバイス設定の検出	

要素	説明
検出	検出してインベントリに追加する要素のタイプ。次のオプションがあります。 • [Policies and Inventory]：ポリシー、インターフェイス、およびサービス モジュール（該当する場合）を検出します。これがデフォルトであり、推奨オプションです。 ポリシーの検出が開始されると、デバイス上の設定が分析され、設定されているサービスとプラットフォームのポリシーがインポートされます。インベントリの検出が開始されると、デバイス上のインターフェイスが分析され、インターフェイス リストがインポートされます。デバイスが複合デバイスの場合は、デバイス内のすべてのサービス モジュールが検出され、インポートされます。 このオプションを選択すると、下のチェックボックスがアクティブになり、それらのチェックボックスを使用して、検出されるポリシーのタイプを制御できます。 （注） 検出中に非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。同じ ACL を展開すると、その ACL は Security Manager によって削除されます。 • [Inventory Only]：インターフェイスとサービス モジュール（該当する場合）を検出します。 • [No Discovery]：すべての検出がスキップされます。デバイスのポリシー、インターフェイス、またはサービス モジュール情報はデバイス インベントリに追加されません。
プラットフォーム設定	プラットフォーム固有のポリシー ドメインとも呼ばれるプラットフォーム設定を検出するかどうかを指定します。プラットフォーム固有のポリシー ドメインは、ファイアウォール デバイスと Cisco IOS ルータ上にあります。これらのドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。詳細については、サービスポリシーとプラットフォーム固有のポリシー （211 ページ）を参照してください。
ファイアウォール ポリシー	ファイアウォール サービスとも呼ばれるファイアウォール ポリシーを検出するかどうかを指定します。ファイアウォール サービスには、アクセル ルール、インスペクション ルール、AAA ルール、Web フィルタ ルール、トランスペアレント ルールなどのポリシーが含まれます。詳細については、ファイアウォール サービスの概要 （755 ページ）を参照してください。
IPS ポリシー	シグニチャや仮想センサーなどの IPS ポリシーを検出するかどうかを指定します。詳細については、IPS 設定の概要 （2088 ページ）またはCisco IOS IPS 設定の概要 （2318 ページ）を参照してください。

要素	説明
RA VPN ポリシー	IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモート アクセス VPN ポリシーを検出するかどうかを指定します。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモート アクセス VPN の管理の基礎（1655 ページ）を参照してください。
Discover Policies for Security Contexts	セキュリティ コンテキストのポリシーを検出するかどうかを指定します。セキュリティ コンテキストは、PIX ファイアウォール デバイス、ASA デバイス、または FWSM デバイスに適用されます。このフィールドは、[IPタイプ（IP Type）] に [スタティック（Static）] を選択し、[システムコンテキスト（System Context）] をオンにした場合にのみアクティブになります。

[Service Module Credentials] ダイアログボックス

[Service Module Credentials] ダイアログボックスは、Catalyst デバイスのサポート対象のサービス モジュールにログインするときに必要なクレデンシャルを追加する場合に使用します。

このダイアログボックスではサポート対象のモジュールが各スロットにまとめられており、モジュールのタイプが示されています。たとえば、グループが **Slot 3 (IDSM) Credentials** という名前である場合、シャーシの 3 番めのスロットに IDSM があることを示しています。

（注） Security Manager は VPN モジュールを検出しますが、その検出はシャーシ経由で実施され、クレデンシャルは必要ありません。ASA サービスモジュール（ASA-SM）は、シャーシを介して検出できません。それらは個別に追加する必要があります。

ナビゲーション パス

サービス モジュールを含めることができる Catalyst シャーシでポリシーを検出すると、そのサービス モジュールを検出するかどうかが確認されます。[はい（Yes）] をクリックすると、このダイアログボックスが表示されます。次のいずれかの方法を使用してポリシー検出を実行できます。

- ネットワークからデバイスを追加する場合。ネットワークからのデバイスの追加 （100 ページ）を参照してください。
- エクスポート ファイルからデバイスを追加する場合。インベントリ ファイルからのデバイスの追加 （122 ページ）を参照してください。
- インベントリにすでにあるデバイスでポリシー検出を実行する場合。Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

フィールド リファレンス

表 *16 : [Service Module Credentials]* ダイアログボックス

要素	説明
Discovery Mode	このモジュールのために検出するポリシーのタイプ。 • [Discover Inventory and Policies]：インベントリとセキュリティ ポリシーを検出します。これは推奨オプションです。 • [Discover Inventory Only]：セキュリティ ポリシーは検出しませんが、VLAN 設定、セキュリティ コンテキスト、インターフェイスなどのインベントリは検出します。サービスモジュールを右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択して、あとでポリシー設定を検出できます。 • [Do Not Discover Module]：このモジュールに対する検出をスキップし、このモジュールをインベントリに追加しません。
Connect to FWSM	Security Manager が FWSM にアクセスする方法。 • [Directly]：FWSM の管理 IP アドレスを使用して、FWSM に接続します。この方法を推奨します。フェールオーバー デバイスに接続している場合には必須の方法となります。それ以外の場合、Security Manager はフェールオーバー後にスタンバイ FWSM に接続することがあります。 • [via Chassis]：シャーシ経由で FWSM に接続します。この方法には、FWSM に定義されているセキュリティ コンテキストの数が 20 個未満であるという制約があります。Security Manager は、SSH 経由で Catalyst デバイスに接続し、その後 **session** コマンドで FWSM に接続します。Catalyst デバイスでは同時 SSH セッションの数が制限されており、デフォルト値は 5 です。ポリシー検出ではセキュリティ コンテキストごとに 1 つの SSH セッションを使用するため、コンテキストの数が多くなると接続が失敗することがあります。[直接アクセス（Directly）] を選択した場合、Security Manager が SSL で FWSM に接続するため、同時セッションの制限が大きくなります。
管理 IP（Management IP）	サービス モジュールの管理 IP アドレス。 FWSM の場合、接続方法に [シャーシ経由（via Chassis）] を選択したときには、このフィールドは使用できません。

要素	説明
ユーザー名	サービス モジュールのユーザ名。 マルチコンテキストモードで動作する FWSM の場合、どのコンテキストのユーザー名およびパスワードを入力すればよいかが脚注に示されます。システムコンテキストか管理コンテキストのいずれかになります。スイッチのシャーシ経由でマルチコンテキスト モードのデバイスに接続している場合は、システム実行スペースと管理コンテキストのいずれにも同じユーザ名およびパスワードを設定し、このダイアログボックスにそのクレデンシャルを指定する必要があります。 ユーザ名は、4 文字以上にします。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェアバージョン 9.6(1) 以降を実行している ASA デバイスの場合、最大 127 文字のパスワードを入力できます。
パスワード	サービス モジュールのユーザ EXEC モード パスワード。[Confirm] フィールドに、パスワードを再入力します。
パスワードを有効にする（Enable Password） （FWSM 専用）	サービス モジュールの特権 EXEC モード パスワード。[Confirm] フィールドに、パスワードを再入力します。

[IPS Module Discovery] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[IPS Module Discovery] ダイアログボックスは、インベントリに追加しているルータで AIM-IPS や NME などの IPS モジュールへのログインに必要なクレデンシャルを追加する場合に使用します。

ナビゲーション パス

IPS モジュールが含まれているルータ シャーシでポリシーを検出すると、そのモジュールを検出するかどうかが確認されます。[はい（Yes）] をクリックすると、このダイアログボックスが表示されます。次のいずれかの方法を使用してポリシー検出を実行できます。

- ネットワークからデバイスを追加する場合。ネットワークからのデバイスの追加 （100 ページ）を参照してください。
- インベントリ ファイルからデバイスを追加する場合。インベントリ ファイルからのデバイスの追加 （122 ページ）を参照してください。

- ネットワークにすでにあるデバイスでポリシー検出を実行する場合。 Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

フィールド リファレンス

表 *17 : [IPS Module Discovery]* ダイアログボックス

要素	説明
検出	このモジュールの検出のタイプ。 • [Discover Inventory and Policies]：インベントリとセキュリティ ポリシーを検出します。これは推奨オプションです。 • [Discover Inventory Only]：セキュリティ ポリシーは検出しませんが、仮想センサーやインターフェイスなどのインベントリは検出します。モジュールを右クリックし、[デバイスでポリシーを検出する（Discover Policies on Device）] を選択して、あとでポリシー設定を検出できます。 • [Do Not Discover Module]：このモジュールに対する検出をスキップし、このモジュールをインベントリに追加しません。
IPアドレス	モジュールの管理 IP アドレス。
HTTP Credentials Group モジュールへのログインに必要なクレデンシャル。	
ユーザー名	モジュールのユーザ名。
パスワード	指定したユーザ名のパスワード。[Confirm] フィールドに、パスワードを再入力します。
HTTP ポート（HTTP Port）	モジュールへのHTTPアクセス用に設定されたポート。デフォルトは 80 です。
HTTPS ポート（HTTPS Port）	モジュールへの SSL（HTTPS）アクセス用に設定されたポート。デフォルトは、[デバイス通信（Device Communication）] ページ（[ツール（Tools）]>[Security Manager管理（Security Manager Administration）]>[デバイス通信（Device Communication）]。詳細については、[Device Communication] ページ （668 ページ）を参照してください）に定義されています。通常使用されるポートは 443 です。 デフォルトを上書きするには、[デフォルトの使用（Use Default）] の選択を解除し、適切なポート番号を入力します。
IPS RDEP Mode	イベント モニタリングのために RDEP または SDEE 接続を確立するときに、IPS デバイスへのアクセスに使用する接続方法。

要素	説明
Certificate Common Name	証明書に割り当てられる名前。共通名は、証明書に割り当てられた個人、システム、またはその他のエンティティの名前にすることができます。[Confirm] フィールドに、共通名を再入力します。

設定ファイルからのデバイスの追加

Security Manager にデバイス設定を処理させることにより、デバイスにログインせずにデバイスをインベントリに追加できます。デバイスごとに、デバイス設定をファイルにコピーし、そのファイルを Security Manager サーバに配置する必要があります。

この手順を使用して、IPS デバイスまたは Catalyst 6500/7600 デバイスをインベントリに追加することはできません。

はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。
- Security Manager サーバ上のディレクトリにデバイス設定ファイルをコピーします。マウントしたドライブを使用することはできません。各設定に適切なデバイス タイプを容易に選択できるような命名ルールを使用してください。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス グループの使用 （164 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

ステップ 1 デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

ステップ 2 [方式を選択（Choose Method）] ページで、[設定ファイルから追加（Add from Configuration File）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます（ [Device Information] ページ - [Configuration File] （113 ページ）を参照）。

ステップ 3 デバイス タイプ セレクタから設定ファイルのデバイス タイプを選択し、適切なシステム オブジェクト ID を選択します。複数のデバイス タイプに対してそれぞれ設定ファイルがある場合は、デバイス タイプに基づいてそれらの設定ファイルを一括して追加します。

ステップ 4 [参照（Browse）] をクリックし、追加する（指定したタイプの）デバイスが含まれている設定ファイルを選択します。

ステップ 5 どのタイプのポリシーを検出するかを示す適切な検出オプションを選択します。

ステップ 6 （任意）[次へ（Next）] をクリックし、新規デバイスを所属させるデバイスグループを選択します。

ステップ 7 [終了（Finish）] をクリックします。Security Manager が [Discovery Status] ダイアログボックスを開きます。ここでは、設定ファイル分析のステータスを参照できます（ [Discovery Status] ダイアログボックス （238 ページ）を参照）。完了したらウィンドウを閉じます。デバイスがインベントリ リストに追加されます。

ヒント ポリシーの検出中に予期しないエラーが返された場合は、設定ファイルに主要な Cisco IOS ソフトウェア バージョンだけが含まれ、ポイント リリース情報が含まれていないことが原因である可能性があります。デバイスに定義されているポリシーによっては、ポイント リリースで使用できるようになった機能を使用しているものがあります。つまり、Security Manager がその機能をサポート対象であると認識していない可能性があります。この問題を解決するには、デバイスを追加したあと、デバイス セレクタでそのデバイスを選択し、右クリックして [デバイスのプロパティ（Device Properties）] を選択します。[全般（General）] ページで、デバイスで実行されているバージョンに最も近く、かつそのバージョンより新しいものではないソフトウェア バージョンで [ターゲット OS バージョン（Target OS Version）] フィールドを更新します（バージョン番号を取得するには、デバイスの CLI で **show version** コマンドを使用します）。その後、右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択して、ポリシーを再検出できます。

ステップ 8 デバイス セレクタでデバイスを選択して Auto Update Server または Configuration Engine によって管理されているデバイスを追加した場合は、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択します。[Auto Update] または [Configuration Engine] 設定で、デバイスで使用するサーバを選択します。サーバがリストにない場合は追加できます。詳細については、 Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）を参照してください。

[Device Information] ページ - [Configuration File]

構成ファイルからデバイスを追加する場合は、New Device ウィザードの [デバイス情報（Device Information）] ページを使用して、構成ファイルを選択し、ポリシー検出オプションを指定します。

ナビゲーション パス

New Device ウィザードを起動するには、デバイス ビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイス セレクタの [追加（Add）] ボタンをクリックします。

関連項目

- デバイス ビューについて （87 ページ）
- 設定ファイルからのデバイスの追加 （112 ページ）
- [Device Groups] ページ （148 ページ）
- ポリシーの検出 （223 ページ）
- [Discovery Status] ダイアログボックス （238 ページ）

フィールド リファレンス

表 *18* : 設定ファイルからデバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ

要素	説明
Device Type selector	デバイスをデバイス タイプ別およびデバイス ファミリ別に整理します。新しいデバイスのデバイス タイプを選択します。追加する設定ファイルに適切なデバイス タイプを選択する必要があります。
System Object ID	デバイス タイプ セレクタから選択したデバイス タイプのシステム オブジェクト ID。デバイスの正しい ID を選択します。
コンフィギュレーション ファイル	インベントリに追加するデバイスの設定ファイル。複数の設定ファイルを指定できますが、そのいずれもデバイス タイプが同じものである必要があります。ファイル名はカンマで区切ります。 複数のセキュリティ コンテキストを持つ ASA、PIX、および FWSM デバイスでは、各セキュリティ コンテキストおよびシステム実行スペース（システム コンテキスト）に対して別々の設定ファイルが存在することを覚えておいてください。システム実行スペースの設定ファイルを選択して、基本デバイスを追加します。 [参照（Browse）] をクリックして、Security Manager サーバーからファイルを選択するか、または手動で（フルパスの）ファイル名を入力します。ファイルの選択の詳細については、 Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）を参照してください。
オプション	デバイスで使用可能な追加オプション。デバイスで IPS 機能を使用できる場合は、[IPS] を選択します。

要素	説明
フェールオーバーのライセンスサポート （ASA 5505、5510 専用）	オプションのフェールオーバーライセンスがデバイスにインストールされているかどうかを示します。オプションは、ASA 5505 および 5510 デバイスのみでアクティブになります。Security Manager は、このオプションが選択されている場合のみ、フェールオーバーポリシーをデバイスに展開します。 **ヒント** デバイスからポリシーを検出した場合、Security Manager はライセンス ステータスを判定し、このオプションを適切に設定します。
デバイス設定の検出	
検出	検出してインベントリに追加する要素のタイプ。次のオプションがあります。 • [Policies and Inventory]：ポリシー、インターフェイス、およびサービスモジュール（該当する場合）を検出します。これがデフォルトであり、推奨オプションです。 ポリシーの検出が開始されると、設定ファイルが分析され、設定されているサービスとプラットフォームのポリシーがインポートされます。インベントリの検出が開始されると、設定ファイルに定義されているインターフェイスが分析され、インターフェイス リストがインポートされます。 このオプションを選択すると、下のチェックボックスがアクティブになり、それらのチェックボックスを使用して、検出されるポリシーのタイプを制御できます。 （注） 検出中に非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。同じ ACL を展開すると、その ACL は Security Manager によって削除されます。 • [Inventory Only]：インターフェイスとサービス モジュール（該当する場合）を検出します。 • [No Discovery]：すべての検出がスキップされます。デバイスのポリシー、インターフェイス、またはサービスモジュール情報はデバイスインベントリに追加されません。
プラットフォーム設定	プラットフォーム固有のポリシー ドメインとも呼ばれるプラットフォーム設定を検出するかどうかを指定します。プラットフォーム固有のポリシー ドメインは、ファイアウォールデバイス上にあります。これらのドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。詳細については、サービスポリシーとプラットフォーム固有のポリシー （211 ページ）を参照してください。

要素	説明
ファイアウォール ポリシー	ファイアウォール サービスとも呼ばれるファイアウォール ポリシーを検出するかどうかを指定します。ファイアウォールサービスには、アクセル ルール、インスペクション ルール、AAA ルール、Web フィルタ ルール、トランスペアレント ルールなどのポリシーが含まれます。詳細については、ファイアウォール サービスの概要 （755 ページ）を参照してください。
IPS ポリシー	シグニチャや仮想センサーなどの IPS ポリシーを検出するかどうかを指定します。詳細については、IPS 設定の概要 （2088 ページ）またはCisco IOS IPS 設定の概要 （2318 ページ）を参照してください。
RA VPN ポリシー	IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモート アクセス VPN ポリシーを検出するかどうかを指定します。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモート アクセス VPN の管理の基礎 （1655 ページ）を参照してください。

手動定義によるデバイスの追加

ネットワークでデバイスがまだアクティブではない場合は、そのデバイスを Security Manager に追加し、デバイスの設定を事前プロビジョニングできます。一般に、ネットワークに存在するデバイスは手動定義しないでください。他のいずれかの手法でデバイスを追加するほうが、はるかに簡単だからです。

はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス グループの使用 （164 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

ステップ 1 デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

ステップ 2 [方式を選択（Choose Method）] ページで、[新規デバイスの追加（Add New Device）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます。

ステップ 3 [Device Information] ページで、少なくとも次のフィールドに値を入力します。すべてのフィールドの詳細については、[Device Information] ページ - [New Device] （118 ページ）を参照してください。

- ページの左側にあるデバイス タイプ セレクタからデバイス タイプを選択し、デバイス タイプ セレクタの一番下にあるシステム オブジェクト ID を選択します。
- [IP Type] フィールドでは、デバイスがスタティック アドレス（IP アドレスはデバイスに定義されます）を使用するのか、ダイナミック アドレス（IP アドレスは DHCP サーバから提供されます）を使用するのかを選択します。
- スタティック アドレスを使用するデバイスの場合、DNS ホスト名とドメイン名、または IP アドレスのいずれか（あるいはその両方）を入力します。
- 表示名を入力します。この名前は Security Manager のデバイス セレクタに表示されます。
- 正しいオペレーティング システムおよびバージョンが選択されていることを確認します。
- サーバを使用してデバイスの設定を管理する場合は、デバイスに対するダイナミックなアドレス指定が必要であり、そのためデバイスを管理する Auto Update Server または Configuration Engine を選択し、サーバがデバイスに使用するデバイス アイデンティティ文字列を入力します。サーバーが表示されていない場合は、[サーバーの追加（Add Server）] を選択し、そのサーバーをインベントリに追加します。サーバーの追加の詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）を参照してください。

デバイス情報を入力したら、[次へ（Next）] をクリックして [デバイスのログイン情報（Device Credentials）] ページに進みます。

ステップ 4 （任意）[Device Credentials] ページで、デバイスへのログインに必要なユーザ名およびパスワードを入力します。一般に、プライマリ デバイス クレデンシャルを入力する必要があります。これは、従来のユーザ EXEC モードと特権 EXEC モードのパスワードです。クレデンシャルを入力しない場合は、あとで [Device Properties] ページでクレデンシャルを追加できます。

クレデンシャルの各種タイプについては、[Device Credentials] ページ （143 ページ）を参照してください。

[次へ（Next）] をクリックします。

ステップ 5 （任意）[Device Grouping] ページで、デバイスを所属させるグループを選択します。[Device Groups] ページ （148 ページ）を参照してください。

ステップ 6 [終了（Finish）] をクリックします。デバイスがインベントリに追加されます。

ヒント PIX、ASA、FWSM のいずれかのデバイスを追加している場合は、デバイスの出荷時のデフォルト設定とそのセキュリティ コンテキストを検出する必要があります。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

[Device Information] ページ - [New Device]

（ネットワークにまだ存在しない）新規デバイスを追加する場合は、新規デバイス（New Device）ウィザードの [デバイス情報（Device Information）] ページを使用して、デバイスの識別情報を指定します。

ナビゲーション パス

New Device ウィザードを起動するには、デバイスビューで **[ファイル（File）] > [新規デバイス（New Device）]** を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。

関連項目

- デバイス ビューについて （87 ページ）
- 手動定義によるデバイスの追加 （116 ページ）
- [Device Credentials] ページ （143 ページ）
- [Device Groups] ページ （148 ページ）

フィールド リファレンス

表 *19* : 新規デバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ

要素	説明
デバイスタイプ（Device Type）	
Device Type selector	デバイスをデバイス タイプ別およびデバイス ファミリ別に整理します。新しいデバイスのデバイス タイプを選択します。
System Object ID	デバイス タイプ セレクタから選択したデバイス タイプのシステム オブジェクト ID。デバイスの正しい ID を選択します。
ID（Identity）	
IP タイプ（IP Type）	デバイスの IP アドレスをスタティックにする（デバイスで定義する）か、またはダイナミックにする（DHCP サーバから取得する）かを指定します。選択した IP タイプによって、表示されるフィールドが異なります。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。IPv6 アドレスは 128 ビットの一意のアドレスです。IPv6 アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは IPv6 アドレスではサポートされません。

要素	説明
ホストネーム （スタティック IP 専用）	デバイスの DNS ホスト名。IP アドレスが不明な場合に、DNS ホスト名を入力します。 最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、およびハイフン（-）です。 （注） DNS ホスト名と IP アドレスのどちらか一方、または両方を入力する必要があります。 2 つのデバイスに同じ DNS ホスト名とドメイン名の組み合わせを使用することはできません。
ドメイン名 （スタティック IP 専用）	デバイスの DNS ドメイン名。 最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、ピリオド（.）、およびハイフン（-）です。
IPアドレス （スタティック IP 専用）	デバイスの管理 IP アドレス。IP アドレスは、10.64.3.8 というように、ドット付きの 4 つの数字列でなければなりません。 （注） IP アドレスと DNS ホスト名のどちらか一方、または両方を入力する必要があります。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。デバイスがデュアルスタックで設定されている場合、Security Manager は、Security Manager に追加されたデバイスの IP アドレスに基づいてデバイスと通信します。IPv6 アドレスは 128 ビットの一意のアドレスです。
表示名	Security Manager のデバイス セレクタに表示する名前。ホスト名または IP アドレスを入力した場合は、そのホスト名または IP アドレスがこのフィールドに自動的に入力されますが、変更することもできます。 最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。 （注） 2 つのデバイスに同じ表示名を設定することはできません。
オペレーティング システム	

要素	説明
OS タイプ	オペレーティング システムのタイプ。デバイス タイプに基づいて、OS タイプが自動的に選択されます。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。この機能は、オペレーティングシステムのタイプが ASA または FWSM であるデバイスでのみ使用できます。
イメージ名（Image Name）	デバイスで実行されるイメージの名前。
ターゲット OS バージョン	設定を適用するターゲット OS バージョン。この選択によって、Security Manager が設定ファイルを生成するときに使用されるコマンドのタイプが決まります。
オプション	デバイスで使用可能な追加オプション。デバイスで IPS 機能を使用できる場合は、[IPS] を選択します。
コンテキスト	デバイスで 1 つのセキュリティ コンテキストをホストするか（[Single]）、または複数のセキュリティ コンテキストをホストするか（[Multi]）を指定します。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 の場合だけです。
動作モード（Operational Mode）	デバイスの動作モード。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 以降の場合だけです。使用可能なオプションは [トランスペアレント（Transparent）] または [ルータ（Router）] です。[コンテキスト（Contexts）] で [マルチ（Multi）] を選択する場合、このモードのデフォルト設定は [混合（Mixed）] になります。[混合（Mixed）] は、ASA 9.0 以降および FWSM 3.1 以降のデバイスと ASA-SM にのみ適用されます。 （注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェア サポートは提供されません。

要素	説明
FXOS モード	デバイスが動作している FXOS モード。使用可能なオプションは [プラットフォーム（Platform）] および [アプライアンス（Appliance）] です。[アプライアンス（Appliance）] モードを選択する場合は、CLI、オンボックスデバイス（ASDM など）、またはマルチデバイスマネージャ（Cisco Security Manager など）のいずれかから、すべてのエンドユーザー設定を実行できます。[プラットフォーム（Platform）] モードオプションは、Firepower 2000 シリーズアプライアンスに対してのみ表示されます。 （注） バージョン 4.20 以降、Security Manager は、Firepower 2000 および 1000 シリーズアプライアンスに対して [アプライアンス（Appliance）] モードをサポートしています。
[Auto Update] または [Configuration Engine] このグループは、選択するデバイス タイプに応じて名前が異なります。 • [Auto Update]：PIX ファイアウォールおよび ASA デバイスの場合。 • [Configuration Engine]：Cisco IOS ルータの場合。 これらのフィールドは、デバイスを管理するサーバ（ある場合）を識別するために使用します。ダイナミック IP アドレスを持つデバイスには、サーバが必須です。Catalyst 6500/7600 デバイスまたは FWSM デバイスのサーバは定義できません。 （注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。	
サーバー（Server）	デバイスを管理する Auto Update Server または Configuration Engine。 サーバーをリストに追加するには、[サーバーの追加（Add Server）] を選択します。[サーバーのプロパティ（Server Properties）] ダイアログボックスが開きます（[Server Properties] ダイアログボックス （132 ページ）を参照）。[サーバーの編集（Edit Server）] を選択して [使用可能なサーバー（Available Servers）] ダイアログボックスを開き、サーバーのプロパティを編集することもできます（[Available Servers] ダイアログボックス （134 ページ）を参照）。 このサーバ リストの管理の詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）を参照してください。
デバイスアイデンティティ	Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列。
その他のフィールド	

要素	説明
Cisco Security Manager での管理	Security Manager でデバイスを管理するかどうかを指定します。このチェックボックスは、デフォルトでオンになっています。 追加しようとしているデバイスの唯一の機能が VPN エンドポイントとして機能することである場合は、このチェックボックスをオフにします。Security Manager は設定を管理せず、このデバイスの設定をアップロードまたはダウンロードしません。詳細については、管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）を参照してください。
管理対象外のデバイスのセキュリティ コンテキスト	親（PIX ファイアウォール デバイス、ASA デバイス、または FWSM デバイス）が Security Manager によって管理されていないセキュリティ コンテキストを管理するかどうかを指定します。 このフィールドがアクティブになるのは、デバイス セレクタで選択したデバイスが PIX ファイアウォール、ASA、FWSM などのファイアウォール デバイスで、かつそのファイアウォール デバイスがセキュリティ コンテキストをサポートしている場合だけです。 1 つの PIX ファイアウォール、ASA、または FWSM のパーティションを、セキュリティ コンテキストとも呼ばれる複数のセキュリティ ファイアウォールに分けることができます。各コンテキストは、それぞれに独自の設定およびポリシーを持つ独立したシステムです。このようなスタンドアロンのコンテキストは、親デバイスが管理対象外であっても、Security Manager で管理できます。詳細については、ファイアウォール デバイスでのセキュリティ コンテキストの設定 （2979 ページ）を参照してください。 （注） このチェックボックスをオンにした場合、セキュリティ モジュールに使用可能なターゲット OS バージョンが [Target OS Version] フィールドに表示されます。
フェールオーバーのライセンスサポート （ASA 5505、5510 専用）	オプションのフェールオーバー ライセンスがデバイスにインストールされているかどうかを示します。オプションは、ASA 5505 および 5510 デバイスのみでアクティブになります。Security Manager は、このオプションが選択されている場合のみ、フェールオーバー ポリシーをデバイスに展開します。 ヒント デバイスからポリシーを検出した場合、Security Manager はライセンス ステータスを判定し、このオプションを適切に設定します。

インベントリ ファイルからのデバイスの追加

Comma-Separated Value（CSV; カンマ区切り値）形式のインベントリ ファイルからデバイスを追加できます。たとえば、CiscoWorks Common Services Device Credential Repository（DCR）ま

たは別の Security Manager サーバからエクスポートしたインベントリ ファイルや、Cisco Security Monitoring, Analysis and Response System（CS-MARS）で使用したシード ファイルなどです。インベントリ ファイル形式の詳細については、インベントリのインポートまたはエクスポートでサポートされている CSV 形式 （609 ページ）を参照してください。

ヒント

- この手順では、デバイスのインポートに CSV ファイルを使用する方法について説明します。インベントリだけではなく、デバイスに割り当てられたポリシーおよびポリシー オブジェクトも含む .dev ファイルがある場合は、この手順を使用できません。代わりに、**[ファイル（File）] > [インポート（Import）]** コマンドを使用して、ポリシーまたはデバイスのインポート （615 ページ）の指示に従います。
- インベントリ ファイルを手作業で構築する場合、最も簡単な方法は Security Manager インベントリを目的の形式でエクスポートし、そのファイルを目的のインベントリ ファイルの基礎として使用することです。
- インポートするデバイスは、デバイス インベントリにすでに存在するデバイスと重複していてはいけません。たとえば、デバイスを再インポートして、インベントリのデバイス情報を更新することはできません。

はじめる前に

この手順を開始する前に、次の準備が完了していることを確認してください。

- Security Manager で管理されるデバイスを準備します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- 認証に ACS を使用する場合は、ACS でデバイスを定義します。『Installation Guide for Cisco Security Manager』を参照してください。
- 使用するインベントリ ファイルを Security Manager サーバに配置します。クライアント システム上のファイルからデバイスをインポートすることはできません。
- デバイスのタイプに非標準の通信プロトコルを使用している場合は、グローバル デバイス通信プロパティを更新して正しいプロトコルを指定します。詳細については、[Device Communication] ページ （668 ページ）を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス グループの使用 （164 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

ステップ 1 デバイス ビューで **[ファイル（File）] > [新規デバイス（New Device）]** を選択するか、デバイス セレクタの [追加（Add）] ボタンをクリックします。[Choose Method] ページに New Device ウィザードが開きます。

ステップ 2 [方式を選択（Choose Method）] ページで、[ファイルから追加（Add from File）] を選択し、[次へ（Next）] をクリックして [デバイス情報（Device Information）] ページを開きます（[Device Information] ページ - [Add Device from File] （125 ページ）を参照）。

ステップ 3 [参照（Browse）] をクリックし、インポートするデバイスが含まれているインベントリファイルを選択します。ファイルの形式を示す正しいファイル タイプを選択していることを確認します。

Security Manager は、インベントリ ファイルの内容を評価し、インポート テーブルにデバイス リストを表示します。ステータスが [Ready to Import] であるすべてのデバイスが自動的に選択されます。このリストから、選択されていないデバイスがなぜインポートできないかがわかります。インポートしないデバイスは、選択を解除できます。

デバイスに関する詳細な情報を参照するには、インポート テーブルでそのデバイスを選択します。詳細が一番下のペインに表示されます。デバイスごとに異なる検出オプションまたは転送設定を選択できます。

ヒント Security Manager 形式のインベントリ ファイルを選択した場合は、ポリシー検出を実行せずにデバイスをインポートすることもできます。これにより、ネットワークで現在アクティブでないデバイスを追加できるようになります。デバイスでポリシー検出を実行する場合は、デバイスを選択し、一番下のパネルで [デバイスディスカバリの実行（Perform Device Discovery）] を選択し、目的の検出オプションを選択します。個々のデバイスではなくフォルダを選択して、そのフォルダ内のすべてのデバイスのポリシー検出設定を選択できます。他の CSV 形式では、インポート時にポリシー検出を実行する必要があります。

リストを分析し、検出設定および転送設定に必要な変更を加えたら、[次へ（Next）] をクリックしてグループを選択する任意の手順を続けるか、または [終了（Finish）] をクリックしてウィザードを完了します。いずれにしても、Security Manager 形式で CSV ファイルを使用し、かつ検出を実行しないようにしている場合を除き、Security Manager は各デバイスにログインし、選択された検出を実行しようとします。他の形式の場合、Security Manager はデバイスにログインしてインベントリにそのデバイスを追加できる必要があります。ステータスが [Discovery Status] ダイアログボックスに表示されます（[Discovery Status] ダイアログボックス （238 ページ）を参照）。

ヒント デバイスの追加中にポリシーを検出している場合は、提示されているメッセージをよくお読みください。これらのメッセージには、次に実行する手順に関する重要な推奨事項が含まれている場合があります。Security Manager が設定の所有権を引き継ぐことができるように、検出した設定をファイルにすぐに展開することを推奨します。展開方法の詳細については、展開方法について（490 ページ）を参照してください。

ステップ 4 （任意）[Device Grouping] ページで、インポートしたデバイスの追加先となるデバイス グループを選択します（[Device Groups] ページ （148 ページ）を参照）。

[終了（Finish）] をクリックします。

ステップ 5 モジュールが含まれているデバイスを追加し、デバイス検出を実行し、さらに Security Manager がそのタイプのデバイスでモジュールの検出をサポートしている場合、デバイスシャーシの検出が完了したときに通知され、デバイスのモジュールを検出するかどうかを確認されます。[はい（Yes）] をクリックすると、次の情報の入力を要求されます。

- Catalyst 6500 サービス モジュール：[Service Module Credentials] ダイアログボックスが開き、シャーシに含まれているモジュールに基づいて次の情報の入力が要求されます。詳細については、[Service Module Credentials] ダイアログボックス （108 ページ）を参照してください。

- FWSM：管理IPアドレス（推奨）、ユーザ名とパスワード、および実行する検出のタイプ。FWSMがフェールオーバーペアの 2 番めのデバイスである場合は、フェールオーバーモジュールの [モジュールを検出しない（Do Not Discover Module）] を選択します。（Security Manager は、プライマリまたはセカンダリのどちらのフェールオーバーサービスモジュールが追加されたにかかわらず、常にアクティブな管理コンテキストを管理します）。
- IDSM：ユーザ名とパスワード、および実行する検出のタイプ。
- ASA-SM：Catalyst 6500 で、シャーシ経由での ASA サービス モジュールの検出はサポートされません。ASA-SM は、ASA-SM の管理 IP アドレスを使用して直接追加する必要があります。

- IPS ルータ モジュール：実行する検出のタイプ、管理 IP アドレス、ユーザ名とパスワード、およびその他の SSL 接続情報。詳細については、[IPS Module Discovery] ダイアログボックス （110 ページ）を参照してください。

Security Manager で管理しないモジュールの検出をスキップできます。

[OK] をクリック[Discovery Status] ダイアログボックスに戻り、サービス モジュールの検出の経過を表示できます。

[Device Information] ページ - [Add Device from File]

インベントリファイルからデバイスを追加するには、New Device ウィザードの [デバイス情報（Device Information）] ページを使用して、インベントリファイルを選択し、ポリシー検出オプションを指定します。インベントリ ファイルは、Security Manager サーバに存在する必要があります。クライアント システム上にあるインベントリ ファイルは使用できません。

インベントリ ファイルに使用できる形式については、インベントリのインポートまたはエクスポートでサポートされている CSV 形式 （609 ページ）で説明します。一般に、インベントリ ファイルは、別の Security Manager サーバまたは CiscoWorks Common Services サーバからエクスポートされたものであるか、または Cisco Security Monitoring, Analysis and Response System（CS-MARS）サーバのインベントリを読み込むときに使用されるシードファイルとなります。

.dev ファイルを使用してデバイスをインポートしようとしている場合は、このページの代わりに [File] > [Import] コマンドを使用する必要があります。詳細については、ポリシーまたはデバイスのインポート （615 ページ）を参照してください。

ヒント モジュールが含まれているデバイス、たとえば FWSM がある Catalyst スイッチを追加している場合は、[完了（Finish）] をクリックするとモジュール検出情報の入力を求められます。

ナビゲーション パス

New Device ウィザードを起動するには、デバイスビューで [ファイル（File）] > [新規デバイス（New Device）] を選択するか、デバイスセレクタの [追加（Add）] ボタンをクリックします。

関連項目

- デバイス ビューについて （87 ページ）
- インベントリ ファイルからのデバイスの追加 （122 ページ）
- [Device Groups] ページ （148 ページ）
- ポリシーの検出 （223 ページ）
- [Device Communication] ページ （668 ページ）
- [Discovery Status] ダイアログボックス （238 ページ）

フィールド リファレンス

表 *20:* インベントリ ファイルからデバイスを追加する場合に使用する *New Device* ウィザードの *[Device Information]* ページ

要素	説明
デバイスのインポート元	インポートするデバイスが含まれているインベントリ ファイル。[参照（Browse）] をクリックして、Security Manager サーバー上のファイルを選択します。 ファイルを選択するときは、Security Manager が Comma-Separated Value（CSV; カンマ区切り値）ファイルを正しく評価できるように、正しいファイル タイプも選択する必要があります。
デバイスインポートテーブル ファイルを選択すると、Security Manager はその内容を評価し、ファイルに定義されているデバイス リストをページ上部のペインのテーブルに表示します。Security Manager は、ステータスが [Ready to Import] であるすべてのデバイスを自動的に選択します。一般には、デバイス インベントリにまだ存在しないデバイスとなります。 テーブルには、次のカラムがあります。	
インポート	デバイスをインベントリに追加するには、このチェックボックスをオンにします。フォルダを選択または選択解除して、そのフォルダ内のすべてのデバイスを選択または選択解除できます。
表示名	Security Manager のデバイス セレクタに表示する名前。
ホスト名	デバイスに定義されているホスト名。
トランスポート（Transport）	デバイスへの接続に使用するトランスポート プロトコル。

要素	説明
ステータス	Security Manager でデバイスをインポートできるかどうかを指定します。デバイスは、ステータスが [Ready to Import] である場合にだけインポートできます。デバイスのステータスの詳細については、デバイスを選択し、ページ右下隅の [ステータス（Status）] テキストボックスでステータス情報を展開してお読みください。
デバイスタイプ	デバイスのタイプ。
[詳細（Details）] ペイン デバイスインポートテーブルの下に、テーブルで選択されているデバイスの詳細を表示するペインがあります。アイデンティティ情報には、テーブルのフィールドがそのまま表示されます。[Status] テキストボックスには、インポートステータスの詳しい説明が表示されます。 [Discover Device Settings] グループおよび [Transport] グループでは、Security Manager でのデバイスのインポート方法を指定できます。デバイスではなくフォルダを選択した場合、選択した設定はフォルダ内のすべてのデバイスに適用されます。設定については、次に説明します。	
デバイス設定の検出	
デバイスディスカバリの実行	デバイスから直接ポリシーを検出するかどうかを指定します。 • インベントリ ファイルが Security Manager 形式である場合は、[Perform Device Discovery] を選択して、インベントリおよびポリシーを検出する必要があります（それ以外の場合、デバイスは評価されずに追加されます）。オフライン デバイスまたはスタンバイ デバイスを追加している場合は、このオプションをオフにしておいても、容易にデバイスをインベントリに追加できます。 • 他のすべてのインベントリ ファイル タイプでは、デバイス検出が必要です。
システムコンテキスト	選択したデバイスがマルチ コンテキスト モードで動作するデバイス上のシステム実行スペースであるかどうか（つまり、複数のセキュリティ コンテキストがデバイスに定義されているかどうか）を指定します。デバイスがシステム実行スペースである場合は、検出が正しく完了するようにこのオプションを選択する必要があります。

要素	説明
検出	検出してインベントリに追加する要素のタイプ。次のオプションがあります。 • [Policies and Inventory]：ポリシー、インターフェイス、およびサービス モジュール（該当する場合）を検出します。これがデフォルトであり、推奨オプションです。 ポリシーの検出が開始されると、デバイス上の設定が分析され、設定されているサービスとプラットフォームのポリシーがインポートされます。インベントリの検出が開始されると、デバイス上のインターフェイスが分析され、インターフェイス リストがインポートされます。デバイスが複合デバイスの場合は、デバイス内のすべてのサービス モジュールが検出され、インポートされます。 このオプションを選択すると、下のチェックボックスがアクティブになり、それらのチェックボックスを使用して、検出されるポリシーのタイプを制御できます。 （注） 検出中に非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。同じ ACL を展開すると、その ACL は Security Manager によって削除されます。 • [Inventory Only]：インターフェイスとサービス モジュール（該当する場合）を検出します。
プラットフォーム設定	プラットフォーム固有のポリシー ドメインとも呼ばれるプラットフォーム設定を検出するかどうかを指定します。プラットフォーム固有のポリシー ドメインは、ファイアウォール デバイスと Cisco IOS ルータ上にあります。これらのドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。詳細については、サービスポリシーとプラットフォーム固有のポリシー （211 ページ）を参照してください。
ファイアウォール ポリシー	ファイアウォール サービスとも呼ばれるファイアウォール ポリシーを検出するかどうかを指定します。ファイアウォール サービスには、アクセル ルール、インスペクション ルール、AAA ルール、Web フィルタ ルール、トランスペアレント ルールなどのポリシーが含まれます。詳細については、ファイアウォール サービスの概要 （755 ページ）を参照してください。
IPS ポリシー	シグニチャや仮想センサーなどの IPS ポリシーを検出するかどうかを指定します。詳細については、IPS 設定の概要 （2088 ページ）またはCisco IOS IPS 設定の概要 （2318 ページ）を参照してください。

要素	説明
RA VPN ポリシー	IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモート アクセス VPN ポリシーを検出するかどうかを指定します。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモート アクセス VPN の管理の基礎（1655 ページ）を参照してください。
セキュリティコンテキストのポリシーの検出	マルチ コンテキスト モードで動作するデバイスの場合、複数のセキュリティ コンテキストが定義されています。ここには、それらのセキュリティ コンテキストを検出するかどうかを指定します。
トランスポート 転送設定によって、Security Manager がデバイスへの問い合わせに使用する方法が決まります。各デバイス タイプにはデフォルトの方法がありますが、任意の転送方法を選択できます。デバイスは、選択した方法に応答するように設定する必要があります。デバイス検出を実行していない場合は、デバイスへの問い合わせが行われません。	
プロトコル	デバイスに接続するときに Security Manager で使用するプロトコル。
サーバー（Server）	Auto Update Server（AUS）または Configuration Engine サーバを使用するデバイスの場合、デバイスが設定更新を取得する際に使用するそのサーバの名前を指定します。このようなサーバを使用するデバイスをインポートするには、サーバが Security Manager にすでに定義されているか、またはインポート リストからサーバを選択する必要があります。
デバイスアイデンティティ	サーバを使用するデバイスの場合、Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列を指定します。

デバイス インベントリの使用

次の項では、デバイス インベントリの管理に関連するタスクについて説明します。

- Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）
- インターフェイス モジュールの追加または変更 （135 ページ）
- デバイス プロパティの表示または変更 （136 ページ）
- 重要なデバイス プロパティの変更 （155 ページ）
- デバイスに含まれている要素の表示 （160 ページ）

- デバイスの複製 （160 ページ）
- Security Manager インベントリからのデバイスの削除 （162 ページ）

これらの項に加え、関連する次の項を参照してください。

- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイス インベントリのエクスポート （605 ページ）
- ポリシーまたはデバイスのインポート （615 ページ）

Auto Update Server または Configuration Engine の追加、編集、または削除

他のサーバを使用して設定を管理するデバイスを Security Manager で管理する場合（たとえば、DHCP サーバからダイナミック IP アドレスが提供されるデバイス。デバイスをリブートすると前回と同じアドレスが提供されるとはかぎりません）、Security Manager でその使用するサーバを識別する必要があります。次に、使用できるサーバを示します。

- Auto Update Server（AUS）。自動更新機能を使用する PIX ファイアウォールおよび ASA デバイス上のデバイス設定ファイルをアップグレードする場合に使用されます。
- Cisco Configuration Engine。Configuration Engine 機能を使用する Cisco IOS ルータ、ASA デバイス、および PIX ファイアウォール上のデバイス設定ファイルをアップグレードする場合に使用されます。

Security Manager は、DHCP を使用してインターフェイス アドレスを取得するデバイスとの直接通信を開始できません。そのデバイスの IP アドレスが事前にはわからないためです。また、管理システムが変更を加える必要があるときに、デバイスが動作中でなかったり、ファイアウォールおよび NAT 境界の背後に配置されていたりする場合があります。このようなデバイスは、Auto Update Server または Configuration Engine に接続して、デバイス情報を取得します。

デバイスを手動で追加したり、デバイス プロパティを表示したりするときに、AUS および Configuration Engine サーバをデバイス インベントリに追加できます。このようなサーバのいずれかを使用するデバイスのプロパティを追加または表示する必要はありません。適切なフィールドに移動して、このようなサーバを追加、編集、または削除するためのコントロールにアクセスします。

また、CiscoWorks Common Services Device Credential Repository（DCR）または別の Security Manager サーバからエクスポートされたインベントリ ファイルからこれらのサーバをインポートする場合は、該当するサーバを追加することもできます。サーバをインポートする場合は、ここで説明する手順をスキップします。デバイスのインポートの詳細については、インベントリ ファイルからのデバイスの追加 （122 ページ）を参照してください。

はじめる前に

デバイスの追加に関係なく、Security Manager インベントリに AUS および Configuration Engine サーバーのリストを読み込む場合、最善の方法は New Device ウィザードを使用し、追加方法

として [新規デバイスの追加（Add New Device）] を選択することです。この方法については、次の手順で説明します。

また、デバイスセレクタでデバイスを選択し、[ツール（Tools）]>[デバイスプロパティ（Device Properties）] をクリックして、サーバーを追加または編集することもできます。デバイスプロパティのコンテンツテーブルで [全般（General）] をクリックします。[Server] フィールドは、[Auto Update] グループまたは [Configuration Engine] グループのいずれかにあります。グループ名で識別されるサーバのタイプだけを追加または編集できます。

ヒント Security Manager では、Configuration Engine を追加するときに Configuration Engine で実行されているソフトウェア バージョンを特定できません。ただし、Security Manager は、設定を Configuration のすべてのバージョンに正しく展開できるとはかぎりません。Configuration Engine がサポートされているリリースを実行していることを確認してください（サポートされている Configuration Engine バージョンについては、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html にあるこの製品バージョンのリリースノートを参照してください）。

関連項目

- ネットワークからのデバイスの追加 （100 ページ）
- 手動定義によるデバイスの追加 （116 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

ステップ 1 デバイス インベントリで AUS エントリまたは Configuration Engine エントリを識別および管理できるフィールドの場所を特定します。

a) [ファイル（File）]>[新規デバイス（New Device）] を選択して [新規デバイス（New Device）] ウィザードを開き、[方法の選択（Choose Method）] ページで [新規デバイスの追加（Add New Device）] を選択し、[次へ（Next）] をクリックします。

b) [Device Information] ページで、デバイス タイプ セレクタから ASA デバイスを選択します。たとえば、Cisco ASA-5580 Adaptive Security Appliance などです。[自動更新（Auto Update）] グループの [サーバー（Server）] フィールドには、ドロップダウンリストに [サーバーの追加（Add Server）] が含まれています。すでに定義されたサーバーがある場合は、[サーバーの編集（Edit Server）] も含まれています。このようなエントリに特定のサーバ タイプ（たとえば、Add Auto Update Server や Add Configuration Engine）がある場合、追加、編集、または削除の対象がそのタイプのサーバに制限されます（この場合、適切なサーバ タイプを探すには、他のタイプのデバイスを選択します）。

ステップ 2 新規 AUS または Configuration Engine サーバーを追加するには、[サーバー（Server）] ドロップダウンリストから [サーバーの追加（Add Server）] を選択して [サーバープロパティ（Server Properties）] ダイアログボックスを開きます（[Server Properties] ダイアログボックス （132 ページ）を参照）。

ステップ 3 サーバーを編集するには、[サーバー（Server）] ドロップダウンリストから [サーバーの編集（Edit Server）] を選択して [利用可能なサーバー（Available Servers）] ダイアログボックスを開きます（[Available Servers] ダイアログボックス （134 ページ）を参照）。その後、サーバーを選択し、[編集（Edit）] をクリックして [サーバープロパティ（Server Properties）] ダイアログボックスを開き、変更を加えることができます。

[Available Servers] ダイアログボックスでは、次の操作も実行できます。

- [作成（Create）] をクリックして、サーバーを追加します。
- サーバーを選択し、[削除（Delete）] をクリックして、インベントリからそのサーバーを削除します。削除の確認が求められます。サーバがインベントリのデバイスによって使用されていないことを確認します。

[Server Properties] ダイアログボックス

[Server Properties] ダイアログボックスは、Auto Update Server または Configuration Engine のプロパティを指定する場合に使用します。

このダイアログボックスでは、その開く方法に応じてタイトルにサーバのタイプを指定できます（たとえば、Auto Update Server Properties や Configuration Engine Properties）。ダイアログボックスは基本的には同じです。

ヒント Security Manager では、Configuration Engine を追加するときに Configuration Engine で実行されているソフトウェア バージョンを特定できません。ただし、Security Manager は、設定を Configuration のすべてのバージョンに正しく展開できるとはかぎりません。Configuration Engine がサポートされているリリースを実行していることを確認してください（サポートされている Configuration Engine バージョンについては、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html にあるこの製品バージョンのリリースノートを参照してください）。

ナビゲーション パス

このダイアログボックスを開くには、次のいずれかを実行します。

- デバイスを手動で追加するときには、新規デバイス（New Device）ウィザードの [デバイス情報（Device Information）] ページで、[Auto Update Server] グループまたは [Configuration Engine] グループの [サーバー（Server）] フィールドから [サーバーの追加...（Add Server...）] を選択します。選択肢は、[Add Auto Update Server] または [Add Configuration Engine] と表示される場合もあります。
- [デバイスのプロパティ（Device Properties）] - [全般（General）] ページで、[Auto Update Server] グループまたは [Configuration Engine] グループの [サーバー（Server）] フィールドから [サーバーの追加...（Add Server...）] を選択します。選択肢は、[Add Auto Update Server] または [Add Configuration Engine] と表示される場合もあります。
- [使用可能なサーバー（Available Servers）] ダイアログボックスで、[作成（Create）] をクリックするか、サーバーを選択し、[編集（Edit）] をクリックします（[Available Servers] ダイアログボックス （134 ページ）を参照）。

関連項目

- [Available Servers] ダイアログボックス （134 ページ）
- [Device Information] ページ - [New Device] （118 ページ）
- [Device Information] ページ - [Add Device from Network] （103 ページ）
- Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

フィールド リファレンス

表 *21 : [Server Properties]* ダイアログボックス

要素	説明
タイプ	定義しているサーバのタイプ。Auto Update Server または Configuration Engine。 このフィールドが表示されるのは、サーバを追加している場合だけです。既存のサーバのタイプは変更できません。 新規サーバの場合、ダイアログボックスのタイトルに追加対象のサーバのタイプが指定されているときにも、このフィールドは表示されません。
サーバー名（Server Name）	サーバの DNS ホスト名。
ドメイン名	サーバの DNS ドメイン名。
[IPアドレス（IP Address）]	サーバの IP アドレス。
表示名	サーバの Security Manager に表示する名前。
ユーザー名	サーバにログインするためのユーザ名。
パスワード	サーバにアクセスするためのパスワード。[Confirm] フィールドに、パスワードを再入力します。
[ポート（Port）]	Auto Update Server または Configuration Engine によって管理されたデバイスがサーバと通信するときに使用するポート番号。通常、ポート番号は 443 です。

要素	説明
URN	このフィールドは、Auto Update Server の場合にだけ表示されます。 Auto Update Server のユニフォーム リソース名。URN は、インターネット上のリソースを識別する名前です。URN は URL の一部で、/autoupdate/AutoUpdateServlet などとなります。完全な URL は、https://: *server ip* :443/autoupdate/AutoUpdateServle のようになります。 引数の説明 • *server ip* は、Auto Update Server の IP アドレスです。 • 443 は、Auto Update Server のポート番号です。 • /autoupdate/AutoUpdateServlet は、Auto Update Server の URN です。

[Available Servers] ダイアログボックス

[Available Servers] ダイアログボックスは、Auto Update Server または Configuration Engine を追加、編集、または削除する場合に使用します。

このダイアログボックスでは、その開く方法に応じてタイトルにサーバのタイプを指定できます（たとえば、Available Auto Update Server や Available Configuration Engine）。ダイアログボックスは基本的には同じです。

各行が 1 台のサーバを表し、Security Manager でのサーバの表示名、IP アドレス、および DNS ホスト名とドメイン名が表示されます。ダイアログボックスのタイトルにサーバタイプが含まれていない場合、[Type] フィールドには [AUS] または [CE (Configuration Engine)] を指定します。

- サーバーを追加するには、[作成（Create）] ボタンをクリックし、[サーバープロパティ（Server Properties）] ダイアログボックスに値を入力します（[Server Properties] ダイアログボックス （132 ページ）を参照）。
- サーバーのプロパティを編集するには、サーバーを選択し、[編集（Edit）]ボタンをクリックします。
- サーバーを削除するには、サーバーを選択し、[削除（Delete）]ボタンをクリックします。削除の確認が求められます。

ナビゲーション パス

このダイアログボックスを開くには、次のいずれかを実行します。

- デバイスを手動で追加するときには、[新規デバイス（New Device）] ウィザードの [デバイス情報（Device Information）]ページで、[自動更新サーバー（Auto Update Server）]または [設定エンジン（Configuration Engine）] グループの [サーバー（Server）] フィールドから [サーバーの編集...（Edit Server...）] を選択します。選択肢は、[Edit Auto Update Server] または [Edit Configuration Engine] と表示される場合もあります。

- [デバイスプロパティ（Device Properties）] - [全般（General）] ページで、[自動更新サーバー（Auto Update Server）] または [設定エンジン（Configuration Engine）] グループの [サーバー（Server）] フィールドから [サーバーの編集...（Edit Server...）] を選択します。選択肢は、[Edit Auto Update Server] または [Edit Configuration Engine] と表示される場合もあります。

関連項目

- [Device Information] ページ - [New Device] （118 ページ）
- [Device Information] ページ - [Add Device from Network] （103 ページ）
- Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

インターフェイス モジュールの追加または変更

多くのデバイスでは、インターフェイスモジュールを追加または変更できます。デバイスでホストされたインターフェイスモジュールに変更を加えるときは、そのデバイスのインベントリを変更します。

インターフェイス カードを追加または変更する場合は、デバイスでインベントリを再検出する必要があります。インベントリを再検出すると、[Interfaces]ポリシー（ルータの場合、[Interfaces] > [Interfaces policy]）が置換され、デバイスで使用可能なインターフェイスの機能が Security Manager に正しく表示されるようになります。

（注） インベントリの再検出は、4 GB イーサネット ファイバ インターフェイス カードを取り付けている ASA 5580 デバイスには特に重要です。他のタイプのデバイスの場合、通常、[Interfaces] ポリシーに手動で変更を加えることができますが、インベントリを再検出する方が簡単であり、信頼性にも優れています。

ステップ 1 デバイスを右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択します。

ステップ 2 [検出タスクの作成（Create Discovery Task）] ダイアログボックスで、少なくとも次に挙げる項目を選択し、[OK] をクリックして再検出を開始します。

- [ライブデバイス（Live Device）] からの検出。
- 検出するポリシー：[インベントリ（Inventory）]。

ステップ 3 検出が完了したら、[Interfaces] または [Interfaces] > [Interfaces policy] を必要に応じて編集し、ポリシーに目的の設定が反映されていることを確認します。

デバイス プロパティの表示または変更

デバイスをインベントリに追加するときは、名前やログイン情報など、デバイスのプロパティをいくつか指定します。インベントリに存在するデバイスの場合、デバイスプロパティを表示および変更できます。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス プロパティについて （93 ページ）
- ポリシーについて （209 ページ）
- 重要なデバイス プロパティの変更 （155 ページ）

ステップ 1 デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

ステップ 2 [Device Properties] ダイアログボックスで、左ペインにあるコンテンツ テーブルで対応するエントリをクリックして、プロパティを表示または変更します。別のページに移動する前に、[保存（Save）] をクリックする必要があります。

- [General]：デバイス アイデンティティ、デバイスで実行されているオペレーティング システム、転送設定など、デバイスに関する一般的な情報。これらのフィールドについては、[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ （137 ページ）を参照してください。
- [Credentials]：デバイスへのログインに必要なデバイス クレデンシャル。これらのフィールドについては、 [Device Credentials] ページ （143 ページ）を参照してください。
- [Device Groups]：デバイスが属しているグループ。これらのフィールドについては、 [Device Groups] ページ （148 ページ）を参照してください。
- [Group Information]：グループのグループ詳細（ある場合）。これらのフィールドについては、[グループ情報（Group Information）] ページ （149 ページ）を参照してください。
- [License Information]：FPR-3100 シリーズデバイスのライセンスの詳細。フィールドの詳細については、[ライセンス情報（License Information）] ページを参照してください。

  （注） ライセンス情報パネルは、CSM 4.24 の FPR-3100 シリーズデバイスに対してのみ表示されます。

- [Policy Object Overrides]：デバイスのポリシー オブジェクトに対するローカルなオーバーライド。[Policy Object Overrides] は、デバイスに使用できるさまざまなポリシー オブジェクト タイプが含まれている

フォルダです。特定のポリシーオブジェクトタイプをクリックすると、デバイスで使用されているそのタイプのポリシー オブジェクトが表示され、オーバーライドもあれば表示されます。フィールドの詳細については、ポリシー オブジェクト オーバーライドのページ （154 ページ）を参照してください。

[デバイスのプロパティ（Device Properties）]：[全般（General）] ページ

[Device Properties] の [General] ページは、デバイスの基本的なプロパティに関する情報を追加または編集する場合に使用します。

ナビゲーション パス

- デバイスセレクタから、デバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択し、[全般（General）] をクリックします。
- デバイスセレクタから、デバイスをダブルクリックし、[全般（General）]をクリックします。
- デバイスを選択し、[ツール（Tools）]>[デバイスのプロパティ（Device Properties）] を選択し、[全般（General）] をクリックします。

関連項目

- デバイス プロパティについて （93 ページ）
- [Device Credentials] ページ （143 ページ）
- [Device Groups] ページ （148 ページ）
- ポリシー オブジェクト オーバーライドのページ （154 ページ）

フィールド リファレンス

表 22 : [Device Properties] の [General] ページ

要素	説明
ID	
デバイスタイプ	デバイスのタイプ。

要素	説明
IP タイプ（IP Type）	デバイスの IP アドレスをスタティックにする（デバイスで定義する）か、またはダイナミックにする（DHCP サーバから取得する）かを指定します。選択した IP タイプによって、表示されるフィールドが異なります。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。IPv6 アドレスは 128 ビットの一意のアドレスです。IPv6 アドレスについては、スタティック IP タイプのみがサポートされています。ダイナミック IP タイプは IPv6 アドレスではサポートされません。
ホストネーム （スタティック IP 専用）	デバイスの DNS ホスト名。 これは、デバイスにホスト名として設定される名前と同じである必要はありません。このプロパティは、[Hostname] デバイス プロパティに指定されているホスト名で更新されません。また、デバイスを再検出する場合には、デバイス設定に定義されている名前でも更新されません。 設定ファイルを追加してデバイスを Security Manager に追加した場合は、ホスト名が当初設定ファイルに指定されている名前に設定されます。ホスト名が設定に指定されていない場合は、ファイルの名前が DNS ホスト名として使用されます。
ドメイン名 （スタティック IP 専用）	デバイスの DNS ドメイン名。
IPアドレス （スタティック IP 専用）	デバイスの管理 IP アドレス。192.168.3.8 など。 （注） IP アドレスと DNS ホスト名のどちらか一方、または両方を入力する必要があります。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。デバイスがデュアルスタックで設定されている場合、Security Manager は、Security Manager に追加されたデバイスの IP アドレスに基づいてデバイスと通信します。IPv6 アドレスは 128 ビットの一意のアドレスです。
表示名	Security Manager のデバイス セレクタに表示する名前。 最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。

要素	説明
オペレーティング システム	
OS タイプ	オペレーティングシステムのタイプ。デバイスタイプに基づいて、OS タイプが自動的に選択されます。 （注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。この機能は、オペレーティングシステムのタイプが ASA または FWSM であるデバイスでのみ使用できます。
イメージ名（Image Name）	デバイスで実行されているイメージの名前。イメージ名は、デバイスに展開するか、またはポリシーを再検出するたびに更新されます。
実行中 OS のバージョン	デバイスで実行されているオペレーティング システムのバージョン。
ターゲット OS バージョン	デバイスの設定が基づく OS バージョン。設定しているルールを使用して設定ファイルを作成するとき、Security Manager はターゲット OS バージョンで使用できるコマンドを使用します。このフィールドは、IPS デバイスの読み取り専用です。 ターゲット OS バージョンを、デバイスに使用できる機能セットが大きく変更されているバージョンに変更することはできません。詳細については、Security Manager の機能セットを変更する変更 （157 ページ）を参照してください。
オプション	値が [NONE] または [IPS] である読み取り専用のフィールド。値 [IPS] は、IPS 機能がデバイスで使用可能であることを示します。
IPS 実行中 OS のバージョン	ルータで実行中の IOS IPS のバージョンを表示する読み取り専用のフィールド。[Options] フィールドの値が [NONE] の場合、このフィールドは表示されません。
IPS ターゲット OS バージョン	ルータで実行中の IOS IPS のターゲット バージョンを表示する読み取り専用のフィールド。[Options] フィールドの値が [NONE] の場合、このフィールドは表示されません。
コンテキスト	デバイスで 1 つのセキュリティ コンテキストをホストするか（[Single]）、または複数のセキュリティ コンテキストをホストするか（[Multi]）を指定します。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 の場合だけです。

要素	説明
動作モード（Operational Mode）	デバイスの動作モード。このフィールドが表示されるのは、OS タイプが FWSM、ASA、または PIX ファイアウォール 7.0 以降の場合だけです。使用可能なオプションは [トランスペアレント（Transparent）] または [ルータ（Router）] です。[コンテキスト（Contexts）] で [マルチ（Multi）] を選択する場合、このモードのデフォルト設定は [混合（Mixed）] になります。[混合（Mixed）] は、ASA 9.0 以降および FWSM 3.1 以降のデバイスと ASA-SM にのみ適用されます。
FXOS モード	デバイスが動作している FXOS モード。使用可能なオプションは [プラットフォーム（Platform）] および [アプライアンス（Appliance）] です。[アプライアンス（Appliance）] モードを選択する場合は、CLI、オンボックスデバイス（ASDM など）、またはマルチデバイスマネージャ（Cisco Security Manager など）のいずれかから、すべてのエンドユーザー設定を実行できます。[プラットフォーム（Platform）] モードオプションは、Firepower 2000 シリーズアプライアンスに対してのみ表示されます。 （注） バージョン 4.20 以降、Security Manager は、Firepower 2000 および 1000 シリーズ アプライアンスに対して [アプライアンス（Appliance）] モードをサポートしています。
デバイス通信設定	
トランスポート プロトコル（Transport Protocol）	Security Manager がデバイスにアクセスするとき、または設定をデバイスに展開するときに使用するトランスポート プロトコル。[デフォルトを使用（Use Default）] を選択した場合は、[デバイス通信（Device Communication）] ページ（[ツール（Tools）] > [Security Manager 管理（Security Manager Administration）] > [デバイス通信（Device Communication）]）のトランスポート プロトコル セットが使用されます（[Device Communication] ページ （668 ページ）を参照）。デバイスがデフォルト プロトコルを使用するように設定されていない場合は、別のプロトコルを選択できます。 使用可能なトランスポート プロトコルは、どのデバイス タイプをサポートするかによって異なります。ASA など一部のデバイス タイプでは、オプションが 1 つだけであるため、フィールドはグレー表示されます。
CS-MARS モニタリング	

要素	説明
モニタリング実施サーバ	このデバイスがモニタ対象である場合には、モニタを実施する CS-MARS サーバ。 [CS-MARS の検出（Discover CS-MARS）] をクリックして、Security Manager でどの CS-MARS サーバーがデバイスをモニターしているかを確認します。1 つの CS-MARS サーバだけがデバイスをモニタしている場合、このフィールドはそのサーバ名で更新されます。複数のサーバがある場合は、使用する CS-MARS サーバを選択するように要求されます。デバイスのポリシー ルール テーブルにファイアウォール アクセス ルールまたは IPS シグニチャを表示しているときに、CS-MARS が収集した syslog またはイベントを表示しようとした場合、ここで選択した内容によってアクセスされるサーバが決まります。 デバイスの CS-MARS サーバを検出する場合は、事前に [CS-MARS] 管理ページ（[Tools] > [Security Manager Administration] > [CS-MARS]）でサーバを Security Manager に登録しておく必要があります。詳細については、[CS-MARS] ページ （650 ページ）を参照してください。
[Auto Update] または [Configuration Engine] このグループは、デバイス タイプに応じて名前が異なります。 • [Auto Update]：PIX ファイアウォールおよび ASA デバイスの場合。 • [Configuration Engine]：Cisco IOS ルータの場合。 これらのフィールドは、デバイスを管理するサーバ（ある場合）を識別するために使用します。ダイナミック IP アドレスを持つデバイスには、サーバが必須です。	
サーバー（Server）	デバイスを管理する Auto Update Server または Configuration Engine。AUS の場合、このサーバは AUS ポリシーに定義されているサーバと一致する必要があります（[AUS] ページ （2597 ページ）を参照）。 サーバーをリストに追加するには、[サーバーの追加（Add Server）] を選択します。[サーバーのプロパティ（Server Properties）] ダイアログ ボックスが開きます（[Server Properties] ダイアログボックス （132 ページ）を参照）。[サーバーの編集（Edit Server）] を選択して [使用可能なサーバー（Available Servers）] ダイアログボックスを開き、サーバーのプロパティを編集することもできます（[Available Servers] ダイアログボックス （134 ページ）を参照）。 このサーバ リストの管理の詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）を参照してください。 展開時にこのようなサーバを使用する方法の詳細については、Auto Update Server または CNS Configuration Engine を使用した設定の展開（532 ページ）を参照してください。

要素	説明
デバイスアイデンティティ	Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列。AUS の場合、この ID は AUS ポリシーに定義されている ID と一致する必要があります（[AUS] ページ （2597 ページ）を参照）。
[ASA-CX/FirePOWER モジュール（ASA-CX/FirePOWER Module）]	
管理 IP（Management IP）	ASA の CX または FirePOWER モジュールの管理 IP アドレス。デバイスの検出時またはデバイスへのモジュールの追加後に検出されます。詳細については、ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）を参照してください。 このフィールドは、Security Manager によってすでに検出されている ASA CX または FirePOWER モジュールについてのみ使用できます。
Manager Address	ASA-CX または FirePOWER モジュールの設定および管理に使用される Cisco Prime Security Manager（PRSM）または FireSIGHT Management Center の IP アドレス。デバイスの検出時またはデバイスへのモジュールの追加後に検出されます。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。 このアドレスは編集できます。ただし、Security Manager は、アドレスの検証を実行せず、再検出または再検出によってこのアドレスが変更される可能性があります。 このフィールドは、Security Manager によってすでに検出されている ASA CX または FirePOWER モジュールについてのみ使用できます。
Cisco Security Manager での管理	Security Manager でデバイスを管理するかどうかを指定します。Security Manager は設定を管理せず、このデバイスの設定をアップロードまたはダウンロードしません。 次の理由では、インベントリに管理されていないデバイスを含めることができます。 • VPN エンド ポイントとして機能することがデバイスの唯一の機能である場合。 • デバイスがフェールオーバーに使用するセキュリティ コンテキストである場合。実際にデバイス自身からコンテキストを削除しないかぎり、管理対象デバイスのセキュリティ コンテキストを削除できません。このため、フェールオーバー コンテキストを管理対象外にする必要があります。

要素	説明
フェールオーバーのライセンスサポート （ASA 5505、5510 専用）	オプションのフェールオーバー ライセンスがデバイスにインストールされているかどうかを示します。オプションは、ASA 5505 および 5510 デバイスのみでアクティブになります。Security Manager は、このオプションが選択されている場合のみ、フェールオーバー ポリシーをデバイスに展開します。 ヒント　デバイスからポリシーを検出した場合、Security Manager はライセンス ステータスを判定し、このオプションを適切に設定します。

[Device Credentials] ページ

[Device Credentials] ページは、デバイス アクセスに必要なユーザ名およびパスワードを追加または変更する場合に使用します。デバイス クレデンシャルの詳細については、デバイス クレデンシャルについて （91 ページ）を参照してください。

[クレデンシャル（Credentials）] ページは、（新規デバイス（New Device）ウィザードで）新規デバイスを追加しているか、既存のデバイスのプロパティを表示しているかにかかわらず同じです。

新規デバイスを追加するときには、手動またはネットワークからデバイスを追加する場合にだけクレデンシャルの入力を求められます。

ヒント　新規デバイス（New Device）ウィザードで、ネットワークからデバイスを追加するときに [次へ（Next）] または [完了（Finish）] をクリックした場合、Security Manager はこのようなクレデンシャルを使用してデバイスに接続できるかどうかをテストします。テストの進行中、[Device Connectivity Test] ダイアログボックスが開いたままになります（[Device Connectivity Test] ダイアログボックス （575 ページ）を参照）。テストが失敗した場合は、[詳細（Details）] をクリックして詳細なエラー情報を表示します。モジュールが含まれているデバイス、たとえば FWSM がある Catalyst スイッチを追加している場合は、モジュール検出情報の入力を求められます。

重要　Cisco Security Manager 管理対象デバイスの場合、[デバイスのプロパティ（Device Properties）] ページでパスワードを変更する場合は、[ユーザーアカウント（User Accounts）] ページでも同じように更新してください。同じように更新しないと、Cisco Security Manager とデバイス間の通信の初期フェーズは成功し、[接続のテスト（Test Connectivity）] も正常に検証されますが、展開は失敗します。これは、[ユーザーアカウント（User Accounts）] ページで設定されたパスワードが [デバイスのプロパティ（Device Properties）] ページで更新されるためです。したがって、ログイン情報の更新が [デバイスのプロパティ（Device Properties）] ページと [ユーザーアカウント（User Accounts）] ページで並行して実行されるようにすることを推奨します。

ナビゲーション パス

- 新規デバイスの場合、デバイスビューで**[ファイル（File）]>[新規デバイス（New Device）]**を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。
- 既存のデバイスの場合、デバイスプロパティを開くには、デバイスセレクタでデバイスをダブルクリックし、[デバイスのプロパティ（Device Properties）] ページで [クレデンシャル（Credentials）] をクリックします。

関連項目

- デバイス クレデンシャルについて （91 ページ）
- ネットワークからのデバイスの追加 （100 ページ）
- 手動定義によるデバイスの追加 （116 ページ）
- [Device Communication] ページ （668 ページ）
- デバイス プロパティについて （93 ページ）
- デバイス プロパティの表示または変更 （136 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- [Discovery Status] ダイアログボックス （238 ページ）

フィールド リファレンス

表 23 : [Device Credentials] ページ

要素	説明
Primary Credentials	
すべてのデバイス タイプに必須です。[HTTP] グループで [プライマリ クレデンシャルを使用（Use Primary Credentials）] を選択した場合、このようなクレデンシャルが SSH 接続と Telnet 接続、および HTTP 接続と HTTPS 接続に使用されます。 デバイス ポリシーで、指定したユーザに対するパスワード、またはイネーブル パスワードを変更する場合、Security Manager は、その展開中には古いパスワードをログインに使用します。展開が正常に完了すると、デバイス クレデンシャルのパスワードが、新しく展開されたパスワードに更新されます。これらのパスワードに関連するデバイス ポリシーを更新する方法については、次の項を参照してください。 • ASA/PIX/FWSM デバイス： デバイス クレデンシャルの設定 （2488 ページ） • IPS デバイス： IPS ユーザ アカウントの設定 （2105 ページ） • IOS デバイス： アカウントおよびクレデンシャル ポリシーの定義 （3130 ページ）	

要素	説明
ユーザー名	デバイスにログインするためのユーザ名。ユーザは特権レベル 15 が必要です。 デバイスがその設定のみにイネーブルパスワードを必要としている場合、[Username] フィールドおよび [Password] フィールドをブランクのままにし、[Enable Password] だけを入力できます。 （注） PIX、ASA、およびFWSMデバイスでは、ユーザ名を 4 文字以上にする必要があります。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェア バージョン 9.6(1) 以降を実行している ASA デバイスの場合、最大 127 文字のパスワードを入力できます。
パスワード	デバイスにログインするためのパスワード（ユーザ EXEC モード）。[Confirm] フィールドに、パスワードを再入力します。
パスワードを有効にする（Enable Password）	イネーブルモード（特権 EXEC モード）がデバイスに設定されている場合に、そのデバイスでイネーブルモードをアクティブにするパスワード。[Confirm] フィールドに、パスワードを再入力します。
HTTP Credentials デバイスへの HTTP 接続または HTTPS 接続を確立するためのクレデンシャル。デバイスの中には、このタイプの接続をサポートするものもあれば、（IPS デバイスのように）必須とするものもあります。	
Use Primary Credentials ユーザ名 パスワード	Security Manager が HTTP 接続および HTTPS 接続に設定済みのプライマリ クレデンシャルを使用するかどうかを指定します。デバイスが HTTP/HTTPS 接続に異なるクレデンシャルを使用している場合は、[プライマリクレデンシャルを使用（Use Primary Credentials）] の選択を解除し、HTTP/HTTPS 用に設定されたユーザ名およびパスワードを入力します。[Confirm] フィールドにパスワードを再入力します。 （注） PIX、ASA、およびFWSMデバイスでは、ユーザ名を 4 文字以上にする必要があります。パスワードには、3 ～ 32 文字を使用できますが、8 文字以上にすることを推奨します。ソフトウェア バージョン 9.6(1) 以降を実行している ASA デバイスの場合、最大 127 文字のパスワードを入力できます。
HTTP ポート（HTTP Port）	HTTP 接続に使用するポート。デフォルトのポートは 80 です。この設定値は、デフォルトとは異なるポートで HTTP 接続を受け付けるようにデバイスが設定されている場合にだけ変更します。

要素	説明
HTTPS ポート（HTTPS Port）	HTTPS 接続に使用するポート。デフォルトのポートは 443 です（Security Manager デバイス通信設定に別のデフォルトが設定されていない場合）。デフォルトを変更するには、まず [デフォルトを使用（Use Default）] の選択を解除します。この設定値は、デフォルトとは異なるポートで HTTPS 接続を受け付けるようにデバイスが設定されている場合にだけ変更します。 （注） ローカル HTTP ポリシーを共有ポリシーとなるように設定して複数のデバイスに割り当てた場合、共有ポリシーが割り当てられるすべてのデバイスを対象に、[Device Credentials] ページに設定されたポート番号が共有ポリシーの HTTPS ポート番号設定で上書きされます。
IPS RDEP Mode	イベント モニタリングのために RDEP または SDEE 接続を確立するときに、IPS デバイスへのアクセスに使用する接続方法。
Certificate Common Name	証明書に割り当てられる名前。共通名は、証明書に割り当てられた個人、システム、またはその他のエンティティの名前にすることができます。[Confirm] フィールドに、共通名を再入力します。
その他のフィールドおよびボタン	
Authentication Certificate Thumbprint （デバイス プロパティ専用）	Security Manager 証明書データ ストアに保存できるデバイスの証明書サムプリント。デバイスから現在の証明書を取得し、Security Manager に格納されている証明書に置き換えるには、[デバイスから取得（Retrieve From Device）] をクリックします。 IPS デバイスでは、IPS 証明書の管理 （2310 ページ）で説明するように、証明書を管理するための追加オプションがあります。
[RX-Boot Mode] ボタン	[RX-Boot Mode Credentials] ダイアログボックス （147 ページ）を開きます。ここでは、縮小コマンド セット イメージ（RX-Boot）からルータを起動するためのクレデンシャルを入力できます。 そのクレデンシャルがフラッシュ メモリから実行する Cisco ルータ用のものである場合（ルータはフラッシュの最初のファイルからだけ起動します）、フラッシュにあるイメージ以外のイメージを実行してフラッシュ イメージをアップグレードする必要があります。Rx-Boot クレデンシャルは、そのような他のイメージを実行するためのものです。
[SNMP] ボタン	[SNMP Credentials] ダイアログボックス （147 ページ）を開きます。ここでは、デバイスに定義されている SNMP コミュニティ ストリングを指定できます。

要素	説明
[Test Connectivity] ボタン （デバイス プロパティおよび手動によるデバイス追加専用）	入力したクレデンシャルおよび設定済みの転送方法を使用して Security Manager がデバイスに接続できるかどうかをテストします。デバイス接続のテストの詳細については、デバイス接続のテスト （573 ページ）を参照してください。

[RX-Boot Mode Credentials] ダイアログボックス

[RX-Boot Mode Credentials] ダイアログボックスは、Rx-Boot モード クレデンシャルを追加する場合に使用します。このクレデンシャルは、縮小コマンド セット イメージ（Rx-Boot）からルータを起動するときに使用されます。Rx-Boot モードのユーザ名およびパスワードを入力します。[Confirm] フィールドに、パスワードを再度入力します。

ナビゲーション パス

[RX-Bootモードログイン情報（RX-Boot Mode Credentials）] ダイアログボックスを開くには、New Device ウィザード（デバイスを手動またはネットワークから追加する場合）または [デバイスのプロパティ（Device Properties）] ページで、[Device Credentials] ページ （143 ページ）にある [RX-Bootモード（RX-Boot Mode）] をクリックします。

[SNMP Credentials] ダイアログボックス

[SNMP Credentials] ダイアログボックスは、SNMP クレデンシャルを追加する場合に使用します。

ナビゲーション パス

[SNMPログイン情報（SNMP Credentials）] ダイアログボックスを開くには、New Device ウィザード（デバイスを手動またはネットワークから追加する場合）または[デバイスのプロパティ（Device Properties）] ページで、[Device Credentials] ページ （143 ページ）の [SNMP] をクリックします。

フィールド リファレンス

表 24 : [SNMP Credentials] ダイアログボックス

要素	説明
SNMP V2C SNMP バージョン 2 を実行しているデバイスのクレデンシャルです。	
RO Community String	読み取り専用のコミュニティ ストリング。[Confirm] フィールドに、コミュニティ ストリングを再入力します。
RW Community String	読み書き可能なコミュニティ ストリング。[Confirm] フィールドに、コミュニティ ストリングを再入力します。

要素	説明
SNMP V3 SNMP バージョン 3 を実行しているデバイスのクレデンシャルです。	
ユーザー名	SNMP バージョン 3 の認証ユーザー名。
パスワード	SNMP バージョン 3 の認証ユーザーパスワード。[Confirm] フィールドに、パスワードを再入力します。
認証アルゴリズム（Auth Algorithm）	パスワードを暗号化するための認可アルゴリズム。MD5 または SHA-1 を選択できます。
プライバシー パスワード（Privacy Password）	SNMP バージョン 3 の暗号化ユーザーパスワード。[Confirm] フィールドに、パスワードを再入力します。
プライバシーアルゴリズム（Privacy Algorithm）	暗号化アルゴリズムとバージョンを選択して、暗号化レベルを指定します。 • DES：56 ビットキーを使用して、Data Encryption Standard（DES; データ暗号規格）暗号アルゴリズムを適用します。 • 3DES：トリプル DES を使用します。Data Encryption Standard（DES; データ暗号規格）暗号アルゴリズムは、各パケットに 3 回適用されます。 • AES128：128 ビットキーで Advanced Encryption Standard を使用します。 • AES192：192 ビットキーで Advanced Encryption Standard を使用します。 • AES256：256 ビットキーで Advanced Encryption Standard を使用します。
エンジンID（Engine ID）	デバイスの SNMP v3 認証エージェントの 16 進数の識別子を入力します。

[Device Groups] ページ

[Device Groups] ページは、デバイスをデバイス グループに割り当てる場合に使用します。このページからデバイス グループを編集または削除することもできます。

ナビゲーション パス

- 新規デバイスの場合、デバイスビューで [ファイル（File）]>[新規デバイス（New Device）] を選択するか、またはデバイスセレクタの [追加（Add）] ボタンをクリックします。

- 既存のデバイスの場合、デバイスプロパティを開くには、デバイスセレクタでデバイスをダブルクリックし、[デバイスプロパティ（Device Properties）] ページで [デバイスグループ（Device Groups）] をクリックします。

関連項目

- デバイスのグループ化について （164 ページ）
- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイス プロパティについて （93 ページ）
- [Discovery Status] ダイアログボックス （238 ページ）

フィールド リファレンス

表 *25 : [Device Grouping]* ページ

要素	説明
[Department] や [Location] などの [Group Types]	Security Manager に定義されているグループ タイプ。[Department] や [Location] など。各フィールドには、そのグループ タイプ内に定義されたデバイス グループのリストが含まれています。デバイスを所属させるデバイス グループを選択します。 新規デバイスグループまたはグループタイプを作成する場合は、いずれかの既存グループタイプのドロップダウンリストから [グループの編集（Edit Groups）] を選択します。これにより、[Edit Device Groups] ページが開きます。ここでは、新規グループおよびグループ タイプを作成または削除できます（[Edit Device Groups] ダイアログボックス （166 ページ）を参照）。
Set values as default	選択したグループをデフォルト グループとして設定するかどうかを指定します。このオプションを選択した場合、他に追加しようとしているデバイスもそのグループに自動的に追加されます。

[グループ情報（Group Information）] ページ

[デバイスプロパティのグループ情報（Device Properties Group Information）] ページを使用して、グループの詳細を表示します。

ナビゲーション パス

- デバイスセレクタから、デバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択し、[グループ情報（Group Information）] をクリックします。
- デバイスセレクタから、デバイスをダブルクリックし、[グループ情報（Group Information）] をクリックします。

- デバイスを選択し、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択し、[グループ情報（Group Information）] をクリックします。

関連項目

- デバイスクラスタの使用 （97 ページ）
- デバイス プロパティについて （93 ページ）
- [Device Credentials] ページ （143 ページ）
- [Device Groups] ページ （148 ページ）
- ポリシー オブジェクト オーバーライドのページ （154 ページ）

フィールド リファレンス

表 *26 : [デバイスプロパティのグループ情報（Device Properties Group Information）]ページ*

要素	説明
グループの詳細（Group Details）	
デバイスタイプ	デバイスのタイプ。
グループ名（Group Name）	グループに割り当てられた名前。
Group Control	制御ユニットとして機能するデバイスのグループメンバー名。 （注） 制御ユニットへの変更は、Security Managerに自動的には反映されません。
デバイスから取得（Retrieve From Device）	[デバイスから取得（Retrieve From Device）] を使用して、制御ユニット情報を更新します。
インターフェイス モード	インターフェイスがレイヤ 2 ロードバランシング（スパンド EtherChannel）またはレイヤ3 ロードバランシング（単独）用のどちら設定されているか。

要素	説明
管理IPプール範囲（Management IP Pool Range）	クラスタの管理に使用する IP アドレスプールを入力します。ユーザコンテキストのデバイスにこの値を指定できます。マルチコンテキスト ASA クラスタの syslog をモニターするために Event Viewer が使用されている場合、このフィールドは必須です。 このフィールドを空白のままにするか、正しくない IP アドレスプールを入力すると、Event Viewer は syslog を特定のコンテキストに分類できず、syslog イベントをドロップします。 （注） 有効な IP アドレスを入力していることを確認してください。Cisco Security Manager は、入力された IP アドレスプールを検証しません。
CSMでの最終更新（Last Update in CSM）	このグループのグループ情報が Security Manager によって最後に更新された日時。
グループVPNモード（Group VPN Mode）	Cisco Security Manager 4.16 以降では、グループ デバイスを検出した後、グループ VPN モードが表示されます。この値は [集中型（Centralized）]または[分散型（Distributed）] です。 （注） この値は、デバイスセレクタビューでデバイスの上にマウスポインタを置いたときに表示されるポップアップウィンドウにも表示されます。
グループVPNバックアップ（Group VPN Backup）	Cisco Security Manager 4.16 以降では、[グループVPNバックアップ（Group VPN Backup）] が表示されます。 分散型モードでは、次のいずれかの値が表示されます 。 • [フラット（Flat）] : グループ VPN バックアップが他のメンバーに存在する場合 • [リモートシャーシ（Remote Chassis）] : グループ VPN バックアップが別のシャーシに存在する場合 グループ VPN バックアップの情報は、集中型 VPN モードでは表示されません。集中型 VPN モードでのこのフィールドの値は N/A です。 （注） この値は、デバイスセレクタビューでデバイスの上にマウスポインタを置いたときに表示されるポップアップウィンドウにも表示されます。
グループノードの詳細（Group Node Details） [グループノードの詳細（Group Node Details）] テーブルには、グループ内の各デバイスの詳細が一覧表示されます。	

要素	説明
グループ ID（Group ID）	グループノードのグループ ID。
ノード名	グループノードのメンバー名。
シリアル番号	グループノードのシリアル番号。
CCL IP	グループノードのグループ制御リンク IP アドレス。
CCL MAC	グループノードのグループ制御リンク MAC アドレス。
サイト ID（Site ID）	現在のグループメンバーが属するサイト。サイト ID を設定すると、MAC アドレスのフラッピングが防止されます。

[ライセンス情報（License Information）] ページ

[デバイスプロパティ（Device properities）] ウィンドウで、FPR-3100 シリーズ デバイスのプラットフォームライセンスのサブスクリプション ステータス、ライセンスの有効期限、およびライセンスの取得日をモニタリングできます。

CSM ライセンススケジューラ

CSM ライセンススケジューラは毎日実行され、デバイスからプラットフォームライセンスの詳細を取得し、CSM データベースで同じ情報を更新します。これは 24 時間ごとに 1 回実行されるバックグラウンドプロセスであり、デフォルトの時刻は午前 4 時です。CSM プロパティファイルのライセンススケジューラの時刻はカスタマイズ可能です。CSM プロパティファイルは、..\CSCOpx\MDC\athena\configcsm.properties にあります。ライセンススケジューラでは、次の 3 つのモードがサポートされています。

- [AM]：0 ～ 11 の任意の時刻を入力でき、スケジューラは毎朝特定の時刻に実行されます。
- [PM]：1 ～ 12 の任意の時刻を入力でき、スケジューラは午後の特定の時刻に実行されます。
- [AMPM]：24 時間形式で設定する場合に使用します。スケジューラは指定した特定の時刻に実行されます。

（注） ライセンススケジューラは、サービスまたはシステムの再起動時に開始され、停止することはできません。

更新されたライセンス情報は、CSM の [ライセンス情報（License Information）] タブの [ポリシーヘッダー（Policy Header）] と [デバイスプロパティ（Device Properties）] に反映されます。

ナビゲーション パス

- デバイスセレクタから、FPR-3100 シリーズ デバイスを右クリックし、[デバイスプロパティ（Device Properties）] を選択して、[ライセンス情報（License Information）] をクリックします。
- デバイスセレクタから、FPR-3100 シリーズデバイスをダブルクリックして、[ライセンス情報（License Information）] をクリックします。
- FPR-3100 シリーズ デバイスを選択し、[ツール（Tools）] > [デバイスプロパティ（Device Properties）] を選択してから、[ライセンス情報（License Information）] をクリックします。

（注） プラットフォームライセンス情報のライセンス取得時刻は、DST 中には表示されません。

[デバイスプロパティ（Device Properties）] のライセンス サブスクリプション ステータス

FPR-3100 シリーズ デバイスで、CSM はプラットフォーム ライセンス サブスクリプションのさまざまなステータスを処理します。[ライセンスの詳細（License Details）] は、[デバイスプロパティ（Device Properties）] ページの [ライセンス情報（License Information）] に表示されます。サポートされているライセンス サブスクリプションのステータスは次のとおりです。

ステータス（Status）	説明（Description）
新規インストール	インストール後のライセンスの変更はありません。
評価モード	設定の変更が完了し、ライセンス機能階層の標準が設定されました。利用可能なライセンスの有効期限は 90 日間です。
評価モードの期限切れ	評価モードの有効期限が切れています。
Compliant	Firepower デバイスはアカウントに登録されており、十分なライセンスがあります。
猶予期間	登録されているデバイスの数に比べて、アカウントのライセンス数が不足しています。設定変更の展開は 90 日間有効です。
猶予期間の期限切れ	猶予期間の期限が切れています。 ヒント アカウントに接続して修正するか、不要なデバイスを登録解除します。

（注） プラットフォームライセンスが期限切れになっているFPR-3100シリーズデバイスは、展開時にアクティビティ検証エラーをトリガーします。アクティビティ検証エラーにより、デバイスを管理できないため、ライセンスをアップグレードして展開を実行するか、CSMからデバイスを削除する必要があります。[インベントリを使用した再検出（Re-discovery via inventory）] オプションを使用して、CSM のプラットフォームライセンスの詳細を一度に更新します。

ポリシーヘッダーのライセンス サブスクリプション ステータス

FPR-3100 シリーズ デバイスの [プラットフォームライセンス（Platform License）] は、CSM のポリシーヘッダー GUI にカラーコードで表示されます。ライセンス詳細のカラーコードは次のとおりです。

- 承認：黒
- 猶予期間：オレンジ
- 評価モード：オレンジ
- 評価モードの期限切れ：赤
- 猶予期間の期限切れ：赤
- 使用中のライセンスなし：黒

（注） ポリシービューには、FPR-3100 シリーズ デバイスのライセンスステータスが表示されません。

ポリシー オブジェクト オーバーライドのページ

選択したデバイスの [Device Properties] ウィンドウから、多くのタイプのポリシー オブジェクトのグローバル設定を上書きできます。これにより、そのデバイスにあるオブジェクトの定義をカスタマイズできます。詳細については、個々のデバイスのポリシーオブジェクトオーバーライドについて （310 ページ）を参照してください。

コンテンツ テーブルの [Policy Object Overrides] フォルダには、特定のデバイス タイプのオーバーライドを作成できるあらゆるタイプのオブジェクトが含まれています。オブジェクト タイプを選択すると、デバイスのオーバーライドを許可するように設定されている既存のポリシー オブジェクトがあれば、右ペインのテーブルに表示されます。オブジェクトにデバイスに対するオーバーライドがすでに定義されている場合、[値がオーバーライドされているか（Value Overridden?）] カラムにチェックマークが付けられます。

このようなオブジェクトのオーバーライドを作成および管理できます。オブジェクトを選択し、次の手順を実行できます。

- オーバーライドを作成するには、[Create Override] ボタンをクリックします。これにより、そのタイプのオブジェクトを編集するためのダイアログボックスが開きます。オブジェクト固有の情報については、[Help] ボタンをクリックしてください。
- 既存のオーバーライドを編集するには、[Edit Override] ボタンをクリックします。
- オーバーライドを削除するには、[Delete Override] ボタンをクリックします。

ナビゲーション パス

デバイスセレクタでデバイスをダブルクリックし、左ペインのコンテンツテーブルにある [ポリシーオブジェクトオーバーライド（Policy Object Overrides）] フォルダで目的のポリシーオブジェクトタイプをクリックします。

関連項目

- [Policy Object Overrides] ウィンドウ （314 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）
- デバイス レベルのオブジェクト オーバーライドの削除 （315 ページ）
- テーブルのフィルタリング （64 ページ）

重要なデバイス プロパティの変更

デバイスのイメージ バージョン、デバイス タイプ、または Security Manager によって管理される FWSM デバイスおよび ASA デバイスのセキュリティ コンテキストまたは動作モードを変更するときには、注意が必要です。このような変更を加えると、デバイスの別の機能セットがイネーブルになる場合があります。その結果、Security Manager でデバイスに設定したポリシーの一部が適用されなく可能性があります。

主要なデバイス変更、その変更が Security Manager のポリシーに及ぼす影響、およびこのようなデバイス変更を実装する際の手順については、以降の項で説明します。

- Security Manager の機能セットを変更しないイメージ バージョン変更 （155 ページ）
- Security Manager の機能セットを変更する変更 （157 ページ）

Security Manager の機能セットを変更しないイメージ バージョン変更

次のイメージバージョン変更は、Security Manager で該当するデバイスに使用できるポリシーのタイプに影響しません。

- 1 つの IOS 個別リリース番号から、同じ Cisco IOS リリース内の別の個別リリース番号へのアップグレード（たとえば IOS 12.3(10) から 12.3(13) へのアップグレード）。
- 任意の IOS 12.1 イメージから任意の 12.2 イメージへのアップグレード。

- 任意の IOS 12.2 イメージから任意の 12.3 イメージへのアップグレード。
- 任意の IOS 15.0 イメージから任意の 15.1 イメージへのアップグレード。
- 任意の IOS 15.2 イメージから任意の 15.3 イメージへのアップグレード。
- 任意の PIX 6.x イメージから別の PIX 6.x イメージへのアップグレード。
- 任意の PIX 7.x イメージから別の PIX 7.x イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の ASA 7.x イメージから別の ASA 7.x イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の ASA 8.0(x) ～ 8.2(x) イメージから別の ASA 8.0(x) ～ 8.2(x) イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の FWSM 2.x イメージから別の 2.x FWSM イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の FWSM 3.x イメージから別の 3.x FWSM イメージへのアップグレード（同じセキュリティ コンテキストおよびモード設定を保持）。
- 任意の IOS 12.x イメージから別の IOS 12.x イメージへの Catalyst 6500/7600 シャーシのアップグレード。

（注） このリストは、Security Manager がサポートするイメージにだけ適用されます。サポートされるイメージのリストについては、次の URL にあるこの製品バージョンの『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください（http://www.cisco.com/en/US/products/ps6498/products_device_support_tables_list.html [英語]）。

このような場合、次の手順を使用してイメージ バージョンを変更します。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス プロパティについて （93 ページ）
- ポリシーについて （209 ページ）
- Security Manager の機能セットを変更する変更 （157 ページ）

ステップ 1 デバイスのイメージ バージョンをアップグレードします。

ステップ 2 デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。

- デバイスを右クリックして、[デバイスプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスプロパティ（Device Properties）] の順に選択します。

ステップ 3 [デバイスプロパティ（Device Properties）] ダイアログボックスで、[全般（General）] ページにある [ターゲットOSバージョン（Target OS Version）] プロパティを更新後のバージョン番号に変更し、[保存（Save）] をクリックします。

Security Manager の機能セットを変更する変更

デバイスに使用できるポリシー フィーチャ セットに影響を与える主要なタイプのデバイス変更です。

- イメージ バージョン変更：次のイメージ バージョン変更は、Security Manager でそのデバイスに使用できるポリシーのタイプに影響を与えます。
  - ASA 8.3(x) 以下のリリースから ASA 8.4(x) 以降のリリースへのアップグレード。
  - ASA 8.2(x) 以下のリリースから ASA 8.3(x) 以降のリリースへのアップグレード。
  - ASA、PIX、FWSM、IPS の各デバイスのメジャーバージョン番号の変更。たとえば、8.x から 9.x への ASA のアップグレード、または 7.x から 6.x への IPS デバイスのダウングレード。
  - IOS 12.1 イメージまたは 12.2 イメージから IOS 12.3 イメージまたは 12.4 イメージへのアップグレード。
  - IOS 12.3 イメージまたは 12.4 イメージから IOS 12.1 イメージまたは 12.2 イメージへのダウングレード。
  - IOS 12.3 以前のリリースから IOS 15.2 以降へのアップグレード。

このような変更を加えた場合でも、その変更の影響を受けるポリシーをまだ定義していなければ、デバイスのターゲット OS バージョンを変更できる可能性があります。管理対象デバイスのターゲット OS バージョンを別のバージョンに変更すると、そのデバイスに使用できるポリシーのタイプが変更される場合、Security Manager ではそのような変更が許可されません。そのような変更を加えることができない場合には（問題のポリシーを特定したうえで）通知されます。このため、まず Security Manager からデバイスを削除し、イメージの変更を実行してから、デバイスを追加し直す必要があります。

アクセス ルールなどポリシーのタイプによっては、イメージバージョンまたはプラットフォーム タイプの変更の影響を受けないものがあります。

8.3 および 9.0.1 ASA リリースで導入された NAT ポリシーの変更では、NAT ポリシーを Security Manager で再検出する必要があります。これは、以下で説明するように、デバイスを削除してから Security Manager に再度追加することで実現できます。または、デバイスのポリシーの検出機能を使用して NAT ポリシーのみを再検出することもできます。デバイスのポリシーの検

出機能については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

（注） ASA デバイスが Security Manager の外で現在のバージョンから上位または下位のバージョンにアップグレードまたはダウングレードされた場合は、デバイスを削除してから、Security Manager に再度追加する必要があります。

- セキュリティ コンテキストおよび動作モードの変更：FWSM デバイスまたは ASA デバイスのセキュリティ コンテキストおよび動作モード設定に変更を加えると、そのデバイスで別の機能セットがイネーブルになります。このような変更は、次のようにデバイスを変更すると発生します。
  - 単一のコンテキストから複数のコンテキスト（またはその逆）。
  - ルーテッド モードからトランスペアレント モード（またはその逆）。

Security Manager では、管理対象デバイスのセキュリティ コンテキストまたは動作モード設定を変更できません。このため、まず Security Manager からデバイスを削除し、コンテキストまたはモードを変更してから、デバイスを追加し直す必要があります。

ポリシー タイプによっては（たとえば、Banner、Clock、Console Timeout、HTTP）、動作モードの変更の影響を受けないものがあります。このほか（Banner および Clock に加えて ICMP、SSH、TFTP のように）セキュリティ コンテキスト設定の変更の影響を受けないものもあります。

- デバイス ハードウェアの交換：特定のデバイスを交換しても、元の連絡先情報（IP アドレスなど）を保持できる場合があります。
  - PIX ファイアウォールを Cisco IOS ルータに交換する場合。
  - PIX ファイアウォールを ASA デバイスに交換する場合。
  - ルータをファイアウォール デバイスに交換する場合。
  - ルータを別のモデルの新規ルータに交換する場合。

このいずれの場合でも、新規デバイスにより、Security Manager でそのデバイスに使用できるポリシーのタイプが変更されます。Security Manager では、既存のデバイスのハードウェア モデルを変更できません。このため、まず Security Manager からデバイスを削除し、物理デバイスを変更してから、デバイスを追加し直す必要があります。

ポリシー タイプによっては（たとえば、アクセル ルール）は、デバイス タイプの変更の影響を受けないものがあります。

変更の影響を受けないデバイスを Security Manager から削除する前に、そのデバイスに設定されたポリシーを共有することを推奨します。このようにすると、Security Manager を追加し直したあと、ポリシーをデバイスに（継承およびポリシー オブジェクト参照はそのままにして）再び割り当てることができるため便利です。次の手順では、その方法について説明します。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス プロパティについて （93 ページ）
- ポリシーについて （209 ページ）
- Security Manager の機能セットを変更しないイメージ バージョン変更 （155 ページ）

ステップ 1 Security Manager でデバイスに設定したすべての変更を送信し、展開します。これにより、イメージのアップグレードよりも前に、目的の設定がデバイスに配置されます。

ステップ 2 デバイスに定義されているローカル ポリシーを共有します。

a) デバイスセレクタでデバイスを右クリックし、[デバイスポリシーの共有（Share Device Policies）] を選択します。デフォルトでは、Share Policies ウィザードでの共有対象として、デバイスに設定されたすべてのポリシー（ローカルおよび共有）が選択されます。

b) ポリシー アイコンに手の形で示されている既存の各共有ポリシーの横にあるチェックボックスをオフにします。この操作が必要になるのは、すでに存在する共有ポリシーのコピーを作成する必要がないためです。イメージ バージョンのアップグレード後に、既存の共有ポリシーを再び割り当てます。

c) 共有ポリシーの名前を入力します。デバイス名を便利な識別手段として使用することを推奨します。たとえば、デバイス名が MyRouter である場合、各共有ポリシーには MyRouter という名前が付与されます。このために、作成しているすべてのポリシーを書き留めます。

d) [終了（Finish）] をクリックします。選択したローカル ポリシーが共有ポリシーになります。

ステップ 3 Security Manager からデバイスを削除します。

ステップ 4 デバイスに目的の変更を加えます。たとえば、イメージ バージョンのアップグレード、動作モードの変更、デバイスの交換などです。

ステップ 5 デバイスを Security Manager に追加し直し、ポリシー検出を実行します。

ステップ 6 デバイスにポリシーを再び割り当てます。

a) デバイスポリシーセレクタに表示された最初のポリシータイプを右クリックし、[共有ポリシーの割り当て（Assign Shared Policy）] を選択します。

b) [Assign Shared Policy] ダイアログボックスで、次のいずれかを実行します。

- ローカルポリシーがデバイスで以前に定義されている場合は、この手順のために作成した共有ポリシーを選択し、[OK] をクリックします。
- このタイプの共有ポリシーがデバイスに以前に割り当てられていた場合は、そのポリシーを選択し、[OK] をクリックします。

c) （ローカルポリシーのみ）デバイスポリシーセレクタで再度ポリシータイプを右クリックし、[ポリシーの共有解除（Unshare Policy）] を選択します。

d) デバイスの設定に関連するポリシータイプごとに、この手順を繰り返します。共有ポリシーが使用できない場合は、これが以前のイメージ バージョンに使用できなかったポリシー タイプであることを示します。

ステップ 7 （任意）この手順のために作成した共有ポリシーをポリシー ビューから削除します。

a) [表示（View）]>[ポリシービュー（Policy View）] を選択するか、またはツールバーの [ポリシービュー（Policy View）] アイコンをクリックします。
b) 削除するポリシーのいずれかを選択し、作業領域の [割り当て（Assignments）] タブをクリックして、ポリシーがどのデバイスにも割り当てられていないことを確認します。
c) 共有ポリシーセレクタの下にある [ポリシーの削除（Delete Policy）] ボタンをクリックして、ポリシーを削除します。
d) 削除するポリシー タイプごとに、この手順を繰り返します。

デバイスに含まれている要素の表示

サービス モジュール、セキュリティ コンテキスト、および仮想センサーを含んでいるデバイスを対象に、それぞれの内容を表示できます。デバイスのタイプに基づいて、このようにデバイスに含まれている要素を表示できます。

- Catalyst 6500 デバイス：IDSM および FWSM サービス モジュール、セキュリティ コンテキスト、および仮想センサー。
- FWSM、PIX ファイアウォール 7.0、および ASA デバイスの場合：デバイスに定義されているセキュリティ コンテキスト。セキュリティ コンテキストの詳細については、ファイアウォールデバイスでのセキュリティ コンテキストの設定（2979ページ）を参照してください。
- IPS デバイス：デバイスに定義されている仮想センサー。

含まれている項目を表示するには、デバイスビューで、該当するタイプのデバイスのいずれかを選択し、[ツール（Tools）] > [内容の表示（Show Containment）] を選択するか、またはデバイスを右クリックし、[内容の表示（Show Containment）] を選択します。[Composite View] ダイアログボックスが開き、選択したデバイスに含まれる要素があれば表示されます。

デバイスの複製

複製した（重複する）デバイスでは、複製元のデバイスの設定およびプロパティが共有されます。デバイスを複製すると、新規デバイスの設定およびプロパティを再作成する必要がないため、時間の節約になります。

複製したデバイスは、デバイスのオペレーティング システム バージョン、クレデンシャル、およびグループ化属性を複製元のデバイスと共有しますが、表示名、IP アドレス、ホスト名、ドメイン名など独自の一意のアイデンティティもあります。一度に複製できるデバイスは、1 つだけです。

（注） Catalyst スイッチまたは Catalyst 6500/7600 デバイスは複製できません。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス間でのポリシーのコピー （251 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、**[ファイル（File）] > [デバイスの複製（Clone Device）]** を選択するか、またはデバイスセレクタでデバイスを右クリックし、[デバイスの複製（Clone Device] を選択します。
- （マップビュー）デバイスを右クリックし、[デバイスの複製（Clone Device] を選択します。

[Create a Clone of Device] ダイアログボックスが表示されます。

ステップ 2 複製の IP アドレスおよび名前をそれぞれ該当するフィールドに入力します。次に、使用可能な属性を示します。

- [IPタイプ（IP Type）] : デバイスでスタティック IP アドレスが使用されるのか、（DHCP から提供される）ダイナミック IP アドレスが使用されるのかを指定します。デバイスを複製するときには、IP タイプは変更できません。
- [ホスト名（Hostname）] :（スタティック IP のみ）。複製したデバイスの DNS ホスト名。
- [ドメイン名（Domain Name）] :（スタティック IP のみ）。複製したデバイスの DNS ドメイン名。ドメイン名を指定しないと、Security Manager ではサーバに設定されたデフォルトのドメイン名が使用されます。
- [IPアドレス（IP Address）] : 複製したデバイスの管理 IP アドレス（10.10.100.1 など）。IP アドレスがわからない場合は、[Hostname] フィールドに DNS ホスト名を入力します。スタティック IP アドレスが設定されたデバイスの IP アドレスまたはホスト名を入力する必要があります。

（注） バージョン 4.12 以降、ASA デバイスに対する Cisco Security Manager サーバーからデバイスへの通信は、IPv6 アドレスまたは IPv4 アドレスのいずれかでサポートされます。

- [表示名（Display Name）] : Cisco Security Manager デバイスリストに表示される名前。最大長は 70 文字です。有効な文字は、0 ～ 9、大文字の A ～ Z、小文字の a ～ z、_ - . :、およびスペースです。
- [デバイスID（Device Identity）] :（ダイナミック IP のみ）。Auto Update Server または Configuration Engine でデバイスを一意に識別する文字列値。このフィールドは、このようなサーバのいずれかを使用するようにデバイスが設定されている場合にだけ表示されます。
- [VPN割り当ての複製（Clone VPN Assignments）] : デバイスに対して定義されている VPN 割り当てをコピーするかどうかを指定します。このフィールドは、デバイスが VPN 割り当てをサポートする場合にだけ表示されます。

ハブアンドスポーク設定のスポークとなっているデバイス、または完全メッシュ トポロジに参加しているデバイスの VPN 割り当てを複製できます。スポーク デバイスを複製した場合、新規デバイスは複製元と同じポリシーで VPN に新規スポークとして追加されます。完全メッシュ VPN のデバイスを複製した場合、

新規デバイスは複製元と同じポリシーで完全メッシュ VPN に追加されます。ポイントツーポイント VPN トポロジのデバイスは複製できません。

ステップ 3 [OK] をクリック複製元のデバイスの複製が、一意の表示名でデバイス セレクタに作成されます。

Security Manager インベントリからのデバイスの削除

あるデバイスをこれ以上 Security Manager で管理しないことにした場合は、そのデバイスをインベントリから削除できます。デバイスを Security Manager から削除しても、デバイスの設定は変更されません。

ヒント そのデバイスに別のユーザがポリシーを設定中であった場合は、ロックが機能してデバイスは削除できません。

デバイスのタイプによっては削除する際に特殊な考慮事項があります。

- デバイスが VPN に参加している場合、デバイスを削除すると VPN からデバイスが削除されます。ただし、デバイスの削除によって VPN トポロジが無効になる場合は、デバイスを削除したときに VPN トポロジ全体も削除されます。このことが警告され、デバイスの削除をキャンセルすることもできます。
- マルチ コンテキスト モードで動作する ASA、PIX、FWSM の各デバイスの場合、または仮想センサーが含まれている IPS デバイスの場合、デバイスを削除するとセキュリティ コンテキストまたは仮想センサーもすべて削除されます。この手順では個々のセキュリティ コンテキストまたは仮想センサーは削除できません。代わりに、目的のセキュリティ コンテキストまたは仮想センサーを削除するように、ホスティング デバイスで適切なポリシーを変更する必要があります。
- 管理対象のサービス モジュールが含まれているデバイスを削除した場合は、その含まれていたデバイスも削除されます。たとえば、FWSM を含めて Catalyst スイッチを追加していた場合に、Catalyst スイッチを削除すると、FWSM も削除されます。含まれているデバイスも削除されることが警告されます。

ヒント デバイスの削除には、データベースから多数の情報を削除する処理が伴います。一度に多数のデバイスを削除すると、処理が完了するまでに時間がかかることがあります。多数のデバイスを削除する場合には、いくつかのグループに分けて削除することを推奨します。

ステップ 1 デバイス ビューで、次のいずれかを実行します。

- 削除するデバイスを選択するか、またはデバイス グループ内のデバイスをすべて削除する場合にはそのグループを選択し、右クリックして、[デバイスの削除（Delete Devices）] を選択します。デバイス

セレクタの上部にある [デバイスの削除（Delete Devices）] ボタン（ゴミ箱アイコン）をクリックすることもできます。

- **[ファイル（File）]>[デバイスの削除（Delete Devices）]** を選択し、[デバイスセレクタ（Device Selector）] ダイアログボックスで削除するデバイスを選択し、[>>] をクリックしてデバイスを選択済みデバイスリストに移動します（リストには、デバイスツリーで選択したデバイスが含まれています）。デバイス グループを選択して、グループのメンバーであるデバイスをすべて削除できます。完了したら、[OK] をクリックします。

ヒント　デバイス グループを選択すると、そのグループ内のデバイスだけが削除され、グループ自体は削除されません。デバイス グループの削除の詳細については、デバイス グループまたはグループ タイプの削除 （169 ページ）を参照してください。

ステップ 2　デバイスを削除するかどうかの確認が求められます。

確認すると、Security Manager はデバイスが削除できるかどうかを検証します。問題または潜在的な問題が明らかになった場合は、その問題が [Device Delete Validation] ダイアログボックス （163 ページ）に記載されます。このダイアログボックスには、（削除できないデバイスを示す）エラーのほか、警告と情報メッセージも表示されます。

警告または情報メッセージがあるデバイスも、メッセージに説明されている結果を受け入れるのであれば削除できます。ダイアログボックスには、選択したすべてのデバイスの削除を続行できる場合は [OK] ボタンが表示され、エラーメッセージがある場合は [続行（Continue）] ボタンが表示されます。[続行（Continue）] をクリックすると、エラー状態でないデバイスだけが削除されます。確認が求められます。

[Device Delete Validation] ダイアログボックス

[Device Delete Validation] ダイアログボックスは、デバイスの削除中に発行されたエラー、警告、および情報メッセージを表示する場合に使用します。デバイスの削除の詳細については、Security Manager インベントリからのデバイスの削除 （162 ページ）を参照してください。

各行が、デバイスを削除しようとしたときに検証で問題が発生したデバイスを表します。表示されるのは、メッセージ重大度アイコン、デバイス表示名、および検証の結果です。検証結果には、デバイスを削除できない理由か、またはデバイスの削除によってもたらされる予期しない結果に関する警告または情報が示されます。メッセージがないデバイスはリストに表示されません。

行をダブルクリックするか、行を選択して [詳細（Details）] ボタンをクリックすると、詳細なメッセージが表示されます。情報がさらに読みやすい形式で [Device Delete Validation Details] ダイアログボックスに表示されます。

メッセージ重大度は次のいずれかになります。

- エラー：デバイスの削除を妨げる問題が検出されました。たとえば、別のユーザがデバイスをロックしています。
- 警告：今後の操作に注意を喚起します。たとえば、デバイスを削除すると、VPN トポロジが無効になり、続行した場合には VPN トポロジも削除されます。

- 情報：小さな問題が発生しています。たとえば、デバイスを削除すると、VPN からデバイスが削除されます。

デバイスの削除を続行するには、[OK] ボタンまたは [Continue] ボタンをクリックします。両者は実質的に同じボタンです。

- [OK] が表示されている場合、このボタンをクリックすると、削除対象に選択したすべてのデバイスが削除されます。
- [続行（Continue）] が表示されている場合、選択したデバイスの中にエラーがあるものがあります。[Continue] をクリックすると、エラーがないデバイスだけが削除されます。

選択したすべてのデバイスにエラーがある場合は、ボタンがグレーになり、[Cancel] をクリックする必要があります。デバイスを削除する前に、エラーを残らず解決します。

ナビゲーション パス

このダイアログボックスが表示されるのは、デバイスを削除しようとしたものの、Security Manager によってその削除に問題があると判断された場合だけです。

デバイス グループの使用

デバイス グループを作成すると、効率よくデバイスを管理できるようにデバイスを編成できます。次の項では、デバイス グループとその使用方法について説明します。

- デバイスのグループ化について （164 ページ）
- デバイス グループ タイプの作成 （167 ページ）
- デバイス グループの作成 （168 ページ）
- デバイス グループまたはグループ タイプの削除 （169 ページ）
- デバイス グループに対するデバイスの追加と削除 （169 ページ）

デバイスのグループ化について

デバイス グループは簡素かつ任意に編成したデバイスの集まりであり、効率よくネットワークを可視化できます。ポリシーを共有するエンティティではありません。各種のポリシー オブジェクト グループ（たとえば AAA サーバ グループ オブジェクトやユーザ グループ オブジェクト）とは異なるものです。ポリシー オブジェクトの詳細については、ポリシー オブジェクトの管理 （287 ページ）を参照してください。

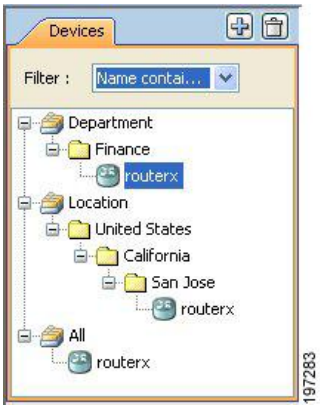
ヒント　デバイスの数が多い場合、グループ化すると、変更をデバイスに展開するときに対象となるデバイスを選択するのが容易になります。たとえば、いくつかのデバイスに同時に変更を展開する場合、それらのデバイスを単一のデバイス グループにまとめておくと、そのグループを選択するだけで展開ジョブを完了できます。ポリシー展開の詳細については、展開の管理 （481 ページ）を参照してください。

デバイスをグループ化すると、インベントリ内のデバイスのサブセットを表示できます。デバイス グループ階層には、次の 2 つのタイプのフォルダがあります。

- デバイス グループ タイプ：グループ タイプが階層の最上位となります。グループ タイプには特定のデバイス グループを含めることができますが、インベントリのすべてのデバイスが含まれる All グループ タイプを除き、デバイスを含めることはできません。Security Manager には、グループ タイプとして Department と Location があらかじめ定義されていますが、必ず使用しなければならないものではなく、削除することもできます。最大 10 個のグループ タイプを作成できます。
- デバイス グループ：デバイス グループは、グループ タイプ フォルダ内のサブフォルダです。複数レベルのネスト デバイス グループを作成できます。デバイス グループ内にデバイスを配置できます。ただし、デバイスを配置できるのはグループ タイプ内の 1 つのグループだけです。たとえば、図 6 : デバイス グループ（Device Groups） では、グループ タイプ Location の下で、routerx を San Jose に割り当てることはできますが、routerx を San Jose と California に割り当てることはできません。

図 6 : デバイス グループ（Device Groups） は、デバイスがいくつかのグループに配置されている、ネストされたデバイスグループの一例を示しています。図を見るとわかるように、1 つのデバイスが複数のグループに存在できます。この例では、routerx が（[Department] グループ タイプの下の）[Finance] グループと、Location > United States > California > San Jose ネスト グループに属しています。これらの所属先のいずれかで routerx を選択した場合、単一のデバイスを設定していることになります（設定は、グループ化とは関連付けられていません）。

図 *6 : デバイス グループ（Device Groups）*



Security Manager では、グループおよびグループ タイプを作成または削除できるほか、インターフェイス内のさまざまな場所でデバイスをグループに配置できます。

- デバイスをインベントリに追加するとき：New Device ウィザードには、[Device Grouping] ページが含まれています。ここでは、デバイス グループ タイプを作成し、新規に追加したデバイスのグループを選択できます。また、デフォルト グループを選択して、そこにすべての新規デバイスを追加することもできます。
- デバイス ビューでデバイス インベントリを表示したとき：[File] > [Edit Device Groups] コマンドを選択すると、ダイアログボックスが開き、グループおよびグループ タイプを作成または削除できます。デバイス セレクタでグループまたはグループ タイプを選択した場合、[File] メニューと右クリックのショートカット メニューにはグループを追加するためのコマンドまたはデバイスをグループに追加するためのコマンドが表示されます。

グループにデバイスを追加したり、グループからデバイスを削除したりするには、グループを選択し、**[ファイル（File）] > [グループへのデバイスの追加（Add Devices to Group）]** を選択します。

- デバイスのプロパティを表示したとき：[Device Grouping] ページでは、デバイスが属するグループを選択し、インベントリに追加したデバイスのデフォルトを設定できます。これは、デバイス グループからデバイスを削除できる唯一の場所となります。デバイス セレクタでデバイスをダブルクリックして、デバイス プロパティを開きます。
- 管理ページを使用しているとき：**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイスグループ（Device Groups）]** を選択して、デバイスグループの管理ページを開きます。ここでは、グループおよびグループタイプを作成または削除できますが、グループにデバイスを追加することはできません。

関連項目

- デバイス グループ タイプの作成 （167 ページ）
- デバイス グループの作成 （168 ページ）
- デバイス グループまたはグループ タイプの削除 （169 ページ）
- デバイス グループに対するデバイスの追加と削除 （169 ページ）

[Edit Device Groups] ダイアログボックス

[Edit Device Groups] ダイアログボックスは、デバイス インベントリに定義されているデバイス グループおよびグループ タイプを管理する場合に使用します。

ナビゲーション パス

次のいずれかを実行します。

- デバイスセレクタでデバイスグループタイプまたはデバイスグループを右クリックし、[デバイスグループの編集（Edit Device Groups）] を選択します。
- **[ファイル（File）] > [デバイスグループの編集（Edit Device Groups）]** を選択します。

- New Device ウィザードの [デバイスのグループ化（Device Grouping）] ページで、または既存のデバイスの場合はデバイスのプロパティで、グループタイプリストから [グループの編集（Edit Groups）] を選択します。 [Device Groups] ページ （148 ページ） を参照してください。

関連項目

- デバイスのグループ化について （164 ページ）
- デバイス グループの使用 （164 ページ）

フィールド リファレンス

表 *27 : [Edit Device Groups]* ダイアログボックス

要素	説明
Groups	デバイス グループとグループ タイプを表示します。 グループ名またはタイプ名を変更するには、グループまたはタイプを選択し、もう一度クリックしてテキストを編集可能にします。新しい名前を入力し、Enter を押します。
[Add Type] ボタン	新しいグループ タイプを作成するには、このボタンをクリックします。タイプはデフォルト名で追加されます。名前を上書き入力し、Enter を押します。 最大 10 個のグループ タイプを設定できます。
[Add Group to Type] ボタン	デバイス グループを選択したデバイス グループまたはグループ タイプに追加するには、このボタンをクリックします。
[Delete] ボタン（ゴミ箱）	選択したデバイス グループまたはグループ タイプとその中に含まれているすべてのデバイス グループを削除するには、このボタンをクリックします。デバイス グループまたはグループ タイプを削除しても、その中に含まれているデバイスは削除されません。

デバイス グループ タイプの作成

この手順では、デバイス グループ タイプを作成する最も直接的な方法について説明します。グループ タイプを追加する他の方法の詳細については、デバイスのグループ化について （164 ページ）を参照してください。

デバイス グループ タイプは、デバイス グループ階層の最上位にあるカテゴリです。デバイス グループを追加する場合は、デバイス グループ タイプの作成 （167 ページ）を参照してください。

関連項目

- デバイスのグループ化について （164 ページ）
- デバイス グループまたはグループ タイプの削除 （169 ページ）
- デバイス グループに対するデバイスの追加と削除 （169 ページ）

ステップ 1 [ファイル（File）] > [デバイスグループの編集（Edit Device Groups）] を選択します。

[Edit Device Groups] ページが開きます（[Edit Device Groups] ダイアログボックス （166 ページ）を参照）。

ステップ 2 [タイプの追加（Add Type）] をクリックします。新規デバイス グループ タイプ エントリがセレクタに追加されます。

ステップ 3 グループタイプの名前を入力し、[入力（Enter）] を押します。

ステップ 4 [OK] をクリックして、[デバイスグループの編集（Edit Device Groups）] ページを閉じます。

デバイス グループの作成

この手順では、デバイス グループを作成する最も直接的な方法について説明します。グループを追加する他の方法の詳細については、デバイスのグループ化について （164 ページ）を参照してください。

デバイス グループはデバイス グループ階層の下位のカテゴリであり、デバイス グループ タイプ（最上位）内または別のデバイス グループ内に追加されます。デバイス タイプ グループを追加する場合は、 デバイス グループ タイプの作成 （167 ページ）を参照してください。

関連項目

- デバイスのグループ化について （164 ページ）
- デバイス グループに対するデバイスの追加と削除 （169 ページ）
- デバイス グループまたはグループ タイプの削除 （169 ページ）

ステップ 1 デバイスセレクタでデバイスグループまたはグループタイプを選択し、[ファイル（File）]>[新規デバイス グループ（New Device Group）] を選択するか、または右クリックして [新規デバイスグループ（New Device Group）] を選択します。

[Add Group] ダイアログボックスが表示されます。

ステップ 2 デバイスグループの名前を入力し、[OK] をクリックします。新規デバイス グループがデバイス セレクタに追加されます。

デバイス グループまたはグループ タイプの削除

不要になったデバイス グループまたはグループ タイプは削除できます。ただし、グループ タイプの中で All グループだけは削除できません。

グループまたはグループ タイプを削除すると、そのグループに含まれるグループが削除されます。ただし、デバイスは削除されません。グループに存在するデバイスはインベントリに残っており、所属先の他のグループに存在していることを確認できます（All グループにはすべてのデバイスがあります）。

デバイス グループおよびグループ タイプを削除するには、さまざまな方法があります。この手順では、最も直接的な方法について説明します。他の方法の詳細については、デバイスのグループ化について （164 ページ）を参照してください。

ステップ 1 [デバイス（Device）] ビューで、[ファイル（File）] > [デバイスグループの編集（Edit Device Groups）] を選択します。[Edit Device Groups] ページが開きます（[Edit Device Groups] ダイアログボックス （166 ページ）を参照）。

ステップ 2 削除するグループタイプまたはグループを選択し、[削除（Delete）]ボタンをクリックします。削除の確認が求められます。

デバイス グループに対するデバイスの追加と削除

デバイス グループにデバイスを追加するには、そのグループを作成する必要があります。グループを作成するには、デバイス グループの作成 （168 ページ）を参照してください。

関連項目

- デバイスのグループ化について （164 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

ステップ 1 デバイスセレクタでデバイスグループを選択し、右クリックし、[グループへのデバイスの追加（Add Devices to Group）] を選択します。[Add Devices to Group] ダイアログボックスが表示されます。

ステップ 2 デバイスをグループに追加するには、使用可能なデバイスセレクタでデバイスを選択し、[>>] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。

デバイスを削除するには、[選択されたデバイス（Selected Devices）] リストでデバイスを選択して、[<<] をクリックします。

ステップ 3 [OK] をクリックデバイス グループ メンバーシップが、[Selected Devices] リストに表示されていたデバイスを含めるように調整されます。

[デバイスステータスビュー（Device Status View）] の使用

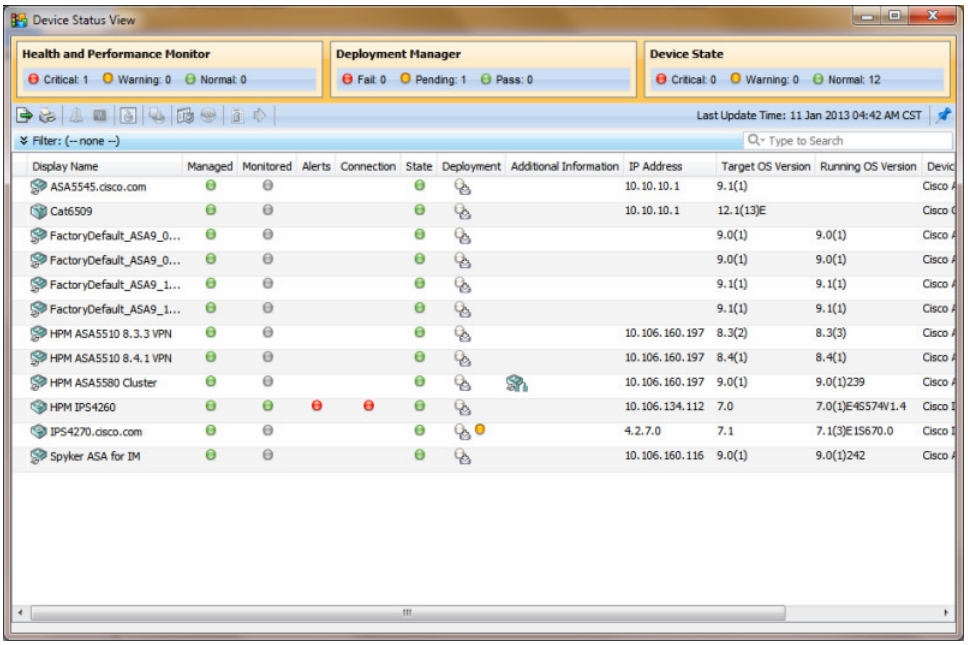
[デバイスステータスビュー（Device Status View）] を使用して、Cisco Security Manager インベントリ内のデバイスのステータスを迅速に確認できます。[デバイスステータスビュー（Device Status View）] ウィンドウには、Cisco Security Manager 内の複数のアプリケーションおよびツールからの情報が集約されています。[デバイスステータスビュー（Device Status View）] を使用して、すべてのデバイスまたは特定のデバイスグループのステータスを迅速に確認し、その情報に基づいて操作する必要がある Cisco Security Manager の領域に簡単に移動できます。

注意 場合によっては、特定のデバイスについて、Health and Performance Monitor に[クリティカル（Critical）]デバイスステータスが表示され、Configuration Manager に [正常（Normal）] デバイスステータスが表示されることがあります。サービスまたはサーバーを再起動しても、この不一致は解消されません。このため、Configuration Manager に加えて HPM でデバイスのステータスを監視する必要があります。

ナビゲーション パス

- [表示（View）] > [デバイスステータスビュー（Device Status View）] を選択します。[デバイスステータスビュー（Device Status View）] ウィンドウが開き、すべてのデバイスの情報が表示されます。
- デバイスセレクタでデバイスグループを選択します。[デバイスステータスビュー（Device Status View）] ウィンドウが開き、そのデバイスグループまたはサブグループの一部であるデバイスの情報が表示されます。

図 *7* : デバイスステータスビュー（***Device Status View***）



フィールド リファレンス

表 *28* : デバイスステータスビュー（***Device Status View***）

要素	説明
[デバイスステータス（Device Status）] の概要ボックス [デバイスステータス（Device Status）] の概要ボックスには、[デバイスステータスビュー（Device Status View）] におけるデバイスの全体的なステータスの概要が表示されます。概要ボックスに表示される数には、現在選択されているデバイスグループ内のデバイスのステータスが反映されています。[表示（View）]>[デバイスステータスビュー（Device Status View）] を選択するか、[すべて（All）] のデバイスグループを選択すると、概要ボックスにすべてのデバイスの数が反映されます。 （注） [デバイスステータスビュー（Device Status View）] ウィンドウでデバイスリストをフィルタリングしても、[デバイスステータス（Device Status）] の概要ボックスのカウントには影響しません。	
[Health and Performance Monitor] 概要ボックス	[クリティカル（Critical）]（赤）、[警告（Warning）]（黄）、および[正常（Normal）]（緑）のアラートステータスのデバイス数を示します。
Deployment Manager の概要ボックス	[失敗（Fail）]（赤）、[保留中（Pending）]（黄）、および[成功（Pass）]（緑）の展開ステータスのデバイス数を示します。

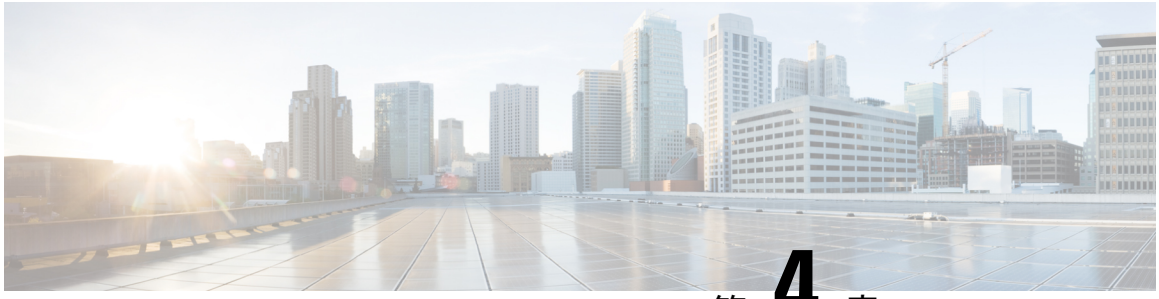
要素	説明
デバイス状態の概要ボックス	[クリティカル（Critical）]（赤）、[警告（Warning）]（黄）、および[正常（Normal）]（緑）のデバイス状態のデバイス数を示します。
[デバイスステータスビュー（Device Status View）] ツールバー [デバイスステータスビュー（Device Status View）] ツールバーには、次のボタンがあります。 （注）　以下のオプションはすべて、デバイスの右クリックメニューからも選択できます。	
	デバイスのステータス情報を PDF ファイルにエクスポートできます。
	デバイスのステータス情報を印刷できます。
	Health and Performance Monitor アプリケーションで選択したデバイスのアラートステータス情報を表示します。 詳細については、ヘルスとパフォーマンスのモニタリング （3611 ページ）を参照してください。
	Health and Performance Monitor アプリケーションで選択したデバイスのモニタリング情報を表示します。 詳細については、ヘルスとパフォーマンスのモニタリング （3611 ページ）を参照してください。
	Deployment Manager を開きます。 詳細については、展開の管理 （481 ページ）を参照してください。
	選択したデバイスの Image Manager アプリケーションを開きます。 詳細については、Image Manager の使用 （3749 ページ）を参照してください。
	選択されているデバイスのデバイスマネージャを開きます。 詳細については、デバイスマネージャの起動 （3697 ページ）を参照してください。
	選択したデバイスの Cisco Prime Security Manager（PRSM）アプリケーションを起動します。詳細については、 Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）を参照してください。

要素	説明
	選択したデバイスの [デバイスのプロパティ（Device Properties）] ダイアログボックスを開きます。詳細については、デバイス プロパティの表示または変更 （136ページ）を参照してください。
	[デバイスステータスビュー（Device Status View）] ウィンドウから選択したデバイスに移動できます。詳細については、デバイス ビューについて （87 ページ）を参照してください。
	現在のページのオンライン ヘルプを開きます。 詳細については、オンライン ヘルプの利用方法 （70 ページ）を参照してください。
	[デバイスステータスビュー（Device Status View）] ウィンドウを切り離すと、ウィンドウを開いた状態で他の製品機能を使用できます。
	[デバイスステータスビュー（Device Status View）] ウィンドウをドッキングします。 （注） デバイスセレクタで選択が変更されている場合、[デバイスステータスビュー（Device Status View）] ウィンドウがドッキングされているときに、現在の選択が作業領域に反映されます。
テーブルフィルタ [デバイスステータスビュー（Device Status View）] テーブルに表示されるデバイスのリストをフィルタ処理して、特定の条件を満たす項目を検索できます。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。	
[デバイスステータス（Device Status）] テーブル	
表示名	デバイスの表示名。これは、Cisco Security Manager デバイスセレクタでの表示に使用される名前であり、デバイスのホスト名と必ずしも同じではありません。
管理対象	Security Manager でデバイスを管理するかどうかを指定します。
監視対象	デバイスが Health and Performance Monitor によって監視されているかどうかを示します。
Alerts	デバイスの現在のアラートレベル（[正常（Normal）]（緑）、[警告（Warning）]（黄）、または [クリティカル（Critical）]（赤））を示します。アラートインジケータにカーソルを合わせると、詳細を表示できます。

要素	説明
Connection	HPM がデバイスに接続可能またはデバイスをポーリング可能かどうかを示します（[接続済み（Connected）]、[認証エラー（Authentication Error）]、[証明書の不一致エラー（Certificate Mismatch Error）]、[接続エラー（Connection error）]、[読み取り操作中のタイムアウト（Timeout during Read operation）]、または [サービスが利用できません（Service unavailable）]）。アラートインジケータにカーソルを合わせると、詳細を表示できます。 （注） デバイスが HPM（[ツール（Tools）] > [デバイスセレクタ（Device Selector）]）で通常または優先監視対象デバイスとして選択されていない場合、このステータスは適用されません。監視対象デバイスの選択に対する変更が有効になり、画面に反映されるまで数分かかる場合があります。
状態	デバイスの現在の状態を示します。アラートインジケータにカーソルを合わせると、詳細を表示できます。 Health and Performance Monitor によって監視されている ASA デバイスの場合、アウトオブバンド変更の可能性が検出されると、[状態（State）] 列にもアラートが表示されます。Health and Performance Monitor でデバイスを監視する前に発生したアウトオブバンド変更は、[状態（State）] 列に反映されません。アウトオブバンド変更の詳細については、アウトオブバンド変更の処理方法について （494 ページ）およびアウトオブバンド変更の検出および分析 （537 ページ）を参照してください。
展開	デバイスの展開方法と現在の展開ステータスを示します。展開ステータスは、[失敗（Fail）]（赤）、[保留中（Pending）]（黄）、および [成功（Pass）]（緑）です。アラートインジケータにカーソルを合わせると、詳細を表示できます。
その他の情報	デバイスの追加情報（デバイスがクラスタモードかどうかなど）を表示します。アラートインジケータにカーソルを合わせると、詳細を表示できます。
IPアドレス	デバイスの管理 IP アドレス。192.168.3.8 など。
Hostname.Domain	デバイスの DNS ホスト名とドメイン名。
ターゲット OS バージョン	デバイスの設定の基となる OS バージョン。
実行中 OS のバージョン	デバイスで実行されているオペレーティングシステムのバージョン。
デバイスタイプ	デバイスのタイプ。

関連項目

- ヘルスとパフォーマンスのモニタリング （3611 ページ）
- Image Manager の使用 （3749 ページ）
- 展開の管理 （481 ページ）



第 4 章

アクティビティの管理

使用しているモードが Workflow モードか Workflow 以外のモードかにかかわらず、すべてのポリシー設定はアクティビティ内部で行われます。アクティビティは、Workflow 以外のモードでは設定セッションとも呼ばれます。Workflow モードでは、アクティビティを明示的に作成および管理する必要があります。これに対し、Workflow 以外のモードでは、アクティビティの作成および管理のほとんどは自動的に行われます。ただし、Workflow 以外のモードでは、ポリシーを変更するときは実際はアクティビティ内部で作業することになるため、アクティビティの基本的な概念を理解しておく必要があります。

チケット管理が有効になっている Workflow 以外のモードでは、チケットを開くたびにアクティビティが自動的かつ透過的に作成されます。このモードでは、チケットを明示的に開いて管理する必要があります。

ここでは、アクティビティに関する情報を提供します。

- アクティビティについて （177 ページ）
- アクティビティ/チケットの操作 （185 ページ）

アクティビティについて

アクティビティとは、ポリシーの定義およびデバイスへの割り当てを行うための一時的なコンテキストです。デバイスをインポート、作成、または削除する場合や、各種のシステム管理タスクを実行する場合は、アクティビティを作成する必要はありません（ただし、アクションの一部としてポリシー ディスカバリを実行する場合を除きます）。

アクティビティを作成または開くための要件は、Workflow モードによって異なります。

- チケット管理が有効になっている Workflow 以外のモード：チケットを開くたびに、アクティビティが自動的かつ透過的に作成されます。チケットを明示的に開かない場合、アクティビティを必要とするアクションを実行するたびに、新しいチケットを作成するか、既存のチケットを開くように要求されます。このモードでは、チケットを明示的に開いて管理する必要があります。
- チケット管理が有効でない Workflow 以外のモード：ポリシーの定義、変更、またはデバイスへの割り当てを行うたびに、アクティビティが自動的かつ透過的に作成されます。変更をデータベースに送信するまでは、同じアクティビティが使用され、必要に応じて自動

的に閉じたり再び開いたりします。Workflow 以外のモードでは、アクティビティを明示的に開いたり管理したりすることはできません。これらのタイプのアクティビティは、設定セッションと呼ばれることもあります。

- Workflow モード：アクティビティを明示的に開かない場合、アクティビティを必要とするアクションを実行すると、新しいアクティビティを作成するか、既存のアクティビティを開くように要求されます。Workflow モードでは、アクティビティを明示的に開いて管理する必要があります。

（注） Workflow モードは、チケット管理が有効か無効かに関係なく、同じように機能します。Workflow モードでチケット管理を有効にすると、アクティビティで使用する [チケット（Ticket）] フィールドが有効になります。チケット ID の入力は必須ではありませんが、使用する場合は、外部の変更管理システムにリンクするように [チケット（Ticket）] フィールドを設定できます。詳細については、「チケット管理」を参照してください。

アクティビティを自分で作成するか、またはアクティビティが自動的に作成されると、Security Managerポリシーデータベースの仮想コピーが開きます。このコピー内でポリシーを定義して割り当てます。このコピー内で行った変更は、コピーの内部でだけ使用可能です。他のユーザが別のアクティビティ内でこれらの変更を表示することはできません。アクティビティが送信されて承認（Workflow モード）されると、このコピー内部の変更がデータベースにコミットされ、他のすべてのユーザが変更を表示できるようになります。そのあと、関連する CLI コマンドを生成してデバイスに展開するための展開ジョブを作成できます。

アクティビティの変更を送信する方法は、Workflow モードによって異なります。

- チケット管理のある Workflow 以外のモード（デフォルト）：**[チケット（Tickets）] > [チケットの送信（Submit Ticket）]** を選択して、変更をポリシーデータベースに送信します。
- チケット管理のない Workflow 以外のモード（デフォルト）：**[ファイル（File）] > [送信（Submit）]** を選択して、変更をポリシーデータベースに送信します。
- Workflow モード：アクティビティアプルーバを使用する場合は、**[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）]** を選択するか、個別のアクティビティアプルーバを使用しない場合は、**[アクティビティ（Activities）]>[アクティビティの承認（Approve Activity）]** を選択します。

ここでは、アクティビティが重要である理由と、Workflow モードでのアクティビティの動作について説明します。

- アクティビティの利点 （179 ページ）
- アクティビティの承認 （179 ページ）
- アクティビティとロッキング （180 ページ）
- アクティビティと複数のユーザ （181 ページ）
- アクティビティ/チケットの状態について （181 ページ）

アクティビティの利点

アクティビティを使用して、ポリシーおよびポリシー割り当てに対して行われる変更を制御します。アクティビティがどのように実装されるかは、選択したワークフロー設定によって異なりますが、すべてのアクティビティに共通して次のような利点があります。

- 監査証跡：アクティビティによって、Security Manager で行われた変更が追跡されます。アクティビティ/チケットのステータスおよび履歴の表示 （207 ページ）で説明しているように、この情報を使用して、どのような変更が誰によって行われたかを判断できます。また、監査レポートの使用 （622 ページ）で説明しているように、Workflow モードと Workflow 以外のモードのどちらにも、アクティビティおよびその他のアクションに可視性を提供するための監査レポートが用意されています。
- 安全性メカニズム：アクティビティは、変更を重ねて実験するための手段を提供します。変更はプライベート データベース ビューに対して行うため、その変更を実装しない場合は、アクティビティまたは設定セッションを廃棄します。詳細については、アクティビティ/チケットの破棄 （205 ページ）を参照してください。
- タスク分離：あるアクティビティ（または設定セッション）内で変更されたポリシーは、別のアクティビティ内で変更されないようにロックされます。このため、変更の競合によりポリシーが不安定になることがありません。詳細については、アクティビティとロッキング （180 ページ）を参照してください。

また、アクティビティ内で行った変更は、そのアクティビティ内部でだけ表示されます。その他のユーザには、最後に承認されたコミット済みの設定だけが表示されます。ただし、（Workflow モードで）アクティビティを閉じる前に他のユーザにアクティビティが表示されていた場合を除きます。

アクティビティの承認

Workflow モードをイネーブルにした場合、アクティビティ アプルーバを使用するかどうかを選択できます。

アクティビティを承認するための上位の権限を持つ別の人が組織に必要な場合は、アプルーバを使用してワークフローをイネーブル化できます。Workflow モードでアプルーバを使用する場合は、ポリシーをデータベースにコミットできるように、適切な権限を持つ人がアクティビティを承認する必要があります。ポリシー定義レベルでこの承認プロセスを使用すると、ネットワーク デバイスに不適切な設定が適用されることはありません。

アプルーバを使用しないように選択した場合は、ポリシーを定義した人がそのポリシーを承認する権限を持ちます。

アクティビティ承認をイネーブルまたはディセーブルにし、デフォルトのアクティビティ アプルーバを変更する方法の詳細については、[Workflow] ページ （745 ページ）を参照してください。

アクティビティとロッキング

複数のユーザが競合する変更を行うことがないように、Workflow モードまたは Workflow 以外のモードでユーザがアクティビティまたは設定セッション内で特定のアクションを実行すると、Security Manager によってアクティビティレベルのロックが取得されます。このため、複数のユーザが同じ機能ポリシー、ポリシー割り当て、またはオブジェクトに対して同時に変更を行うことができなくなります。

また、Security Manager では、ロッキングを使用して、コミット済みの設定に関連する操作が常に互いに排他的に実行されるようにしています。これらの操作は、2 つのカテゴリに分けられます。

コミット済みの設定を変更する操作：

- アクティビティの承認。Workflow以外のモードでの設定セッションの送信が含まれます。
- デバイスの削除。
- デバイス プロパティの編集。

コミット済みの設定を読み込む操作：

- 設定のプレビュー。
- 展開（Workflow 以外のモード）。
- 展開ジョブの作成（Workflow 以外のモード）。
- アクティビティまたは設定セッションの検証。

コミット済みの設定を変更する操作を実行している間は、その操作が完了するまで、他のユーザはどちらのリストの操作も実行できません。ユーザが操作を試行すると、アクションおよびアクティビティ（または Workflow 以外のモードではユーザ）がロックされていることを示すエラー メッセージが表示されます。たとえば、アクティビティを承認している間（Workflow 以外のモードでは、アクティビティが送信されると自動的に実行される）、その承認が完了するまで、他のユーザがデバイスを削除したり、別のアクティビティを検証したりすることはできません。このタイプのロッキングは、コミット済みの設定を複数のユーザが同時に変更することを回避できるため、マルチユーザ設定においては特に重要になります。

コミット済みの設定を読み込む操作を実行している間、コミット済みの設定を変更する操作はだれも実行できません。たとえば、アクティビティを検証している間、別のユーザはアクティビティを承認できません。ただし、設定を読み込む別の操作を他のユーザが実行することはできます。たとえば、アクティビティを検証している間、別のユーザは展開ジョブを作成できます。同様に、展開前に設定をプレビューしている間、別のユーザも同じように設定をプレビューできます。これは、この2つの操作ではコミット済みの設定が読み込まれるだけで、設定が変更されることはないためです。

ヒント　アクティビティ ロッキングの方が、ポリシー ロッキングよりも広範囲です。これについては、ポリシーのロックについて （217 ページ）で説明しています。ポリシー ロッキングにより、2 人のユーザが同じデバイス上の同じポリシーを同時に変更することを回避しています。

関連項目

- アクティビティの承認または拒否（Workflow モード） （203 ページ）
- Security Manager インベントリからのデバイスの削除 （162 ページ）
- デバイス プロパティの表示または変更 （136 ページ）
- 展開および Configuration Archive の使用 （511 ページ）
- アクティビティ/チケットの検証 （200 ページ）

アクティビティと複数のユーザ

各アクティビティ内でポリシーを同時に定義または変更できるのは、1 人のユーザだけです。ただし、Workflow モードがイネーブルになっている場合、または Workflow 以外のモードでチケット管理がイネーブルになっている場合は、アクティビティ内で複数のユーザーが順番に作業できます。つまり、アクティビティまたはチケットが閉じている（ただし、承認はされておらず、承認のための送信もされていない）場合は、別のユーザーがそのアクティビティを開いて変更できます（必要な権限を持っている場合）。複数のユーザは、異なるアクティビティで並行して作業できます。

アクティビティ/チケットの状態について

Workflow モードでのアクティビティと Workflow 以外のモードでのチケット（チケット管理が有効な場合）の状態について、次の表で説明します。主要な状態は太字で示しています。

表 *29*：アクティビティ/チケットの状態

状態	説明
Edit	アクティビティ/チケットは作成されましたが、現在編集中ではありません。アクティビティ/チケットは、[編集（Edit）]状態のとき、開いたり破棄したりできます。

状態	説明
Edit Open	アクティビティ/チケットは編集用に開かれています。アクティビティ/チケット内で、ポリシーの定義や割り当てなどの変更を実行できます。アクティビティ/チケット内で設定中または変更中のポリシー、ポリシー割り当て（ポリシーを割り当てるデバイス）、およびオブジェクトは、ロックされます。つまり、これらを別のアクティビティ/チケットのコンテキスト内で設定または変更することはできません。アクティビティは、[編集がオープン（Edit Open）] 状態のとき、閉じる、破棄、送信、または承認できます。チケットは、[編集がオープン（Edit Open）] 状態のとき、閉じる、破棄、または送信できます。 設定の変更は、アクティビティ/チケットのコンテキストでのみ確認できます。
送信済み（Submitted） Submitted Open	アクティビティが確認および承認のために送信されたか、またはチケットが送信されました（Workflow モードでは、アクティビティ承認が必要な場合だけこの状態を使用できます。詳細については、[Workflow] ページ（745 ページ）を参照してください）。アクティビティ/チケット内でこれ以上変更することはできません。ポリシー、（ポリシー割り当てを介する）デバイス、またはポリシー変更の影響を受けるオブジェクトは、他のアクティビティ/チケットに対してロックされたままになります。 アクティビティが送信されると、電子メールがアプルーバに送信されます。アプルーバは、アクティビティを（読み取り専用モードで、[Submitted Open] 状態に移行して）開いて、アクティビティ内の変更を確認してから、変更を承認または拒否できます。承認されたアクティビティは、[Approved] 状態に移行します。拒否されたアクティビティは、[Edit] 状態に戻ります。
承認済み（Approved）（Workflow モードのみ）	アクティビティは承認され、対応する設定要素がコミット済みのポリシー設定となりました。ポリシー変更の影響を受けるデバイスは、他のアクティビティに対してロック解除されます。アクティビティは、[承認済み（Approved）] 状態のときに展開できます。
承認失敗（Approve Failed）（Workflow モードのみ）	承認中に（電源障害などにより）エラーが発生すると、アクティビティは [Approve Failed] 状態になります。この場合は、アクティビティを再び承認するか、サーバをリブートしてください。
破棄（Discarded）	アクティビティ/チケットの作成後にアクティビティ/チケットに対して行われた変更は破棄され、アクティビティ/チケットをそれ以上変更することはできません。アクティビティ/チケットに関連付けられているデバイスはロック解除され、新しいアクティビティ/チケットで使用できるようになります。アクティビティ/チケットは、システムから削除されないかぎりテーブルに残り、[破棄（Discarded）] 状態が表示されます。

図 8 : チケットのワークフロー （183 ページ）は、チケットワークフローの段階を示しています。図 9 : アプルーバを使用しないアクティビティ ワークフロー （184 ページ）は、アプルーバを使用しないアクティビティワークフローの段階を示しています。図 10 : アプルーバを使用するアクティビティ ワークフロー （185 ページ）は、アプルーバを使用するアクティビティワークフローの段階を示しています。

図 *8 :* チケットのワークフロー

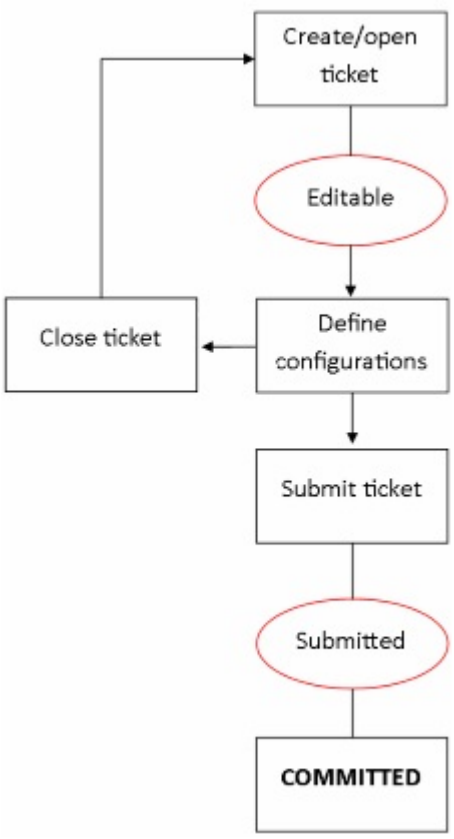


図 *9:* アプルーバを使用しないアクティビティ ワークフロー

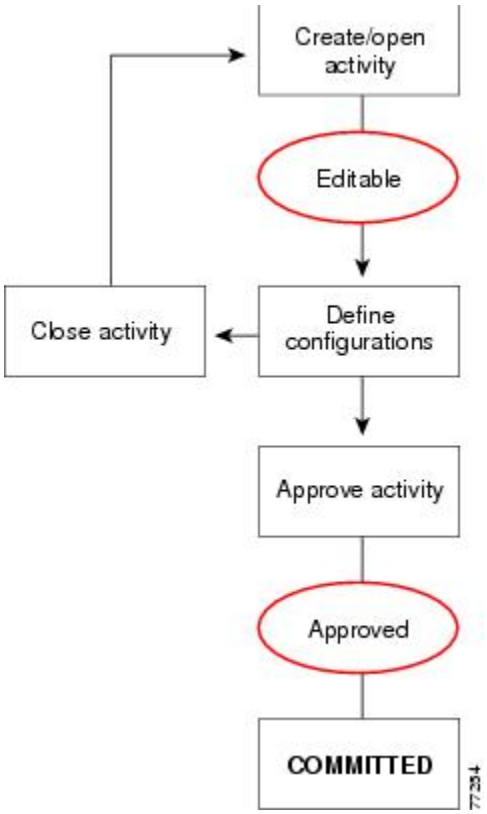
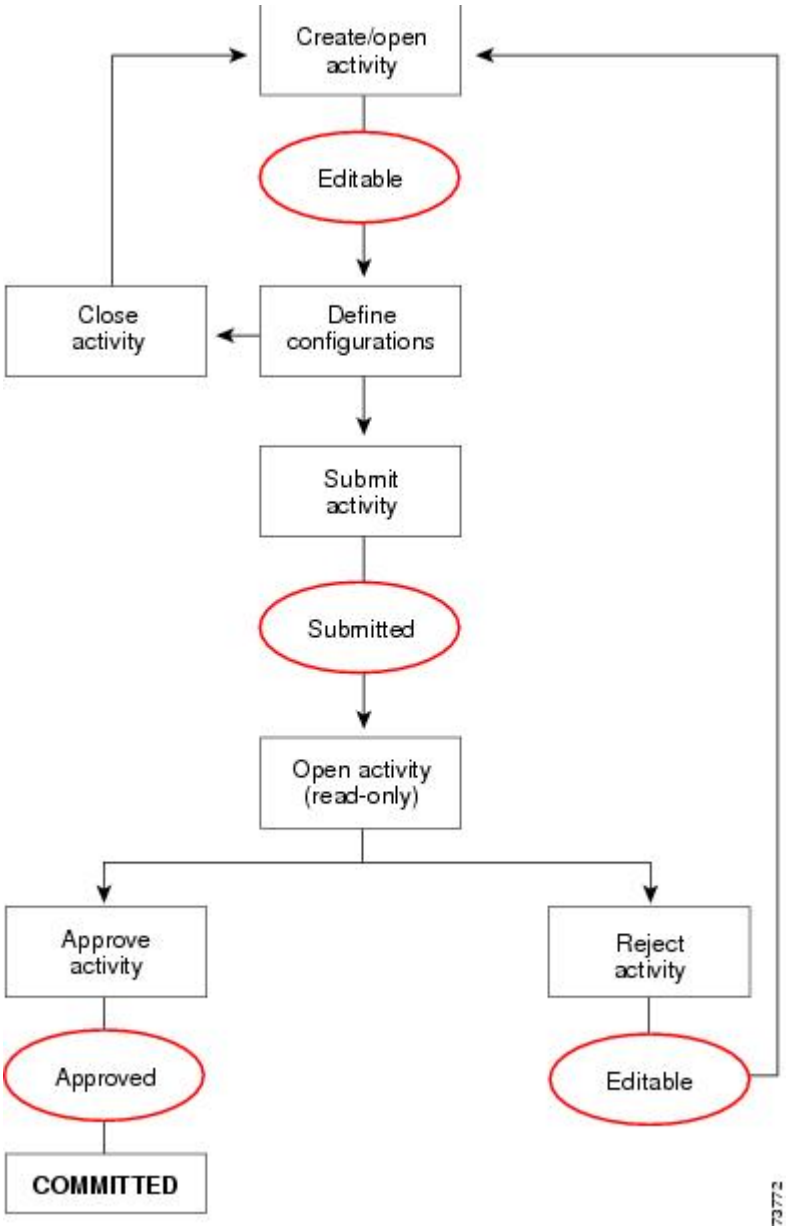


図 *10* : アプルーバを使用するアクティビティ ワークフロー



アクティビティ/チケットの操作

ここでは、アクティビティおよび設定セッションを使用する際に役立つ情報を提供します。

- Workflow モードでのアクティビティ機能へのアクセス （186 ページ）
- Workflow 以外のモードでのチケット機能へのアクセス （188 ページ）
- アクティビティ/チケットの作成 （193 ページ）

- アクティビティ/チケットを開く （195 ページ）
- アクティビティ/チケットを閉じる （196 ページ）
- 変更レポートの表示 （197 ページ）
- アクティビティ/チケットの検証 （200 ページ）
- 承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） （202 ページ）
- アクティビティの承認または拒否（Workflow モード） （203 ページ）
- アクティビティ/チケットの破棄 （205 ページ）
- アクティビティ/チケットのステータスおよび履歴の表示 （207 ページ）

Workflow モードでのアクティビティ機能へのアクセス

Workflow モードでは、次の方法でアクティビティ管理機能にアクセスできます。

- **[管理（Manage）] > [アクティビティ（Activities）]** を選択します。[Activity Manager] ウィンドウに、既存のアクティビティとその状態が一覧表示されます。このウィンドウから、新しいアクティビティを作成したり、既存のアクティビティの開閉、送信、承認、拒否、または廃棄を行ったりできます。詳細については、アクティビティ/チケット マネージャ ウィンドウ （189 ページ）を参照してください。
- メイン ツールバーの [Activities] 部分にあるボタンをクリックするか、[Activities] メニューで対応するコマンドを選択します。ボタンまたはコマンドがアクティブになるかどうかは、ユーザの権限、アクティビティの状態、およびワークフローでアプルーバを使用しているかどうかによって決まります。次の表に、ボタン、コマンド、およびそれを使用できる条件について説明します。

（注） アクティビティが開いている場合、Configuration Manager インターフェイスの右上隅にある [グローバル検索（Global Search）] の上にアクティビティ名が表示されます。アクティビティ名をクリックすると、[Activity Manager] ウィンドウが開きます。

表 *30 : Workflow* モードがイネーブルになっているときの *[Activities]* ツール バーのボタンおよびコマンド

ボタン	[Activities] メニュー コマンド	説明
	New Activity	アクティビティを作成します。

ボタン	[Activities] メニュー コマンド	説明
	Open Activity	アクティビティを開きます。アクティビティは、[Edit] または [Submitted] 状態にある場合に開くことができます。 送信済みのアクティビティを開くには、そのアクティビティで行った変更を承認または拒否するためのユーザ権限を持っている必要があります。詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。
	Close Activity	アクティビティが開いている間に行われた変更をすべて保存し、アクティビティを閉じます。 アクティビティは、[Edit Open] または [Submit Open] 状態のときに閉じることができます。
	変更の表示	アクティビティで行われたすべての変更を評価し、PDF 形式のアクティビティ変更レポートを別のウィンドウ内に生成します。詳細については、変更レポートの表示 （197 ページ）を参照してください。
	Validate Activity	現在のアクティビティ内で変更されたポリシーの整合性を検証します。アクティビティを検証することにより、ポリシー変更の際の設定エラーをチェックできます。
	Submit Activity	アクティビティ アプルーバを使用する Workflow モードで、アクティビティを承認のために送信します。アクティビティは、[Edit] または [Edit Open] 状態にある場合に送信できます。
	Approve Activity	アクティビティ内で提案された変更を承認します。 アクティビティは、アクティビティ アプルーバを使用している場合は [Submitted] 状態のときに承認できます。アプルーバを使用していない場合は [Edit] または [Edit Open] 状態のときに承認できます。アクティビティ内で提案された変更を受け入れるためのユーザ権限を持っている必要があります。詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。
	Reject Activity	アクティビティ アプルーバを使用する Workflow モードで、アクティビティ内で提案された変更を拒否します。 アクティビティは、[Submitted] または [Submitted Open] 状態のときに拒否できます。アクティビティ内で提案された変更を拒否するためのユーザ権限を持っている必要があります。詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

ボタン	[Activities] メニュー コマンド	説明
	Discard Activity	選択したアクティビティを廃棄します。アクティビティは廃棄され、[Tools] > [Security Manager Administration] > [Workflow] で設定したアクティビティの経過時間を超えるとシステムから削除されます。アクティビティが実際にシステムから削除されるまでは、アクティビティ状態は [Discarded] として表示されます。

Workflow 以外のモードでのチケット機能へのアクセス

チケット管理が有効になっている Workflow 以外のモードでは、次の方法でチケット管理機能にアクセスできます。

- **[管理（Manage）] > [チケット（Tickets）]** を選択します。[チケットマネージャ（Ticket Manager）] ウィンドウには、既存のチケットとチケットの状態のリストが含まれています。このウィンドウから、新しいチケットを作成したり、既存のチケットを開閉、送信、または破棄したりできます。詳細については、アクティビティ/チケット マネージャ ウィンドウ （189 ページ）を参照してください。
- [メイン（Main）] ツールバーの [チケット（Tickets）] 部分にあるボタンをクリックするか、[チケット（Tickets）] メニューで対応するコマンドを選択します。ボタンやコマンドのアクティブ状態は、ユーザーのアクセス許可とチケットの状態によって異なります。次の表に、ボタン、コマンド、およびそれを使用できる条件について説明します。

（注） チケットが開いている場合、チケット ID は、Configuration Manager インターフェイスの右上隅にある [グローバル検索（Global Search）] フィールドの上に表示されます。チケット ID をクリックして、[チケットマネージャ（Ticket Manager）] ウィンドウを開くことができます。

表 *31 : Workflow* 以外のモードでチケット管理が有効になっている場合の *[チケットツールバー（Tickets Tool Bar）]* のボタンとコマンド

ボタン	[Activities] メニュー コマンド	説明
	新しいチケット（New Ticket）	チケットを作成します。
	チケットを開く（Open Ticket）	チケットを開きます。[編集（Edit）] 状態のチケットを開くことができます。

ボタン	[Activities] メニュー コマンド	説明
	チケットを閉じる（Close Ticket）	チケットが開いている間に行われた変更をすべて保存し、チケットを閉じます。 [編集オープン（Edit Open）] 状態のチケットを閉じることができます。
	変更の表示	チケットで行われたすべての変更を評価し、PDF 形式のチケット変更レポートを別のウィンドウ内に生成します。詳細については、変更レポートの表示 （197 ページ）を参照してください。
	チケットの検証（Validate Ticket）	現在のチケット内で変更されたポリシーの整合性を検証します。チケットを検証することで、ポリシー変更の際の設定エラーをチェックできます。
	チケットの送信（Submit Ticket）	チケットを送信します。チケットを送信すると、提案された変更がデータベースに保存されます。チケットに関連付けられたデバイスはロック解除されるため、ポリシー定義に含めたり、他のチケットで変更したりできます。チケットは、[編集（Edit）] 状態または [編集オープン（Edit Open）] 状態にある場合に送信できます。
	チケットを破棄（Discard Ticket）	選択したチケットを破棄します。チケットは破棄され、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [チケット管理（Ticket Management）]** で設定したチケットの経過時間を超えるとシステムから削除されます。チケットが実際にシステムから削除されるまで、チケットの状態は [破棄（Discarded）] と表示されます。詳細については、[チケット管理（Ticket Management）] ページ （740 ページ）を参照してください。

アクティビティ/チケット マネージャ ウィンドウ

アクティビティ管理とチケット管理は非常によく似たプロセスです。アクティビティとチケットの主な違いは、チケットは承認プロセスを使用しないことです。さまざまな動作モードの比較については、Workflow モードの比較 （29 ページ）を参照してください。

- Activity Manager：[Activity Manager] ウィンドウを使用して、アクティビティの作成と管理、およびアクティビティのステータスと履歴の表示を行います。上半分のペインに、作成されたアクティビティが一覧表示されます。アクティビティを選択すると、下半分のペインにそのアクティビティの詳細と履歴が表示されます。
- Ticket Manager：[Ticket Manager] ウィンドウを使用して、チケットの作成と管理、およびチケットのステータスと履歴を表示します。上半分のペインに、作成されたチケットが一

覧表示されます。チケットを選択すると、下半分のペインにそのチケットの詳細と履歴が表示されます。

（注） [Activity Manager] ウィンドウは、Workflow モードで作業している場合だけ使用可能です。[Ticket Manager] ウィンドウは、チケット管理が有効になっている Workflow 以外のモードを運用している場合にのみ使用できます。チケット管理が有効でない Workflow 以外のモードでは、Security Manager によって自動的かつ透過的にアクティビティが管理されます。モードの選択の詳細については、ワークフロー モードの変更 （36 ページ）を参照してください。

ナビゲーション パス

- チケット管理が有効になっている Workflow 以外のモードでは、[メイン（Main）] ツールバーの [Ticket Manager] ボタンをクリックするか、**[管理（Manage）]>[チケット（Tickets）]** を選択します。
- Workflow モードでは、[メイン（Main）] ツールバーで [Activity Manager] ボタンをクリックするか、**[管理（Manage）] > [アクティビティ（Activities）]** を選択します。

フィールド リファレンス

表 *32*：アクティビティ/チケット マネージャ ウィンドウ

要素	説明
*	未承認の変更がある（編集、編集がオープン、または送信済みの状態）アクティビティ、または未送信の変更がある（編集または編集がオープンの状態）チケットには、簡単に識別できるようにフラグが付けられます。
アクティビティ チケット（Ticket）	アクティビティの名前またはチケットの ID。Workflow モードでチケット管理が有効になっている場合、両方の列が表示されます。 チケット管理が有効になっている場合、チケット ID をクリックしてチケットの詳細を表示できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
最終変更日（Last Modified）	アクティビティ/チケットが最後に変更された日時。
状態	アクティビティ/チケットの状態。状態のリストについては、アクティビティ/チケットの状態について （181 ページ）を参照してください。

要素	説明
ユーザー（User）	アクティビティ/チケットの状態を最後に変更したユーザーの名前。
直前のアクション	アクティビティ/チケットに対して実行された最新のアクション。
[Create] ボタン	このボタンをクリックすると、新しいアクティビティまたはチケットが作成され、ポリシーの作成や変更、またはデバイスへのポリシーの割り当てができるようになります。詳細については、アクティビティ/チケットの作成 （193 ページ）を参照してください。
[Open] ボタン	このボタンをクリックすると、選択したアクティビティ/チケットが開き、アクティビティ/チケット内から変更（ポリシーの定義や割り当てなど）が取り込まれます。アクティビティは、[Edit] または [Submitted] 状態にある場合に開くことができます。送信済みのアクティビティは、読み取り専用で開かれます。[編集（Edit）] 状態のチケットを開くことができます。詳細については、アクティビティ/チケットを開く （195 ページ）を参照してください。
[Close] ボタン	後でポリシーの設定を続行する場合は、このボタンをクリックして、選択したアクティビティ/チケットを閉じます。詳細については、アクティビティ/チケットを閉じる （196 ページ）を参照してください。
[Validate] ボタン	このボタンをクリックして、選択したアクティビティ/チケットを作成してから現在の時刻までに行った変更を検証します。アクティビティ/チケットを検証すると、ポリシーの整合性と展開可能性がチェックされ、エラーが検出された場合は詳細なエラー情報が表示されます。詳細については、アクティビティ/チケットの検証 （200 ページ）を参照してください。
\[Submit\] ボタン [Submitぼたん]	アクティビティ アプルーバを使用する Workflow モードで、このボタンをクリックして、選択したアクティビティを送信します。アクティビティを送信すると、指定したアプルーバに、アクティビティの確認の準備ができたという通知が送信されます。アクティビティは、[Edit] または [Edit Open] 状態にある場合に送信できます。 チケット管理が有効になっている Workflow 以外のモードでは、このボタンをクリックすると、選択したチケットが送信されます。チケットを送信すると、提案された変更がデータベースに保存されます。チケットに関連付けられたデバイスはロック解除されるため、ポリシー定義に含めたり、他のチケットで変更したりできます。チケットは、[編集（Edit）] 状態または [編集オープン（Edit Open）] 状態にある場合に送信できます。 コメントの入力を求められます。詳細については、承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード）（202 ページ）を参照してください。

要素	説明
[Approve] ボタン（Activity Manager のみ）	このボタンをクリックすると、選択したアクティビティが承認され、提案された変更がデータベースに保存されます。アクティビティに関連付けられたデバイスはロック解除されるため、ポリシー定義に含めたり、他のアクティビティで変更したりできます。アクティビティを承認するための適切なユーザ権限を持っている必要があります。 アプルーバを使用しない Workflow モードでは、各自のアクティビティを [Edit] 状態のときに承認できます。アプルーバを使用する Workflow モードでは、アクティビティを送信する必要があります。アプルーバがアクティビティを承認できるのは、アクティビティが [Submitted] 状態のときだけです。 承認コメントの入力を求められます。詳細については、アクティビティの承認または拒否（Workflow モード） （203 ページ）を参照してください。
[Reject] ボタン（Activity Manager のみ）	アクティビティアプルーバを使用する Workflow モードで、このボタンをクリックして、選択したアクティビティで提案された変更を拒否します。アクティビティを拒否するための適切なユーザ権限を持っている必要があります。アクティビティが拒否された場合、送信者はアクティビティの変更を続行できます。アクティビティに関連付けられたデバイスはロック解除されないため、ポリシー定義に含めたり、他のアクティビティで変更したりできません。アクティビティは、[Submitted] または [Submitted Open] 状態のときだけ拒否できます。 拒否コメントの入力を求められます。詳細については、アクティビティの承認または拒否（Workflow モード） （203 ページ）を参照してください。
[Discard] ボタン	このボタンをクリックして、選択したアクティビティ/チケットを破棄します。このアクティビティ/チケットと関連付けられているデバイスはロック解除され、他のアクティビティ/チケットで使用できるようになります。複数のアクティビティ/チケットを同時に破棄できます。 コメントの入力を求められます。詳細については、アクティビティ/チケットの破棄 （205 ページ）を参照してください。 廃棄されたアクティビティは、Security Manager の Workflow 設定で定義されている設定に従って、システムから削除されます。アクティビティがシステムから削除されるまでは、アクティビティ状態は [Discarded] として表示されます。詳細については、[Workflow] ページ （745 ページ）を参照してください。 廃棄されたチケットは、Security Manager のチケット管理設定で定義されている設定に従って、システムから削除されます。チケットがシステムから削除されるまで、チケットの状態は [破棄（Discarded）] と表示されます。詳細については、[チケット管理（Ticket Management）] ページ （740 ページ）を参照してください。

要素	説明
変更の表示	このボタンをクリックして、選択したアクティビティ/チケットのレポートを PDF 形式で生成します。アクティビティ/チケットが閉じている場合、このボタンはグレー表示されます。詳細については、変更レポートの表示（197 ページ）を参照してください。
[Refresh] ボタン	このボタンをクリックして、ウィンドウに表示されている情報をリフレッシュします。
[Details] タブ	選択したアクティビティ/チケットの詳細情報が表示されます。詳細には、テーブルから繰り返される情報の他に、次の情報が含まれます。 • [Activity ID]：アクティビティを作成したときに Security Manager によって割り当てられた識別番号。 • [チケット ID（Ticket ID）]：チケットの作成時に入力された識別番号。チケット ID の横にある [チケットの編集（Edit Ticket）] ボタンをクリックして、チケット ID を編集できます。 • [作成日時（Created）]：アクティビティ/チケットが作成された日時。 • [最終変更日（Last Modified）]：アクティビティ/チケットが最後に変更された日時。 • [説明（Description）]：アクティビティ/チケットが作成されたときに入力された説明。 • [コメント履歴（Comments History）]：このアクティビティ/チケットに入力されたコメントの履歴を表示します。コメントを入力したユーザーと、コメントが入力された日時が表示されます。コメント履歴テーブルの下にあるボタンを使用すると、コメントを追加および編集できます。
[履歴（History）] タブ	選択したアクティビティ/チケットに行われた変更のログが表示されます。ログの内容は、状態の変更、変更を行ったユーザ、変更日時（Security Manager サーバの時間が基準）、およびユーザが入力した変更を説明するコメントです。

アクティビティ/チケットの作成

Workflow モードでは、ポリシーを作成する前、またはデバイスにポリシーを割り当てる前に、アクティビティを作成する必要があります。Workflow 以外のモードでは、チケット管理が有効になっている場合、ポリシーを作成または変更するかデバイスにポリシーを割り当てる前に、チケットを作成する必要があります。

ヒント　Workflow 以外のモードでチケットが無効になっている場合は、必要に応じてアクティビティが自動的に作成されます。

関連項目

- アクティビティについて　（177 ページ）
- アクティビティ/チケットを開く　（195 ページ）

ステップ 1　次のいずれかを実行します。

アクティビティの場合：

- アクティビティツールバーで [アクティビティの作成（Create Activity）] ボタンをクリックします。
- [アクティビティ（Activities）] > [新規アクティビティ（New Activity）] を選択します。
- [Activity Manager] ウィンドウで [作成（Create）] をクリックします。

チケットの場合：

- チケットツールバーで [チケットの作成（Create Ticket）] ボタンをクリックします。
- [チケット（Tickets ）] > [新規チケット（New Ticket）] を選択します。
- [Ticket Manager] ウィンドウで [作成（Create）] をクリックします。

[アクティビティ/チケットの作成（Create Activity/Ticket）] ダイアログボックスが表示されます。

ステップ 2　[アクティビティ/チケットの作成（Create Activity/Ticket）] ダイアログボックスで、アクティビティの名前を入力するか、システムにより生成された名前を保持します。デフォルトの名前には、ユーザー名、日付、およびアクティビティ/チケットの作成時刻が含まれます。また、アクティビティ/チケットを説明するコメントも入力できます。

[チケットの管理（Ticket Management）] では、チケット ID と外部チケット管理システムの間のリンクがサポートされます。詳細については、[チケット管理（Ticket Management）] ページ　（740 ページ）を参照してください。

ヒント　カンマを使用して、複数のチケット ID を区切ることができます。

ステップ 3　[OK] をクリック

アクティビティ/チケットが [Activity Manager]/[Ticket Manager] ウィンドウにリストされます。詳細については、アクティビティ/チケット マネージャ ウィンドウ　（189 ページ）を参照してください。

[必要なアクティビティ/チケットへの応答（Responding to the Activity/Ticket Required）] ダイアログボックス

Workflow モードでは、ポリシーを作成または変更する前に、アクティビティを作成するか開く必要があります。Workflow 以外のモードで、チケット管理が有効になっている場合は、ポリシーを作成または変更する前にチケットを作成するか開く必要があります。アクティビティ/チケットを作成しても開いてもいない状態で、アクティビティまたはチケットを必要とするアクションを実行しようとすると、[必要なアクティビティ/チケット（Activity/Ticket Required）] ダイアログボックスで、それを実行するよう促されます。

次のオプションの中から選択できます。

- [新規アクティビティを作成（Create a new activity）]：全く新しいアクティビティ/チケットを作成し、アクティビティ名またはチケット ID を指定し、任意でアクティビティ/チケットの目的の説明を入力します。デフォルトのアクティビティ/チケットの名前には、ユーザー名、日付、およびアクティビティ/チケットの作成時刻が含まれます。
- [既存のアクティビティ/チケットを開く（Open an existing activity/ticket）]：[アクティビティ/チケット（Activity/Ticket）] リストから選択したアクティビティ/チケットを開きます。このオプションは、編集状態の使用可能なアクティビティ/チケットがある場合にだけ表示されます。

関連項目

- アクティビティ/チケットの作成　（193 ページ）
- アクティビティ/チケットの状態について　（181 ページ）

アクティビティ/チケットを開く

Workflow モードでは、他のユーザが開いていない既存のアクティビティを開くことができます。[Edit] 状態の既存のアクティビティを開いて、さらにポリシーを変更したり、[Submitted] 状態の既存のアクティビティを開いて、提案されたポリシー変更を承認または拒否する前に確認したりできます（適切な権限を持っているユーザが、アプルーバを使用する Workflow モードで作業している場合）。

[編集（Edit）] 状態のアクティビティは変更できますが、[送信済み（Submitted）] 状態のアクティビティは表示しかできません。

Workflow 以外のモードでは、チケット管理が有効になっている場合、他のチケットが開かれていないときに、既存のチケットを開いてポリシーをさらに変更できます。

アクティビティ/チケットを開くには、次のいずれかを実行します。

- アクティビティの場合：
  - アクティビティツールバーで [開く（Open）] ボタンをクリックするか、[アクティビティ（Activities）]>[アクティビティを開く（Open Activity）] を選択します。[Openable Activities] ダイアログボックスに、開くことができるすべてのアクティビティが一覧

表示されます。また、アクティビティの名前、その状態、およびアクティビティを作成したユーザ名も表示されます。開くアクティビティを選択し、[OK] をクリックします。

- [管理（Manage）] > [アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウから、開くアクティビティを選択し、[開く（Open）] をクリックします。

- チケットの場合：
  - チケットツールバーの [開く（Open）] ボタンをクリックするか、[チケット（Tickets）] > [チケットを開く（Open Ticket）] を選択します。[開くことができるチケット（Openable Tickets）] ダイアログボックスには、チケット ID、状態、チケット作成者のユーザー名などの情報を含めて、開くことができるすべてのチケットが一覧表示されます。開くチケットを選択し、[OK] をクリックします。
  - [管理（Manage）] > [チケット（Tickets）] を選択します。[Ticket Manager] ウィンドウから、開くチケットを選択し、[開く（Open）] をクリックします。

ヒント Workflow 以外のモードで、チケット管理が無効になっている場合、必要に応じて（まだ送信していない）直前の設定セッションが開かれます。アクティビティを必要とするアクションを次に実行するときに、新しいアクティビティが作成されます。

（注） Workflow モードおよびチケット管理が有効になっている非 Workflow モードでは、Security Manager を起動すると、アクティビティ/チケットを開くか作成するように求められます。

関連項目

- アクティビティについて （177 ページ）

アクティビティ/チケットを閉じる

あとで引き続きポリシーを設定できるように、アクティビティを承認なしで（または承認のために送信せずに）閉じる、またはチケットを送信せずに閉じることができます。

管理者権限を持つユーザは、別のユーザが開いたアクティビティ/チケットを閉じることができます。

開いているアクティビティ/チケットを閉じるには、次のいずれかを実行します。

- アクティビティの場合：
  - アクティビティツールバーで [閉じる（Close）] ボタンをクリックします。

- [アクティビティ（Activities）] > [アクティビティを閉じる（Close Activity）] を選択します。
- [管理（Manage）] > [アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウから、[閉じる（Close）] をクリックします。

- チケットの場合：
  - チケットツールバーで [閉じる（Close）] ボタンをクリックします。
  - [チケット（Tickets ）] > [チケットを閉じる（Close Ticket ）] を選択します。
  - [管理（Manage）] > [チケット（Tickets）] を選択します。[Ticket Manager] ウィンドウから、[閉じる（Close）] をクリックします。

ヒント　チケット管理が無効の Workflow 以外のモードでは、ログアウトするたびに設定セッションが閉じます。次回ログインすると、同じセッションが再び開きます。

関連項目

- アクティビティについて （177 ページ）

変更レポートの表示

インターフェイス内には、変更レポートを開ける場所が多数あります。通常、レポートを生成するためのボタンまたはコマンドは、[変更の表示（View Changes）] です。これらの変更レポートは、Workflow モードか Workflow 以外のモードのいずれを使用しているかにかかわらず、ポリシーおよびポリシーオブジェクトの変更や、操作が実行されたデバイス、アクティビティ/チケット内で作成されたデバイスに関する詳細情報を提供します。

変更レポートは、Adobe Acrobat（PDF）形式です。[bookmarks] タブを含むすべての Acrobat 機能を使用して、レポートを表示できます。

デバイスを検出した場合、またはデバイス上のポリシーを再検出した場合、同じアクティビティ/チケット内でそのデバイスに対してそれ以降に実行されたポリシー変更は、アクティビティ変更レポートに一覧表示されません。これは、別のデバイスから複製したデバイスについても当てはまります。

変更レポートを表示するための方法を次に示します。

- チケット管理のある Workflow 以外モード：
  - [チケット（Tickets）] > [変更の表示（View Changes）] を選択するか、ツールバーで [変更の表示（View Changes）] ボタンをクリックすると、現在開いているチケット内で行われた変更が表示されます。

- [チケットマネージャ（Ticket Manager）] ウィンドウでチケットを強調表示し、[変更の表示（View Changes）] をクリックして、そのチケットに行われた変更を表示します。

- チケット管理のない Workflow 以外モード：
  - [ファイル（File）>[変更の表示（View Changes）] を選択すると、現在の設定セッション中に行われた変更が表示されます。
  - [管理（Manage）] > [レポートの変更（Change Reports）] を選択すると、以前のセッション中に行われた変更が表示されます（これらのセッションは、変更を送信するか廃棄すると閉じます）。[レポートの変更（Change Report）] ウィンドウから設定セッションを選択し、[変更の表示（View Changes）] をクリックします（チケット管理が無効になっている Workflow 以外のモードでの変更レポートの選択 （200 ページ） を参照。）

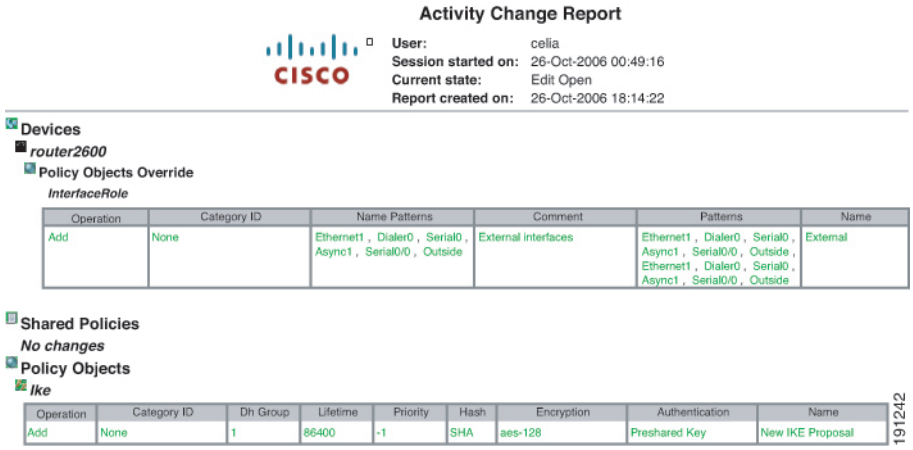
- Workflow モード：
  - [アクティビティ（Activities）] > [変更の表示（View Changes）] を選択するか、ツールバーで [変更の表示（View Changes）] ボタンをクリックすると、現在開いているアクティビティ内で行われた変更が表示されます。
  - [アクティビティマネージャ（Activity Manager）] ウィンドウでアクティビティを強調表示し、[変更の表示（View Changes）] をクリックすると、そのアクティビティ内で行われた変更が表示されます。

- すべてのモードで、展開ジョブを作成するときに、さまざまなダイアログボックスから変更を表示できます。

（注） アクティビティ レポートが確実に開くように、ポップアップブロッカ アプリケーションが実行されていればそれをディセーブルにする必要があります。

次の図に、アクティビティ レポートの例を示します。

図 *11 : Activity Change Report*



変更レポートには、次の要素が含まれます。

- [Activity name/Ticket ID]：アクティビティの名前（名前がない場合は、ユーザおよびセッションの開始日時）またはチケット ID。
- [Created by]：アクティビティ/チケットを作成したユーザ名、および日時。
- [Current state]：アクティビティの現在の状態。
- [Report created on]：レポートが作成された日時。
- [Devices section]：アクティビティ/チケット内で操作が実行されたデバイス（つまり、追加、変更、または削除されたデバイス）の要約。ローカルポリシーに対する変更は、ここに表示されます。

レポートのこのセクションおよび他のセクションの中の変更は、区別しやすいように色分けされます。

- 緑：新しく挿入された項目を示します。
- 赤：削除された項目、または変更された項目の古い値を示します。
- 青：変更された項目の新しい値を示します。
- [Shared Policies] セクション：ここには、すべての共有ポリシーに対する変更が表示されます。
- [Policy Bundles]：すべてのポリシーバンドルへの変更がここに表示されます。
- [Policy Objects]：ここには、すべてのポリシーオブジェクトに対する変更が表示されます。
- [VPN]：新たに検出された VPN と削除された VPN トポロジを含め、VPN トポロジとポリシーに対する変更はここに表示されます。

チケット管理が無効になっている Workflow 以外のモードでの変更レポートの選択

チケット管理が無効になっている Workflow 以外のモードでは、**[管理（Manage）] > [変更レポート（Change Reports）]** を選択して、[変更レポート（Change Report）] ダイアログボックスでセッションを選択することにより、閉じている設定セッションの変更レポートを表示できます。

チケット管理が無効になっている Workflow 以外のモードでは、変更を送信または廃棄すると、設定セッションが完了したと見なされます。[Change Report] ダイアログボックスに、閉じているすべてのセッションが一覧表示され、セッションが閉じられた日時、セッションを閉じたアクション（送信または廃棄）、およびそのセッションに関連付けられているユーザ名が示されます。これらのセッションは、Workflow モードでのアクティビティに相当します。セッションを選択し、[変更の表示（View Changes）] をクリックすると、レポートが表示されます。このレポートの解釈については、変更レポートの表示 （197 ページ）を参照してください。

ヒント　現在の設定セッションのレポートを表示するには、このダイアログボックスを閉じ、**[ファイル（File）] > [変更の表示（View Changes）]** を選択します。

アクティビティ/チケットの検証

Workflow モードでは、アクティビティを承認のために送信すると、Security Manager によってアクティビティが検証されます。また、アクティビティ内でポリシーの作成中および変更中はいつでも、アクティビティを検証できます。アクティビティが送信されたあとも、検証レポートはスタティックなままです。

Workflow 以外のモードでは、ポリシーをデータベースに送信した場合、ポリシーの展開を試行した場合、またはポリシーを検証した場合に、Security Manager によってポリシーが検証されます。検証プロセスでは、変更が送信または展開されるまでに行われたポリシーの変更についてレポートされます。

検証プロセスでは、次の領域がチェックされます。エラーがあった場合は、検証結果の詳細な要約を表示できます。

- ポリシーの整合性：解決不可能な参照（欠落しているオブジェクト、未解決のインターフェイス ロール、必須設定のオーバーライドなど）がないこと。
- ポリシーの展開可能性：ポリシーを適切に CLI コマンドに変換できるように、ターゲットデバイスでプラットフォーム、オペレーティング システム、および設定済みの機能がサポートされていること。

ポリシーに、特定のデバイス タイプまたはオペレーション システム バージョンを必要とするオプションが含まれている場合は、サポートされていないデバイスに関する検証警告が表示されますが、Security Manager は、サポートされていないデバイスに対して関連コマンドを生成しません。このため、特定のデバイスに限定されたポリシーを作成せずに、広範囲のデバイスに適用されるポリシーを作成できます。

- FlexConfig の整合性：破損した FlexConfig オブジェクトがないこと。破損したオブジェクトが見つかると、破損した FlexConfig オブジェクトのリストとともに警告が表示されます。
- FlexConfig の構文：構文エラーが見つかると、影響を受ける FlexConfig とその構文エラーとともに警告が表示されます。
- FlexConfigオブジェクト参照：すべてのオブジェクト参照が解決可能であること。FlexConfig オブジェクトが存在しないオブジェクトを参照している場合、存在しないオブジェクトのリストとともに警告が表示されます。

関連項目

- 承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） （202 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）

ステップ 1 次のいずれかを実行します。

- ワークフロー モードで、次の手順を実行します。
  - アクティビティを開いて、アクティビティツールバーの [検証（Validate）] ボタンをクリックするか、[アクティビティ（Activities）] > [アクティビティの検証（Validate Activity）] を選択します。
  - [管理（Manage）] > [アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[検証（Validate）] をクリックします。
- チケット管理が有効になっている非ワークフローモードで、次の手順を実行します。
  - チケットを開き、チケットツールバーの [保存された変更の検証（Validate Saved Changes）] ボタンをクリックするか、[チケット（Tickets）] > [チケットの検証（Validate Ticket）] を選択します。
  - [管理（Manage）] > [チケット（Tickets）] を選択します。[Ticket Manager] ウィンドウでチケットを選択し、[検証（Validate）] をクリックします。
- チケット管理が有効になっている非ワークフローモードで、[ファイル（File）] > [検証（Validate）] を選択するか、ポリシーのプレビューまたは展開を試行します。

Security Managerによって検証が実行され、検証結果が要約された情報メッセージダイアログボックスが開きます。エラーがない場合、検証は成功です。エラーまたは警告がある場合は、[詳細設定（Details）] をクリックして [検証（Validation）] ダイアログボックスを開きます。このダイアログボックスで、エラーの詳細情報を確認できます。

ステップ 2 エラーを評価して、エラーの修正方法を決定します。

[Validation] ダイアログボックスでは、エラーと警告が次の 2 つの方法で編成され、別々のタブに表示されます。

- [Errors] タブ：[Errors] タブでは、検証の問題がエラーのタイプに基づいて編成されます。各エラーは、影響を受けるデバイスの数およびエラーの重大度を示しています。

上半分のペインでエラーを選択すると、左下のペインに、エラーのあるデバイス（およびデバイス タイプ）のリストが表示されます。右下のペインには、エラー、エラーの原因、および修正方法が表示されます。

- [Devices] タブ：[Devices] タブでは、検証の問題がデバイスに基づいて編成されます。各デバイスは、デバイスのエラーや警告の数とタイプ、およびデバイス タイプを示しています。デバイス ステータスは、デバイス設定の最悪の問題（エラーまたは警告）を示しています。

上半分のペインでデバイスを選択すると、左下のペインにそのデバイスのエラーが一覧表示されます。エラーを選択すると、右下のペインにエラー、エラーの原因、および修正方法が表示されます。

アクティビティを送信する前に、エラーを修正する必要があります。Security Manager では、検証エラーのあるアクティビティの送信はできません。

（注）　（エラーとは異なり）検証警告があっても、アクティビティの承認または展開はできます。

承認のためのアクティビティの送信（アクティビティアプルーバを使用する Workflow モード）

アクティビティ アプルーバを使用する Workflow モードでは、承認のためにアクティビティを送信する必要があります。アクティビティを送信すると、アクティビティの整合性と展開可能性が検証されます。検証プロセスおよびレポートの詳細については、アクティビティ/チケットの検証　（200 ページ）を参照してください。

また、アクティビティが閉じられて、アクティビティの承認権限を持つユーザがそれを開くことができるようになります。アクティビティが承認されると、その設定が Security Manager データベースにコミットされ、設定をデバイスに展開できるようになります。

アクティビティを送信すると、Security Manager によって、関連するアプルーバに、アクティビティに承認が必要であることを通知するための電子メールが送信されます。

アクティビティ アプルーバを使用しない Workflow モードでは、アクティビティを送信する必要はありません（実際に、アクティビティの送信はできません）。アクティビティを自分で承認できます。アクティビティ承認設定の変更方法、および通知用の電子メールアドレスの設定方法の詳細については、[Workflow] ページ　（745 ページ）を参照してください。

関連項目

- アクティビティについて　（177 ページ）
- アクティビティ/チケットを開く　（195 ページ）
- アクティビティ/チケットの状態について　（181 ページ）
- 電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定　（34 ページ）

ステップ 1 次のいずれかを実行します。

- アクティビティを開いて、アクティビティツールバーの [アクティビティの送信（Submit Activity）] ボタンをクリックするか、**[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）]** を選択します。
- **[管理（Manage）] > [アクティビティ（Activities）]** を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[送信（Submit）] をクリックします。

[Submit Activity] ダイアログボックスが開きます。

ステップ 2 [Submit Activity] ダイアログボックスで、次のフィールドに入力します。

- [アプルーバ（Approver）]：デフォルトのアドレスが適切でない場合に、アクティビティを承認するユーザの電子メールアドレスを入力します。このユーザが、送信の通知を受け取ります。

デフォルトの電子メール アドレスは、[Tools] > [Security Manager Administration] > [Workflow] で設定します。

- [コメント（Comment）]：アプルーバがアクティビティを評価する際に参考になるコメントを入力します。
- [送信者（Submitter）]：デフォルトのアドレスが適切でない場合に、承認要求を送信するユーザの電子メールアドレスを入力します。このフィールドには、Security Manager へのログインに使用したユーザ名に関連付けられている電子メール アドレスが最初から埋め込まれています。アクティビティ状態変更の通知は、このアドレスに送信されます。

必要に応じて、[変更を表示（View Changes）] ボタンをクリックして、アクティビティ内で行われた変更のレポートを PDF 形式で表示します。詳細については、変更レポートの表示 （197 ページ）を参照してください。

ステップ 3 [OK] をクリックします。[Activity Manager] ウィンドウでアクティビティのステータスが [Submitted] に変わり、通知が送信されます。

（注） 電子メールを送信できない場合は、Security Manager によって警告されます。この場合は、アプルーバに直接連絡する必要があります。

アクティビティの承認または拒否（Workflow モード）

アクティビティ内の変更をデータベースにコミットする前に、アクティビティを承認する必要があります。アクティビティの承認権限を持っている場合は、アクティビティを開いて、ポリシーおよびポリシー割り当てを確認してから、アクティビティを承認または拒否できます。

アプルーバを使用しない Workflow モードでは、各自のアクティビティを承認できます。アプルーバを使用せずに作業している場合は、アクティビティを拒否できません。ただし、変更を保存しない場合は、変更を廃棄できます。Workflow 以外のモードでは、[file] メニューで [Submit]

および [Discard] コマンドを使用して、設定セッションを送信（して自動的に承認）するか、または設定セッションを廃棄します。

アクティビティ アプルーバを使用する Workflow モードでは、アクティビティを送信しないと、アクティビティを開いたり承認したりできません。このモードでは、アクティビティを拒否することもできます。

アクティビティを承認すると、ポリシーおよびポリシー割り当てがデータベースにコミットされ、デバイスまたはファイルに展開できるようになります。アクティビティに関連付けられたデバイスはロック解除されるため、ポリシー定義に含めたり、他のアクティビティで変更したりできます。

アクティビティを拒否すると、アクティビティは [Edit] 状態に戻ります。送信者は、アクティビティを再び開いて必要な変更を行い、承認のために再送信できます。アクティビティに関連付けられたデバイスはロック解除されないため、ポリシー定義に含めたり、他のアクティビティで変更したりできません。

（注） アクティビティの承認後に変更を元に戻すことはできません。新しいアクティビティを作成し、ポリシーおよびポリシー割り当てを手動で目的の状態に変更する必要があります。

関連項目

- アクティビティについて （177 ページ）
- アクティビティ/チケットを開く （195 ページ）
- アクティビティ/チケットの状態について （181 ページ）

ステップ 1 以下の適切な手順を実行します。

- アクティビティを承認するには、次のいずれかを実行します。
  - アクティビティを開いて、アクティビティツールバーの [アクティビティの承認（Approve Activity）] ボタンをクリックするか、メニューから **[アクティビティ（Activities）] > [アクティビティの承認（Approve Activity）]** を選択します。
  - **[管理（Manage）] > [アクティビティ（Activities）]** を選択します。[Activity Manager] ウィンドウでアクティビティを選択し、[承認（Approve）] をクリックします。
- 1 つまたは複数のアクティビティを拒否するには、次のいずれかを実行します。
  - アクティビティを開いて、アクティビティツールバーの [アクティビティの拒否（Reject Activity）] ボタンをクリックするか、メニューから **[アクティビティ（Activities）] > [アクティビティの拒否（Reject Activity）]** を選択します。
  - **[管理（Manage）] > [アクティビティ（Activities）]** を選択します。[Activity Manager] ウィンドウで 1 つまたは複数のアクティビティを選択し、[拒否（Reject）] をクリックします。

[アクティビティの承認（Approve Activity）]、[アクティビティの拒否（Reject Activity）]、または [複数のアクティビティの拒否（Reject Multiple Activities）] ダイアログボックスが表示されます。

ステップ 2 [コメント（Comment）] フィールドに、1 つまたは複数のアクティビティを承認または拒否する理由を示す簡単な説明を入力します。拒否する場合は、推奨リビジョンを含めることができます。

ステップ 3 [OK]（単一のアクティビティの場合）または [拒否（Reject）]（複数のアクティビティの場合）をクリックします。[Activity Manager] ウィンドウで、アクティビティ ステータスが [Approved] または [Edit]（拒否された場合）に変わります。このウィンドウの要素の詳細については、アクティビティ/チケット マネージャ ウィンドウ （189 ページ）を参照してください。

アクティビティ/チケットの破棄

アクティビティ/チケット（Workflow 以外のモードでは設定セッション）が不要になった場合は、破棄できます。アクティビティ/チケットを破棄すると、そのアクティビティ内で定義されていたすべてのポリシーおよびポリシー割り当てが削除されます。これらのポリシーおよびポリシー割り当てはデータベース内には存在しないため、展開はできません。

廃棄されたアクティビティは、Security Manager の Workflow 設定で定義されている設定に基づいてシステムから削除されます。また、そのアクティビティに関連付けられているデバイスがロック解除され、他のアクティビティで使用できるようになります。詳細については、[Workflow] ページ （745 ページ）を参照してください。

破棄されたチケットは、Security Manager の [チケット管理（Ticket Management）] で定義されている設定に基づいてシステムから削除されます。また、そのチケットに関連付けられているデバイスがロック解除され、他のアクティビティで使用できるようになります。チケットがシステムから削除されるまで、チケットの状態は [破棄（Discarded）] と表示されます。詳細については、[チケット管理（Ticket Management）] ページ （740 ページ）を参照してください。

（注） チケットが破棄されても、そのチケットに割り当てられたイメージ管理ジョブは自動的に破棄されません。必要に応じて、Image Manager で該当するチケット ID を持つ保留中のイメージ管理ジョブを検索し、それらのジョブを削除する必要があります。

アクティビティ/チケットを破棄するには：

Workflow モード：次のいずれかを実行します。

- 単一のアクティビティを破棄するには、次のいずれかを実行します。
  - アクティビティを開いてから、アクティビティツールバーの [破棄（Discard）] ボタンをクリックするか、[アクティビティ（Activities）] > [アクティビティの破棄（Discard Activity）] を選択します。
  - [管理（Manage）] > [アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[破棄（Discard）] をクリックします。廃棄できるのは、Edit または Edit Open の状態にあるアクティビティだけです。

どちらの方法を使用した場合も、[Discard Activity] ダイアログボックスでプロンプトが表示されます。このダイアログボックスで、アクティビティを廃棄する理由を説明する任意のコメントを入力できます。コメントを入力し、[OK] をクリックしてアクティビティを破棄します。

- 複数のアクティビティを破棄するには、[管理（Manage）]>[アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウで、破棄するアクティビティを選択してから、[破棄（Discard）] をクリックします。破棄できるのは、[編集（Edit）] または [編集中（Edit Open）] の状態にあるアクティビティだけです。

[複数のアクティビティを破棄（Discard Multiple Activities）] ダイアログボックスでプロンプトが表示されます。このダイアログボックスで、アクティビティを破棄する理由を説明する任意のコメントを入力できます。他のユーザーに属するアクティビティを選択した場合は、それらのアクティビティを破棄するか、[選択した他のユーザーに属するアクティビティも破棄する（Discard selected activities of other users as well）] チェックボックスを使用しないことにするかを選択できます。コメントを入力し、必要に応じて [選択した他のユーザーに属するアクティビティも破棄する（Discard selected activities of other users as well）] チェックボックスをオンまたはオフにしてから、[OK] をクリックして、選択したアクティビティを破棄します。

チケット管理が有効な Workflow 以外のモード：次のいずれかを実行します。

- 単一のチケットを破棄するには、次のいずれかを実行します。
  - チケットを開き、チケットツールバーの [破棄（Discard）] ボタンをクリックするか、[チケット（Tickets）] > [チケットの破棄（Discard Ticket）] を選択します。
  - [管理（Manage）] > [チケット（Tickets）] を選択します。[Ticket Manager] ウィンドウでチケットを選択し、[破棄（Discard）] をクリックします。破棄できるのは、[編集（Edit）] または [編集中（Edit Open）] の状態にあるチケットだけです。

どちらの方法を使用した場合も、[チケットの破棄（Discard Ticket）] ダイアログボックスでプロンプトが表示されます。このダイアログボックスで、チケットを破棄する理由を説明する任意のコメントを入力できます。コメントを入力し、[OK] をクリックしてチケットを破棄します。

- 複数のチケットを破棄するには、[管理（Manage）] > [チケット（Tickets）] を選択します。[Ticket Manager] ウィンドウで、破棄するチケットを選択してから、[破棄（Discard）] をクリックします。破棄できるのは、[編集（Edit）] または [編集中（Edit Open）] の状態にあるチケットだけです。

[複数のチケットを破棄（Discard Multiple Tickets）] ダイアログボックスでプロンプトが表示されます。このダイアログボックスで、チケットを破棄する理由を説明する任意のコメントを入力できます。他のユーザーに属するチケットを選択した場合は、それらのチケットを破棄するか、[選択した他のユーザーに属するチケットも破棄する（Discard selected tickets of other users as well）] チェックボックスを使用しないことにするかを選択できます。コメントを入力し、必要に応じて [選択した他のユーザーに属するチケットも破棄する（Discard selected tickets of other users as well）] チェックボックスをオンまたはオフにしてから、[OK] をクリックして、選択したチケットを破棄します。

チケット管理が無効な Workflow 以外のモード：[ファイル（File）] > [破棄（Discard）] を選択して、現在の設定セッション内の変更を廃棄します。

関連項目

- アクティビティについて （177 ページ）
- アクティビティ/チケットを開く （195 ページ）
- アクティビティ/チケットの状態について （181 ページ）

アクティビティ/チケットのステータスおよび履歴の表示

Workflow モードでは、[Activity Manager] ウィンドウでアクティビティの変更のステータスおよび履歴を表示できます。チケット管理が有効になっている Workflow 以外のモードでは、Ticket Manager ウィンドウでチケットのステータスと変更の履歴を表示できます。

アクティビティのウィンドウを開くには、ツールバーで [Activity Manager] ボタンをクリックするか、[管理（Manage）] > [アクティビティ（Activities）] を選択します。

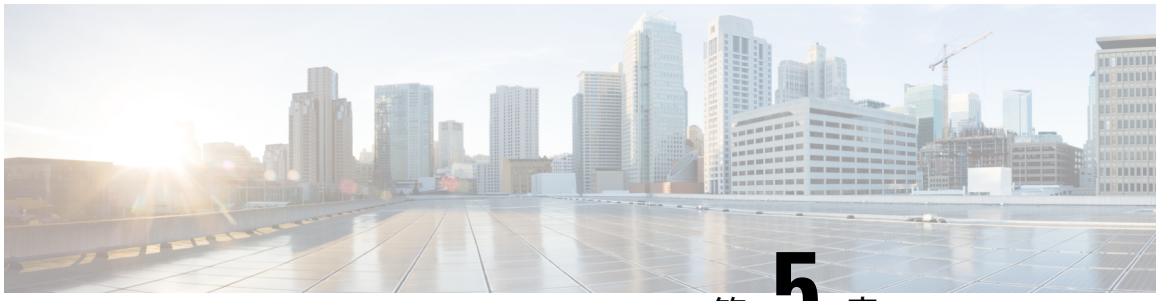
チケットのウィンドウを開くには、ツールバーで [Ticket Manager] ボタンをクリックするか、[管理（Manage）] > [チケット（Tickets）] を選択します。

上部ペインに、アクティビティ/チケットの現在の状態を含む、すべての使用可能なアクティビティ/チケットが一覧表示されます。アクティビティ/チケットを選択すると、下部ペインの次のタブに追加情報が表示されます。

- [詳細（Details）] タブ：アクティビティ/チケットが作成された日時とその説明が表示されます。
- [履歴（History）] タブ：アクティビティ/チケットのトランザクション履歴が表示されます。状態が変更されるたびに、変更のレコード（変更を行ったユーザーや、変更に関するコメントなど）が保持されます。

関連項目

- アクティビティについて （177 ページ）
- アクティビティ/チケット マネージャ ウィンドウ （189 ページ）



第 5 章

ポリシーの管理

ここでは、Cisco Security Manager におけるポリシーの概念およびポリシーの使用方法や管理方法について説明します。

- ポリシーについて （209 ページ）
- ポリシーの検出 （223 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）
- ポリシーバンドルの管理 （281 ページ）

ポリシーについて

Security Manager におけるポリシーとは、ネットワークの特定の設定項目を定義した一連のルールまたはパラメータのことです。ネットワークを設定するには、デバイス（個々のデバイス、サービス モジュール、セキュリティ コンテキスト、仮想センサーなど）のポリシーおよび複数のデバイスで構成される VPN トポロジを定義し、これらのポリシーで定義された設定をこれらのデバイスに展開します。

特定のソリューションを設定するためにさまざまなタイプのポリシーが必要になる場合があります。たとえば、サイト間 VPN を設定するには、IPsec、IKE、GRE などの複数のポリシーを設定することが必要になる場合があります。

ポリシーは、1 つ以上のデバイスに割り当てられます。ポリシーがデバイスに割り当てられたあとでポリシー定義を変更すると、デバイスの動作が変わります。

ここでは、ポリシーについて詳しく説明します。

- 設定ベースのポリシーとルールベースのポリシー （210 ページ）
- サービスポリシーとプラットフォーム固有のポリシー （211 ページ）
- ローカルポリシーと共有ポリシー （211 ページ）
- ルールの継承について （213 ページ）
- ポリシー管理とオブジェクト （217 ページ）

• ポリシーのロックについて （217 ページ）
• ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ （221 ページ）

設定ベースのポリシーとルールベースのポリシー

Security Manager のポリシーは、ルールベースまたは設定ベースのポリシーとして構造化されます。

ルールベースのポリシー

ルールベースのポリシーには、選択されたデバイス上のトラフィックの処理方法を制御する 1 つ以上のルールが含まれます。たとえば、ファイアウォール サービスの一部として定義されたアクセス ルールやインスペクション ルールなどがあります。ルールベースのポリシーには、テーブルに配置された数百または数千のルールを含めることができ、それぞれのルールで同じパラメータ セットに異なる値を定義できます。トラフィック フローには、定義がフローと一致する最初のルール（最初の一致と呼ばれる）が割り当てられるため、ルールの順序は非常に重要です。

ルール テーブルの構造は、ローカル ポリシーまたは共有ポリシー（ローカルポリシーと共有ポリシー （211 ページ）を参照）のどちらを設定するかによって異なります。単一デバイスにルールベースのローカル ポリシーを設定した場合、ポリシーにはローカル ルールのフラットなテーブルが含まれます。デバイス ビューまたはポリシー ビューでルールベースの共有ポリシーを設定した場合、テーブルは [Mandatory] セクションと [Default] セクションの 2 つに分割されます。必須ルールは、常にデフォルト ルールよりも優先され、ローカル ルールやデフォルト ルールで上書きできません。[Default] セクションには、必須ルールやローカル ルールで上書きできるルールが含まれます。ルールを [Mandatory] セクションまたは [Default] セクションで定義したり、カットアンドペーストを使用して 2 つのセクション間でルールを移動したりできます。

ファイアウォール サービス ポリシーなどの特定タイプのルールベースのポリシーを定義する場合は、ポリシーを階層化することができます。この階層では、下位レベルのルールは上位レベルのルールからプロパティを取得します。これはルールの継承と呼ばれます。たとえば、すべてのファイアウォールにグローバルに適用される一連のインスペクション ルールを定義し、デバイスのサブセットに適用できる追加ルールでこれらのルールを補足できます。親ポリシーで共通のルールを保持すると、継承によって、展開失敗の原因となる設定エラーの発生を抑えることができます。詳細については、ルールの継承について （213 ページ）を参照してください。

設定ベースのポリシー

設定ベースのポリシーには、セキュリティまたはデバイス動作の側面を定義した一連の関連パラメータが含まれます。たとえば、Cisco IOS ルータを設定する場合、Quality of Service（QoS）ポリシーを定義して、ポリシーに含めるインターフェイス、QoS を適用するトラフィックのタイプ、およびトラフィックのキューイング方法やシェーピング方法を定義できます。同じパラメータ セットの値を含む数百のルールを格納できるルールベースのポリシーとは異なり、デバイスに定義される各設定ベースのポリシーには 1 つのパラメータ セットしか定義できません。

関連項目

- ポリシーについて （209 ページ）

サービスポリシーとプラットフォーム固有のポリシー

Security Manager のポリシーは、いくつかのドメインに分割され、各ドメインは主なポリシー カテゴリを表します。これらのドメインは、サービス ポリシーおよびプラットフォーム固有のポリシーという 2 つのカテゴリに分類できます。

サービス ポリシーは、次のポリシー ドメインに分割されます。

- ファイアウォール
- サイト間 VPN
- リモート アクセス VPN
- IPS サービス ポリシー

たとえば、ファイアウォール ポリシー ドメインには、アクセル ルール、インスペクション ルール、トランスペアレント ルールなどのポリシーが含まれます。サイト間 VPN ポリシー ドメインには、IKE プロポーザル、IPsec プロポーザル、事前共有キーなどのポリシーが含まれます。サービス ポリシーは、プラットフォームにかかわらず任意の種類のデバイスに適用できますが、ポリシー定義はデバイス タイプによって異なる場合があります。

プラットフォーム固有のポリシー ドメインには、選択したプラットフォームに固有の機能を設定するポリシーが含まれています。すべてのプラットフォーム固有のポリシーがセキュリティに直接関連付けられるわけではありません。たとえば、ルータ ポリシー ドメインには、ルーティング ポリシー、アイデンティティ ポリシー（ネットワーク アドミッション コントロールおよび 802.1x）、デバイス管理に関連するポリシー（DHCP、SNMP、デバイス アクセス）、および QoS や NAT などのその他のポリシーが含まれます。

ルータおよびファイアウォール（ASA、PIX、FWSM）の場合は、管理するプラットフォーム固有のポリシーを選択できます。詳細については、ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ （221 ページ）を参照してください。

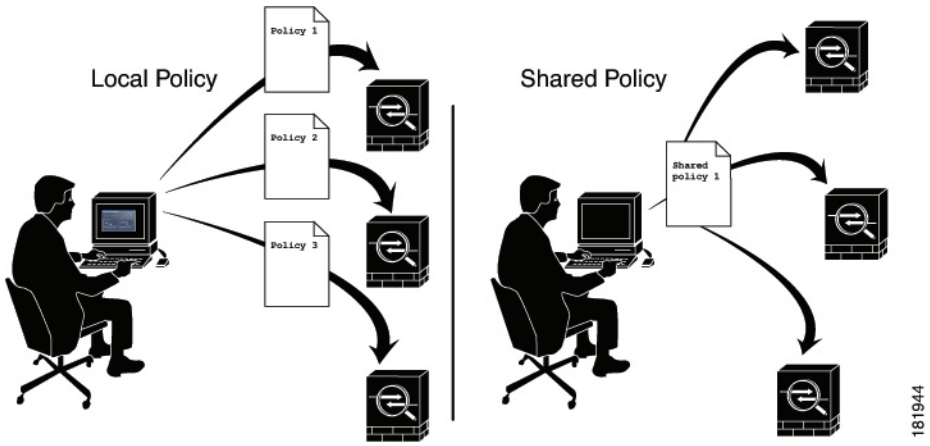
ローカルポリシーと共有ポリシー

デバイスには、ローカル ポリシーまたは共有ポリシーを設定できます。ローカル ポリシーとは、単一デバイスに定義されるポリシーのことです。ローカル ポリシーに加えた変更は、そのデバイスだけに反映されます。ローカル ポリシーは、小規模ネットワークや標準以外の設定を必要とするデバイスに適しています。たとえば、ネットワーク内の他のルータで使用されるポリシーとは異なる OSPF ルーティング ポリシーを必要とするルータにローカル ポリシーを設定します。ローカル ポリシーに対して実行できるアクションの詳細については、基本的なポリシー管理の実行 （248 ページ）を参照してください。

デバイスごとにローカル ポリシーを保持している場合は、ネットワークが拡大するにつれ、ポリシーを包括的かつ効率的に管理するために必要な作業が増加します。この問題に対処するた

めに、Security Managerにはポリシー共有という機能が用意されています。ポリシー共有では、1 つのポリシーを作成し、そのポリシーを複数のデバイスに割り当てることができます。詳細については、ローカル ポリシーの共有 （262 ページ）を参照してください。

図 *12 :* ローカルポリシーと共有ポリシー



たとえば、ネットワーク内のすべての Cisco IOS ルータで同じ Network Admission Control（NAC; ネットワーク アドミッション コントロール）ポリシーを実装する場合は、1 つの NAC ポリシーだけを定義し、そのポリシーを共有します。その後、1 つのアクションでネットワーク内のすべてのルータに共有ポリシーを割り当てることができます。詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）を参照してください。

共有ポリシーに加えた変更は、そのポリシーが割り当てられているすべてのデバイスに自動的に適用されます。このため、共有ポリシーを使用すると、ポリシー作成プロセスを合理化して、デバイス設定の一貫性や同一性を保持することができます。

共有ポリシーに対して実行できるアクションの詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）を参照してください。

ヒント

- 共有ポリシーをグループ化して、ポリシーバンドルを形成できます。ポリシーバンドルを使用すると、特に多数のデバイスを操作する場合に、共有ポリシーの割り当てを簡単に管理できます。詳細については、ポリシーバンドルの管理 （281 ページ）を参照してください。
- ポリシーの共有以外に、同じタイプの別のポリシーを定義するときに、ルールベースのポリシーのルールを継承することもできます。これにより、たとえば、すべてのファイアウォール デバイスに適用される一連の企業アクセス ルールを保持しながら、必要に応じて個々のデバイスに追加ルールを定義するという柔軟性が得られます。詳細については、ルールの継承について （213 ページ）を参照してください。
- 複数の Security Manager サーバーを使用する場合、プライマリサーバーから定期的に共有ポリシーをエクスポートし、他のサーバーにインポートすることで、サーバー間で一貫性のあるポリシーセットを維持できます。公式のポリシー ソースとして使用するサーバを決

定する必要があります。詳細については、共有ポリシーのエクスポート （612 ページ）およびポリシーまたはデバイスのインポート （615 ページ）を参照してください。

- バージョン 4.7 では、Cisco Security Manager に、デバイスフィルタで使用可能なフィルタリングの選択肢に新しいオプションが追加されました。この新しいオプションは、共有ポリシーが適用されているデバイスのフィルタを提供します。Security Manager GUI でこれを表示するには、[ドロップダウンリスト内（in the dropdown list）] で、[表示（View）] > [デバイス表示（Device View）]>[フィルタ：（Filter:）]>[フィルタの作成（Create Filter）]... に移動します。[フィルタの作成（Create Filter）] ダイアログボックスが表示されたら、ドロップダウンリストを使用して、「Device,」「has,」「Shared Policy,」を選択すると、結果として「Device has 'Shared Policy」フィルタが設定されます。

共有ポリシーと VPN

共有ポリシーを使用すると、デバイス設定の場合と同様に、VPN の設定も簡単に行うことができます。たとえば、共有 IPsec プロポーザル ポリシーを作成し、そのポリシーを複数のサイト間 VPN に割り当てることができます。共有ポリシーに加えた変更は、そのポリシーが割り当てられているすべての VPN に反映されます。

共有ポリシーは、Site-to-Site VPN Manager を使用して、既存の VPN に割り当てることができます。そのためには、共有可能なポリシーを右クリックし、[共有ポリシーの割り当て（Assign Shared Policy）] を選択します。これは、デバイス ビューで共有ポリシーを割り当てる方法とほぼ同じです。 VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定（1395 ページ）で説明しているように、共有ポリシーを Create VPN ウィザードで使用するデフォルト ポリシーとして設定することもできます。

関連項目

- ポリシーについて （209 ページ）

ルールの継承について

ローカルポリシーと共有ポリシー （211 ページ）で説明しているように、共有ポリシーを使用すると、共通のポリシー定義を設定して複数のデバイスに割り当てることができます。ルールの継承では、この機能がさらに拡張されており、共有ポリシーに定義されているルールをデバイスに含めるだけでなく、そのデバイスに固有のローカルルールを含めることもできます。Security Manager では、継承を使用することにより、階層の下位レベルのポリシー（子ポリシーと呼ばれる）が、上位レベルで定義されているポリシー（親ポリシーと呼ばれる）のルールを継承するという階層構造を適用できます。

（注） ポリシーバンドルに他の共有ポリシーから継承する共有ポリシーが含まれている場合、継承されたルールは、ポリシーバンドルが適用されるすべてのデバイスにも適用されます。

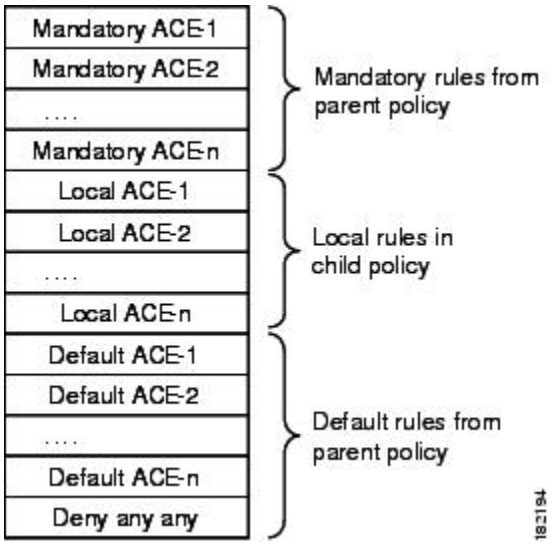
継承使用時のルールの順序

アクセス ルールについて （913 ページ）で説明しているように、アクセス コントロール リスト（ACL）は、テーブルに配置されたルール（アクセス コントロール エントリ（ACE）とも呼ばれる）で構成されます。着信パケットは、ACL内の最初のルールと照合されます。パケットは、そのルールと一致する場合、ルールに従って許可または拒否されます。一致しない場合、パケットは、一致するルールが見つかって実行されるまでテーブル内の次のルールと照合されます。

この最初の一致方式では、テーブル内のルールの順序が非常に重要になります。共有アクセス ルール ポリシーを作成すると、Security Manager はルール テーブルを複数のセクション（[Mandatory] と [Default]）に分割します。[Mandatory] セクションには、子ポリシーで定義されているローカル ルールによって上書きできないルールが含まれます。[デフォルト（Default）] セクションには、ローカル ルールでオーバーライドできるルールが含まれます。

次の図に、継承使用時のルールテーブルにおけるルールの順序付けを示します。

図 *13* : 継承使用時のルール順序



継承を使用する利点

ルールベースのポリシーを階層構造で定義すると、ルールセットを定義するときの柔軟性が大幅に向上します。また、階層レベルを必要な数だけ増やすことができます。たとえば、ブランチ オフィスにあるデバイスのアクセス ルール ポリシーを定義します。このポリシーは、地域レベルのアクセスを決定する親ポリシーからルールを継承します。一方、この親ポリシーは、企業レベルでルールを設定する階層最上位のグローバル アクセス ルール ポリシーからルールを継承します。

この例では、ルールは次のようにルール テーブルで順序付けられています。

```
Mandatory corporate access rules
    Mandatory regional access rules
        Local rules on branch device
```

```
    Default regional access rules
Default corporate access rules
```

ブランチ デバイスに対して定義されているポリシーは、地域ポリシーの子であり、企業ポリシーの孫です。このように継承を構造化すると、すべてのデバイスに適用されるが、階層下位レベルのルールによって上書きされない、企業レベルの必須ルールを定義できます。同時に、ルールの継承により、必要に応じて特定のデバイスのローカル ルールを柔軟に追加できます。

デフォルトルールを使用すると、ルールテーブルで上位に表示される必須ルールとデフォルトルールにギャップがある場合に、「deny any any」などのグローバルデフォルトルールを定義できます。グローバルデフォルトルールは、すべてのアクセスルールリストの最後に表示され、最終的なセキュリティ手段となります。

継承の例

たとえば、企業アクセス ルール ポリシーに必須のワーム軽減ルールを定義して、1 つのエントリですべてのデバイスに対するワームを軽減またはブロックできます。地域アクセス ルール ポリシーが設定されたデバイスは、ワーム軽減ルールを企業ポリシーから継承し、一方で地域レベルに適用されるルールを追加できます。たとえば、特定の地域のすべてのデバイスには FTP トラフィックを許可するが、他のすべての地域のデバイスには FTP をブロックするというルールを作成できます。ただし、企業レベルの必須ルールは、常にアクセス ルール リストの最上位に表示されます。子ポリシーで定義した必須ルールは、親ポリシーで定義された必須ルールのあとに配置されます。

デフォルト ルールでは、順序は逆になります。つまり、子ポリシーで定義されたデフォルト ルールは、親ポリシーから継承されたデフォルト ルールの前に表示されます。デフォルト ルールはデバイスに定義されたローカル ルールのあとに表示されるため、デフォルト ルールを上書きするローカル ルールを定義できます。たとえば、特定の地域のデフォルト ルールで、ある宛先リストに対する FTP トラフィックが拒否されている場合、この宛先のうちの 1 つには FTP を許可するローカル ルールを定義できます。

IPS ポリシーの継承

IPS デバイスのイベント アクション フィルタ ポリシーでは、継承を使用して、親ポリシーに定義されたルールを特定のデバイスに定義されたローカル ルールに追加することもできます。唯一の違いは、アクティブ ルールと非アクティブ ルールは Security Manager インターフェイスに表示されますが、すべての非アクティブ ルールは継承されたデフォルト ルールのあとで最後に展開される点です。

IPS デバイスのシグニチャ ポリシーでは、シグニチャごとに適用できる別の継承タイプが使用されます。シグニチャの設定 （2169 ページ） を参照してください。

関連項目

- 設定ベースのポリシーとルールベースのポリシー （210 ページ）
- アクセス ルールについて （913 ページ）
- グローバル アクセス ルールについて （915 ページ）
- 継承と割り当て （216 ページ）

- ルールの継承または継承の解除　（269 ページ）

継承と割り当て

ルールの継承とポリシーの割り当ての違いを理解しておくことが重要です。

- 継承：選択したポリシーからルールを継承した場合、デバイスにすでに設定されているローカル ルールは上書きされません。代わりに、継承されたルールがローカルルールに追加されます。継承されたルールが必須ルールの場合、ローカル ルールの前に追加されます。継承されたルールがデフォルトルールの場合、ローカルルールのあとに追加されます。継承されたルールに対して親ポリシー内で変更を加えると、このルールを継承するポリシーにも反映されます。

（注）　IPS シグニチャ ポリシーとシグニチャ イベント アクションでは、継承の動作は異なります。詳細については、 シグニチャ継承について　（2168 ページ）を参照してください。

- 割り当て：共有ポリシーをデバイスに割り当てると、デバイスにすでに設定されているポリシーは、選択したポリシーに置き換わります。これは、デバイスにローカルポリシーまたは別の共有ポリシーがすでに設定されていたかどうかにかかわらず、あてはまります。

したがって、アクセス ルールなどのルールベースのポリシーを使用する場合は、これらのオプションを慎重に選択する必要があります。継承は、デバイス上のローカル ルールを、親ポリシーからの追加ルールで補足する場合に使用します。割り当ては、デバイス上のポリシーを、選択した共有ポリシーに置き換える場合に使用します。

ヒント　ローカル ルールを誤って上書きしないように、Security Manager では、ルールベースのポリシーに対して [Assigned Shared Policy] オプションを選択するときに警告メッセージが表示されます。このメッセージには、ポリシーを割り当てる代わりにポリシーのルールを継承するオプションがあります。ローカル ルールを保持する場合は、継承オプションを選択します。

関連項目

- ルールの継承について　（213 ページ）
- ルールの継承または継承の解除　（269 ページ）
- ローカルポリシーと共有ポリシー　（211 ページ）
- 設定ベースのポリシーとルールベースのポリシー　（210 ページ）

ポリシー管理とオブジェクト

オブジェクトを使用すると、必要なときにいつでも適用できる論理的な覚えやすい名前を一連の値に付けることによって、Security Manager で簡単にポリシーを設定できます。たとえば、ネットワークの一連の IP アドレスが含まれる、MyNetwork というネットワーク/ホスト オブジェクトを定義できます。このアドレスを必要とするポリシーを設定するときは、MyNetwork オブジェクトを参照するだけで済むため、毎回手動でアドレスを入力する必要がありません。

ポリシーを定義するときに、値としてオブジェクトを受け入れるフィールドの横にある [選択（Select）]ボタンをクリックして、すぐにオブジェクトを作成できます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。Policy Object Manager （290 ページ）で、システム全体のオブジェクトを作成したり管理したりすることもできます。

すでにデバイスに存在するポリシーが検出された場合にも、ポリシー オブジェクトが作成されます。ポリシーの検出 （223 ページ）で説明しているように、デバイスを Security Manager インベントリに追加するときにポリシーを検出したり、インベントリにすでに存在するデバイス上のポリシーを検出したりできます。新しく検出されたポリシーに対して、すでに定義されているポリシー オブジェクトを再利用するように Security Manager を設定できます。検出用のポリシー オブジェクト設定の詳細については、[Discovery] ページ （674 ページ）を参照してください。

特定のタイプのオブジェクトを使用すると、定義済みの値をデバイス レベルで上書きできるため、ポリシーでオブジェクトを使用しながら、特定の値をカスタマイズできます。詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。

オブジェクトの詳細およびポリシーの定義時にオブジェクトを使用する方法の詳細については、ポリシー オブジェクトの管理 （287 ページ）を参照してください。

関連項目

- ポリシーについて （209 ページ）

ポリシーのロックについて

Security Manager には、ポリシーのロック メカニズムがあります。これは、複数のユーザが設定を変更する権限を持つ組織で役立ちます。複数のユーザが同じデバイス、ポリシー、ポリシーの割り当て、またはオブジェクトを同時に変更する可能性がある状況を回避できます。ロックを適用すると、そのデバイスまたはポリシーにアクセスする他のユーザに対して、作業領域の上部にメッセージが表示されます。

ヒント ユーザが特定のアクションを実行すると、Security Manager はポリシー ロックよりも適用範囲が広いアクティビティ（または設定セッション）ロックを取得します。詳細については、アクティビティとロッキング （180 ページ）を参照してください。

ロック タイプ

Security Manager は、次の 2 つの異なるロック タイプを使用します。

- ポリシー コンテンツ ロック：特定のポリシーのコンテンツをロックします。作業領域の上に表示されるバナーは次のようになります。

This data for this policy is locked by activity/user: <name>.

コンテンツ ロックにより、他のユーザはロックされたポリシーの設定を変更できなくなります。

- 割り当てロック：特定のデバイスに対するポリシータイプの割り当てをロックします。作業領域の上に表示されるバナーは次のようになります。

The assignment of this policy is locked by activity/user: <name>.

ローカルポリシーの場合は、割り当てロックが適用されると、他のユーザはポリシーの割り当てを解除したり、ローカルポリシーの代わりに同じタイプの共有ポリシーを割り当てたりすることができなくなります。共有ポリシーの場合は、割り当てロックが適用されると、他のユーザはすでに割り当てられているポリシーの代わりに同じタイプの別の共有ポリシーを割り当てることができなくなります。

これらのロックは、ユーザによって実行されるアクションに応じて、連携して機能するか、相互に独立して機能します。両方のロックが同時にアクティブになった場合、作業領域の上に表示されるバナーは次のようになります。

This policy is locked by activity/user: <name>.

実行可能なアクションに対するロックの効果の概要については、ロックとポリシーについて（219 ページ）を参照してください。

ロックの解除

ロックをイネーブルにすると、変更を送信するか（Workflow 以外のモードでの作業時）またはアクティビティを送信および承認する（Workflow モードでの作業時）までロックは解除されません。アクティビティを廃棄すると、そのアクティビティによって生成されたロックも廃棄されます。ワークフロー モードの詳細については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。

次の点を考慮してください。

- ロックは、デバイスの IP アドレスではなくデバイス名に基づきます。そのため、Security Manager では、IP アドレスが同じで名前が異なる 2 つのデバイスを定義しないことを推奨します。特に同時に両方のデバイスに展開しようとすると、予期しない結果が発生します。
- ロックは異なる操作にまたがって適用されることはありません。たとえば、あるユーザが、別のユーザによって検出されたデバイスと同じデバイスに対して展開することをロックで防ぐことはできません。

ロックの詳細については、次の項を参照してください。

• ロックとポリシーについて （219 ページ）
• ロックと VPN トポロジについて （220 ページ）
• ロックとオブジェクトについて （220 ページ）

ロックとポリシーについて

次のテーブルに、Security Manager におけるポリシーロックの効果の概要を示します。

（注） ポリシーやポリシーの割り当てを変更できるかどうかは、ユーザに割り当てられているユーザ権限によって決まります。『Installation Guide for Cisco Security Manager』を参照してください。

表 *33* : ロックの概要

別のユーザまたはアクティビティによる処理	不可能な操作	可能な操作
ポリシー定義を変更する。	• ポリシーを変更したり、他のデバイスに割り当てたりする。 • ポリシーの割り当てを解除する（ローカル ポリシーの場合）。	デバイスからポリシーの割り当てを解除する（共有ポリシーの場合）。
子孫を持つルールベースのポリシーの定義を変更する。	• 親ポリシーまたはその子孫のいずれかを変更する。 • 親ポリシーまたはその子孫のいずれかを追加デバイスに割り当てる。 • 親ポリシーまたはその子孫のいずれかのルール継承を変更する。	デバイスからポリシーの割り当てを解除する。
ポリシーの割り当てを、その定義を変更しないで変更する。	ポリシーを変更する。 （注） ポリシー ビューでは、コンテンツ ロックはポリシーに適用されます。デバイス ビューでは、割り当てロックは割り当てが他のユーザによって変更されるデバイスに適用されます。	ポリシーを割り当てたり、他のデバイスからポリシーの割り当てを解除したりする。
ポリシー定義を変更し、その割り当てを変更する。	ポリシーを変更したり、他のデバイスに割り当てたりする。	デバイスからポリシーの割り当てを解除する。

関連項目

- ポリシーのロックについて （217 ページ）
- ポリシーについて （209 ページ）

ロックと VPN トポロジについて

VPN トポロジのデバイス割り当てを変更したり、特定の VPN ポリシーを変更したりする場合、ロックは VPN トポロジ全体、およびポリシーが共有される他のトポロジに適用されます。つまり、他のユーザはデバイス割り当てを変更したり、VPN トポロジに定義されている VPN ポリシーを変更したりすることはできません。

サイト間 VPN ポリシーを表示したり変更したりするには、VPN トポロジ内の各デバイスに対する権限が必要です。また、デバイスを VPN トポロジに追加するための権限も必要です。VPN トポロジ内のデバイスに対して異なるレベルの権限を持っている場合は、最低の権限レベルがトポロジ全体に適用されます。たとえば、ハブアンドスポーク トポロジ内のスポークに対する読み取り/書き込み権限があり、ハブとして機能するデバイスに対する読み取り専用権限がある場合、ハブアンドスポーク トポロジ内のポリシーとデバイスに対する読み取り専用権限が与えられます。権限の詳細については、『Installation Guide for Cisco Security Manager』を参照してください。

（注） VPN トポロジからデバイスの割り当てを解除すると、VPN トポロジ内にデバイス ロックが作成されます。つまり、これらのデバイスはインベントリから削除できません。影響を受けるすべてのデバイス（削除するデバイスなど）に設定を展開するまでは、他のユーザはトポロジのデバイス割り当てを編集できません。デバイスは、設定が展開されるまで実際にはトポロジから削除されません。

関連項目

- ポリシーのロックについて （217 ページ）
- サイト間 VPN の管理：基本 （1379 ページ）

ロックとオブジェクトについて

再利用可能なオブジェクトを作成または変更すると、そのオブジェクトはロックされ、他のユーザは同じオブジェクトを変更または削除できなくなります。オブジェクトのロックに関するその他のルールは次のとおりです。

- オブジェクトのロックによって、そのオブジェクトを使用するポリシーの定義や割り当てを変更できなくなることはありません。
- ポリシーに適用されたロックによって、そのポリシー定義に含まれているオブジェクトを変更できなくなることはありません。

- オブジェクトの定義は、権限を持たないデバイスに割り当てられたポリシーの一部である場合でも、変更できます。
- オブジェクトが他のオブジェクト（ネットワーク/ホスト オブジェクト、AAA サーバ グループ オブジェクトなど）を利用する場合、オブジェクトのロックによって、別のユーザがそれらの他のオブジェクトを変更できなくなることはありません。たとえば、AAA サーバ グループ オブジェクトを変更する場合、そのオブジェクトのロックによって、AAA サーバ グループを構成する AAA サーバを別のユーザが変更できなくなることはありません。

オブジェクトがロックされると、そのオブジェクトを変更しようとするユーザには、関連するダイアログボックスの読み取り専用バージョンが表示されます。Workflow モードで作業している場合、メッセージにオブジェクトをロックしているアクティビティが示されます。

関連項目

- ポリシーのロックについて （217 ページ）
- ポリシー オブジェクトの管理 （287 ページ）

ルータおよびファイアウォールデバイスのポリシー管理のカスタマイズ

Cisco IOS ルータまたは ASA、PIX、FWSM ファイアウォール デバイスを管理する場合、Security Manager で管理するポリシー タイプや管理対象外にするポリシー タイプを選択できます。ポリシー タイプの管理とは、Security Manager がポリシーの設定を管理し、データベースに格納するそのポリシーの情報を必要な設定であると認識することを意味します。Security Manager では、管理対象外のポリシータイプを設定したり、他の方法で設定されたこれらのタイプの設定を追跡したりはしません。たとえば、SNMP ポリシーを管理しない場合、CLI コマンドを使用して設定した SNMP 設定は Security Manager に認識されません。

注意 AUS または CNS を使用して設定を ASA または PIX デバイスに展開する場合は、デバイスが AUS または CNS から完全な設定をダウンロードする点に注意してください。そのため、Security Manager で管理されているポリシーを減らすと、実際にはデバイスから設定が削除されます。管理対象の一部の ASA/PIX ポリシーを選択解除し、Security Manager とともに他のアプリケーションを使用してデバイスを設定する場合は、AUS または CNS を使用しないでください。

ルータおよびファイアウォールにおけるポリシー管理をカスタマイズして、たとえば Security Manager を使用して DHCP および NAT ポリシーを管理し、一方で EIGRP や RIP などのルーティング プロトコル ポリシーを管理対象外のままにすることができます。これらの設定は、管理権限を持つユーザだけが変更でき、すべての Security Manager ユーザに影響します。

管理対象外のポリシーは、デバイス ビューとポリシー ビューの両方から削除されます。そのタイプの既存のポリシー（ローカルまたは共有）は、Security Manager データベースから削除されます。

ルータとファイアウォールのポリシー管理をカスタマイズするには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー管理（Policy Management）]**を選択して [Policy Management] ページ （729 ページ）を開きます。ポリシータイプはフォルダに整理され、ルータとファイアウォール（すべてのASA、PIX、およびFWSMデバイスを含む）は別々に処理されます。必要に応じてポリシータイプを選択または選択解除し、[保存（Save）] をクリックします。その後の処理は、ポリシータイプを管理対象にするか管理対象外にするかによって異なります。

- [ポリシータイプを管理対象外にする（Unmanaging a policy type）]：ポリシータイプを管理対象外にするときに、そのタイプのいずれかのデバイスにそのポリシーが設定されている場合は、管理対象外にする前にポリシーの割り当てを解除する必要があります。Security Manager によって、そのタイプのポリシーが割り当てられているすべてのデバイスのリスト（ポリシー名、デバイス名、およびポリシーをロックしているユーザまたはアクティビティを含む）が表示されます。[はい（Yes）] をクリックしてポリシーを管理対象外にすると、Security Managerは必要なロックを取得し、ポリシーの割り当てを解除してポリシータイプを管理対象外にします。

1 つでもデバイスのロックを取得できなかった場合、ポリシーの割り当ては解除されず、ポリシータイプは管理対象外になりません。この場合、問題が通知されます。その後、影響を受けるデバイスから手動でポリシーの割り当てを解除するか、ユーザまたはアクティビティのロックを解除し、ポリシー タイプを管理対象外にする操作を再試行できます。

（注） ポリシーを管理対象外にしても、デバイスで実行されているアクティブな設定に影響はありません。つまり、Security Manager はデバイスから設定を削除しません。代わりに、ポリシーがデータベースから削除され、Security Manager ではデバイス設定のその部分が考慮されなくなります。

- [以前に管理対象外にしたポリシータイプを管理する（Managing a previously-unmanaged policy type）]：以前に Security Manager で管理しなかったポリシータイプの管理を開始する場合は、デバイス上のアクティブな設定に、新たに管理対象にしたポリシータイプによって制御されるコマンドが含まれている可能性があります。**したがって、そのタイプのすべてのデバイス（すべてのルータまたはすべての ASA、PIX、FWSM デバイス）上のポリシーを再検出することが重要です**。これにより、Security Managerはこれらのポリシーに関する現在の設定を保持できます。

ポリシーを再検出せず、新たに管理対象にしたポリシーを未設定のままにすると、デバイスへの次の展開時に、デバイスに定義されている既存の設定が削除されます。すでに管理対象になっているデバイス上のポリシーの検出については、 Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

（注） Security Manager によって管理対象外にされた機能は、CLI コマンドまたは FlexConfig を使用して手動で変更できます。FlexConfig の詳細については、FlexConfig の管理 （431 ページ）を参照してください。

ポリシーの検出

ポリシー検出を使用すると、既存のネットワーク設定を Security Manager に取り込んで管理できます。ポリシー検出は、動作中のデバイスの設定をインポートするか、または設定ファイルをインポートすることによって実行できます。構成ファイルをインポートする場合、ファイルはデバイスで（たとえば、Cisco IOS ソフトウェアデバイスで **show run** コマンドを使用して）生成されている必要があります。他の形式の構成ファイルは検出できません。

ポリシー検出は、New Device ウィザードで関連するオプションを選択してデバイスを追加するときに開始できます。詳細については、デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。

デバイス ビューから既存のデバイスのポリシー検出を開始することもできます。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

デバイスのポリシー検出を開始すると、そのデバイス上の設定が分析され、デバイスを管理できるように Security Manager ポリシーおよびポリシー オブジェクトに変換されます。インポートした設定によって一部のポリシーだけが定義される場合、警告が表示されます。追加の設定が必要な場合は、Security Manager インターフェイスの関連するページに移動して、ポリシー定義を完了する必要があります。インポートした設定が無効な場合も、警告とエラーが表示されます。

ポリシー検出の実行後、変更を送信して（または、Workflow モードで作業している場合はアクティビティを承認して）、情報を変更レポートに含め、情報を他のユーザが使用できるようにする必要があります。検出されたポリシーを変更した場合は、変更を有効にするためにデバイスに展開する必要があります。詳細については、展開の管理 （481 ページ）を参照してください。

ヒント すべてのデバイスに適用される検出関連の設定を行うには、[Security Manager Administration] ウィンドウを使用します。詳細については、[Discovery] ページ （674 ページ）を参照してください。

ポリシー検出と VPN

Security Manager では、個々のデバイスに対して検出を実行する以外に、ネットワークにすでに展開されている VPN を検出できます。VPN の検出方法は、検出対象の VPN のタイプによって異なります。

- サイト間 VPN：ウィザードに従って検出手順を実行します。詳細については、サイト間 VPN ディスカバリ （1406 ページ）を参照してください。

ヒント　サイト間VPNの検出後すぐにファイルに展開することを推奨します。これにより、Security Manager はデバイスで設定されている、関連する CLI コマンドを完全に管理できます。

- IPSec および SSL リモート アクセス VPN：デバイスをインベントリに追加する場合、またはインベントリにすでに存在するデバイスのポリシーを検出する場合は、デバイスのポリシーを検出するときに IPSec および SSL VPN を検出できます。これらの VPN に関連するポリシーは、通常のデバイス ポリシーとして扱われます。ただし、検出オプションを選択するときに、RA VPN ポリシーを検出するように選択する必要があります。リモート アクセス VPN ポリシー検出の詳細については、リモート アクセス VPN ポリシーの検出（1669ページ）を参照してください。ポリシー検出の実行の詳細については、デバイス インベントリへのデバイスの追加 （94 ページ）および Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

（注）　設定ファイルを使用してデバイスを追加し、デバイスの追加中にセキュリティ ポリシーを検出する場合、Security Manager では、検出対象のデバイスからファイルをダウンロードする必要があるポリシーを正常に検出できません。これは、特に SSL VPN 設定に **svc image** コマンドを含むデバイスに影響します。Security Manager のデータベースには参照先ファイルはないため、検出された設定に対して **no** 形式のコマンドが生成されます。

ポリシー検出および Cisco IOS ルータと Catalyst デバイス

Security Manager では、Cisco IOS ソフトウェアで使用可能なすべてのコマンドのサブセットがサポートされ、そのほとんどはセキュリティ関連のコマンドです。サポートされているすべての Cisco IOS コマンドを検出できます。サポートされていないコマンドは、Security Manager で設定されているポリシーと直接競合しないかぎり、そのまま残されます。Cisco IOS ルータに対するポリシー検出の実行の詳細については、ルータ ポリシーの検出 （3004 ページ）を参照してください。Catalyst デバイスに対するポリシー検出の実行の詳細については、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出 （3402 ページ）を参照してください。

ヒント　Cisco IOS ルータまたは Catalyst デバイスの検出後すぐにファイルに展開することを推奨します。これにより、Security Manager はデバイスで設定されている、関連する CLI コマンドを完全に管理できます。

ポリシー検出およびファイアウォール セキュリティ コンテンツ

セキュリティ コンテキストを含むデバイスを追加する場合、すべてのコンテキストとポリシーを同時に検出する必要があります。それ以外の場合、各コンテキストのポリシーを別々に検出する必要があります。デバイスを追加するときに、コンテキストとして [MULTI] を選択しま

す。[管理対象外デバイスのセキュリティコンテキスト（Security Context of Unmanaged Device）] は選択しません（このオプションを選択すると、管理コンテキストだけがインポートされますが、管理コンテキストにはデバイス上の他のセキュリティコンテキストとの関連性がありません。このオプションは、セキュリティコンテキストを親デバイスとは無関係に管理する場合に選択してください）。デバイスの追加方法によっては、セキュリティコンテキストを検出するオプションを選択しなければならない場合があります。検出中、Security Manager はセキュリティコンテキスト名を親の名前の末尾に付加して、各セキュリティコンテキストを識別し、個別のデバイスとしてデバイスリストに追加します。たとえば、親が pix_141 の場合、管理コンテキストは pix_141_admin となります（セキュリティ コンテキストの命名ルールを制御できます。詳細については、[Discovery] ページ （674 ページ）を参照してください）。新しいセキュリティ コンテキストを作成したり、既存のコンテキストを削除したりする以外に、それらのコンテキストのポリシーを作成または削除することもできます。

Catalyst 6500 デバイスに含まれる FWSM の複数のセキュリティ コンテキストを作成し、シャーシで IOS ソフトウェアを実行する場合は、シャーシの SSH クレデンシャルを使用してシャーシ デバイスを追加します。その後、Security Manager はシャーシの各 FWSM を識別し、それぞれを追加するためのオプションを表示できます。FWSM の検出中、Security Manager は FWSM や各コンテキストのポリシーなど、各 FWSM のセキュリティ コンテキストを検出します。ただし、デバイスで Catalyst OS を使用する場合は、各 FWSM を個別に検出する必要があります。

デバイスをインベントリに追加する方法の詳細については、デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。

ポリシー検出および IPS デバイス

IPS デバイスのポリシーを検出すると、そのデバイスに定義されている仮想センサーが、その仮想センサーに定義されているポリシーとともに検出されます。複数の仮想センサーで同じポリシーが使用される場合、そのポリシーは共有ポリシーとして作成され、仮想センサーに割り当てられます。1 つの仮想センサーに定義されたポリシーまたは親デバイスだけに定義されたポリシーは、ローカルポリシーとして作成されます。個々の仮想センサーだけのポリシーは検出できません。検出できるのは、親デバイス上のポリシーだけです。仮想センサーに割り当てられていない親デバイス上のポリシーが検出された場合、それらのポリシーはデバイスまたは仮想センサーに割り当てられない共有ポリシーとして作成されます。

仮想センサーを含む IPS デバイスの検出後、仮想センサーをデバイス セレクタに表示するには、変更をデータベースに送信する必要があります。

ポリシー検出とオブジェクトグループ

ポリシー検出を実行すると、PIX、ASA、FWSM、および IOS 12.4(20)T+ デバイスにすでに設定されているオブジェクト グループは、ポリシー オブジェクトとして Security Manager に取り込まれます。Security Manager のポリシー オブジェクトがオブジェクト グループに変換される方法およびその逆の方法の詳細については、ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （426 ページ）を参照してください。

さらに、ASA 8.3+ デバイス上の [オブジェクトネットワーク（Object Network）] 設定と [オブジェクトサービス（Object Service）] 設定は、ホスト、ネットワーク、またはアドレス範囲ネットワーク/ホストオブジェクトあるいは（サービス グループ オブジェクトではなく）サービス オブジェクトとして Security Manager に取り込まれます。唯一の例外として、範囲の開始と終

了に同じアドレスを持つアドレス範囲オブジェクトは、代わりにホスト ネットワーク/ホスト オブジェクトとして作成されます。

（注） IOS デバイスの場合、ACL オブジェクトとして検出されたアクセス コントロール リストで使用されている検出済みオブジェクトは、その後の展開時にオブジェクトのコンテンツによって置き換えられます。ACL オブジェクトで使用されるオブジェクト グループは保持されませんが、Security Manager ポリシー オブジェクトとして検出されます。

ポリシー検出および Security Manager ポリシー オブジェクト

ポリシー検出を実行すると、Security Manager は Security Manager ですでに作成されているポリシー オブジェクトを再利用しようとします。デバイス設定のコンテンツに基づいて、次のアクションが実行される可能性があります。

- 設定内の名前付きポリシー オブジェクト：既存のポリシー オブジェクトのコンテンツがデバイス上の設定と一致する場合は、そのオブジェクトが再利用されます。

  名前付きポリシーオブジェクトのコンテンツが一致しない場合は、ポリシーオブジェクトが再利用され、[検出（Discovery）] 管理ページで [検出されたポリシーオブジェクトのデバイスオーバーライドを許可（Allow Device Override for Discovered Policy Objects）] が選択されていれば、デバイスレベルのオーバーライドが作成されます。詳細については、次の項を参照してください。

  - 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
  - [Discovery] ページ （674 ページ）

- 設定内の名前のないポリシー オブジェクト：既存のポリシー オブジェクトのコンテンツがデバイス上の設定と一致する場合は、そのオブジェクトが使用されます。この動作は、[検出（Discovery）] 管理ページの [ポリシーオブジェクトをインライン値に再利用する（Reuse Policy Objects for Inline Values）] 設定の値を変更することによって制御できます。
- 冗長なオブジェクトを検出するために定義した設定にかかわらず、既存のオブジェクトと同じ定義を持つオブジェクトを検出できます。この設定の詳細については、[Policy Objects] ページ （732 ページ）を参照してください。

ポリシーオブジェクトの詳細については、ポリシーオブジェクトの管理 （287 ページ）を参照してください。

ポリシー検出およびアクセス制御リスト

Security Manager のポリシーには、標準 ACL だけをサポートするもの、または拡張 ACL だけをサポートするものがあります。これは、CLI で両方のタイプがサポートされている場合でも同様です。このような場合、ポリシー検出は次のように機能します。

- Security Manager のポリシーで拡張 ACL だけがサポートされる場合（たとえば、ファイアウォール サービス ポリシー）、そのポリシー用にデバイスで設定されている標準 ACL は、拡張 ACL としてインポートされます。

- Security Manager のポリシーで標準 ACL だけがサポートされる場合（たとえば、IOS ルータ上の SNMP トラップ）、そのポリシー用にデバイスで設定されている拡張 ACL は、標準 ACL としてインポートされます。

検出プロセス中、Security Manager には、インポートされた非アクティブな ACL は無効な状態で表示されます。あとでこれらの無効な ACL を展開すると、ACL はデバイス設定から削除されます。

関連項目

- ポリシー検出に関する FAQ （243 ページ）
- ポリシー検出タスクのステータスの表示 （237 ページ）
- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）

Security Manager にすでに存在するデバイス上のポリシーの検出

インベントリにデバイスを追加する場合、デバイスの追加と同時にポリシーを検出できます。ただし、ポリシー検出をスキップしてあとで実行したり、デバイスの追加後にポリシーを再検出したりすることもできます。

既存のデバイスに対してポリシー検出を開始できるのは、次のような場合です。

- device upgrade などの CLI コマンドを使用してデバイス設定を変更します。このような場合、Security Manager データベースに最新の情報が格納されるように、デバイス上の既存のポリシーを再検出できます。再検出を実行するよりも Security Manager でアウトオブバンド変更を入力することを推奨します。ただし、バージョン 4.13 以降では、単一の検出アクションですべてのポリシーが適切に検出されます（ASA 8.x から 9.x へのアップグレードに適用可能）。
- Security Manager に最初にデバイスを追加するときに検出されなかったポリシーのサブセット（プラットフォーム固有の設定など）を検出する場合。
- ファイアウォールデバイスの出荷時のデフォルト設定をインポートする場合。詳細については、ファイアウォールのデフォルト設定 （2333 ページ）を参照してください。

注意 Security Manager でポリシーを設定した後に、変更を展開するまでにデバイスに対してポリシー検出を実行すると、検出されたポリシーによって、未展開の変更が上書きされます。たとえば、プラットフォーム固有の設定を検出するオプションを選択した場合、検出された設定によって、Security Manager で設定したプラットフォーム固有の未展開のポリシーが上書きされます。検出された設定に、設定した固有のプラットフォームポリシーが含まれていない場合でも、上書きされます。たとえば、プラットフォーム固有の設定を検出すると、検出された設定にルーティング情報が含まれていない場合でも、Security Manager でこのデバイス用に設定したルーティング ポリシーが上書きされます。また、再検出の結果、デバイスに設定された共有ポリシーが検出されたローカル ポリシーに置き換えられる場合もあります。

注意 特定の条件下では、Security Manager がシステムコンテキストで ASA インターフェイスを検出できない場合があります。具体的には、「インベントリ」をチェック（選択）せずにマルチコンテキスト ASA のシステム コンテキストで再検出/展開が行われた場合、Security Manager は他のセキュリティコンテキストのインターフェイスを検出できない可能性があります。これにより、その後の展開で Security Manager が他のコンテキストのインターフェイス設定を変更するか、完全に削除する可能性があります。この問題を回避するには、システムコンテキストの再検出を行うときに、必ず「インベントリ」を選択してください。

はじめる前に

デバイスにポリシーを設定しているユーザやデバイスに設定を展開しているユーザがいないことを確認します。展開ジョブによってデバイスに設定が展開されている間にデバイスのポリシーを再検出すると、再検出後に、展開された変更が表示されないことがあります。ポリシーを再検出する前に、Deployment Manager を使用して、該当デバイスを含むアクティブなジョブがないかどうかを確認してください（**[管理（Manage）] > [展開（Deployments）]** を選択）。展開ジョブ中に間違ってポリシーを再検出した場合は、展開ジョブが完了するまで待ってから再度ポリシーを検出して、Security Manager がデバイスと同期されるようにします。

関連項目

- ポリシー検出タスクのステータスの表示 （237 ページ）
- ポリシーの検出 （223 ページ）
- ポリシー検出に関する FAQ （243 ページ）
- ポリシーについて （209 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）

ステップ 1 単一デバイス上のポリシーを検出するかどうか、または一度に複数のデバイス上のポリシーを検出するかどうかを決定します。ポリシー検出オプションは、検出プロセスの開始方法によって異なります。

- **単一デバイスの検出**：次のいずれかに関連するポリシーを検出する必要がある場合は、単一デバイスの検出だけを使用してポリシーを検出できます（単一デバイスの検出は、インベントリにデバイスを追加するときに実行される検出タイプです）。
  - マルチ コンテキスト モードで実行されている ASA、PIX、および FWSM デバイスのセキュリティ コンテキスト設定
  - IPS デバイスの仮想センサー設定
  - Catalyst デバイスのサービス モジュール情報
  - 設定ファイルからのポリシー検出
  - 出荷時のデフォルト設定からのポリシー検出
- **バルク再検出**：複数のデバイスのポリシーを検出する必要がある場合は、バルク再検出を実行できます。ただし、バルク再検出は、動作中のデバイス（つまり、ネットワークで現在稼働し、アクセス可能なデバイス）に対してだけ実行できます。セキュリティ コンテキスト、仮想センサー、または Catalyst サービス モジュール設定は検出できません（サービス モジュールを含むデバイスを選択するのではなく、サービス モジュールを直接選択した場合は、サービス モジュールを検出できます）。

ステップ 2 **単一デバイスの検出を実行する場合は**、次の手順を実行します。

a) デバイス ビューまたはマップ ビューで、1 つのデバイスだけが選択されていることを確認し、右クリックして [デバイスでポリシーを検出（Discover Policies on Device）] を選択します。[Create Discovery Task] ダイアログボックスが開きます。

ヒント：[バルク再検出（Bulk Rediscovery）] ダイアログボックスが表示された場合は、ダイアログボックスを閉じて再試行する必要があります。1 つのデバイスだけが選択されていることを確認し、コマンドを再発行します。右クリック メニューを使用する必要があります。これが単一デバイスの検出を実行する唯一の方法です。

b) 必要に応じて検出タスク名を変更し、次の検出オプションを選択します。詳細については、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （231 ページ）を参照してください。

- [検出元（Discover From）]：動作中のデバイス（ネットワークでアクティブであり、アクセス可能なデバイス）から検出するか、設定ファイルから検出するか（[参照（Browse）] をクリックして Security Manager サーバー上のファイルを選択）、または出荷時のデフォルト設定（出荷時のデフォルト設定が存在する OS バージョンを実行している ASA、PIX、および FWSM デバイス）から検出するかを指定します。シングル コンテキスト モードで実行されているデバイスまたは個々のセキュリティ コンテキストだけのデフォルト設定を検出できます。

ヒント：PIX、ASA、および FWSM デバイスを手動で追加する場合は（手動定義によるデバイスの追加 （116 ページ）を参照）、[工場出荷時のデフォルト設定（Factory Default Configuration）] 設定を使用することを推奨します。シングル コンテキスト モードのデバイスおよびマルチ コンテキスト モードのデバイスの各セキュリティ コンテキストのデフォルト設定を検出する必要があります。出荷時のデ

フォルトポリシーの詳細については、ファイアウォールのデフォルト設定 （2333 ページ）を参照してください。

- [セキュリティコンテキストのポリシーを検出（Discover Policies for Security Contexts）]：マルチコンテキストモードで実行されているファイアウォールデバイスに定義されているセキュリティコンテキストのポリシーを検出する場合は、このオプションを選択します。

c) 検出するポリシーのタイプを選択します。ポリシー タイプ間の相違の詳細については、サービスポリシーとプラットフォーム固有のポリシー （211 ページ）を参照してください。

- [ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）]：CX モジュールまたはFirePOWER モジュールがインストールされているかどうかを確認します。詳細については、ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）を参照してください。
- [Inventory]：デバイスの基本情報（ホスト名、ドメイン名など）、インターフェイス、およびマルチコンテキスト モードで実行されているデバイス上のセキュリティ コンテキストを検出します。Cisco IOS ルータでは、DSL、PPP、PVC ポリシーなどのすべてのインターフェイス関連ポリシーも検出されます。
- [Platform Settings]：ルーティング ポリシーなどのプラットフォーム固有のポリシーを検出します。
- [Firewall Services]：すべてのプラットフォーム上にある、アクセス ルールやインスペクション ルールなどのファイアウォール サービス ポリシーを検出します。
- [NATポリシー（NAT Policies）]：アドレスプール、スタティック変換ルール、ダイナミック NAT/PAT といったネットワークアドレス変換（NAT）ポリシーを検出します。NAT ポリシーの検出は、ASA、ASA-SM、PIX、および FWSM デバイスでサポートされています。
- [ルーティングポリシー（Routing Policies）]：ASA デバイスのルーティングポリシーを検出します。
- [SSL ポリシー（SSL Policy）]：ASA デバイスの SSL ポリシーを検出します。
- [RA VPNポリシー（RA VPN Policies）]：IKE プロポーザルや IPsec プロポーザルなどの IPSec および SSL リモートアクセス VPN ポリシーを検出します。
- [IPS]：シグニチャや仮想センサーなどの IPS ポリシーを検出します。

詳細については、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （231 ページ）を参照してください。

d) [OK] をクリックします。検出タスクが開始され、[Discovery Status] ダイアログボックスが開くため、タスク ステータスを表示できます（[Discovery Status] ダイアログボックス （238 ページ）を参照）。検出の進行中は Security Manager で他のタスクを実行できません。

ステップ 3 バルク再検出を実行する場合は、次の手順を実行します。

a) デバイス ビューで、次のいずれかを実行します。

- デバイスグループまたは複数のデバイスを選択し、右クリックして [デバイスでポリシーを検出（Discover Policies on Device）] を選択します。[Bulk Rediscovery] ダイアログボックスが開くことを確認します。

ヒント：[ディスカバリタスクの作成（Create Discovery Task）] ダイアログボックスが表示された場合は、ダイアログボックスを閉じて再試行する必要があります。デバイス グループまたは複数のデバイスが選択されていることを確認し、コマンドを再発行します。

- **[ポリシー（Policy）] > [デバイスでポリシーを検出（Discover Policies on Device）]**を選択します。[Device Selector] ダイアログボックスが開きます。[使用可能なデバイス（Available Devices）] リストから検出するデバイスを選択し、[>>] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。[次へ（Next）] をクリックします。

（注） 右クリック コマンドを使用する場合、Security Manager は目的のデバイスが選択されていると見なします。いつでも [戻る（Back）] ボタンをクリックして [デバイスセレクタ（Device Selector）] 画面に戻り、デバイスリストを変更できます。

b) 必要に応じて検出タスク名を変更し、検出オプションを選択します。詳細については、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （231 ページ）を参照してください。

デバイスはデバイス タイプに従ってグループにまとめられ、各タイプ内にデバイス グループ（ある場合）が表示されます。

- 特定のタイプのデバイスすべてに対するオプションを変更するには、デバイス タイプのフォルダを選択し、[Discover Device Settings] オプションを変更します。[Discover] ドロップダウン リストに [Multiple Values] が表示される場合は、そのタイプのデバイスに異なる検出オプションが選択されています。値を変更すると、その変更はすべてのデバイスに適用されます。前述の単一デバイスの検出で説明したポリシー タイプのチェックボックスは、[Policies and Inventory] を選択した場合だけ使用できます。選択したグループ内のすべてのデバイスに使用できるオプションだけが表示されます。そのため、最も適切なオプション セットを選択するには、個々のデバイスを別々に選択する必要があります。
- 単一デバイスのオプションを変更するには、デバイスが見つかるまでフォルダの横にある [+] アイコンをクリックして開き、デバイスを選択して検出オプションを選択します。

（注） オプションのリストが展開されていない場合、すべてのポリシー、すなわちプラットフォーム設定、ファイアウォールポリシー、NAT ポリシー、および RA VPN が検出されます。ただし、オプションのリストを展開すると、使用可能なリストから選択したオプションに基づいて検出が行われます。

c) [終了（Finish）] をクリックします。検出タスクが開始され、[Discovery Status] ダイアログボックスが開くため、タスク ステータスを表示できます（[Discovery Status] ダイアログボックス （238 ページ）を参照）。検出の進行中は Security Manager で他のタスクを実行できません。

[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス

デバイス インベントリにすでに存在するデバイスのポリシーを Security Manager で検出するには、[Create Discovery Task] ダイアログボックスを使用します。一度に複数のデバイスのポリシーを検出するには、[Bulk Rediscovery] ダイアログボックスを使用します。ポリシー検出のオプションは、使用するダイアログボックスによって異なります。これらの各ダイアログボック

スを開く方法など、手順の詳細については、 Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

インベントリにデバイスを追加するときにポリシーを検出することもできます。デバイスの追加の詳細については、 デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。

ナビゲーション パス

デバイス ビューで、デバイス セレクタからデバイスを選択し、次のいずれかを実行します。

- [ポリシー（Policy）] > [デバイスでポリシーを検出（Discover Policies on Device）] を選択して、バルク再検出を実行します。
- デバイスセレクタでデバイスを右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択します。単一デバイスを選択した場合は、[Create Discovery Task] ダイアログボックスが表示されます。それ以外の場合は、バルク再検出を実行します。

ヒント マップビューでデバイスを右クリックし、[デバイスでポリシーを検出（Discover Policies on Device）] を選択することもできます。

関連項目

- ポリシーの検出 （223 ページ）
- ポリシー検出タスクのステータスの表示 （237 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）
- [Discovery Status] ダイアログボックス （238 ページ）

フィールド リファレンス

表 34 : [Create Discovery Task] ダイアログボックス

要素	説明
Discovery Task Name	検出タスクに割り当てられる名前。タスクの名前は、現在の日時に基づいて自動的に生成されますが、必要に応じてこの名前を変更できます。

要素	説明
[Selected Devices] テーブル （バルク再検出だけ）	再検出対象として選択したデバイス。デバイスはデバイスタイプに従ってグループにまとめられ、各タイプ内にデバイスグループ（ある場合）が表示されます。 • 特定のタイプのデバイスすべてに対するオプションを変更するには、デバイスタイプのフォルダを選択し、[Discover Device Settings] オプションを変更します。[Discover] ドロップダウンリストに [Multiple Values] が表示される場合は、そのタイプのデバイスに異なる検出オプションが選択されています。値を変更すると、その変更はすべてのデバイスに適用されます。前述の単一デバイスの検出で説明したポリシータイプのチェックボックスは、[Policies and Inventory] を選択した場合だけ使用できます。選択したグループ内のすべてのデバイスに使用できるオプションだけが表示されます。そのため、最も適切なオプションセットを選択するには、個々のデバイスを別々に選択する必要があります。 • 単一デバイスのオプションを変更するには、デバイスが見つかるまでフォルダの横にある [+] アイコンをクリックして開き、デバイスを選択して検出オプションを選択します。 **ヒント**：再検出対象として選択したデバイスを変更するには、[戻る（Back）] をクリックして [デバイスセレクタ（Device Selector）] ダイアログボックスに移動します。
Discover From Config. ファイル（File） （バルク再検出には使用不可）	検出するポリシー情報のソース： • [Live Device]：デバイスから直接ポリシーを検出します。 • [Config File]：設定ファイルからポリシーを検出します。[設定ファイル（Config File）] フィールドにファイルの場所を指定します。[参照（Browse）] をクリックして、Security Manager サーバー上のファイルを選択します。 デバイスで（たとえば、**show run** コマンドを使用して）生成された設定ファイルからだけポリシーを検出できます。詳細については、設定ファイルからのデバイスの追加 （112 ページ）を参照してください。 • [Factory Default Configuration]：ファイアウォールデバイスの出荷時のデフォルト設定を含むファイルを使用して、そのデバイスに対して検出を実行します。Security Managerによって、選択したデバイスに適切なファイル（[Config File] 編集ボックスに表示される）が自動的に選択されます。このオプションは、Security Manager に ASA、PIX、または FWSM デバイスで実行されている OS バージョンのデフォルト設定がある場合だけ使用できます。シングルコンテキストモードで実行されているデバイスまたは個々のセキュリティコンテキストだけのデフォルト設定を検出できます。詳細については、ファイアウォールのデフォルト設定 （2333 ページ）を参照してください。

要素	説明
セキュリティコンテキストのポリシーの検出 （バルク再検出には使用不可）	マルチ コンテキスト モードで実行されているファイアウォール デバイスに設定されている各セキュリティ コンテキストのポリシーを検出するかどうかを指定します。このフィールドは、PIX、ASA、およびFWSMデバイスだけに適用されます。 選択を解除すると、Security Manager はデバイス全体をシングルコンテキスト モードで設定された単一のポリシー セットを持っているものとして処理します。 セキュリティ コンテキストの詳細については、ファイアウォール デバイスでのセキュリティ コンテキストの設定（2979ページ）を参照してください。

要素	説明
Policies to Discover（単一デバイスの検出の場合） Discover Device Settings（バルク再検出の場合）	

要素	説明
	選択したデバイス上の検出するポリシー タイプ。 （注） バルク再検出の場合、[検出（Discover）] ドロップダウンメニューから [ポリシーとインベントリ（Policies and Inventory）] を選択し、[インベントリのみ（Inventory Only）]（他のポリシータイプを検出しないでインベントリを検出する場合）または [ASA-CX/FirePOWER モジュールの検出（Detect ASA-CX/FirePOWER Module）]（他のポリシーを検出せずに CX または FirePOWER モジュールがインストールされるかどうかを確認する場合）をオンにします。ドロップダウンリストで [複数の値（Multiple Values）] が選択されている場合は、選択したグループ内のデバイスで別の検出オプションが選択されています。選択を変更すると、変更はグループ内のすべてのデバイスに適用されます。 次の検出オプションがあります。 • [ASA-CX/FirePOWER モジュールの検出（Detect ASA-CX/FirePOWER Module）]：CX モジュールまたは FirePOWER モジュールがインストールされているかどうかを確認します。詳細については、ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）を参照してください。 • [Inventory]：ホスト名、ドメイン名などのデバイス情報、インターフェイス、およびマルチコンテキストモードで実行されているファイアウォール デバイスのセキュリティ コンテキストが含まれます。Cisco IOS ルータでは、DSL、PPP、PVC ポリシーなどのすべてのインターフェイス関連ポリシーも検出されます。 • [Platform Settings]：選択したデバイスに設定できるすべてのプラットフォーム固有のポリシーが含まれます。 • [Firewall Services]：すべてのファイアウォール サービス ポリシーが含まれます。詳細については、ファイアウォール サービスの概要 （755 ページ）を参照してください。 • [NAT ポリシー（NAT Policies）]：アドレスプール、スタティック変換ルール、ダイナミック NAT/PAT といった、選択したデバイスで設定されているすべてのネットワークアドレス変換（NAT）ポリシーが含まれます。NAT ポリシーの検出は、ASA、ASA-SM、PIX、および FWSM デバイスでサポートされています。詳細については、ネットワーク アドレス変換の設定 （1307 ページ）を参照してください。 • [ルーティングポリシー（Routing Policies）]：ASA デバイスのルーティングポリシーを検出します。詳細については、ファイアウォール デバイスでのルーティング ポリシーの設定 （2703 ページ）を参照してください。 • [SSL ポリシー（SSL Policy）]：ASA デバイスの SSL ポリシーを検出し

要素	説明
	ます。 • [RA VPN Policies]：選択したデバイスに設定されているすべての IPSec および SSL リモート アクセス VPN ポリシーが含まれます。デバイスがリモート アクセス VPN 設定をサポートしていない場合、このオプションはディセーブルになります。詳細については、リモートアクセス VPN の管理の基礎 （1655 ページ）を参照してください。 • [IPS Policies]：選択したデバイスに設定されているすべての IPS ポリシーが含まれます。詳細については、IPS 設定の概要 （2088 ページ）または Cisco IOS IPS 設定の概要 （2318 ページ）を参照してください。
	（注） • [ルーティングポリシー（Routing Policies）] オプションと [SSL ポリシー（SSL Policy）] オプションは、適応型セキュリティアプライアンス（ASA）デバイスにのみ適用されます。 • 検出するポリシーとして [プラットフォーム設定（Platform Settings）] を選択する場合、[プラットフォーム設定（Platform Settings）] のサブオプションである [ルーティングポリシー（Routing Policies）] と [SSL ポリシー（SSL Policy）] の選択は解除できません。 • ルーティングポリシーと SSL ポリシーのいずれかまたは両方を検出するには、[プラットフォーム設定（Platform Settings）] オプションの選択を解除し、[ルーティングポリシー（Routing Policies）] と [SSL ポリシー（SSL Policy）] のいずれかまたは両方を選択して、それらのポリシーのみを検出します。 • 非 ASA デバイスの場合、[ルーティングポリシー（Routing Policies）] オプションおよび [SSL ポリシー（SSL Policy）] オプションが表示される場合がありますが、常に選択できません。 • バルク再検出では、トランスペアレントモードおよびシステムコンテキストの場合、[ルーティングポリシー（Routing Policies）] オプションを選択できますが、検出は行われません。

ポリシー検出タスクのステータスの表示

ポリシー検出を開始すると、検出タスクが作成されます。検出対象のデバイスの数にかかわらず、ポリシー検出の開始ごとにタスクが 1 つだけ作成されます。

現在のポリシー検出タスクのステータスは、タスクの開始時に自動的に開く [Discovery Status] ダイアログボックスで確認できます。このダイアログボックスには、タスクに関する概要情報や検出対象の各デバイスに関する詳細など、検出タスクに関する更新されたステータス情報が表示されます。

必要に応じて検出タスクを中断できます。単一デバイスに対してポリシー検出を実行する場合、タスクを中断すると、検出は不完全になります。このような場合は、情報を削除し、検出を再度開始することを推奨します。複数のデバイスに対してポリシー検出を実行する場合、操作を中断する前に検出が完了したデバイスは完全に検出されます。検出が不完全なデバイスの情報は、Security Manager によって自動的に廃棄されます。

検出プロセス中に問題が発生した場合は、[Discovery Status] ダイアログボックスに該当する警告やエラー メッセージも表示されます。たとえば、設定ファイル内の CLI コマンドで完全な Security Manager ポリシーが定義されていない場合は、関連する Security Manager ポリシー ページでポリシー定義を完了する必要があることを示す警告メッセージが表示されます。

詳細については、[Discovery Status] ダイアログボックス （238 ページ）を参照してください。

以前の検出タスクに関する情報を表示するには、**[管理（Manage）] > [ポリシー検出ステータス（Policy Discovery Status）]** を選択して、[ポリシー検出ステータス（Policy Discovery Status）] ウィンドウを開きます。ウィンドウの上部のペインで検出タスクを選択すると、タスクの結果が下部のペインに表示されます。[Policy Discovery Status] ウィンドウの使用法の詳細については、[Policy Discovery Status] ページ （240 ページ）を参照してください。

関連項目

- Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）
- ポリシー検出に関する FAQ （243 ページ）
- ポリシーの検出 （223 ページ）

[Discovery Status] ダイアログボックス

[Discovery Status] ダイアログボックスでは、現在のポリシー検出タスクに関する詳細情報を表示します。このダイアログボックスには、タスクのステータスに関する一般情報および検出対象のデバイスによって生成された警告やエラーに関する詳細情報が表示されます。

[Discovery Status] ダイアログボックスは、既存のデバイスに対して検出タスクを開始するとき、およびネットワーク、設定ファイル、またはエクスポート ファイルからデバイスを追加するときに自動的に開きます。検出タスクの開始の詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

関連項目

- ポリシー検出タスクのステータスの表示 （237 ページ）
- ポリシーの検出 （223 ページ）
- ネットワークからのデバイスの追加 （100 ページ）
- ネットワークからのデバイスの追加 （100 ページ）
- インベントリ ファイルからのデバイスの追加 （122 ページ）

フィールド リファレンス

表 *35 : [Discovery Status]* ダイアログボックス

要素	説明
進行状況バー	現在のデバイスに対する検出タスクの何 % が完了したかを示します。
ステータス	検出タスクの現在の状態。
Devices to be discovered	このタスクで検出するデバイスの合計数。この数には、サービスモジュール、セキュリティ コンテキスト、および仮想センサーが含まれます。
Devices discovered successfully	エラーが発生することなく検出されたデバイスの数。
Devices discovered with errors	検出中にエラーを生成したデバイスの数。

[Discovery Details] テーブル	検出対象のデバイス。デバイスを選択すると、概要リストの下にあるメッセージ リストに、そのデバイスの検出中に生成されたメッセージが表示されます。デバイス名以外にテーブルに含まれる情報は次のとおりです。
	• [Severity]：検出タスクの全体の重大度。たとえば、検出タスクが正常に完了した場合は、情報アイコンが表示されます。タスクが失敗した場合は、エラー アイコンが表示されます。
	• [State]：選択したデバイスにおけるポリシー検出タスクの現在の状態。
	  • [Device Added]：デバイスが Security Manager に追加されましたが、ポリシー検出はまだ開始されていません。
	  • [Discovery Started]：ポリシー検出が開始されました。
	  • [Reading and Parsing Device Config]：ポリシー検出タスクによってデバイス設定が解釈されています。
	  • [Importing Objects]：ポリシー検出タスクによって設定からオブジェクトがインポートされています。
	  • [Importing Policies]：ポリシー検出タスクによって設定からポリシーがインポートされています。
	  • [Discovery Complete]：ポリシー検出が正常に完了しました。
	  • [Discovery Failed]：ポリシー検出がエラーにより失敗しました。
	• [Discovered From]：ポリシー情報のソース。たとえば、設定ファイルからの検出時は、このフィールドにファイルの名前とパスが表示されます。

要素	説明
Messages list	選択したデバイスの検出中に生成されたメッセージ。メッセージを選択すると、リストの右側のフィールドに詳細情報が表示されます。
説明	[Message list] で選択されたメッセージに関する詳細情報。
操作	説明されている問題を解決するために実行する必要がある手順。
[Generate Report] ボタン	このジョブの検出ステータス レポートを作成するには、このボタンをクリックします。レポートは、ジョブの概要を含む PDF ファイルとして、クライアント システムに保存されます。ユーザはこのレポートを独自の目的で使用したり、Cisco TAC の問題のトラブルシューティングに使用したりできます。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成 （636 ページ）を参照してください。
[Abort] ボタン	検出タスクを中断します。 単一デバイスに対するポリシー検出の実行時にタスクを中断すると、そのデバイスの検出は不完全になります。このような場合は、情報を削除し（たとえば、アクティビティを廃棄して）、検出を再度開始することを推奨します。 複数のデバイスに対するポリシー検出の実行時にタスクを中断すると、検出が不完全なデバイスの情報は自動的に廃棄されます。操作を中断する前に検出が完了したデバイスは完全に検出されます。

[Policy Discovery Status] ページ

[Policy Discovery Status] ページでは、以前のポリシー検出タスクやデバイス追加タスクのステータスを表示します。

ナビゲーション パス

[管理（Manage）] > [ポリシー検出ステータス（Policy Discovery Status）] を選択します。

関連項目

- ポリシー検出タスクのステータスの表示 （237 ページ）

フィールド リファレンス

表 *36 : [Policy Discovery Status]* ページ

要素	説明
[Task] テーブル ウィンドウの上部に、以前のポリシー検出タスクまたはデバイス追加タスクが表示されます。タスクを選択すると、ウィンドウの下部にそのタスクに関する詳細情報が表示されます。テーブルのカラムには、タスクの全体的なステータス情報が表示されます。 セキュリティ コンテキストを含むデバイスを追加すると、コンテキスト検出が個別のポリシー検出タスクとして表示されます。	
名前	検出タスクまたはデバイス追加タスクの名前。これは、システムによって生成された名前またはデバイス ポリシーの再検出時に指定した名前です。
タイプ（Type）	タスクのタイプ。[Policy Discovery]（デバイス ポリシーを再検出する場合）、または [Add Device]（New Device ウィザードを使用してデバイスを追加し、ポリシーの検出を選択した場合）。
開始時刻	タスクが開始された時刻。
終了時間（End Time）	タスクが終了した時刻。
ステータス	タスクの全体のステータス。次のいずれかです。 • [Completed successfully]：タスクは成功しました。 • [Completed with errors]：タスクは部分的に成功しました。一部のポリシーが検出されなかった場合、またはデバイスが追加されてポリシーが検出されなかった場合は、このステータスが表示されます。 • [Completed with warnings]：タスクは成功しましたが、軽微な問題が発生しました。 • [Failed]：タスクは失敗しました。エラーまたは検出の中断により、ポリシーが検出されなかったか、またはデバイスが追加されませんでした。

要素	説明
[Generate Report] ボタン	選択したジョブの検出ステータス レポートを作成するには、このボタンをクリックします。 レポートは、ジョブの概要を含む PDF ファイルとして、クライアント システムに保存されます。ユーザはこのレポートを独自の目的で使用したり、Cisco TAC の問題のトラブルシューティングに使用したりできます。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成 （636 ページ）を参照してください。
[Refresh] ボタン	このボタンをクリックすると、タスク リストがリフレッシュされ、バックグラウンドで実行されているタスクがある場合、または新しいタスクが作成された場合に情報が更新されます。
[削除（Delete）] ボタン	このボタンをクリックすると、選択したタスクがデータベースから削除されます。古いタスクを削除しても、関連するデバイスや検出されたポリシーに影響しません。
[Discovery Details] または [Import Details] テーブル これらのテーブルには、選択したタスクに含まれるデバイスが表示されます。テーブル名は、タスクのタイプによって異なります（ポリシー検出タスクの場合は [Discovery Details]、デバイスの追加タスクの場合は [Import Details]）。 デバイスを選択すると、テーブルの下にあるメッセージ リストに、そのデバイスに対するタスクの実行中に生成されたメッセージが表示されます。	
デバイス	デバイスの名前。名前のあとに (deleted) が続く場合、デバイスは Security Manager インベントリに存在しません。
Config File （[Import Details] だけ）	設定ファイルの場所。このフィールドは、設定ファイルからインポートする場合だけ表示されます。
タスク タイプ（Task Type） （[Import Details] だけ）	次のいずれかです。 • [Import only]：デバイスを Security Manager に追加します。 • [Import and Discover]：デバイスを追加してポリシーとインベントリを検出するか、またはデバイスを追加してポリシーを検出します。
重大度	次のいずれかのアイコンが表示されます。 • エラー：デバイスの追加またはポリシー検出が失敗しました。 • 情報：デバイスが正常に追加されたか、またはポリシー検出が成功しました。

要素	説明
状態 詳細（Details）	これらのフィールドは、[Discovery Details] テーブルと [Import Details] テーブルで異なる名前が使用されますが、意味は同じです。デバイスに対するタスクのステータスが表示されます。 • [Device Added]：デバイスは正常にインベントリに追加されました。 • [Device Add Failed]：デバイスはインベントリに追加されませんでした。 • [Discovery Completed]：検出は成功し、検出されたポリシーが Security Manager データベースに追加されました。 • [Discovery Failed]：エラーが発生したため、ポリシーは検出されませんでした。
Discovered From （[Discovery Details] だけ）	次のいずれかです。 • [Live Device]：Security Manager は、デバイスに接続して設定とポリシー情報を取得しました。 • [File]：Security Manager は、設定ファイルから設定とポリシー情報を取得しました。
Messages list	選択したデバイスに対するタスクの実行中に生成されたメッセージ。メッセージを選択すると、リストの右側のフィールドに詳細情報が表示されます。重大度アイコンには、次の意味があります。 • エラー：問題が検出されました。 • 警告：検出中に軽微な問題が発生しました。 • 情報：選択したデバイスに関する情報メッセージ。
説明	[Message list] で選択されたメッセージに関する詳細情報。
操作	説明されている問題を解決するために実行する必要がある手順。

ポリシー検出に関する FAQ

次の質問と回答では、ポリシー検出によってデバイス設定を Security Manager ポリシーに取り込む方法について説明します。

質問：ポリシー検出はどのように動作しますか。

回答：ポリシー、設定、およびインターフェイス（インベントリ）を検出するデバイスを選択すると、Cisco Security Manager は動作中のデバイスから実行コンフィギュレーションを取得す

るか、または指定された設定（構成ファイルからの検出時）を取得し、CLI を Cisco Security Manager のポリシーとオブジェクトに変換します。インポートされた設定は、デバイスの初期設定として Configuration Archive に追加されます。検出後、検出されたポリシーとオブジェクトを確認したり、データベースにコミットするかどうかを決定したりできます。検出されたポリシーやオブジェクトが適切でない場合は、廃棄できます。コミットと廃棄は検出されたすべてのデバイス全体に影響し、デバイス単位で実行することはできません。

質問：どのようなときにポリシーを検出する必要がありますか。

回答：通常は、デバイスを Cisco Security Manager に追加するときにポリシーを検出します。ただし、動作中のデバイスまたは設定ファイルをインポートするのではなく、Security Manager でデバイスを作成する場合は、デバイスの追加後にポリシー検出を実行する必要があります。また、たとえば CLI を使用してデバイスに加えられたアウトオブバンド変更と Security Manager を同期する場合にも、ポリシー検出を実行する必要があります。

質問：検出結果はどのように確認すればよいですか。

回答：検出タスクを開始すると、ウィンドウが開き、検出のステータスと結果が表示されます。[ポリシー検出スタータス（Policy Discovery Status）] ページ（**[管理（Manage）] > [ポリシー検出スタータス（Policy Discovery Status）]** を選択）で検出タスク結果の履歴を表示することもできます。

質問：検出されないコマンドは Cisco Security Manager に表示されますか。また、それらのコマンドにはどう対処すればよいですか。

回答：検出ステータスウィンドウの [メッセージの概要（Message Summary）] セクションに移動し、[未検出のコマンド（Commands Not Discovered）] を選択します。[Description] フィールドに検出されなかったコマンドが表示されます。コマンドをデバイスから削除して検出プロセスを繰り返すか、またはそのまま続行できます。続行すると、Security Manager によって次回の展開時にサポートされないコマンドが削除されます。

デバイスで見つかったコマンドが Security Manager でサポートされていない場合、一般に検出は中断されません。ただし、デバイスにサポートされていないオブジェクトグループを参照するアクセス コントロール エントリ（ACE）がある場合、検出は中断されます。「**User groups not supported**」などのその他のエラーメッセージにも、検出されなかったコマンドに関する詳細が示される場合があります。推奨対処については、[Action] ボックス内の情報を参照してください。

質問：検出されたポリシーは、ユーザーインターフェイスにどのように反映されますか。

回答：Cisco Security Manager によってデバイスコマンドがポリシーに変換されます。デバイス設定から検出されたポリシーと、Security Manager で直接定義されたポリシーの間に、表示上の違いはありません。

質問：PIX または ASA デバイスに Auto Update Server を使用しています。ポリシーを検出するにはどうすればよいですか。

回答：デバイスにスタティック IP アドレスが割り当てられている場合は、デバイスからポリシーを検出できます。デバイスにダイナミック IP アドレスが割り当てられている場合は、デバイスの構成ファイルから（オフラインで）ポリシーを検出する必要があります。

質問：Cisco Secure ACS を使用して Cisco Security Manager に対する認証と認可を管理しています。これはポリシー検出にどのように影響しますか。

回答：ポリシー検出を実行して Cisco Security Manager で該当デバイスを管理する前に、すべての管理対象デバイスを Cisco Secure ACS に追加する必要があります。これには、PIX/ASA/FWSM デバイス上のセキュリティ コンテキストが含まれます。詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

質問：VPN またはルータ プラットフォーム ポリシーを検出したあと、何をすればよいですか。

回答：これらの機能の検出方法では、Cisco Security Manager は、検出された VPN ポリシーやルータ プラットフォーム ポリシーを展開するまで、ポリシーを管理しません。つまり、ルータを検出してから、いずれかのポリシーの割り当てを解除して展開すると、ルータの設定からコマンドは削除されません。そのため、VPN ポリシーまたはルータ プラットフォーム ポリシーを検出後すぐにファイルへの展開を実行し、その後これらのポリシーに変更を加えることを推奨します。最初の展開後、必要に応じてこれらのポリシーを再設定したり、変更を展開したりできます。

質問：デバイス上のポリシーを検出し、変更しないで Cisco Security Manager から展開した場合、デバイス上の元の設定と展開後の設定にはどのような違いがありますか。

回答：一般に、サポートされていない CLI コマンドの FlexConfig を設定した場合、新しい設定と元の設定の間に違いはありません。ただし、ACL またはオブジェクト グループの命名方式が多少変更になる場合があります。詳細については、ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （426 ページ）を参照してください。さらに、ポリシーで使用されていない検出済みオブジェクトは設定から削除されます。新しい設定が古い設定と機能的に同じであっても、同じコマンドが使用されない場合もあります。

質問：Cisco Security Manager では、ACL やオブジェクトグループの現在の CLI 命名方式はどのように処理されますか。

回答：デバイスからポリシーを検出すると、Cisco Security Manager は使用されているポリシーと同じ名前を使用しようとします。ただし、命名方式によっては、デバイスに対して定義したポリシーと検出により作成されたポリシーの間に若干の違いが生じることがあります。さらに、デバイス上の既存の ACL やオブジェクトと、新しいポリシーやオブジェクトに必要な名前の間に、名前の競合が発生する可能性があります。この場合、デバイスが誤って設定されないように、Security Manager によって別の名前が生成されます。たとえば、検出されたオブジェクトの名前が、Security Manager にすでに存在する同じタイプのオブジェクトと競合する場合は、新しいオブジェクトの名前にサフィックスが追加されて一意の名前が生成されるか、またはデバイス レベルのオーバーライドが作成されます。

質問：Cisco Security Manager では、すべてのコンフィギュレーション コマンドが検出されて、取り込まれますか。

回答：Cisco Security Manager ですべてのデバイス コンフィギュレーション コマンドが検出されるわけではありません。代わりに、セキュリティ ポリシーが検出されます。検出されなかったコンフィギュレーション コマンドについては、FlexConfig 機能を使用して、Security Manager でサポートされていないコマンドを追加します。

質問：すでに Cisco Security Manager に存在するデバイス上のポリシーを再検出した場合、デバイスに割り当てられているポリシーはどうなりますか。

回答：すでに Cisco Security Manager で管理されているデバイス上のポリシーを再検出すると、デバイスに割り当てられているポリシーは、新たに検出されたポリシーに置き換えられます。Security Manager データベース内のポリシーとは異なるデバイス上のポリシーだけでなく、選択したポリシー ドメイン内のすべてのポリシー（ファイアウォール サービス、プラットフォーム設定、またはこれらの両方）が置き換えられます。デバイスに共有ポリシーが割り当てられている場合は、割り当てが解除され、共有ポリシーは変更されません（そのため、共有ポリシーを使用する他のデバイスは影響を受けません）。ポリシー検出後、デバイスに割り当てられているすべてのポリシーは、そのデバイス固有になります。つまり、他のデバイスと共有されません。デバイスで共有ポリシーを使用する場合は、ポリシー検出後に割り当てをやり直す必要があります。

さらに、ローカルポリシーに対して行われたカスタマイズも失われます。たとえば、セクションを使用してルールベースのファイアウォールポリシーを編成した場合、セクションは削除され、再検出されたポリシーはエントリのフラットリストになります。

質問：Cisco Security Manager は、ポリシー検出中に既存のポリシーやオブジェクトを使用しますか。

回答：ポリシー検出中、Cisco Security Manager はデバイスのポリシーを作成するときに既存のポリシーオブジェクト（Cisco Security Manager ですでに定義されているオブジェクト）を使用します。ただし、Security Manager は既存のポリシーを再利用しません。検出中に作成されたすべてのポリシーは検出対象のデバイスに対してローカルになります。したがって、Security Manager にデバイスを追加する前に、ネットワーク オブジェクトなどのポリシー オブジェクトを定義すると役立つ場合があります。

質問：デバイスを追加してポリシーを検出したあと、変更をデータベースに送信できません。その代わりに、「Connection Policies Not Set」などの警告が表示されます。デバイスの追加を完了するにはどうすればよいですか。

回答：デバイスを追加してポリシーを検出すると（特に構成ファイルからデバイスを追加する場合）、作成される構成が不完全でデバイスを正しく管理できなくなる場合に Cisco Security Manager から警告が表示されます。たとえば、接続ポリシーは、デバイスへのログインに必要なデバイス クレデンシャル（ユーザ名およびパスワード）と、その他の接続関連の設定（HTTP 設定など）である場合があります。これらの設定がなければ設定が無効になるか、または Security Manager があとでデバイスに接続してデバイスを管理できなくなるため、変更をデータベースに送信できません。これらの設定が完了し、設定が有効であることを確認して、変更をデータベースに再送信してください。

質問：AAA ポリシーにデバイスで検出した AAA 設定が表示されないのはなぜですか。

回答：AAA ポリシーには、認証、許可、およびアカウンティングのデフォルト設定が含まれています。特定のリスト名を指定する他の AAA コマンドは、それらのコマンドを参照するポリシーにマッピングされます。リスト名は、ポリシーによって参照されない場合は検出されません。

質問：ルータに設定されている AAA 方式リストの定義の一部が検出されないのはなぜですか。

回答：Cisco Security Manager では、if-needed などの特定のキーワードがサポートされていません。これらのキーワードを含む方式リストは、キーワードなしに検出されます。デバイス上の

デフォルトの AAA 定義にサポートされていないキーワードが含まれる場合、コマンド全体が検出されません。

質問：server-private コマンドを使用して設定された、IOS ソフトウェアを実行しているデバイスで AAA サーバーを検出できますか。

回答：はい。AAA サーバーを検出できます。ただし、Security Manager によって標準の AAA サーバに変換されます。これらのサーバは、グローバルに使用したり、複数の AAA サーバ グループで使用したりできます。server-private コマンドはサポートされません。

質問：検出とデバイスホスト名について知っておくべきことは何ですか。

回答：デバイスを検出すると、デバイスで検出されたホスト名がホスト名ポリシーに読み込まれます。ただし、[Device Properties] に表示されているホスト名は、この値で更新されません。デバイス プロパティで定義されたホスト名がデバイスの正しい DNS 名であることを確認してください。詳細については、デバイス プロパティについて （93 ページ）を参照してください。

質問：検出された ASA ポリシーからポリシーマップのポリシーに関する説明が CSM によって削除されるのはなぜですか。

回答：ポリシーの検出中、CSM では、ポリシーマップの説明はポリシーからデータベースに移動されないため、設定をプレビューすると、ポリシーマップ内の説明は空白になります。展開後、ASA は、CSM によって展開されたポリシーマップを説明なしで表示します。

デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理

次の項で説明するように、デバイス ビューまたは Site-to-Site VPN Manager を使用して、ローカル ポリシーと共有ポリシーの両方を管理できます。

- ポリシー ステータス アイコン （248 ページ）
- 基本的なポリシー管理の実行 （248 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

デバイスビューにアクセスするには、[ビュー（View）] > [デフォルトビュー（Device View）] を選択するか、またはツールバーの [デバイスビュー（Device View）] ボタンをクリックします。Site-to-Site VPN Manager にアクセスするには、[管理（Manage）] > [サイト間VPN（Site-to-Site VPNs）] を選択するか、またはツールバーの [サイト間VPN Manager（Site-to-Site VPN Manager）] ボタンをクリックします。

関連項目

- デバイス インベントリについて （87 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）

- ポリシーについて （209 ページ）

ポリシー ステータス アイコン

ポリシー名の横に表示されるアイコンを確認すると、ひと目で Security Manager のポリシーのステータスがわかります。

表 *37*：ポリシー ステータス アイコン

アイコン	ステータス（**Status**）
147969	ポリシーが設定されていません。展開時に、デバイス上にすでに存在するこのタイプのポリシーが削除されます。
147967	ローカル ポリシーが設定されています。このポリシーの定義は、このポリシーが設定されているデバイスまたは VPN トポロジだけに影響します。
147968	共有ポリシーが設定されています。このポリシーの定義に加えた変更は、このポリシーが割り当てられているすべてのデバイスまたは VPN トポロジに影響します。
	ポリシーバンドルが設定されています。このポリシーの定義を変更すると、これらのポリシーが同じポリシーバンドル、共有ポリシーを含む別のポリシーバンドルを使用して割り当てられているか、共有ポリシーがポリシーバンドル経由ではなく直接割り当てられているかにかかわらず、このポリシーが割り当てられているすべてのデバイスまたは VPN トポロジに影響します。

関連項目

- ポリシーについて （209 ページ）

基本的なポリシー管理の実行

ここでは、デバイス ビューでローカル ポリシーに対して実行できる操作について説明します。ローカル ポリシーとは、そのポリシーが設定されているデバイスまたは VPN トポロジに固有のポリシーのことです。他のネットワーク要素によって共有されることはありません。

- デバイス ビューにおけるローカル ポリシーの設定 （249 ページ）
- デバイス間でのポリシーのコピー （251 ページ）
- ポリシーの割り当て解除 （255 ページ）（この項は、Site-to-Site VPN Manager にも適用されます）

関連項目

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）
- ポリシーについて （209 ページ）

デバイス ビューにおけるローカル ポリシーの設定

個々のデバイスのローカル プラットフォームやサービス ポリシーを設定するには、デバイス ビューを使用します。各ポリシーでは、NAT、OSPF ルーティング、インスペクション ルールなどのデバイスで実行できる特定の設定やセキュリティ タスクを定義します。ローカル ポリシーとは、そのポリシーが定義されている個々のデバイスに固有の、名前のないポリシーのことです。ローカル ポリシーに加えた変更は、Security Manager で管理されている他のデバイスには反映されません。

ポリシーを設定すると、そのポリシーにロックが適用され、他のユーザは同じポリシーを同時に変更できなくなります。 ポリシーのロックについて （217 ページ）を参照してください。

特定のデバイスに割り当てられたローカル ポリシーを変更できるのは、ポリシーを変更する権限とそのデバイスにアクセスする権限がある場合です。権限の詳細については、Cisco Security Manager インストレーション ガイド [英語] を参照してください。

ポリシーの設定後、デバイス上で変更を有効にするには、そのデバイスに変更を展開する必要があります。詳細については、展開の管理 （481 ページ）を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- デバイス間でのポリシーのコピー （251 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

ステップ 1 デバイス ビューで、デバイス セレクタからデバイスを選択し、デバイス ポリシー セレクタからそのデバイスのポリシーを選択します。ポリシーの詳細は作業領域に表示されます。

ステップ 2 必要に応じてポリシーの定義を変更します。[Help] ボタンをクリックすると、選択したポリシーに固有の情報が表示されます。詳細については、以下を参照してください。

- サイト間 VPN の管理：基本 （1379 ページ）
- リモート アクセス VPN の管理の基礎 （1655 ページ）
- ファイアウォール サービスの概要 （755 ページ）
- IPS 設定の概要 （2088 ページ）

- Cisco IOS IPS 設定の概要 （2318 ページ）
- ルータの管理 （3001 ページ）
- ファイアウォール デバイスの管理 （2331 ページ）
- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理 （3401 ページ）

ステップ 3 [保存（Save）] をクリックして変更を保存します。

この特定のデバイスにこのポリシーを設定するのが初めての場合は、選択したポリシーの横にあるアイコンが変わり、ポリシーが設定されてデバイスにローカルに割り当てられたことを示します。ポリシー ステータス アイコンの詳細については、を参照してください。

ポリシーを保存すると、ポリシーは設定されますが、変更を表示できるのは自分だけです。変更をコミットしてデバイスに展開するには、追加手順を実行します。変更は、Workflow モードで作業しているか、または Workflow 以外のモードで作業しているかによって異なります。追加手順を実行する前に、展開するすべてのポリシーを設定します。ポリシーの変更を一度に 1 つずつ展開する必要はありません。

実行する必要がある追加手順の概要を次に示します。

- 変更を送信します。送信すると、Security Manager サーバ上のデータベースが変更で更新されます。
  - Workflow 以外のモードで、[ファイル（File）] > [送信（Submit）] を選択して変更を送信します。[ファイル（File）] > [送信と展開（Submit and Deploy）] を選択して、1 つの手順で変更の送信と展開を実行することもできます。
  - Workflow モードでは、アクティビティ アプルーバと連携している場合、アクティビティを送信します。アクティビティが承認されると変更がコミットされます。アクティビティ アプルーバと連携していない場合は、自分で自分のアクティビティを承認すると、変更がコミットされます。詳細については、 承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） （202 ページ）および アクティビティの承認または拒否（Workflow モード） （203 ページ）を参照してください。

Workflow モードと Workflow 以外のモードの両方において、ポリシーは送信時に検証されます。検証の詳細については、 アクティビティ/チケットの検証 （200 ページ）を参照してください。

- 変更を展開します。展開すると、デバイスが直接新しい設定で更新されるか、自分で展開できる設定ファイルが作成されるか、またはデバイスが更新を取得する中間サーバ（Auto Update Server、Configuration Engine、または Token Management Server）に設定ファイルがコピーされます。使用する方法は、組織の要件によって決まり、デバイスごとに異なる方法を選択できます。展開の一般情報については、 展開および Configuration Archive の使用 （511 ページ）を参照してください。Workflow モードに基づく特定の手順および展開方法については、次の各項を参照してください。
  - Workflow 以外のモードでの設定の展開 （515 ページ）
  - Workflow モードでの展開ジョブの展開 （530 ページ）
  - Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
  - Token Management Server への設定の展開 （534 ページ）

- デバイスへの直接展開 （491 ページ）
- 中間サーバを使用したデバイスへの展開 （492 ページ）
- ファイルへの展開 （493 ページ）

デバイス間でのポリシーのコピー

複数のポリシーまたはポリシー一式を、あるデバイスから、選択したポリシーをサポートする他のデバイスにコピーすることによって、デバイス設定を合理化できます。これにより、たとえば、既存のファイアウォールデバイスに設定されているのと同じポリシーを新しいファイアウォール デバイスにすばやく簡単に設定できます。

デバイス間でポリシーをコピーすると、ソース デバイス上のローカル ポリシーはターゲット デバイスにローカルにコピーされます。ソース デバイスに割り当てられた共有ポリシーは、ターゲット デバイスにも共有ポリシーとしてコピーされます。

ヒント

- 1 つの共有ポリシーを追加デバイスに割り当てる場合は、ポリシーのコピーではなく、割り当て機能を使用することを推奨します。デバイス ビューにおけるポリシーの共有の詳細については、 デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）を参照してください。
- ソース デバイスと同じ設定やプロパティ（オペレーティング システムのバージョン、クレデンシャル、グループ化属性など）を共有する同じタイプの新しいデバイスを作成するには、[Clone Device] 機能を使用します。詳細については、デバイスの複製 （160 ページ）を参照してください。

関連項目

- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- デバイス ビューにおけるローカル ポリシーの設定 （249 ページ）
- デバイス ビューについて （87 ページ）
- ポリシー ステータス アイコン （248 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

ステップ 1 デバイス ビューで、次のいずれかを実行します。

- [ポリシー（Policy）] > [デバイス間でポリシーをコピー（Copy Policies Between Devices）] を選択します。Copy Policies ウィザードが起動し、手順 1 の [Copy Policies from this Device] ページが表示されます。コピーするポリシーを含むデバイスを選択し、[次へ（Next）] をクリックします。

- デバイスセレクタでデバイスを右クリックし、[デバイス間でポリシーをコピー（Copy Policies Between Devices）] を選択します。Copy Policies ウィザードによってデバイスがソース デバイスとして選択され、手順 2 の [Select Policies to Copy] ページが表示されます。[戻る（Back）] をクリックしてソースデバイスを変更できます。

ヒント　マップビューでデバイスを右クリックし、[デバイス間でポリシーをコピー（Copy Policies Between Devices）] を選択することもできます。

ステップ 2 [Select Policies to Copy] ページでコピーするポリシーを選択します。最初は、ソース デバイスのコピー可能なほとんどのポリシー（ローカルと共有の両方）が選択されます。選択を変更できますが、別のポリシーに依存するポリシーを選択する場合は、従属するポリシーを選択する必要があります。選択が有効でない場合は、選択するように求められます。

ポリシーを選択する場合は、次の点を考慮してください。

- ポリシー グループのチェックボックスをオンにすると、そのグループ内のすべてのポリシーが選択されます。
- ファイアウォールデバイス（ASA、PIX、FWSM）間でポリシーをコピーする場合、フェールオーバー ポリシーをコピーすると自動的にインターフェイス ポリシーがコピーされ、その逆も同様にコピーされます。
- 通常は、インターフェイス ポリシーをコピーしないことを推奨します。これらのポリシーには固有の IP アドレスが含まれている場合があるからです。コピー前に慎重に検討する必要があるその他のポリシー タイプとして、IOS デバイス上の NAT、ルーティング、または IPS ポリシーがあります。
- セキュリティ コンテキスト ポリシー（FWSM、PIX ファイアウォール、または ASA デバイスの場合）を選択する場合は、コンテキストがデバイス セレクタに表示されるように、デバイスをコピーしたあとで変更を送信する必要があります。Workflow 以外のモードで、[ファイル（File）]>[送信（Submit）] を選択します。Workflow モードでは、アクティビティを送信します。

ステップ 3 ポリシー オブジェクトのコピー オプションを使用して、ポリシー オブジェクトの処理方法を指定します。これらのオプションは相互に排他的ではありません。選択する組み合わせには、ターゲット デバイスでのポリシーの定義方法に関連する重要な意味があります。

選択可能なオプションの組み合わせとその意味を次に示します。

- ターゲットデバイスにソースデバイスと同じポリシーオブジェクト設定を適用するには、[ポリシーオブジェクトのグローバル値をコピーする（Copy the Global Values of Policy Objects）] と [ポリシーオブジェクトのオーバーライド値をコピーする（Copy the Overridden Values of Policy Objects] の両方を選択します。
- ポリシーオブジェクトをターゲットデバイスで使用する場合に値がオーバーライドされないようにするには、**どちらの**オプションも選択しません。選択したポリシーでポリシーオブジェクトが使用され、ターゲットデバイス上の対応するポリシーで同じポリシーオブジェクトが使用される場合、ターゲットデバイスで定義されているポリシーオブジェクトの値が保持されます。ターゲットデバイスでポリシーオブジェクトが使用されない場合、ポリシーはポリシーオブジェクトのグローバル値を使用してソースデバイスにコピーされます（ソースデバイス上のオーバーライドは無視されます）。

- ターゲットデバイス上のすべてのポリシーオブジェクトが、ポリシーオブジェクトのグローバル値を使用するには、[ポリシーオブジェクトのグローバル値をコピーする（Copy the Global Values of Policy Objects）] を選択し、[ポリシーオブジェクトのオーバーライド値をコピーする（Copy the Overridden Values of Policy Objects] の選択を解除します。ソース デバイスにポリシー オブジェクトを使用するポリシーが含まれている場合は、ポリシー オブジェクトにグローバル値を使用するポリシーだけがコピーされます。ターゲットデバイスが、ポリシーオブジェクトのローカル値を使用する同等のポリシーをもつ場合、ローカル値はポリシーオブジェクトのグローバル値に置き換えられます。
- ソースデバイス上のローカル値を持つポリシーオブジェクトだけをターゲットデバイスにコピーするには、[ポリシーオブジェクトのグローバル値をコピーする（Copy the Global Values of Policy Objects）] の選択を解除し、[ポリシーオブジェクトのオーバーライド値をコピーする（Copy the Overridden Values of Policy Objects] を選択します。ソースデバイスにポリシーオブジェクトを使用するポリシーが含まれている場合は、ポリシーオブジェクトのグローバル値をオーバーライドするポリシーのみがコピーされます。ターゲットデバイスは、ソースデバイスのポリシーオブジェクトのオーバーライド値を取得します。

次の表は、2 つのオプションのどちらが選択されているかに応じて、ポリシーオブジェクトをコピーした場合に生じ得る結果を示しています。

送信元デバイス	ターゲットデバイス	ユーザ オプション	ターゲットデバイス（コピーの結果）
グローバル定義	参照しない	任意（Any）	グローバル定義
グローバル定義	グローバル定義	任意（Any）	グローバル定義
グローバル定義	デバイスレベルのオーバーライド	どちらのオプションも選択しない	ターゲットデバイスのオーバーライドを保持
		[ポリシーオブジェクトのグローバル値のみをコピーする（Copy the Global Values of Policy Objects）]	グローバル定義
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects）]	ターゲットデバイスのオーバーライドを保持
		両方のオプションを選択	グローバル定義

送信元デバイス	ターゲットデバイス	ユーザ オプション	ターゲットデバイス（コピーの結果）
デバイスレベルのオーバーライド	参照しない	どちらのオプションも選択しない	グローバル定義
		[ポリシーオブジェクトのグローバル値 のみをコピーする（Copy the Global Values of Policy Objects）]	グローバル定義
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects]	ソースデバイスのオーバーライドを使用
		両方のオプションを選択	ソースデバイスのオーバーライドを使用
デバイスレベルのオーバーライド	グローバル定義	どちらのオプションも選択しない	グローバル定義
		[ポリシーオブジェクトのグローバル値のみをコピーする（Copy the Global Values of Policy Objects）]	グローバル定義
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects]	ソースデバイスのオーバーライドを使用
		両方のオプションを選択	ソースデバイスのオーバーライドを使用
デバイスレベルのオーバーライド	デバイスレベルのオーバーライド	どちらのオプションも選択しない	ターゲットデバイスのオーバーライドを保持
		[ポリシーオブジェクトのグローバル値のみをコピーする（Copy the Global Values of Policy Objects）]	ターゲットデバイスのオーバーライドを保持
		[ポリシーオブジェクトのオーバーライド値のみをコピーする（Copy the Overridden Values of Policy Objects]	ソースデバイスのオーバーライドを使用
		両方のオプションを選択	ソースデバイスのオーバーライドを使用

[次へ（Next）] をクリックします。

ステップ 4 [Copy Policies to these Devices] ページで、ポリシーのコピー先のターゲット デバイスを選択します。デバイス グループのチェックボックスをオンにすると、そのグループ内のすべてのデバイスが選択されます。

デバイス セレクタには、コピー対象として選択したすべてのポリシーをサポートするデバイスだけが表示されます。ポリシーのコピー先のデバイスが一部表示されない場合は、ポリシー選択ページに戻って制約

の厳しいポリシーの選択を解除します。次に、もう一度ウィザードを使用して、制約の厳しいポリシーを、そのポリシーをサポートするデバイスのサブセットにコピーします。

インベントリ内に、選択したすべてのポリシーをサポートできる他のデバイスがない場合、デバイス リストは空になります。

ヒント デバイスの選択後、[プレビュー（Preview）] ボタンをクリックすると、コピーするポリシーの概要が表示されます。概要には、選択したデバイス、それらのデバイスにコピーされるポリシー、およびポリシーのコピーにより作成、更新、または削除されるオーバーライドが表示されます。

ステップ 5 [終了（Finish）] をクリックします。ポリシーのコピーを確認するように求められます。

ポリシーは、ターゲットデバイスにコピーされます。ターゲットデバイスに対するコピー操作が失敗すると、成功したデバイスに対するコピーは取り消され、問題のある各デバイスでコピーが失敗した原因のリストが表示されます。一般に、コピーが失敗するのは、他のユーザがポリシーまたはデバイスをロックしたか、またはデバイスに対する必要な権限がないことが原因です。

ポリシーの割り当て解除

すでにデバイスに展開されているポリシーの割り当てを解除すると、ほとんどの場合、ポリシーに定義された値が消去され、デバイスの計画設定からポリシーが削除されます。展開を実行すると、デバイスにすでに存在するこの機能の設定が削除されます。

正確な動作は、割り当てを解除するポリシーのタイプによって異なります。

- ファイアウォール サービス ポリシー：ポリシーの割り当てを解除すると、デバイスからポリシーが消去されます。
- VPN ポリシー：
  - サイト間 VPN ポリシー：必須のサイト間 VPN ポリシーは、トポロジ内のデバイスから割り当て解除できません。必須ポリシーの共有を解除すると、影響を受けるデバイスにデフォルト値が割り当てられます。オプション ポリシーの割り当てを解除すると、デバイスから設定が消去されます。詳細については、サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （1385 ページ）を参照してください。
  - IPSec リモート アクセス VPN ポリシー：ポリシーの割り当てを解除すると、必須ポリシーの場合でもデバイスからポリシーが消去されます。ほとんどの場合、必須ポリシーの新しい定義を作成しなければ展開は失敗します。展開が失敗しない場合は、デバイスで VPN トンネルを確立できません。
  - SSL VPN ポリシー：ポリシーの割り当てを解除すると、デバイスからポリシーが消去されます。
- Catalyst 6500/7600 または Catalyst スイッチ ポリシー：インターフェイスおよび VLAN ポリシーは共有または割り当て解除できません。プラットフォーム ポリシー（IDSM 設定、VLAN アクセス リストなど）の割り当てを解除すると、デバイスからポリシーが削除されます。

- IPS ポリシー：すべての IPS デバイスおよびサービス ポリシーでは、デフォルトのポリシーがデバイスに割り当てられます。
- PIX/ASA/FWSM ポリシー：他のデバイスと共有できないポリシーは、そのポリシーが作成されたデバイスから割り当て解除できません。これには、インターフェイス、フェールオーバー、セキュリティ コンテキスト、およびリソース ポリシーが含まれます。その他のポリシー タイプ（タイムアウト ポリシーなど）については、Security Manager は可能なかぎりデバイス上のシステム デフォルト設定を復元します。
- IOS ルータ ポリシー：基本的なインターフェイス設定やアカウントなどのコア接続ポリシーとクレデンシャル ポリシーは、それらのポリシーが作成されたデバイスから割り当て解除できません。デバイスを設定するためのパスワードの定義に使用されたデバイス アクセス ポリシーの割り当てを解除すると、Security Manager はそのデバイスを今後設定できなくなる可能性があります。詳細については、Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）を参照してください。

VTY またはコンソール ポリシーの割り当てを解除すると、Security Manager はデフォルト設定を復元して、デバイスとの通信が継続されるようにします。その他のすべてのポリシー タイプの場合、ポリシーの割り当てを解除すると、デバイスから設定が消去されます。

関連項目

- デバイス ビューにおけるローカル ポリシーの設定 （249 ページ）
- デバイス間でのポリシーのコピー （251 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）割り当てを解除するポリシーが含まれているデバイスを選択します。
- （Site-to-Site VPN Manager）割り当てを解除するポリシーが含まれている VPN トポロジを選択します。

ステップ 2 ローカルポリシーを右クリックし、[ポリシーの割り当て解除（Unassign Policy）] を選択します。

（注） ロールに割り当て権限がマップされている場合にのみ、ポリシーの共有を解除できます。Cisco Security Manager は認証のエラーメッセージを表示します。

現在のポリシーの割り当てを解除することを確認するように求められます。

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用

共有ポリシーを使用すると、複数のデバイスに共通のポリシーを設定できます。これにより、ポリシー定義の一貫性が維持され、管理作業が合理化されます。共有ポリシーに加えた変更

は、そのポリシーが割り当てられているすべてのデバイスおよび VPN トポロジに反映されます。これにより、たとえば、Cisco IOS ルータに割り当てられている共有 Quality of Service ポリシーを更新して、これらのすべてのデバイスを新しい Quality of Service ポリシーで簡単に更新できます。

デバイス ビューまたは Site-to-Site VPN Manager で作業する場合、ローカル ポリシー（デバイス検出中に作成されたポリシーなど）を取得して共有できます。その後、共有ポリシー（別のユーザによってロックされていない場合（ポリシーのロックについて （217ページ）を参照））を必要な数のデバイスや VPN トポロジに割り当てたり、これらの割り当てをいつでも変更したりできます。ローカルポリシーから作成されたこれらの共有ポリシーを取得して、ポリシーバンドルに追加することもできます。ポリシーバンドルの詳細については、ポリシーバンドルの管理 （281 ページ）を参照してください。

ヒント 他のデバイスを作成するためのテンプレートとして使用しているデバイスがある場合は、テンプレートデバイスに基づくデバイス設定に使用できるポリシーバンドルをすばやく作成できます。作成するには、最初にデバイス共有ポリシーですべてのポリシーを作成し（選択したデバイスの複数のポリシーの共有 （263 ページ）を参照）、次にそれらの共有ポリシーからポリシーバンドルを作成します。

さらに、デバイスまたは VPN トポロジに割り当てられている共有ポリシーを取得し、それを特定のデバイスまたはトポロジのローカルポリシーにすることができます。これにより、そのデバイスまたはトポロジだけに反映される特別な設定を作成できます。共有ポリシーが割り当てられている他のデバイスやトポロジは、前と同じように共有ポリシーを使用し続けます。

ローカル ポリシーを共有する代わりに、ポリシー ビューを使用して新しい共有ポリシーを作成し、そのポリシーをネットワーク レベルで管理できます。詳細については、ポリシー ビューにおける共有ポリシーの管理 （273ページ）を参照してください。ポリシー ビューで共有ポリシーを作成し、デバイスまたはVPNトポロジに割り当てたら、デバイス ビューまたはSite-to-Site VPN Managerに戻って、次の項で説明するようにポリシーに対して追加操作を実行できます。デバイス ビューまたはSite-to-Site VPN Managerで作成したすべての共有ポリシーは、ポリシー ビューに自動的に共有ポリシーとして表示されます。

ヒント デバイス ビューまたは Site-to-Site VPN Manager で共有ポリシーを編集すると、変更はそのポリシーを共有するすべてのデバイスまたは VPN に適用されます。したがって、ポリシー ビューに移動して共有ポリシーを編集する必要はありません。共有ポリシーを編集しようとすると、目的以外のデバイスやトポロジに誤って変更を加えることがないように、警告が表示されます。1 つのデバイスまたはトポロジだけのポリシーを変更する必要がある場合は、ポリシーの共有解除 （265ページ）で説明しているように、そのポリシーを編集する前にポリシーの共有を解除できます。

次の項では、ポリシーの共有方法およびデバイス ビューまたは Site-to-Site VPN Manager でそれらのポリシーに対して実行できる操作について説明します。

- ポリシー バナーの使用 （258 ページ）

- デバイス ビューおよびSite-to-Site VPN Managerにおけるポリシー ショートカット メニュー コマンド （260 ページ）
- ローカル ポリシーの共有 （262 ページ）
- 選択したデバイスの複数のポリシーの共有 （263 ページ）
- ポリシーの共有解除 （265 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）
- 共有ポリシーへのローカル ルールの追加 （267 ページ）
- ルールの継承または継承の解除 （269 ページ）
- 共有ポリシーのクローニング（コピー） （270 ページ）
- 共有ポリシー名の変更 （270 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更 （271 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）

関連項目

- ポリシーまたはデバイスのインポート （615 ページ）
- ポリシーについて （209 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）

ポリシー バナーの使用

デバイス ビューでデバイス ポリシーを表示する場合、または Site-to-Site VPN Manager でサイト間 VPN ポリシーを表示する場合は、作業領域のポリシー コンテンツの上にバナーが表示されます。バナーには、ポリシーがデバイスに対してローカルであるか、または共有ポリシーであるかに関する情報が含まれます。共有ポリシーの場合、バナーは、そのポリシーを使用するデバイスの数も示します。継承を許可するポリシーの場合、バナーには継承に関する情報が含まれます。

バナーの下に、次の内容のメッセージが表示される場合があります。

- ポリシーは他のユーザによってロックされています。他のユーザが変更を送信（および承認）するか、編集をキャンセルするか、または変更を廃棄するまで、ポリシーへの変更を保存できません。
- 共有ポリシーがインポートされました。ポリシーが異なるサーバで管理されている場合、インポートされたポリシーは今後、再度インポートされる可能性があります。ポリシーに加えた変更は、ポリシーが再度インポートされた場合には削除されます。ポリシーを編集する前に、ポリシー管理およびインポート用に組織で使用されているプロトコルを確実に

理解してください。[Tools] > [Security Manager Administration] > [Policy Management] ページのオプションを使用して、このメッセージを表示するかどうかを制御できます（[Policy Management] ページ （729 ページ）を参照）。

バナーのリンクを使用して、共有ポリシーを作成または割り当てたり、ポリシーの継承を設定したりできます。次の図に、デバイスのポリシー マナーの例を示します。

ポリシー バナーのフィールドには、次の意味と用途があります。

- [Policy Assigned]：このデバイスまたは VPN に割り当てられているポリシーの名前。名前がリンクになっている場合は、そのリンクをクリックして共有ポリシーを要素に割り当てることができます。リンクがない場合は、共有ポリシーをこの特定のタイプのポリシーに割り当てることはできません。
  - [Local]：ポリシーは共有ポリシーではなくローカル ポリシー（このデバイスのみに設定されたポリシー）です。
  - 特定のポリシー名：デバイス ポリシーに共有ポリシーが割り当てられています。
- [Assigned To]：共有ポリシーが割り当てられている場合は、ポリシーが割り当てられているデバイスまたは VPN の数。共有ポリシーが割り当てられていない場合は、[ローカルデバイス（local device）] または [このVPN（this VPN）] が表示されます。名前がリンクになっている場合は、次の操作を実行できます。
  - [Local Device] または [This VPN] リンク：リンクをクリックして、このローカル ポリシーから共有ポリシーを作成します。作成した共有ポリシーは、他のデバイスまたは VPN に割り当てることができます。
  - デバイスまたは VPN の数のリンク：リンクをクリックして、共有ポリシーに割り当てられているデバイスまたは VPN を変更します。
- [Inherits From]：このポリシーがルールを継承するポリシーの名前。このフィールドは、継承を許可するポリシーに対してだけ表示されます。リンクをクリックして、ポリシーがルールを継承するポリシーまたはポリシーのセットを指定します。継承の詳細については、ルールの継承について （213 ページ）を参照してください。

  このフィールドには、次のエントリが含まれる可能性があります。
  - [None]：ポリシーは他のポリシーからルールを継承しません。
  - 1 つのポリシー名：ポリシーはこのポリシーからルールを継承します。
  - > 記号で区切られた複数のポリシー名：ポリシーは表示されたポリシーの階層からルールを継承します。
- [割り当て済みのポリシーバンドル（Policy Bundle Assigned）]：このデバイスまたは VPN に割り当てられているポリシーバンドルの名前。

関連項目

- ポリシーについて （209 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- ローカル ポリシーの共有 （262 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）
- 共有ポリシーへのローカル ルールの追加 （267 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更 （271 ページ）
- 継承と割り当て （216 ページ）
- ポリシーのロックについて （217 ページ）
- ポリシーまたはデバイスのインポート （615 ページ）

デバイス ビューおよび Site-to-Site VPN Manager におけるポリシー ショートカット メニュー コマンド

デバイス ビューまたは Site-to-Site VPN Manager でポリシーを右クリックすると、ポリシーに対して使用できるコマンドのリストが表示されます。このショートカット コマンド リストには、選択したポリシーに使用できるコマンドだけが含まれるため、リストは選択したポリシーによって異なります。

使用できるコマンドは、ポリシーの次の状態によって決まります。

- ポリシーが割り当てられているかどうか。
- ポリシーに特定のデバイスまたは VPN トポロジのローカル ポリシーが含まれているかどうか。
- ポリシーに複数のデバイスまたは VPN トポロジに割り当てることができる共有ポリシーが含まれているかどうか。
- ポリシーを共有できるかどうか。デバイスまたはトポロジ間で共有できないポリシーにはショートカット コマンドがありません。

ポリシー名の横に表示されるアイコンで各ポリシータイプの現在のステータスが示されます。ポリシー ステータス アイコン （248 ページ）を参照してください。

次の表に、表示されるコマンドの一覧を示します。

表 *38* : ポリシー ショートカット コマンド

メニュー コマンド	説明
ローカルポリシーと共有ポリシーの両方で使用できるコマンド	
Assign Shared Policy	選択したデバイスまたは VPN トポロジに既存の共有ポリシーを割り当てます。ポリシーがすでに共有ポリシーとして割り当てられている場合は、選択によって既存のポリシーの代わりに新しい共有ポリシーが割り当てられます。 デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）を参照してください。
Inherit Rules	ルールの継承元の共有ポリシーを特定できます。または、子ポリシーから継承を削除します。子ポリシーは、親ポリシーに定義されている必須ルールとデフォルト ルールの両方を継承します。 ルールの継承または継承の解除 （269 ページ）を参照してください。
その他のローカル ポリシー コマンド	
Share Policy	ローカル ポリシーを共有して、他のデバイスや VPN トポロジに割り当てることができるようにします。 ローカル ポリシーの共有 （262 ページ）を参照してください。
Unassign Policy	デバイスまたはVPN トポロジからポリシーの割り当てを解除します。展開時に、このポリシーに定義されている設定に対応する設定がデバイスまたはトポロジ内のデバイスから削除されます。 ポリシーの割り当て解除 （255 ページ）を参照してください。
その他の共有ポリシー コマンド	
Unshare Policy	共有ポリシーのローカル コピーを作成し、共有ポリシーの代わりにデバイスまたは VPN トポロジに割り当てます。 ポリシーの共有解除 （265 ページ）を参照してください。
Edit Policy Assignments	現在表示しているデバイスまたは VPN トポロジだけでなく、このポリシーに割り当てられているデバイスまたは VPN トポロジを変更できます。 デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）を参照してください。
ポリシーの複製	新しい名前でポリシーのコピーを作成します。このオプションは、作成時のポリシーと同じ定義を持つ新しいポリシーを作成し、そのポリシーを編集できるようにする場合に使用します。 共有ポリシーのクローニング（コピー） （270 ページ）を参照してください。
Rename Policy	選択したポリシーの名前を変更します。 共有ポリシー名の変更 （270 ページ） を参照してください。

ローカル ポリシーの共有

ネットワークが拡大するにつれて、ローカル ポリシーを、複数のデバイスまたは VPN トポロジに割り当て可能な共有ポリシーに変換することが必要になってくる可能性があります（ローカルポリシーと共有ポリシー （211 ページ）を参照）。ポリシーを共有すると、ポリシーに割り当てられているすべてのデバイスまたはトポロジの設定の一貫性を保持できる合理的な管理が可能になります。たとえば、一連のファイアウォール インスペクション ルールを特定のデバイスに設定し、そのデバイスのインスペクション ルール ポリシーを共有すると、そのポリシーを他のデバイスに割り当てられるため、各デバイスを個別に設定する必要がなくなります。デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）を参照してください。

さらに、共有ポリシーを使用すると、割り当てられている各デバイスまたはトポロジの設定を一度に更新できるため、時間を短縮したり、一連の管理対象デバイスの一貫性を向上させることができます。

ポリシーを共有する場合は、ポリシーに名前を付ける必要があります（ローカルポリシーは単一のデバイスまたはトポロジにのみ関連付けられているため、名前は付けません）。名前を付けることで、ポリシービューで共有ポリシーを管理するときにポリシーを識別できます。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー ステータス アイコン （248 ページ）
- ポリシー バナーの使用 （258 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）
- ポリシーの共有解除 （265 ページ）
- 共有ポリシーへのローカル ルールの追加 （267 ページ）
- 選択したデバイスの複数のポリシーの共有 （263 ページ）
- ルールの継承または継承の解除 （269 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタからポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）**[ポリシー（Policy）] > [ポリシーの共有（Share Policy）]** を選択します。
- ポリシーを右クリックし、[ポリシーの共有（Share Policy）] を選択します。
- ポリシーバナーの [割り当て先（Assigned To）] フィールドの [ローカルデバイス/このVPN（local device/this VPN）] リンクをクリックします。「Local Policies Cannot Be Assigned to Multiple Devices」と

いうメッセージを含む警告ダイアログボックスが開き、ローカル ポリシーを表示していることが示されます。[ポリシーの共有（Share Policy）] をクリックして続行します。

[Share Policy] ダイアログボックスが表示されます。

ステップ 2 共有ポリシーの名前を入力し、[OK] をクリックします。

ポリシー名は、スペースや特殊文字を含めて最大 255 文字です。

選択したデバイスの複数のポリシーの共有

1 つの手順で、特定のデバイスに設定されている複数のポリシーを共有できます。この手順を実行すると、デバイスに設定されているすべてのポリシーを共有するか、またはその一部のポリシーだけを共有するかを選択できます。たとえば、ASA デバイスに定義されているすべてのファイアウォール サービス ポリシーを取得して共有できます。

最初は、生成される共有ポリシーは手順を実行したデバイスにだけ割り当てられます。ただし、これらの共有ポリシーを必要に応じて他のデバイスに割り当てることができます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）を参照してください。

この機能により、単一デバイスに設定されたポリシーを簡単に取得し、同様のデバイスを設定するためのテンプレートとしてこのポリシーを使用できます。たとえば、ブランチ オフィスのデバイスの検出後に、1 つの手順で同様のデバイスに設定されているローカル アクセス ルールをすべて取得し、それらのルールを共有して、ブランチ オフィスのデバイスに割り当てることができます。

ヒント この手順を使用して、デバイス上のポリシーを共有ポリシーにして、これらの共有ポリシーからポリシー バンドルを作成できます。その後、このポリシー バンドルを使用して、テンプレート デバイスに基づいて新しいデバイスをすばやく構成できます。

ヒント ソース デバイスと同じ設定やプロパティ（デバイスのオペレーティング システムのバージョン、クレデンシャル、グループ化属性など）を共有する同じタイプの新しいデバイスを作成するには、デバイスの複製を作成します。詳細については、デバイスの複製（160 ページ）を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス間でのポリシーのコピー （251 ページ）
- ローカル ポリシーの共有 （262 ページ）

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）
- ポリシーの共有解除 （265 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

ステップ 1 デバイス ビューで、次のいずれかを実行します。

- **[ポリシー（Policy）] > [デバイスポリシーの共有（Share Device Policies）]** を選択します。Share Policies ウィザードが開き、[Share Policies from this Device] ページ（手順 1）が表示されます。ポリシーを共有するデバイスを選択し、[次へ（Next）] をクリックします。
- デバイスを右クリックし、[デバイスポリシーの共有（Share Device Policies）] を選択します。ポリシーの共有（Share Policies）ウィザードが開き、[共有するポリシーを選択（Select Policies to Share）] ページ（手順 2）が表示されます。必要に応じて [戻る（Back）] をクリックして手順 1 に戻り、別のデバイスを選択できます。

ヒント マップビューでデバイスを右クリックし、[デバイスポリシーの共有（Share Device Policies）] を選択することもできます。

ステップ 2 [Select Policies to Share] ページで、共有するすべてのポリシーを選択します。最初は、デバイスに設定されているすべての共有可能なポリシー（ローカルまたは共有）が選択されています。共有しない各ポリシーの横にあるチェックボックスをオフにします。

次にいくつかのヒントを示します。

- チェックボックスをオフにしたローカル ポリシーは、選択したデバイスに対してローカルのままです。
- すでに共有されているポリシーを選択すると、ウィザードで定義した名前を使用して、そのポリシーのコピーが作成されます。
- ポリシー グループのチェックボックスをオンにすると、そのグループ内のすべてのポリシーが選択されます。
- デバイスにポリシーが設定されており、そのポリシーを選択できない（チェックボックスがグレーになっている）場合、そのポリシーは共有不可能なポリシーです。

ステップ 3 共有ポリシーの名前を入力します。すべてのポリシーに同じ名前が付けられます。あとで個々のポリシーの名前を変更できます。詳細については、 共有ポリシー名の変更 （270 ページ）を参照してください。

すでに共有されているポリシーを選択すると、この名前を使用して、そのポリシーのコピーが作成されます。

ステップ 4 [終了（Finish）] をクリックします。選択したポリシーは共有ポリシーになり、必要に応じて他のデバイスに割り当てることができます。詳細については、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）を参照してください。

ポリシーの共有解除

特定のデバイスまたはVPN トポロジに割り当てられている共有ポリシーの共有を解除すると、そのデバイスまたはポリシーのローカルポリシーになるコピーが作成されます。つまり、その後ローカル ポリシーに加えた変更は、この特定のデバイスまたはトポロジだけに反映されます。元の共有ポリシーが割り当てられている他のデバイスやトポロジは、これまでと同様に共有ポリシーを使用し続けます。

（注） ロールに割り当て権限が定義されている場合にのみ、ポリシーの共有を解除できます。Cisco Security Manager は認証のエラーメッセージを表示します。

（注） ポリシーバンドルの一部としてデバイスに割り当てられているポリシーは共有解除できません。デバイスからポリシーバンドルの割り当てを解除するか、デバイスに割り当てられているポリシーバンドルから共有ポリシーを削除する必要があります。

たとえば、Security Manager が、20 台のルータに割り当てられている MyBGP という BGP ルーティング ポリシーを管理しているとします。そのうち 1 台のルータ（ルータ 1）でこのポリシーの変更が必要な場合、デバイスを選択し、ポリシーの共有を解除して、そのルータに必要な変更を行うことができます。それ以降、ルータ 1 にはローカル BGP ポリシーが割り当てられ、他の 19 台のルータは引き続き MyBGP という元の共有ポリシーを使用します。

関連項目

- デバイス ビューについて （87 ページ）
- ローカル ポリシーの共有 （262 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）
- ポリシー ステータス アイコン （248 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタからポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）**[ポリシー（Policy）] > [ポリシーの共有解除（Unshare Policy）]** を選択します。
- 共有ポリシーを右クリックし、[ポリシーの共有解除（Unshare Policy）] を選択します。

（注） ロールに割り当て権限がマップされている場合にのみ、ポリシーの共有を解除できます。Cisco Security Manager は認証のエラーメッセージを表示します。

ステップ 2 [OK] をクリック共有ポリシーは、選択したデバイスまたは VPN トポロジのローカル ポリシーに変換されます。ポリシー セレクタの共有ポリシー アイコンは、ローカル ポリシー アイコンに置き換わります。

デバイスまたは VPN トポロジへの共有ポリシーの割り当て

デバイス ビューまたは Site-to-Site VPN Manager で割り当てた共有可能なポリシー（ローカルまたは共有）を同じタイプの既存の共有ポリシーに置き換えることができます。たとえば、Cisco IOS ルータにローカル NAT ポリシーが割り当てられている場合、そのポリシーの代わりに共有 NAT ポリシーを割り当てることができます。同様に、ルータに共有 NAT ポリシーが割り当てられている場合、そのポリシーを別の共有 NAT ポリシーに置き換えることができます。

ヒント 複数のバンドル共有ポリシーを一緒に使用して、それらのポリシーの割り当てを容易にすることができます。詳細については、ポリシーバンドルの管理 （281 ページ）を参照してください。

ルールベースのローカル ポリシー（インスペクション ルール ポリシーなど）に代えて共有ポリシーを割り当てる場合、設定済みのローカル ルールは共有ポリシーに定義されているルールに置き換えられます。警告メッセージが表示され、ローカル ポリシーの代わりに共有ポリシーを割り当てるのではなく、共有ポリシーのルールを継承することによって、ローカル ルールを保持することもできます。詳細については、継承と割り当て （216 ページ）を参照してください。

ヒント 共有ポリシーに定義されているルールを使用し、ローカル ルールを保持する場合は、ポリシーを割り当てるのではなく、[Inherit Rules] オプションを選択することを推奨します。詳細については、ルールの継承または継承の解除 （269 ページ）を参照してください。

（注） IPS シグニチャ ポリシーとシグニチャ イベント アクションを継承することもできますが、継承の動作はルールベースのポリシーとは異なります。詳細については、シグニチャ継承について （2168 ページ）を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー バナーの使用 （258 ページ）
- ポリシーの割り当て解除 （255 ページ）
- 共有ポリシーへのローカル ルールの追加 （267 ページ）
- デバイス間でのポリシーのコピー （251 ページ）

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタからポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）[ポリシー（Policy）] > [共有ポリシーの割り当て（Assign Shared Policy）] を選択します。
- ポリシーセレクタでポリシーを右クリックし、[共有ポリシーの割り当て（Assign Shared Policy）] を選択します。
- ポリシー バナーの [Policy Assigned] フィールドのリンクをクリックします。

割り当て可能な共有ポリシーがある場合は、[Assign Shared Policy] ダイアログボックスが表示されます。

ステップ 2 表示されたリストからデバイスまたは VPN トポロジに割り当てる共有ポリシーを選択し、[OK] をクリックします。ポリシーで継承が許可されていない場合は、選択したデバイスに共有ポリシーが割り当てられ、終了します。

ステップ 3 ポリシーで継承が許可されている場合は、現在のポリシーが共有ポリシーに置き換えられることを示す警告が表示され、[ローカルポリシーが置き換えられる（Local Policy Will Be Replaced）] ダイアログボックスにルールを継承するためのオプションが表示されます。 [Customize Desktop] ページ （654 ページ）

選択できるオプションは、次のとおりです。

- [Assign Policy]：既存のローカル ポリシーを置き換える共有ポリシーを割り当てます。割り当てを選択した場合は、すべてのローカル ルールが削除され、取得できなくなります。
- [Inherit From Policy]：共有ポリシーのルールを継承します。継承を選択した場合は、継承されたルールがデバイスのローカルポリシーですでに定義されているローカルルールに追加されます。定義済みの一連のローカル ルールをデバイスで保持する必要がある場合は、割り当てではなく継承を使用します。

ヒント [次回から表示しない（Do not show this again）] を選択して選択内容を保存し、今後ルールベースのポリシーを割り当てるときに常にこの設定を適用できます。このオプションを選択しない場合は、ポリシーを割り当てるたびにメッセージが表示されるため、状況に応じて異なる選択を行うことができます。このオプションを選択した場合、[Customize Desktop] 管理設定ページ（を参照）でリセットすると、このオプションをオフにすることができます。

共有ポリシーへのローカル ルールの追加

アクセス ルールなどのルールベースの共有ポリシーをデバイスに割り当てると、そのデバイスに対してローカルなポリシーに追加ルールを定義できます。このオプションを選択すると、継承関係が作成され、デバイスに定義されているポリシーは共有ポリシーからルールを継承し、この特定のデバイスだけに影響するルールを追加できます。継承の詳細については、ルールの継承について （213 ページ）を参照してください。

デバイスに追加したローカル ルールは、デバイスが残りのルールを継承する共有ポリシーには影響しません。たとえば、共有ポリシー Access_Rules_South を 5 台のデバイスに割り当てて、このうち 1 台のデバイスにローカル ルールを定義した場合、そのデバイスのアクセス ルール ポリシーは Access_Rules_South とローカル ルールで構成されます。他の 4 台のデバイスは引き続き Access_Rules_South に定義されているルールだけを使用します。

はじめる前に

デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）の説明に従って、ルールベースの共有ポリシーをデバイスに割り当てます。

関連項目

- デバイス ビューについて （87 ページ）
- 共有ポリシーのクローニング（コピー） （270 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）
- ポリシーの共有解除 （265 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

ステップ 1 デバイス ビューで、デバイス セレクタからデバイスを選択し、デバイス ポリシー セレクタからそのデバイスに割り当てられている共有ポリシーを選択します。アクセス ルールなどのルールベースのポリシーを選択する必要があります。ポリシーの詳細は作業領域に表示されます。

ステップ 2 次のいずれかを実行します。

- [ポリシー（Policy）] > [ローカルルールの追加（Add Local Rules）] を選択します。
- ポリシーを右クリックし、[ローカルルールの追加（Add Local Rules）] を選択します。

このデバイスのポリシーが共有ポリシーからルールを継承する子ポリシーとして定義されることを示すメッセージが表示されます。その共有ポリシーが別の共有ポリシーからルールを継承する場合は、それらのルールも自動的に継承されます。

（注） このポリシーがルールを継承する親ポリシーを変更する場合は、ルールの継承または継承の解除（269 ページ）を参照してください。

ステップ 3 [OK] をクリックして確認します。作業領域で、共有ポリシーから継承された必須ルールとデフォルト ルールに加えて、ローカルの必須ルールとデフォルト ルールの見出しが追加されます。

デバイス ポリシー セレクタで、ステータス アイコンがローカル ポリシーのアイコンに変わります。詳細については、 ポリシー ステータス アイコン （248 ページ）を参照してください。

ステップ 4 必要に応じてローカル ルールを定義します。

ヒント　ローカル ルールの追加後に共有ポリシーを割り当てると、継承されたルールとローカル ルールの両方が、選択した共有ポリシーに置き換えられます。

ルールの継承または継承の解除

ここでは、特定タイプのルールベースのポリシー（アクセス ルールなど）が同じタイプの共有ポリシーからルールを継承する方法について説明します。子ポリシーは、親ポリシーに定義されている必須ルールとデフォルト ルールの両方を継承します。

デバイス ビューで作業する場合、選択したデバイスに対してローカルな追加ルールを定義できます。詳細については、共有ポリシーへのローカル ルールの追加 （267 ページ）を参照してください。

デバイス ビューまたはポリシー ビューからルールの継承を編集できます。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）
- ルールの継承について （213 ページ）
- 継承と割り当て （216 ページ）
- ポリシー バナーの使用 （258 ページ）
- ポリシーについて （209 ページ）

ステップ 1　デバイス ビューまたはポリシー ビューでルールベースのローカルまたは共有ポリシーを選択し、次のいずれかを実行します。

- **[ポリシー（Policy）] > [ルールの継承（Inherit Rules）]** を選択します。
- ポリシーを右クリックし、[ルールの継承（Inherit Rules）] を選択します。
- （デバイス ビューだけ）ポリシー バナーの [Inherits From] フィールドのリンクをクリックします。

[Inherit Rules] ダイアログボックスが表示されます。このダイアログボックスには、継承関係を含む、選択したタイプの共有ポリシーすべてのリストが表示されます。

ステップ 2　ルールを継承するポリシーを選択するか、または [継承なし（No Inheritance）] を選択して子ポリシーから継承を削除します。親ポリシーの名前がセレクタの下に表示されます。

たとえば、West Coast というアクセス ルール ポリシーを選択した場合、アクセス ポリシーは West Coast ポリシーのルールを継承します。West Coast ポリシーが US という別のアクセス ルール ポリシーの子ポリシーである場合、ポリシーは US ポリシーのプロパティを継承する West Coast ポリシーのプロパティを継承します。

ステップ 3 [OK] をクリックして定義を保存します。作業領域の親ポリシー名の下に継承されたルールが表示され、定義されている場合はローカル ルールが元の共有ポリシー名の下に表示されます。

共有ポリシーのクローニング（コピー）

既存の共有ポリシーを複製できます。これにより、既存のポリシーに似た新しいポリシーを簡単に作成できます。複製の作成後、必要に応じて複製を変更できます。

継承が適用されたルールベースのポリシーを複製した場合、新しいポリシーには作成元のポリシーと同じ継承プロパティが含まれます。詳細については、ルールの継承について （213 ページ）を参照してください。

ヒント デバイス ビューまたは Site-to-Site VPN Manager でポリシーを複製すると、新しいポリシーは選択したデバイスまたは VPN トポロジに割り当てられます。ポリシーの割り当てを変更しないでポリシーを複製する場合は、ポリシー ビューで複製を作成します。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）
- 共有ポリシー名の変更 （270 ページ）
- 共有ポリシーの削除 （280 ページ）

ステップ 1 デバイス ビュー、ポリシー ビュー、または Site-to-Site VPN Manager で共有ポリシーを選択し、次のいずれかを実行します。

- （デバイスビューまたはポリシービューのみ）**[ポリシー（Policy）] > [ポリシーの複製（Clone Policy）]** を選択します。
- 共有ポリシーを右クリックし、[ポリシーの複製（Clone Policy）] を選択します。

[Clone Policy] ダイアログボックスが表示されます。

ステップ 2 新しいポリシーの名前を入力し、[OK] をクリックします。

名前は、スペースや特殊文字を含めて最大 255 文字です。

共有ポリシー名の変更

共有ポリシーの名前を変更できます。新しい名前は、ポリシーが割り当てられているすべてのデバイスまたは VPN トポロジにすぐに反映されます。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）
- 共有ポリシーのクローニング（コピー） （270 ページ）
- 共有ポリシーの削除 （280 ページ）

ステップ 1 デバイス ビュー、ポリシー ビュー、または Site-to-Site VPN Manager で共有ポリシーを選択し、次のいずれかを実行します。

- （デバイスビューまたはポリシービュー）[ポリシー（Policy）]>[ポリシーの名前変更（Rename Policy）] を選択します。
- ポリシーを右クリックし、[ポリシーの名前変更（Rename Policy）] を選択します。

[Rename Policy] ダイアログボックスが表示されます。

ステップ 2 選択したポリシーの新しい名前を入力し、[OK] をクリックします。

名前は、スペースや特殊文字を含めて最大 255 文字です。

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー定義の変更

デバイス ビューまたは Site-to-Site VPN Manager で共有ポリシーを変更できます。変更するには、ポリシーが割り当てられているいずれかのデバイスまたは VPN トポロジを選択し、必要な変更を加えてその変更を Security Manager サーバに保存します。デバイス ビューまたは Site-to-Site VPN Manager で共有ポリシーに加えた変更は、共有ポリシーが割り当てられているすべてのデバイスに自動的に反映されます。

ヒント 変更するデバイスまたは VPN トポロジだけに変更を適用するには、まずポリシーの共有を解除する必要があります（ポリシーの共有解除 （265 ページ）を参照）。このアクションによって、ポリシーがローカル ポリシーに変換され、変更が他のデバイスやトポロジに反映されなくなります。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー バナーの使用 （258 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）
- デバイス ビューにおけるローカル ポリシーの設定 （249 ページ）

- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）変更する共有ポリシーが含まれているデバイスを選択します。
- （Site-to-Site VPN Manager）変更する共有ポリシーが含まれている VPN トポロジを選択します。

ステップ 2 必要に応じてポリシーを再定義します。

ステップ 3 [保存（Save）] をクリックします。ポリシーが割り当てられているすべてのデバイスまたはトポロジに変更が適用されることを示す警告が表示され、変更の保存を確認するように求められます。

デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更

特定の共有ポリシーが割り当てられているデバイスまたは VPN トポロジのリストを必要に応じて変更できます。ポリシー割り当てからデバイスまたはトポロジを削除すると、そのポリシーはデバイスまたはトポロジの計画設定から削除されます。展開時には、デバイスまたはトポロジに存在するそのタイプの設定が削除されます。ポリシーの割り当て解除の意味の詳細については、 ポリシーの割り当て解除 （255 ページ）を参照してください。

注意 ポリシー割り当てを解除すると、その設定がデバイスまたはトポロジから削除され、予期しない結果が発生するおそれがあるため、ポリシー割り当て機能は慎重に使用してください。たとえば、Cisco IOS ルータからデバイス アクセス ポリシーの割り当てを解除し、その変更を展開すると、Security Manager は今後そのデバイスを設定できなくなる可能性があります（ Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）を参照）。

ポリシー割り当ては、ポリシー ビューから変更することもできます。詳細については、 ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

関連項目

- デバイス ビューについて （87 ページ）
- ポリシー バナーの使用 （258 ページ）
- デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）
- ポリシーの割り当て解除 （255 ページ）
- デバイス間でのポリシーのコピー （251 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）
- 継承と割り当て （216 ページ）

• ルールの継承または継承の解除 （269 ページ）

ステップ 1 デバイス ビューまたは Site-to-Site VPN Manager で、ポリシー セレクタから共有ポリシーを選択し、次のいずれかを実行します。

- （デバイスビューのみ）**[ポリシー（Policy）] > [ポリシー割り当ての編集（Edit Policy Assignments）]** を選択します。
- ポリシーを右クリックし、[ポリシー割り当ての編集（Edit Policy Assignments）] を選択します。
- ポリシーバナーの [割り当て先（Assigned To）] フィールドの [nデバイス/VPN（n device/VPN）] リンクをクリックします。

ステップ 2 次のように、ポリシーが割り当てられているデバイスまたは VPN トポロジのリストを変更します。

- 選択したポリシーを追加のデバイスまたはトポロジに割り当てるには、[使用可能なデバイス/VPN（Available Devices/VPNs）] リストからデバイスまたはトポロジを選択し、[>>] をクリックして [割り当て済みデバイス（Assigned Devices）] リストに移動します。
- デバイスまたはトポロジから選択したポリシーの割り当てを解除するには、[割り込み済みデバイス/VPN（Assigned Devices/VPNs）] リストからデバイスまたはトポロジを選択し、[<<] をクリックして [利用可能なデバイス/VPN（Available Devices/VPNs）] リストに戻します。ポリシーの割り当てが解除されたデバイスまたはトポロジは、展開時にこのポリシーを実行コンフィギュレーションから削除します。

ヒント ポリシーをデバイスグループ内のすべてのデバイスに割り当てるには、デバイスグループの名前を選択してから、[>>] をクリックします。

ステップ 3 [OK] をクリックして割り当ての変更を保存します。

ポリシー ビューにおける共有ポリシーの管理

Security Manager で設定されたすべての共有ポリシーをグローバルに管理するには、ポリシー ビューを使用します。選択したデバイスに設定されているすべてのポリシーを管理するためのデバイス ビューとは異なり、ポリシー ビューでは、デバイスにかかわらず特定のタイプの共有ポリシーをすべて管理できます。

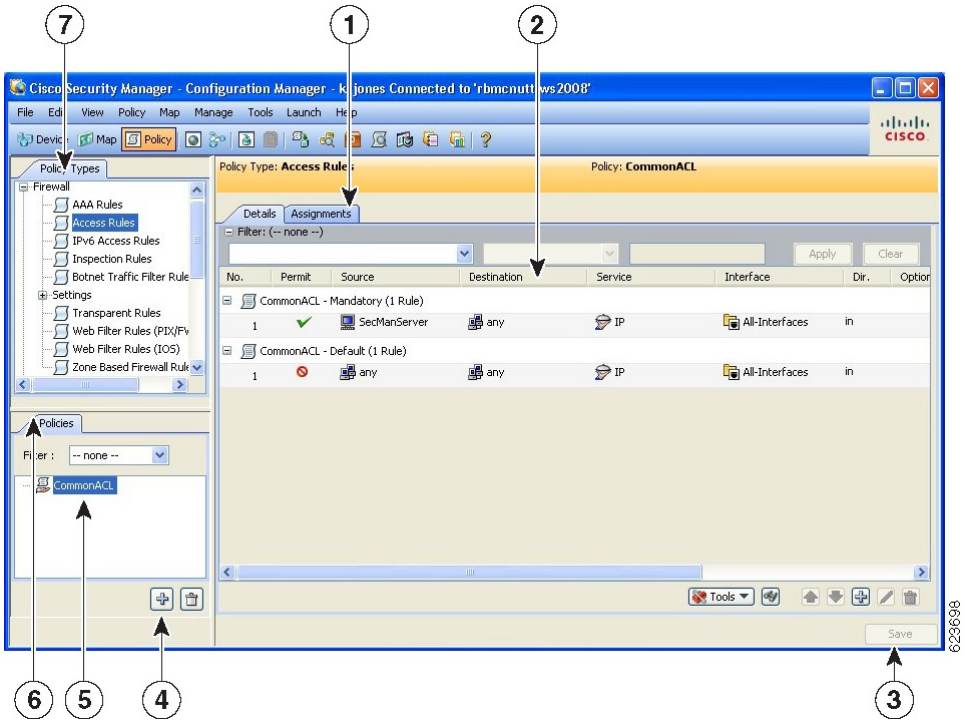
ポリシー ビューでは、次の操作を実行できます。

- 新しい共有ポリシーの作成
- ポリシー設定の編集
- 共有ポリシーが割り当てられているデバイスまたは VPN のリストの変更
- どのデバイスまたは VPN にも割り当てられていない共有ポリシーの削除

ポリシー ビューにアクセスするには、**[表示（View）] > [ポリシービュー（Policy View）]** を選択するか、またはツールバーの [ポリシービュー（Policy View）] アイコンをクリックします。

下の図は、ポリシービューのメイン領域を示します。

図 *14 : Policy View*



1	**[Assignments] タブ**	5	**共有ポリシー セレクタ**
2	作業領域と [Details] タブ	6	共有ポリシー フィルタ
3	[Save] ボタン	7	ポリシータイプセレクタ
4	[Create a Policy] および [Delete a Policy] ボタン		

- （7）ポリシータイプセレクタ：Security Manager で使用できるポリシータイプがカテゴリ別に表示されます。セレクタでポリシー タイプをクリックすると、共有ポリシー セレクタにそのタイプに定義されているすべての共有ポリシーが表示されます。新しいポリシーを作成するには、ポリシータイプを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）] を選択するか、または共有ポリシーセレクタで [ポリシーの作成（Create a Policy）] ボタンをクリックします。詳細については、ポリシー ビューのセレクタ （275 ページ）を参照してください。
- （4、5、6）共有ポリシーセレクタ：選択したタイプに定義されている共有ポリシーが表示されます。セレクタでポリシーをクリックすると、作業領域にポリシーの定義と割り当てが表示されます。詳細については、ポリシー ビューのセレクタ （275 ページ）を参照してください。

セレクタでポリシーを右クリックし、ポリシーに対してアクションを実行します。使用可能なコマンドの詳細については、ポリシー ビュー-共有ポリシー セレクタのオプション （277 ページ）を参照してください。

セレクタに表示されるポリシーのリストをフィルタリングするには、[Filter] フィールドを使用します。フィルタの作成の詳細については、セレクタ内の項目のフィルタリング （60 ページ）を参照してください。

- （1、2、3）作業領域：次の 2 つのタブがあります。
  - [Details]：選択したポリシーの定義を表示および編集する場合に使用します。必要に応じて定義を変更できます。作業領域で [保存（Save）] をクリックして変更を保存します。変更は、ポリシーが割り当てられているすべてのデバイスまたは VPN トポロジに反映されます。[Details] タブに表示される情報は、デバイス ビューまたは Site-to-Site VPN Manager に表示される情報と同じであり、まったく同じ方法で変更できます。ポリシー ビューのセレクタ （275 ページ）を参照してください。
  - [Assignments]：共有ポリシーが割り当てられているデバイスまたは VPN のリストを表示および編集する場合に使用します。詳細については、ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

関連項目

- ポリシーまたはデバイスのインポート （615 ページ）
- デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

ポリシー ビューのセレクタ

ポリシー ビューには 2 つのセレクタがあります。上部のセレクタには、選択したポリシー ドメインの使用可能なポリシー タイプがすべて表示されます。ポリシー タイプ セレクタのルートは、ポリシー ドメイン名です。別のポリシー ドメインのポリシー タイプを表示するには、ツリーのルートをクリックし、リストから別のドメインを選択します。

ポリシー ドメインは次のとおりです。

- [Firewall]：ファイアウォール サービスを設定するためのすべてのポリシー タイプが表示されます。ファイアウォール サービスの概要 （755 ページ）を参照してください。
- [NAT (PIX/ASA/FWSM)]：PIX、ASA、および FWSM デバイスに設定されているすべての NAT ポリシーが表示されます。セキュリティ デバイスの NAT ポリシー （1326 ページ）を参照してください。
- [NAT (Router)]：Cisco IOS ルータに設定されているすべての NAT ポリシーが表示されます。Cisco IOS ルータにおける NAT ポリシー （1313 ページ）を参照してください。

- [Site-to-Site VPN]：サイト間 VPN を設定するためのすべてのポリシー タイプが表示されます。サイト間 VPN の管理：基本 （1379 ページ）を参照してください。
- [Remote Access VPN]：リモート アクセス IPSec および SSL VPN を設定するためのすべてのポリシー タイプが表示されます。リモート アクセス VPN の管理の基礎 （1655 ページ）を参照してください。
- [Catalyst Platform]：Catalyst スイッチおよび 7600 ルータを設定するためのすべてのポリシー タイプが表示されます。Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理 （3401 ページ）を参照してください。
- [IPS]：IPS デバイスを設定するためのすべてのポリシー タイプが表示されます。IPS 設定の概要 （2088 ページ）を参照してください。
- [IPS (Router)]：IOS ルータに Cisco IOS IPS ポリシーを設定するためのすべてのポリシー タイプが表示されます。Cisco IOS IPS 設定の概要 （2318 ページ）を参照してください。
- [PIX/ASA/FWSM Platform]：PIX/ASA/FWSM プラットフォーム固有のポリシーを設定するためのすべてのポリシー タイプが表示されます。ファイアウォール デバイスの管理 （2331 ページ）を参照してください。
- [Router Interfaces]：プラットフォーム固有の Cisco IOS ルータ インターフェイス ポリシーを設定するためのすべてのポリシー タイプが表示されます。ルータの管理 （3001 ページ）を参照してください。
- [Router Platform]：プラットフォーム固有の Cisco IOS ルータ ポリシーを設定するためのすべてのポリシー タイプが表示されます。ルータの管理 （3001 ページ）を参照してください。
- [FlexConfigs]：すべての FlexConfig ポリシーが表示されます。FlexConfig の管理 （431 ページ）を参照してください。

セレクタを必要に応じて展開および縮小して、使用可能なすべてのポリシー タイプとサブタイプを表示できます。新しいポリシーを作成するには、ポリシー タイプを右クリックし、[新規 [ポリシー タイプ]ポリシー（New [policy type] Policy）] を選択するか、または共有ポリシー セレクタで [ポリシーの作成（Create a Policy）] ボタンをクリックします。

ポリシー タイプ セレクタからポリシー タイプを選択すると、共有ポリシー セレクタにそのタイプのすべての共有ポリシーが表示されます。デバイス ビューで設定されたローカル ポリシーは表示されません。

たとえば、NAT 変換ルールなどの設定ポリシー タイプを選択すると、共有ポリシー セレクタにそのタイプの各共有ポリシーを含むフラットなリストが表示されます。ファイアウォール アクセス ルールなどのルールベースのポリシー タイプを選択すると、共有ポリシー セレクタに共有ポリシーの階層ツリーが表示されます。これにより、さまざまなポリシー間の継承関係を確認できます。共有ポリシー セレクタには、そのポリシーに対して実行できるアクション（名前の変更など）のオプションを含むショートカット メニューがあります。

ヒント　フィルタを作成して割り当てることにより、共有ポリシーセレクタに表示されるポリシーのリストを短くすることができます。フィルタの詳細については、セレクタ内の項目のフィルタリング （60 ページ）を参照してください。

ポリシー ビュー - 共有ポリシー セレクタのオプション

ポリシー ビューの共有ポリシー セレクタでポリシーを右クリックすると、選択したポリシーに対して機能を実行するためのショートカット メニューが表示されます。

関連項目

- ポリシー ビューのセレクタ （275 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）

フィールド リファレンス

表 *39* : 共有ポリシー セレクタのオプション

メニュー コマンド	説明
ポリシーの複製	複製時のポリシーと同じ定義を持つ新しい共有ポリシーを作成します。共有ポリシーのクローニング（コピー） （270ページ）を参照してください。
Rename Policy	選択したポリシーの名前を変更します。共有ポリシー名の変更 （270 ページ）を参照してください。
ポリシーバンドルに追加（Add to Policy Bundle）	選択した共有ポリシーをポリシーバンドルに追加できます。ポリシーバンドルの管理 （281 ページ）を参照してください。
Inherit Rules	アクセスルールなどのルールベースのポリシーだけに適用されます。 ルールベースのポリシーは同じタイプの別の共有ポリシーのルールを継承します。ルールの継承または継承の解除 （269ページ）を参照してください。
[New [policy type] Policy]	選択したタイプの新しい共有ポリシーを作成します。新しい共有ポリシーの作成 （278 ページ）を参照してください。
Delete Policy	選択した共有ポリシーを削除します。共有ポリシーの削除 （280 ページ） を参照してください。

新しい共有ポリシーの作成

新しい共有ポリシーを作成するには、ポリシー ビューを使用します。ほとんどの場合、新しいポリシーは最初は未定義の状態ですが、特定の場合には（IPsec プロポーザルや GRE モードなどの多くのサイト間 VPN ポリシーなど）デフォルト値が指定されます。いずれの場合でも、新しいポリシーは最初はデバイスに割り当てられていません。新しいポリシーが、継承をサポートするルールベースのポリシーである場合は、同じタイプの既存の共有ポリシーの子として作成できます。詳細については、ルールの継承について （213 ページ）を参照してください。

ヒント デバイス ビューでローカル ポリシーを変換して共有ポリシーを作成することもできます。詳細については、ローカル ポリシーの共有 （262 ページ）を参照してください。

関連項目

- ポリシーまたはデバイスのインポート （615 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）
- 共有ポリシーの削除 （280 ページ）

ステップ 1 ポリシー ビューで、ポリシー タイプ セレクタからポリシー タイプを選択します。

ステップ 2 次のいずれかを実行します。

- ポリシータイプセレクタでポリシータイプを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）] を選択します。
- 共有ポリシーセレクタでポリシーを右クリックし、[新規[ポリシータイプ]ポリシー（New [policy type] Policy）]を選択します。
- 共有ポリシーセレクタの下にある [ポリシーの作成（eate a Policy）] ボタンをクリックします。

[Create a Policy] ダイアログボックスが表示されます。

ステップ 3 新しいポリシーの名前を入力します。ポリシー名は、スペースや特殊文字を含めて最大 255 文字です。

セキュリティデバイス（PIX/ASA/FWSM）で NAT ルールの変換ルールポリシーを作成する場合は、デバイスのソフトウェアバージョンとして **PIX/ASA 6.3-8.2** または **ASA 8.3 & 以降**を選択する必要があります。

ステップ 4 [OK] をクリック新しいポリシーが共有ポリシー セレクタに表示されます。

新しい共有ポリシーの定義を設定するには、[Details] タブが開いている状態でツールバーの [Help] ボタンをクリックして、作成するポリシーのタイプに固有の情報を表示します。新しい共有ポリシーを割り当てるには、ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

ポリシー ビューにおけるポリシー割り当ての変更

ポリシー ビューの [Assignments] タブでは、選択した共有ポリシーが割り当てられているデバイスまたは VPN トポロジのリストを変更します。[割り当て（Assignments）] タブには、選択した共有ポリシーが現在割り当てられているすべてのデバイスのリストが表示されます。また、継承によってポリシーが割り当てられているデバイスも表示されます。

ポリシーをデバイスまたは VPN に割り当てると、Security Manager で以前にデバイスに割り当てられた同じタイプのポリシー（ローカルまたは共有）が上書きされます。展開すると、新たに割り当てられたポリシーは、すでにデバイスに設定されている同じタイプのポリシーを上書きします。このポリシーは、Security Manager を使用して設定されたか、または CLI などの別の方法を使用して設定されたかにかかわらず上書きされます。

デバイスまたは VPN トポロジから共有ポリシーの割り当てを解除すると、そのデバイスまたは VPN トポロジの計画設定からポリシーが削除されます。ポリシーによって定義された設定を展開すると、すでにデバイス（VPN トポロジ内のデバイスを含む）に設定されている同じタイプの設定は削除されます。詳細については、ポリシーの割り当て解除 （255 ページ）を参照してください。

したがって、特定のデバイスまたは VPN トポロジに別の共有ポリシーを割り当てるために割り当てを解除する場合は、置換ポリシーを選択し、展開を実行する前に割り当てを実行することが重要です。

ヒント　置換ポリシーの割り当ては、特にデバイス アクセス ポリシーを使用して Cisco IOS ルータのイネーブル パスワードまたはイネーブル シークレット パスワードを設定する場合に重要です。このポリシーの割り当てを解除したときに、展開前に別のパスワードを定義しなかった場合、Security Manager は今後このデバイスを設定できなくなる可能性があります。詳細については、Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）を参照してください。

このほか、デバイス ビューに戻って、デバイスに割り当てられている共有ポリシーを別の共有ポリシーに置き換える方法もあります。詳細については、デバイスまたは VPN トポロジへの共有ポリシーの割り当て （266 ページ）を参照してください。

（注）　IKE プロポーザル ポリシーなどの必須のサイト間 VPN ポリシーの割り当てを解除すると、そのポリシーは Security Manager によって自動的にデフォルト ポリシーに置き換えられます。必須のリモート アクセス VPN ポリシーの割り当てを解除すると、その同じタイプの新しいポリシーを手動で設定する必要があります。そうしなければ展開は失敗します。

関連項目

- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）

• ポリシー ビューにおける共有ポリシーの管理 （273 ページ）

ステップ 1 ポリシー ビューで、ポリシー タイプ セレクタからポリシー タイプを選択し、共有ポリシー セレクタからポリシーを選択します。これらのセレクタの使用に関する詳細については、ポリシー ビューのセレクタ（275 ページ）を参照してください。

ステップ 2 作業領域で [割り当て（Assignments）] タブをクリックします。

[割り当て（Assignments）] タブには、選択した共有ポリシーが現在割り当てられているすべてのデバイスのリストが表示されます。また、継承によってポリシーが割り当てられているデバイスも表示されます。

ステップ 3 次のように、ポリシーが割り当てられているデバイスまたは VPN のリストを変更します。

- 選択したポリシーを追加のデバイスまたはVPNに割り当てるには、[利用可能なデバイス/VPN（Available Devices/VPNs）] リストから 1 つ以上の項目を選択し、[>>] をクリックして [割り当て済みデバイス/VPN（Assigned Devices/VPNs）] リストに移動します。

ヒント ポリシーをデバイスグループ内のすべてのデバイスに割り当てるには、デバイスグループの名前を選択してから、[>>] をクリックします。

- デバイスまたは VPN から選択したポリシーの割り当てを解除するには、[割り当て済みデバイス/VPN（Assigned Devices/VPNs）] リストから 1 つ以上の項目を選択し、[<<] をクリックして [利用可能なデバイス/VPN（Available Devices/VPNs）] リストに戻します。

（注） Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。ただし、以前の ASA バージョンでは、IPv6 アクセスルールの別のページが引き続きデバイスビューで提供されますが、ポリシービューでは、AAA ルール、アクセスルール、およびインスペクションルールのポリシータイプの IPv4 および統合バージョンが提供されます。IPv4 AAA ルール、アクセスルール、またはインスペクションルール共有ポリシーを 9.0 以降のデバイスに割り当てると、これらのポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合AAA ルール、アクセスルール、またはインスペクションルール共有ポリシーを 9.0 以降のデバイスに割り当てると、これらの共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれません。

ステップ 4 [保存（Save）] をクリックして割り当ての変更を保存します。

共有ポリシーの削除

Security Manager から共有ポリシーを削除するには、ポリシー ビューを使用します。

共有ポリシーを削除する前に、そのポリシーを使用するデバイスからポリシーの割り当てを解除し、そのデバイスの置換ポリシーを設定する必要があります。共有ポリシーがデバイスに割

り当てられている場合、そのポリシーを削除すると、削除した共有ポリシー用に設定されているポリシーがデバイスから削除されます。ただし、そのポリシータイプのデフォルトは存在する可能性があります。割り当ての削除の詳細については、ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

（注） 共有ポリシーが、デバイスに割り当てられているポリシーバンドルの一部である場合、共有ポリシーを削除する前に割り当てを解除する必要があります。

関連項目

- 新しい共有ポリシーの作成 （278 ページ）
- 共有ポリシーのクローニング（コピー） （270 ページ）
- ポリシー ビューにおける共有ポリシーの管理 （273 ページ）

ステップ 1 ポリシー ビューで、ポリシー タイプ セレクタからポリシー タイプを選択し、共有ポリシー セレクタから削除するポリシーを選択します。これらのセレクタの使用に関する詳細については、ポリシー ビューのセレクタ （275 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- ポリシーを右クリックして、[ポリシーの削除（Delete Policy）] を選択します。
- 共有ポリシーセレクタの下にある [ポリシーの削除（Delete Policy）] ボタンをクリックします。

削除の確認が求められます。

ポリシーバンドルの管理

ポリシーバンドルは、グループとして管理できる共有ポリシーのコレクションです。ポリシーバンドルを使用すると、バンドルを1回作成してから、バンドル内のすべてのポリシーを新しいデバイスに一度に割り当てることができるため、共有ポリシーの管理が容易になります。バンドルの一部である共有ポリシーは、他の共有ポリシーと同じように機能し、バンドルの一部である共有ポリシーを変更すると、直接またはポリシーバンドルを介してそのポリシーが割り当てられているすべてのデバイスに影響します。

ポリシーバンドルを作成するときは、各タイプの共有ポリシーを1つだけポリシーバンドルに割り当てることができます。ポリシーバンドルのポリシータイプが重複しない限り、複数のポリシーバンドルをデバイスに割り当てることができます。

ポリシーバンドルをデバイスに割り当てるときに、そのデバイスのローカルポリシーがポリシーバンドルに含まれているものと同じポリシータイプである場合、既存のポリシーを継承するか、置き換えるかを選択できます。

（注） ポリシーバンドルの割り当てを解除すると、そのバンドルの一部であるすべてのポリシーがデバイスから削除されます。ローカルポリシーは失われ、取得できなくなります。

ここでは、次の内容について説明します。

- 新しい共有ポリシーの作成 （278 ページ）
- ポリシーバンドルの複製 （283 ページ）
- ポリシーバンドルの名前変更 （284 ページ）
- ポリシーバンドルのデバイスへの割り当て （284 ページ）

新規ポリシーバンドルの作成

ポリシーバンドルビューを使用して、新しいポリシーバンドルを作成できます。ポリシーバンドルを作成するとき、各タイプの共有ポリシーを1つだけポリシーバンドルに割り当てることができます。

関連項目

- ポリシーバンドルの管理 （281 ページ）
- ポリシーバンドルの複製 （283 ページ）
- ポリシーバンドルの名前変更 （284 ページ）
- ポリシーバンドルのデバイスへの割り当て （284 ページ）

ステップ 1 次のいずれかの方法を使用して、ポリシーバンドルを作成できます。

- ポリシーバンドルビューで、次のいずれかを実行します。
  - [すべての共有ポリシー（All Shared Policies）] ビューから、バンドルする共有ポリシーを選択し、選択した共有ポリシーを右クリックして [ポリシーバンドルの作成（Create Policy Bundle）] を選択します。
  - ポリシーバンドルセレクタで既存のポリシーバンドルを右クリックし、[ポリシーバンドルの作成（Create Policy Bundle）] を選択します。
  - 共有ポリシーバンドルセレクタの下にある [ポリシーバンドルの作成（Create a Policy Bundle）] ボタンをクリックします。
- デバイス上のすべての共有ポリシーを含む新しいポリシーバンドルを作成するには、デバイスビューのデバイスセレクタでデバイスを右クリックし、[ポリシーバンドルの作成（Create Policy Bundle）] を選択します。

[ポリシーバンドルの作成（Create Policy Bundle）] ダイアログボックスが表示されます。

ステップ 2 新しいポリシーバンドルの名前を入力します。

ステップ 3 [OK] をクリック

ポリシーバンドルは、ポリシーバンドルビューの [ポリシーバンドル（policy bundles）] リストに追加されます。

ステップ 4 ポリシー バンドルの定義を設定するには、次のいずれかを実行します。

- ポリシーバンドルビューで：
  - 共有ポリシーをバンドルに追加するには、ポリシーバンドルセレクタで [すべての共有ポリシー（All Shared Policies）] を選択し、必要な共有ポリシーをポリシーバンドルにドラッグアンドドロップします。
  - バンドルから共有ポリシーを削除するには、ポリシーバンドルセレクタでバンドルを選択します。[ポリシーバンドルビュー（Policy Bundle View）] ウィンドウの [詳細（Details）] タブで削除する共有ポリシーを選択し、[削除（Delete）] をクリックします。
- ポリシービューで、ポリシーバンドルに追加する共有ポリシーを右クリックし、[ポリシーバンドルに追加（Add to Policy Bundle）] を選択してから、共有ポリシーを追加するバンドルを選択します。

ポリシーバンドルの複製

ポリシーバンドルビューを使用して、既存のバンドルを複製して新しいポリシーバンドルを作成できます。

関連項目

- ポリシーバンドルの管理 （281 ページ）
- 新しい共有ポリシーの作成 （278 ページ）
- 共有ポリシー名の変更 （270 ページ）
- ポリシーバンドルのデバイスへの割り当て （284 ページ）

ステップ 1 ポリシーバンドルビューのポリシーバンドルセレクタで既存のポリシーバンドルを右クリックし、[ポリシーバンドルの複製（Clone Policy Bundle）] を選択します。

[ポリシーバンドルの複製（Clone Policy Bundle）] ダイアログボックスが表示されます。

ステップ 2 新しいポリシーバンドルの名前を入力します。

ステップ 3 [OK] をクリック

新しいポリシーバンドルが共有ポリシーバンドルセレクタに表示されます。

ポリシーバンドルの名前変更

ポリシーバンドルビューから既存のポリシーバンドルの名前を変更できます。ポリシーバンドルの名前を変更しても、デバイスの割り当てには影響しません。

関連項目

- ポリシーバンドルの管理 （281 ページ）
- 新しい共有ポリシーの作成 （278 ページ）
- ポリシーバンドルの複製 （283 ページ）
- ポリシーバンドルのデバイスへの割り当て （284 ページ）

ステップ 1 ポリシーバンドルビューのポリシーバンドルセレクタで既存のポリシーバンドルを右クリックし、[ポリシーバンドルの名前変更（Rename Policy Bundle）] を選択します。

[ポリシーバンドルの名前変更（Rename Policy Bundle）] ダイアログボックスが表示されます。

ステップ 2 ポリシーバンドルの新しい名前を入力します。

ステップ 3 [OK] をクリック

ポリシーバンドルセレクタでポリシーバンドル名が更新されます。

ポリシーバンドルのデバイスへの割り当て

特定のポリシーバンドルが割り当てられているデバイスのリストを必要に応じて変更できます。ポリシーバンドルのポリシータイプが重複しない限り、複数のポリシーバンドルをデバイスに割り当てることができます。ポリシーバンドルをデバイスに割り当てるときに、そのデバイスのローカルポリシーがポリシーバンドルに含まれているものと同じポリシータイプである場合、既存のポリシーを継承するか、置き換えるかを選択できます。

（注） ポリシーバンドルに含まれるいずれかのポリシーに、割り当てようとしているデバイスとの互換性がない場合、そのバンドルを割り当てることはできません。

ポリシーバンドルの割り当てからデバイスを削除すると、そのバンドルに含まれるすべてのポリシーが、デバイスの計画中の設定から完全に削除されます。ローカルポリシーは失われ、取得できなくなります。展開時に、デバイスに存在するそのタイプの設定が削除されます。ポリシーの割り当て解除の意味の詳細については、ポリシーの割り当て解除 （255 ページ）を参照してください。

注意 ポリシーバンドルの割り当てを解除すると、その設定がデバイスから削除され、予期しない結果が発生するおそれがあるため、ポリシーバンドル割り当て機能は慎重に使用してください。たとえば、Cisco IOS ルータからデバイス アクセス ポリシーの割り当てを解除し、その変更を展開すると、Security Manager は今後そのデバイスを設定できなくなる可能性があります（Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）を参照）。

関連項目

- ポリシーバンドルの管理 （281 ページ）
- 新しい共有ポリシーの作成 （278 ページ）
- ポリシーバンドルの複製 （283 ページ）
- ポリシーバンドルの名前変更 （284 ページ）

ステップ 1 ポリシーバンドルビューのポリシーバンドルセレクタで、既存のポリシーバンドルを選択します。

ポリシーバンドルの詳細は、ポリシーバンドルのメインウィンドウに表示されます。

ステップ 2 [割り当て（Assignment）] タブをクリックします。

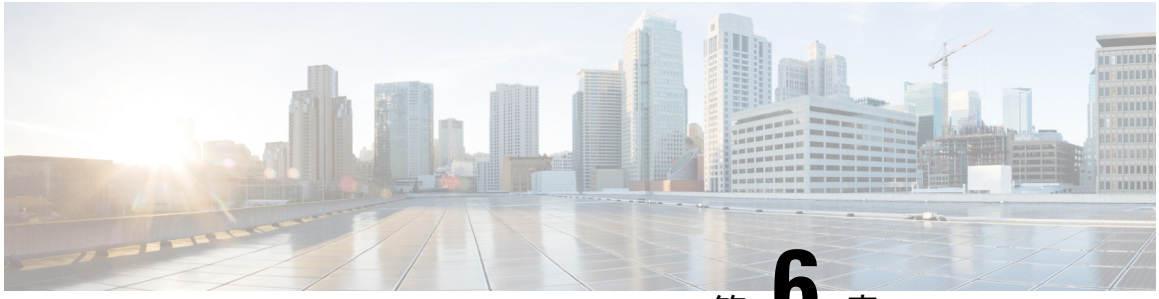
ステップ 3 次のように、ポリシーバンドルが割り当てられているデバイスのリストを変更します。

- 選択したポリシーバンドルを追加のデバイスに割り当てるには、[使用可能なデバイス（Available Devices）] リストからデバイスを選択し、[>>] をクリックして [割り当て済みデバイス（Assigned Devices）] リストに移動します。
- デバイスから選択したポリシーバンドルの割り当てを解除するには、[割り当て済みデバイス（Assigned Devices）] リストからデバイスを選択し、[<<] をクリックして [使用可能なデバイス/VPN（Available Devices/VPNs）] リストに戻します。ポリシーの割り当てが解除されたデバイスまたはトポロジは、展開時にこのポリシーを実行コンフィギュレーションから削除します。

ヒント ポリシーをデバイスグループ内のすべてのデバイスに割り当てるには、デバイスグループの名前を選択してから、[>>] をクリックします。

ステップ 4 [OK] をクリックして割り当ての変更を保存します。

ポリシーバンドル名がポリシーバンドルセレクタで更新されます。



第 6 章

ポリシー オブジェクトの管理

ポリシー オブジェクトを使用すると、要素の論理集合を定義できます。ポリシー オブジェクトは再利用可能な名前付きコンポーネントであり、他のオブジェクトやポリシーで使用できます。オブジェクトを使用すると、ポリシーを定義するたびにそのコンポーネントを定義する必要がなくなるため、ポリシーを定義するときに役立ちます。また、オブジェクトを使用すると、オブジェクトはオブジェクトまたはポリシーの内蔵コンポーネントになります。つまり、特定のオブジェクトの定義を変更すると、そのオブジェクトを参照しているすべてのオブジェクトおよびポリシーにこの変更が反映されます。

オブジェクトは個別に識別でき、また 1 箇所に集めて維持できるため、ネットワーク更新を簡単に行うことができます。たとえば、ネットワーク内のサーバを、MyServers という名前のネットワーク/ホスト オブジェクトとして識別し、これらのサーバで許可するプロトコルをサービス オブジェクトとして識別します。次に、サービス オブジェクトで定義されているサービスのトラフィックを、MyServers ネットワーク/ホスト オブジェクトが送受信することを許可するアクセス ルールを作成します。これらのサーバで変更を行う場合は、ネットワーク/ホスト オブジェクトまたはサービス オブジェクトを更新して再展開するだけで済み、サーバを使用している各ルールを見つけて編集する必要がなくなります。

オブジェクトはグローバルに定義されます。つまり、オブジェクトの定義は、そのオブジェクトを参照しているすべてのオブジェクトおよびポリシーで同じになります。ただし、多くのオブジェクト タイプ（インターフェイス ロールなど）は、デバイス レベルで上書きできます。したがって、ほとんどのデバイスに対して有効なオブジェクトを作成してから、要件が若干異なる特定のデバイスの設定にあうようにオブジェクトをカスタマイズできます。詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。

この章は次のトピックで構成されています。

- ポリシーのオブジェクトの選択 （288 ページ）
- Policy Object Manager （290 ページ）
- ポリシー オブジェクトの操作：基本手順 （298 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- 時間範囲オブジェクトの設定 （379 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

- マップ オブジェクトについて （388 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- プールオブジェクトについて （407 ページ）
- SAML ID プロバイダの構成 （415 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （426 ページ）

ポリシーのオブジェクトの選択

ドラッグアンドドロップを使用したポリシーの変更

既存のポリシーを変更する場合は、Policy Object Manager からポリシーの該当するフィールドにオブジェクトをドラッグアンドドロップすることで、ポリシー定義を簡単に更新できます。[Policy Object Manager] ウィンドウからオブジェクトの範囲を選択するには、範囲内の最初のオブジェクトを選択してから、Shift キーを押しながら範囲内の最後のオブジェクトを選択します。Ctrl キーを押しながらオブジェクトをクリックすると、複数のオブジェクトを選択できます。オブジェクトの範囲を選択してから、Ctrl キーを使用して選択範囲にオブジェクトを追加することもできます。複数のオブジェクトをドラッグするには、Ctrl キーを押しながらドラッグするか、マウスの右ボタンを使用してドラッグします。

オブジェクトセレクタを使用したポリシーの作成

ポリシーを作成するときに、多くの場合、ポリシー定義に含めるオブジェクトを 1 つ以上選択する必要があります。たとえば、ファイアウォール ポリシーでは、ネットワーク/ホスト オブジェクト、インターフェイス ロール オブジェクト、およびサービス オブジェクトが使用されます。

オブジェクトをポリシーに含めるには、オブジェクト名を手動で入力するか、[選択（Select）] ボタンをクリックしてオブジェクト セレクタ ダイアログボックスを表示します。オブジェクトセレクタは、設定しているポリシーに適用可能なオブジェクトだけを表示するように、事前にフィルタリングされている場合があります。たとえば、サブネットを必要とするポリシーを設定している場合、オブジェクト セレクタには、単一ホストを表すネットワーク/ホスト オブジェクトではなく、サブネットを表すネットワーク/ホスト オブジェクトだけが表示されます。オブジェクトセレクタにより、特定のポリシーに含めるオブジェクトを簡単に選択できます。

また、オブジェクトセレクタでは、そのタイプのオブジェクトをその場で作成および編集できます。これにより、定義中のポリシーを離れて Policy Object Manager を開かなくても、オブジェクトを簡単に操作できます。たとえば、ダイナミック NAT ルールの作成中に、必要な ACL オブジェクトが存在しないことがわかった場合、[Create] ボタンをクリックして、ACL オブジェクトを作成するためのダイアログボックスを開くことができます。オブジェクトの作成を終了すると、オブジェクト セレクタに戻ります。オブジェクト セレクタでは、新しいオブジェクトが選択され、ポリシーに含めることができるようになっています。既存のオブジェクトを変更してから使用する必要がある場合は、そのオブジェクトを選択し、[Edit] ボタンをク

リックして変更し、[OK] をクリックして変更を保存します。これにより、オブジェクト セレクタに戻ります。

セレクタからオブジェクト エディタを開いてオブジェクトを作成する場合、新しいオブジェクトは、セレクタが開かれた元のフィールドの要件に準拠している必要があります。たとえば、ホストを必要とするフィールドからセレクタを開き、そのフィールドのネットワーク/ホスト オブジェクトを作成する場合は、ネットワーク/ホスト オブジェクトをホストとして定義する必要があります。

オブジェクト セレクタには 2 つのタイプがあります。1 つのオブジェクトを選択する必要があるポリシー用の単純リスト セレクタと、特定のタイプの複数のオブジェクトを選択できるポリシー用のデュアル セレクタです。次の表に、これらのセレクタとその使用方法を示します。

表 *40* : オブジェクト セレクタ

要素	説明
タイプ	セレクタに表示するオブジェクトのタイプ（オプションがある場合）。次に例を示します。 • 一部のルールベースのポリシーで送信元および宛先を設定する場合、ネットワーク/ホスト オブジェクトまたはインターフェイス ロールを選択できます。 • 一部の ACL を設定する場合（Catalyst 6500/7600 デバイスで VLAN ACL を設定する場合など）、標準または拡張 ACL オブジェクトを選択できます。 **ヒント** 一部のポリシーでは、複数のオブジェクト タイプを選択した場合、フィールド内の別のタブに表示されます。
Available（オブジェクト タイプ）	設定しているポリシーまたはオブジェクトに関連するすべてのオブジェクトが表示されます。 インターフェイスを選択するときは、同じ名前のインターフェイスやインターフェイス ロールが存在する場合があることに注意してください。これらは名前の横に表示されるアイコンで区別できます。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。 **ヒント** リスト ボックスを選択してオブジェクト名の入力を開始することによって、セレクタ内でオブジェクトを迅速に見つけることができます。
Selected（オブジェクト タイプ）	編集しているポリシーまたはオブジェクトに適用するために選択したオブジェクトが表示されます。
複数オブジェクト セレクタ ボタン	

要素	説明
[>>] ボタン [<<] ボタン	選択したオブジェクトが一方のリストから他方のリスト（示されている方向）に移動します。Ctrl を押しながらクリックすることで、複数のオブジェクトを選択できます。 ダブルクリックするか、選択して Enter を押すことによって、リスト間でオブジェクトを移動することもできます。
上下の矢印ボタン	オブジェクトタイプの数が制限される場合、順序が問題になります。セレクタに [上へ移動（Move Up）] および [下へ移動（Move Down）] ボタンがある場合は、オブジェクトを優先順に配置します。たとえば、AAA の方式リストを定義する場合、矢印を使用して、さまざまなタイプの AAA サーバ グループが使用される順序を決定します。
共通ボタン	
[Create] ボタン	このタイプのオブジェクトを作成するには、このボタンをクリックします。 **ヒント** ネットワーク/ホストオブジェクトやサービスオブジェクトなどでは、このボタンをクリックするとリストが表示され、そのリストからオブジェクトの特定のタイプを選択する必要があります。
[編集（Edit）] ボタン	選択したユーザ定義オブジェクトを編集するには、このボタンをクリックします。システム定義のオブジェクトを編集しようとした場合は、読み取り専用モードで開かれます。

関連項目

- ポリシー オブジェクトの上書きの許可 （311 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

Policy Object Manager

Policy Object Manager は、次の目的に使用します。

- 使用可能なすべてのオブジェクトをオブジェクトタイプ別にグループ化して表示する。
- ポリシー オブジェクトを作成、コピー、編集、および削除します。
- オブジェクトを既存のポリシーにドラッグアンドドロップして、ポリシー定義を更新する。
- 使用状況レポートを生成します。このレポートでは、選択したオブジェクトが他の Security Manager オブジェクトおよびポリシーによってどのように使用されているかが示されます。

ナビゲーション パス

デバイスビューまたはポリシービューで、ツールバーの [Policy Object Manager] ボタンをクリックするか、[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択します（Policy Object Manager は、マップビューから開くことはできません）。

（注） Policy Object Manager を開くと、オブジェクトのドラッグアンドドロップを容易にするために、最初は現在のビューの下半分にペインとして表示されます。このペインのドッキングを解除して、Policy Object Manager を別のウィンドウにすることができます。ウィンドウを再度ドッキングすることもできます。詳細については、ポリシーオブジェクト マネージャー: ドッキング解除とドッキング （296 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- オブジェクト使用状況レポートの生成 （306 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *41 : [Policy Object Manager]* ウィンドウ

要素	説明
オブジェクトタイプセレクタまたはコンテンツテーブル （左側のペイン）	Security Manager で使用可能なオブジェクト タイプが一覧表示されます。オブジェクトタイプを選択すると、そのタイプの既存のすべてのオブジェクトが右側のペインの表に表示されます。 オブジェクトは、[お気に入り（Favorites）]、[最新オブジェクト（Recent Objects）]、および [すべてのオブジェクトタイプ（All Object Types）] の 3 つのフォルダに編成されます。フォルダ名の左側にある矢印をクリックして、そのフォルダを展開します。 お気に入りのオブジェクトタイプを指定できます。これらのオブジェクトタイプは別のリストに表示されるため、より簡単にアクセスできます。オブジェクトタイプをお気に入りリストに追加するには、オブジェクトを右クリックし、[お気に入りに追加（Add to Favorites）] を選択します。お気に入りリストからオブジェクトタイプを削除するには、オブジェクトを右クリックし、[お気に入りから削除（Remove from Favorites）] を選択します。 [最新オブジェクト（Recent Objects）] は、最近変更された 10 個のオブジェクトのリストです。最新オブジェクトをクリックすると、名前、タイプ、説明、最終更新日を含むオブジェクトの概要が表示されます。オブジェクトの [オブジェクトの表示（View Object）]、[オブジェクトの編集（Edit Object）]、および [使用状況の検索（ Find Usage）] ボタンにアクセスすることもできます。 [すべてのオブジェクトタイプ（All Object Types）] フォルダを展開すると、使用可能なすべてのタイプのオブジェクトが表示されます。

要素	説明
ポリシー オブジェクト テーブル（右側のペイン） 右側のペインのポリシー オブジェクト テーブルには、コンテンツ テーブルで選択されたタイプの既存のオブジェクトが表示されます。このテーブルを使用して、新しいオブジェクトを作成し、既存のオブジェクトを操作します。テーブルの下にあるボタンを使用するか、テーブル内を右クリックしてその他のコマンドを表示できます（Policy Object Manager のショートカットメニュー （297 ページ）を参照）。 アクセス コントロール リスト（ACL）オブジェクトを除き、オブジェクト タイプごとに 1 つのテーブルがあります。ACL の場合は、拡張 ACL、標準 ACL、Web ACL および統合 ACL を分けるタブがあります。該当するタブを選択して、目的のオブジェクト タイプを操作します。 テーブルのカラムは、選択するオブジェクトのタイプによって異なります。テーブルの見出しを右クリックし、[Show Columns] コマンドのカラムを選択または選択解除することによって、テーブルに表示されるカラムを変更できます。カラム見出しをクリックすることで、カラムのコンテンツによって情報をソートすることもできます。見出しをクリックして、アルファベット順のソートと逆アルファベット順のソートを切り替えます。 テーブルに表示される設定の詳細については、テーブルの下にある [Create] または [Edit] ボタンをクリックし、開かれるダイアログボックスで [Help] をクリックしてください。次のセクション「表のカラム」では、通常表示される列について説明します。	
表の上のボタン	
参照（Referenced）	オブジェクトの参照情報を表示するには、このオプションを選択します。選択すると、[参照（Referenced）] 列がテーブルに追加され、オブジェクトがポリシーまたはポリシーオブジェクトによって使用されているかどうかに関する情報が表示されます。
Find Usage	使用状況の検索機能を使用して、選択したオブジェクトを使用しているポリシーまたはポリシーオブジェクト、およびオブジェクトのデバイスオーバーライドに関するレポートを表示します。詳細については、オブジェクト使用状況レポートの生成 （306 ページ）を参照してください。
View Object	テーブルで 1 つのオブジェクトが選択されている場合、このボタンをクリックすると、そのタイプのオブジェクトの [編集（Edit）] ダイアログボックスが読み取り専用モードで開き、その特定のオブジェクトの設定を表示できます。
エクスポート	エクスポート機能を使用して、選択したオブジェクトタイプのオブジェクトデータの CSV ファイルをダウンロードします。
印刷（Print）	印刷機能を使用して、選択したオブジェクトタイプのオブジェクトデータを印刷します。

要素	説明
Filter	行をフィルタリングして表示し、大きいテーブルで項目を見つけやすくします。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
表のカラム	
*	ポリシーオブジェクトのステータスを示します。 • - ポリシーオブジェクトは編集がロックされています。ロックアイコンにカーソルを合わせると、オブジェクトをロックしているユーザとチケット/アクティビティが表示されます。 • - 現在のチケット/アクティビティでポリシーオブジェクトが変更されましたが、変更が送信されていません。 （注） ステータスアイコンにカーソルを合わせると、ポリシーオブジェクトを変更/ロックしたチケット/アクティビティの詳細を表示したり、そのチケット/アクティビティに移動したりできます。
アイコン（ラベルのないフィールド）	オブジェクトが表示される場所（ルール テーブル内など）では常に、ポリシー オブジェクト タイプに対して表示されるアイコンによって、そのタイプのオブジェクトが識別されます。アイコン内に鉛筆のイメージがある場合は、編集が可能です。
名前	ポリシー オブジェクトの名前。
Content	オブジェクト定義の概要。定義されているすべての設定が含まれていない場合があります。
許可（Permit）	ACL オブジェクトの場合、アクセス コントロール エントリ（ACE）によってトラフィックが許可されるときに、[Permit] カラムにチェックマークが表示されます。アクションが拒否の場合は、スラッシュの入った赤色の丸が表示されます。
カテゴリ	オブジェクトに割り当てられているカテゴリ オブジェクト（ある場合）。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
オーバーライド	ユーザがデバイス レベルでオブジェクトのプロパティを上書きできるかどうか。チェックマークは、オブジェクトを上書きできることを示します。すべてのオブジェクトタイプを上書きできるわけではありません。 オブジェクトがオーバーライドされている場合、[オーバーライド（Overrides）]列には、そのオブジェクトのオーバーライドの数が表示されます。数字をクリックすると、オーバーライドのリストが表示されます。 デバイスのオーバーライドの詳細については、オブジェクト オーバーライドの管理 （309 ページ）を参照してください。
参照（Referenced）	オブジェクトがポリシー定義で使用されているかどうか。使用状況の検索機能を使用して、選択したオブジェクトを使用しているポリシーまたはポリシーオブジェクト、およびオブジェクトのデバイス オーバーライドを見つけることができます（オブジェクト使用状況レポートの生成 （306 ページ）を参照）。 （注） 参照情報を表示するには、ポリシーオブジェクトテーブルの上にあるツールバーで [参照（Referenced）] オプションが選択されていることを確認します。 （注） [参照（Referenced）] 列では、すべてのアクティビティ/チケット全体にわたるコミットされたデータとコミットされていないデータの両方に基づいた使用状況がレポートされますが、[使用状況の検索（Find Usage）]機能では、コミットされたデータと現在のアクティビティ/チケットからのデータに基づいた使用状況のみがレポートされます。
説明	オブジェクトの説明。列が狭すぎて説明を表示できない場合は、アイコンをダブルクリックして説明を表示するか、アイコンの上にマウスを移動します。
[最後のチケット（Last Ticket(s)）]	チケットが有効になっている場合、オブジェクトの変更に最後に使用されたチケットのチケット ID が表示されます。をクリックできます。 チケットが有効になっている場合、オブジェクトへの最後の変更に関連付けられたチケットが表示されます。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
最終更新日	オブジェクトが最後に変更された日時を示します。

要素	説明
テーブルの下のボタン	
	新しいオブジェクトを作成するには、[New Object] ボタンをクリックします。テーブルに項目を追加するすべてのボタンに、同じアイコンが使用されます。 ヒント　ネットワーク/ホストオブジェクトやサービスオブジェクトなどでは、このボタンをクリックするとリストが表示され、そのリストからオブジェクトの特定のタイプを選択する必要があります。 このボタンをクリックすると、オブジェクトを作成するダイアログボックスが開きます。選択されたオブジェクトタイプについては、ダイアログボックス内の [Help] ボタンをクリックしてください。また、「ポリシー オブジェクトの作成 （299ページ）」を参照してください。
	選択したオブジェクトを編集するには、[Edit Object] ボタンをクリックします。テーブル内のオブジェクトの編集には、同じアイコンが使用されます。 オブジェクトの編集に使用するダイアログボックスは、オブジェクトの作成に使用するダイアログボックスと同じです。システム定義のデフォルトオブジェクトを編集しようとすると、オブジェクトのコンテンツの表示だけが許可されます。設定については、ダイアログボックス内の [Help] ボタンをクリックしてください。詳細については、オブジェクトの編集 （303 ページ）を参照してください。
	選択したオブジェクトを削除するには、[Delete Object] ボタンをクリックします。ポリシーまたは別のポリシーオブジェクトで現在使用されていないユーザ定義のオブジェクトだけを削除できます。詳細については、オブジェクトの削除 （308 ページ）を参照してください。

ポリシーオブジェクト マネージャー: ドッキング解除とドッキング

Policy Object Manager を開くたびに、オブジェクトのドラッグアンドドロップを容易にするため、最初は現在のビューの下半分にペインとして表示されます。このペインのドッキングを解除して、Policy Object Manager を別のウィンドウにすることができます。ウィンドウを再度ドッキングすることもでき、ペインまたはウィンドウを閉じることも可能です。

- [Configuration Manager] ウィンドウの現在のビューから [Policy Object Manager] をドッキング解除するには、ペインのタイトルバーの右上隅にある [ウィンドウのドッキング解除（Undock Window）] ボタンをクリックします。

- フローティングウィンドウをもう一度 [Configuration Manager] ウィンドウのペインにするには、[Policy Object Manager] ウィンドウの右上隅にある [フレームのドッキング（Dock Frame）] ボタンをクリックします。
- ペインまたはフローティングウィンドウを閉じるには、右上隅にある [閉じる（Close）] ボタンをクリックします。

ナビゲーション パス

デバイスビューまたはポリシービューで、ツールバーの [Policy Object Manager] ボタンをクリックするか、[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択します（Policy Object Manager をマップビューから開くことはできません）。

Policy Object Manager のショートカットメニュー

Policy Object Manager （290 ページ）でポリシー オブジェクト テーブル内を右クリックすると、選択したオブジェクト タイプに対してさまざまな機能を実行するためのショートカット メニューが表示されます。

フィールド リファレンス

表 *42 : Policy Object Manager* のショートカットメニュー

メニュー コマンド	説明
New Object	新しいポリシーオブジェクトを作成するには、このコマンドを選択します。オブジェクトタイプ固有の情報については、開かれるダイアログボックス内の [Help] をクリックしてください。また、「ポリシー オブジェクトの作成 （299 ページ）」を参照してください。 **ヒント** ネットワーク/ホスト オブジェクトまたはサービス オブジェクトの場合、サブメニューからオブジェクト タイプを選択する必要もあります。
Edit Object	テーブルで選択したポリシーオブジェクトを編集するには、このコマンドを選択します。システム定義のデフォルト オブジェクトを選択すると、オブジェクト定義の参照専用の画面が表示されます。詳細については、オブジェクトの編集 （303 ページ）を参照してください。
Delete Object	テーブルで選択したポリシーオブジェクトを削除するには、このコマンドを選択します。ポリシーまたは別のポリシー オブジェクトで使用されていないユーザ定義のオブジェクトだけを削除できます。詳細については、オブジェクトの削除 （308 ページ）を参照してください。

メニュー コマンド	説明
デバイスのオーバーライドの有効化/無効化	Enable Device Overrides コマンドを選択して、オーバーライドが無効になっている 1 つ以上のデバイスでデバイスオーバーライドを有効にします。Disable Device Overrides コマンドを選択して、オーバーライドが有効になっている 1 つ以上のデバイスでデバイスオーバーライドを無効にします。
Edit Device Overrides	[Policy Object Overrides] ウィンドウ （314 ページ）を使用してこのオブジェクトのデバイスレベルのオーバーライドを変更するには、このコマンドを選択します。オーバーライドを作成、編集、および削除できます。詳細については、 オブジェクト オーバーライドの管理 （309 ページ）を参照してください。
Clone Object	ポリシーオブジェクトのコピーを作成するには、このコマンドを選択します。詳細については、 オブジェクトのクローニング（複製） （305 ページ）を参照してください。
Copy Object	選択した 1 つまたは複数のオブジェクトをシステムのクリップボードにコピーするには、このコマンドを選択します。 ヒント　**Ctrl+C** を使用してオブジェクトをコピーすることもできます。
Paste Object	このコマンドを選択して、システムクリップボードのオブジェクトを別のオブジェクトに貼り付けます。たとえば、ホストタイプのネットワーク/ホストオブジェクトを既存のグループタイプのネットワーク/ホストオブジェクトに追加できます。2 つのオブジェクトタイプに互換性がある必要があります。 ヒント　**Ctrl+V** を使用して、オブジェクトを貼り付けることもできます。
Find Usage	[オブジェクトの使用状況（Object Usage）] ダイアログボックスを使用して、選択したオブジェクトの使用状況レポートを生成するには、このコマンドを選択します。使用状況レポートには、オブジェクトが現在使用されている場所が示されます。詳細については、オブジェクト使用状況レポートの生成 （306 ページ）を参照してください。
View Object	オブジェクトの編集ダイアログボックスの読み取り専用バージョンを使用してオブジェクトの定義を表示するには、このコマンドを選択します。詳細については、 オブジェクトの詳細の表示 （305 ページ）を参照してください。

ポリシー オブジェクトの操作：基本手順

次の項では、ポリシーオブジェクトに対して実行できるアクションについて説明します。一部のタスクは、特定のタイプのオブジェクトに限定されます。たとえば、すべてのタイプのオブ

ジェクトを上書きできるわけではありません。定義済みオブジェクトは編集できません。また、すべてのオブジェクトをインポートまたはエクスポートできるわけではありません。

ここでは、次の内容について説明します。

- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクトのクローニング（複製） （305 ページ）
- オブジェクトの詳細の表示 （305 ページ）
- オブジェクト使用状況レポートの生成 （306 ページ）
- オブジェクトの削除 （308 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトのインポートおよびエクスポート （318 ページ）

ポリシー オブジェクトの作成

Security Manager には、ポリシーを定義するために使用できる、さまざまなタイプの定義済みポリシーオブジェクトがあります。また、必要に応じて独自のオブジェクトを作成できます。

次の 2 つの方法のいずれかでオブジェクトを作成できます。

- [Policy Object Manager] ウィンドウの使用。このオプションは、特定のポリシーを定義するとき以外に、1 つ以上のオブジェクトを定義する状況に最適です。 Policy Object Manager （290 ページ）を参照してください。
- オブジェクトセレクタの使用。オブジェクトを使用するポリシーを定義する際には、オブジェクトを作成および編集するためのボタンがオブジェクトセレクタに表示されるため、定義しているポリシーを離れる必要はありません。ポリシー作成中に、状況に適した特定のオブジェクトタイプが要求され、ポリシーに対して必要な設定をより意識するようになるため、多くの場合これが最適な方法です。ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

ヒント 同じ定義の複数のオブジェクトを作成できるかどうかは、[Cisco Security Manager管理（Security Manager Administration）] ウィンドウ（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択）の [ポリシーオブジェクト（Policy Objects）] ページの設定によって決まります。デフォルトでは、既存のオブジェクトの定義と同じ定義のオブジェクトを作成すると、Security Manager から警告が表示されますが、続行できます。詳細については、[Policy Objects] ページ （732 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの管理 （287 ページ）
- ポリシー オブジェクトの操作：基本手順 （298 ページ）

ステップ 1 次のいずれかを実行します。

- **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （290 ページ）を開きます。作成するオブジェクトのタイプを目次から選択し、テーブル内を右クリックして、[新規オブジェクト（New Object）] を選択します。
- ルールの設定中に、ポリシーオブジェクトを許可または要求するフィールドの横にある [選択（Select）] を選択します。オブジェクトセレクタで、使用可能なオブジェクトリストの下にある [作成（Create）] ボタンをクリックします。

ヒント ネットワーク/ホスト オブジェクトやサービス オブジェクトなどでは、これらのボタンをクリックするとリストが表示され、そのリストからオブジェクトの特定のタイプを選択する必要があります。

選択したタイプのオブジェクトを追加するためのダイアログボックスが開きます。オブジェクトの個々のタイプの詳細については、次の項を参照してください。

- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- [ASパスオブジェクトの追加（（Add AS Path Object）]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924 ページ）
- [ASA Group Policies] ダイアログボックス （1918 ページ）
- [BFDテンプレートの追加または編集（Add or Edit BFD Template）] ダイアログボックス
- カテゴリ オブジェクトの使用 （304 ページ）
- [コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （2926 ページ）
- クレデンシャル ポリシー オブジェクトの設定 （1610 ページ）
- [Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）および FlexConfig ポリシー オブジェクトの作成 （465 ページ）
- アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）
- [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）
- [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

- IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）
- [Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （347 ページ）
- マップ オブジェクトについて （388 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- [PKI Enrollment] ダイアログボックス （1554 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）
- プールオブジェクトについて （407 ページ）
- [Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス （1977 ページ）
- ポート リスト オブジェクトの設定 （420 ページ）
- [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）
- リスク評価ポリシーオブジェクトの構成 （2230 ページ）
- [ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （2901 ページ）
- セキュリティ グループ オブジェクトの作成 （863 ページ）
- Cisco Secure Desktop 設定オブジェクトの作成 （1913 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- [Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス （1980 ページ）
- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）
- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス （2011 ページ）
- [Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス （2020 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- [Add Text Object]/[Edit Text Object] ダイアログボックス （470 ページ）
- 時間範囲オブジェクトの設定 （379 ページ）
- トラフィック フロー オブジェクトの設定 （2965 ページ）
- [Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）

- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化 （1825 ページ）

ステップ 2 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

オブジェクト名は、大文字と小文字が区別されず、128 文字に制限されています。オブジェクト名は、文字、数字、またはアンダースコアで始めることができます。オブジェクト名の残りの部分では、文字、数字、特殊文字、およびスペースを混在させることができます。

サポートされている特殊文字は次のとおりです。

- ハイフン（-）、
- 下線（_）、
- ピリオド（.）、および、
- プラス記号（+）。

バージョン 4.12 以降、Cisco Security Manager では、次の追加の特殊文字を使用できます。

- 感嘆符（!）、
- アットマーク（@）、
- ハッシュ記号（#）、
- パーセント記号（%）、
- アンパサンド記号（&）、および
- 括弧または丸括弧（）。

Cisco Security Manager は、次の文字をサポートしていません。

- キャレット文字（^）
- ドル文字（$）

一部のオブジェクトでは、オブジェクト名にコロン（:）を使用できますが、名前にコロンが含まれているオブジェクトは、IPS デバイスではサポートされていません。IPS デバイスを含む異なるデバイスタイプ間でオブジェクトを共有する場合は、オブジェクト名にコロン（:）を使用しないでください。

（注） 特定のオブジェクト タイプ（AAA サーバ グループ、ASA ユーザ グループ、マップ、ネットワーク/ホスト オブジェクト、サービス オブジェクト、トラフィック フローなど）には、異なる命名ガイドラインがあります。詳細については、各オブジェクト タイプの作成中にオンライン ヘルプを参照してください。

ステップ 3 オブジェクト タイプ固有の設定を行います。ダイアログボックスについては、オンライン ヘルプ ページを参照してください。

ステップ 4 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照。

ステップ 5 （任意）オブジェクトタイプにオプションがある場合は、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、そのオブジェクトのプロパティを個々のデバイスで再定義できます。 ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 6 [OK] をクリックしてオブジェクトを保存します。

オブジェクトの編集

必要に応じて、ユーザ定義オブジェクトを編集できます。オブジェクトに対して行った変更は、そのオブジェクトを使用するすべてのポリシー（およびその他のオブジェクト）に反映されます。ただし、デバイスに対してオブジェクトのオーバーライドがすでに定義されている場合、編集はそれらのデバイスで使用されているオブジェクトに反映されません。

ヒント

- 定義済みオブジェクトは編集できませんが、コピーして新しいオブジェクトを作成できます。 オブジェクトのクローニング（複製） （305 ページ）を参照してください。
- [Edit] ダイアログボックスの一番上に、次の状況を示すメッセージが表示されます。
  - オブジェクトへの読み取り専用アクセスができます。これらのオブジェクトへの変更を保存できません。
  - ポリシーまたはデバイスのインポート （615 ページ）で説明する手順を使用して、ポリシーオブジェクトがインポートされました。インポートされたオブジェクトを使用する共有ポリシーが異なるサーバで管理されている場合、そのオブジェクトは今後、再度インポートされる可能性があります。ポリシーオブジェクトに加えた変更は、ポリシーオブジェクトが再度インポートされた場合には削除されます。オブジェクトを編集する前に、ポリシー管理およびインポート用に組織で使用されているプロトコルを確実に理解してください。**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー管理（Policy Management）]** ページのオプションを使用して、このメッセージを表示するかどうかを制御できます（[Policy Management] ページ （729 ページ）を参照）。
- このオブジェクトタイプを使用するポリシーまたはオブジェクトを定義するときに、オブジェクトを編集することもできます。詳細については、ポリシーのオブジェクトの選択（288 ページ）を参照してください。

はじめる前に

オブジェクトが使用されているかどうか、および変更の影響を受けるポリシー、オブジェクト、デバイスを判別します。このために使用状況レポートを生成できます。 オブジェクト使用状況レポートの生成 （306 ページ） を参照してください。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （290 ページ）を開きます。

ステップ 2 コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3 編集するオブジェクトを右クリックし、[オブジェクトの編集（Edit Object）] を選択します。

ステップ 4 必要に応じて、そのオブジェクトタイプの [編集（Edit）] ダイアログボックスでフィールドを変更し、[OK] をクリックして変更を保存します。オブジェクト タイプ固有の情報については、[Help] ボタンをクリックしてください。

カテゴリ オブジェクトの使用

カテゴリは、オブジェクトに関する中間レベルの詳細を示します。カテゴリをオブジェクトに割り当てることによって、カテゴリの名前および色を確認して、ルールテーブル内のルールおよびオブジェクトを簡単に識別できます。ルールを作成するときに、ルールまたはオブジェクトにカテゴリを割り当てることができます。または、カテゴリ情報が含まれるようにルールまたはオブジェクトをあとで編集できます。カテゴリ割り当てに対してデバイス コンフィギュレーション コマンドは生成されません。

ポリシー オブジェクトにカテゴリを割り当てることの利点は、次のとおりです。

- 分類されたオブジェクトを使用してルールテーブルを表示すると、可視性が向上します。
- カテゴリに基づいてルールテーブル内でオブジェクトをフィルタリングでき、ルールを保守しやすくなります。

たとえば、ネットワーク/ホスト オブジェクトを作成し、管理のためにその使用を追跡する場合があります。このネットワーク/ホスト オブジェクトを定義するときに、カテゴリに関連付けます。アクセス ルール テーブルを表示すると、このネットワーク/ホスト オブジェクトを使用しているルールを簡単に識別できます。テーブルをフィルタリングして、カテゴリに関連付けられている項目だけを表示することもできます。

Security Manager には、定義済みのカテゴリのセットがあります。色は変更できませんが、名前および説明を変更できます。次の手順では、名前および説明を変更する方法について説明します。

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [カテゴリ（Categories）] を選択します。

ステップ 3 [オブジェクトの編集（Edit Object）] をクリックして、[カテゴリエディタ（Category Editor）] ダイアログボックスを開きます。

ステップ 4 必要に応じて、定義済みのカテゴリ オブジェクトの名前および説明を変更します。

- [Label]：カテゴリに関連付けられている色。

- [Name]：カテゴリ名。名前は最大 128 文字で、特殊文字とスペースを使用できます。
- [Description]：オブジェクトに関する追加情報（最大 1024 文字）。

ステップ 5 [OK] をクリックして変更を保存します。

オブジェクトのクローニング（複製）

ポリシーオブジェクトを最初から作成する代わりに、既存のオブジェクトのクローン作成または複製ができます。新しいオブジェクトには、コピー元のオブジェクトの属性がすべて含まれます。必要に応じて、名前およびすべての属性を変更できます。

クローニングは、編集できない定義済みオブジェクトに基づいたオブジェクトの作成に役立ちます。

関連項目

- ポリシー オブジェクトの操作：基本手順 （298 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （290 ページ） を開きます。

ステップ 2 コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3 複製するオブジェクトを右クリックし、[オブジェクトの複製（Clone Object）] を選択します。

そのオブジェクト タイプのダイアログボックスが表示されます。[名前（Name）] フィールドには、新しいオブジェクトのデフォルト名（Copy of コピー元オブジェクトの名前）が入ります。残りのフィールドには、コピー元オブジェクトと同じ値が入ります。

ステップ 4 必要に応じて、新しいオブジェクトの名前およびその設定を変更します。そのオブジェクト タイプ固有の情報については、[Help] ボタンをクリックしてください。

ステップ 5 [OK] をクリックして変更を保存します。

オブジェクトの詳細の表示

オブジェクトが別のアクティビティによってロックされている場合でも、オブジェクトのコンテンツを読み取り専用モードで表示できます。これは、[Policy Object Manager] ウィンドウでは定義を完全には表示できない複雑なオブジェクトの設定の詳細を完全に表示する必要がある場合、またはユーザ権限によってオブジェクト情報の表示だけが許可されている場合に役立ちます。

関連項目

- ポリシー オブジェクトの操作：基本手順 （298 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、 Policy Object Manager （290 ページ）を開きます。

ステップ 2 コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3 オブジェクトを右クリックし、[オブジェクトの表示（View Object）] を選択します。

そのオブジェクトのダイアログボックスが読み取り専用モードで表示されます。

オブジェクト使用状況レポートの生成

ポリシーオブジェクトを変更する前に、そのオブジェクトが使用されているかどうかを判別する必要があります。これを行うには、[Policy Object Manager] ウィンドウの [参照（Referenced）] 列を表示します。ポリシーオブジェクトテーブルの上にある [参照（Referenced）] ボタンを選択して [参照（Referenced）] 列を有効にします。

参照されているオブジェクトについて、選択したオブジェクトが使用されているために、そのオブジェクトに対する変更の影響を受けるポリシー、オブジェクト、VPN、およびデバイスを示す使用状況レポートを生成できます。使用状況レポートには、現在のアクティビティで選択したオブジェクトへの参照、およびデータベースにコミットされたデータで見つかった参照が含まれています。

（注） [参照（Referenced）] 列では、すべてのアクティビティ/チケット全体にわたるコミットされたデータとコミットされていないデータの両方に基づいた使用状況がレポートされますが、[使用状況の検索（Find Usage）] 機能では、コミットされたデータと現在のアクティビティ/チケットからのデータに基づいた使用状況のみがレポートされます。

次の方式のいずれかを使用して、使用状況レポートを生成できます。

- Policy Object Manager：[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、 Policy Object Manager （290 ページ）を開きます。オブジェクトのタイプを目次から選択し、オブジェクトを右クリックして、[使用状況の検索（Find Usage）] を選択します。
- ファイアウォール ルール ポリシー：ファイアウォール ルール テーブルでオブジェクトをクリックし、右クリックして、[使用状況の検索（Find Usage）] を選択します。

使用状況情報が [Object Usage] ダイアログボックスに表示されます。テーブルの上にある適切な使用状況タイプを選択して、選択したオブジェクトを使用するデバイス、ポリシー、VPN、またはその他のオブジェクトを表示します。

特定のポリシー：

次の表に、ダイアログボックスのフィールドを示します。

表 *43 : [Object Usage]* ダイアログボックス

要素	説明
名前 タイプ 説明	使用状況を検索しているオブジェクトに関する一般情報は、[オブジェクトの使用状況（Object Usage）] ダイアログボックスの上部に表示されます。
デバイス ポリシー オブジェクト VPN	表示する参照のタイプ。たとえば、[オブジェクト（Objects）] を選択すると、他のオブジェクトからのオブジェクトの参照だけを表示できます。
使用者	選択したオブジェクトを参照しているデバイス、ポリシー、VPN、またはオブジェクトの名前。
タイプ（Type）	選択したオブジェクトを参照している項目のタイプ。これは、デバイス、ポリシー、VPN、または別のオブジェクトです。
使用方法（Usage）	オブジェクトがどのように参照されているかが示されます。たとえば、選択したオブジェクトがデバイスによって参照されている場合、このカラムには、オブジェクトを参照しているのはデバイスに割り当てられたポリシーであることが示されます。
プロキシミティ（Proximity）	選択したオブジェクトとそれを使用している項目との関係が示されます。次に例を示します。 • 定義内にネットワーク/ホストオブジェクトが含まれているポリシーは、そのオブジェクトと直接的な関係を持ち、オブジェクトに含まれる他のネットワーク/ホストオブジェクトと間接的な関係を持ちます。 • このポリシーが割り当てられているデバイスは、ネットワーク/ホストオブジェクトを直接的に参照し、オブジェクトに含まれる他のネットワーク/ホストオブジェクトを間接的に参照します。

要素	説明
詳細パネル	特定のタイプの参照に関する追加の詳細情報が表示されます。 • [デバイス（Devices）]：サポートされているポリシータイプの場合、デバイス情報が [詳細（Details）] パネルに表示されます。 • [ポリシー（Policies）]：次のサポートされているポリシータイプの場合、オブジェクトを参照する実際のルールが [詳細（Details）] パネルに表示されます。 • AAA ルール • アクセル ルール • IPv6 アクセスルール • インスペクション ルール • 変換ルール • Web フィルタルール（PIX/FWSM/ASA） • ゾーンベースのファイアウォールルール [詳細（Details）] パネルから、ルールへの移動、ルールデータのエクスポート、またはルールデータの印刷を行うことができます。 • [オブジェクト（Objects）]：指定したオブジェクトを参照している他のオブジェクトの詳細情報が [詳細（Details）] パネルに表示されます。[オブジェクトの使用状況（Object Usage）] ダイアログボックスの [詳細（Details）] パネルから、詳細情報のエクスポート、情報の印刷、読み取り専用モードでのオブジェクトの表示、オブジェクトの編集、またはオブジェクトの使用状況の検索を行うことができます。

オブジェクトの削除

ユーザ定義のオブジェクトは、ポリシーまたは他のオブジェクトで使用されていない場合にだけ削除できます。定義済みのオブジェクトは削除できません。デバイスレベルのオーバーライドが定義されているオブジェクトを削除すると、オーバーライドもすべて削除されます。

ヒント　使用されていないオブジェクトをデータベースから削除できない場合があります。たとえば、オブジェクトを使用していたローカル ポリシーを、オブジェクトを使用しない共有ポリシーと置き換える場合などです。オブジェクトの削除が失敗する場合は、保留中の変更をすべて送信または廃棄してから（Workflow モードで、保留中のアクティビティをすべて送信または廃棄）、オブジェクトの削除を再試行します。または、データベース内の使用されていないオブジェクトはポリシーに影響しないため、そのままにしておくことができます。

はじめる前に

オブジェクトが現在使用されているかどうか、および削除の影響を受けるポリシー、オブジェクト、デバイスを判別します。オブジェクトを削除する前に、オブジェクトへの参照をすべて削除する必要があります。このために使用状況レポートを生成できます。オブジェクト使用状況レポートの生成　（306 ページ）を参照してください。

ステップ 1　**[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、Policy Object Manager　（290 ページ）を開きます。

ステップ 2　コンテンツ テーブルからオブジェクト タイプを選択します。

ステップ 3　削除するオブジェクトを右クリックして [オブジェクトの削除（Delete Object）] を選択するか、オブジェクトを選択して [オブジェクトの削除（Delete Object）] ボタンをクリックします。削除の確認が求められます。

オブジェクト オーバーライドの管理

ポリシー オブジェクトを作成するときに、オブジェクトの上書きを許可できます。これにより、一般的なポリシーの作成を可能にする汎用オブジェクトを作成できるようになります。個々のデバイスで、ポリシー オブジェクト定義を上書きして、ポリシーがデバイスに適切に適用されるようにします。

Policy Object Manager　（290 ページ）から、上書き可能なポリシー オブジェクトを選択し、そのグローバル オブジェクトに対して定義するデバイス レベルのオーバーライド テーブルを生成できます。オブジェクトを右クリックし、[デバイスのオーバーライドの編集（Edit Device Overrides）] を選択してテーブルを生成します（[Policy Object Overrides] ウィンドウ　（314 ページ）を参照）。

デバイス レベルのオーバーライドは、次の 2 つの場所で作成できます。

- 選択したデバイスの [Device Properties] ウィンドウ。選択したデバイスだけのオーバーライドを作成および管理できます。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集　（312 ページ）を参照してください。

- [Policy Object Manager] ウィンドウ。複数のデバイスのオーバーライドを一度に作成および管理できます。詳細については、複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）を参照してください。

ヒント　デバイス レベルでオブジェクト定義を上書きすると、あとからグローバル レベルでポリシー定義を変更しても、オブジェクトが上書きされたデバイスには影響しません。

次の項では、ポリシー オブジェクト オーバーライドについてより詳細に説明します。

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）
- デバイス レベルのオブジェクト オーバーライドの削除 （315 ページ）
- Cisco Security Manager のオーバーライド可能なオブジェクト （316 ページ）

個々のデバイスのポリシー オブジェクト オーバーライドについて

多くのタイプのポリシーオブジェクトでは、特定のデバイスについてオブジェクトの上書きを許可できます。そのため、ほとんどのデバイスに定義を適用できるオブジェクトを作成し、若干異なる定義を必要とする少数のデバイスについてオブジェクトを変更することが可能です。または、上書きが必要なオブジェクトをすべてのデバイスに対して作成することもできます。これにより、すべてのデバイスに対してポリシーを1つ作成できます。オブジェクト オーバーライドでは、デバイス全体で使用する共有ポリシーの小さなセットを作成し、個々のデバイスに対して必要に応じてポリシーを変更することが可能です。

たとえば、社内のさまざまな部門へのICMPトラフィックを拒否する場合があります。それぞれの部門は、異なるネットワークに接続されています。これを実行するには、Departmental Network という名前のネットワーク/ホスト オブジェクトを含むルールを使用して、アクセス ルール ファイアウォール ポリシーを定義します。このオブジェクトのデバイス オーバーライドを許可することによって、関連する各デバイスで、デバイスが接続されている実際のネットワークを指定するオーバーライドを作成できます。

デバイスレベルのオブジェクトオーバーライドは、VPNポリシーの定義にグローバルオブジェクトが含まれている場合に特に重要です。VPN ポリシーは VPN トポロジ内のすべてのデバイスに適用されます。たとえば、サイト間 VPN で PKI ポリシーを定義するときに、PKI 登録オブジェクトを選択します。VPNのハブでスポークとは異なるCAサーバが使用されている場合は、デバイスレベルのオーバーライドを使用して、ハブで使用されているCAサーバを指定する必要があります。PKI ポリシーは 1 つの PKI 登録オブジェクトを参照しますが、このオブジェクトによって表される実際のCAサーバは、定義するデバイスレベルのオーバーライドに基づいて、ハブごとに異なります。

オブジェクトがオーバーライド可能かどうかは、 Policy Object Manager （290 ページ）のオブジェクトテーブルの [オーバーライド（Overridable）] 列ですぐに確認できます。緑色のチェックマークは、オブジェクトに対してオーバーライドを作成できることを示します。カラムが存在することは、オブジェクト タイプでオーバーライドが許可されていることを示します。

関連項目

- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）
- デバイス レベルのオブジェクト オーバーライドの削除 （315 ページ）

ポリシー オブジェクトの上書きの許可

オブジェクトのオーバーライドを作成するには、オブジェクトでオーバーライドが許可されている必要があります。すべてのオブジェクト タイプでオーバーライドが許可されているわけではありません。

オーバーライドを許可する場合、オブジェクトを定義するときに [デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択し、オーバーライド許可としてオブジェクトを定義します。このオプションを選択したあと、オーバーライドを定義する前に、[OK] をクリックしてオブジェクトを保存する必要があります。オブジェクトの作成の詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。

インベントリに追加するデバイスでポリシーを検出するときに、既存のオブジェクトに対してデバイス レベルのオーバーライドを作成するように Security Manager を設定することもできます。検出中に、検出されたポリシーに既存のオブジェクトが該当するが、完全には適合しないと Security Manager が判断した場合、オブジェクトは使用されますが、差異を表すためにデバイス レベルのオーバーライドが作成されます。たとえば、Security Manager で、ACL ポリシー オブジェクトと同じ名前の ACL を持つデバイスでポリシー検出を実行すると、検出されたポリシー オブジェクトの名前が再利用されますが、オブジェクトに対してデバイス レベルのオーバーライドが作成されます。検出中にデバイス レベルのオーバーライドを許可しない場合、名前に番号が付加されて新しいポリシー オブジェクトが作成されます。これがデフォルトです。

検出中にデバイスのオーバーライドを許可するように Security Manager を設定するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [検出（Discovery）] を選択し、[検出されたポリシーオブジェクトに対するデバイスのオーバーライドを許可（Allow Device Override for Discovered Policy Objects）] を選択します。

（注） 検出中に特定のポリシーオブジェクトがデバイス レベルのオーバーライドに再利用されるようにするには、ポリシー検出の前に、Policy Object Manager で、該当するポリシーオブジェクトに対して [デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] チェックボックスがオンになっていることを確認します。

関連項目

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）
- デバイス レベルのオブジェクト オーバーライドの削除 （315 ページ）

単一デバイスのオブジェクト オーバーライドの作成または編集

[Device Properties] ウィンドウから、デバイス レベルのオブジェクト オーバーライドを作成または編集できます。

オーバーライドによって、選択したデバイスだけに影響するグローバル オブジェクトの定義が指定されます。たとえば、あるデバイスについて、他のデバイスとは異なる AAA サーバ グループを表すように、AAA サーバ グループ オブジェクトの定義を上書きできます。

関連項目

- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）
- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- デバイス レベルのオブジェクト オーバーライドの削除 （315 ページ）

ステップ 1 （デバイス ビュー）デバイス セレクタでデバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。

ステップ 2 上書きするオブジェクト タイプを [ポリシー オブジェクトの上書き（Policy Object Overrides）] フォルダから選択します。

デバイス レベルで上書き可能な、選択したタイプのすべてのオブジェクトがテーブルに表示されます。オブジェクトにデバイスに対するオーバーライドがすでに定義されている場合、[値がオーバーライドされているか（Value Overridden?）] カラムにチェックマークが付けられます。

ステップ 3 オーバーライドを変更するオブジェクトを選択し、次のいずれかを実行します。

- [オーバーライドの作成（Create Override）] ボタンをクリックするか、右クリックして [オーバーライドの作成（Create Override）] を選択します。
- [オーバーライドの編集（Edit Override）] ボタンをクリックするか、右クリックして [オーバーライドの編集（Edit Override）] を選択します。

そのタイプのオブジェクトを定義するためのダイアログ ボックスが表示され、現在のプロパティ（グローバル プロパティまたはローカル オーバーライド）が示されます。

ステップ 4 オブジェクトの定義を変更し、[OK] をクリックして、デバイスレベルのオーバーライドを保存します。[Device Properties] ウィンドウで、[Value Overridden?] カラムに緑色のチェック マークが表示されます。

複数デバイスのオブジェクト オーバーライドの一括での作成または編集

[Policy Object Manager] ウィンドウから、デバイスレベルのオブジェクト オーバーライドを作成または編集できます。

この方式では、複数のデバイスに対してオブジェクト オーバーライドを同時に作成できます。同じ VPN トポロジに参加している複数のデバイスのオーバーライドを作成するときに特に役立ちます。たとえば、VPN のある部分に配置されたスポークが、VPN の別の部分に配置されたスポークとは異なる CA サーバを使用する場合、これらのデバイスのサーバを定義する PKI 登録オブジェクトを上書きできます。これは、デバイス ビューから各デバイスを個別に選択し、[Device Properties] ウィンドウでオーバーライドを定義するよりも便利な方式です。

関連項目

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）
- デバイスレベルのオブジェクト オーバーライドの削除 （315 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して、 Policy Object Manager （290 ページ）を開きます。

ステップ 2 上書きするオブジェクト タイプをコンテンツ テーブルから選択し、上書きするオブジェクトを選択します。

ヒント すべてのオブジェクト タイプでオーバーライドが許可されているわけではなく、すべてのオブジェクトが上書き可能として定義されているわけではありません。[Overridable] カラムの緑色のチェックマークを確認してください。オブジェクト タイプでオーバーライドが許可されているが、このオブジェクトにチェックマークがない場合は、オブジェクトのオーバーライドを許可するようにオブジェクトを編集します（ポリシー オブジェクトの上書きの許可 （311 ページ）を参照）。

ステップ 3 チェックマークをダブルクリックするか、オブジェクトを右クリックして[デバイスオーバーライドの編集（Edit Device Overrides）] を選択し、 [Policy Object Overrides] ウィンドウ （314 ページ）を開きます。このウィンドウには、オブジェクトに対してオーバーライドが定義されている各デバイスを一覧表示するテーブルがあります。

ヒント オーバーライド可能なオブジェクトを編集し、[オーバーライド（Overrides）] フィールドの横の [編集（Edit）] をクリックすることもできます。

ステップ 4 次のいずれかを実行します。

- オーバーライドを追加するには、[オーバーライドの作成（Create Override）] ボタンをクリックし、オーバーライドを適用するデバイスを選択して、オーバーライドを定義します。

オーバーライドを作成および編集するためのダイアログボックスは、オブジェクトの作成に使用されるものと同じです。[Help] ボタンをクリックすると、オブジェクトのタイプに関する情報が表示されます。

作成したオーバーライドは、オブジェクトを使用するデバイス上のすべてのポリシーに適用されます。あるポリシーについてオブジェクトをオーバーライドし、別のポリシーについてはオーバーライドしない、という処理は不可能です。

- オーバーライドを編集するには、オーバーライドを選択し、[オーバーライドの編集（Edit Override）] ボタンをクリックします。

[Policy Object Overrides] ウィンドウ

[Policy Object Overrides] ウィンドウを使用して、選択したオブジェクトに対して定義されているすべてのデバイスレベルのオーバーライドのリストを表示します。テーブルに表示されるコンテンツはオブジェクトのタイプによって異なりますが、デバイス名、デバイスの説明、およびカテゴリは常に含まれます。オーバーライドなどのオブジェクトのコンテンツが表示される場合もあります。

- オーバーライドを追加するには、[オーバーライドの作成（Create Override）] ボタンをクリックします。[デバイスのオーバーライドの作成（Create Overrides for Device）] ウィンドウで、使用可能リストからデバイスを選択し、[>>] をクリックして選択済みリストに移動します。[OK] をクリックすると、オーバーライドを定義するためのダイアログボックスが表示されます。オーバーライドは新しく選択したすべてのデバイスに適用されます（グレーになっているデバイスのオーバーライドは変更されません）。

（注） 使用可能なデバイスのリストには、オブジェクトに対してオーバーライドがまだ定義されていないデバイスが表示されます。オーバーライドを持つデバイスは、選択済みのデバイスのリストにグレーで表示されます。

オーバーライドを作成および編集するためのダイアログボックスは、オブジェクトの作成に使用されるものと同じです。[Help] ボタンをクリックすると、オブジェクトのタイプに関する情報が表示されます。

作成したオーバーライドは、オブジェクトを使用するデバイス上のすべてのポリシーに適用されます。あるポリシーについてオブジェクトをオーバーライドし、別のポリシーについてはオーバーライドしない、という処理は不可能です。

- オーバーライドを編集するには、オーバーライドを選択し、[オーバーライドの編集（Edit Override）] ボタンをクリックします。
- オーバーライドを削除するには、オーバーライドを選択し、[オーバーライドの削除（Delete Override）] ボタンをクリックします。

オーバーライドの削除によって、オブジェクトの削除またはデバイス割り当てからのオブジェクトの削除は行われません。オーバーライドを削除すると、オブジェクトを使用するデバイスのポリシーでは、オブジェクトのグローバル定義の使用が開始されます。これにより、ポリシーの意味が変わります。

ヒント　選択したデバイスの [Device Properties] ウィンドウから、デバイスレベルのオーバーライドを作成および編集することもできます。[Device Properties] ウィンドウを使用すると、単一デバイスによって使用されているすべてのオブジェクトのオーバーライドの管理が簡単になります。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）を参照してください。

ナビゲーション パス

Policy Object Manager （290 ページ） を開きます。上書き可能なオブジェクトタイプ（オブジェクトページに [オーバーライド（Overrides）] というカラムがある）を選択し、次のいずれかを実行します。

- [オーバーライド（Overrides）] カラムの緑色のチェックマークをダブルクリックします。
- オブジェクトを右クリックし、[デバイスのオーバーライドの編集（Edit Device Overrides）] を選択します。
- 上書き可能なオブジェクトを編集し、[オーバーライド（Overrides）] フィールドの横の [編集（Edit）] をクリックします。

関連項目

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）
- デバイスレベルのオブジェクト オーバーライドの削除 （315 ページ）
- テーブルのフィルタリング （64 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

デバイスレベルのオブジェクト オーバーライドの削除

デバイスレベルのオブジェクト オーバーライドを削除すると、オブジェクトのグローバル定義が、選択したデバイスに復元されます。オーバーライドは、[Device Properties] ウィンドウまたは [Policy Object Manager] ウィンドウから削除できます。

- デバイスビューからのオーバーライドの削除：デバイスを右クリックし、[デバイスプロパティ（Device Properties）] を選択し、[ポリシーオブジェクトオーバーライド（Policy

Object Overrides）] フォルダからオブジェクトタイプを選択します。削除するオーバーライドを選択し、[オーバーライドの削除（Delete Override）] をクリックします。

- Policy Object Manager からのオーバーライドの削除：コンテンツテーブルからオブジェクトタイプを選択し、オブジェクトを右クリックして [デバイスのオーバーライドの編集（Edit Device Overrides）] を選択します。削除するオーバーライドを選択し、[オーバーライドの削除（Delete Override）] をクリックします。

関連項目

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）
- ポリシー オブジェクト オーバーライドのページ （154 ページ）
- [Policy Object Overrides] ウィンドウ （314 ページ）

Cisco Security Manager のオーバーライド可能なオブジェクト

Security Manager では、次のオブジェクトをオーバーライドできます。

- **VPN オブジェクト**
  - AAA サーバーグループ
  - PKI 登録 （CA サーバー）
  - WINS Server List
  - SSL VPN カスタマイゼーション
  - SAML ID プロバイダー
  - Web ACL
  - Port Forwarding List
  - ブックマーク
  - スマートトンネルリスト
  - スマート トンネル ネットワーク リスト
  - スマートトンネル自動サインオンリスト
  - シングルサインオンサーバー
  - 参照 ID
- **ファイアウォールオブジェクト**
  - アイデンティティ ユーザー グループ
  - Networks/Hosts

- Port Lists
- セキュリティ グループ（Security Group）
- サービス
- アクセスコントロールリスト（拡張、標準、Web、統合）
- AS パス
- BFD テンプレート（BFD Template）
- コミュニティ リスト（Community List）
- 資格情報
- アイデンティティポリシー（IOS）
- アイデンティティ ユーザー グループ
- Interface Roles
- LDAP 属性マップ
- LDAP 属性マップ（IOS）
- ポリシー リスト
- プレフィックス リスト
- プレフィックスリスト IPV6
- Risk Rating
- ルート マップ
- セキュリティ グループ（Security Group）
- テキスト オブジェクト
- TLS プロキシ
- プールオブジェクト（DHCP V6、IPV4 プール、IPV6 プール、MAC アドレスプール、NET プール）
- マップ（AVP、正規表現グループ、正規表現、TCP マップ）
- クラスマップ：検査（AOL、DCE/RPC、DIAMETER、DNS、eDonkey、FastTrack、FTP、GunTella、H.323（ASA/PIX/FWSM）、H.323（IOS）、HTTP（ASA/PIX/FWSM）、HTTP（IOS）、ICQ、IM、IMAP、Kazaa2、MSN メッセンジャー、POP3、Scansafe、SIP（ASA/PIX/FWSM）、SIP（IOS）、SMTP、SUN RPC、Windows Messenger、Yahoo Messenger）
- クラスマップ：Web フィルタ（ローカル、N2H2、トレンド、Websense）
- パラメータマップ：検査（検査パラメータ、プロトコル情報パラメータ）

- パラメータマップ：Web フィルタ（Loal、N2H2、傾向、URL フィルタ、URLF Glob パラメータ、Websense）
- ポリシーマップ：検査（DCE/RPC、DIAMETER、DNS、ESMTP、FTP、GTP、H.323（ASA/PIX/FWSM）、H.323（IOS）、HTTP ASA7.1.x/PIX7.1.x/ FWSM3.x/IOS）、HTTP（ASA7.2 以降/PIX7.2 以降）、HTTP（ゾーンベースの IOS）、IM（ASA7.2 以降/PIX7.2 以降）、IM（IOS）、IM（ゾーンベースのIOS）、IMAP、IP オプション、IPSec パススルー、IPV6、LISP、M3UA、NetBIOS、P2P、POP3、Scansafe、Sctp、SIP（ASA/PIX/FWSM）、SIP（IOS）、Skinny、SMTP、SNMP、SUN RPC）
- ポリシーマップ：Web フィルタ（Web フィルタ）

ポリシー オブジェクトのインポートおよびエクスポート

Security Manager には Perl スクリプトが含まれており、このスクリプトを使用して、ネットワーク/ホスト オブジェクト、サービス オブジェクト、およびポート リスト ポリシー オブジェクトを別の Security Manager サーバにインポートできるように、エクスポートできます。この情報には、ポリシー オブジェクトのデバイス レベルのオーバーライドが含まれています。

（注） コマンドは、IPv4 アドレスのみを含むネットワーク/ホスト オブジェクトで機能します。コマンドを使用して、ネットワーク/ホスト IPv6 オブジェクトをインポートすることはできません。

インポート可能な CSV ファイルを手動で作成することもできます。たとえば、ネットワークへのエントリを拒否するネットワークまたはホストを識別する IP アドレスのリストを取得できます。Policy Object Manager でオブジェクトを手動で作成するよりも簡単な場合は、リストを 1 つ以上のネットワーク/ホスト オブジェクトとしてバルクロードする CSV ファイルを作成できます。

ヒント このコマンドを使用する以外に、他の機能を使用して、共有ポリシーに割り当てられたポリシー オブジェクトまたはローカル デバイス ポリシーで設定されたポリシー オブジェクトをエクスポートおよびインポートできます。詳細については、トピックSecurity Manager クライアントからのデバイス インベントリのエクスポート（605 ページ）、共有ポリシーのエクスポート（612 ページ）、およびポリシーまたはデバイスのインポート（615 ページ）を参照してください。

Perl コマンドは $NMSROOT\bin（通常は C:\Program Files\CSCSpx\bin）にあります。コマンドの構文は次のとおりです。

perl [*path*]**PolicyObjectImportExport.pl -u** *username* **-p** *password* **-o {import | export}** [**-a** *activity*] **-t** *object_type* **-f** *filename* [**-c {true | false}**] [**-d {true | false}**] [**-e {true | false}**] [**-g {true | false}**] [**-h**]

構文

perl [*path*] **PolicyObjectImportExport.pl**	Perl スクリプト コマンド。システム パス変数内に PolicyObjectImportExport.pl ファイルへのパスが定義されていない場合は、そのパスを追加します。 ヒント 「perl」コマンドを含めるのを忘れた場合、システムは入力を受け入れますが、何も行われず、エラーに関するフィードバックも提供しません。Ctrl+Z を使用して、コマンドプロンプトに戻ります。
-u *username*	Security Manager のユーザ名。エクスポートされるデータは、このユーザに割り当てられた権限によって制限されます。ポリシー オブジェクトのインポートまたはエクスポートには、ユーザに Modify Objects 権限が必要であり、デバイス レベルのオーバーライドのインポートまたはエクスポートには、さらに Modify Devices 権限が必要です。 Workflow 以外のモードでオブジェクトをインポートする場合は、Submit および Approve 権限も必要です。
-p *password*	ユーザーのパスワード。
-o {import | export}	実行する操作のタイプ。ポリシー オブジェクトを既存のファイルからインポートするか、ポリシー オブジェクトを CSV ファイルにエクスポートするかです。コミットされたオブジェクトだけがエクスポートされます。
-a *activity*	（オプション）Workflow アクティビティの名前。名前を指定しない場合、新しいアクティビティは username_time という名前で作成されます。
-t *object_type*	オブジェクト タイプ。次のいずれかです。 • network：ネットワーク/ホスト オブジェクトの場合。 • service：サービス オブジェクトの場合。 • portlist：ポートリストオブジェクトの場合。
-f *filename*	CSV ファイルの名前。エクスポート時にファイルが存在する場合は、上書きされます。

-c {true | false}	（オプション）オブジェクトをインポートするときに、ポリシー オブジェクトの競合検出をイネーブルにするかどうか。 • false：既存のオブジェクトに同じコンテンツがある場合でも、オブジェクトはインポートされます。 • true：インポートされるオブジェクトと同じコンテンツが既存のオブジェクトにある場合、インポートされるオブジェクトはスキップされます。[Policy Objects] ページ（732 ページ）の [冗長オブジェクトが検出された場合（When Redundant Objects Detected）] オプションで、[適用（Enforce）] を選択する必要もあります。
-d {true | false}	（オプション）インポートまたはエクスポート操作中にデバイス レベルのポリシー オブジェクト オーバーライドを処理する方法。 • true：グローバルに定義されたすべてのオブジェクトおよびオブジェクトのデバイス レベルのすべてのオーバーライドを含めます。 • false：ポリシー オブジェクトのグローバル定義だけを含めます。デバイス レベルのポリシー オブジェクト オーバーライド情報は含めません。これがデフォルトです。
-e {true | false}	（オプション）サービスオブジェクトおよびサービス グループ オブジェクトのポートリストオブジェクトを「フラット化」するかどうか。 • true：サービスオブジェクトおよびサービス グループ オブジェクトで見つかったポートリストオブジェクトの名前は、リストの実際のポートに置き換えられます。つまり、2 つのオブジェクト（ポートリストとサービス、またはポートリストとサービスグループ）は、単一のサービスまたはサービスグループに「フラット化」されます。 ポートリストオブジェクトは、Security Manager でポート定義のセットをグループ化するために使用され、サービスおよびサービス グループ オブジェクトを定義するときに使用されます。ただし、PRSM ではポートリストオブジェクトはサポートされていません。 • false：サービス内のポートリストオブジェクトおよびサービス グループ オブジェクトはフラット化されません。これがデフォルトです。

-g {true | false}	（オプション）CSV ファイルにオブジェクトタイプとオブジェクトグループタイプを含めるかどうか。 • true：ファイルの最後の列は[タイプ（Type）]で、「サービス」または「ネットワーク」を示します。 • false：[タイプ（Type）]列は含まれません。これがデフォルトです。
-h	（オプション）コマンドラインのヘルプを表示します。このオプションを指定すると、他のすべてのオプションは無視されます。

ポリシー オブジェクトのインポート

オブジェクトをインポートするときに、オブジェクトが別のオブジェクトを参照している場合は、そのオブジェクトが Security Manager ですでに定義されている必要があります。または、インポートする同じ CSV ファイル内で定義されている必要があります。そのオブジェクトが同じ CSV ファイル内にある場合は、それを参照するオブジェクトよりも前にある必要があります（Security Manager では、オブジェクトはエクスポート時に必要に応じて自動的にソートされます）。

インポートするポリシー オブジェクトと同じ名前のポリシー オブジェクトが Security Manager 内にすでに存在する場合、オブジェクトはスキップされてインポートされません。名前の競合は、別のユーザがオブジェクトを作成したが、まだ公開用にコミットしていない場合にも発生する可能性があります。そのため、競合しているオブジェクトを参照できない場合があります。Security Manager では、新しいオブジェクトだけが作成され、既存のオブジェクトは更新されません。-c オプションを使用して、既存のオブジェクトと同じコンテンツの新しいオブジェクトを作成できるかどうかを指定します。

コマンドを実行したときに、ファイル内にエラーがあると、影響を受けるオブジェクトだけがインポートされません。これらの問題は発生時にエラー メッセージによって示され、Security Manager ではファイル内のすべてのレコードの評価が続行されます。正しく定義されたすべてのポリシーオブジェクトはインポートされ、エラーがあるオブジェクトはスキップされます。インポートされなかったポリシー オブジェクトの合計数と名前が出力画面に表示されます。

インポート コマンドの完了後、追加のアクションは、使用している Workflow モードによって異なります。

- Workflow モード：同じユーザ名とパスワードを使用して Security Manager にログインし、インポート中に指定したアクティビティを送信する必要があります。変更を有効にするには、アクティビティが送信されて承認される必要があります。
- Workflow 以外のモード：インポートされたオブジェクトは自動的に送信されて承認されます。アクションは必要ありません。ただし、入力したユーザ名に Submit および Approve 権限がない場合はエラーが表示され、インポート操作は失敗します。

CSV ファイル形式

1 つのファイル内のすべてのオブジェクトは、同じポリシー オブジェクト タイプになります。ファイルは、標準的な Comma-Separated Values（CSV; カンマ区切り値）形式です。最初の行はカラムの見出しです。各行は、1 つのポリシー オブジェクトを表します。カラムは、左から右へという順で、次のとおりです。

- [名前（Name）]：（必須）オブジェクトの名前。
- [Node]：ポリシー オブジェクトのオーバーライドが定義されているデバイスの表示名。ポリシー オブジェクトがグローバル レベルで定義されている場合、このフィールドは空です。オブジェクトをインポートするときに、表示名が Security Manager インベントリにすでにあるデバイスと一致しない場合、オブジェクトはスキップされてインポートされません。
- [Description]：オブジェクトの説明（ある場合）。
- [Category]：オブジェクトのカテゴリ ID（ある場合）。カテゴリ ID は 10 ～ 19 です。
- [Allow Override]：オブジェクトが上書き可能かどうか。ポリシー オブジェクトがデバイス レベルで上書き可能な場合は True。上書き不可の場合は False（または空のフィールド）。
- [Group]：このポリシー オブジェクトによって参照される、同じタイプの他のポリシー オブジェクトの名前。複数のオブジェクトがある場合は、カンマで区切られます。たとえば、ネットワーク構築ブロック Net1 がネットワーク構築ブロック Net2 および Net3 を参照しています。Net1 の [グループ（Group）] フィールドの値は、「Net2,Net3」になります。
- [Data]：オブジェクトのコンテンツ。
- [Subtype]：ネットワーク/ホスト オブジェクトおよびサービス オブジェクトのオブジェクト サブタイプ（ある場合）。ネットワーク/ホストオブジェクトタイプおよびサービスオブジェクトタイプの説明については、ネットワーク/ホストオブジェクトについて （391 ページ）およびサービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。値は以下のとおりです。
  - ブランク（スペース）：オブジェクトはグループ オブジェクト（ネットワーク/ホストまたはサービス）です。
  - NH：（ネットワーク/ホストオブジェクトのみ）単一ホストのネットワーク/ホストオブジェクト。
  - NF：（ネットワーク/ホストオブジェクトのみ）単一の完全修飾ドメイン名（FQDN）ネットワーク/ホストオブジェクト。
  - NN：（ネットワーク/ホストオブジェクトのみ）単一のネットワークアドレスのネットワーク/ホストオブジェクト。
  - NR：（ネットワーク/ホストオブジェクトのみ）単一のアドレス範囲のネットワーク/ホストオブジェクト。
  - SO：（サービスオブジェクトのみ）単一サービスのサービスオブジェクト。

- [タイプ（Type）]：このエントリによって表されるオブジェクトのタイプ（「ネットワーク」または「サービス」）。

特定のフィールドに値がない場合、そのフィールドは出力でブランクになります。フィールドに複数の値がある場合、フィールドは二重引用符で囲まれます。

AAAサーバおよびサーバグループオブジェクトについて

AAA サーバ オブジェクトを使用して、ネットワーク内で使用される AAA サーバを識別します。AAA によって、デバイスでは次に示すように、ユーザがだれか（認証）、ユーザが何を許可されているか（認可）、ユーザが実際に何をしたか（アカウンティング）を判別できます。

- 認証：認証とは、ネットワークおよびネットワーク サービスへのアクセスを許可される前に、ユーザが認証される方法です。有効なユーザー クレデンシャル（通常は、ユーザー名とパスワード）を要求することで、アクセスが制御されます。すべての認証方式（ローカル認証、回線パスワード認証、およびイネーブル認証を除く）は、AAA を使用して定義する必要があります。認証だけで使用することも、認可およびアカウンティングとともに使用することもできます。
- 認可：認証の完了後、認可によって、認証済みの各ユーザが使用できるサービスおよびコマンドが制御されます。認可は、ユーザが実行を認可されていることを示す属性のセットをアセンブルすることによって機能します。これらの属性は、データベースに含まれている特定のユーザの情報と比較され、結果は、ユーザの実際の機能と制約を決定するために AAA に返されます。データベースは、アクセス サーバまたはルータにローカルに配置するか、RADIUS または TACACS+ セキュリティ サーバでリモートでホスティングできます。認可を使用しない場合は、認証が単独で、認証済みのすべてのユーザに対してサービスへの同じアクセスを提供します。認可は認証とともに使用する必要があります。
- アカウンティング：アカウンティングは、ユーザがアクセスしているサービス、およびユーザが消費しているネットワーク リソース量を追跡するために使用されます。AAA アカウンティングをアクティブにすると、ネットワーク アクセス サーバによって、ユーザ アクティビティがアカウンティング レコードの形式で RADIUS または TACACS+ セキュリティ サーバ（実装したセキュリティ方式によって異なる）にレポートされます。アカウンティング情報には、セッションの開始時刻と停止時刻、ユーザー名、セッションごとのデバイスを通過したバイト数、使用されたサービス、および各セッションの時間が含まれています。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。アカウンティングは、単独で使用するか、認証および認可とともに使用することができます。

AAA によって、アクセル ルール（ACL）だけを使用するよりも、ユーザ アクセスについて高いレベルの保護と制御が提供されます。たとえば、すべての外部ユーザが DMZ ネットワーク上のサーバで Telnet の使用を試行できるアクセス ルールを作成できます。一部のユーザだけが実際にサーバに到達できるようにする場合（さらに、それらのユーザの IP アドレスが常にわかるわけではないため、単純なアクセス ルールを設定できない場合）、認証済みまたは認可済みのユーザだけがネットワーク デバイス（ASA やルータなど）を通過することを AAA が許

可できるようにすることができます。そのため、ユーザはTelnetサーバに到達する前に認証する必要があり、サーバでは Telnet が別のログインを要求することもできます。

AAA サーバ オブジェクトを AAA サーバ グループ オブジェクトにまとめることができます。通常、AAA を必要とするポリシー（Easy VPN、リモート アクセス VPN、Secured Device Provisioning や 802.1x などのルータ プラットフォーム ポリシーなど）は、AAA サーバ グループ オブジェクトを参照します。これらのオブジェクトには、同じプロトコル（RADIUS や TACACS+ など）を使用する複数の AAA サーバが含まれています。AAA サーバ グループとは、ネットワーク セキュリティ ポリシー全体の特定の側面を実施することに焦点を当てた認証サーバの集合のことです。たとえば、内部トラフィック、外部トラフィック、またはリモート ダイヤルイン ユーザの認証専用のサーバや、ファイアウォール デバイスの管理を認可するサーバをグループ化できます。

次の項では、AAA サーバ オブジェクトを操作する方法について説明します。

- サポートされる AAA サーバ タイプ （324 ページ）
- ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）
- 定義済みの AAA 認証サーバ グループ （328 ページ）
- デフォルトの AAA サーバ グループおよび IOS デバイス （329 ページ）
- AAA サーバ オブジェクトの作成 （330 ページ）
- [Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）
- [Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （347 ページ）
- AAA サーバ グループ オブジェクトの作成 （349 ページ）

サポートされる AAA サーバ タイプ

すべてのデバイスに RADIUS プロトコルを使用し、IPS 以外のすべてのデバイスに TACACS+ プロトコルと LDAP プロトコルを使用する AAA サーバを使用できます。ASA、PIX、および FWSM デバイスの場合は、 ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）で説明されているプロトコルを使用することもできます。

- RADIUS：Remote Authentication Dial-In User Service（RADIUS）は、無許可のアクセスに対してネットワークを保護する分散クライアント/サーバーシステムです。シスコの実装では、RADIUS クライアントはシスコ デバイス上で実行され、すべてのユーザ認証およびネットワーク サービス アクセス情報を持つ中央の RADIUS サーバに認証要求を送信します。

RADIUS は、固有のデバイス タイプでサポートされているプロトコルに応じて、他の AAA セキュリティ プロトコル（TACACS+、Kerberos、ローカル ユーザ名検索など）とともに使用できます。RADIUS はすべての Cisco プラットフォームでサポートされますが、RADIUS でサポートされる一部の機能は、指定されたプラットフォームだけで実行されます。

Cisco Security Manager 4.17 以降、IPv6 は RADIUS プロトコルで有効になっています。このサポートは、ASA 9.9.2 以上のデバイスにのみ適用されます。ユーザーは、[AAAサーバーを追加（Add AAA Server）] ダイアログボックスで Radius 認証の IPv6 ホストアドレスを設定できるようになりました（[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）を参照）。サポートされていないデバイスバージョンに対しても、アクティビティの検証が導入されています。

- TACACS+：Terminal Access Controller Access Control System（TACACS+）は、ユーザーによるルータまたはネットワーク アクセス サーバーへのアクセス試行の集中的な確認を可能にするセキュリティアプリケーションです。TACACS+ の目的は、単一の管理サービスから複数のネットワーク アクセス ポイントを管理する方法を提供することです。

TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）で各サービスを独立して提供することが可能です。

- LDAP：Lightweight Directory Access Protocol（LDAP）。LDAP サーバの使用法は、ポリシーごとに固有です。たとえば、ASA でのアイデンティティ ファイアウォール設定、ASA での VPN 設定、IOS デバイスでの ScanSage 設定などです。ASA での LDAP サーバの使用の詳細については、 ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）を参照してください。

関連項目

- ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）
- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ASA、PIX、および FWSM デバイスでのその他の AAA サポート

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

RADIUS および TACACS+ をサポートする以外に、ASA、PIX 7.0+、および FWSM 3.1+ デバイスでは、次のプロトコルを実行する AAA サーバをサポートできます。詳細については、該当するデバイス タイプおよびオペレーティング システム バージョンの設定ガイドで AAA の使用方法の説明を参照してください。

- **Kerberos**：これらのデバイスでは、認証に Kerberos サーバーを使用できます。3DES、DES、および RC4 暗号化タイプがサポートされています。
- **NT**：これらのデバイスでは、NTLMv1 認証に Windows ドメインサーバーを使用できます。

- **SDI サーバー**：RSA Security, Inc. の SecurID サーバーは SDI サーバーと呼ばれます。ユーザが VPN アクセスを確立しようとし、該当するトンネル グループ ポリシーが SDI 認証サーバ グループを指定している場合、ASA デバイスはユーザ名およびワンタイム パスワードを SDI サーバに送信します。デバイスは、サーバからの応答に基づいてユーザ アクセスを付与するか拒否します。SDI のバージョン 5.0 では、単一ノード シークレット ファイル（SECURID）を共有する SDI プライマリ サーバーおよびセカンダリ サーバーの概念が導入されました。その結果、SDI サーバを AAA サーバ オブジェクトとして設定する場合、サーバがバージョン 5.0 かそれよりも前のバージョンかを指定する必要があります。
- **LDAP**：これらのデバイスでは、VPN 認可に Lightweight Directory Access Protocol（LDAP）サーバーを、アイデンティティ対応ファイアウォール ポリシーにユーザ グループ ID を使用できます。これらのデバイスでは LDAP バージョン 3 がサポートされ、任意の v3 または v2 ディレクトリ サーバと互換性があります。ただし、パスワード管理は、Sun Microsystems JAVA System Directory Server および Microsoft Active Directory だけでサポートされています。

その他のタイプの LDAP サーバ（Novell や OpenLDAP など）では、パスワード管理以外のすべての LDAP 機能がサポートされています。したがって、これらのサーバのいずれかを認証用に使用してこれらのデバイスのいずれかにログインしようとし、パスワードが期限切れになっている場合、デバイスでは接続はドロップされ、手動でのパスワードのリセットが必要になります。

LDAP サーバに対して LDAP クライアント（この場合は、ASA、PIX、または FWSM デバイス）を認証するように Simple Authentication and Security Layer（SASL）メカニズムを設定できます。これらのデバイスおよび LDAP サーバでは、複数のメカニズムをサポートできます。両方のメカニズム（MD5 および Kerberos）が使用可能な場合、ASA、PIX、または FWSM デバイスは、より強力なメカニズム（Kerberos）を認証に使用します。

VPN アクセスのユーザ認証が成功し、該当するトンネル グループ ポリシーが LDAP 認証サーバ グループを指定している場合、ASA、PIX、または FWSM デバイスは LDAP サーバを照会し、受け取った認可を VPN セッションに適用します。

- **HTTP-Form**：これらのデバイスでは、WebVPN ユーザだけの Single Sign-On（SSO; シングルサインオン）認証に HTTP Form プロトコルを使用できます。シングル サインオンのサポートによって、WebVPN ユーザはユーザ名とパスワードを 1 回だけ入力して、複数の保護されているサービスおよび Web サーバにアクセスできます。セキュリティ アプライアンスで実行されている WebVPN サーバは、認証サーバに対して、ユーザのプロキシとして機能します。ユーザがログインすると、SSO 認証要求（ユーザ名とパスワードを含む）が WebVPN サーバから認証サーバに HTTPS を使用して送信されます。サーバによって認証要求が承認されると、SSO 認証クッキーが WebVPN サーバに返されます。セキュリティ アプライアンスでは、ユーザに代わってこのクッキーが保持され、SSO サーバによって保護されているドメイン内のセキュア Web サイトに対してユーザを認証するために使用されます。

次の表に、各プロトコルでサポートされている AAA サービスを示します。

表 *44 : ASA*、*PIX*、および *FWSM* デバイスでサポートされている *AAA* サービス

AAA サービス	データベース タイプ							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
認証								
VPN ユーザ	対応	対応	対応	対応	対応	対応	対応	○ 1
ファイアウォール セッション	対応	対応	対応	対応	対応	対応	対応	×
管理者	対応	対応	対応	対応 2	対応	対応	対応	×
許可								
VPN ユーザ	対応	対応	×	×	×	×	対応	×
ファイアウォール セッション	なし	対応 3	対応	×	×	×	×	×
管理者	対応 4	×	対応	×	×	×	×	×
アカウンティング								
VPN 接続	×	対応	対応	×	×	×	×	×
ファイアウォール セッション	×	対応	対応	×	×	×	×	×
管理者	非対応	対応 5	対応	×	×	×	×	×

1. HTTP-Form プロトコルでは、WebVPN ユーザだけの Single Sign-On（SSO; シングル サインオン）認証がサポートされます。2. SDI は、HTTP 管理アクセスについてはサポートされません。3. ファイアウォール セッションの場合、RADIUS 許可はユーザ固有の ACL だけでサポートされます。ユーザ固有の ACL は、RADIUS 認証応答で受信または指定されます。4. ローカル コマンド許可は、特権レベルに限りサポートされます。5. コマンド アカウンティングは、TACACS+ でのみ使用できます。

関連項目

- サポートされる AAA サーバ タイプ （324 ページ）
- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

定義済みの AAA 認証サーバ グループ

特定の AAA サーバを指定しないで認証方式を定義するいくつかの定義済みの AAA サーバ グループがあります。IPSec プロポーザルなどのポリシーでは、これらの定義済みのサーバ グループを使用して、実行する AAA 認証のタイプとそれらの実行順序を定義できます。

以下の表に、定義済みの AAA 認証サーバーグループを示します。

表 *45*：定義済みの *AAA* 認証サーバ グループ

名前	説明
有効化（Enable）	デバイス上で定義されたイネーブル パスワードを認証に使用します。
KRB5 KRB5-Telnet	Kerberos 5 を認証に使用します。Telnet を使用して接続する場合は、KRB5-Telnet を使用します。 Cisco IOS ルータの場合、Kerberos 5 クライアント設定は、このプロトコルをサポートする IOS ソフトウェア バージョンを実行している選択済みプラットフォームだけで使用できます。サーバ設定はサポートされていません。デバイスに Advanced シリーズ フィーチャ セット（k9 暗号イメージ）が含まれている必要があります。
if-authenticated	if-authenticated 方式を使用します。この方式では、認証済みの場合に、ユーザは要求した機能にアクセスできます。
回線（Line）	デバイス上で定義された回線パスワードを認証に使用します。
ローカル（Local） local-case	（デバイス上で定義された）ローカル ユーザ名データベースを認証に使用します。ログインで大文字と小文字を区別する場合に、local-case を使用します。
なし（None）	認証を使用しません。
RADIUS TACACS+	RADIUS または TACACS+ 認証を使用します（Cisco IOS ルータには適用されません）。 これらの AAA サーバ グループには AAA サーバは含まれていません。ポリシーを定義するときにこれらのいずれかを使用するには、デバイス レベルのオーバーライドを作成し、グループに関連付ける AAA サーバを定義する必要があります。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）を参照してください。

関連項目

- AAA サーバ グループ オブジェクトの作成 （349 ページ）
- デフォルトの AAA サーバ グループおよび IOS デバイス （329 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

デフォルトの AAA サーバ グループおよび IOS デバイス

IOS ソフトウェアを使用すると、AAA サーバ グループのメンバーとして、または個別のサーバとして、AAA サーバを定義できます。ただし、Security Manager では、すべての AAA サーバは AAA サーバ グループに属している必要があります。

したがって、AAA サーバ グループに属していない個別の AAA サーバがデバイス設定に含まれている IOS デバイスを検出した場合、それらのサーバを含めるために次のサーバ グループが Security Manager によって作成されます。

- RADIUS の場合：CSM-rad-grp
- TACACS+ の場合：CSM-tac-grp

これらの特別な AAA サーバ グループは、どちらも、Policy Object Manager で、これらのプロトコルのデフォルト グループとしてマークされます。これは、[このグループをデフォルトAAA サーバーグループとする（Make this Group the Default AAA Server Group）] チェックボックスで指定されます。

これらのグループは、Security Manager による管理のためだけに作成されます。展開中に、これらの特別なグループ内の AAA サーバは、グループの一部としてではなく、個別のサーバーとして IOS デバイスに展開されます。

独自のデフォルト グループを作成することもできます。デフォルト グループはほとんどの場合に使用できますが、同じプロトコルを使用する複数の AAA サーバ グループを設定する必要がある場合を除きます。たとえば、1 つのグループを認証用に使用し、もう 1 つのグループを認可用に使用できるように、複数の RADIUS グループを定義する場合があります。サービス プロバイダーは、VRF を使用するときに、カスタマーを分離するために同じプロトコルで複数のグループを定義する場合があります。

（注） PIX/ASA/FWSM デバイスに対して定義されるポリシーでこれらのデフォルト AAA サーバ グループのいずれかを使用する場合、AAA サーバは、個別のサーバとしてではなく、グループとしてそのデバイスに展開されます。これは、PIX/ASA/FWSM デバイス上のすべての AAA サーバは、AAA サーバ グループに属している必要があるためです。

注意 これらのデフォルトAAAサーバ グループをポリシー定義で使用する場合は注意してください。各 AAA サーバーグループに対して一度、すべての個別の AAA サーバーに対して一度定義できる特定のコマンドがあります（たとえば、**ip radius** および **ip tacacs**。これらは、[AAAサーバー（AAA Server）] ダイアログボックスの [インターフェイス（Interface）] フィールドを使用して定義されます）。デフォルトグループ内の AAA サーバーは IOS デバイスに個別のサーバーとして展開されるため、Security Manager によって管理されていないサーバを含む、デバイス上で設定されたすべての個別の AAA サーバーの **ip radius** または **ip tacacs** 設定を間違って変更する可能性があります。（その場合の設定は変更されないままとなります）

関連項目

- 定義済みの AAA 認証サーバ グループ （328 ページ）
- AAA サーバ グループ オブジェクトの作成 （349 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

AAA サーバ オブジェクトの作成

AAA サーバ オブジェクトを作成し、AAA ルール、Easy VPN、802.1x などのポリシーによって参照される AAA サーバ グループ オブジェクトに読み込むことができます。IPS デバイス上の AAA ポリシーなどでは、AAA サーバ オブジェクトがポリシーによって直接使用される場合があります。

AAA サーバーオブジェクトを作成する場合、外部 AAA サーバの IP アドレスまたは DNS 名、およびサーバーによって使用されるプロトコルを指定する必要があります。必要な他の設定はプロトコルによって異なります。

（注） PIX/ASA/FWSM デバイスでは、ポリシーによって参照されていないデバイス設定内の AAA オブジェクトは、次の展開中にデバイスから削除されます。ただし、RADIUS および TACACS+ という名前の定義済みの AAA オブジェクトは、ポリシーによって参照されていない場合でも、PIX 6.3 デバイスから削除されません。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）
- サポートされる AAA サーバ タイプ （324 ページ）
- ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [AAAサーバー（AAA Servers）] を選択します。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）を開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 AAA サーバを識別します。

- [Host] フィールドに、AAA サーバの IP アドレスか、ASA または PIX 7.2 以降のデバイスの場合は、AAA サーバのホスト名を入力します。ホスト IP アドレスを含むネットワーク/ホストオブジェクトの名前を入力するか、または [選択（Select）] をクリックしてオブジェクトを選択することもできます。

- 任意で、[Interfaces] フィールドに、すべての発信 RADIUS または TACACS+ パケットに対して、その IP アドレスが使用されるインターフェイスまたはインターフェイス ロール（デバイスで単一のインターフェイス名に解決される必要があります）の名前を入力します。IPS デバイス上で使用されているオブジェクトのインターフェイスを指定しないでください。
- 任意で、AAA サーバを応答なしと見なすまでの待機時間を入力します。

ステップ 6 AAAサーバによって使用されるプロトコルを選択し、プロトコル固有のプロパティを設定します。RADIUS はすべてのデバイス タイプで使用でき、TACACS+ は IPS デバイス以外のすべてのデバイス タイプで使用できます。Kerberos、LDAP、NT、SDI、およびHTTP-FORMプロトコルは、ASA、PIX 7.x+、およびFWSM 3.1+ デバイスだけで使用できます。

プロパティの詳細については、次の項を参照してください。

- RADIUS： [AAA Server] ダイアログボックス - RADIUS 設定 （334 ページ）を参照してください。
- TACACS+： [AAA Server] ダイアログボックス - TACACS+ 設定 （337 ページ）を参照してください。
- Kerberos： [AAA Server] ダイアログボックス - Kerberos 設定 （338 ページ）を参照してください。
- LDAP： [AAA Server] ダイアログボックス - LDAP 設定 （339 ページ）を参照してください。
- NT： [AAA Server] ダイアログボックス - NT 設定 （343 ページ）を参照してください。
- SDI： [AAA Server] ダイアログボックス - SDI 設定 （344 ページ）を参照してください。
- HTTP-FORM： [AAA Server] ダイアログボックス - HTTP-FORM 設定 （345 ページ）を参照してください。

ステップ 7 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

[Add AAA Server]/[Edit AAA Server] ダイアログボックス

[Add AAA Server]/[Edit AAA Server] ダイアログボックスを使用して、AAA サーバ オブジェクトを作成、コピー、および編集します。これらのオブジェクトは AAA サーバ グループ オブジェクトにまとめられ、さまざまな AAA ポリシーを定義するときに、これらのオブジェクトによって使用するAAAサーバが識別されます。これらのオブジェクトは、AAA ポリシーで直接使用される場合があります。

使用できるプロトコルの説明については、サポートされる AAA サーバ タイプ （324 ページ）およびASA、PIX、およびFWSM デバイスでのその他の AAA サポート （325 ページ）を参照してください。

（注） オブジェクトがすでにAAAサーバグループに含まれている場合、プロトコルは編集できません。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]を選択し、オブジェクトタイプセレクタから[AAAサーバー（AAA Servers）]を選択します。作業領域内を右クリックして[新規オブジェクト（New Object）]を選択するか、行を右クリックして[オブジェクトの編集（Edit Object）]を選択します。

関連項目

- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- AAA サーバ オブジェクトの作成 （330 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *46 : [AAA Server]* ダイアログボックス - 一般設定

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
ホスト（Host）	認証要求の送信先の AAA サーバのアドレス。次のいずれかを指定します。 • IP アドレス：AAA サーバーの IPv4 または IPv6 アドレス。ホスト IP アドレスを含むネットワーク/ホストオブジェクトの名前を入力するか、または[選択（Select）]をクリックしてオブジェクトを選択することもできます。 （注） AAA：IPV6 ホストは、LDAP および TACACS+ プロトコルでのみサポートされます。Cisco Security Manager 4.17 以降、Radius プロトコルの IPv6 ホストは ASA 9.9(2) デバイス以降でサポートされます。 • [DNS Name]（PIX/ASA 7.2 以降のデバイスの場合だけ）：AAA サーバの DNS ホスト名。最大 128 文字。ホスト名は英数字およびハイフンですが、ホスト名の各要素は英数字で始まり、英数字で終わる必要があります。

要素	説明
インターフェイス	すべての発信 RADIUS または TACACS パケットに対して、その IP アドレスが使用されるインターフェイス（送信元インターフェイスと呼ばれます）。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは[選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。 **ヒント** • インターフェイスの名前を入力する場合、この AAA オブジェクトを使用するポリシーが、この名前のインターフェイスを含むデバイスに割り当てられるようにします。 • インターフェイス ロールの名前を入力する場合、ロールが複数のインターフェイスではなく、1 つのインターフェイスを表すようにします。 • AAA サーバ グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。グループ内の別の AAA サーバで異なる送信元インターフェイスが使用されている場合、変更を送信するとエラーが表示されます。 AAA サーバ グループ オブジェクトの作成 （349 ページ）を参照してください。 • IPS デバイス上で使用されている AAA サーバのインターフェイス名を指定しないでください。
タイムアウト（Timeout）	AAA サーバを応答なしと見なすまでの要求に対する待機時間。グループに他のサーバがなければ、次のサーバが試行されます。 • Cisco IOS ルータ：範囲は 1 ～ 1000 秒です。デフォルトは 5 秒です。 • ASA/PIX 7.x 以降、FWSM 3.1 以降のデバイス：範囲は 1 ～ 300 秒です。デフォルトは 10 秒です。 • PIX 6.3 ファイアウォール：範囲は 1 ～ 512 秒です。デフォルトは 5 秒です。 • IPS デバイス：範囲は 1 ～ 512 秒です。デフォルトは 3 秒です。

要素	説明
プロトコル	AAA サーバによって使用されるプロトコル。プロトコルリストの下側のフィールドは、選択によって変わります。 フィールドの詳細については、示されている項を参照してください。 • 次に、最も一般的なプロトコルを示します。 • RADIUS：すべてのデバイス タイプ。[AAA Server] ダイアログボックス - RADIUS 設定 （334 ページ）を参照してください。 • TACACS+：IPS 以外のすべてのデバイス タイプ。[AAA Server] ダイアログボックス - TACACS+ 設定 （337 ページ）を参照してください。 • 次のプロトコルは、ASA/PIX 7.x+ および FWSM 3.1+ デバイスについてサポートされます。LDAP は ScanSafe ポリシーをサポートする IOS デバイスでサポートされます。 • Kerberos：[AAA Server] ダイアログボックス - Kerberos 設定 （338 ページ）を参照してください。 • LDAP：[AAA Server] ダイアログボックス - LDAP 設定 （339 ページ）を参照してください。 • NT：[AAA Server] ダイアログボックス - NT 設定 （343 ページ）を参照してください。 • SDI：[AAA Server] ダイアログボックス - SDI 設定 （344 ページ）を参照してください。 • HTTP-FORM：[AAA Server] ダイアログボックス - HTTP-FORM 設定 （345 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

[AAA Server] ダイアログボックス - RADIUS 設定

[AAA Server] ダイアログボックスの RADIUS 設定を使用して、RADIUS AAA サーバ オブジェクトを設定します。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [RADIUS] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *47 : [AAA Server]* ダイアログボックス - *RADIUS* 設定

要素	説明
キー（Key） 確認（Confirm）	ネットワーク デバイス（クライアント）と AAA サーバ間でデータを暗号化するために使用される共有秘密キー。キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。 このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。 次の点に注意してください。 • キーは、IPS AAA ポリシーで使用される AAA サーバ オブジェクトに必須です。それ以外の場合、キーはオプションです。 • PIX、ASA、または FWSM デバイスではスペースを使用できません。これ以外のデバイスでは、スペースは使用できません。 • キーを定義しない場合、AAA サーバとその AAA クライアント間のすべてのトラフィックは暗号化されずに送信されます。
Authentication/Authorization Port	AAA 認証および認可が実行されるポート。デフォルトは 1645 です。 **ヒント** IPS デバイスのデフォルト ポートは 1812 です。このため、IPS 用のオブジェクトの設定時にデフォルト ポートを使用する場合は、この値を変更する必要があります。
Accounting Port	AAA アカウンティングが実行されるポート。デフォルトは 1646 です。

要素	説明
RADIUS Password 確認（Confirm） （ASA、PIX 7.x 以上、および FWSM 3.x 以上のデバイスだけ）	このデバイスを介して RADIUS 認可サーバにアクセスするユーザに共通のキーワード（最大 127 文字で大文字と小文字を区別する英数字）です。[Confirm] フィールドにパスワードを再入力します。 RADIUS 認可サーバーでは、各接続ユーザーに対してパスワードおよびユーザー名が必要です。RADIUS サーバ管理者は、このデバイス経由で RADIUS サーバに対して認可を行う各ユーザにこのパスワードが関連付けられるように RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバー管理者に伝えてください。 共通のユーザー パスワードを指定しなかった場合、各ユーザーのパスワードはユーザー名になります。 RADIUS 認可サーバーを認証に使用することは避けてください。共通パスワードやユーザー名を転用したパスワードは、ユーザーごとに一意のパスワードに比べ、安全性が低くなります。 **ヒント** • パスワードは認可サーバーにのみ適用され、認証サーバーには適用されません。RADIUS 認証サーバーに対しては、共通のパスワードは設定しないでください。 • このパスワードは、認可のため RADIUS プロトコルや RADIUS サーバによって要求されますが、ユーザが知っている必要はありません。デバイスはパスワードを自動的に提供します。
再試行間隔（Retry Interval） （ASA、PIX 7.x 以上、および FWSM 3.x 以上のデバイスだけ）	AAA サーバへのアクセス試行の間隔。値は次のとおりです。 • ASA/FWSM デバイス：1 ～ 10 秒。 • PIX デバイス：1 ～ 5 秒。

要素	説明
ACL Netmask Convert （ASA、PIX 7.x 以上、および FWSM 3.x 以上のデバイスだけ）	RADIUS サーバから受信したダウンロード可能 ACL に含まれているネットマスク表現を処理する方式。ASA/PIX/FWSM は、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると想定します。一方、Cisco IOS ソフトウェアを使用するデバイスは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカードネットマスク表現が含まれていると想定します。ワイルドカード マスクには、無視するビット位置に 1 が、一致するビット位置に 0 が入っています。ワイルドカード ネットマスク表現の変換は、RADIUS サーバ上で ACL の設定を変更しなくても、Cisco IOS ルータ用に作成されたダウンロード可能 ACL が ASA/PIX/FWSM デバイスによって使用可能であることを意味します。 次のオプションのいずれかを選択します。 • [Standard]：セキュリティ アプライアンスでは、RADIUS サーバから受信したすべてのダウンロード可能 ACL に標準ネットマスク表現だけが含まれていると想定します。ワイルドカード ネットマスク表現からの変換は実行されません。これがデフォルトです。 • [Auto-Detect]：セキュリティ アプライアンスでは、ダウンロード可能 ACL で使用されているネットマスク表現のタイプを判別しようとします。ワイルドカード ネットマスク表現を検出した場合は、標準ネットマスク表現に変換します。 RADIUS サーバーの設定方法が不明な場合は、このオプションが役立ちます。ただし、「穴」があるワイルドカードネットマスク表現は、正しく検出および変換できません。たとえば、ワイルドカードネットマスク 0.0.255.0 は、第 3 オクテットに任意の値を許可します。ただし、デバイスでは、この表現をワイルドカードネットマスクとして検出できません。 • [Wildcard]：セキュリティ アプライアンスでは、RADIUS サーバから受信したすべてのダウンロード可能 ACL にワイルドカード ネットマスク表現だけが含まれていると想定します。ワイルドカード ネットマスク表現は、標準ネットマスク表現に変換されます。

[AAA Server] ダイアログボックス - TACACS+ 設定

[AAA Server] ダイアログボックスの TACACS+ 設定を使用して、TACACS+ AAA サーバ オブジェクトを設定します。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [TACACS+] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *48 : [AAA Server]* ダイアログボックス - *TACACS+* 設定

要素	説明
キー（Key） 確認（Confirm）	クライアントと AAA サーバ間でデータを暗号化するために使用される共有秘密キー。キーは、大文字と小文字が区別される最大 127 文字の英数字文字列（米国英語）です。スペースと特殊文字を使用できます。 このフィールドで定義するキーは、TACACS+ サーバ上のキーと一致する必要があります。確認フィールドでもう一度キーを入力します。 次の点に注意してください。 • PIX、ASA、または FWSM デバイス上でスペースを含むキーを定義しようとすると、アクティビティ検証が失敗します。 • キーを定義しない場合、AAA サーバとその AAA クライアント間のすべてのトラフィックは暗号化されずに送信されます。
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 49 です。

[AAA Server] ダイアログボックス - Kerberos 設定

[AAA Server] ダイアログボックスの Kerberos 設定を使用して、Kerberos AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [Kerberos] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *49 : [AAA Server]* ダイアログボックス - *Kerberos* 設定

要素	説明
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 88 です。
Kerberos レルム名	Kerberos 認証サーバーおよびチケット保証サーバーを含むレルムの名前（最大 64 文字、通常はすべて大文字）。たとえば、EXAMPLE.COM となります。
再試行間隔（Retry Interval）	AAA サーバへのアクセス試行の間隔。間隔の範囲は、1 ～ 10 秒です。

[AAA Server] ダイアログボックス - LDAP 設定

[AAA Server] ダイアログボックスの LDAP 設定を使用して、LDAP AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバーは、ASA、PIX 7.x 以上、FWSM 3.1 以上、および IOS のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [LDAP] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *50 : [AAA Server]* ダイアログボックス - *LDAP* 設定

要素	説明
[LDAP over SSL/セキュア通信を有効にする（Enable LDAP over SSL/Secure Communication）]	デバイスと LDAP サーバ間にセキュアな SSL 接続を確立するかどうか。 **ヒント** パスワード管理をイネーブルにするために Microsoft Active Directory LDAP サーバを使用する場合は、このオプションを選択する必要があります。
[非ネゴシエーション（No Negotiation）] （IOS のみ）	このチェックボックスをオンにすると、以降はネゴシエーションが行われなくなり、以前に確立され、受け入れられたチャネルを受け入れるようになります。
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 389 です。
[ログインディレクトリ（Login Directory）]	認証済みバインディングに使用される LDAP 階層内のユーザー名またはディレクトリオブジェクトの名前（最大 128 文字）。認証済みバインディングは、一部の LDAP サーバ（Microsoft Active Directory サーバなど）によって、他の LDAP 操作の実行前に要求されます。このフィールドには、デバイスの認証特性が記述されます。これらの特性は、管理者特権を持つユーザーの特性に対応している必要があります。 この文字列では、大文字と小文字が区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。 通常は、DOMAIN\Administrator などのユーザ名です。従来型のフォーマット（cn=Administrator、OU=Employees、DN=example、DN=com など）を使用してもかまいません。
ログイン パスワード	LDAP サーバにアクセスするための、大文字と小文字が区別される英数字のパスワード（最大 64 文字）。スペースは使用できません。
[暗号化（IOS）（Encrypted (IOS)）]	ログイン パスワードを暗号化するかどうか。
LDAP Hierarchy Location	ベース Distinguished Name（DN; 識別名）。これは、認証サーバが認可要求を受け取ったときに検索する LDAP 階層内の場所です。たとえば、OU=Cisco のように指定します。最大長は 128 文字です。 文字列では、大文字と小文字が区別されます。スペースは使用できませんが、他の特殊文字は使用できます。
[PIX/ASA/FWSM] タブ	

要素	説明
LDAP Scope	認可要求を受け取ったサーバで行われる検索の範囲を指定します。次のオプションを使用できます。 • [onelevel]：ベース DN の 1 レベル下だけを検索します。このタイプの検索スコープは、範囲が狭いためサブツリー検索よりも高速です。これがデフォルトです。 • [サブツリー（subtree）]：ベース DN の下にあるすべてのレベル（つまりサブツリー階層全体）が検索対象となります。このオプションを選択すると、検索の実行に時間がかかります。
LDAP Distinguished Name	LDAP サーバのエントリを一意に識別する Relative Distinguished Name 属性を指定します（複数可）。共通の名前付き属性は、Common Name（CN）、sAMAccountName、userPrincipalName、および User ID（uid）です。この英数字の文字列は、最大 128 文字で、大文字と小文字が区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。
SASL MD5 Authentication SASL Kerberos Authentication Kerberos Server Group	これらのオプションによって、LDAP クライアント（ASA/PIX/FWSM デバイス）を LDAP サーバに認証するために、Simple Authentication and Security Layer（SASL）メカニズムが確立されます。これらのオプションのいずれかを選択しない場合は、シンプルなメカニズムが使用され、ユーザー名とパスワードがクリアテキストで送信されます。 1 つまたは両方の SASL 認証メカニズムを定義できます。SASL 認証のネゴシエーション時に、ASA/PIX/FWSM デバイスは、LDAP サーバで設定されている SASL メカニズムのリストを取得し、両方のデバイスで設定されている最も強力なメカニズムを選択します。 • [SASL MD5 Authentication]：デバイスから LDAP サーバに、ユーザ名とパスワードから計算された MD5 値を送信するかどうか。ユーザーパスワードを元に戻せる方法で保存するように LDAP サーバーを設定する必要があります。そうしないと LDAP サーバーがパスワードを検証できません。 • [SASL Kerberos Authentication]：デバイスから LDAP サーバに、Generic Security Services Application Programming Interface（GSSAPI）Kerberos メカニズムを使用してユーザ名とレルムを送信するかどうか。このメカニズムの方が MD5 メカニズムよりも強力です。 Kerberos を選択する場合、SASL 認証に使用される Kerberos AAA サーバ グループの名前も入力する必要があります。最大長は 16 文字です。

要素	説明
[LDAPサーバータイプ（LDAP Server Type）]	AAA に使用される LDAP サーバのタイプ。 • [Auto-Detect]：ASA/PIX/FWSM デバイスがサーバ タイプを自動的に判別しようとします。これがデフォルトです。 • [Microsoft]：LDAP サーバは Microsoft Active Directory サーバです。 （注） Microsoft Active Directory によるパスワード管理をイネーブルにするように LDAP over SSL を設定する必要があります。 • [Sun]：LDAP サーバは Sun Microsystems JAVA System Directory Server です。 • [OpenLDAP]：サーバは OpenLDAP サーバです。これは、ASA/PIX 8.0 以上のデバイスだけで使用できます。 • [Novell]：サーバは Novell LDAP サーバです。これは、ASA/PIX 8.0 以上のデバイスだけで使用できます。
LDAP Attribute Map	LDAP サーバにバインドするための LDAP 属性設定。LDAP 属性マップポリシーオブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストから名前を選択するか新しいオブジェクトを作成します。 LDAP 属性マップは、ユーザが定義した属性名をシスコ定義の属性にマッピングします。詳細については、[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （347 ページ）を参照してください。
Group Base DN	（Microsoft LDAP AD サーバーのみ）すべてのユーザーグループが定義されるベース指定名（DN）。ASA がユーザ グループ メンバーシップについて AD サーバにアクセスすると、検索はこの DN で開始されます。すべてのグループは、LDAP ディレクトリ階層内のこの DN の下に存在する必要があります。このパスの外側にはグループを配置できません。グループを配置した場合には、グループは見つけられません。この場所を指定すると、ユーザ グループ検索の実行にかかる時間が短縮されます。 英数字文字列は大文字と小文字が区別され、最大 128 文字まで指定できます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。 次に例を示します。 DN=cisco,DN=com ヒント グループベース DN を指定しない場合、LDAP 識別名の設定がグループ検索の開始点として使用されます。

要素	説明
Group Search Timeout	（Microsoft LDAP AD サーバーのみ）ユーザーグループ情報のクエリーに対する Active Directory サーバーからの応答を待機する最長時間（秒単位）。デフォルトは 10 秒で、範囲は 1 ～ 300 秒です。
[IOS] タブ	
[セキュアな暗号（Secure Cipher）]	使用される暗号化方式。
Attribute Map (IOS)	サーバーが使用する IOS 属性マップの名前。
[セキュアなトラストポイント（Secure Trust Point）]	証明書のトラストポイントの名前。
[認証でバインドが先（Authentication bind-first）]	このオプションにより、認証要求の検索とバインドの順序を設定できます。デフォルトでは、検索の後にバインドが実行されます。
[承認は不要（No Authorization Required）]	認証要求に承認は不要です。
Authentication Compare	このチェックボックスを選択すると、バインド要求を認証の比較要求に置き換えることができます。デフォルトでは、認証要求はバインド要求で実行されます。
User Object Filter	検索要求で使用される検索フィルタのユーザー属性タイプを指定します。これは、検索要求されたユーザーをフィルタ処理するために役立ちます。

[AAA Server] ダイアログボックス - NT 設定

[AAA Server] ダイアログボックスの NT 設定を使用して、NT AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [NT] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *51 : [AAA Server]* ダイアログボックス - *NT* 設定

要素	説明
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 139 です。
NT Authentication Host	認証ドメイン コントローラ ホスト名の名前（最大 16 文字）。

[AAA Server] ダイアログボックス - SDI 設定

[AAA Server] ダイアログボックスの SDI 設定を使用して、SDI AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [SDI] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *52 : [AAA Server]* ダイアログボックス - *SDI* 設定

要素	説明
サーバポート（Server Port）	AAA サーバとの通信に使用するポート。デフォルトは 5500 です。
再試行間隔（Retry Interval）	AAA サーバへのアクセス試行の間隔。間隔の範囲は、1 ～ 10 秒です。デフォルトは 10 秒です。
SDI Server Version	SDI サーバのバージョン。 • [SDI-pre-5]：バージョン 5.0 よりも前のすべての SDI バージョン。 • [SDI-5]：SDI バージョン 5.0 以降。
SDIバージョン5より前のセカンダリサーバー（SDI pre-5 Secondary Server）	（任意）5.0 よりも前の SDI バージョンを使用している場合に、プライマリ サーバに障害が発生したときに認証に使用されるセカンダリ サーバ。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてオブジェクトを選択します。または、新しいオブジェクトを作成します。

[AAA Server] ダイアログボックス - HTTP-FORM 設定

[AAA Server] ダイアログボックスの HTTP-FORM 設定を使用して、Single Sign-On 認証（SSO; シングル サインオン）用の HTTP-Form AAA サーバ オブジェクトを設定します。

（注） このタイプの AAA サーバは、ASA、PIX 7.x 以上、および FWSM 3.1 以上のデバイスだけで設定できます。

ナビゲーション パス

[Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）に移動して、[プロトコル（Protocol）] フィールドで [HTTP-FORM] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）

フィールド リファレンス

表 *53 : [AAA Server]* ダイアログボックス - *HTTP-Form* 設定

要素	説明
Start URL	セキュリティ アプライアンスの WebVPN サーバがオプションのプリログイン クッキーを取得する URL。URL の最大長は 1024 文字です。 認証 Web サーバは、ログイン ページのコンテンツとともに Set-Cookie ヘッダーを送信することによって、プリログイン シーケンスを実行する場合があります。このフィールドの URL によって、クッキーを取得する場所が定義されます。 （注） 実際のログインシーケンスは、プリログインクッキーシーケンスのあとに開始されます。
Action URI	セキュリティアプライアンスが Single Sign-On（SSO; シングル サインオン）認証の HTTP POST 要求を送信する Web サーバ上の認証プログラムの場所と名前を定義する Uniform Resource Identifier（URI）。 アクション URI の最大長は 2048 文字です。 ヒント 認証 Web サーバー上のアクション URI を見つけるには、ブラウザで直接 Web サーバーのログインページに接続します。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバーのアクション URI です。
Username Parameter	SSO 認証の HTTP POST 要求に含まれているユーザ名パラメータの名前。最大長は 128 文字です。 ログイン時に、ユーザは実際の名前の値を入力します。それが HTTP POST 要求に入力され、認証 Web サーバに渡されます。
Password Parameter	SSO 認証の HTTP POST 要求に含まれているパスワードパラメータの名前。最大長は 128 文字です。 ログイン時に、ユーザは実際のパスワードの値を入力します。それが HTTP POST 要求に入力され、認証 Web サーバに渡されます。
Hidden Values	SSO 認証の HTTP POST 要求に含まれている非表示パラメータ。ユーザ名やパスワードと異なりユーザには表示されないため、非表示パラメータと呼ばれます。 非表示パラメータの最大長は 2048 文字です。 ヒント 認証 Web サーバから受け取るフォームで HTTP ヘッダー アナライザを使用することによって、Web サーバが POST 要求で想定している非表示パラメータを検出できます。

要素	説明
Authentication Cookie Name	セキュリティ アプライアンスによって SSO に使用される認証クッキーの名前。最大長は 128 文字です。 SSO 認証が成功すると、認証 Web サーバはこの認証クッキーをクライアント ブラウザに渡します。クライアント ブラウザは、このクッキーを提示して、SSO ドメイン内の他の Web サーバに対して認証します。

[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス

[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックスを使用して、Cisco Lightweight Directory Access Protocol（LDAP）属性名をカスタムのユーザ定義属性名に解釈する名前マッピングを使用する属性マップを読み込みます。

既存の LDAP ディレクトリにセキュリティ アプライアンスを導入している場合、既存のカスタム LDAP 属性の名前と値は、Cisco 属性の名前と値とは異なる場合があります。既存の属性の名前を変更するのではなく、カスタムの属性名と値を Cisco の属性名と値にマッピングする、LDAP 属性マップを作成できます。セキュリティ アプライアンスは、単純な文字列置換を使用して、ユーザ独自のカスタム名と値だけを提供します。次に、ユーザは、必要に応じてこれらの属性マップを LDAP サーバにバインドしたり、削除したりできます。属性マップ全体を削除したり、名前および値の個々のエントリを削除したりできます。

ASA、PIX、および FWSM デバイスでの LDAP のサポートの詳細については、ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [LDAP属性マップ（LDAP Attribute Map）] を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- AAA サーバ オブジェクトの作成 （330 ページ）
- [AAA Server] ダイアログボックス - LDAP 設定 （339 ページ）

フィールド リファレンス

表 54 : [Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。

要素	説明
説明	（任意）オブジェクトの説明。
[Attribute Map] テーブル	このテーブルには、マッピングされた値が表示されます。各エントリは、カスタマー マップ名、Cisco マップ名、およびカスタマー名から Cisco 名への属性マッピングを示します。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックして、[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス （348 ページ）を開きます。 • マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス

[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックスを使用して、カスタムの属性名および一致した Cisco 属性名と値に対してユーザ定義の属性値を適用する値マッピングを使用する属性マップを読み込みます。

ナビゲーション パス

[Add LDAP Attribute Map]/[Edit LDAP Attribute Map] ダイアログボックス （347 ページ）で、[行の追加（Add Row）] ボタンをクリックして新しいマッピングを追加するか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 55 : [Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス

要素	説明
Customer Map Name	Cisco マップに関連する属性マップの名前。
Cisco Map Name	カスタマー マップ名にマッピングする Cisco 属性マップ名。
[Customer to Cisco Map Value] テーブル	カスタマー名から Cisco 名へのマッピング。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックして、[Add Map Value]/[Edit Map Value] ダイアログボックス （349 ページ）を開きます。 • マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Add Map Value]/[Edit Map Value] ダイアログボックス

[Add Map Value]/[Edit Map Value] ダイアログボックスを使用して、カスタマー LDAP 属性値を Cisco マップ値にマッピングします。Cisco 値と一致させる、LDAP マップの値を入力します。

ナビゲーション パス

[Add LDAP Attribute Map Value]/[Edit LDAP Attribute Map Value] ダイアログボックス （348 ページ）で、[行の追加（Add Row）] ボタンをクリックして新しいマッピングを追加するか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

AAA サーバ グループ オブジェクトの作成

認証や認可などの AAA サービスを必要とする Security Manager ポリシー用に、AAA サーバ グループ オブジェクトを作成できます。各 AAA サーバ グループ オブジェクトには複数の AAA サーバを含めることができ、それらはすべて同じプロトコル（RADIUS や TACACS+ など）を使用します。たとえば、RADIUS を使用してネットワーク アクセスを認証し、TACACS+ を使用して CLI アクセスを認証する場合、少なくとも 2 つの AAA サーバ グループ オブジェクトを作成する必要があります。1 つは RADIUS サーバ用、1 つは TACACS+ サーバ用です。

また、グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。グループ内の別の AAA サーバで異なる送信元インターフェイスが使用されている場合、変更を送信するとエラーが表示されます。

（注） エラーは、送信元として定義されている実際のインターフェイスによってトリガーされます。インターフェイスを表すインターフェイス ロールの名前ではありません。つまり、2 つの AAA サーバは、どちらも同じデバイス インターフェイスに解決されるかぎり、送信元インターフェイスとして定義された異なるインターフェイス ロールを持つことができます。送信元インターフェイスに対して定義されたインターフェイス ロールが、デバイス上の複数の実際のインターフェイスと一致した場合にも、エラーが表示されます。

作成できる AAA サーバ グループ オブジェクトの数および各グループ オブジェクトに含めることができる AAA サーバ オブジェクトの数は、選択されているプラットフォームによって異なります。たとえば、ASA デバイスでは、最大 18 個のシングルモード サーバ グループ（それぞれ最大 16 個のサーバ）と、7 個のマルチモード サーバ グループ（それぞれ最大 4 個のサーバ）がサポートされます。PIX ファイアウォールでは、最大 14 個のサーバ グループ（それぞれ最大 14 個のサーバ）がサポートされます。

（注） Security Manager には、認証を Cisco IOS ルータ内でローカルに実行するときに使用できる定義済みの AAA サーバ グループ オブジェクトが含まれています。

ヒント このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに、AAA サーバ グループ オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）
- 定義済みの AAA 認証サーバ グループ （328 ページ）
- デフォルトの AAA サーバ グループおよび IOS デバイス （329 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [AAAサーバーグループ（AAA Server Groups）] を選択します。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [AAA Server Group] ダイアログボックス （351 ページ）を開きます。

ステップ 4 オブジェクトの名前を入力します。名前の最大長は、このオブジェクトを ASA、PIX、または FWSM デバイスで使用する場合は 16 文字、Cisco IOS ルータの場合は 128 文字です。スペースはサポートされていません。

（注） Cisco IOS ルータでは、AAA サーバ グループ名として RADIUS、TACACS、TACACS+ はサポートされていません。また、これらの名前の短縮形（rad や tac など）を使用することは推奨しません。

ステップ 5 グループ内のサーバによって使用されるプロトコルを選択します。

ステップ 6 グループに含める AAA サーバを定義する AAA サーバ ポリシー オブジェクトの名前を入力します。[選択（Select）] を選択して、選択したプロトコルによってフィルタリングされたリストからオブジェクトを選択します。選択リストから、新しい AAA サーバ オブジェクトを作成することもできます。複数のオブジェクトを指定する場合は、カンマで区切ります。

ステップ 7 必要な追加オプションを設定します。

- [Make this Group the Default AAA Server Group]：IOS デバイスの場合だけ、このグループをデフォルト グループとして使用するかどうか。AAA を必要とするすべてのポリシーに対して、このプロトコルの単一のグローバル サーバ グループを持つ場合、このオプションを使用します。詳細については、デフォルトの AAA サーバ グループおよび IOS デバイス （329 ページ）を参照してください。
- ASA 8.4(2) 以降のデバイス：Active Directory エージェントサーバーを含む RADIUS グループを作成している場合は、[AD エージェントモード（AD Agent Mode）] を選択します。このオプションは、グループ内のサーバーがフル機能の RADIUS サーバーではなく、アイデンティティ認識型ファイアウォールに AD エージェント機能を提供することを示します。このグループは、アイデンティティ オプションのポリシーで使用してください。
- ASA、PIX、FWSM デバイス：応答を停止した AAA サーバの処理方法について、およびアカウンティング メッセージの送信方法について、オプションを選択します。詳細については、[AAA Server Group] ダイアログボックス （351 ページ）を参照してください。

ステップ 8 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 9 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

[AAA Server Group] ダイアログボックス

[AAA Server Group] ダイアログボックスを使用して、AAA サーバ グループを作成、コピー、および編集します。認証、許可、またはアカウンティングに AAA サーバを使用するポリシーを定義するときは、サーバが属しているサーバ グループを選択することによって、サーバを選択します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから [AAAサーバーグループ（AAA Server Groups）] を選択します。作業領域内を右

クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- AAA サーバ グループ オブジェクトの作成 （349 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- [Add AAA Server]/[Edit AAA Server] ダイアログボックス （331 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 56 : [AAA Server Group] ダイアログボックス

要素	説明
名前	オブジェクト名（このオブジェクトをファイアウォール デバイスで使用する場合は最大 16 文字。Cisco IOS ルータの場合は最大 128 文字）。オブジェクト名では、大文字と小文字が区別されません。スペースはサポートされていません。 次の重要事項を考慮してください。 • Cisco IOS ルータでは、RADIUS、TACACS、または TACACS+ という名前の AAA サーバ グループはサポートされていません。また、これらの名前の短縮形（rad や tac など）を使用することは推奨しません。 • この AAA サーバ グループを RADIUS または TACACS+ のデフォルト グループとして定義する場合、ここで定義する名前は、展開時にデバイス設定でデフォルト名（RADIUS または TACACS+）によって自動的に置き換えられます。
説明	（任意）オブジェクトの説明。
プロトコル	グループ内の AAA サーバによって使用されるプロトコル。これらのオプションの詳細については、サポートされる AAA サーバ タイプ （324 ページ）および ASA、PIX、および FWSM デバイスでのその他の AAA サポート （325 ページ）を参照してください。

要素	説明
AAAサーバ	サーバ グループを構成する AAA サーバ ポリシー オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、選択したプロトコルを使用する AAA サーバーオブジェクトだけを表示するようにフィルタ処理されたリストから選択します。複数のオブジェクトを指定する場合は、カンマで区切ります。選択リストから新しいオブジェクトを作成することもできます。
Make this Group the Default AAA Server Group (IOS) （IOS デバイスのみ）	この AAA サーバ グループを RADIUS または TACACS+ プロトコルのデフォルト グループとして指定するかどうか。AAA を必要とする特定のデバイスのすべてのポリシーに対して、選択したプロトコルで 1 つのグローバル グループを使用する場合、このオプションを選択します。 複数の RADIUS または TACACS+ AAA サーバ グループを作成する場合は、このオプションを選択しないでください。異なる AAA 機能を分離するため（たとえば、認証用に 1 つのグループを使用し、認可用に別のグループを使用）、または VRF 環境で異なるカスタマーを分離するために、複数のグループを使用できます。 （注） IOS ルータを検出するときに、AAA サーバ グループのメンバーではないデバイス設定内の AAA サーバは、CSM-rad-grp（RADIUS の場合）および CSM-tac-grp（TACACS+ の場合）という特別なグループに配置されます。これらはどちらもデフォルト グループとしてマークされています。これら 2 つのグループは、Security Manager でこれらのサーバを管理できるようにするためだけに作成されています。展開中に、これらの特別なグループ内の AAA サーバは、個別のサーバとしてデバイスに展開されます。詳細については、デフォルトの AAA サーバ グループおよび IOS デバイス （329 ページ）を参照してください。
ADエージェントモード（AD Agent Mode） （ASA 8.4(2) 以降のデバイスのみ）。	グループ内のサーバーが、ID 認証ファイアウォール構成で使用される Active Directory エージェントであるかどうかを指定します。AD エージェントグループがフル機能の RADIUS サーバーグループではないことを示すには、このオプションを選択する必要があります。 AD エージェントグループは、アイデンティティオプションのポリシーで使用します。詳細については、Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。

要素	説明
動的認可（Dynamic Authorization） （ASA 9.2(1) 以降のデバイスのみ）。	RADIUS プロトコルを使用している場合は、[動的認可（Dynamic Authorization）] チェックボックスをオンにして、AAA サーバーグループに対して RADIUS 動的認可の認可変更（CoA）サービスを有効にします。 [ポート（Port）] フィールドで、RADIUS CoA 要求のリスニング ポートを指定します。有効数は 1024 ～ 65535 であり、デフォルト値は 1700 です。 一旦定義されると、対応する RADIUS サーバーグループが CoA 通知用に登録され、AAA は Cisco Identity Services Engine（ISE）から CoA ポリシーの更新を行うポートをリッスンします。
中間アカウントの更新（Interim Account Update） （ASA 9.2(1) 以降のデバイスのみ）。	RADIUS プロトコルを使用している場合は、[中間アカウントの更新（Interim Account Update）] チェックボックスをオンにして、RADIUS 中間アカウンティング更新メッセージの生成を有効にします。現在、これらのメッセージは、VPN トンネル接続がクライアントレス VPN セッションに追加された場合にだけ生成されます。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。 [間隔（Interval）] フィールドの定期アカウンティング更新の間隔（時間単位）を指定します。有効数は 1 ～ 120 であり、デフォルト値は 24 です。
認可のみ（Authorize only） （ASA 9.2(1) 以降のデバイスのみ）。	RADIUS プロトコルを使用している場合は、[認可のみ（Authorize only）] チェックボックスをオンにして、RADIUS サーバーグループの認可専用モードを有効にします。このチェックボックスを選択する場合、個別の AAA サーバに対して設定する共通パスワードは不要なため、設定する必要はありません。
Max Failed Attempts （PIX、ASA、FWSM デバイスだけ）	サーバーグループ内の所定のサーバーが非アクティブ化されるまでに、そのサーバーで許容される接続試行の失敗回数。デフォルトは 3、指定できる範囲は 1 ～ 5 です。
内部レルム ID（Internal Realm ID） （ASA 9.8(1) 以降のデバイスのみ）	AAA サーバー グループ ポリシー オブジェクトの RADIUS または LDAP プロトコルに対応するレルム ID を入力します。 （注） レルム ID は、1 から 65535 の一意の値であり、RADIUS および LDAP プロトコルにのみ適用されます。

要素	説明
Reactivation Mode （PIX、ASA、FWSM デバイスだけ）	グループ内の障害が発生したサーバーを再アクティブ化するときに使用する方式。 • [枯渇（Depletion）]：グループ内のすべてのサーバーが非アクティブになった後に、障害の発生したサーバーのみ再度アクティブ化します。これがデフォルトです。 非アクティブになったサーバーは、グループにある他のすべてのサーバーが非アクティブになるまで非アクティブのままです。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。 ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定していて、グループ内のすべてのサーバーが応答しない場合、そのグループは応答なしと見なされ、フォールバック方式が試行されます。グループの最後のサーバーが無効になってから、すべてのサーバーを再度有効にするまでの経過時間（分単位）を決定する [再アクティブ化のデッドタイム（Reactivation Deadtime）] 値を設定できます。 フォールバック方式として設定されていない場合、デバイスは引き続きグループ内のサーバーにアクセスしようとします。 • [Timed]：ダウンタイムの 30 秒後に、障害が発生したサーバを再アクティブ化します。このオプションは、グループの最初のサーバーがプライマリサーバーであり、可能な限りバックアップサーバーではなくプライマリサーバーを使用する場合に役立ちます。このポリシーは、UDP サーバーの場合は機能しません。サーバーが存在しない場合でも UDP サーバーへの接続は失敗しないため、UDP サーバーはすぐに再度オンラインになります。サーバーグループに到達不能な複数のサーバーが含まれている場合、接続時間が遅くなったり、接続に失敗したりする場合があります。
Reactivation Deadtime （PIX、ASA、FWSM デバイスだけ）	再アクティブ化モードとして [枯渇（Depletion）] を選択した場合、グループ内にある最後のサーバーの非アクティブ化とグループ内の全サーバーの再アクティブ化の間に必要な時間（分）。デフォルトは 10 で、範囲は 0 ～ 1440（24 時間）です。

要素	説明
Group Accounting Mode （PIX、ASA、FWSM デバイスだけ）	RADIUS または TACACS+ プロトコルを使用する場合、アカウンティング メッセージをグループ内の AAA サーバに送信する方式。 アカウンティングにサーバーグループを使用する場合（プロトコルは RADIUS または TACACS+）、アカウンティングメッセージをグループ内の AAA サーバーに送信する方式。 • [Single]：アカウンティング メッセージは、グループ内の 1 つのサーバに送信されます。これがデフォルトです。 • [Simultaneous]：アカウンティング メッセージは、グループ内のすべてのサーバに同時に送信されます。このオプションを選択する場合、再アクティブ化モードとして [指定時刻（Timed）] を使用することが ASA により強制されます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

アクセス コントロール リスト オブジェクトの作成

アクセス コントロール リスト（ACL）オブジェクトは、1 つ以上のアクセス コントロール エントリ（ACE）、1 つ以上の ACL オブジェクト、または両方の組み合わせで構成されます。各 ACE は、ACL 内の個々の許可または拒否ステートメントです。ACL ポリシー オブジェクトを、複数のその他のポリシーおよびポリシー オブジェクト内で使用できます。

Cisco Security Manager バージョン 4.13 以降、オブジェクトグループに VM 属性が含まれていて、それが他のポリシー （アクセス ルールを除く）に適用されている場合、展開は失敗します。VM 属性オブジェクトは、object-group-search access-control がイネーブルになっている場合に、ASA 9.7.1 以降のデバイスに適用されます。

次のタイプの ACL オブジェクトを作成できます。

- 拡張：拡張 ACL では、送信元および宛先アドレスとサービス（またはトラフィックプロトコル）を指定できます。さらに、プロトコルタイプに基づいて、ポート（TCP または UDP の場合）または ICMP タイプ（ICMP の場合）を指定できます。拡張 ACL オブジェ

クトの詳細については、拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）を参照してください。

- 標準：標準 ACL は、トラフィックの照合に送信元アドレスを使用します。標準 ACL オブジェクトの詳細については、標準アクセス コントロール リスト オブジェクトの作成 （360 ページ）を参照してください。
- Web：Web ACL では、宛先アドレスおよびポート、または URL フィルタが使用されます。Web タイプ ACL オブジェクトの詳細については、Web アクセス コントロール リスト オブジェクトの作成 （361 ページ）を参照してください。
- 統合：統合 ACL オブジェクトを使用すると、送信元ネットワーク/ホスト、送信元セキュリティグループ、ユーザ、宛先ネットワーク/ホスト、宛先セキュリティグループ、およびサービスを使用してトラフィックを照合できます。さらに、ネットワーク/ホストの指定には、IPv4 アドレス、IPv6 アドレス、またはその両方の組み合わせを含めることができます（Security Manager 4.4 および ASA 9.0 以降のリリースでは、個別の IPv4 および IPv6 アドレス指定/オブジェクトが「統合」されました）。これらの ACL の詳細については、統合アクセス制御リストオブジェクトの作成 （363 ページ）を参照してください。
- Ethertype：EtherType ACL は、ルーテッドモードおよびトランスペアレントモードのブリッジ グループ メンバーのインターフェイスの非 IP レイヤ 2 トラフィックにのみ適用されます。これらのルールを使用して、レイヤ 2 パケットの EtherType 値に基づいてトラフィックを許可またはドロップできます。EtherType ACL を使用すると、デバイス全体の非 IP トラフィックのフローを制御できます。トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください。

これらのオブジェクトで使用されるダイアログボックスの参照情報については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）を参照してください。

（注） CSM には、参照位置の ACL オブジェクトに対する設計レベルの制約があります。したがって、[Policy Object Manager] テーブルの [参照（Referenced）] ボタンは無効になります。

拡張アクセス コントロール リスト オブジェクトの作成

拡張アクセス コントロール リストを使用すると、特定の IP アドレスから特定の宛先 IP アドレスおよびポートへのトラフィックを許可または拒否でき、トラフィックのプロトコル（ICMP、TCP、UDP など）を指定できます。拡張 ACL の範囲は 100 ～ 199 であり、Cisco IOS ソフトウェアリリース 12.0.1 以降を実行しているデバイスの場合は 2000 ～ 2699 です。

拡張 ACL の例：

```
access-list 110 - Applied to traffic leaving the office (outgoing)
access-list 110 permit tcp 10.128.2.0 0.0.0.255 any eq 80
```

ACL 110 は、10.128.2.0 ネットワーク上の任意のアドレスから送信されたトラフィックを許可します。「All-IPv4-Addresses」ステートメントは、ポート 80 へという制限付きで、トラフィックが任意の宛先アドレスを持つことが許可されることを意味します。0.0.0.0/255.255.255.255 という値を「All-IPv4-Addresses」として指定できます。

用途：

- NAT（ポリシー NAT および NAT 免除）のアドレスの識別：ポリシー NAT では、拡張アクセス リストで送信元および宛先アドレスとポートを指定することによって、アドレス変換のローカル トラフィックを識別できます。通常の NAT では、ローカル アドレスだけを考慮できます。ポリシー NAT とともに使用されるアクセス リストは、アクセス コントロール エントリ（ACE）を拒否するように設定することはできません。
- IOS ダイナミック NAT のアドレスの識別：ユーザ定義の ACL の場合、VPN トラフィックから NAT トラフィックを推定するときに、NAT プラグインによって独自の ACL CLI が生成されます。
- Network Admission Control（NAC; ネットワーク アドミッション コントロール）によって代行受信されるトラフィックのフィルタリング。
- モジュラ ポリシーのトラフィック クラス マップ内のトラフィックの識別：アクセス リストを使用して、クラス マップ内のトラフィックを識別できます。クラス マップは、TCP および一般接続設定、検査、IPS、QoS など、Modular Policy Framework をサポートする機能のために使用されます。1 つ以上のアクセス リストを使用して、特定のタイプのトラフィックを識別できます。
- トランスペアレント モードの場合、ルーテッド モードのセキュリティ アプライアンスによってブロックされるプロトコル（BGP、DHCP、マルチキャスト ストリームなど）のイネーブル化。これらのプロトコルには、リターン トラフィックを許可するセキュリティ アプライアンス上のセッションがないため、両方のインターフェイス上にアクセス リストも必要です。
- VPN アクセスの確立：VPN コマンドで拡張アクセス リストを使用して、IPsec サイト間トンネルについてデバイスでトンネリングする必要があるトラフィックを識別できます。または、VPN クライアントについてデバイスでトンネリングする必要があるトラフィックを識別できます。次の表に示すポリシーオブジェクトおよび設定とともに使用します。

表 *57*：ポリシー オブジェクトおよび設定

ポリシーオブジェクト	Device	目的
VPN トポロジ	任意（Any）	保護ネットワークの選択。
ASA ユーザ グループ	ASA	インバウンド ファイアウォール ポリシー、アウトバウンド ファイアウォール ポリシー、フィルタ ACL。

ポリシーオブジェクト	Device	目的
トラフィック フロー	ASA、PIX 7+	サービス ポリシールール（MPC）。トラフィック フローBB（クラスマップ）は、トラフィック一致タイプの 1 つとして拡張 ACL を使用します。
ユーザー グループ	• IOS • Catalyst 6500/7600 • PIX 6.3	Easy VPN、スプリット トンネル ACL、およびファイアウォール ACL（IOS デバイスだけ）用。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセスコントロールリスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。デフォルトで [拡張（Extended）] タブが表示されます。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add Extended Access List] ダイアログボックスが表示されます（ [Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）を参照）。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックス （947 ページ）を参照してください。

ステップ 5 ダイアログボックスのテーブル内で右クリックし、[追加（Add）] を選択します。

[Add Extended Access Control Entry] ダイアログボックスが表示されます。

ステップ 6 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセスコントロールエントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックが発生する送信元アドレス、トラフィックが到達する宛先アドレス、およびトラフィックの特性を定義す

るサービスを入力します。[詳細設定（Advanced）] をクリックして、ロギングオプションを定義します。ダイアログボックスのフィールドの詳細については、 [Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス （367 ページ）を参照してください。

- [ACLオブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 7 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[Add Extended Access List] ページに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 8 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 9 [OK] をクリックしてオブジェクトを保存します。

標準アクセス コントロール リスト オブジェクトの作成

標準アクセス コントロール リストを使用すると、特定の IP アドレスからのトラフィックを許可または拒否できます。パケットの宛先と関連するポートは任意です。標準 IP ACL の範囲は 1 ～ 99 です。

標準 ACL の例：

```
access-list 10 permit 192.168.2.0 0.0.0.255
```

用途：

- OSPF ルート再配布の識別。
- SNMP を使用するコミュニティ ストリングのユーザのフィルタリング。
- Catalyst 6500/7600 デバイスの VLAN ACL の設定。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセスコントロールリスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。

ステップ 3 [標準（Standard）] タブをクリックします。

ステップ 4 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add Standard Access List] ダイアログボックスが表示されます（[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）を参照）。

ステップ 5 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックス （947 ページ）を参照してください。

ステップ 6 テーブル内で右クリックし、[追加（Add）] を選択します。

[Add Standard Access Control Entry] ダイアログボックスが表示されます。

ステップ 7 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセスコントロールエントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックが発生する送信元アドレスを入力し、ロギング オプションを選択します。ダイアログボックスのフィールドの詳細については、[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス （370 ページ）を参照してください。
- [ACL オブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 8 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[Add Standard Access List] ダイアログボックスに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

Web アクセス コントロール リスト オブジェクトの作成

Web ACL（WebVPN とも呼ばれる）を使用すると、Web ブラウザを使用して、セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立できます。ソフトウェアまたはハードウェア クライアントは必要ありません。WebVPN によって、幅広い Web リソースや、Web 対応アプリケーションとレガシー アプリケーションの両方に、HTTPS インターネット サイトに到達できるほとんどのコンピュータから簡単にアクセスできます。WebVPN では、Secure Socket Layer プロトコルとその後継である Transport Layer Security（SSL/TLS1）を

使用して、リモートユーザーと、セントラルサイトで設定した特定のサポート対象内部リソース間のセキュアな接続が提供されます。

次の表に、Web VPN ACL の例を示します。

表 *58 : Web VPN ACL* の例

Action	フィルタ	影響
拒否	url http://*.yahoo.com/	Yahoo! すべてへのアクセスを拒否します。
拒否	url cifs://fileserver/share/directory	指定された場所にあるすべてのファイルへのアクセスを拒否します。
拒否	url https://www.company.com/directory/file.html	指定されたファイルへのアクセスを拒否します。
許可	url https://www.company.com/directory	指定された場所へのアクセスを許可します。
拒否	url http://*:8080/	ポート 8080 を介した任意の場所への HTTPS アクセスを拒否します。
拒否	url http://10.10.10.10	10.10.10.10 への HTTP アクセスを拒否します。
許可	url any	任意の URL へのアクセスを許可します。通常は、url アクセスを拒否する ACL のあとに使用されます。

用途：

- ASA ユーザ グループ ポリシー オブジェクトのフィルタ ACL として（[SSL VPN] > [Clientless]）。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセスコントロールリスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。

ステップ 3 [Web] タブをクリックします。

ステップ 4 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add WebType Access List] ダイアログボックスが表示されます（[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）を参照）。

ステップ 5 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、[Firewall ACL Setting] ダイアログボックス （947 ページ）を参照してください。

ステップ 6 アクセス コントロール エントリ テーブル内で右クリックし、[追加（Add）] を選択します。

[Add Web Access Control Entry] ダイアログボックスが表示されます。

ステップ 7 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセスコントロールエントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックのネットワーク宛先（ネットワーク フィルタ）または Web アドレス（URL フィルタ）に基づいてフィルタリングできます。ダイアログボックスのフィールドの詳細については、[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス （372 ページ）を参照してください。
- [ACL オブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 8 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[Add WebType Access List] ページに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

統合アクセス制御リストオブジェクトの作成

統合アクセス制御リストを使用すると、特定のネットワーク、ホスト、セキュリティグループ、およびユーザーからの、特定のネットワーク、ホスト、およびセキュリティグループ宛てのトラフィックを許可または拒否できます。関連するサービスも指定します。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アクセス制御リスト（Access Control Lists）] を選択します。

[Access Control List] ページが表示されます。

ステップ 3 [統合（Unified）] タブをクリックします。

ステップ 4 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[拡張アクセスリストの追加（Add Extended Access List）] ダイアログボックスが表示されます（ [Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）を参照）。

ステップ 5 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

（注） ACL オブジェクトの名前が一意であり、ファイアウォール ACL 設定で定義されたファイアウォール ルール ACL と同じ名前でないことを確認してください。詳細については、 [Firewall ACL Setting] ダイアログボックス （947 ページ）を参照してください。

ステップ 6 ダイアログボックスのテーブル内で右クリックし、[追加（Add）] を選択します。

[統合アクセス制御エントリの追加（Add Unified Access Control Entry）] ダイアログボックスが表示されます。

ステップ 7 アクセス コントロール エントリを作成します。

- [タイプ（Type）] で [アクセス制御エントリ（Access Control Entry）] を選択した場合は、照合するトラフィックの特性とトラフィックを許可または拒否するかを指定します。トラフィックが発生する送信元アドレスを入力し、ロギング オプションを選択します。ダイアログボックスのフィールドの詳細については、[Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）] ダイアログボックス （375 ページ）を参照してください。
- [ACL オブジェクト（ACL Object）] を選択した場合は、使用可能なオブジェクトのリストでオブジェクトを選択し、[>>] をクリックしてそのオブジェクトを選択されたオブジェクトのリストに追加します。

ステップ 8 [OK] をクリックして変更を保存します。

ダイアログボックスが閉じ、[標準アクセスリストの追加（Add Standard Access List）] ダイアログボックスに戻ります。新しいエントリがテーブルに表示されます。必要に応じて、そのエントリを選択し、上下ボタンをクリックして目的の位置に移動します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

[Add Access List]/[Edit Access List] ダイアログボックス

[Add Access List]/[Edit Access List] ダイアログボックスを使用して、ACL オブジェクトのアクセス コントロール エントリ（ACE）を定義します。このページから、テーブル内の ACE と ACL オブジェクトの順序の変更、ACE と ACL オブジェクトの追加、編集、削除を行うことができます。

ダイアログボックスのタイトルは、作成する ACL のタイプ（拡張、標準、または Web タイプ）を示します。ダイアログボックスは基本的には同じであり、ACEテーブルに表示されるカラムだけが異なります。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [アクセス制御リスト（Access Control Lists）] を選択します。作成する ACL オブジェクトのタイプのタブを選択し、作業領域内で右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- 拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）
- 標準アクセス コントロール リスト オブジェクトの作成 （360 ページ）
- Web アクセス コントロール リスト オブジェクトの作成 （361 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

フィールド リファレンス

表 *59 : [Add Access List]/[Edit Access List]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明

Access Control Entry table	ACL の一部であるアクセス コントロール エントリ（ACE）および ACL オブジェクト。テーブルには、エントリまたはオブジェクトの名前、説明、オプション、サービス、およびエントリのその他の属性が表示されます。
	
	[Permit] カラムで、緑色のチェックマークはエントリがトラフィックを許可することを示し（通常、トラフィックは定義しているサービスについて一致と見なされます）、スラッシュの入った赤色の丸はトラフィックが拒否されることを示します（通常、トラフィックは不一致と見なされ、定義しているサービスは拒否されたトラフィックには適用されません）。
	
	送信元アドレスおよび（該当する場合）宛先アドレスは、ホスト IP アドレス、ネットワーク アドレス、またはネットワーク/ホスト ポリシー オブジェクトです。
	
	• ACE を追加するには、[Add] ボタンをクリックし、作成するタイプの ACL のダイアログボックスに入力を行います。
	  • [Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス （367 ページ）
	  • [Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス （370 ページ）
	  • [Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス （372 ページ）
	
	• ACE を編集するには、ACE を選択し、[Edit] ボタンをクリックします。
	
	• ACE を削除するには、ACE を選択し、[Delete] ボタンをクリックします。
	
	• エントリの位置を変更するには、エントリを選択し、必要に応じて上下の矢印ボタンをクリックします。エントリは上から下へ評価されるため、正しく位置付けることが意図した結果を得るために重要です。

カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用（304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックス

[Add Extended Access Control Entry]/[Edit Extended Access Control Entry] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトを拡張 ACL オブジェクトに追加します。

ナビゲーション パス

拡張 ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）から、ACEテーブルの[追加（Add）]ボタンをクリックするか、行を選択して[編集（Edit）]ボタンをクリックします。

関連項目

- 拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 *60 : [Add Extended Access Control Entry]/[Edit Extended Access Control Entry]* ダイアログボックス

要素	説明
タイプ	追加するエントリのタイプ。ダイアログボックスのフィールドは、選択に応じて変わります。 • [Access Control Entry]：ACE を定義します。 • [ACL Objects]：既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>]ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して[<<]をクリックします。選択されたオブジェクト リスト内のオブジェクトを編集することもできます。

要素	説明
操作	エントリで定義されトラフィックに対するアクション： • [Permit]：この ACL に関連付けられているサービスはこのトラフィックに適用されます。つまり、トラフィックはサービスの使用が許可されます。 • [Deny]：この ACL に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACL と比較されます。そのトラフィックが ACL 内の permit エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
送信元 接続先	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 次のアドレスタイプを組み合わせて入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 • ネットワーク/ホストオブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 （ASA 8.4(2) 以降のみ）FQDN ネットワーク/ホストオブジェクトを選択して、完全修飾ホスト名に基づいてトラフィックを選択できます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。

要素	説明
Users	（ASA 8.4(2) 以降のみ）ルールの Active Directory（AD）ユーザー名、ユーザーグループ、またはアイデンティティ ユーザー グループ オブジェクト（使用する場合）。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。項目をカンマで区切って複数の値を入力できます。 次の値を組み合わせて入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。 [選択（Select）] をクリックしてリストからオブジェクト、ユーザー、またはユーザーグループを選択するか、新しいオブジェクトを作成します。 詳細については、以下を参照してください。 • ポリシーでのアイデンティティ ユーザの選択 （835 ページ） • アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ） • アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）
サービス	動作対象のトラフィック タイプを定義するサービス。項目をカンマで区切って複数の値を入力できます。 サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明
[Advanced] ボタン	このボタンをクリックして、エントリのロギング オプションを定義します。 • PIX、ASA、および FWSM デバイスの場合、次の項目をイネーブルにすることができます。 • [Default logging]：パケットが拒否されると、メッセージ 106023 が生成されます。パケットが許可された場合、メッセージは生成されません。 • [Per ACE logging]：パケットが拒否されると、メッセージ 106100 が生成されます。メッセージのロギング重大度レベルおよびメッセージを生成する間隔（1 ～ 600 秒）を選択できます。 • IOS デバイスの場合、ロギングをイネーブルにすると、エントリと一致したパケットに関する情報メッセージがコンソールに送信されます。入力インターフェイスおよび送信元 MAC アドレスまたは VC をロギング出力に含めるように選択することもできます。

[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス

[Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトを標準 ACL オブジェクトに追加します。

ナビゲーション パス

標準 ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）から、ACE テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。

関連項目

- 標準アクセス コントロール リスト オブジェクトの作成 （360 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 61 : [Add Standard Access Control Entry]/[Edit Standard Access Control Entry] ダイアログボックス

要素	説明
タイプ	追加するエントリのタイプ。ダイアログボックスのフィールドは、選択に応じて変わります。 • [Access Control Entry]：ACE を定義します。 • [ACL Objects]：既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>] ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して [<<] をクリックします。選択されたオブジェクト リスト内のオブジェクトを編集することもできます。
操作	エントリで定義されトラフィックに対するアクション： • [Permit]：この ACL に関連付けられているサービスはこのトラフィックに適用されます。つまり、トラフィックはサービスの使用が許可されます。 • [Deny]：この ACL に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACL と比較されます。そのトラフィックが ACL 内の permit エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
ソース（Source）	トラフィックの送信元。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを組み合わせて入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビットマスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。
説明	（任意）オブジェクトの説明。
Log Option	トラフィックがエントリ基準を満たしたときにログ エントリを作成するかどうか。ACL ロギングによって、拒否されたパケットに対して syslog メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、拒否パケットが存在している必要があります。

[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックス

[Add Web Access Control Entry]/[Edit Web Access Control Entry] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトを Web タイプ ACL オブジェクトに追加します。

ナビゲーション パス

Web タイプ ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）から、ACE テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。

関連項目

- Web アクセス コントロール リスト オブジェクトの作成 （361 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 *62 : [Add Web Access Control Entry]/[Edit Web Access Control Entry]* ダイアログボックス

要素	説明
タイプ	追加するエントリのタイプ。ダイアログボックスのフィールドは、選択に応じて変わります。 • [Access Control Entry]：ACE を定義します。 • [ACL Objects]：既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>] ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して [<<] をクリックします。選択されたオブジェクト リスト内のオブジェクトを編集することもできます。
操作	エントリで定義されトラフィックに対するアクション： • [Permit]：この ACL に関連付けられているサービスはこのトラフィックに適用されます。つまり、トラフィックはサービスの使用が許可されます。 • [Deny]：この ACL に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACL と比較されます。そのトラフィックが ACL 内の permit エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。
Filter Destination	エントリがネットワーク フィルタ（ホストまたはネットワーク アドレス）を指定するか、URL フィルタ（Web サイト アドレス）を指定するか。ダイアログボックスのフィールドは、選択に応じて変わります。そのフィールドについては次で説明します。

要素	説明
[接続先（Destination）] （ネットワーク フィルタだけ）	トラフィックの宛先。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを組み合わせて入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。
ポート （ネットワーク フィルタだけ）	トラフィックが使用するポートを定義するポート番号またはポート リスト ポリシー オブジェクト（ポート ID を使用する場合）。項目をカンマで区切って複数の値を入力できます。 次のタイプを組み合わせて入力できます。 • ポート リスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいポート リスト オブジェクトを作成することもできます。 • ポート番号。80 など。 • ポート範囲。80 ～ 90 など。
URL Filter （URL フィルタだけ）	トラフィックの Universal Resource Locator（URL）つまり Web アドレス。すべての値と一致するワイルドカードとして、アスタリスクを使用できます。たとえば、http://*.cisco.com は、cisco.com ネットワーク上のすべてのサーバと一致します。任意の有効な URL を指定できます。
ログ	このエントリに対して使用するロギングのタイプ。 • ログ エントリを作成しない場合は、[Log Disabled] を選択します。 • デバイスのデフォルト設定を使用する場合は、[Default] を選択します。 • 使用可能なその他のすべてのオプションでは、ロギングがイネーブルになり、使用されるログ レベルが指定されます。

要素	説明
ロギング間隔（Logging Interval）	ロギング メッセージの生成に使用される間隔（秒単位）。1～600。デフォルトは 300 です。このフィールドは、[Logging] フィールドでロギング レベルを選択した場合にだけ変更できます。
時間範囲	エントリに関連付けられる時間範囲を定義する時間範囲ポリシー オブジェクト。時間範囲によってデバイスへのアクセスが定義されます。時間範囲は、デバイスのシステムクロックによって異なります。詳細については、時間範囲オブジェクトの設定 （379 ページ）を参照してください。 オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しい時間範囲オブジェクトを作成することもできます。 （注） 時間範囲は、FWSM 2.x デバイスまたは PIX 6.3 デバイスではサポートされていません。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用（304 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

[Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）] ダイアログボックス

[ユニファイドアクセスコントロールエントリの追加（Add Unified Access Control Entry）]/[ユニファイドアクセスコントロールエントリの編集（Edit Unified Access Control Entry）] ダイアログボックスを使用して、アクセス コントロール エントリ（ACE）または ACL オブジェクトをユニファイド ACL オブジェクトに追加します。

ナビゲーション パス

拡張 ACL オブジェクトの [Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）から、ACE テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。

関連項目

- 統合アクセス制御リストオブジェクトの作成 （363 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

• セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 *63 : [Webアクセスコントロールエントリの追加（Add Web Access Control Entry）]/[Webアクセスコントロールエントリの編集（Edit Web Access Control Entry）]* ダイアログボックス

要素	説明
タイプ	エントリのタイプ。ダイアログボックスのフィールドは、選択した項目に応じて変化します。 • [Access Control Entry]：ACE を定義します。 • [ACLオブジェクト（ACL Objects）]：1 つ以上の既存の ACL オブジェクトを追加します。使用可能な ACL オブジェクトのリストが表示されます。追加するオブジェクトを選択し、[>>] ボタンをクリックして選択されたオブジェクトリストに移動します。オブジェクトを削除するには、オブジェクトを選択して [<<] をクリックします。選択されたオブジェクトリスト内のオブジェクトを編集することもできます。
操作	エントリで定義されトラフィックに対するアクション： • [許可（Permit）]：ACE に関連付けられているサービスはこのトラフィックに適用されます。つまり、このエントリで定義されたトラフィックはサービスの使用が許可されます。 • [拒否（Deny）]：ACE に関連付けられているサービスはこのトラフィックに適用されません。サービスに複数の ACL が設定されている場合、拒否されたトラフィックは、通常はリスト内の次の ACE と比較されます。そのトラフィックが ACL 内の許可エントリと一致しない場合、サービスはトラフィックに適用されません。トラフィックがネットワークからドロップされるかどうかは、サービスによって決まります。

要素	説明
ソース	このルールのトラフィックソースを指定します。ネットワークとホストを指定できます。次の1つ以上に対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 • [ネットワーク/ホスト（Networks/Hosts）]：さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイスオブジェクトをソースとして選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。これらのフィールドのいずれかに、項目をカンマで区切るか範囲を指定して、複数の値を入力します。 「All-Address」オブジェクトは、ルールを特定のホスト、ネットワーク、またはインターフェイスに制限しません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホストオブジェクト、インターフェイス、またはインターフェイス ロールの IPv4 または IPv6 アドレスです。 （注） （ASA 8.4.2 以降のみ）完全修飾ドメイン名（FQDN）は、FQDN ネットワーク/ホストオブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを入力することによってのみ指定できます。FQDN を直接入力することはできません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについて （391 ページ）、ポリシー定義中の IP アドレスの指定 （401 ページ）およびインターフェイス ロール オブジェクトについて （381 ページ）を参照してください。 （注） IPv6アドレスは、コンマ区切りの値のみで入力してください。IPv6アドレスが範囲として指定されている場合、設定のプレビューでエラーが表示されます。 すべての送信元、送信元SG、およびユーザの指定領域を組み合わせて、トラフィックの一致をすべてのソース定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックです。
送信元SG（Source SG）	（ASA 9.0 以降のみ）ACE の 1 つ以上の送信元セキュリティグループの名前またはタグ番号を入力または選択します（存在する場合）。セキュリティグループの詳細については、次を参照してください。 • ポリシーでのセキュリティグループの選択 （865 ページ） • TrustSec ベースのファイアウォールルールの設定 （866 ページ） • セキュリティ グループ オブジェクトの作成 （863 ページ）

要素	説明
Users	（ASA 8.4.2 以降のみ）ACE の Active Directory（AD）ユーザ名、ユーザグループ、またはアイデンティティ ユーザ グループ オブジェクトを入力するか選択します（存在する場合）。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。項目をカンマで区切って複数の値を入力できます。 次の値の任意の組み合わせを入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。 詳細については、以下を参照してください。 • ポリシーでのアイデンティティ ユーザの選択 （835 ページ） • アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ） • アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）
[接続先（Destination）]	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 （注） IPv6アドレスは、コンマ区切りの値のみで入力してください。IPv6アドレスが範囲として指定されている場合、設定のプレビューでエラーが表示されます。 この ACE のトラフィックの宛先、およびオプションで宛先セキュリティ グループ（ASA 9.0 以降のみ）を提供します。送信元エントリと同様に、次の 1 つ以上の宛先について、値またはオブジェクト名を入力するか、オブジェクトを選択できます。
宛先SG（Destination SG）	（ASA 9.0 以降のみ）ACE の 1 つ以上の送信元セキュリティグループの名前またはタグ番号を入力または選択します（存在する場合）。セキュリティグループの詳細については、次を参照してください。 • ポリシーでのセキュリティグループの選択 （865 ページ） • TrustSec ベースのファイアウォールルールの設定 （866 ページ） • セキュリティ グループ オブジェクトの作成 （863 ページ）

要素	説明
サービス	動作対象のトラフィック タイプを定義するサービス。項目をカンマで区切って複数の値を入力できます。 サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。サービスを入力する場合は、有効な値の入力を求められます。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
[Advanced] ボタン	このボタンをクリックして [詳細設定（Advanced）] ダイアログボックスを開き、ACE のログオプションを定義します。PIX、ASA、および FWSM デバイスの場合、次の項目をイネーブルにすることができます。 • [Default logging]：パケットが拒否されると、メッセージ 106023 が生成されます。パケットが許可された場合、メッセージは生成されません。 • [Per ACE logging]：パケットが拒否されると、メッセージ 106100 が生成されます。メッセージのロギング重大度レベルおよびメッセージを生成する間隔（1 ～ 600 秒）を選択できます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

時間範囲オブジェクトの設定

[Add Time Range]/[Edit Time Range] ダイアログボックスを使用して、時間範囲オブジェクトを作成、編集、またはコピーします。

時間ベースの ACL および一部のファイアウォール ルールを作成するときに使用する時間範囲オブジェクトを作成できます。機能は拡張 ACL と同様ですが、時間ベースの ACL では時間を考慮したアクセス コントロールが可能です。時間範囲が特定のルールに適用され、それらのルールは範囲で定義された特定の時間アクティブになります。たとえば、特定のタイプのアクセスを許可または阻止する通常の勤務時間のルールを実装できます。

また、VPN アクセスを週のうちの特定の時間に制限するように ASA ユーザ グループを定義する場合に、時間範囲オブジェクトを使用できます。詳細については、ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照してください。

時間範囲オブジェクトは、デバイスのシステムクロックに依存させることができますが、ネットワーク タイム プロトコル（NTP）同期を使用すると最適に動作します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]を選択し、次に、オブジェクトタイプセレクタから [時間範囲（Time Ranges）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 64 : [Time Range] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。
開始時刻（Start Time） 終了時間（End Time）	時間範囲オブジェクトの全体的な開始時刻および終了時刻。 • [Start Now]：展開の時刻を開始時刻として定義します。 • [Never End]：範囲の終了時刻を定義しません。 • [Start At]、[End At]：特定の開始日と開始時刻または終了日と終了時刻を定義します。カレンダー アイコンをクリックして、日付選択用のツールを表示します。24 時間形式（HH:MM）を使用して [Time] フィールドに時刻を入力します。
Recurring Ranges	全体的な開始時刻および終了時刻内で発生する繰り返し期間（ある場合）。たとえば、勤務時間を定義する時間範囲オブジェクトを作成する場合、全体的な範囲については [Start Now] および [Never End] を選択し、平日の 08:00 ～ 18:00 という繰り返し範囲を入力できます。 • 範囲を追加するには、[新しい繰り返し範囲（New Recurring Range）] ボタンをクリックし、[Recurring Ranges] ダイアログボックス （381 ページ）に入力します。 • 範囲を編集するには、その範囲を選択して [繰り返し範囲の編集（Edit Recurring Range）] ボタンをクリックします。 • 範囲を削除するには、その範囲を選択して [繰返し範囲の削除（Delete Recurring Range）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

[Recurring Ranges] ダイアログボックス

[Recurring Ranges] ダイアログボックスを使用して、時間範囲オブジェクトの一部として定義される繰り返し時間間隔を追加または編集します。必要な数の繰り返し範囲を定義できます。

ナビゲーション パス

[時間範囲の追加（Add Time Range）]/[時間範囲の編集（Edit Time Range）] ダイアログボックスに移動し、[繰り返し範囲（Recurring Ranges）] の下の [新しい繰り返し範囲（New Recurring Range）] ボタンをクリックするか、範囲を選択して [繰り返し範囲の編集（Edit Recurring Range）] をクリックします。時間範囲オブジェクトの設定 （379 ページ）を参照してください。

フィールド リファレンス

表 *65 : [Recurring Ranges]* ダイアログボックス

要素	説明
Specify days of the week and times during which this recurring range will be active	特定の曜日と時間に基づく繰り返し範囲を定義します。次の中から選択できます。 • 毎日 • 平日（Weekdays） • Weekends • [On these days of the week]：範囲に含める特定の日を選択します。 1 日のうちの開始時刻と終了時刻も選択します。デフォルトはすべての日です。
Specify a weekly interval during which this recurring range will be active	毎週の繰り返し範囲を定義します。開始日と開始時刻および終了日と終了時刻を選択します。たとえば、週の期間を日曜日に開始し、木曜日に終了できます。

インターフェイス ロール オブジェクトについて

インターフェイス ロール オブジェクトには次の用途があります。

- 複数のインターフェイスの指定：インターフェイス ロール オブジェクトを使用すると、各インターフェイスの名前を手動で定義することなく、複数のデバイス上の特定のインターフェイスにポリシーを適用できます。ほとんどのデバイスはインターフェイスについて標準的な命名ルールに従っているため、特定のインターフェイス タイプを示す命名パターンを定義し、そのパターンと一致するすべてのインターフェイスにポリシーを適用できます。

- ゾーン：インターフェイス ロール オブジェクトを使用して、ゾーンベースのファイアウォール ルール ポリシーでゾーンを定義できます。

たとえば、DMZ* という命名パターンでインターフェイス ロールを定義します。このインターフェイスロールをポリシーに含めると、そのポリシーは、選択したデバイス上の名前が「DMZ」で始まるすべてのインターフェイスに適用されます。結果として、たとえばすべての DMZ インターフェイスでアンチ スプーフィング チェックを有効にするポリシーを、該当するすべてのデバイス インターフェイスに 1 回のアクションで適用できます。インターフェイス ロールは、デバイス上の実際のインターフェイスのいずれかを参照できます。インターフェイスには、物理インターフェイス、サブインターフェイス、仮想インターフェイス（ループバック インターフェイスなど）があります。

インターフェイス ロールは、一方のインターフェイスと他方のポリシー間の間接エンティティとして機能します。このことにより、割り当てられたロールに基づいて、特定のデバイス インターフェイスにポリシーを適用できます。また、特定のインターフェイス タイプに対して使用されている命名ルールを変更する場合に、どのポリシーが変更を影響を受けるかを判別する必要がありません。インターフェイス ロールを編集するだけで済みます。

インターフェイス ロールは、新しいデバイスにポリシーを適用するときに特に役立ちます。追加するデバイスが既存のデバイスと同じインターフェイス命名方式を共有しているかぎり、追加割り当てを行わなくても、該当するポリシーをそれらに拡張できます。

Security Manager には、次の定義済みのインターフェイス ロールがあります。

- All-Interfaces：特定のデバイスで定義されているすべてのインターフェイスが含まれます。
- Internal：ネットワークの内側にある、特定のインターフェイスだけが含まれます。リストについてはオブジェクト定義を参照してください。
- External：ネットワークの外側にある、特定のインターフェイスだけが含まれます。リストについてはオブジェクト定義を参照してください。
- Self：いずれのインターフェイスも含まれません。Self インターフェイス ロールは、ゾーンベースのファイアウォール ルール ポリシーに固有です。Self ゾーンはルータ自体です。これを使用して、ルータから送信されたトラフィックまたはルータに送信されるトラフィックを識別できます。ルータを通過するトラフィックは含まれません。

次の項では、インターフェイス ロール オブジェクトを操作する方法について説明します。

- インターフェイス ロール オブジェクトの作成 （383 ページ）
- ポリシー定義中のインターフェイスの指定 （386 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （387 ページ）
- インターフェイスとインターフェイス ロール間の名前の競合の処理 （388 ページ）
- トラフィック ゾーンの管理 （1287 ページ）

インターフェイス ロール オブジェクトの作成

デバイス上の 1 つ以上のインターフェイスを表すインターフェイス ロール オブジェクトを作成できます。これらのロールは、インターフェイスまたはゾーンを必要とするポリシーを定義するときに使用できます。インターフェイス ロール オブジェクトを作成する場合、オブジェクトに含めるデバイスインターフェイスの命名パターンを定義する必要があります。インターフェイス ロールは、デバイス上の実際のインターフェイスのいずれかを参照できます。インターフェイスには、物理インターフェイス、サブインターフェイス、仮想インターフェイスがあります。

ヒント このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに、インターフェイス ロール オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）
- ポリシー定義中のインターフェイスの指定 （386 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （387 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- トラフィック ゾーンの管理 （1287 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [インターフェイスロール（Interface Roles）] を選択します。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Interface Role] ダイアログボックスが表示されます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。名前は最大 128 文字、説明は最大 1024 文字です。

ステップ 5 インターフェイス ロール オブジェクトの命名パターンを 1 つ以上入力します。名前は、インターフェイス、サブインターフェイス、およびその他の仮想インターフェイスの完全な名前または名前の一部です。複数の名前パターンを指定する場合は、カンマで区切ります。

次のワイルドカードを使用して、複数のインターフェイスに適用する名前パターンを作成できます。

- ピリオド（.）は、1 文字を表すワイルドカードとして使用します。ピリオドをパターン自体の一部として使用するには、ピリオドの前にバックスラッシュ（\）を入力します。

- アスタリスク（*）は、インターフェイス パターンの末尾にある 1 つ以上の文字を表すワイルドカードとして使用します。

たとえば、**DMZ*** には名前が「DMZ」で始まるすべてのインターフェイスが含まれ、**DMZ.** は DMZ1 や DMZ2 などのインターフェイスには一致しますが、DMZ10 には一致しません。

パターンにワイルドカードが含まれていない場合は、インターフェイスの名前と正確に一致する必要があります。たとえば、パターン **FastEthernet** は、パターンの最後にアスタリスクを含めない限り、FastEthernet0/1 とは一致しません。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

[Interface Role] ダイアログボックス

[Interface Role] ダイアログボックスを使用して、インターフェイス ロール オブジェクトを作成、コピー、または編集します。インターフェイス ロール オブジェクトには次の用途があります。

- 複数のインターフェイスの指定：インターフェイス ロール オブジェクトを使用すると、各インターフェイスの名前を手動で定義することなく、複数のデバイス上の特定のインターフェイスにポリシーを適用できます。
- ゾーン：インターフェイス ロール オブジェクトを使用して、ゾーンベースのファイアウォール ルール ポリシーでゾーンを定義できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから [インターフェイスロール（Interface Roles）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （387 ページ）
- ポリシー定義中のインターフェイスの指定 （386 ページ）

- インターフェイス ロール オブジェクトについて （381 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *66 : [Interface Role]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
Interface Name Patterns	このインターフェイス ロールに含める名前。名前は、インターフェイス、サブインターフェイス、およびその他の仮想インターフェイスの完全な名前または名前の一部です。複数の名前パターンを指定する場合は、カンマで区切ります。 （注） ファイアウォールデバイスの場合は、ハードウェアポート識別子（Ethernet0 など）ではなく、インターフェイスに割り当てられた名前（内部、外部、または DMZ など）を使用します。 次のワイルドカードを使用して、複数のインターフェイスに適用する名前パターンを作成できます。 • ピリオド（.）は、1 文字を表すワイルドカードとして使用します。ピリオドをパターン自体の一部として使用するには、ピリオドの前にバックスラッシュ（\）を入力します。 • アスタリスク（*）は、インターフェイス パターンの末尾にある 1 つ以上の文字を表すワイルドカードとして使用します。 たとえば、DMZ* には、名前が「DMZ」で始まるすべてのインターフェイスが含まれ、DMZ. は DMZ1 や DMZ2 などのインターフェイスには一致しますが、DMZ10 には一致しません。 パターンにワイルドカードが含まれていない場合は、インターフェイスの名前と正確に一致する必要があります。たとえば、パターン「FastEthernet」は、パターンの最後にアスタリスクを含めない限り、FastEthernet0/1 とは一致しません。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ポリシー定義中のインターフェイスの指定

インターフェイスの識別を必要とするポリシーを設定する場合、次に示すように、インターフェイスを指定するための複数のオプションがあります。

- インターフェイスの名前（Ethernet0 など）を手動で入力します。

ポリシー定義の一部としてサブインターフェイスを手動で指定するには、ピリオドの前にバックスラッシュ（\）を入力する必要があります。Ethernet0\.1 などのように入力します。

バックスラッシュなしでピリオドを入力すると、ピリオドは Security Manager によって 1 文字のワイルドカードとして処理されます。たとえば、Ethernet1/1.0 をアクセスルールの一部として定義する場合は、**Ethernet1/1\.0** と入力する必要があります。代わりに **Ethernet1/1.0** と入力すると、単独のピリオドはワイルドカードとして処理されるため、名前は Ethernet1/1.0 や Ethernet1/1/0 というインターフェイスと一致します。

- インターフェイス ロールの名前を手動で入力します。インターフェイス ロールの詳細については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
- インターフェイスまたはインターフェイス ロールをリストから選択します。[インターフェイス（Interfaces）] フィールドの横の [選択（Select）] をクリックすることにより、有効なインターフェイス名およびインターフェイスロールのリストが表示されます。サブインターフェイスは、名前の中のピリオドの前にバックスラッシュが付いて表示されます。

リストから選択することによって、エントリが有効であることを保証できます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

ポリシーで複数のインターフェイスが許可されている場合、エントリをカンマで区切ります。

ポリシーおよびオブジェクト セレクタでは、インターフェイスとインターフェイス ロールはアイコンによって区別されます。インターフェイスと同じ名前のインターフェイス ロールを作成する場合は、必要なものを正確に選択するように注意してください。次の表でアイコンについて説明します。

表 *67* : インターフェイスおよびインターフェイス ロールのアイコン

タイプ（Type）	アイコン
インターフェイス	
インターフェイス ロール ロールを編集できる場合は、鉛筆のイメージがアイコンに重なっています。	
ASA 8.3+デバイス上のグローバル「インターフェイス」。インターフェイス固有ではなくグローバルとして作成されたルールに対して使用されます。	

関連項目

- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- ファイアウォール デバイスのインターフェイスの設定 （2333 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）
- 単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用 （387 ページ）

単一のインターフェイス指定が許可されている場合のインターフェイス ロールの使用

インターフェイス ロール オブジェクトは、ロールの定義方法に応じて、デバイス上で定義されている実際のインターフェイスと一致する数が変化します。つまり、特定のデバイスについて、インターフェイスロールが 0 個、1 個、または複数個のインターフェイスと一致する場合があります。インターフェイス ロールをポリシーで使用すると、Security Manager によってロールはコマンドに変換されます。これらのコマンドによって、デバイス上で定義されている、ロールと一致するすべてのインターフェイスが設定されます。

ただし、多くのポリシーでは、単一のインターフェイス名を指定する必要があります。ポリシーによって単一のインターフェイス名が許可されている状況でインターフェイス ロールを使用する場合は、単一のインターフェイスと一致するようにインターフェイス ロールを定義する必要があります。デバイス上の複数のインターフェイスと一致するインターフェイス ロールを使用すると、Security Manager によってロールと一致するデバイス上の最初のインターフェイスが選択されますが、それが該当するインターフェイスではない場合があります（該当するインターフェイスの場合は適切に機能します）。

関連項目

- ポリシー定義中のインターフェイスの指定 （386 ページ）

- インターフェイス ロール オブジェクトについて （381 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）

インターフェイスとインターフェイス ロール間の名前の競合の処理

通常の状況では、デバイス上の実際のインターフェイスと同じ名前のインターフェイス ロールを設定できます。ポリシーを定義するときにオブジェクトセレクタを使用する場合（ポリシーのオブジェクトの選択 （288 ページ）を参照）、使用可能な選択肢としてインターフェイスとインターフェイス ロールの両方が表示され、いずれかを選択できます。ポリシーを定義するときにこの共通の名前を入力すると、Security Manager によって、インターフェイスではなくインターフェイス ロールがポリシーに自動的に関連付けられます。

ただし、次の状況では名前の競合が発生する可能性があります。

1. ポリシーを定義するときにインターフェイスの名前を入力します。
2. その後、同じ名前のインターフェイス ロールを作成します。
3. ポリシーを定義するときにこの名前を再度入力します。
4. [選択（Select）] をクリックしてオブジェクトセレクタを表示するか、[保存（Save）] をクリックしてポリシーを保存するか、一部の場合には、[OK] をクリックしてポリシーを更新します。

この一連のイベントが発生すると、インターフェイスを指定するかインターフェイス ロールを指定するかを選択できるように、[Interface Name Conflict] ダイアログボックスが自動的に開きます。ダイアログボックスには、競合が発生している名前だけが表示されます。

関連項目

- ポリシー定義中のインターフェイスの指定 （386 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

マップ オブジェクトについて

Policy Object Manager の Maps フォルダ内のオブジェクトを使用すると、インスペクション ルール、ゾーンベースのファイアウォール ルール、IPS、QoS、接続ルールの各ポリシーのクラス マップ、パラメータ マップ、およびポリシー マップを設定できます。これらのポリシーで使用できるマップのタイプは、デバイスで実行されているオペレーティング システムおよび特定のバージョン番号によって異なるため、通常は、ポリシーを設定するときにマップを設定するのが最適です。

ヒント　デバイスでは、設定するすべてのマップに一意の名前が必要です。たとえば、同じデバイス上の FTP と DNS クラス マップに対して同じ名前は使用できません。デバイスに対して同じ名前のマップを選択すると、Security Manager によって、重複する名前に数値のサフィックスが自動的に付加されます。dnsmap_1 などです。

Maps フォルダには、次のフォルダが含まれています。サブフォルダによって、マップはインスペクションに使用されるか Web コンテンツ フィルタリングに使用されるかに基づいて整理されます。

- Class Maps：動作対象のトラフィックを識別するために使用されるレイヤ 7 クラス マップ。
- Parameter Maps：ゾーンベースのファイアウォール ルール ポリシーで使用される設定を設定するパラメータ マップ、またはその他のマップ。
- Policy Maps：選択されたトラフィックに対して実行するアクションを識別するために使用されるレイヤ 7 ポリシー マップ。

Maps フォルダには、TCP マップ オブジェクト（レイヤ 4 オブジェクト）、正規表現オブジェクト、および正規表現グループ オブジェクトのエントリも含まれています。

次の項では、さまざまなタイプのマップについて詳細に説明します。

クラス マップ

クラス マップは、ポリシー マップの下位にあります。クラス マップをデバイス ポリシーで直接指定することはできません。代わりに、ポリシー マップを作成してクラス マップを組み込みます。クラス マップ自体では、インスペクション ルールまたはゾーンベースのファイアウォール ルールで対象とするトラフィックの一致条件が定義されます。

- ASA/PIX 7.2 以降、および FWSM デバイス：DNS、FTP、HTTP、IM、および SIP トラフィックのインスペクション用のクラスマップを作成できます。トラフィック一致をポリシー マップ オブジェクト内で直接定義するオプションもありますが、別々のクラス マップを作成すると、複数のポリシー マップで再利用できます。
- IOS 12.4(6)T 以降のデバイス：IM アプリケーション（AOL、ICQ、MSN Messenger、Windows Messenger、および Yahoo Messenger）、P2P アプリケーション（eDonkey、FastTrack、Gnutella、Kazaa2）、H.323、HTTP、IMAP、POP3、SIP、SMTP、Sun RPC のインスペクション用のクラスマップを作成できます。ローカル、N2H2、Trend、および Websense オブジェクトを使用して、Web コンテンツのフィルタリング用のクラス マップを作成することもできます。

ASA/PIX/FWSM に使用されるクラス マップとは異なり、別々のクラス マップを作成し、関連するポリシー マップから参照する必要があります。これらのポリシー マップは、ゾーンベースのファイアウォール インスペクション ルールまたはコンテンツ フィルタリング ルールで使用できます。詳細については、次の項を参照してください。

- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）

クラス マップを作成するには、次の項を参照してください。

- インスペクション ポリシーのクラス マップの設定 （1011 ページ）
- ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ）

クラス マップ、パラメータ マップ、およびポリシー マップで使用できる正規表現および正規表現グループを作成するには、次の項を参照してください。

- 正規表現の追加/編集 （1126 ページ）
- 正規表現グループの設定 （1125 ページ）

パラメータ マップ

パラメータ マップによって、ゾーンベースのファイアウォール インスペクション ルールまたはコンテンツ フィルタリング ルール、あるいは他のポリシー マップ オブジェクトで使用できる設定が定義されます。

- インスペクション：一般的なゾーンベースのファイアウォール ルール パラメータ用のインスペクション パラメータ マップ、または IM アプリケーション インスペクションで使用するプロトコル情報パラメータ マップを作成できます。
- コンテンツ フィルタリング：ローカル、N2H2、Trend、URL フィルタ、URLF Glob、Websense パラメータ マップを作成して、Web コンテンツ フィルタリングを定義できます。

ポリシー マップ

ポリシー マップを設定して、インスペクションのデフォルト アクションを変更したり、ゾーンベースのファイアウォール設定ポリシーで Web コンテンツ フィルタリングを設定したりすることができます。ポリシーマップは、通常、特別な処理を必要とするアプリケーションに適用されます。特別な処理は、埋め込み IP アドレス情報が存在したり、動的に割り当てられたポート上でトラフィックがセカンダリ チャネルを開く場合などに必要となります。

ポリシーマップによって、マップ内で指定された条件と一致するトラフィックに対して実行するアクションが識別されます。ほとんどのポリシー マップでは、クラス マップを参照することによってトラフィック一致条件を指定できます。ただし、一部のポリシーマップでは、ポリシー マップ内で一致基準を指定する必要があります。

次のタイプのポリシー マップを設定できます。

- インスペクションルール：インスペクションルールを設定する場合、Security Manager を使用して、次のアプリケーションのポリシーマップオブジェクトを作成できます。DCE/RPC、DNS、ESMTP、FTP、GTP、H.323、HTTP、IM、IP options、IPsec、NetBIOS、

SIP、Skinny、およびSNMP。詳細については、インスペクションのプロトコルおよびマップの設定 （1004 ページ）を参照してください。

- ゾーンベースのファイアウォール インスペクション ルール：ゾーンベースのファイアウォール インスペクション ルールを設定する場合、Security Manager を使用して、次のアプリケーションのポリシーマップオブジェクトを作成できます。H.323、HTTP、IM（AOL、ICQ、MSN Messenger、Windows Messenger、Yahoo Messenger を含む）、IMAP、P2P（eDonkey、FastTrack、Gnutella、Kazaa2 を含む）、POP3、SIP、SMTP、Sun RPC。詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）を参照してください。
- ゾーンベースのファイアウォール コンテンツ フィルタリング ルール：ゾーンベースのファイアウォール コンテンツ フィルタリング ルールを設定する場合、Security Manager を使用して Web フィルタ ポリシー マップを作成できます。HTTP トラフィックを検査するように HTTP ポリシー マップを設定することもできます。詳細については、ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）を参照してください。
- IPS、QoS、および接続ルール：PIX 7.x+ および ASA デバイスに固有のこのサービス ポリシーを設定する場合、TCP マップを使用して TCP インスペクションをカスタマイズできます。詳細については、「TCP マップの設定 （2971 ページ）」および「ファイアウォール デバイスでのサービス ポリシールールの設定 （2941 ページ）」を参照してください。

ネットワーク/ホストオブジェクトについて

ネットワーク/ホストオブジェクトは、ネットワーク、ホスト、またはこれらの両方を表す IP アドレスの論理集合です。

（注） Security Manager 4.4 では、IPv4 と IPv6 で別々のネットワーク/ホストオブジェクトが使用されなくなりました。単一の統合されたネットワーク/ホストオブジェクトがあり、IPv4 アドレス、IPv6 アドレス、またはその両方（グループオブジェクトの場合）を受け入れることができます。ただし、IPv4 アドレスと IPv6 アドレスが混在するグループオブジェクトは、ASA 9.0.1 以降のデバイスのポリシーにのみ割り当てることができます。詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 （14 ページ）を参照してください。

ネットワーク/ホストオブジェクトを作成するときに、オブジェクトのタイプを選択する必要があります。これにより、オブジェクトに含めることができるアドレスのタイプが定義および制限されます。

- グループ：次のタイプのアドレスの組み合わせを含めることができます。
  - ネットワークまたはサブネット。IPv4 アドレスとサブネットマスク、または IPv6 プレフィックスとプレフィックス長で指定されます。

- IPv4 または IPv6 ネットワーク アドレスの範囲。
- 個別のホスト。IPv4 または IPv6 アドレス（ドメイン名ではなく）で指定されます。
- その他のネットワーク/ホストオブジェクト。完全修飾ドメイン名（FQDN）オブジェクトを含む、既存のネットワーク/ホストオブジェクトのリストから選択されます。

- FQDN：（ASA 8.4(2) 以降のみ）このオブジェクトには、www.cisco.com などの単一ホストの完全修飾ドメイン名を含めることができます。デバイスは DNS を使用して FQDN をその IP アドレスに定期的に解決します。
- ホスト：このオブジェクトには、単一のホストの IPv4 または IPv6 アドレスを含めることができます（10.100.10.10、2001:DB8::0DB8:800:200C:417A など）。
- 属性：このオブジェクトには、1 つ以上のポリシーベースの VM 属性エージェントを含めることができます。これにより、ユーザはネットワークオブジェクトを定義することにより、VMware vCenter で管理している VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に従ってトラフィックをフィルタリングできます。各 VM 属性エージェントは、単一の vCenter サーバーと通信します。
- アドレス範囲：このオブジェクトには、IPv4 または IPv6 アドレスの範囲を 1 つ含めることができます。開始アドレスと終了アドレスは異ななる必要があり、開始アドレスが終了アドレスよりも小さい必要があります。
- ネットワーク：このオブジェクトには、単一の IPv4 ネットワークアドレスおよびサブネットマスク（10.100.10.0/24 など）、または単一の IPv6 プレフィックスおよびプレフィックス長（2001:DB8::/32 など）を含めることができます。

ネットワーク/ホストグループオブジェクトによって、スケーラブルなポリシーの管理が簡単になります。ネットワーク/ホストオブジェクトの連携機能を使用することで、ネットワークとともにポリシーを拡張できます。たとえば、ネットワーク/ホストオブジェクトに含まれているアドレスのリストを変更すると、変更は、その他のすべてのネットワーク/ホストオブジェクトおよびそのネットワーク/ホストオブジェクトを参照するポリシーに伝播します。

ホスト、ネットワーク、アドレス範囲オブジェクトには、ASA 8.3 以降のデバイスのポリシーで使用される際の特別な用途があります。これらのデバイスでは、ポリシーオブジェクト自体にオブジェクト NAT ルールを設定できます。その他のタイプのデバイスでオブジェクトを使用した場合、この NAT 設定は無視されます。

次の項では、ネットワーク/ホストオブジェクトを操作する方法について説明します。

- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）
- ネットワーク/ホストオブジェクトの作成 （394 ページ）
- 未指定ネットワーク/ホストオブジェクトの使用 （400 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- VM 属性ポリシー （403 ページ）

連続および不連続ネットワーク マスク（IPv4 アドレスに対応）

ネットワーク マスクによって、IPv4 アドレスのどの部分でネットワークを識別し、どの部分でホストを識別するかが決定されます。IP アドレスと同様に、マスクは 4 つのオクテットで表されます（オクテットは、0 ～ 255 の範囲の 10 進数に相当する 8 ビットの 2 進数です。）マスクの特定のビットが 1 の場合、IP アドレスの対応するビットはアドレスのネットワーク部分にあり、マスクの特定のビットが 0 の場合、IP アドレスの対応するビットはホスト部分にあります。

標準の（つまり、連続した）ネットワーク マスクは、0 個以上の 1 で始まり、そのあとに 0 個以上の 0 が続きます。このようなネットワーク マスクは、連続した IP アドレス範囲で構成されるネットワークを表すため、連続と見なされます。たとえば、ネットワーク 192.168.1.0/255.255.255.0 には、192.168.1.0 ～ 192.168.1.255 の範囲のすべての IP アドレスが含まれます。

次の表に、一般的に使用される標準のネットワーク マスクを表すさまざまな方式を示します。

表 *68 :* 標準のネットワーク マスク

ドット付き 10 進表記	Classless Inter-Domain Routing（CIDR）表記
255.0.0.0	/8
255.255.0.0	/16
255.255.255.0	/24
255.255.255.255	/32

たとえば、255.255.255.0 は、IP アドレスの最初の 3 つのオクテット（24 ビット、または CIDR 表記で /24）が 1 で構成され、ネットワークを示します。最後のオクテットは 0 で構成され、ホストを示します。

不連続ネットワーク マスク

非標準の（つまり、不連続の）ネットワーク マスクは、連続フォーマットに準拠しないマスクです。たとえば、10.0.1.1/255.0.255.255 は、オクテット 1、3、および 4 と正確に一致するアドレスを照合するが、オクテット 2 については任意の値が受け入れられることを示します。

不連続ネットワーク マスクは通常はネットワーク設定で使用しませんが、特定のコマンド用に使用する場合があります。アクセス コントロール リスト（ACL）を定義するときのフィルタリング コマンドなどです。Security Manager では、非標準のネットワーク マスクは、非標準のネットワーク マスクの使用が CLI コマンドによってサポートされているポリシーで使用できます。不連続ネットワーク マスクがサポートされていないポリシーで不連続ネットワーク マスクを定義しようとすると、エラーが表示されます。

ネットワーク マスクと検出

検出中に、Security Manager は、ネットワーク/ホスト オブジェクトを Policy Object Manager に定義されている既存の同等のオブジェクトと照合しようとします。

- 連続ネットワーク マスクの場合：標準のネットワークだけを含む 2 つのネットワーク/ホスト オブジェクトが同じ IP アドレスのセットで構成されている場合、同等と見なされます。
- 不連続ネットワーク マスクの場合：標準のネットワークが同じ IP アドレスのセットで構成され、非標準のネットワークが構文的に同等の場合にだけ、2 つのネットワーク/ホスト オブジェクトは同等と見なされます。

ネットワーク マスクの表示方法

ドット付き 10 進表記を使用して連続ネットワーク マスクと不連続ネットワーク マスクの両方を入力できますが、すべての連続ネットワーク マスクは CIDR 表記に変換されます。このことにより、ドット付き 10 進表記だけで表示される不連続ネットワーク マスクと区別しやすくなります。

関連項目

- ネットワーク/ホストオブジェクトの作成 （394 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- 未指定ネットワーク/ホストオブジェクトの使用 （400 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

ネットワーク/ホストオブジェクトの作成

ネットワーク、個別のホスト、または両方のグループを表すネットワーク/ホストオブジェクトを作成できます。ネットワーク/ホストオブジェクトを作成するときは、オブジェクトのタイプ（グループ、ホスト、FQDN、ネットワーク、属性、アドレス範囲）を選択する必要があります。作成後は、オブジェクト タイプを変更できません。

ヒント このオブジェクトタイプを使用するポリシーまたはオブジェクトを定義するときに、ネットワーク/ホストオブジェクトを作成できます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

ロールにマップされた変更権限を持っている場合にのみ、NAT オブジェクトを指定できます。

関連項目

- ネットワーク/ホストオブジェクトについて （391 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- VM 属性ポリシー （403 ページ）

- 未指定ネットワーク/ホストオブジェクトの使用 （400 ページ）
- ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （427 ページ）

ステップ 1 [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。詳細については、 Policy Object Manager （290 ページ）を参照してください。

ステップ 2 オブジェクトタイプセレクタから [ネットワーク/ホスト（Networks/Hosts）] を選択します。

ステップ 3 ウィンドウの下部にある [新規オブジェクト（New Object）] ボタンをクリックし、次のタイプのネットワーク/ホスト オブジェクトのいずれかを選択して [Add Network/Host]/[Edit Network/Host] ダイアログボックス（395 ページ）を開きます。作業領域で右クリックして [新規オブジェクト（New Object）] を選択し、次のオプションのいずれかを選択してダイアログボックスを開くこともできます。

- [グループ（Group）]：1 つ以上のエントリを持つオブジェクトを作成します。ネットワーク、ホスト、アドレス範囲、または他のネットワーク/ホストオブジェクト（FQDN オブジェクトを含む）の組み合わせを含めることができます。
- [FQDN]：（ASA 8.4(2) 以降のみ）www.cisco.com などの単一ホストの完全修飾ドメイン名を持つオブジェクトを作成します。
- [ホスト（Host）]：単一のホストアドレス（10.100.10.10（IPv4）、2001:DB8::12ab:5689（IPv6）など）を持つオブジェクトを作成します。
- [属性（Attribute）]：（ASA 9.7.1以降のみ）ネットワークオブジェクトを定義して、VMware vCenter で管理している VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に従ってトラフィックをフィルタリングします。
- [アドレス範囲（Address Range）]：単一のアドレス範囲（10.100.10.1-10.100.10.255 など）を持つオブジェクトを作成します。
- [ネットワーク（Network）]：単一のネットワークアドレス（10.100.10.0/24、2001:DB8::/32 など）を持つオブジェクトを作成します。

ヒント ホスト、ネットワーク、およびアドレス範囲オブジェクトについては、ASA 8.3 以降のデバイスのオブジェクト NAT 規則を設定することもできます。その他のデバイスでは NAT 設定は無視されます。

ステップ 4 [Add Network/Host]/[Edit Network/Host] ダイアログボックス （395 ページ）に、適切な情報を入力します。

[Add Network/Host]/[Edit Network/Host] ダイアログボックス

[Add Network/Host]/[Edit Network/Host] ダイアログボックスを使用して、ネットワーク/ホストオブジェクトを表示、作成、または編集します。ダイアログボックスのタイトル、コンテンツ

および外観は、作成するネットワーク/ホストオブジェクトのタイプ（グループ、FQDN、ホスト、属性、アドレス範囲、またはネットワーク）によってもいくらか異なります。FQDN オブジェクトには、ASA 8.4.2 以降のデバイスが必要です。属性オブジェクトには、ASA 9.7.1 以降のデバイスが必要です。グループタイプでは、複数の定義を入力できるため、ネットワーク、ホスト、および他のネットワーク/ホストオブジェクトの集合にすることができますが、他のタイプでは単一の定義のみを入力できます。

[ホスト（Host）]、[ネットワーク（Network）]、および [アドレス範囲（Address Range）] バージョンのダイアログボックスには、[全般（General）] と [NAT] の 2 つのタブ付きパネルオプションがあります。次の表で、[全般（General）] パネルのオプションと、タブのないバージョンのダイアログボックスについて説明します。 NAT オプションについては [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）で説明されています。

（注） Security Manager 4.4 では、IPv4 と IPv6 で別々のネットワーク/ホストオブジェクトが使用されなくなりました。単一の統合されたネットワーク/ホストオブジェクトがあり、IPv4 アドレス、IPv6 アドレス、またはその両方（グループオブジェクトのみの場合）を受け入れることができます。ただし、IPv4 アドレスと IPv6 アドレスが混在するグループオブジェクトは、ASA 9.0.1 以降のデバイスのポリシーにのみ割り当てることができます。

ASA 8.3 以降のデバイスで使用する IPv4 ベースのホスト、ネットワーク、またはアドレス範囲オブジェクトを作成する場合や、ASA 9.0.1 以降のデバイスで使用する統合されていないホスト、ネットワーク、またはアドレス範囲オブジェクトを作成する場合は、ダイアログボックスの [NAT] タブでオブジェクト NAT ルールを設定することもできます。どちらの場合も、オブジェクト NAT を許可するには、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択する必要があります。[NAT] タブの参照情報については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）を参照してください。

加えて、アドレスを持たないオブジェクトを作成できます。このようなオブジェクトの場合、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択し、そのオブジェクトを使用するすべてのデバイスに対してオーバーライドを作成する必要もあります。未指定アドレスの使用の詳細については、未指定ネットワーク/ホストオブジェクトの使用 （400 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから [ネットワーク/ホスト（Networks/Hosts）] を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連ボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- ネットワーク/ホストオブジェクトの作成 （394 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- Policy Object Manager （290 ページ）
- ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （427 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 *69 : [*ネットワーク/ホスト（*Networks/Hosts***）*]* ダイアログボックス（*[*全般（***General***）*]* タブ）**

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 **ヒント** ホスト、アドレス範囲、またはネットワーク オブジェクトの NAT を設定する場合は、このオプションを選択する必要があります。NAT 設定はデバイスのオーバーライドとして作成され、オブジェクト内には保持されません。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。
グループオブジェクトのオプション	

要素	説明
[使用可能なネットワーク/ホスト（Available Networks/Hosts）] [グループ内のメンバー（Members In Group）] [IPアドレスをカンマで区切って入力（Type in comma separated IP addresses）]	[グループ内のメンバー（Members In Group）] リストには、オブジェクトに含まれるネットワーク、ホスト、および他のネットワーク/ホストオブジェクトが表示されます。リストに入力するには、次のいずれかの組み合わせを実行します。 • [既存のネットワーク/ホスト（Existing Networks/Hosts）] リストで1つ以上のアドレス、属性、FQDN、グループ、ホスト、ネットワークの各オブジェクトを選択し、リスト間の [>>] ボタンをクリックします。 • [IPアドレスをカンマで区切って入力（Type in comma separated IP addresses）] フィールドに 1 つ以上の IP アドレスを入力し、リスト間の [>>] ボタンをクリックします。複数のアドレスをカンマで区切ります。これらは [メンバー（Members）] リストに別々の行として追加されます。 IPv4 アドレスの場合、ホストアドレス、ネットワークアドレス（/ 文字のあとにサブネットマスクを入力。10.100.10.0/24 など）、またはアドレスの範囲（開始アドレスと終了アドレスをハイフンで区切り、オプションでサブネットマスクを指定）を含めることができます。 IPv6 アドレスの場合、ホストアドレス、ネットワークアドレス（/ 文字のあとにプレフィックスを入力。2001:DB8::/32 など）、またはアドレスの範囲（2001:DB8::1-2001:DB8::100 など）を含めることができます。 詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 • [グループ内のメンバー（Members In Group）] リストから項目を削除するには、項目を選択し、該当する [<<] ボタンをクリックして、項目を元の場所に戻します。一度に複数の項目を選択して削除できます。 （注） IPv4アドレスとIPv6アドレスが混在するグループオブジェクトは、ASA 9.0.1 以降のデバイスのポリシーにのみ割り当てることができます。
FQDN オブジェクトのオプション	

要素	説明
[FQDN] [FQDNタイプ（FQDN Type）]	単一のホストの完全修飾ドメイン名（たとえば somehost.cisco.com など）。 FQDN タイプは、指定されたドメインにマッピングされる IP アドレスのタイプを指定します（[IPv4のみ（IPv4 Only）]、[IPv6のみ（IPv6 Only）]、またはデバイス固有のデフォルトが適用される [デフォルト（Default）]）。すべての非 ASA デバイスおよび 9.0.1 より前の ASA デバイスの場合、デフォルトは IPv4 です。
ホストオブジェクトのオプション	
IPアドレス	オブジェクトに含める単一ホストの IPv4 または IPv6 アドレス。
属性オブジェクトのオプション	
エージェント名（Agent Name） タイプ（Type） 値	VM 属性エージェント名。VM 属性エージェントのリストから選択するか、新しい VM 属性エージェントを追加します。 [VM属性エージェントタイプ（VM Attribute Agent Type）] は 128 文字以下にする必要があります。 [VM属性エージェント値（VM Attribute Agent Value）] は 128 文字以下にする必要があります。 （注） ユーザーは、一連の VM にカスタム属性のタイプと値を割り当てて、共通のユーザー定義の特性を持つ一連の VM に共通のポリシーセットを適用できます。
アドレス範囲オブジェクトのオプション	
開始 IP アドレス 終了 IP アドレス	アドレスの範囲を定義する最初と最後の IP アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
ネットワークオブジェクトのオプション	
IPアドレス [ネットマスク/プレフィックス（Net Mask/Prefix）]	ネットワークを表す IPv4 または IPv6 アドレス（たとえば 10.100.10.0 または 2001:DB8::/32 など）。 IPv4 アドレスを入力した場合は、そのサブネットマスクを [ネットマスク/プレフィックス（Net Mask/Prefix）] フィールドに入力します。マスクは、24（スラッシュなし）などの CIDR 形式、または 255.255.255.0 などのドット付き 10 進法形式のいずれかで入力できます。 IPv6 アドレスを入力した場合は、そのプレフィックス長を [ネットマスク/プレフィックス（Net Mask/Prefix）] フィールドに入力します。

未指定ネットワーク/ホストオブジェクトの使用

ネットワーク/ホストオブジェクトを定義するときに、[アドレス（address）] フィールドをブランクのままにして、値が未指定のネットワーク/ホストオブジェクトを作成できます。値が未指定のネットワーク/ホストオブジェクトでは、それらを使用するすべてのデバイスでオーバーライドを作成する必要があります。

値が指定されていないネットワーク/ホストオブジェクトを使用する利点は、そのオブジェクトを使用するすべてのデバイスで、デバイスレベルのオーバーライドを作成せずに変更を送信すると、Security Manager がエラーを表示することです。対照的に、プレースホルダ値（10.10.10.10 など）でグローバルオブジェクトを定義する場合、オーバーライドの定義に失敗すると、そのグローバル値が誤って展開される可能性があります。

次の手順では、値が未指定のネットワーク/ホストオブジェクトを作成および導入する方法について説明します。

関連項目

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- ネットワーク/ホストオブジェクトの作成 （394 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

ステップ 1 ネットワーク/ホストオブジェクトを作成します。次の点に注意します。

- [アドレス（address）] フィールドをブランクのままにします（Members In Group、IP Address、Net Mask/Prefix、FQDN、または Start IP Address、End IP Address など）。
- [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] チェックボックスをオンにします。

詳細については、 ネットワーク/ホストオブジェクトの作成 （394 ページ）を参照してください。

ステップ 2 オブジェクトを使用する各デバイスのオーバーライドを作成します。

a) [ネットワーク/ホスト（Networks/Hosts）] テーブルのオブジェクトの [オーバーライド（Overridable）] カラムで、緑色のチェックマークをクリックして、[Policy Object Overrides] ウィンドウ （314 ページ）を開きます。

b) [オーバーライドの作成（Create Override）] ボタンをクリックし、オーバーライドを作成するデバイスを選択して、[アドレス（address）] フィールドの値を定義します。この時点で、このオーバーライド値は選択したすべてのデバイスに適用されます。詳細については、複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）を参照してください。

c) [Policy Object Overrides] ダイアログボックスで各デバイスをダブルクリックし、そのデバイスが必要とする値のアドレス フィールドを変更します。

ステップ 3 このオブジェクトを必要とするポリシーを定義します。次の 2 つの方式のいずれかを使用できます。

- デバイス ビューで、1 つのデバイス上でポリシーを定義し、ポリシーを共有し、ポリシーを他のデバイスに割り当てます。ローカル ポリシーの共有 （262 ページ）およびデバイス ビューまたは Site-to-Site VPN Manager における共有ポリシー割り当ての変更 （272 ページ）を参照してください。
- ポリシー ビューで、共有ポリシーを作成し、[Assignments] タブを使用してポリシーを他のデバイスに割り当てます。ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

（注） 値が未指定のネットワーク/ホストオブジェクトを参照するネットワーク/ホストグループオブジェクトを作成できます。オブジェクトを含むポリシーをデバイスに割り当てる前に、デバイスレベルのオーバーライドを作成する必要はありません。

ポリシー定義中の IP アドレスの指定

多くのポリシーおよびポリシー オブジェクトでは、ホストまたはネットワークの IP アドレスを入力する必要があります。一部のポリシーまたはオブジェクトについては、1 つのホストだけ、または1つのネットワークだけを入力する必要があります。その他のポリシーまたはオブジェクトについては、ホストとネットワークの組み合わせを入力できます。状況に合わないアドレスを入力または選択することはできません。

次に、IPv4およびIPv6アドレスの両方に使用できるすべての形式の説明を示します。ただし、特定のポリシーやオブジェクトでは使用できない形式もあります（たとえば、インターフェイスロールは、非常に限定された数のポリシーでのみアドレス指定として使用できます）。ポリシーまたはオブジェクトで許可されている場合、複数のアドレスをカンマで区切って入力できます。

- ネットワーク/ホストオブジェクト。オブジェクトの名前を入力するか、または [選択（Select）]をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホストオブジェクトを作成することもできます

（注） 完全修飾ドメイン名（FQDN）を指定するには、FQDNネットワーク/ホストオブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを使用する必要があります。FQDN を直接入力することはできません。

- v4 または v6 形式のホスト IP アドレス。
  - 完全な IPv4 アドレス（10.10.10.100 など）
  - 8 つのコンポーネントすべてを示す完全な IPv6 アドレス。たとえば、2001:DB8:0:0:0DB8:800:200C:417A のように使用します。個々のフィールドに先行ゼロを含める必要はありません。Security Manager では、アドレスを可能な限り圧縮形式に変換します。

- 圧縮 IPv6 アドレス。フィールドのグループは 2 つのコロン（::）で置き換えられます。IPv6 アドレスには、通常、連続するゼロの 16 進フィールドが含まれます。IPv6 アドレスの先頭、中間、または末尾にある連続した 0 の 16 進フィールドを 2 つのコロン（::）を使用して圧縮すると、IPv6 アドレスが扱いやすくなります（2 つのコロンは連続した 0 の 16 進フィールドを表します）。IPv6 アドレスで :: は最大 1 回しか使えません。たとえば、2001:DB8::0DB8:800:200C:417A のように使用します。未指定のアドレス 0:0:0:0:0:0:0:0 は :: として表すことができます。ループバック アドレスは ::1 です。
- IPv4 アドレスの IPv6 表現。IPv4/IPv6 混合環境では、IPv4 アドレスを別の IPv6 形式（x:x:x:x:x:x:d.d.d.d）で表現できます（x は最初の 6 つのフィールドの 16 進値を示し、d はピリオドで区切られたオクテットで表した IPv4 アドレスを示します）。最初の 6 つのフィールドはすべて 0、::FFFF、または 2001:DB8:: のいずれかです。たとえば、0:0:0:0:0:0:10.1.68.3 は圧縮形式では ::10.1.68.3、0:0:0:0:0:FFFF:10.1.68.3、または 2001:DB8::10.1.68.3 になります。

- IPv4 または IPv6 形式のネットワークアドレス：
  - IPv4 アドレス（サブネットマスクを含む）。CIDR 形式（10.10.10.0/24）またはドット付き 10 進法形式（10.10.10.0/255.255.255.0）で指定。
  - IPv6 アドレス。IPv4 の CIDR 表記と同様の方法で指定する 10 進形式のプレフィックス長を含む（/64 など）。数字は、プレフィックスを構成する左端の連続したアドレス ビットの数を指定します。たとえば、2001:DB8:0:CD30::/60 のように使用します。

（注） 2001:DB8:0:CD30::/60 を 2001::CD30:0:0:0:0/60 のように入力することもできます。ただし、末尾の 0 を圧縮する方法を推奨します。Security Manager では、アドレスを 2001:DB8:0:CD30::/60 に変換します。

IPv6 アドレッシングの詳細については、IETF RFC 4291、IP Version 6 Addressing Architecture [英語]（http://www.ietf.org/rfc/rfc4291.txt）を参照してください。

- IP アドレスの範囲。最初のアドレスと最後のアドレスはハイフンで区切ります。この範囲は、ポリシーで要求されていないかぎり、1 つのサブネット内である必要はありません。

CIDR 形式のプレフィックスやサブネットマスクを含めることもできます。例：2001:db8::1 ～ 2001:db8::2/64 または 10.10.10.100 ～ 10.10.10.200/24。

- 10.10.0.10/255.255.0.255 形式の IPv6 アドレスのパターン。この場合のマスクは不連続なビットマスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。
- インターフェイス ロール オブジェクト（まれな場合）。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します（オブジェクト タイプとして [インターフェイスロール（Interface Role）] を選択する必要があります）。インターフェイス ロールを使用する場合は、選択したインターフェイスの IP アドレスを

指定した場合と同様にルールが動作します。デバイスに割り当てられる IP アドレスを把握できないため、DHCP を経由してアドレスを取得するインターフェイスの場合に有効です。詳細については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

ネットワーク/ホストオブジェクトを作成するか、ポリシーの一部として IP アドレスを定義すると、Cisco Security Manager によって、アドレスの構文が正しいこと、および必要に応じてマスクやプレフィックスが入力されていることが検証されます。たとえば、ホストを必要とするポリシーを定義する場合、マスクやプレフィックスを入力する必要はありません。ただし、サブネットを必要とするポリシーを定義する場合、マスクやプレフィックスとともにアドレスを入力するか、マスクやプレフィックスが定義されたネットワーク/ホストオブジェクトを選択する必要があります。

関連項目

- ネットワーク/ホストオブジェクトの作成 （394 ページ）
- 連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）
- 未指定ネットワーク/ホストオブジェクトの使用 （400 ページ）
- Policy Object Manager （290 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

VM 属性ポリシー

VMware ESXi 環境の 1 つ以上の仮想マシン（VM）に関連付けられている属性に基づき、ネットワークオブジェクトを定義し、トラフィックをフィルタリングできます。この環境は、VMware vCenter によって管理されます。ユーザは、ESXi 環境内の VM に属性を割り当て、属性エージェントを設定できます。属性エージェントは、HTTPS および要求を使用して vCenter または単一の ESXi ホストに接続し、特定の属性を ESXi VM のプライマリ IP アドレスに関連付ける 1 つ以上のバインディングを取得します。

1 つの ASA では複数の属性エージェントを定義でき、それぞれを異なる vCenter と通信させるか、または 複数の属性エージェントを同じ vCenter と通信させることができます。

これにより、ユーザはアクセス制御リスト（ACL）を定義して、1 つ以上の属性を共有する VM のグループからのトラフィックにポリシーを割り当てることができます。この機能は、VM 属性に基づくポリシーと呼ばれます。

VM 属性機能は、すべてのハードウェア プラットフォームと、ESXi、KVM または HyperV ハイパーバイザで動作するすべての ASAv プラットフォームでサポートされます。VM 属性は、ESXi ハイパーバイザ上で動作する VM からのみ取得できます。

（注） ASA では、属性または属性タイプという用語を使用して、監視対象の特性を表します。VMWare では、同じ特性に対してプロパティという用語を使用します。これらの用語は同義で使用される場合があります。

VM 属性エージェントと vCenter 間の通信

VM 属性エージェントと vCenter の間で交換されるメッセージには、プロパティリクエストとバインド更新の 2 種類があります。

- プロパティリクエスト：これは、ASA から vCenter Server の IP アドレスに送信される HTTPS メッセージであり、設定されている属性エージェントの属性に関連付けられたネットワークオブジェクトに現在設定されている属性タイプの完全なリストを示します。このメッセージには、vCenter への接続を認証するために必要な SSL ログイン情報が含まれています。vCenter は、対応する HTTPS 応答で応答します。
- バインド更新：これは、1 つ以上の VM の属性が変更されるたびに、vCenter から ASA に送信される非同期 HTTPS メッセージです。各バインド更新は、属性の変更を報告する VM の IP アドレスによって識別されます。複数の属性が 1 つのエージェントによってモニターされている場合、1 件のバインド更新に各 VM のすべてのモニター対象属性の現在の値が含まれます。エージェントによってモニターされている特定の属性が、ある VM には設定されていない場合、その VM のバインドには空の属性値が含まれます。ある VM にモニター対象の属性が設定されていない場合、vCenter はバインド更新を ASA に送信しません。

属性エージェントが新しい属性タイプを含むプロパティリクエストを発行すると、vCenter は、その属性タイプが設定されている各 VM に関するバインド更新で応答します。これ以降、VM で属性値が追加または変更されると、vCenter だけが新しいバインドを発行します。

属性エージェントの状態

属性エージェントの状態には、接続状態とエージェント状態の 2 種類があります。

- 接続状態：これは、属性エージェントが現在 vCenter と接続しているかどうかを示します。

接続状態（Connection State）	説明
ホストクレデンシャルなし（No Host Credentials）	ユーザは host サブコマンドを使用して vCenter ホストのクレデンシャルを入力していません。または、エージェントを引き続き使用しているネットワークオブジェクトが存在しているときに、エージェントが no attribute source-group コマンドを使用して削除されています。

接続状態（Connection State）	説明
切断（Disconnected）	エージェントにはホストクレデンシャルが定義されていますが、現在 vCenter と接続していません。ASA がキープアライブパケットに対する HTTP 200 応答を受信すると、接続が確立されます。
コネクテッド	エージェントは、vCenter から最新のキープアライブ パケットに対する応答を受け取りました。
無効なホストクレデンシャル（Invalid Host Credentials）	エージェントは、vCenter に接続してプロパティリクエストを発行しようとしましたが、ユーザ名またはパスワード（またはその両方）が正しくなかったため、リクエストは拒否されました。エージェントは、新しいクレデンシャルが入力されるまでこの状態を維持します。入力された時点で、vCenter からキープアライブ応答を受信するまで、切断状態に移行します。

- [エージェントの状態（Agent State）]：このエージェントを介して属性タイプをモニターするようにネットワークオブジェクトが構成されているかどうかを示します。

表 *70*：エージェント状態の表

エージェント状態（Agent State）	説明
非アクティブ	現在、エージェントには属性が設定されていません。
Active	エージェントには、1 つ以上の属性が設定されています。 vCenter への接続がない場合でも、エージェントをアクティブにすることができます。

vCenter 仮想マシンの設定に関するガイドライン

VM 属性機能を利用するには、管理対象の仮想マシンがそれらの属性を vCenter サーバーで使用できるようにする必要があります。例として、いくつかの属性について説明します。

- summary.config.name：仮想マシンに関連付けられたユーザー定義の名前（例：VM-build-machine-1）
- summary.config.guestFullName：仮想マシンで実行されているゲスト OS の完全な名前（例：Red Hat Enterprise Linux 7（64 ビット））
- summary.config.annotation：仮想マシンのテキスト説明フィールド。

文字列の属性値（summary.config.annotation など）の場合、ネットワークオブジェクト属性の定義に含まれる値は、VM から vCenter に報告される値と完全に一致している必要があります。たとえば、ネットワークオブジェクトの属性値「This is a Build Machine」は、VM の

summary.config.annotation 値「this is a build machine」と一致しません。後者の文字列を含むバインド更新は、前者のホストマップに追加されません。

VM 属性機能によってモニタリングされている VM には、VMware ツールがインストールされている必要があります。VMware ツールは、VM の IPv4 アドレスまたは IPv6 アドレスを vCenter サーバーに報告するソフトウェアコンポーネントです。VM 属性の機能は、IP アドレスを属性タイプ/値のペアにバインドすることであるため、vCenter は、VMware ツールを実行していない VM のバインド情報を報告しません。

ESXi 環境内では、VM はプライマリ IP アドレスによって定義されます。これは ASA の管理 IP アドレスにほぼ対応します。VM ごとに設定可能なプライマリアドレスは 1 つのみです。IPv4 アドレスと IPv6 アドレスのいずれかを使用できます。バインドは、常にプライマリ IP アドレスと属性のタイプ/値のペアの間で設定されます。VM に複数の IP アドレス（IPv6 リンクローカルアドレスなど）が設定されている場合、vCenter は、プライマリアドレス（通常は最初に設定されたアドレス）のバインド更新のみを送信します。

（注） ユーザーは、一連の VM にカスタム属性のタイプと値を割り当てて、共通のユーザー定義の特性を持つ一連の VM に共通のポリシーセットを適用できます。

属性の包括的なリストと関連するガイドラインについては、VMware vCenter 5.5/6.0 のドキュメントを参照してください。

VM 属性ポリシーの設定

VM 属性に基づいてポリシーを設定するには、次の 3 つの手順があります。

ステップ 1 ネットワークオブジェクト属性を設定します。

a) [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから [ネットワーク/ホスト（Networks/Hosts）] を選択します。作業領域内を右クリックし、[新規オブジェクト（New Object）] > [属性（Attribute）] を選択します。ペインの下部にある [+] ボタンを使用して新しいネットワークオブジェクト属性を追加することもできます。

（注） ネットワーク属性オブジェクトは、object-group-search が有効になっている場合にのみ使用できます。

b) VM 属性エージェントを選択し、VM 属性タイプを指定して、VM 属性値の値を追加します。

ステップ 2 VM 属性エージェントを追加します。

a) VM 属性エージェントの名前を指定し、VM 属性エージェントの説明を追加します。
b) デフォルトでは、エージェントタイプは esxi です。
c) [DNS のホスト名/IP アドレス（DNS Host Name/IP Address）] フィールドに vCenter サーバーのプライマリ IP アドレスを入力します。
d) vCenter サーバーへの認証を受けるユーザー名とパスワードを指定します。

e) エージェントが vCenter サーバーに接続しているときに接続がアクティブな状態を維持する時間を指定します。再試行間隔のデフォルト値は 30 秒です。
f) [再試行回数（Retry Count）] フィールドで、エージェントが vCenter サーバーを非アクティブと宣言する前にサーバーへの接続を試行する回数を指定します。デフォルト値は 3 です。
g) OK をクリックします。

ステップ 3 VM 属性を使用してアクセスリストを設定します。詳細については、アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。

（注） VM 属性は、アクセスリストオブジェクトのみをサポートします。

プールオブジェクトについて

プールオブジェクトには次の用途があります。

- ASA クラスタのレイヤ 3 ロードバランシングで使用するプールの指定
- ASA クラスタのレイヤ 3 EIGRP および OSPFv3 で使用するプールの指定

次の項では、プールオブジェクトを操作する方法について説明します。

- [IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス （407 ページ）
- [IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックス （409 ページ）
- [MACアドレスプールの追加または編集（Add or Edit MAC Address Pool）] ダイアログボックス （410 ページ）
- [NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックス（411 ページ）
- [DHCPv6プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス （413 ページ）

[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス

[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックスを使用して、IPv4 プールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects ）] > [IPv4プールオブジェクト（IPv4 Pool Object）]** を選択し

ます。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

フィールド リファレンス

表 *71 : [IPv4プールオブジェクトの追加（Add IPv4 Pool Object）] ダイアログボックス*

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
タイプ（Type）	プールオブジェクトが単一の IP アドレスであるか、IP アドレスの範囲であるかを選択します。
アドレス（Address）	オブジェクトに含める単一ホストの IPv4 アドレス。
開始アドレス（Start Address） 終了アドレス（End Address）	アドレスの範囲を定義する最初と最後の IP アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
Mask	IP アドレスまたはアドレスの範囲のサブネットマスク。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 （注） IPv4 プールオブジェクトは常にオーバーライド可能です。このオプションをクリアすると、エラーが発生します。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックス

[IPv6プールの追加または編集（Add or Edit IPv6 Pool）] ダイアログボックスを使用して、IPv6 プールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから [プールオブジェクト（Pool Objects ）] > [IPv6プールオブジェクト（IPv6 Pool Object）] を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連ボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

フィールド リファレンス

表 *72 : [IPv6プールオブジェクトの追加（Add IPv6 Pool Object）] ダイアログボックス*

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
アドレス（Address）	オブジェクトに含めるアドレス/プレフィックス長形式の IPv6 アドレス。
メンバー数（Count）	プールに含めるアドレスの数。1 から 16384 の間である必要があります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[MACアドレスプールの追加または編集（AddorEditMACAddressPool）] ダイアログボックス

[MACアドレスプールの追加または編集（Add or Edit MAC Address Pool）] ダイアログボックスを使用して、MAC アドレスプールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects ）] > [MACアドレスプールオブジェクト（MAC Address Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集

（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

フィールド リファレンス

表 *73 : [MAC*アドレスプールの追加（*Add MAC Address Pool*）*]* ダイアログボックス

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
開始MACアドレス（Start MAC Address） 終了MACアドレス（End MAC Address）	アドレスの範囲を定義する最初と最後の MAC アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可（311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックス

[NETプールオブジェクトの追加または編集（Add or Edit NET Pool Object）] ダイアログボックスを使用して、Network Entity Title プールオブジェクトを表示、作成、または編集します。

ナビゲーション パス

[管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects）] > [NETプールオブジェクト（NET Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連ボタンを使用して、いずれかのダイアログボックスを開くこともできます。

関連項目

- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

フィールド リファレンス

表 *74 : [NETプールオブジェクトの追加（Add NET Pool Object）] ダイアログボックス*

要素	説明
名前	オブジェクト名（最大 64 文字）。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
開始NETアドレス（Start NET Address） 終了 NET アドレス（End NET Address）	アドレスの範囲を定義する最初と最後の NET アドレス。開始アドレスと終了アドレスは異なっており、開始の方が終了よりも小さいアドレスである必要があります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[DHCPv6プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス

このダイアログボックスを使用して、DHCPv6 サーバープールを追加または編集します。ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併用するクライアントについては、クライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

ナビゲーション パス

- [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects）] > [DHCPv6プールオブジェクト（DHCPv6 Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

または

- [DHCPv6プールの追加（Add DHCPv6 Pool）] ダイアログボックスには、[DHCPv6プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスからアクセスできます。[使用可能なDHCPv6プール（Available DHCPv6 Pool）] テーブルの下にある [行の追加（Add Row）] または [行の編集（Edit Row）] ボタンをクリックします。[DHCPv6プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスには、[インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [IPv6] パネルの [インターフェイスIPv6 DHCP（Interface IPv6 DHCP）] セクションにある [サーバープール（Server Pool）] オプションボタンからアクセスできます。

関連項目

- [IPv6 Address for Interface] ダイアログボックス （2417 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）
- デバイスインターフェイス、ハードウェアポート、ブリッジグループの管理 （2373 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

フィールド リファレンス

表 *75 : [DHCPv6プールの追加（Add DHCPv6 Pool）] ダイアログボックス*

要素	説明
名前	DHCPv6 プール名は 200 文字までです。オブジェクト名では、大文字と小文字が区別されません。 詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
• 1 つ以上のタブでパラメータを設定し、IR メッセージに対する応答をクライアントに提供します。 • タブごとに、必要に応じて次の内容を指定します。 • DNS/SIP/NIS/NISP/SNTP サーバー：サーバー名を入力します。IPv6 アドレスが正しい形式であることを確認してください。IPv6 アドレス形式の詳細については、http://www.ietf.org/rfc/rfc2373.txt を参照してください。 • DNS/SIP/NIS/NISP ドメイン名：ドメイン名を入力します。ドメイン名の先頭と末尾は数字または文字にする必要があります。内部文字として使用できるのは文字、数字、ハイフンのみです。ラベルはドットで区切ります。各ラベルは最大 63 文字で、ホスト名全体は最大 255 文字です。ドメイン名形式の詳細については、http://www.ietf.org/rfc/rfc1123.txt を参照してください。 （注） import コマンドは、プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバから取得した 1 つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じコマンドを手動と import コマンドで設定することはできません。	
[サーバ（Server）] タブ	（任意）DNS サーバー名とドメイン名を指定します。
[SIP] タブ	（任意）SIP サーバー名と SIP ドメイン名を指定します。
[NIS] タブ	（任意）NIS サーバー名と NIS ドメイン名を指定します。
[NISP] タブ	（任意）NISP サーバー名と NISP ドメイン名を指定します。
[SNTP] タブ	（任意）SNTP サーバー名を指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

SAML ID プロバイダの構成

バージョン 4.10 以降、Security Manager では、ASA VPN の Security Assertion Markup Language（SAML）2.0 ベースのシングルサインオンおよびシングルログアウトを設定できます。シングルサインオンサーバーの設定は、ASA バージョン 9.5(2) からサポートされなくなりました。これは SAML ID プロバイダーに置き換えられました。

セキュリティ アサーション マークアップ言語（SAML）は、当事者間、特に ID プロバイダーとサービスプロバイダーの間で認証および許可データを交換するための XML ベースのオープン標準のデータ形式です。アイデンティティプロバイダーは、ユーザーのアイデンティティを別のリソースにアサートできるサービスです。アイデンティティ プロバイダーは、アイデンティティ管理システムでユーザーを認証する責任があります。サービスプロバイダーは、ユーザーがアクセスするサービスです（パブリックまたはプライベート Web アプリケーションなど）。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [SAML IDプロバイダー（SAML Identity Provider）] を選択します。

SAML アイデンティティ プロバイダーの追加または編集

[SAMLアイデンティティプロバイダーの追加または編集（Add or Edit SAML Identity Provider）] ダイアログボックスを使用して、新しい SAML アイデンティティプロバイダーを追加するか、既存の行を編集します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [SAMLアイデンティティプロバイダー（SAML Identity Provider）] を選択し

ます。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *76 : [SAML*アイデンティティプロバイダーの追加または編集（*Add or Edit SAML Identity Provider*）*]*

要素	説明
名前	SAML アイデンティティ プロバイダーの名前を 4 ～ 256 文字で入力します。
説明	（任意）SAML アイデンティティ プロバイダーの説明を入力します。
[サインインURL（Sign In URL）]	この URL は、アイデンティティ プロバイダーへのサインインに使用されます。http:// または https:// を先頭に付けます（大文字と小文字は区別されません）。サインイン URL の長さは 500 文字以下にする必要があります。[サインインURL（Sign In URL）] フィールドでは、次の特殊文字のみを使用できます。 :、/、*、[、]、.
[サインアウトURL（Sign Out URL）]	（任意）この URL は、アイデンティティ プロバイダーからサインアウトする際のリダイレクトに使用されます。http:// または https:// を先頭に付けます（大文字と小文字は区別されません）。サインアウト URL の長さは 500 文字以下にする必要があります。[サインアウトURL（Sign Out URL）] フィールドでは、次の特殊文字のみを使用できます。 :、/、*、[、]、.
[ベースURL（Base URL）]	（任意）クライアントレス VPN のベース URL です。この URL は、サードパーティ製アイデンティティ プロバイダーに提供される SAML メタデータで使用されます。そうすることで、アイデンティティ プロバイダーはエンドユーザーを ASA にリダイレクトできます。ベース URL が設定されていない場合は、ASA デバイスのホスト名とドメイン名から取得されます。たとえば、ホスト名が ssl-vpn でドメイン名が xyz の場合、使用されるベース URL は https://ssl-vpn.xyz.com になります。http:// または https:// をベース URL の先頭に付けます（大文字と小文字は区別されません）。ベース URL の長さは 500 文字以下にする必要があります。[ベースURL（Base URL）] フィールドでは、次の特殊文字のみを使用できます。 :、/、*、[、]、. （注） SAML を設定するには、ベース URL またはドメイン名のいずれかを ASA デバイスで設定する必要があります。

要素	説明
アイデンティティ プロバイダー	[CAサーバーセレクタ（CA Servers Selector）] ダイアログボックスから [アイデンティティプロバイダー（Identity Provider）] を選択します。アイデンティティ プロバイダーは、ユーザーのアイデンティティを別のリソースにアサートできるサービスです。アイデンティティ プロバイダーは、アイデンティティ管理システムでユーザーを認証する責任があります。
サービス プロバイダー	（任意）[CAサーバーセレクタ（CA Servers Selector）] ダイアログボックスから [サービスプロバイダー（Service Provider）] を選択します。サービスプロバイダーは、ユーザーがアクセスするサービスです（パブリックまたはプライベート Web アプリケーションなど）。
要求のタイムアウト（Request Timeout）	（任意）1 ～ 7200 の値を入力します。デフォルトでは、SAML タイムアウトは設定されていません。
Enable Signature	（任意）SAML 要求内の署名を有効または無効にします。これが有効になっている場合は、サービスプロバイダーを設定する必要があります。 [認証要求（Authentication Request）] ドロップダウンで署名用の暗号スイートを選択します。署名を有効にすると、SHA-256 暗号スイートがデフォルトで選択されます。暗号スイートは、[認証要求（Authentication Request）] ドロップダウンで変更できます。デフォルトでは、署名は無効になっており、[認証要求（Authentication Request）] ドロップダウンは非表示になっています。 （注） SAML署名の認証要求を指定できるのは、ASA 9.8.1 以降のみです。
[内部の有効化（Enable Internal）]	（任意）SAML アイデンティティ プロバイダーの内部フラグを有効または無効にします。有効にすると、内部フラグはプライベートネットワーク内のアイデンティティ プロバイダーを識別するようになり、SAML アイデンティティ プロバイダーには WebVPN 接続を介してのみアクセスできます。これは、ASA がゲートウェイとして機能することも意味します。 デフォルトでは、内部フラグは無効になっており、アイデンティティ プロバイダーに直接アクセスできます。
[再認証の強制の有効化（Enable Force Re-Authentication）]	（任意）SAML アイデンティティ プロバイダーの再認証の強制を有効または無効にします。有効にすると、アイデンティティ プロバイダーは、以前のセキュリティコンテキストに依存するのではなく、プレゼンタを直接認証する必要があります。 デフォルトでは、[再認証の強制（Force Re-Authentication）] フラグが有効になっています。

要素	説明
カテゴリ	（任意）CAT-A ～ CAT-J の間でカテゴリを選択します。
デバイスごとに値のオーバーライドを許可	（任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] が選択されている場合は、[オーバーライド（Overrides）] を編集します。

サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定

Security Manager の多くのポリシーでは、ポリシーが適用されるサービスを識別する必要があります。サービスは、プロトコルと、特定のタイプのトラフィックを識別するポート定義です。多くの場合、サービスはポリシー内に直接指定できます。必要なサービスを定義するサービス ポリシー オブジェクトを選択するか、サービス オブジェクトとポリシー固有のサービス指定の組み合わせを使用することもできます。

サービス オブジェクトを使用すると、特定のアプリケーションの構成を表すオブジェクトを作成したり、ネットワーク上に存在する論理組織（開発チームや企業部門など）を基にしてオブジェクトをモデル化したりできるため、サービス オブジェクトは有用です。次の 2 つのタイプのサービス ポリシー オブジェクトがあります。

- サービス グループ：1 つ以上のサービス（他のサービス オブジェクトを含む）を含めることができます。これは、すべての Security Manager 3.x リリースで使用可能だったサービス オブジェクトのタイプです。
- サービス オブジェクト：1 つのサービスを含めることができます。

サービスを識別する必要があるポリシーを設定するときに、[サービス（Services）] フィールドの横の [選択（Select）] ボタンをクリックして、サービスオブジェクトを選択または作成できます。選択ダイアログボックスから新しいサービスを作成するには、サービスリストの下の [追加（Add）] ボタンをクリックし、タイプ（グループまたはオブジェクト）を選択します。コンテンツテーブルから **[サービス（Services）]>[サービス（Services）]** を選択し、[オブジェクトの追加（Add Object）] ボタンをクリックし、グループまたはオブジェクトを選択することによって、[Policy Object Manager] からサービスを作成することもできます。サービス オブジェクトを作成するときに使用できる特定のフィールドについては、サービス オブジェクトの設定 （422 ページ）を参照してください。

Security Manager には、定義済みのサービス グループ オブジェクトの包括的なコレクションがあります。HTTP、Syslog、POP3、Telnet、SNMP など、一般的に使用されるサービス用の ICMP メッセージおよびオブジェクトが含まれています。定義済みのサービス グループ オブジェクトを使用する前に、オブジェクト定義を確認して、使用しているネットワーク実装に準拠していることを確認する必要があります。定義済みのオブジェクトがニーズに合わない場合（別の宛先ポートが必要な場合など）、新しいサービス オブジェクトを最初から作成するか、既存の

オブジェクトのコピーを基に作成できます。詳細については、オブジェクトのクローニング（複製） （305 ページ）を参照してください。

サービス オブジェクトを作成する場合もポリシー内にサービスを直接指定する場合も、次の形式を使用してサービスを指定できます。入力に応じて、Security Manager によってエントリに関連するテキストコンプリート オプションが示される場合があります。リストから値を選択して、Enter または Tab を押します。複数のサービスをカンマで区切って入力できます。

- *protocol*：プロトコルは、1 ～ 255 または tcp、udp、gre、icmp などの広く知られているプロトコル名です。数字を入力すると、その数字は関連付けられている名前に変換されます。
- **icmp**/*message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知の ICMP メッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp/unreachable/1** または **icmp/echo-reply**）。
- **icmp6**/*message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知の ICMP メッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp6/unreachable/1** または **icmp6/echo-reply**）。
- **{tcp | udp | tcp&udp}**/{*destination_port_number* | *port_list_object* }：宛先ポート番号は、1 ～ 65535 またはポートリストオブジェクトの名前です。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。送信元ポート番号は、Default Range ポート リスト オブジェクトです。Default Range オブジェクトには、[Policy Objects] ページ （732 ページ）（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー オブジェクト（Policy Objects）] を選択）で選択した設定に応じて、すべてのポート（1 ～ 65535）またはすべてのセキュアポート（1024 ～ 65535）が含まれています。

たとえば、サービスを tcp/10 として定義すると、10 が宛先ポートであり、送信元ポートは定義されないことを意味します。

ポートを指定するときに、番号の前に特別なキーワード**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、および **neq**（等しくない）を使用することもできます。たとえば、**lt 440** と入力すると、440 未満のすべてのポートが指定されます。

ヒント　ポートリストオブジェクトを作成するには、[Policy Object Manager] で **[サービス（Services）] > [ポートリスト（Port Lists）]** を選択し、[オブジェクトの追加（Add Object）] ボタンをクリックします。詳細については、ポート リスト オブジェクトの設定 （420 ページ）を参照してください。

- **{tcp | udp | tcp&udp}**/{*source_port_number* | *port_list_object* }/ {*destination_port_number* | *port_list_object* }：送信元ポート番号および宛先ポート番号は、1 ～ 65535 またはポートリストオブジェクトの名前です。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。

たとえば、サービスを tcp/10/20 として定義すると、10 が送信元ポート、20 が宛先ポートであることを意味します。宛先ポートを指定しない場合は、Default Range ポート リスト オブジェクトを使用します。tcp/10/Default Range などです。

- （サービスグループのみ）*service_object_name*：別の既存のサービスオブジェクトの名前。他のオブジェクトを指定する場合、オブジェクト定義を入れ子にすることができます。[選択（Select）]をクリックしてサービスオブジェクトを選択するか、新しいオブジェクトを作成します。

IOS デバイスにのみ適用される次の ICMP メッセージタイプは、ASA/PIX/FWSM デバイスでサポートされる ICMP メッセージタイプに自動的に置き換えられます。

- ICMP-Mobile-Redirect
- ICMP-Host-Unreachable
- ICMP-Network-Redirect
- ICMP-Port-Unreachable
- ICMP-Protocol-Unreachable
- ICMP-Reassembly-Timeout
- ICMP-Redirect
- ICMP-protocol-redirect

関連項目

- ポリシーのオブジェクトの選択　（288 ページ）
- ポリシー オブジェクトの作成　（299 ページ）
- オブジェクトの編集　（303 ページ）
- カテゴリ オブジェクトの使用　（304 ページ）
- サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法　（429 ページ）
- オブジェクト オーバーライドの管理　（309 ページ）
- ポリシー オブジェクトの上書きの許可　（311 ページ）

ポート リスト オブジェクトの設定

[Port List] ダイアログボックスを使用して、ポート リスト オブジェクトを作成、編集、またはコピーします。各ポートリストオブジェクトには、1つ以上のポートまたはポート範囲（1-1000 や 2000-2500 など）を含めることができます。また、ポート リスト オブジェクトに他のポート リスト オブジェクトを含めることもできます。

通常はサービスを定義するときにポート リスト オブジェクトを使用しますが、ポート番号を入力しないで、ポートを識別するためにさまざまなポリシーで使用することもできます。サービス定義でのポート リストの使用の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。

ヒント　定義済みの Default Range ポートリストオブジェクトには、[Security Manager管理（Security Manager Administration）] ウィンドウ（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシーオブジェクト（Policy Objects）] を選択。[Policy Objects] ページ （732 ページ）を参照）で選択した設定に応じて、すべてのポート（1 ～ 65535）またはすべてのセキュアポート（1024 ～ 65535）が含まれます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [サービス（Services）] > [ポートリスト（Port Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- サービス オブジェクトの設定 （422 ページ）

フィールド リファレンス

表 *77 : [Port List]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明
ポート	ポート リスト オブジェクトに含まれるポートまたは範囲。443 や 1-1000 など。単一ポート、ポートの範囲、複数のポート範囲、または単一ポートと範囲の組み合わせを定義できます。複数のエントリを指定する場合は、カンマで区切ります。ポート値の範囲は 1 ～ 65535 です。 次の演算子を使用して範囲を指定できます。 • **gt**：より大きい。gt 1000 など。 • **lt**：より小さい。lt 1000 など。 • **eq**：等しい。eq 1000 など。ただし、**eq 1000** は単純に **1000** と入力するのと同じ意味です。 • **neq**：等しくない。neq 1000 など。 この演算子を使用する場合、[Ports] フィールドでは neq 値だけを使用できます。ただし、オブジェクトにポート範囲を含めることができます。したがって、1150 を除く 1000 ～ 1200 のすべてのポートを指定するオブジェクトを作成する場合は、1000 ～ 1200 の範囲のポート リスト オブジェクトと、neq 1150 を指定し、さらにそのポート リスト オブジェクトを含む別のオブジェクトを作成します。
Port Lists	オブジェクトに含める他のポートリストオブジェクト（ある場合）。ポートリストの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

サービス オブジェクトの設定

[Add Service]/[Edit Service] ダイアログボックスを使用して、サービス オブジェクトを作成または編集します。サービス オブジェクトを作成して、ネットワーク内のデバイスによって伝送さ

れるトラフィックのタイプを記述できます。サービス オブジェクトを作成するときは、サービスによって使用されるプロトコルを指定する必要があります。

サービス オブジェクトを作成するときは、オブジェクト タイプを選択する必要があります。

- サービス グループ：1 つ以上のサービス（他のサービス オブジェクトを含む）を含めることができます。これは、すべての Security Manager 3.x リリースで使用可能なサービス オブジェクトのタイプです。
- サービス オブジェクト：1 つのサービスを含めることができます。

Security Manager には、定義済みのサービス グループ オブジェクトが数多く用意されています。オブジェクトを作成する前に、Policy Object Manager でリストを参照し、既存のオブジェクトがニーズに合うかどうかを確認します。定義済みのオブジェクトは複製できますが、編集することはできません。

Cisco Security Manager は、show running configuration で使用可能な定義を持つサービスオブジェクトをサポートします。定義済みオブジェクトの場合、定義を show running configuration で使用することはできません。そのため、ASA デバイスの定義済みオブジェクトを使用して設定されたポリシーは、Cisco Security Manager では検出されません。

デバイスの動作に合わせるために、Cisco Security Manager バージョン 4.17 で、定義済みオブジェクトのサポートが導入されました。新しい定義済みサービスオブジェクトが ASA に追加されるたびにデバイスがそのオブジェクトを使用して更新される場合、ASA 定義済みオブジェクトが検出されます。この機能は、イメージをサポートするすべてのバージョンの ASA でサポートされています。

（注） PPTP の定義済みオブジェクトはサポートされていません。

ただし、Cisco Security Manager は、ASA バージョンに関するアクティビティの検証をサポートしていません。また、Cisco Security Manager の ICMP および ICMPv6 の定義済みオブジェクトは、デバイスの定義済みオブジェクトに変換されます。したがって、Cisco Security Manager の定義済みオブジェクトを使用すると、そのポリシーが無効になり再作成されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [サービス（Services）] > [サービス（Services）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか（その後オブジェクトタイプを選択）、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 78 : [Add Service]/[Edit Service] ダイアログボックス

要素	説明
名前	オブジェクト名。ソフトウェア バージョン 8.x を実行する ASA または PIX デバイス用のオブジェクトを使用する場合は、名前の長さを 64 文字に制限します。その他のデバイスの場合、名前は最大 128 文字です。 オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
Services（グループの場合） Service（オブジェクトの場合）	このポリシー オブジェクトに含めるサービス。サービス グループを作成する場合、複数のサービスをカンマで区切って入力できます。サービス オブジェクトを作成する場合、1 つのサービスだけを入力できます。 次の形式を使用して、サービスを指定できます。入力に応じて、Security Managerによってエントリに関連するテキストコンプリート オプションが示される場合があります。定義済みのサービス オブジェクトに直接変換されるサービスを入力した場合、エントリは定義済みのオブジェクト名に変換されます。たとえば、TCP/80 は HTTP に変換されます。 • *protocol*：プロトコルは、1 ～ 255 または tcp、udp、gre、icmp などの広く知られているプロトコル名です。数字を入力すると、その数字は関連付けられている名前に変換されます。 • **icmp/***message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知のICMPメッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp/unreachable/1** または **icmp/echo-reply**）。 • **icmp6/***message_type* /*message_code* ：メッセージタイプは 1 ～ 255 またはエコーなどの既知のICMPメッセージタイプ名であり、メッセージコードは 0 ～ 255 です（たとえば、**icmp6/unreachable/1** または **icmp6/echo-reply**）。

要素	説明
	• **{tcp | udp | tcp&udp}**/{*destination_port_number* | *port_list_object*}：宛先ポート番号には、1 ～ 65535 またはポートリストオブジェクトの名前を指定できます。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。この場合には、送信元ポート番号は、Default Range ポート リスト オブジェクト（1 ～ 65535 の範囲を指定）です（ポート リスト オブジェクトの作成および編集については、ポート リスト オブジェクトの設定 （420 ページ）を参照してください）。 ポートを指定するときにはいつでも、番号の前に特別なキーワード**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、および **neq**（等しくない）を使用することもできます。たとえば、**lt 440** と入力すると、440 未満のすべてのポートが指定されます。 • **{tcp | udp | tcp&udp}**/{*source_port_number* | *port_list_object* }/{*destination_port_number* | *port_list_object*}：送信元ポート番号および宛先ポート番号には、1 ～ 65535 またはポートリストオブジェクトの名前を指定できます。ハイフンを使用してポート範囲を入力できます（たとえば、10-20）。 • （サービスグループのみ）*service_object_name* ：別の既存のサービスオブジェクトの名前。他のオブジェクトを指定する場合、オブジェクト定義を入れ子にすることができます。[選択（Select）]をクリックしてサービスオブジェクトを選択するか、新しいオブジェクトを作成します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用（304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）]ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

IOS デバイスにのみ適用される次の ICMP メッセージタイプは、ASA/PIX/FWSM デバイスでサポートされる ICMP メッセージタイプに自動的に置き換えられます。

- ICMP-Mobile-Redirect
- ICMP-Host-Unreachable
- ICMP-Network-Redirect
- ICMP-Port-Unreachable

- ICMP-Protocol-Unreachable
- ICMP-Reassembly-Timeout
- ICMP-Redirect
- ICMP-protocol-redirect

ポリシーオブジェクトがオブジェクトグループとしてプロビジョニングされる方法

オブジェクト グループは、ASA、PIX、FWSM、および IOS 12.4(20)T 以降のデバイスの機能であり、IP ホスト、ネットワーク、プロトコル、ポート、ICMP メッセージ タイプなどのオブジェクトをグループ化することによって、アクセス ルールのサイズを減らすことができます。オブジェクト グループの機能は Security Manager のポリシー オブジェクトの機能と似ていますが、実装において重要な違いがいくつかあります。

このため、ポリシーをデバイスに展開するときに、Security Manager で設定したポリシー オブジェクトの正確なコピーであるオブジェクト グループを作成できるとはかぎりません。たとえば、ポリシー オブジェクト名は Security Manager ではオブジェクト タイプごとに一意ですが（つまり、ネットワーク/ホスト オブジェクトとサービス オブジェクトを同じ名前で定義できます）、デバイス上で定義されるすべてのタイプのオブジェクト グループは、1 つの命名方式を共有します。したがって、デバイス上の既存のサービス オブジェクト グループと名前が一致するネットワーク/ホスト オブジェクトを展開する場合、サービス オブジェクト グループと区別するために、ネットワーク/ホスト オブジェクトの名前にサフィックスが付加されます。

（注） オブジェクト グループを展開するときに使用できるオプションについては、[Deployment] ページ （658 ページ）を参照してください。

同様に、デバイス上のポリシーを検出するときに、デバイス上で設定されたオブジェクト グループの正確なコピーであるポリシー オブジェクトを作成できるとはかぎりません。ただし、元の設定は Security Manager によって可能なかぎり保持されます。

（注） IOS デバイスの場合、アクセス コントロール リスト オブジェクトによって使用されるポリシー オブジェクトは、あとで展開中にオブジェクトのコンテンツによって置き換えられます。ACL オブジェクトで使用されるオブジェクト グループは保持されませんが、Security Manager ポリシー オブジェクトとして検出されます。

次の項では、ポリシー オブジェクトをデバイス上のオブジェクト グループにプロビジョニングするとき、またはこれらのデバイス上のポリシーの検出時にポリシー オブジェクトを作成するときに行われる変更について説明します。

• ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （427 ページ）
• サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （429 ページ）

ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービスオブジェクトがオブジェクトグループとしてプロビジョニングされるときの命名方法

ほとんどの場合、ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトは、オブジェクト名が変更されることなく、オブジェクト グループとしてプロビジョニングされます。次のテーブルに、サポート対象デバイス上のオブジェクトグループにオブジェクト名を直接変換できない場合に、名前が変更される方法を示します。

（注） 定義済みのネットワーク/ホストオブジェクト **any** は、オブジェクトグループとしてプロビジョニングされません。

表 *79*：ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトのオブジェクト グループとしての命名方法

条件	新しい名前（New Name）	例
オブジェクト名にスペースが含まれている。	スペースはアンダースコアに置き換えられます。	**my object** という名前のオブジェクトは、**my_object** という名前のオブジェクトグループとしてプロビジョニングされます。
オブジェクト名の長さが 64 文字（オブジェクト グループでサポートされる最大）を超えている。	64 文字の制限内に収めながらオブジェクト グループで必要とされるサフィックス（_TCP や _UDP など、または _1 などの一意の番号）を付加できるように、名前は切り捨てられます。	

条件	新しい名前（New Name）	例
デバイスにすでに同じ名前のオブジェクト グループ（プロトコル/ICMP/サービス）がある。	数値のサフィックスが 1 から順に名前に付加されます。	**West** という名前のネットワーク/ホストオブジェクトがあり、デバイスに **West** という名前の TCP サービス オブジェクト グループがすでにある場合、展開時にオブジェクト グループの名前は **West_1** に変更されます。
同じ名前のネットワーク/ホスト オブジェクト グループがすでに作成されている。	数値のサフィックスが 1 から順に名前に付加されます。	どちらも **West** という名前のネットワーク/ホストオブジェクトとポートリストまたはサービスオブジェクトがある場合、ネットワーク/ホストオブジェクトは **West** として展開され、ポートリストは **West_1** として展開されます。

（注） ASA ソフトウェアバージョン 8.2 以前の場合、Security Manager でネットワーク オブジェクト タイプのオブジェクトを作成する場合、オブジェクト名は同じでネットワーク オブジェクト グループ タイプのオブジェクトを持つ ASA デバイスを検出すると、Security Manager は新しいオブジェクトを作成しません。代わりに、既存のオブジェクトを再利用します。ただし、ASA ソフトウェアバージョン 8.3 以降では、Security Manager でネットワーク オブジェクト タイプのオブジェクトを作成する場合、オブジェクト名は同じでネットワーク オブジェクト グループ タイプのオブジェクトを持つ ASA デバイスを検出すると、Security Manager は、name_1、name_2 などのような新しいオブジェクトを作成します。これは、ソフトウェアバージョン 8.2 以前を実行している ASA デバイスを管理する Security Manager の場合、ASA をバージョン 8.3 以降にアップグレードすると、新しいオブジェクトが作成されることを意味します。

関連項目

- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （429 ページ）
- ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （426 ページ）

サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法

次の表に、サービス オブジェクトをサポート対象デバイスに展開するときに、Security Manager によってオブジェクト グループが作成される方法を示します。

ヒント ASA 8.3 以降のデバイスの場合、サービスオブジェクトは **object-group** コマンドではなく **object service** コマンドを使用してプロビジョニングされます。

表 *80* : サービス オブジェクトがオブジェクト グループとしてプロビジョニングされる方法

条件	生成されるオブジェクト グループ	例

サービス オブジェクトに ICMP プロトコルおよび ICMP メッセージ タイプが含まれている。	ICMP タイプのオブジェクト グループがサービス オブジェクトと同じ名前で生成されます。	サービスオブジェクト service1：**icmp/icmp-echo, 23**
		オブジェクト グループ：
		`object-group icmp-type service1`
		`  icmp-object icmp-echo`
		`  icmp-object 23`

サービス オブジェクトにプロトコルだけが含まれている。	プロトコル オブジェクト グループがサービス オブジェクトと同じ名前で生成されます。	サービスオブジェクト service1：**tcp, gre, 34**
		オブジェクト グループ：
		`object-group protocol service1`
		`  protocol-object tcp`
		`  protocol-object gre`
		`  protocol-object 34`

サービス オブジェクトにより、送信元ポートと宛先ポート両方のポート リスト オブジェクトが使用されている。	ポート リスト オブジェクトと一致するサービス オブジェクト グループが生成されます。	

サービス オブジェクトに複数のポートまたはポート範囲が含まれているが、送信元ポートのポート リスト オブジェクトは使用されていない。	送信元ポートの <ObjectName>.src という名前のサービス オブジェクト グループが生成されます。	サービスオブジェクト serv1：**tcp/400,600/23-80**
		オブジェクト グループ：
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`

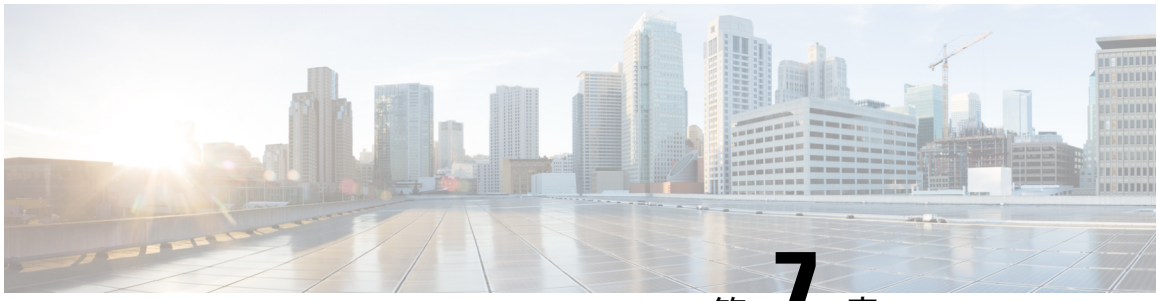
条件	生成されるオブジェクト グループ	例

サービス オブジェクトに複数のポートまたはポート範囲が含まれているが、宛先ポートのポート リスト オブジェクトは使用されていない。	宛先ポートのサービス オブジェクト グループがサービス オブジェクトと同じ名前で生成されます。	サービスオブジェクト serv1：
		tcp/400,600/23-80, 566
		オブジェクト グループ：
		`object-group service serv1 tcp`
		`  port-object range 23 80`
		`  port-object eq 566`
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`

サービス オブジェクトに TCP&UDP プロトコルが含まれており、定義済みのポートが含まれている。		サービスオブジェクト serv1：
		tcp&udp/400,600/23-80, 566
		オブジェクト グループ：
		`object-group service serv1 tcp`
		`  port-object range 23 80`
		`  port-object eq 566`
		`object-group service serv1.src tcp`
		`  port-object eq 400`
		`  port-object eq 600`
		`object-group protocol tcp-udp`
		`  protocol-object tcp`
		`  protocol-object udp`

関連項目

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- ネットワーク/ホスト オブジェクト、ポート リスト オブジェクト、およびサービス オブジェクトがオブジェクト グループとしてプロビジョニングされるときの命名方法 （427 ページ）
- ポリシー オブジェクトがオブジェクト グループとしてプロビジョニングされる方法 （426 ページ）



第 7 章

FlexConfig の管理

FlexConfig ポリシーを使用すると、Security Manager ではサポートされていないデバイス コマンドを設定できます。FlexConfig を使用することで、Security Manager によるデバイス設定の制御を拡張したり、製品をアップグレードする前に新しいデバイス機能を利用したりできます。

FlexConfig ポリシーは、FlexConfig オブジェクトで構成されます。これらのオブジェクトは、基本的には、スクリプト言語コマンド、デバイス コマンド、および変数を格納できるサブルーチンです。オブジェクトは、Security Manager 設定をデバイスに適用する前に処理されるように設定するか、または設定後に処理されるように設定できます。Security Manager では、オブジェクトが指定した順に処理されるため、別のオブジェクトの処理に依存するオブジェクトを作成できます。FlexConfig ポリシーオブジェクトの内容は、単一の簡単なコマンド文字列から、スクリプトや変数が組み込まれた複雑な CLI コマンド構造にいたるまでさまざまです。

（注） Cisco Security Manager は、FlexConfig の作成または変更後に FlexConfig を 1 回だけ展開するように設定したり、展開ごとに FlexConfig を展開するように設定したりできます。デフォルトでは、Cisco Security Manager は FlexConfig を 1 回展開します。展開ごとに FlexConfig を展開する必要がある場合は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] ページで [新規または変更された Flexconfig のみを展開する（Deploy only new or modified Flexconfigs）] 設定をディセーブルにします。この設定を変更した後は、展開後に 1 回限りの FlexConfig を削除して管理する必要があります。詳細については、[Deployment] ページ （658 ページ）を参照してください。

FlexConfig ポリシー オブジェクトを理解して使用するには、ポリシーとオブジェクトについて理解することが重要です。Security Manager によるポリシーの定義および使用方法の詳細については、ポリシーの管理 （209 ページ）を参照してください。Security Manager によるオブジェクトの定義および使用方法の詳細については、ポリシー オブジェクトの管理 （287 ページ）を参照してください。

（注） **[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）]** ページの [新規または変更済みFlexConfigのみを展開する（Deploy only new or modified FlexConfigs）] 設定を有効にした場合、変更のあるアクティビティを開いているときに、FlexConfig を展開しようとすると、Cisco Security Manager は、（他のアクティビティの変更ではなく）開いているアクティビティのみに固有の FlexConfig の変更を考慮します。一方、すべてのアクティビティが送信済みで、開いているアクティビティがない場合、Security Manager は、変更とともに送信された、最後に送信されたアクティビティに固有の FlexConfig の変更を考慮します。そのため、展開中にアクティビティを反映させるために FlexConfig の変更が必要な場合は、変更が単一のアクティビティで実行され、送信され、展開されていることを確認してください。

ここでは、FlexConfig ポリシーとポリシー オブジェクトおよびそれらの使用方法について説明します。

- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）
- FlexConfig ポリシーとポリシー オブジェクトの設定 （461 ページ）
- [FlexConfig Policy] ページ （475 ページ）
- FlexConfig のトラブルシューティング （478 ページ）

FlexConfig ポリシーとポリシー オブジェクトについて

FlexConfig ポリシー オブジェクトは、FlexConfig ポリシーで使用されます。これらのオブジェクトを使用すると、Security Manager ではサポートされないデバイス機能を設定したり、デバイス設定を微調整したりできます。これらのポリシーオブジェクトにはデバイス コンフィギュレーション コマンドと変数が含まれます。また、処理を制御するスクリプト言語命令が含まれることもあります。FlexConfig オブジェクトは、基本的には Security Manager によって生成されたデバイス設定に内容を追加するプログラミング ルーチンです。

FlexConfig ポリシー オブジェクトは、最初から作成するか、または Security Manager に付属のオブジェクトを複製して作成できます。

FlexConfig ポリシーは、FlexConfig ポリシー オブジェクトの単なる順序リストです。オブジェクトは指定した順序で処理されます。

FlexConfig ポリシー オブジェクト、さらに FlexConfig ポリシーの概要については、次の項を参照してください。ポリシー オブジェクト全般の詳細については、ポリシー オブジェクトの管理 （287 ページ）を参照してください。

- FlexConfig ポリシー オブジェクトにおける CLI コマンドの使用 （433 ページ）
- スクリプト言語命令の使用 （434 ページ）
- FlexConfig オブジェクトの変数について （436 ページ）
- 定義済みの FlexConfig ポリシー オブジェクト （454 ページ）

FlexConfig ポリシー オブジェクトにおける CLI コマンドの使用

FlexConfig Editor に入力するコンフィギュレーション コマンドは、PIX ファイアウォールや Cisco IOS ルータなどのデバイスの設定に使用される実際の CLI コマンドです。Security Manager でサポートされていない CLI コマンドを含めることができます。コマンドを理解し、デバイス タイプに適した構文を使用してコマンドを実装する必要があります。詳細については、特定のオペレーティング システムのコマンド リファレンスを参照してください。

FlexConfig ポリシー オブジェクトを作成するとき、通常の Security Manager ポリシーから生成された設定の先頭と末尾のどちらに、コマンドや命令を追加するかを指定します。

- プリペンドされるオブジェクト：設定の最初に処理される FlexConfig オブジェクト。Security Manager ポリシーでオブジェクトに含まれているのと同じコマンドが設定されている場合、プリペンドされるコマンドは設定ファイルの展開時に置き換えられます。
- 付加されるオブジェクト：設定の最後（設定ファイル内の他のすべてのコマンドから **write mem** コマンドまでの間）に処理される FlexConfig オブジェクト。

アペンドされるコマンドがデバイスにすでに設定されている場合、それらのコマンドをもう一度追加しようとすると、エラーが生成されます。このことを解決するための回避策が 2 つあります。

- アペンドされるコマンドとして、問題のある設定を削除するコマンドを入力します。たとえば、コマンドが **xyz** の場合は、次の 2 行を入力します。

```
no xyz
xyz
```

- デバイスが「警告」するアクションを制御する設定を変更します。これは、[ツール（Tools）] > [セキュリティ管理（Security Administration）] > [展開（Deployment）] で設定します。

この設定変更は、アペンドされるコマンドとして指定されたコマンドだけでなく、展開されるすべてのコマンドについて、デバイスの動作に反映されます。

（注） デバイスに展開する場合は、最初の展開後、ほとんどのアペンドされるコマンドを削除する必要があります。このことは、バインドされていないオブジェクト グループがコマンドの生成中に [Ending Command] セクションで置き換えられ、設定がデバイスに展開されるたびに再送信されるオブジェクト グループに特に当てはまります。ファイアウォール デバイスによってオブジェクト グループがすでに存在することが示されるため、エラーが表示されます。ファイルまたは AUS に展開する場合は、アペンドされるコマンドを削除しません。

スクリプト言語命令の使用

FlexConfig ポリシー オブジェクトでスクリプト言語命令を使用して、オブジェクト内のコマンドの処理方法を制御できます。スクリプト言語命令は、Velocity テンプレート エンジンでサポートされているコマンドのサブセットです。Velocity テンプレート エンジンは、ループ、if/else ステートメント、および変数をサポートする Java ベースのスクリプト言語です。

Security Manager では、**include** コマンドと **parse** コマンドを除くすべての Velocity テンプレートエンジンのコマンドがサポートされています。サポートされている他のコマンドの詳細については、Velocity テンプレート エンジンのマニュアルを参照してください。

次の各項では、最も一般的に使用される機能の例を示します。

- スクリプト言語の例 1：ループ （434 ページ）
- スクリプト言語の例 2：2 次元配列でのループ （434 ページ）
- 例 3：If/Else ステートメントを使用したループ （435 ページ）

スクリプト言語の例 1：ループ

Plain Old Telephone Service（POTS; 一般電話サービス）ダイヤル ピアを使用すると、電話番号を音声ポートに関連付けることによって、テレフォニー デバイスで着信コールを受信できます。次の例では、POTS ダイヤル ピアのセットの発信者番号をイネーブルにします。

オブジェクト本体

```
#foreach ($peer_id in ["2", "3", "4"])
    dial-peer voice $peer_id pots
    caller-id
#end
```

CLI 出力

```
dial-peer voice 2 pots
caller-id
dial-peer voice 3 pots
caller-id
dial-peer voice 4 pots
caller-id
```

スクリプト言語の例 2：2 次元配列でのループ

この例では、着信コールをルータで受信できるように電話番号のセットが音声ポートに関連付けられています。

オブジェクト本体

```
#foreach ($phone in [ [ "2000", "15105552000", "1/0/0" ], [ "2100",
"15105552100", "1/0/1" ], [ "2200", "15105552200", "1/0/2" ] ] )
    dial-peer voice $phone.get(0) pots
```

```
 destination-pattern $phone.get(1)
 port $phone.get(2)
#end
```

CLI 出力

```
dial-peer voice 2000 pots
destination-pattern 15105552000
port 1/0/0
dial-peer voice 2100 pots
destination-pattern 15105552100
port 1/0/1
dial-peer voice 2200 pots
destination-pattern 15105552200
port 1/0/2
```

例 3：If/Else ステートメントを使用したループ

この例では、着信コールをルータで受信できるように電話番号のセットが音声ポートに関連付けられています。さらに、電話番号の別のセットを IP アドレスに関連付けて、ルータからの Voice over IP 発信コールをイネーブルにしています。

オブジェクト本体

```
#foreach ( $phone in [ [ "2000", "15105552000", "1/0/0", "" ],
[ "2100", "15105552100", "1/0/1", "" ],
[ "2200", "15105552200", "", "ipv4:150.50.55.55"]
[ "2300", "15105552300", "", "ipv4:150.50.55.55"] ] )
    dial-peer voice $phone.get(0) pots
     destination-pattern $phone.get(1)
 #if ( $phone.get(2) == "" )
     session target $phone.get(3)
 #else
     port $phone.get(2)
 #end

#end
```

CLI 出力

```
dial-peer voice 2000 pots
    destination-pattern 15105552000
 port 1/0/0

dial-peer voice 2100 pots
    destination-pattern 15105552100
 port 1/0/1

dial-peer voice 2200 pots
    destination-pattern 15105552000
 session target ipv4:150.50.55.55

dial-peer voice 2300 pots
    destination-pattern 15105552300
 session target ipv4:150.50.55.55
```

FlexConfig オブジェクトの変数について

FlexConfig ポリシー オブジェクトの変数は、$ 文字で始まります。たとえば、次の行では、$inside が変数です。

```
interface $inside
```

FlexConfig ポリシー オブジェクトで使用できる変数には 3 つのタイプがあります。

- ポリシーオブジェクト変数：特定のプロパティを参照する静的変数。たとえば、テキストオブジェクトは、ポリシーオブジェクト変数のタイプの 1 つです。これらの変数は名前と値のペアであり、値には単一の文字列、文字列のリスト、または文字列のテーブルを指定できます。これらの変数には、任意のポリシーオブジェクトによる参照または操作の対象となる、任意のタイプのテキスト データを入力できます。

ポリシー オブジェクト変数を FlexConfig ポリシー オブジェクトに追加するには、次の 3 通りの方法があります。まず、カーソルを目的の位置に移動し、次の作業を実行します。

- 右クリックし、[テキストオブジェクトの作成（Create Text Object）] を選択します。このコマンドによってダイアログボックスが開きます。このダイアログボックスでは、簡単な単一値のテキストオブジェクトを作成して値を割り当てることができます。[OK] をクリックすると、変数がオブジェクトに追加され、[Policy Object Manager] ウィンドウの定義済みテキストオブジェクトのリストに追加されます。この変数は、他のオブジェクトで使用したり、定義を編集したりできます。簡単なテキスト変数の作成例については、FlexConfig ポリシー オブジェクトの変数の例 （437 ページ）を参照してください。
- 右クリックし、[ポリシーオブジェクトの挿入（Insert Policy Object）] サブメニューからポリシーオブジェクトタイプを選択します。セレクタ ダイアログボックスが開き、挿入する変数が格納される特定のポリシー オブジェクトを選択できます。ポリシー オブジェクトを選択すると、[Property Selector] ダイアログボックスが表示されます。このダイアログボックスで、使用するオブジェクトの特定のプロパティを選択したり、プロパティに関連付けられている変数の名前を任意で変更したりします。

この方法を使用すると、使用する値がプロパティに含まれていることがわかっている場合に、既存のポリシーオブジェクトからそのプロパティを追加できます。たとえば、RADIUS プロトコルを指定する変数を RADIUS という名前の AAA サーバー グループ ポリシー オブジェクトから挿入する場合は、右クリックして [ポリシーオブジェクトの挿入（Insert Policy Object）] > [AAAサーバーグループ（AAA Server Group）] を選択し、[AAA Server Group Selector] ダイアログボックスで [RADIUS] を選択して [OK] をクリックします。次に、[AAA Server Group Property Selector] ダイアログボックスの [オブジェクトのプロパティ（Object Property）] フィールドで [プロトコル（Protocol）] を選択し、[OK] をクリックします。$protocol 変数がカーソル位置に挿入され、選択したオブジェクトに定義されているプロパティの値が変数リストに追加されます。

- 変数名を入力します。変数を入力しても、[Add FlexConfig]/[Edit FlexConfig] ダイアログボックスで [OK] をクリックするまでは、変数に値を割り当てることができません。変数が未定義であることが通知され、値を定義するように促されます。[FlexConfig Undefined Variable] ダイアログボックスで、目的の値を含むポリシー オブジェクトのオブジェクト

タイプを選択できます。これにより、特定のポリシーオブジェクトと変数を選択するように要求されます。この操作は、実質的には前述のポリシーオブジェクト変数を挿入する処理と同じです。いずれの方法を使用するかは任意であり、最終的な結果は同じになります。

- システム変数：展開中、設定が生成されるときに値を参照する動的変数。値は、ターゲット デバイスまたはターゲット デバイスに設定されているポリシーから取得されます。FlexConfigポリシー オブジェクトでオプションにする（つまり、変数をデバイスに展開するために変数に値を割り当てる必要がない）ようにシステム変数を宣言できます。

システム変数をFlexConfigポリシーオブジェクトに挿入するには、カーソルを目的の位置に移動し、右クリックして [システム変数の挿入（Insert System Variable）] サブメニューから変数を選択します。使用可能なシステム変数の説明については、FlexConfig システム変数 （438 ページ）を参照してください。

- ローカル変数：ループおよび割り当てによる派生物（**for each** および **set** ステートメント）内でローカルな変数。ローカル変数では、Velocity テンプレート エンジンから直接値を取得します。ローカル変数の値を指定する必要はありません。

ローカル変数を挿入するには、単純にそれを入力します。[FlexConfigの追加（Add FlexConfig）]/[FlexConfigの編集（Edit FlexConfig）] ダイアログボックスで [OK] をクリックすると、未定義の変数を定義するかどうか確認されます。[No] をクリックできます。[Yes] をクリックして他の変数を定義する場合は、ローカル変数のオブジェクト タイプを [Undefined] のままにできます。

FlexConfig ポリシー オブジェクトの変数の例

CLI コマンドや変数を使用すると、FlexConfig ポリシー オブジェクトを作成して Cisco ルータ上の内部インターフェイスやクリプト マップに名前を付けることができます。

```
interface $inside
crypto map $mapname
```

次の例は、これらのコマンドを追加し、$inside の値を **serial0**、$mapname の値を **my_crypto** として設定する FlexConfig ポリシーオブジェクトの作成方法を示しています。

FlexConfigポリシー オブジェクトをデバイスに追加し、設定が生成されると、次の出力が作成されます。

```
interface serial0
crypto map my_crypto
```

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 目次から [FlexConfigs] を選択します。右ペインのテーブルには、既存の FlexConfig オブジェクトが一覧表示されます。

ステップ 3 テーブル内で右クリックし、[新規オブジェクト（New Object）] を選択します。[Add FlexConfig] ダイアログボックスが表示されます（ [Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を参照）。

ステップ 4 名前を入力し、任意でオブジェクトの説明を入力します。

ヒント グループ名を入力することもできます。グループを使用すると、多くの FlexConfig オブジェクトを作成する場合にオブジェクトを見つけやすくなります。グループ名を入力するか、またはドロップダウン リストから既存のグループを選択します。

ステップ 5 コマンドがデバイス設定の末尾に追加されるように、タイプの [付加（Appended）] を選択したままにします。

ステップ 6 オブジェクトの内容を作成します。

a) FlexConfig 編集ボックス（大きな白いボックス）内をクリックし、**interface** に続けてスペースを入力します。
b) 右クリックし、[テキストオブジェクトの作成（Create Text Object）] を選択します。
c) [テキストオブジェクトの作成（Create Text Object）] ダイアログボックスで、名前として **inside**、値として **serial0** を入力します。[OK] をクリックして変数を追加します。
d) Enter を押して次の行に移動し、**crypto map** に続けてスペースを入力します。
e) 右クリックし、[テキストオブジェクトの作成（Create Text Object）] を選択します。
f) [テキストオブジェクトの作成（Create Text Object）] ダイアログボックスで、名前として **mapname**、値として **my_crypto** を入力します。[OK] をクリックして変数を追加します。

ステップ 7 編集ボックスの上にある [FlexConfigの検証（Validate FlexConfig）] アイコンボタンをクリックして、オブジェクトの整合性と展開可能性を確認します。エラーが特定された場合は、修正します。

ステップ 8 [OK] をクリックしてポリシーオブジェクトを保存します。これで、オブジェクトをデバイスのローカルまたは共有 FlexConfig ポリシーに追加できます。

FlexConfig システム変数

システム変数は、展開中、設定が生成されるときに値を参照します。Security Manager には、定義済みのシステム変数のセットが用意されており、これを使用して FlexConfig ポリシー オブジェクトを定義できます。値は、ターゲット デバイスに作成したポリシーから取得されます。これらの変数の値は、特に指定のないかぎり必須です。これらの変数の詳細については、次の表を参照してください。

- デバイス システム変数：表 81 : デバイス システム変数（すべてのデバイス タイプに適用） （439 ページ）。デバイスを検出または設定してこれらの変数の値を取得する方法の詳細については、デバイス インベントリの管理 （87 ページ）を参照してください。
- ファイアウォール システム変数：表 82 : ファイアウォール システム変数 （441 ページ）。ファイアウォール ポリシーの詳細については、ファイアウォール デバイスの管理 （2331 ページ）およびファイアウォール サービスの概要 （755 ページ）を参照してください。
- ルータ プラットフォーム システム変数：表 83 : ルータ プラットフォーム システム変数 （446 ページ）。ルータ ポリシーの詳細については、ルータの管理 （3001 ページ）を参照してください。

- VPN システム変数：表 84 : VPN システム変数 （447 ページ）。VPN ポリシーの詳細については、サイト間 VPN の管理：基本 （1379 ページ）を参照してください。
- リモートアクセス システム変数：表 85 : リモートアクセス システム変数 （453 ページ）。リモートアクセスポリシーの詳細については、リモートアクセス VPN の管理の基礎 （1655 ページ）を参照してください。

表 *81* : デバイス システム変数（すべてのデバイス タイプに適用）

名前	次元	説明
SYS_DEVICE_IDENTITY	[0]	[Tools] > [Device Properties] > [General] タブで定義された、Configuration Engine または Auto Update Server（AUS）によって管理されているデバイスの一意のデバイス アイデンティティ。これらのサーバによって管理されているデバイスのデバイス アイデンティティが必要です。
SYS_DOMAIN_NAME	[0]	[Tools] > [Device Properties] > [General] タブで定義された DNS ドメイン名。これは、[Platform] > [Device Admin] > [Hostname] ポリシーで定義された値と必ずしも同じではありません。
SYS_FW_OS_MODE	[0]	[Tools] > [Device Properties] > [General] タブで定義された FWSM または ASA デバイスのオペレーティング システム モード。値は、ROUTER（ルーテッド モード）、TRANSPARENT、または NOT_APPLICABLE です。
SYS_FW_OS_MULTI	[0]	FWSM または ASA がシングルコンテキスト モードまたはマルチコンテキスト モードのどちら（[Tools] > [Device Properties] > [General] タブで定義）で実行されているか。値は、SINGLE、MULTI、または NOT_APPLICABLE です。
SYS_HOSTNAME	[0]	[Tools] > [Device Properties] > [General] タブで定義されたデバイス ホスト名。これは、[Platform] > [Device Admin] > [Hostname] ポリシーで定義された値と必ずしも同じではありません。
SYS_IMAGE_NAME	[0]	[Tools] > [Device Properties] > [General] タブで定義されたデバイス イメージ名。

名前	次元	説明
SYS_INTERFACE_IP_LIST	1	インターフェイス ポリシーで設定されたインターフェイスの IP アドレスとマスク。 IP アドレスとマスクは、x.x.x.x/nn という形式になります（たとえば、10.20.1.2/24）。デバイスに定義されているインターフェイスがない場合、リストは返されません。 SYS_INTERFACE_NAME_LIST および SYS_INTERFACE_IP_LIST 内の各要素は、インターフェイスの同じインデックスを共有します。たとえば、SYS_INTERFACE_NAME_LIST 内の要素 3 が Ethernet1 である場合、SYS_INTERFACE_IP_LIST 内の要素 3 は Ethernet1 の IP アドレスです。Ethernet1 に IP アドレスがない場合、SYS_INTERFACE_IP_LIST 内の要素 3 は空になります。 この変数はオプションです。
SYS_INTERFACE_NAME_LIST	1	インターフェイス ポリシーで設定されたデバイス上のインターフェイスの名前。デバイスに定義されているインターフェイスがない場合、リストは返されません。詳細については、前述の SYS_INTERFACE_IP_LIST の説明を参照してください。 この変数はオプションです。
SYS_MANAGEMENT_IP	[0]	[Tools] > [Device Properties] > [General] タブで定義されたデバイスの管理 IP アドレス。
SYS_MDF_TYPE	[0]	デバイス モデルを示す Cisco MetaData Framework（MDF）デバイス タイプ。この値は、[Tools] > [Device Properties] > [General] タブに表示され、デバイスを Security Manager に追加するときに決定されます。
SYS_OS_RUNNING_VERSION	[0]	[Tools] > [Device Properties] > [General] タブに表示される、デバイスで実行されているオペレーティング システムのソフトウェア バージョン。たとえば、IOS プラットフォームでは 12.1, 12.2S などになります。この値は、デバイスからポリシーを検出するときに決定されます。
SYS_OS_TARGET_VERSION	[0]	[Tools] > [Device Properties] > [General] タブで定義された、デバイス設定の生成時に使用されるオペレーティング システム バージョン。

名前	次元	説明
SYS_OS_TYPE	[0]	[Tools] > [Device Properties] > [General] タブで定義されたデバイスのオペレーティング システム。値は、IOS、PIX、ASA、FWSM、またはIPSです。この値は、デバイスを Security Manager に追加するときに設定します。
SYS_SYS_OID	[0]	デバイスのシステム オブジェクトID（SysObjId）。デバイスを Security Manager に追加するときに決定されます。

表 *82 :* ファイアウォール システム変数

名前	次元	説明
SYS_FPM_INPUT_SP	1	「入力」方向の SYS_FPM_INTERFACE リスト内のエントリに対応するインターフェイスに適用される FPM ポリシーマップ名。 このデータは、Security Manager では設定されません。ルータの実行コンフィギュレーションから取得され、IOS_FPM FlexConfig で使用されます。
SYS_FPM_INTERFACE	1	インターフェイス名。 このデータは、Security Manager では設定されません。ルータの実行コンフィギュレーションから取得され、IOS_FPM FlexConfig で使用されます。
SYS_FPM_OUTPUT_SP	1	「出力」方向の SYS_FPM_INTERFACE リスト内のエントリに対応するインターフェイスに適用される FPM ポリシーマップ名。 このデータは、Security Manager では設定されません。ルータの実行コンフィギュレーションから取得され、IOS_FPM FlexConfig で使用されます。
SYS_FW_ACL_IN_NAME	1	インバウンド方向のトラフィック フィルタリング用にインターフェイスに適用される ACL の名前。各要素は、Cisco IOS ルータ、PIX ファイアウォール、ファイアウォール サービス モジュール、および ASA デバイスの SYS_INTERFACE_NAME_LIST 変数と 1 対 1 で対応します。 ファイアウォール アクセス ルールを設定して、この変数の値を生成します。

名前	次元	説明
SYS_FW_ACL_OUT_NAME	1	アウトバウンド方向のトラフィック フィルタリング用にインターフェイスに適用される ACL の名前。この配列の各要素は、Cisco IOS ルータ、PIX ファイアウォール、ファイアウォール サービス モジュール、および ASA デバイスの SYS_INTERFACE_NAME_LIST 変数と 1 対 1 で対応します。 Access Rules ポリシーを設定して、この変数の値を生成します。
SYS_FW_BRIDGE_INTERFACE_NAMES	1	ブリッジ インターフェイスの名前。 この変数は、IOS トランスペアレント ファイアウォールにだけ適用されます。 [Firewall] > [Transparent Rules] ポリシーを設定して、この変数の値を生成します。
SYS_FW_ETHERTYPERULE_ ACL_NAMES	1	着信または発信トラフィック フィルタリングのためにインターフェイスに適用される EtherType アクセス リストの名前。この配列の各要素は、SYS_FW_ETHERTYPERULE_INTERFACE_NAMES および SYS_FW_ETHERTYPERULE_DIRECTION_NAMES 変数の要素と 1 対 1 で対応します。 [Firewall] > [Transparent Rules] ポリシーを設定して、この変数の値を生成します。
SYS_FW_ETHERTYPERULE_ DIRECTION_NAMES	1	EtherType アクセス リストが適用される方向。値は「in」または「out」のいずれかです。各要素は、SYS_FW_ETHERTYPERULE_ACL_NAMES および SYS_FW_ETHERTYPERULE_INTERFACE_NAMES 変数の要素と 1 対 1 で対応します。 [Firewall] > [Transparent Rules] ポリシーを設定して、この変数の値を生成します。

名前	次元	説明
SYS_FW_ETHERTYPERULE_INTERFACE_NAMES	1	EtherType アクセス リストが適用されるインターフェイス名。各要素は、SYS_FW_ETHERTYPERULE_ACL_NAMES および SYS_FW_ETHERTYPERULE_DIRECTION_NAMES 変数と 1 対 1 で対応します。 [Firewall] > [Transparent Rules] ポリシーを設定して、この変数の値を生成します。
SYS_FW_INSPECT_IN_NAME	1	インバウンド方向の Cisco IOS ルータ インターフェイスに適用されるインスペクション ルールの名前。この配列の各要素は、Cisco IOS ルータの SYS_INTERFACE_NAME_LIST 変数と 1 対 1 で対応します。 [Inspection Rules] ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。
SYS_FW_INSPECT_OUT_NAME	1	アウトバウンド方向の Cisco IOS ルータ インターフェイスに適用されるインスペクション ルールの名前。この配列の各要素は、Cisco IOS ルータの SYS_INTERFACE_NAME_LIST 変数と 1 対 1 で対応します。 インスペクション ルール ポリシーをこの変数の値として設定します。 この変数はオプションです。
SYS_FW_INTERFACE_HARDWARE_ID_ LIST	1	デバイスのハードウェア ID。 デバイスで Interface ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。
SYS_FW_INTERFACE_NETWORK_LIST	1	デバイスのインターフェイス ネットワーク。 デバイスで Interface ポリシーを設定して、この変数の値を生成します。
SYS_FW_INTERFACE_SECURITY_LEVEL_LIST	1	デバイスのインターフェイス セキュリティ レベル。 デバイスで Interface ポリシーを設定して、この変数の値を生成します。

名前	次元	説明
SYS_FW_INTERFACE_STATE_LIST	1	デバイスのインターフェイス状態。 デバイスで Interface ポリシーを設定して、この変数の値を生成します。
SYS_FW_INTERFACE_VLAN_ID_LIST	[0]	デバイスの VLAN ID。 デバイスで Interface ポリシーを設定して、この変数の値を生成します。
SYS_FW_IPV6_ACL_IN_NAME	1	デバイスで In 方向に適用するすべての IPv6 ACL のリスト。 デバイスで In 方向に適用する IPv6 アクセス ルール ポリシーを設定して、この変数の値を生成します。
SYS_FW_IPV6_ACL_OUT_NAME	1	デバイスで Out 方向に適用するすべての IPv6 ACL のリスト。 デバイスで Out 方向に適用する IPv6 アクセス ルール ポリシーを設定して、この変数の値を生成します。
SYS_FW_MPCRULE_TRAFFICFLOW_TUNNELGROUPNAME	1	トラフィック フロー オブジェクトで指定されたトンネル グループの名前。 トラフィック フロー オブジェクトは PIX/ASA デバイスで **class-map** コマンドを設定し、トラフィック フロー オブジェクト内のトンネルグループの名前がこの変数に読み込まれます。この変数は、PIX/ASA デバイス上のトンネル グループを作成するために ASA_define_traffic_flow_tunnel_group FlexConfig オブジェクトによって使用されます。 この変数はオプションです。
SYS_FW_MULTICAST_PIM_ACCEPT_REG_ROUTEMAP	[0]	**pim accept-register route-map** コマンドで使用されるルートマップ名。 ルートマップの名前を入力し（[Platform] > [Multicast] > [PIM] > [Request Filter]）、FlexConfig でその機能を設定して、この変数の値を生成します。 この変数はオプションです。

名前	次元	説明
SYS_FW_NAT0_ACL_NAMES	1	**nat** *interface_name* **0 access-list acl_name** コマンドで使用される ACL の名前。 この変数はオプションです。
SYS_FW_OSPF_PROCESS_ID_LIST	1	PIX ファイアウォール、ファイアウォール サービス モジュール、および ASA デバイスにグローバルに設定される OSPF ルーティング プロセスの ID。 [Platform] > [Routing] > [OSPF] ポリシーを設定して、この変数の値を生成します。
SYS_FW_OSPF_REDISTRIBUTION_ROUTE_MAP_LIST	1	PIX ファイアウォール、ファイアウォール サービス モジュール、および ASA デバイスに設定された OSPF redistribute コマンドに適用されるルートマップの名前。 [Platform] > [Routing] > [OSPF] ポリシーを設定して、この変数の値を生成します。
SYS_FW_POLICY_NAT_ACL_NAMES	1	**policy nat** コマンド（0 以外のプール ID が指定された nat コマンド）で使用される ACL の名前。 NAT（[NAT] > [Translation Rules] > [Policy NAT]）を設定して、この変数の値を生成します。この変数は、PIX 6.3(3) 以上、PIX/ASA 7.x、8.0(x)、8.1(x)、8.2(x)、および FWSM デバイスにだけ適用されます。この変数は、Cisco IOS ルータには適用されません。 この変数はオプションです。
SYS_FW_POLICY_STATIC_ACL_NAMES	1	アクセスリストを含む **policy static** コマンドで使用される ACL の名前。 NAT 0（[NAT] > [Translation Rules] > [Policy NAT]）を設定して、この変数の値を生成します。変数には、**nat-0**、**policy nat**、および **policy static** コマンドで使用されるアクセスリスト名が含まれます。 この変数は、PIX 6.3(3) 以上、PIX/ASA 7.x、8.0(x)、8.1(x)、8.2(x)、および FWSM デバイスにだけ適用されます。この変数は、Cisco IOS ルータには適用されません。 この変数はオプションです。

表 *83 :* ルータ プラットフォーム システム変数

名前	次元	説明
SYS_ROUTER_BGP_AS_NUMBERS_LIST	1	デバイス上のボーダー ゲートウェイ プロトコル（BGP）および Exterior Gateway Protocol（EGP）の自律システム（AS）番号。 [Router Platform] > [Routing] > [BGP] ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。
SYS_ROUTER_EIGRP_AS_ NUMBERS_LIST	1	デバイス上の別の Enhanced Internet Gateway Routing Protocol（EIGRP）および Interior Gateway Protocol（IGP）の自律システム（AS）番号。 [Router Platform] > [Routing] > [EIGRP] ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。
SYS_ROUTER_OSPF_PROCESS_ IDS_LIST	1	デバイス上の Open Shortest Path First（OSPF）Interior Gateway Protocol（IGP）プロセス番号。 [Router Platform] > [Routing] > [OSPF Process] ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。
SYS_ROUTER_QOS_CLASS_MAP_LIST	1	デバイス上の QoS クラス マップの名前。 Quality of Service ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。
SYS_ROUTER_QOS_POLICY_MAP_LIST	1	デバイス上の QoS ポリシー マップの名前。 Quality of Service ポリシーを設定して、この変数の値を生成します。 この変数はオプションです。

表 *84 : VPN* システム変数

名前	次元	説明
トポロジ デバイスが参加している VPN に関連する変数。VPN を設定して、これらの変数の値を生成します。		
SYS_VPN_TOPOLOGY	1	バーチャル プライベート ネットワーク（VPN）トポロジ タイプ。値は、HUB_AND_SPOKE、POINT_TO_POINT、または FULL_MESH です。
SYS_VPN_TOPOLOGY_NAME	1	デバイスが参加している VPN トポロジの名前。
SYS_VPN_TOPOLOGY_ROLE	1	VPN 内のデバイスのロールに関する詳細。値は、PEER、HUB、または SPOKE です。
[デバイス （Devices）] デバイスが参加している VPN 内のデバイスに関連する変数。VPN を設定して、これらの変数の値を生成します。		
SYS_VPN_HOST_NAME	1	デバイスのホスト名。
SYS_VPN_LOCAL_PREFIXES	2	保護ネットワークのインターフェイスおよびネットワーク IP アドレス。
SYS_VPN_PRIVATE_INTERFACES	2	プライベート インターフェイスの名前。
SYS_VPN_PRIVATE_TUNNEL_ENDPT_IP	1	インターフェイス トンネル IP アドレス。
SYS_VPN_PUBLIC_INTERFACES	2	パブリック インターフェイスの名前。
SYS_VPN_TUNNEL_ENDPT_INTERFACE_IP	1	VPN エンドポイントの IP アドレス。IPSec では、エンドポイントは VPNインターフェイスであり、GRE ではトンネル ソースです。

名前	次元	説明
SYS_VPN_TUNNEL_ENDPT_ INTERFACE_NAME	1	VPN エンドポイントの名前。IPSec では、エンドポイントは VPN インターフェイスであり、GRE ではトンネル ソースです。
SYS_VPN_VPNSM_PUBLIC_IFC	2	Catalyst 6000 シリーズ スイッチのエクスポート ポート名。
Remote Peers デバイスが参加しているリモート ピアに関連する変数。VPN を設定して、これらの変数の値を生成します。		
SYS_VPN_REM_PEER_BAK_ LOGICAL_PRIVATE_IP	3	フェールオーバー ハブのリモート ピアのインターフェイス トンネル IP アドレス。この値は、Next Hop Resolution Protocol（NHRP）の DMVPN で使用されます。
SYS_VPN_REM_PEER_BAK_PREFIX	3	フェールオーバー ハブのリモート ピアの保護ネットワーク（インターフェイスおよびネットワーク IP アドレス）。
SYS_VPN_REM_PEER_BAK_PUBLIC_IP	3	フェールオーバー ハブのリモート ピアのパブリック インターフェイス名。
SYS_VPN_REM_PEER_BAK_TUNNEL_SRC	3	リモート ピアの VPN エンドポイントの IP アドレス。IPSec では、エンドポイントは VPN インターフェイスであり、GRE ではトンネル ソースです。
SYS_VPN_REM_PEER_DEVICE_NAME	2	リモート ピアのデバイス ホスト名。
SYS_VPN_REM_PEER_LOGICAL_ PRIVATE_IP	2	リモート ピアのインターフェイス トンネル IP アドレス。この値は、Next Hop Resolution Protocol（NHRP）の DMVPN で使用されます。
SYS_VPN_REM_PEER_PREFIX	3	リモート ピアの保護ネットワーク（インターフェイスおよびネットワーク IP アドレス）。

名前	次元	説明
SYS_VPN_REM_PEER_PRIVATE_IP	2	リモート ピアのプライベート インターフェイス名。
SYS_VPN_REM_PEER_PUBLIC_IP	2	リモート ピアのパブリック インターフェイス名。
SYS_VPN_REM_PEER_TUNNEL_SRC	2	トンネル ソース（リモート ピアのインターフェイス トンネルに含まれている場合）。
IPSec Proposal IPSec Proposal ポリシーに関連する変数。詳細については、サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）および VPN トポロジにおけるハイ アベイラビリティの設定 （1450 ページ）を参照してください。 IPSec Proposal ポリシーを設定して、この変数の値を生成します。		
SYS_VPN_CRYPTO_MAP_TYPE	1	クリプト マップ タイプ。値は、STATIC または DYNAMIC です。
SYS_VPN_DYNAMIC_CRYPTO_NAME	1	ダイナミック クリプト マップ名。
SYS_VPN_DYNAMIC_CRYPTO_NUM	1	ダイナミック クリプト マップ番号。
SYS_VPN_STATIC_CRYPTO_NAME	1	スタティック クリプト マップ名。
SYS_VPN_STATIC_CRYPTO_NAME_BAK	1	フェールオーバーハブのスタティック クリプト マップ名。
SYS_VPN_STATIC_CRYPTO_NUM	2	スタティック クリプト マップ番号。
SYS_VPN_STATIC_CRYPTO_NUM_BAK	2	フェールオーバーハブのスタティック クリプト マップ番号。
事前共有キー 事前共有キーおよび IKE プロポーザル ポリシーに関連する変数。詳細については、IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。		
SYS_VPN_IKE_AUTHENTICATION_MODE	1	IKE ポリシーの認証方式。値は、pre-share、rsa-sig、rsa-encr、または dsa-sig です。 IKE Proposal ポリシーを設定して、この変数の値を生成します。

名前	次元	説明
SYS_VPN_IKE_PRIORITY	1	IKE ポリシーのプライオリティ番号。 IKE Proposal ポリシーを設定して、この変数の値を生成します。
SYS_VPN_NEGOTIATION_MODE	1	ネゴシエーション方式。値は、MAIN_ADDRESS、MAIN_HOST、または AGGRESSIVE です。 Preshared Key ポリシーを設定して、この変数の値を生成します。
GRE モード GRE Modes ポリシーに関連する変数。詳細については、[GRE Modes] ページについて （1575 ページ）を参照してください。		
SYS_VPN_BAK_TUNNEL_IFC	2	フェールオーバー ハブのリモートピアのインターフェイス トンネル番号（たとえば、tunnel0）。 VPN を設定して、この変数の値を生成します。
SYS_VPN_SIGP_PROCESS_NUMBER	1	Interior Gateway Protocol（IGP）のプロセス番号。 GRE Modes ポリシーを設定して、この変数の値を生成します。
SYS_VPN_SIGP_ROUTING_PROTOCOL	1	使用される保護された Interior Gateway Protocol（IGP）のタイプ。値は、STATIC、OSPF、EIGRP、RIPV2、BGP、または ODR です。 GRE Modes ポリシーを設定して、この変数の値を生成します。
SYS_VPN_SPOKE_TO_SPOKE_ CONN	1	スポークツースポーク接続用に DMVPN を設定するかどうか。値は true または false です。 GRE Modes ポリシーを設定して、この変数の値を生成します。

名前	次元	説明
SYS_VPN_TUNNEL_IFC	2	リモート ピアのインターフェイス トンネル番号（たとえば、tunnel0）。 VPN を設定して、この変数の値を生成します。
VRF Virtual Routing and Forwarding（VRF）に関連する変数。詳細については、VRF 対応 IPsec の設定 （1445 ページ）を参照してください。 VPN VRF を設定して、これらの変数の値を生成します。		
SYS_VPN_VRF_AREA_ID	1	OSPF プロセス番号が選択された場合の領域 ID 番号。
SYS_VPN_VRF_MPLS_INTERFACE_IP	1	マルチプロトコル ラベル スイッチング（MPLS）インターフェイスの IP アドレス。
SYS_VPN_VRF_MPLS_INTERFACE_NAME	1	マルチプロトコル ラベル スイッチング（MPLS）インターフェイスの名前。
SYS_VPN_VRF_NAME	1	VRF 名。
SYS_VPN_VRF_PROCESS_NUMBER	1	Interior Gateway Protocol（IGP）プロセス番号。
SYS_VPN_VRF_RD	1	RD 値。
SYS_VPN_VRF_ROUTING_PROTOCOL	1	Interior Gateway Protocol（IGP）値。IGP は、プロバイダー エッジ（PE）/マルチプロトコル ラベル スイッチング（MPLS）ネットワークへの IPSec Aggregator のルーティングに使用されます。 値は、STATIC、OSPF、EIGRP、RIPV2、または BGP です。
SYS_VPN_VRF_SOLUTION	1	Virtual Routing and Forwarding（VRF）ソリューション。値は、1BOX または 2BOX です。

名前	次元	説明
CA 認証局ポリシーに関連する変数。詳細については、サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。		
SYS_VPN_CA_NAME	2	Certificate Authority（CA; 認証局）名。 PKI ポリシーを設定して、この変数の値を生成します。
EZVPN EZVPN に関連する変数。詳細については、Easy VPN について （1599 ページ）を参照してください。		
SYS_VPN_EZVPN_GROUP_NAME	2	ユーザ グループ名。 User Group ポリシーを設定して、この変数の値を生成します。
ダイヤル バックアップ ダイヤル バックアップ設定に関連する変数。詳細については、ダイヤル バックアップの設定 （1432 ページ）を参照してください。		
SYS_VPN_RTR_WATCH	1	RTR/監視番号。 ダイヤルバックアップを設定して、この変数の値を生成します。
GETVPN Group Encrypted Transport（GET）VPN に関連する変数。詳細については、Group Encrypted Transport（GET）VPN について （1619 ページ）を参照してください。		
SYS_GDOI_GROUP_NAME	1	Group Domain Of Interpretation（GDOI）グループの名前。 Group Encryption ポリシーを設定して、この変数の値を生成します（[Manage] > [Site-to-Site VPNs] > [Group Encryption Policy] > [Group Settings]）。

名前	次元	説明
SYS_GM_GET_ENABLED_INTF_NAME	1	プロバイダー エッジ（PE）へのVPN対応の外部インターフェイス。このインターフェイスで発信または終了するトラフィックは、暗号化または復号化が適宜評価されます。 グループ メンバーを設定して、この変数の値を生成します（[Manage] > [Site-to-Site VPNs] > [Group Members]）。
SYS_IPSEC_PROFILE_NAME	1	2 つのグループ メンバー間の IPsec 暗号化に使用されるパラメータを定義する、プロファイルの名前。 Group Encryption ポリシーを設定して、この変数の値を生成します（[Manage] > [Site-to-Site VPNs] > [Group Encryption Policy] > [Security Associations]）。
SYS_KS_REG_INTERFACE	[0]	Group Domain Of Interpretation（GDOI）登録を処理するために割り当てられるキーサーバのインターフェイス。登録インターフェイスが指定されていない場合、GDOI登録は任意のインターフェイスで行われる可能性があります。 キー サーバを設定して、この変数の値を生成します（[Manage] > [Site-to-Site VPNs] > [Key Servers]）。

表 *85 :* リモート アクセス システム変数

名前	次元	説明
SYS_ASA_RA_TUNNEL_GROUP_NAME	2	ASA デバイスのトンネル グループ名。
SYS_ASA_RA_USER_GROUP_NAME	2	ASA ユーザ グループの名前。
SYS_EZVPN_RA_DYNAMIC_CRYPTO_MAP_NAME	1	EZVPNのダイナミック クリプトマップ名。

名前	次元	説明
SYS_EZVPN_RA_DYNAMIC_CRYPTO_MAP_SEQ_NUM	1	EZVPN のダイナミック クリプト マップ番号。
SYS_EZVPN_RA_PUBLIC_INTERFACE_PIX	2	PIX ファイアウォールおよび ASA デバイス専用の EZVPN の外部インターフェイス名。
SYS_EZVPN_RA_STATIC_CRYPTO_MAP_NAME	1	EZVPN のスタティック クリプトマップ名。
SYS_EZVPN_RA_STATIC_CRYPTO_MAP_SEQ_NUM	1	EZVPN のスタティック クリプト マップ番号。
SYS_IOS_RA_CA_NAME	1	Cisco IOS デバイスの Certificate Authority（CA; 認証局）名。
SYS_IOS_RA_PUBLIC_INTERFACE	1	Cisco IOS デバイスの外部インターフェイス名。
SYS_IOS_RA_USER_GROUP	1	Cisco IOS デバイスのユーザ グループ名。
SYS_IOS_RA_VRF_NAME	1	Cisco IOS デバイスの Virtual Routing and Forwarding（VRF）名。

定義済みの FlexConfig ポリシー オブジェクト

Security Manager には、使用可能な定義済みの FlexConfig ポリシー オブジェクトが用意されています。これらのポリシーオブジェクトには、コマンドとスクリプトが事前に定義されています。

定義済みの FlexConfig ポリシー オブジェクトは読み取り専用オブジェクトです。これらの定義済みの FlexConfig ポリシー オブジェクトを編集するには、目的のオブジェクトを複製し、コピーに変更を加えて新しい名前で保存します。このようにすると、元の定義済みの FlexConfig は変更されません。これらの定義済みのポリシーオブジェクトのリストおよび各オブジェクトの詳細については、次の表を参照してください。

- 定義済みの ASA FlexConfig ポリシー オブジェクト：表 88 : 定義済みの Cisco IOS FlexConfig ポリシー オブジェクト （458 ページ）
- 定義済みの Catalyst FlexConfig ポリシー オブジェクト：表 87 : 定義済みの Catalyst 6500/7600 FlexConfig ポリシー オブジェクト （457 ページ）
- 定義済みの Cisco IOS FlexConfig ポリシー オブジェクト：表 88 : 定義済みの Cisco IOS FlexConfig ポリシー オブジェクト （458 ページ）
- 定義済みの PIX Firewall FlexConfig ポリシー オブジェクト：表 89 : 定義済みの PIX 6.3 Firewall FlexConfig ポリシー オブジェクト （459 ページ）

- 定義済みのルータ FlexConfig ポリシー オブジェクト：表 90 : 定義済みのルータ FlexConfig ポリシー オブジェクト （460 ページ）

表 *86 :* 定義済みの *ASA FlexConfig* ポリシー オブジェクト

名前	説明
ASA_add_ACEs	アクセス コントロール エントリ（ACE）をデバイス上のすべてのアクセス コントロール リストに追加します。
ASA_add_EtherType_ACL_remark	EtherType アクセス リスト名のリストをループし、ACE または備考をリストに追加します。EtherType アクセス リストは、Security Manager におけるファイアウォールのトランスペアレント ルールと同じです。この FlexConfig で CLI によって設定された備考は、トランスペアレント ルールの [description] フィールドに表示されます。
ASA_add_IPv6_ACEs	IPv6 アクセスリストのリストをループし、ACL の末尾に **deny ip any any log** エントリを追加します。
ASA_command_alias	**copy running-config** および **copy startup_config** コマンドに対して「save」という名前のコマンドエイリアスを作成します。
ASA_copy_image	TFTP サーバからフラッシュにイメージ パッケージをコピーします。
ASA_csd_image	ASA Cisco Secure Desktop イメージを提供します。Cisco Security Manager サーバー上の /CSCOpx/tftpboot/device-hostname から CSD イメージをデバイスにコピーし、CSD イメージパスを設定します。[デバイスのプロパティ（Device Properties）] にデバイスのホスト名を必ず入力してください。イメージ名がデフォルトと異なる場合は、[Device Properties] > [Policy Object Overrides] > [Text Objects] > [AsaCsdImageName] で上書きできます。イメージがコピーおよび設定されたあとでデバイスからのこの FlexConfig を割り当て解除します。
ASA_define_traffic_flow_tunnel_group	SYS_FW_MPCRULE_TRAFFICFLOW_TUNNELGROUPNAME システム変数内のサイト間 VPN トンネル グループを定義します。この変数には、トラフィック フロー オブジェクトに定義されているトンネル グループ名が読み込まれます。

名前	説明
ASA_established	セキュリティ アプライアンスを介したアウトバウンド接続のリターン アクセスを許可します。このコマンドは、あるネットワークからのアウトバウンド接続であり、かつ、セキュリティ アプライアンスによって保護されている元の接続と、外部ホスト上の同じ2つのデバイス間におけるインバウンドのリターン接続に対して機能します。 **established** コマンドを使用して、接続の検索に使用する宛先ポートを指定します。指定することで、コマンドをより詳細に制御でき、宛先ポートが既知で送信元ポートが不明なプロトコルがサポートされます。**permitto** および **permitfrom** キーワードでは、リターン インバウンド接続を定義します。
ASA_FTP_mode_passive	FTP モードをパッシブに設定します。
ASA_generate_route_map	[プラットフォーム（Platform）] > [マルチキャスト（Multicast）] > [PIM] > [要求フィルタ（Request Filter）] で設定された、**pim accept-register route-map** コマンドで使用されるルートマップを生成します。Cisco Security Manager は、**pim** コマンドで使用されるルートマップ名をエクスポートして、必要に応じて設定できるようにします。
ASA_IP_audit	**ip-audit** コマンドを使用して次の処理を実行します。 • 攻撃シグニチャと一致するパケットに対するデフォルト アクション（alarm、drop、reset）を設定します。 • 情報シグニチャと一致するパケットに対するデフォルト アクション（alarm、drop、reset）を設定します。 • パケットが定義済みの攻撃シグニチャまたは情報シグニチャと一致する場合に実行するアクション（alarm、drop、reset）を特定する名前付き監査ポリシーを作成します。 • 監査ポリシーのシグニチャをディセーブルにします。 • 監査ポリシーをインターフェイスに割り当てます。
ASA_MGCP	メディア ゲートウェイ コントロール プロトコル（MGCP）インスペクションのパラメータを定義するための特定のマップを示します。
ASA_no_router_Id	各 OSPF プロセスのルータ ID を削除します。
ASA_no_shut_Intf	デバイス上のすべてのインターフェイスをループし、イネーブルにします。

名前	説明
ASA_privilege	**configuration**、**show**、および **clear** コマンドの権限レベルを設定します。
ASA_route_map	各 OSPF プロセスの再配布ルート マップ名を定義します。
ASA_RSA_KeyPair_generation	証明書の RSA キー ペアをリセットし、生成します。
ASA_svc_image	ASA SSL VPN クライアント イメージを提供します。Cisco Security Manager サーバー上の /CSCOpx/tftpboot/device-hostname から SVC イメージをデバイスにコピーし、SVC イメージパスを設定します。[デバイスのプロパティ（Device Properties）] にデバイスのホスト名を必ず入力してください。イメージ名がデフォルトと異なる場合は、[Device Properties] > [Policy Object Overrides] > [Text Objects] > [AsaSvcImageName] で上書きできます。イメージがコピーおよび設定されたあとでデバイスからのこの FlexConfig を割り当て解除します。
ASA_sysopt	**sysopt** コマンドを使用して、次の手順を実行します。 • TCP 最大セグメント サイズが設定した値を超えないこと、または最小サイズが指定したサイズ未満であることを確認します。 • 最終的な通常の TCP クローズダウン シーケンスのあと、各 TCP 接続が 15 秒以上短縮 TIME_WAIT 状態で維持されるよう強制します。 • DNS A レコード アドレスを変更する DNS インスペクションをディセーブルにします。 • RADIUS アカウンティング応答内の認証キーを無視します。 • Web ブラウザがセキュリティ アプライアンス上の仮想 HTTP サーバを使用して再認証するときに、キャッシュからユーザ名とパスワードを入力できるようにします。
ASA_virtual	仮想 HTTP および Telnet サーバを設定します。

表 *87 :* 定義済みの *Catalyst 6500/7600 FlexConfig* ポリシー オブジェクト

名前	説明
Cat6K_ECLB_algorithm	モジュールの EtherChannel ロード バランス アルゴリズムを設定します。

名前	説明
Cat6K_ECLB_port_mode	IPS センサーが接続されている Catalyst トランクポートに EtherChannel を適用します。ポートがトランクモードで設定されていることを確認します。
Cat6K_ECLB_portchannel	ポート チャネルをトランク モードに設定し、トランクが許可された VLAN を追加します。
Cat6K_firewall_multiple_vlan_interfaces	複数の SVI をプロビジョニングする必要がある場合は、複数の VLAN インターフェイス モードを設定します。

表 *88* : 定義済みの *Cisco IOS FlexConfig* ポリシー オブジェクト

名前	説明
IOS_add_bridge_interface_desc	ブリッジインターフェイスのリストをループし、「this is a bridge interface」という説明を追加します。
IOS_CA_server	認証局サーバを設定します。
IOS_compress_config	大きな Cisco IOS 設定を圧縮します。
IOS_config_root_wireless_station	851 や 871 などの Cisco IOS ルータに、ワイヤレス LAN のルート無線ステーションを作成し、設定します。
IOS_console_AAA_bypass	次のシナリオの例を示します。 • 認証、許可、アカウンティング（AAA）アクセス コントロール モデルをイネーブルにします。 • ログイン時に AAA を設定します。 • ログインに対する AAA 認証をイネーブルにします。
IOS_Copy_Image	SVC イメージを Security Manager サーバからデバイスにコピーし、SVC イメージ パスを設定します。イメージがコピーおよび設定されたあとでデバイスからのこの FlexConfig を割り当て解除します。
IOS_enable_SSL	SSL をイネーブルにします。
IOS_FPM	トラフィック クラス定義ファイルをルータにコピーし、ポリシー マップを適用します。
IOS_IPS_PUBLIC_KEY	IOS IPS デバイスの公開キーを定義します。公開キーは、Security Manager がシグニチャ更新を実行するために必要です。

名前	説明
IOS_IPS_SIGNATURE_CATEGORY	ios_ips 基本カテゴリ内のシグニチャを除くすべてのシグニチャを再試行します。
IOS_PKI_with_AAA	サブジェクト名全体を使用して PKI AAA 認可を設定します。
IOS_set_clock	クロックを Security Manager サーバの現在の時刻に設定します。
IOS_VOIP_advance	POTS ポート番号をループし、電話番号とポート番号または IP アドレス番号に関連付けます。
IOS_VOIP_simple	POTS ポート番号を電話番号とポート番号に関連付けます。
IOS_VPN_config_gre_tunnel	VPN 変数を使用して、デバイスが参加している各 VPN の GRE トンネルを設定します。
IOS_VPN_set_interface_desc	VPN 変数を使用して、デバイスが参加している各 VPN のパブリック インターフェイスの説明を更新します。
IOS_VPN_shutdown_inside_interface	VPN 変数を使用して、デバイスが参加している各 VPN のすべての内部インターフェイスをシャットダウンします。
IOS_VRF_on_vFW	仮想ファイアウォール インターフェイスの Virtual Routing and Forwarding（VRF）を設定します。

表 *89 :* 定義済みの *PIX 6.3 Firewall FlexConfig* ポリシー オブジェクト

名前	説明
PIX6.3_nat0_acl_compiled	NAT 0 アクセス コントロール リストのコンパイルされたアクセス リストを生成します。
PIX6.3_policy_nat_acl_compiled	Policy NAT ACL のコンパイルされたアクセス リストを生成します。
PIX6.3_policy_static_acl_compiled	Policy Static ACL のコンパイルされたアクセス リストを生成します。
PIX_VPDN	Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）を設定します。

表 *90 :* 定義済みのルータ *FlexConfig* ポリシー オブジェクト

名前	説明
ROUTER_add_inspect_rules	インスペクション ルールをループし、追加します。
ROUTER_BGP_no_auto_summary	**no auto-summary** サブコマンドを使用して、各 BGP プロセスの自動ルート要約を無効にします。 この FlexConfig ポリシー オブジェクトは、SYS_ROUTER_BGP_AS_NUMBERS_LIST システム変数内のボーダー ゲートウェイ プロトコル（BGP）番号のリストを使用します。
ROUTER_BGP_untrusted_info	**distance bgp 255 255 255** サブコマンドを使用して、各ボーダー ゲートウェイ プロトコル（BGP）の BGP ルーティング情報を信頼できない情報とします。 この FlexConfig ポリシー オブジェクトは、SYS_ROUTER_BGP_AS_NUMBERS_LIST システム変数内の BGP 番号のリストを使用します。
ROUTER_EIGRP_min_cost_routes	複数のルートで同じ宛先ネットワークへのコスト ルートが異なる場合、最小コストルートを使用するようにトラフィックを設定します。このことを行うには、等コスト パスを持つ異なるインターフェイスに対してマルチインターフェイス ロード分割を使用します。 この FlexConfig ポリシー オブジェクトは、SYS_ROUTER_EIGRP_AS_NUMBERS_LIST システム変数内のルータの Enhanced Interior Gateway Routing Protocol（EIGRP）番号のリストを使用します。
Router_EIGRP_no_auto_summary	**no auto-summary** サブコマンドを使用して、各ルータの Enhanced Interior Gateway Routing Protocol（EIGRP）プロセスの自動ルート要約を無効にします。この FlexConfig ポリシー オブジェクトは、SYS_ROUTER_EIGRP_AS_NUMBERS_LIST システム変数内の EIGRP 番号のリストを使用します。
ROUTER_interface_prevent_dos_attacks	すべてのデバイス インターフェイスに対する Denial-of-Service（DoS; サービス拒絶）攻撃を阻止します。 この FlexConfig ポリシー オブジェクトは、SYS_INTERFACE_NAME_LIST システム変数内のインターフェイス名のリストを使用します。

名前	説明
ROUTER_OSPF_no_router_Id	各 OSPF プロセスのルータ OSPF ID を削除します。 この FlexConfig ポリシーは、SYS_ROUTER_OSPF_PROCESS_IDS_LIST システム変数内の OSPF ID のリストを使用します。
ROUTER_QoS_Class_Map _description	QoS クラス マップの説明を設定します。 この FlexConfig ポリシー オブジェクトは、SYS_ROUTER_QOS_CLASS_MAP_LIST システム変数内のルータ QOS クラス名のリストを使用します。
ROUTER_QoS_Policy_Map _description	QoS ポリシーの説明を設定します。 この FlexConfig ポリシー オブジェクトは、SYS_ROUTER_QOS_POLICY_MAP_LIST システム変数内のルータ QOS ポリシー名のリストを使用します。

FlexConfig ポリシーとポリシー オブジェクトの設定

FlexConfig ポリシー オブジェクトの作成および管理方法は、他のポリシー オブジェクトを作成する方法と同じです。ここでは、FlexConfig ポリシーとポリシー オブジェクトの作成方法について説明します。FlexConfig ポリシー オブジェクトに対して実行できるその他のタスク（削除など）については、ポリシー オブジェクトの操作：基本手順 （298 ページ）を参照してください。

- FlexConfig の作成シナリオ （461 ページ）
- FlexConfig ポリシー オブジェクトの作成 （465 ページ）
- FlexConfig ポリシーの編集 （473 ページ）

FlexConfig の作成シナリオ

このシナリオでは、Security Manager に付属している定義済みの FlexConfig ポリシー オブジェクトのいずれかを使用して、ASA デバイスのメディア ゲートウェイ コントロール プロトコル（MGCP）を設定する手順を示します。MGCP は、メディア ゲートウェイ（電話回線のオーディオをデータ パケットに変換するデバイス）を制御するためにコール エージェント アプリケーションによって使用されます。Security Manager では MGCP の設定はサポートされませんが、FlexConfig ポリシー オブジェクトを使用して設定を行うことができます。これは、FlexConfig を使用すると Security Manager ではサポートされない機能をネットワークに合わせてカスタマイズできることを示しています。

このシナリオでは、次の作業を実行します。

1. 既存のポリシー オブジェクトを複製して、ポリシー オブジェクトを作成します。

2. ポリシー オブジェクトをデバイスに割り当てます。
3. 設定をプレビューして、設定が正しいことを確認します。
4. ポリシー オブジェクトを別のデバイスと共有します。
5. 設定をデバイスに展開します。

定義済みの FlexConfig ポリシー オブジェクトのコピーを作成して変更したり、独自のオブジェクトを作成したりして、このシナリオを他の機能を実装するための例として使用できます。

はじめる前に

このシナリオ用に 2 つの ASA デバイスを Security Manager に追加します。

ステップ 1 次の手順を実行して、FlexConfig ポリシー オブジェクトを複製します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。
b) コンテンツテーブルから [FlexConfigs] を選択します。右ペインのテーブルには、既存の FlexConfig オブジェクトが一覧表示されます。
c) ASA_MGCP FlexConfig を右クリックし、[オブジェクトの複製（Clone Object）] を選択します。[Add FlexConfig] ダイアログボックスが表示されます（[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を参照）。
d) 新しい FlexConfig オブジェクトの名前（この例では MyASA_MGCP）を入力します。
e) 新しいグループ名とオブジェクトの説明を入力します。

ヒント グループ名と説明は任意です。作成するオブジェクトの説明とグループを設定することを推奨します。

f) [OK] をクリック新しい FlexConfig オブジェクトがリストに表示されます。

ステップ 2 $callAgentList テキスト オブジェクトを複製し、編集します。

元の ASA_MGCP FlexConfig オブジェクトは、テキスト オブジェクトである変数 $callAgentList を使用します。このテキストオブジェクトは読み取り専用であり、編集できません。このテキスト オブジェクトを複製すると、複製オブジェクトを編集してネットワーク設定に適用できます。

a) コンテンツテーブルから [テキストオブジェクト（Text Objects）] を選択します。
b) **callAgentList** を右クリックし、[オブジェクトの複製（Clone Object）] を選択します。[Add Text Object] ダイアログボックスが表示されます。
c) テキスト オブジェクトの名前を編集します。この例では、名前を mycallAgentList に変更します。
d) カラム A の最初の値をダブルクリックし、ネットワークのコール エージェントの IP アドレスを入力します。この例では、値を 10.10.10.10 に変更します。
e) カラム B の最初の値をダブルクリックし、ネットワークのコール エージェントのポート番号を入力します。この例では、値を 105 に変更します。
f) 別のコール エージェントの IP アドレスとポート番号の値を変更します。この例では、IP アドレスを 20.20.20.20 に変更し、ポート番号を 106 に変更します。または、ネットワーク内にコール エージェントが 1 つだけある場合、[Number of Rows] フィールドの数を減らすことによって、テーブルの 2 行目を

削除できます。同様に、コールエージェントが 3 つ以上ある場合は、このフィールドの数を増やすことによって、行を追加できます。

このことは、[Number of Columns] フィールドの増減によってカラム数を増減するのと似ています。

g) [OK] をクリック新しいテキスト オブジェクトがテキスト オブジェクトのリストに表示されます。

ステップ 3 次の手順を実行して、新しい変数を使用するように新しい FlexConfig ポリシー オブジェクトを編集します。

a) コンテンツテーブルから [FlexConfigs] を選択します。
b) MyASA_MGCP をダブルクリックします。[Edit FlexConfig] ダイアログボックスが表示されます。
c) $mycallAgentList を読み取るように $callAgentList を編集します。
d) [OK] をクリック

「次の変数は定義されていません：mycallAgentList 今すぐ定義しますか？（The following variables are undefined: mycallAgentList Define them now?）」という警告が表示されます。

e) 警告の [はい（Yes）] をクリックします。

[FlexConfig Undefined Variables] ダイアログボックスが表示され、[Variable Name] カラムに mycallAgentList が表示されます。

f) [オブジェクトタイプ（Object Type）] リストから [テキストオブジェクト（Text Objects）] を選択します。[Text Objects] ウィンドウが表示されます。
g) [使用可能なテキストオブジェクト（Available Text Objects）] リストから **mycallAgentList** を選択し、[OK] をクリックします。
h) [FlexConfig未定義変数（FlexConfig Undefined Variables）] ウィンドウで [OK] をクリックします。

[Edit FlexConfig] ダイアログボックスの [Variables] リストに mycallAgentList 変数が表示されます。

i) [FlexConfigの編集（Edit FlexConfig）] ダイアログボックスで、[OK] をクリックします。
j) [Policy Object Manager] ウィンドウを閉じます。

ステップ 4 次の手順を実行して、新しい FlexConfig ポリシー オブジェクトをデバイスに割り当てます。

a) デバイス ビューで、MGCP を設定するデバイスを選択します。
b) ポリシーセレクタから [FlexConfigs] を選択します。[FlexConfigs Policy] ページが表示されます。
c) [追加（Add）] ボタンをクリックします。[FlexConfigs Selector] ダイアログボックスが表示されます。
d) 新しい MyASA_MGCP FlexConfig ポリシーオブジェクトを選択し、[>>] をクリックしてポリシーオブジェクトを [選択されたFlexConfig（Selected FlexConfigs）] 列に追加します。

Ctrl キー（複数のオブジェクトを選択する場合）または Shift キー（複数の連続するオブジェクトを選択する場合）を押しながら選択すると、一度に複数のポリシー オブジェクトを選択できます。

e) [OK] をクリック

MyASA_MGCP ポリシー オブジェクトは設定にアペンドされるように設定されているため、このオブジェクトは [Appended FlexConfigs] テーブルに追加されます。設定の先頭に追加する FlexConfig ポリシー オブジェクトをプリペンドされるポリシー オブジェクトとして設定します。

f) [保存（Save）] をクリックします。

ステップ 5 次の手順を実行して、コマンドが生成されてデバイスに送信される前にコマンドをプレビューします。

a) [FlexConfigs Policy] ページで、MyASA_MGCP ポリシー オブジェクトを選択します。

b) [プレビュー（Preview）] をクリックします。

この FlexConfig ポリシー オブジェクトで生成されたコマンドおよび選択したデバイスに割り当てられている値が表示されます。変更された値を確認します。

例：

```
class-map sj_mgcp_class
  match access-list mgcp_list
  exit
mgcp-map inbound_mgcp
       call-agent 10.10.10.10 105
       call-agent 20.20.20.20 106
       gateway 10.10.10.115 101
       gateway 10.10.10.116 102
  command-queue 150
  exit
policy-map inbound_policy
  class sj_mgcp_class
    inspect mgcp inbound_mgcp
    exit
exit
service-policy inbound_policy interface outside
```

ステップ 6 MGCP を必要とする他の ASA デバイスがある場合は、次の手順を実行して、このポリシーをそれらのデバイスと共有できます。

a) ポリシーセレクタで [FlexConfigs] を右クリックし、[ポリシーの共有（Share Policy）] を選択します。

[Share Policy] ダイアログボックスが表示されます。

b) ポリシーの名前を入力し、[OK] をクリックします。この例では、MyShared_ASA_MGCP と入力します。

FlexConfigs ポリシーの上にあるバナーに、デバイスが共有ポリシーを使用していることと、ポリシーの名前が示されます。

c) FlexConfig バナーで、[Assigned To] フィールドのリンクをクリックします。この例では、リンクには [1個のデバイス（1 Device）] というラベルが付いています。これは、この共有ポリシーが 1 つのデバイス（表示しているデバイス）に割り当てられていることを示します。

リンクをクリックすると、[Shared Policy Assignments] ダイアログボックスが表示されます。このダイアログボックスを使用して、[使用可能なデバイス（Available Devices）] リストでこのポリシーを使用する他のデバイスを選択し、[>>] をクリックして、ポリシーが割り当てられているデバイスのリストに追加できます。

d) [OK] をクリック[Shared Policy Assignments] ダイアログボックスが閉じ、選択した追加デバイスが共有ポリシーを使用するように設定されます。バナーのリンクが変わり、現在このポリシーを使用しているデバイスの数が示されます（この例では [2個のデバイス（2 Devices）]）。

ヒント　ポリシー ビューからポリシーを共有することもできます。[ビュー（View）]>[ポリシービュー（Policy View）] を選択し、ポリシータイプセレクタで [FlexConfigs] を選択して MyShared_ASA_MGCP ポリシーを選択します。次に、[割り当て（Assignments）] タブをクリックし、ポリシーを割り当てるデバイスを選択して [>>] をクリックしてから [保存（Save）] をクリックします。

ステップ 7　変更を送信し、設定をデバイスに展開します。設定の展開の詳細については、展開および Configuration Archive の使用　（511 ページ）を参照してください。

FlexConfig ポリシー オブジェクトの作成

FlexConfig ポリシー オブジェクトを作成して、Security Manager でサポートされない機能をデバイスに設定できます。FlexConfig オブジェクトの詳細については、FlexConfig ポリシーとポリシー オブジェクトについて　（432 ページ）を参照してください。

ヒント　このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに FlexConfig ポリシー オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択　（288 ページ）を参照してください。

はじめる前に

コマンドがデバイスの VPN またはファイアウォール設定とまったく競合していないことを確認します。

次の点を考慮してください。

- Security Manager は、コマンドを操作または検証しません。コマンドをデバイスに展開するだけです。
- インターフェイスのコマンド セットが複数ある場合は、最後のコマンド セットだけが展開されます。したがって、開始コマンドと終了コマンドを使用してインターフェイスを設定しないことを推奨します。
- ルートマップを含む FlexConfig オブジェクト（たとえば、OSPF またはマルチキャストルートマップ）を編集する場合は、ルートマップの前に対応するアクセスコントロールリスト（ACL）を定義する必要があります。これはデバイスの要件です。ルートマップの前に ACL を定義しない場合は、展開エラーが発生します。

関連項目

- FlexConfig の作成シナリオ　（461 ページ）
- ポリシー オブジェクトの操作：基本手順　（298 ページ）
- ポリシー オブジェクトの作成　（299 ページ）
- ポリシーの管理　（209 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] ウィンドウを開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 ポリシー オブジェクト タイプ セレクタから [FlexConfigs] を選択します。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[FlexConfigオブジェクトの追加（Add FlexConfig Object）] ダイアログボックスが表示されます（[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を参照）。

ステップ 4 オブジェクトの名前を入力し、任意で説明を入力します。その他の任意の情報フィールドは次のとおりです。

- [Group]：既存のグループ名を選択するか、または新しいグループ名を入力します。この名前は、使用するオブジェクトの識別に役立ちます。
- [Negate For]：この FlexConfig オブジェクトが別のオブジェクトを無効にする設計になっている場合は、このオブジェクトによって取り消すコマンドを含むFlexConfigオブジェクトの名前を入力します。

ステップ 5 [Type] フィールドで、オブジェクト内のコマンドをSecurity Managerポリシーから生成された設定にプリペンド（設定の先頭に配置）するか、またはアペンド（設定の末尾に配置）するかを選択します。

ステップ 6 オブジェクト本体領域に、目的の設定ファイル出力を生成するためのコマンドと命令を入力します。次のタイプのデータを入力できます。

- 処理を制御するためのスクリプト作成コマンド。詳細については、スクリプト言語命令の使用 （434 ページ）を参照してください。
- FlexConfig ポリシー オブジェクトの展開先のデバイスで実行されているオペレーティング システムでサポートされる CLI コマンド。詳細については、FlexConfig ポリシー オブジェクトにおける CLI コマンドの使用 （433 ページ）を参照してください。
- 変数。右クリックメニューを使用して変数を挿入できます。これにより、単純な単一値テキスト変数の作成（[テキストオブジェクトの作成（Create Text Object）]）、既存のポリシーオブジェクトからの変数の選択（[ポリシーオブジェクトの挿入（Insert Policy Object）]）、またはシステム変数の選択（[システム変数の挿入（Insert System Variable）]）ができます。詳細については、FlexConfig オブジェクトの変数について （436 ページ）を参照してください。

ヒント 変数を削除する場合は、オブジェクト本体で変数を選択し、[Cut] ボタンをクリックするか、または Back Space キーか Del キーを押します。[OK] をクリックして変更を保存すると、変数が変数のリストから削除されます。

ステップ 7 オブジェクト本体の上にある [FlexConfigの検証（Validate FlexConfig）] アイコンボタンをクリックして、オブジェクトの整合性と展開の可能性を確認します。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス

[Add FlexConfig]/[Edit FlexConfig] ダイアログボックスを使用して、FlexConfig ポリシー オブジェクトを作成または編集します。FlexConfig オブジェクトは、Security Manager ポリシーから生成された設定の前後にコンフィギュレーション コマンドを追加できる小さなプログラムであり、製品の機能を拡張してデバイスを設定できます。これらのポリシー オブジェクトは、FlexConfig デバイスまたは共有ポリシーで使用します。

FlexConfig ポリシー オブジェクトを作成する前に、FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）の各項をお読みください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [FlexConfigs] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- FlexConfig ポリシー オブジェクトの作成 （465 ページ）
- FlexConfig ポリシーの編集 （473 ページ）

フィールド リファレンス

表 *91 : FlexConfig Editor* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成（299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
グループ	このオブジェクトが属している FlexConfig オブジェクトのグループの名前（ある場合）。名前を入力するか、またはリストから既存の名前を選択できます。このフィールドは情報提供だけを目的としており、Policy Object Manager の [FlexConfig Objects] ページで FlexConfig オブジェクトを検索するのに役立ちます。
タイプ（Type）	オブジェクト内のコマンドを設定にプリペンド（設定の先頭に配置）するか、またはアペンド（設定の末尾に配置）するか。

要素	説明
Negate For	この FlexConfig オブジェクトで取り消すコマンドを含む FlexConfig オブジェクトの名前。このフィールドは情報提供だけを目的としており、オブジェクトの処理には影響しません。 たとえば、FlexConfig A にコマンド **banner login** があり、FlexConfig B にコマンド **no banner login** がある場合、FlexConfig B は FlexConfig A の設定を無効にします。
FlexConfig Object Body	
[Object Body] 編集ボックス	目的の設定ファイル出力を生成するためのコマンドと命令。次のタイプのデータを入力できます。 • 処理を制御するためのスクリプト作成コマンド。詳細については、スクリプト言語命令の使用 （434 ページ）を参照してください。 • FlexConfig ポリシー オブジェクトの展開先のデバイスで実行されているオペレーティング システムでサポートされる CLI コマンド。詳細については、FlexConfig ポリシー オブジェクトにおける CLI コマンドの使用 （433 ページ）を参照してください。 • 変数。右クリックメニューを使用して変数を挿入できます。これにより、単純な単一値テキスト変数の作成（[テキストオブジェクトの作成（Create Text Object）]）、既存のポリシーオブジェクトからの変数の選択（[ポリシーオブジェクトの挿入（Insert Policy Object）]）、またはシステム変数の選択（[システム変数の挿入（Insert System Variable）]）ができます。詳細については、FlexConfig オブジェクトの変数について （436 ページ）を参照してください。
[Undo] ボタン	直前のアクションを取り消します。
[Redo] ボタン	直前に取り消したアクションを実行します。
[Cut] ボタン	強調表示されているテキストを削除し、クリップボードにコピーします。
[Copy] ボタン	強調表示されているテキストをクリップボードにコピーします。
[Paste] ボタン	直前に切り取ったテキストまたはコピーしたテキストを貼り付けます。
[Find] ボタン	オブジェクト本体の指定したテキスト文字列を検索します。
[Validate FlexConfig] ボタン	FlexConfig オブジェクトの整合性および展開の可能性を確認します。
FlexConfig Object Variables このテーブルには、FlexConfig オブジェクトで使用されている変数が一覧表示されます。	

要素	説明
名前	変数の名前。セルをクリックして名前を編集します。これにより、FlexConfig オブジェクト本体内の名前も変更されます。
デフォルト値（Default Value）	値が指定されていない場合に使用する値。セルをクリックして、ユーザ定義の変数の値を編集します。システム定義の変数は編集できません。 （注） オプションの変数を除き、デフォルト値が指定されていない場合は、変数の値を指定する必要があります。
Object Property	オブジェクトのプロパティ。オブジェクトのプロパティ名の形式は次のとおりです。 *type.name* .data.*property* ここで • [タイプ（Type）]：オブジェクトのタイプ。テキスト、ネットワーク、AAA サーバーなど。 • [名前（Name）]：オブジェクトの名前。 • [Data]：オブジェクトのプロパティがデータであることを示します。 • [プロパティ（Property）]：データのプロパティ。
次元	変数のデータの構造。値は以下のとおりです。 • 0：スカラ（単一の文字列） • 1：1 次元配列（文字列のリスト） • 2：2 次元配列（文字列のテーブル）
オプション	変数に値が必要かどうか。
説明	オブジェクトの内容の説明。セルをクリックして説明を編集します。

[Create Text Object] ダイアログボックス

[Create Text Object] ダイアログボックスをショートカットとして使用して、FlexConfig ポリシーオブジェクトで使用する次元 0 のテキストオブジェクト（単一値の変数）を作成します。変数の名前およびその変数に割り当てる値を入力します。[OK] をクリックすると、変数がカーソル位置の FlexConfig オブジェクトに追加され、オブジェクトの変数のリストに追加されます。

ナビゲーション パス

[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）で、オブジェクト本体のフィールドを右クリックし、[テキストオブジェクトの作成（Create Text Object）] を選択します。

ヒント　複数値のテキストオブジェクトを作成する場合は、右クリックして [ポリシーオブジェクトの挿入（Insert Policy Object）] > [テキストオブジェクト（Text Objects）] を選択し、使用可能なオブジェクトのリストの下にある [追加（Add）] ボタンをクリックします。詳細については、 [Add Text Object]/[Edit Text Object] ダイアログボックス （470 ページ）を参照してください。

[Add Text Object]/[Edit Text Object] ダイアログボックス

[Add Text Object]/[Edit Text Object] ダイアログボックスを使用して、テキスト オブジェクトを作成、編集、複製、および表示します。テキスト オブジェクトを受け入れる別のポリシー オブジェクトで、テキスト オブジェクトを参照または操作する必要がある場合は、テキスト オブジェクトを作成します。

テキスト オブジェクトは、ポリシー オブジェクト変数のタイプの 1 つです。これらの変数は名前と値のペアであり、値には単一の文字列、文字列のリスト、または文字列のテーブルを指定できます。FlexConfig ポリシーによる参照または操作の対象となる任意のタイプのテキストデータを入力できます。FlexConfig の詳細については、 FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

まず次元を選択して変数を作成します。たとえば、簡単な単一値の変数の場合は 0 次元、変数のリストの場合は 1 次元、変数のテーブルの場合は 2 次元を選択します。次元（および該当する場合は、行数とカラム数）を選択して目的のグリッドを作成したあと、まずセルをクリックして各セルにデータを入力します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [テキストオブジェクト（Text Objects）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 92 : [Text Object] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。

要素	説明
説明	（任意）最大 1024 文字のオブジェクトの説明。
次元	変数のデータの構造。 • 0：スカラ（単一の文字列） • 1：1 次元配列（文字列のリスト） • 2：2 次元配列（文字列のテーブル）
Number of Rows	1 次元または 2 次元の場合は、変数内のデータ行の数。
Number of Columns	2 次元の場合は、変数内のデータ カラムの数。
[text field]	テキスト オブジェクトの内容。セルをクリックしてデータを入力します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[FlexConfig Undefined Variables] ダイアログボックス

[FlexConfig Undefined Variables] ダイアログボックスを使用して、FlexConfig オブジェクトで使用される、まだ定義されていない変数を定義します。ポリシー オブジェクト タイプのリストから選択するか、または使用する新しいポリシー オブジェクトを追加できます。

テーブル内の各行は、単一の未定義の変数を表します。

ヒント 処理の制御のためにスクリプト言語で使用されるローカル変数を定義する必要はありません。変数の詳細については、FlexConfig オブジェクトの変数について （436 ページ）を参照してください。

ナビゲーション パス

[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）で変数名を入力してその変数の値を定義していない場合は、[OK] をクリックすると、Security Manager に警告が表示され、変数を定義するかどうか尋ねられます。[はい（Yes）] をクリックすると、このダイアログボックスが開きます。

フィールド リファレンス

表 *93 : [FlexConfig Undefined Variables]* ダイアログボックス

要素	説明
変数名	FlexConfig オブジェクトで使用されている未定義の変数の名前。
オブジェクト タイプ	変数に割り当てる値が含まれているポリシー オブジェクトのタイプ。ローカル変数の場合は、[Undefined] オブジェクト タイプを使用します。 定義する変数について、選択した変数に割り当てる特定のポリシー オブジェクトとそのオブジェクト内の値を選択する必要があります。 まず、このリストからポリシー オブジェクトのタイプを選択します。特定のポリシー オブジェクトを選択するように要求されます。[OK] をクリックすると、目的の値を含むそのオブジェクト内の特定のプロパティを選択するように要求されます（ [Property Selector] ダイアログボックス （472 ページ）を参照）。[プロパティセレクタ（Property Selector）] ダイアログボックスで値を選択し、[OK] をクリックすると、値が変数に割り当てられます。
Object Property	オブジェクトのプロパティ。詳細な説明については、[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を参照してください。
オプション	変数に値が必要かどうか。

[Property Selector] ダイアログボックス

[Property Selector] ダイアログボックスを使用して、FlexConfig ポリシー オブジェクト内の変数に割り当てる、選択したポリシー オブジェクト内の特定のプロパティを選択します。ダイアログボックスのタイトルは、選択したポリシー オブジェクトのタイプを示します（たとえば、[AAA Server Groups Property Selector]）。

変数の詳細については、 FlexConfig オブジェクトの変数について （436 ページ）を参照してください。

ナビゲーション パス

- [Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）で右クリックし、[ポリシーオブジェクトの挿入（Insert Policy Object）] メニューから特定のポリシー オブジェ

クト グループ タイプを選択し、要求されたら特定のポリシーオブジェクトを選択して [OK] をクリックします。

- [FlexConfig Undefined Variables] ダイアログボックス （471 ページ）で [オブジェクトタイプ（Object Type）] フィールドからポリシーオブジェクトタイプを選択し、要求されたら特定のポリシーオブジェクトを選択して [OK] をクリックします。

フィールド リファレンス

表 *94 : [Property Selector]* ダイアログボックス

要素	説明
Object Property	変数に割り当てる値が含まれているオブジェクトのプロパティ。プロパティの詳細については、それらのオブジェクトの設定に関連する項目を参照してください。
名前	変数の名前。このフィールドは、未定義の変数を定義している場合には使用できません。
説明	（任意）変数の説明。このフィールドは、未定義の変数を定義している場合には使用できません。

FlexConfig ポリシーの編集

デバイスビューまたはポリシービュー（共有ポリシーの場合）でポリシーセレクタから [FlexConfigs] を選択して、FlexConfig ポリシーをデバイスに割り当てることができます。Security Manager によって生成された設定を展開する場合と同様に、これらのポリシーを含む設定を展開できます。FlexConfig ポリシー オブジェクトを設定して共有 FlexConfig ポリシーを作成する手順のシナリオについては、FlexConfig の作成シナリオ （461 ページ）を参照してください。

（注） [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] ページの [新規または変更済みFlexConfigのみを展開する（Deploy only new or modified FlexConfigs）] 設定を有効にした場合、変更のあるアクティビティを開いているときに、FlexConfig を展開しようとすると、Cisco Security Manager は、（他のアクティビティの変更ではなく）開いているアクティビティのみに固有の FlexConfig の変更を考慮します。一方、すべてのアクティビティが送信済みで、開いているアクティビティがない場合、Security Manager は、変更とともに送信された、最後に送信されたアクティビティに固有の FlexConfig の変更を考慮します。そのため、展開中にアクティビティを反映させるために FlexConfig の変更が必要な場合は、変更が単一のアクティビティで実行され、送信され、展開されていることを確認してください。

FlexConfig ポリシーを編集するときに、次のアクションを実行できます。

- **FlexConfig オブジェクトの追加**：FlexConfig オブジェクトをポリシーに追加するには、[追加（Add）] アイコンボタンをクリックし、目的のオブジェクトを選択します。オブジェクト セレクタ ダイアログボックスから新しいオブジェクトを作成することもできます。オブジェクトは、その定義方法に応じて、プリペンド リストまたはアペンド リストに追加されます。
- **FlexConfig オブジェクトの削除**：ポリシーにオブジェクトを含める必要がなくなった場合は、そのオブジェクトを選択し、[削除（Remove）] アイコンボタンをクリックします。このアクションによって、オブジェクトはポリシーから削除されますが、Security Manager からは削除されません。オブジェクトの削除の詳細については、オブジェクトの削除（308 ページ）を参照してください。
- **オブジェクトの順序の変更**：オブジェクトは、指定した順序で処理されます。オブジェクトが別のオブジェクトの処理に依存している場合は、オブジェクトの順序を正しく指定することが重要です。順序を変更するオブジェクトを選択し、オブジェクトが目的の位置に配置されるまで上矢印ボタンまたは下矢印ボタンをクリックします。

ルートマップを含む FlexConfig オブジェクト（たとえば、OSPF またはマルチキャスト ルートマップ）の順序を変更する場合は、ルートマップの前に対応するアクセス コントロール リスト（ACL）が定義されていることを確認します。これはデバイスの要件です。ルートマップの前に ACL を定義しない場合は、展開エラーが発生します。

- **ポリシーオブジェクトで使用されている変数に割り当てられた値の変更**：オブジェクトのデバイスレベルのオーバーライドを作成して、特定のデバイスについて変数に別の値を設定する場合は、オブジェクトを選択し、[値（Values）] をクリックします。[Values Assignment] ダイアログボックスで、[Values] セルをクリックして値を変更します。詳細については、[Values Assignment] ダイアログボックス （476 ページ）を参照してください。
- **ポリシーオブジェクトに対して生成される CLI のプレビュー**：デバイスビューで、オブジェクトを選択し、[プレビュー（Preview）] をクリックして、ポリシーオブジェクトに対して生成される CLI を表示できます。このことは、生成される CLI コマンドがデバイスに実装する予定のコマンドであることを確認する場合に、特に役立ちます。

（注） 展開中、Security Manager サーバで FlexConfig ポリシー オブジェクトがコンパイルされるときに、正しいシステム変数値と設定がコマンドの生成に使用されます。ただし、プレビュー機能では展開時の通常の方法ではこれらの値にアクセスできないため、一部の CLI コマンドが表示されない場合があります。さらに、プレビュー機能によってクライアントに CLI コマンドが生成されるため、FlexConfig ポリシー オブジェクトで使用される一部のマクロがサーバ設定ではなくクライアント設定に反映されます。

関連項目

- FlexConfig オブジェクトの変数について （436 ページ）
- FlexConfig ポリシー オブジェクトの作成 （465 ページ）

- ポリシーの管理 （209 ページ）
- 展開の管理 （481 ページ）

[FlexConfig Policy] ページ

[FlexConfig Policy] ページを使用して、FlexConfig ポリシーを作成します。FlexConfig ポリシーには、FlexConfig ポリシー オブジェクトの順序リストが含まれます。これらのオブジェクトは、Security Manager の機能を拡張してデバイスを設定できるサブルーチンです。FlexConfig ポリシー オブジェクトの詳細については、 FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [FlexConfigs] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [FlexConfigs] を選択し、既存のポリシーを選択するか、または [ポリシーの作成（Create a Policy）] ボタンをクリックして新しいポリシーを作成します。

関連項目

- FlexConfig ポリシー オブジェクトの作成 （465 ページ）

フィールド リファレンス

表 95 : [FlexConfigs Policy] ページ

要素	説明
Prepended FlexConfigs	設定の先頭に追加される FlexConfig ポリシー オブジェクト。オブジェクトは示されている順序で処理されます。
Appended FlexConfigs	設定の末尾に追加される FlexConfig ポリシー オブジェクト。オブジェクトは示されている順序で処理されます。
[Values] ボタン	このボタンをクリックすると、 [Values Assignment] ダイアログボックス （476 ページ）を使用して、選択した FlexConfig ポリシー オブジェクトで使用されている変数に割り当てられた値を表示、変更、または検証できます。
[Preview] ボタン （デバイス ビューだけ）	このボタンをクリックすると、選択した FlexConfig ポリシー オブジェクトに対して生成される CLI コマンドを表示できます。 ポリシービューでは、まず [値（Values）] をクリックし、[値の割り当て（Values Assignment）] ダイアログボックスでデバイスを選択して [プレビュー（Preview）] をクリックすると、CLI をプレビューできます。

要素	説明
上下の矢印ボタン	選択したオブジェクトをリスト内で上下に移動するには、これらのボタンをクリックします。オブジェクトは表示された順序で処理されるため、処理が別のオブジェクトの処理に依存するオブジェクトは、そのオブジェクトが依存するオブジェクトのあとに配置することが重要です。
[追加（Add）] ボタン	このボタンをクリックすると、FlexConfig ポリシー オブジェクトがポリシーに追加されます。オブジェクト自体に、プリペンド リストに追加されるか、またはアペンド リストに追加されるかが定義されています。新しい FlexConfig オブジェクトを作成するか、または既存のオブジェクトを選択できます。
[編集（Edit）]ボタン	このボタンをクリックすると、選択した FlexConfig ポリシー オブジェクトを編集できます。変更は、編集したオブジェクトを使用するすべてのデバイスに反映されます。つまり、変更はデバイスのローカル ポリシー オブジェクトのオーバーライドではありません。 （注） Security Manager に付属している定義済みの FlexConfig ポリシー オブジェクトまたは編集権限がないオブジェクトを選択した場合は、オブジェクト定義の表示だけが許可されます。
[Remove] ボタン	このボタンをクリックすると、選択したオブジェクトがポリシーから削除されます。Security Manager からは削除されず、FlexConfig ポリシーから削除されるだけです。

[Values Assignment] ダイアログボックス

[Values Assignment] ダイアログボックスを使用して、FlexConfig ポリシー オブジェクトで使用されている変数を表示したり、オブジェクトを検証したり、オブジェクトから生成される CLI をプレビューしたりします。詳細については、FlexConfig オブジェクトの変数について （436 ページ） [FlexConfig Policy] ページ （475 ページ） を参照してください。

ナビゲーション パス

[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）でオブジェクトを選択し、[値（Values）] をクリックします。

フィールド リファレンス

表 *96 : [Values Assignment]* ダイアログボックス

要素	説明
[Assigned Devices] （ポリシー ビューだけ）	共有 FlexConfig ポリシーが割り当てられているデバイス。変数値を表示するデバイスを選択します。
名前	変数の名前。
値	変数に使用する値。値を変更するには、セルをダブルクリックします。この値を変更すると、Security Manager によって、ポリシー オブジェクトのデバイスレベルのオーバーライドが作成されます。値を上書きできないようにポリシー オブジェクトが設定されている場合は、値を編集できません。 変数のデフォルト値が設定されていない場合は、オプションの変数の場合を除き値を指定する必要があります。
デフォルト値（Default Value）	ポリシー オブジェクトの変数に割り当てられている値。このセルをダブルクリックすると、変数の値を定義するポリシーオブジェクトの定義が表示されます。
オーバーライド	変数の値を上書きできるかどうか。値を編集できるのは、このカラムにチェックマークが付いている変数だけです。
Object Property	オブジェクトのプロパティ。詳細な説明については、[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を参照してください。
次元	変数のデータの構造。 • 0：スカラ（単一の文字列） • 1：1 次元配列（文字列のリスト） • 2：2 次元配列（文字列のテーブル）
オプション	変数値を空にできるかどうか。
説明	変数の説明。
[Validate] ボタン	このボタンをクリックすると、Velocity テンプレート言語の構文を検証し、すべての必須変数に値が指定されていること、変数が SYS_ で始まらないこと、および参照先のポリシー オブジェクトが存在することを確認できます。

要素	説明
[Preview] ボタン	このボタンをクリックすると、選択した FlexConfig ポリシー オブジェクトに対して生成される CLI コマンドが表示されます。

[FlexConfig Preview] ダイアログボックス

[FlexConfig Preview] ダイアログボックスを使用して、FlexConfig ポリシーに定義されている選択オブジェクトの変数に基づいて生成される CLI コマンドを表示します。

ナビゲーション パス

FlexConfig ポリシーのプレビュー ダイアログボックスを開くには、次のいずれかを実行します。

- [Values Assignment] ダイアログボックス （476 ページ）で、[プレビュー（Preview）] をクリックします。ポリシービューでは、最初にデバイスを選択する必要があります（デバイスビュー）。デバイスを選択し、[FlexConfig] をクリックします（[FlexConfig Policy] ページ （475 ページ）を参照）。FlexConfig ポリシー内のオブジェクトを選択し、[プレビュー（Preview）] をクリックします。

FlexConfig のトラブルシューティング

問題：Cisco Security Manager クライアントを使用して FlexConfig を追加すると、次のエラーメッセージが表示される場合があります。

```
Syntax Error: Failed to setup Velocity Engine to validate syntax.
```

この問題は、Microsoft Windows の管理者権限が原因です。Microsoft Windows Vista および Microsoft Windows 7 で FlexConfig 機能を使用する場合、Security Manager は管理者権限を要求します。

解決策：この問題を解決するには、次のいずれかの方法で、管理者権限を使用して Security Manager クライアントを起動します。

- 管理者権限で Security Manager クライアントを起動するには、[Configuration Manager] ショートカットを右クリックし、[管理者として実行（Run as administrator）] を選択します。
- Security Manager クライアントの管理者権限を永続的に有効にするには、[Configuration Manager] ショートカットを右クリックし、[プロパティ（Properties）] を選択します。[互換性（Compatibility）] タブで、[管理者としてこのプログラムを実行する（Run this program as an administrator）] を選択し、[OK] を選択します。

問題：FlexConfig を使用して ASA ファイアウォールに **reload in x noconfirm** と **reload cancel** の 2 つのコマンドを 1 つのジョブで展開すると、次のエラーメッセージが表示されます。

```
An error response from the device prevented successful completion of this
```

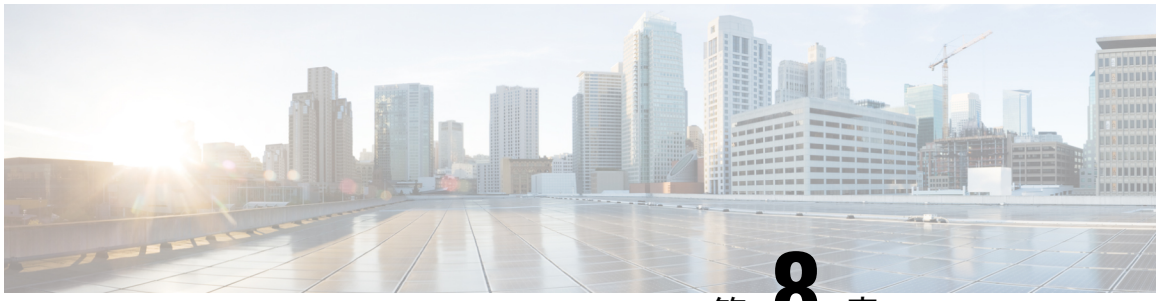
```
operation. The device provided the following description: reload cancel No
reload is scheduled
```

残念ながら、両方のコマンドがあまりにも速くプッシュされ、デバイスでリロードスケジュールがアクティブ化される前に **reload cancel** が送信されるため、展開は常に失敗します。

解決策：この問題を回避するには、手動で作成した2つの別個の展開でコマンドを送信する必要があります。

問題：FlexConfig がデバイスに割り当てられて展開されている場合、FlexConfig がデバイスから削除された後でも、完全な設定プレビューに FlexConfig が表示されることがあります。

解決策：回避する必要はありません。展開中はデルタ設定のみがデバイスにプッシュされるため、FlexConfig は展開に含まれません。



第 8 章

展開の管理

Security Manager に定義する設定およびポリシーは、ネットワークに実装できるようにデバイスに展開する必要があります。設定をデバイスに展開するための手順は、Workflow モードまたは Workflow 以外のモードのいずれを使用しているのかによって異なります。Workflow 以外のモードが Security Manager の操作のデフォルト モードですが、社内で必要な場合には Workflow モードを使用できます。詳細については、ワークフローおよびアクティビティの概要 （26 ページ）を参照してください。

ここでは、各 Workflow モードで設定をデバイスに展開する方法について説明します。

- 展開について （481 ページ）
- Deployment Manager および Configuration Archive の概要 （497 ページ）
- 展開および Configuration Archive の使用 （511 ページ）
- 設定のロールバック （560 ページ）

展開について

展開ジョブでは、設定変更をデバイスに送信する方法を定義します。展開ジョブでは、設定を展開するデバイスや設定をデバイスに展開するための方法など、パラメータをいくつか定義できます。また、展開スケジュールを作成して、一定の間隔で展開ジョブを自動的に生成できます。

以降のトピックは、展開ジョブの理解を深めて、効果的に使用するのに役立ちます。

- 展開プロセスの概要 （482 ページ）
- Workflow 以外のモードでの展開 （484 ページ）
- Workflow モードでの展開タスク フロー （486 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開方法について （490 ページ）
- デバイス OS バージョン不一致の処理 （495 ページ）

展開プロセスの概要

展開とは、大まかに言うと、3つの手順からなるプロセスです。各手順を次の表で説明します。

表 *97 :* 展開プロセスの概要

手順	導入手順
ステップ 1	Security Manager は、デバイスの現在の設定を取得し、その設定を Security Manager に保存されているデバイスの最新のポリシーと比較します。Security Manager で現在の設定と見なされるものは、デバイスのタイプ、展開方法、および展開プリファレンスの設定によって異なります。次に、ソースになりうるものと、そのソースが使用される条件を示します。 • デバイスから現在実行中の設定を取得します。 実行コンフィギュレーションは、展開方法が AUS、TMS、または CNS でないかぎり、デバイスに展開するときに使用されます。展開の環境設定として（**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、[展開（Deployment）] を選択） [デバイスへの展開時に次の場所から参照設定を取得：設定アーカイブ（When Deploying to Device Get Reference Config from: Config Archive）] を選択すると、Security Manager で強制的に Configuration Archive を使用できます。 • Security Manager Configuration Archive から最後の完全な設定を取得します。Configuration Archive は、次の場合に使用されます。 • ファイルを展開する場合。ただし、展開の環境設定として [デバイスへの展開時に次の場所から参照設定を取得：デバイス（When Deploying to File Get Reference Config from: Device] を選択した場合を除きます。 • 展開方法が TMS または CNS である場合。 • デバイスが Security Manager によって管理されていない場合。 • デバイスに展開する場合（ただし、失敗したデバイスから設定をアップロードする場合）。Configuration Archive は、ライブ デバイスから設定を取得するためのバックアップとして使用されます。 • プレビュー設定の場合。 • 工場出荷時のデフォルト設定を使用します。 工場出荷時のデフォルト設定は、AUS 展開方法を使用する場合に、PIX デバイスまたは ASA デバイスで使用されます。展開および設定プレビューに使用されます。
ステップ 2	Security Manager は、デルタ設定を構築します。デルタ設定には、デバイス設定と割り当てられたポリシーの一貫性を確保できるよう、デバイス設定を更新するために必要なコマンドが含まれています。このほか、完全なデバイス設定も構築します。

手順	導入手順
ステップ 3：	デバイスに展開している場合、Security Manager は使用している展開方法に応じてデルタ設定または完全な設定を展開します。ファイルに展開している場合、Security Manager は次の 2 つのファイルを作成します。デルタ設定用の *device_name*_delta.cfg と、完全な設定用の *device_name*_full.cfg です。どちらの場合も、設定は Configuration Archive にも追加されます。次に、展開方法に基づいた処理を示します。 • SSL（HTTPS）、SSH、または Telnet：Security Manager は直接デバイスに問い合わせて、デルタ設定をそのデバイスに送信します。 • PIX デバイスおよび ASA デバイスの Auto Update Server（スタンドアロンまたは Configuration Engine で稼働）：Security Manager は Auto Update Server にすべての設定を送信し、デバイスはサーバから設定を取得します。デルタ設定は送信されません。 • IOS デバイスの Configuration Engine：Security Manager は Configuration Engine にデルタ設定を送信し、デバイスはエンジンから設定を取得します。 • TMS：Security Manager は TMS サーバにデルタ設定を送信します。サーバから eToken に設定をダウンロードし、デバイス上にロードできます。

展開中に、デバイスの設定が最後に展開された設定と異なることを Security Manager が確認した場合、デフォルトでは変更が上書きされます。この動作は、展開の環境設定を使用して制御できます。そのためには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、[展開（Deployment）] を選択し、[アウトオブバンド変更の検出時（When Out of Band Changes Detected）] 設定を探します。ジョブの展開方法を編集して、特定の展開ジョブのためにこの動作を制御することもできます。

Security Manager の管理外でデバイス設定に変更を加えた場合、その変更を Security Manager に反映させるには 2 つの選択肢があります。

1. デバイスでポリシーを再検出できます。その場合、デバイスのすべてのポリシーがローカル ポリシーになり、デバイスに割り当てていた共有ポリシーがあればすべて削除されます。
2. Security Manager で必要な変更を加えて、デバイスに再展開できます。展開中は、アウトオブバンド変更がデバイスで見つかった場合に強制的にエラーにするオプションを選択しないでください。この方法を推奨します。

アウトオブバンド変更が展開に与える影響の詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

設定の展開後、Security Manager が制御する設定に変更を加えるときには、Security Manager だけを使用してください。Security Manager が制御する設定は、オペレーティング システムによって異なります。IPS デバイスの場合、Security Manager は設定全体を制御します。IOS、ASA、PIX、FWSM の各デバイスの場合、Security Manager が制御するデバイス設定のさまざまな側面を柔軟に制御できます。Security Manager でルーティング ポリシーなど機能のポリシーを作成しない場合、Security Manager はデバイスでその機能を制御しません。機能のポリシーを作成

すると、Security Managerに定義した設定でデバイスの設定が上書きされます。管理設定では、デバイスに使用可能なポリシーのタイプを制御して、Security Manager で機能のポリシーを表示または変更できないようにすることができます。使用可能な機能を参照し、Security Managerでの管理対象にするかどうかを制御するには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、[ポリシー管理（Policy Management）] を選択します。Security Manager は、VPN 関連のポリシーを管理します。

関連項目

- Workflow 以外のモードでの展開 （484 ページ）
- Workflow モードでの展開タスク フロー （486 ページ）
- [Deployment] ページ （658 ページ）
- [Policy Management] ページ （729 ページ）

Workflow 以外のモードでの展開

以降のトピックは、Workflow 以外のモードで展開を理解するのに役立ちます。

- Workflow 以外のモードでの展開 （484 ページ）
- Workflow 以外のモードでのジョブの状態 （485 ページ）

Workflow 以外のモードでの展開タスク フロー

Workflow 以外のモードでの展開タスク フローは、3 つの簡単な手順で構成されています。

1. **ジョブの作成**：次のいずれかを実行すると、展開ジョブが作成されます。
   - [メイン（Main）] ツールバーの [変更の送信と展開（Submit and Deploy Changes）] ボタンをクリックするか、**[ファイル（File）] > [送信して展開（Submit and Deploy）]** を選択します。

（注） これらのオプションは、チケット管理が有効になっている場合は使用できません。

   - **[ファイル（File）] > [展開（Deploy）]** を選択します。
   - **[管理（Manage）] > [展開（Deployments）]** を選択し、[展開（Deploy）] をクリックします。

1. **ジョブの定義**：どのデバイスに設定を展開するのか、直接デバイスに展開するのかファイルに展開するのかなど、パラメータを指定します。

   この手順では、設定をプレビューし、その設定を以前に展開した設定またはデバイスで現在実行中の設定と比較することもできます。

（注） あるジョブのために選択したデバイスをそれ以外のジョブに含めることはできません。この制約により、ポリシーを展開する順序が常に正しいものとなります。ただし、展開スケジュールに指定されているデバイスは含めることができます。

2. **ジョブの展開**：ジョブを展開すると、生成したCLIが直接または中間転送サーバー（AUS、CNS、TMSなど）経由でデバイスに送信されるか、または出力ファイルに送信されます。宛先（デバイスまたはファイル）は、ジョブを定義するときに選択します。転送サーバはデバイスのプロパティで指定します。展開方式と転送サーバを定義する方法については、展開方法について （490 ページ）を参照してください。

Workflow 以外のモードでのジョブの状態

Workflow 以外のモードでは、[Deployment Manager] ウィンドウの [Status] 列に、各ジョブの状態が表示されます。次の表に、Workflow 以外のモードでのジョブの有効な状態とその説明を示します。詳細については、[Deployment Manager] ウィンドウ （499 ページ）を参照してください。

表 *98 : Workflow* 以外のモードでのジョブの状態

状態	説明
導入済み	ジョブに含まれるすべてのデバイスの設定が、デバイスまたは設定ファイルに正常に展開されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
展開	ジョブに生成された設定を、デバイスまたは Security Manager サーバのディレクトリに展開しています。[Deployment Status] ウィンドウがまだ開かれていない場合には、[Deployment Manager] ウィンドウでジョブの経過表示をモニタできます。
中断	ジョブが手動で停止されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
失敗しました（Failed）	ジョブに含まれる 1 つまたは複数のデバイスへの展開に失敗しました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
Rolling Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定を展開しています。[Rolling Back] 状態にあるジョブは中断可能です。
Rolled Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定の展開に成功しました。

Workflow モードでの展開

以降のトピックは、Workflow モードで展開を理解するのに役立ちます。

- Workflow モードでの展開タスク フロー （486 ページ）
- Workflow 以外のモードでのジョブの状態 （485 ページ）
- 展開ジョブの承認 （489 ページ）
- 展開ジョブと複数のユーザ （489 ページ）

Workflow モードでの展開タスク フロー

次に、Workflow モードでの代表的なタスク フローを示します（図 15 : ワークフローモードでの展開タスクフロー （487 ページ）を参照）。

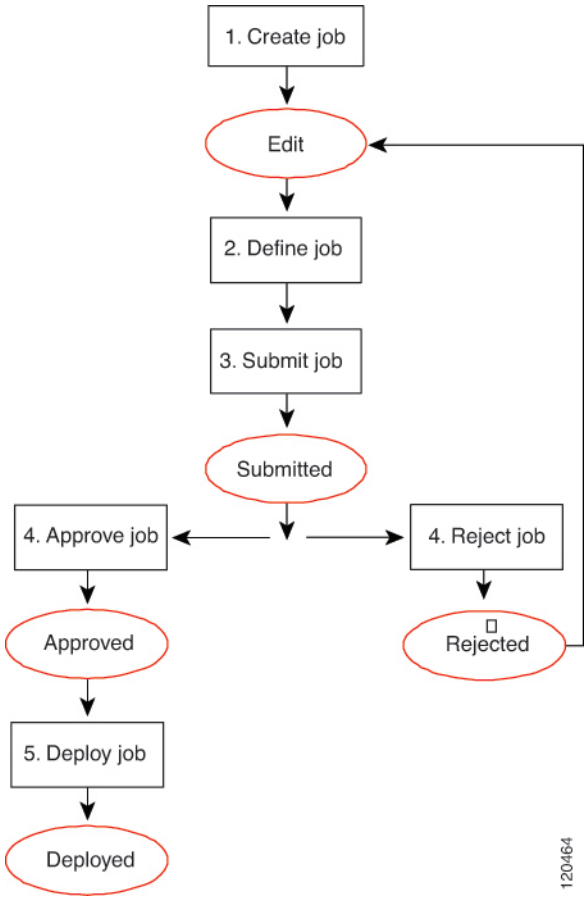
1. **ジョブの作成**：設定をデバイスに展開する前に、展開ジョブを作成する必要があります。
2. **ジョブの定義**：ジョブを作成するときは、どのデバイスに設定を展開するのか、直接デバイスに展開するのかファイルに展開するのか、いつジョブを実行するのかなどのパラメータを指定します。
3. **ジョブの送信**：組織によっては、適切な権限を持つ別のユーザがジョブを承認しなければジョブを展開できないようになっていることがあります。この場合、展開ジョブのアプルーバによって Workflow モードがイネーブルになり、送信者はこのユーザにジョブを送信して確認してもらう必要があります。アプルーバはジョブを確認し、承認または拒否を行います。
4. **ジョブの承認または拒否**：展開ジョブのアプルーバを割り当てて Workflow モードで作業している場合は、アプルーバがジョブを確認し、承認または拒否の決定を下します。ジョブが承認された場合、送信者はジョブを展開できます。ジョブが拒否された場合、送信者はジョブを廃棄し、ジョブを最初からやり直すかまたは修正を加えてから再送信します。

アプルーバを割り当てずに Workflow モードで作業している場合は、ジョブを自分自身で承認できます。

- **ジョブの展開**：ジョブを展開すると、生成したCLIがデバイス、中間転送サーバー（AUS、CNS、TMS など）、またはファイルに送信されます。宛先（デバイスまたはファイル）は、ジョブを定義するときに選択します。転送サーバはデバイスのプロパティで指定します。展開方式と転送サーバを定義する方法については、展開方法について （490 ページ）を参照してください。

（図 15 : ワークフローモードでの展開タスクフロー （487 ページ）に赤で表示される）ジョブの状態については、 Workflow モードでのジョブの状態 （487 ページ）を参照してください。

図 *15* : ワークフローモードでの展開タスクフロー



Workflow モードでのジョブの状態

Workflow モードでは、[Deployment Manager] ウィンドウの [Status] 列に、各ジョブの状態が表示されます。次の表に、ジョブの有効な状態とその説明を示します。[Deployment Manager] ウィンドウの詳細については、[Deployment Manager] ウィンドウ （499 ページ）を参照してください。

表 *99* : *Workflow* モードでのジョブの状態

状態	説明
Edit	ジョブは作成されましたが、現在編集中ではありません。ジョブが [Edit] 状態であるときは、ジョブを開く、承認する（自動承認モード）、廃棄するという操作を実行できます。
Edit-In Use	ジョブは編集用に開いています。ジョブが [Edit Open] 状態であるときは、ジョブを閉じる、承認する、廃棄する、送信するという操作を実行できます。

状態	説明
送信済み（Submitted）	ジョブは確認のために送信されました。ジョブが [Submitted] 状態であるときは、ジョブを表示できますが、編集はできません。[Submitted] 状態の場合、ジョブを表示する、廃棄する、拒否する、承認するという操作を実行できます。この状態になるのは、展開ジョブの承認が必要な場合に Workflow モードがイネーブルになった場合だけです。
承認（Approved）	ジョブは承認され、展開する準備ができています。ジョブが [承認（Approved）] 状態であるときは、ジョブを展開できます。
拒否	ジョブは拒否されました。ジョブが [Rejected] 状態であるときは、ジョブを開いて編集または廃棄できます。この状態になるのは、展開ジョブの承認が必要な場合に Workflow モードがイネーブルになった場合だけです。
破棄（Discarded）	ジョブは廃棄されました。これ以上ジョブに変更を加えることができません。ジョブは、システムから削除されるまで、[Discarded] 状態となってこれまでどおり [Deployment] テーブルに残ります。ジョブに含まれるデバイスを別のジョブに追加できます。
導入済み	ジョブに含まれるすべてのデバイスの設定が、デバイスまたは設定ファイルに正常に展開されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
展開	ジョブに生成された設定を、デバイスまたは Security Manager サーバのディレクトリに展開しています。[Deployment Manager] ウィンドウでジョブの経過表示をモニタできます。
中断	ジョブが手動で停止されました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
失敗しました（Failed）	ジョブに含まれる 1 つまたは複数のデバイスへの展開に失敗しました。これで、ジョブに含まれるデバイスを別のジョブに追加できます。
Scheduled to run at [date]	ジョブは、指定の日時に展開するようにスケジューリングされます。
Rolling Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定を展開しています。[Rolling Back] 状態にあるジョブは中断可能です。
Rolled Back	Security Manager は、展開ジョブに含まれるデバイスの以前の設定に復帰し、その設定の展開に成功しました。

展開ジョブの承認

デフォルトでは、Security Manager は Workflow 以外のモードで動作します。展開ジョブは、背後で処理され、ユーザはジョブまたはその承認を意識する必要はありません。Workflow モードを使用している場合は、展開ジョブ アプルーバを割り当てるかどうかを選択できます。

アプルーバを割り当てないことにした場合は、ジョブを定義し、承認する権限が与えられます。

新規の設定または変更を加えた設定をデバイスに展開してよいかどうかを、自分よりも強い権限を持つ別のユーザが承認するようになっている場合は、展開ジョブアプルーバを割り当てて Workflow モードを使用します。展開ジョブ アプルーバを割り当てて Workflow モードを使用する場合は、適切な権限を持つ担当者がジョブを確認してそのジョブを承認するか拒否するかを判断する必要があります。この承認プロセスにより、不適切な設定がネットワーク デバイスに到達しなくなり、展開ジョブが効率よくスケジューリングされるようになります。

（注） 展開ジョブの承認は、[Tools] > [Security Manager Administration] > [Workflow] からイネーブルおよびディセーブルにできます。詳細については、[Workflow] ページ （745 ページ）を参照してください。

展開ジョブと複数のユーザ

個々の展開ジョブ内のパラメータまたはデバイスを定義または変更できるのは、一度に 1 人のユーザだけです。ただし、複数のユーザが同じ展開ジョブに対して順に作業することはできます。あるユーザが展開ジョブを閉じれば、別のユーザがそのジョブを開いて変更を加えることができます。複数のユーザが、それぞれ異なる展開ジョブを並行して作業できます。

展開ジョブまたは展開スケジュールにデバイスを含める操作

展開ジョブまたは展開スケジューリングを作成するときは、そのジョブまたはスケジュールに含めるデバイスを選択します。デバイスを含めると、他のジョブまたはスケジュールでのそのデバイスの使用方法に影響を与えます。特定のジョブのデバイスを選択すると、そのジョブが展開、拒否（Workflow モード）、廃棄、または中断されるまで、選択したデバイスは他のジョブに選択できません。このメカニズムにより、複数のユーザが変更を同じデバイスに同時に展開できなくなり、ポリシーがデバイスに正しい順序で展開されます。

一方、デバイスは展開スケジューリングに含め、特定の展開ジョブに選択できます。展開ジョブが実行されている間、デバイスはロックされます。展開ジョブが実行されている間、デバイスを他のジョブに含めることができません。

展開ジョブを作成すると、Security Manager にはポリシーに変更が加えられたものの、まだ展開されていないデバイスが表示されます。このようなデバイスに展開し、ジョブに含めるデバイスをさらに選択できます。必要な数だけデバイスを展開ジョブに追加できます（制限はありません）が、実用上の理由からジョブあたりのデバイス数を制限することを推奨します。多数のデバイスを選択した場合や、大きな設定ファイルがあるデバイスをいくつか選択した場合に

は、展開ジョブが失敗することがあります。展開で障害が発生した場合は、選択されたデバイスの数を減らしてジョブを送信し直してください。

VPN の場合、Security Manager は、ジョブに選択したデバイスに定義されているポリシーの影響を受けるデバイスに対してコマンドを生成する必要があります。そのため、VPN を構成するデバイスを選択すると、Security Manager は他の関連するデバイスをジョブに追加します。たとえば、スポークでトンネルポリシーを定義し、ジョブ用にそのスポークを選択した場合、Security Manager はスポークに割り当てられたハブをジョブに追加します。ジョブの生成中、VPN 設定が完了し、トンネルを確立できるように、Security Manager は両方のピア用のコマンドを生成します。VPN に関連付けられたデバイスのいずれも選択しない場合、Security Manager はデバイスを取り外すと VPN が正しく機能しなくなることを警告します。

展開方法について

Security Manager では、主に 3 つの方法で設定をデバイスに展開できます。直接デバイスに展開する方法、設定ファイルに展開する方法（その後手動でデバイスに適用する必要があります）、および中間サーバに展開する方法（直接デバイスに展開する方法と同じように処理されます）です。システムにデフォルトの展開方法は、直接デバイスに展開する方法です。

デバイスを Security Manager に追加するときに、そのデバイスで使用する展開方法を選択します。これにより、（ファイルではなく）デバイスへの展開に使用する方法が決まります。展開ジョブを作成すると、展開方法のデフォルトが一体的にジョブに適用されます。これにより、設定ファイルを作成するかどうか、あるいはデバイスに選択した方法で設定をデバイスに送信するかどうかが決まります。このデフォルトは、管理設定で制御します（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択し、[展開（Deployment）] を選択。[Deployment] ページ （658 ページ）を参照）。展開ジョブを作成する際に、[ジョブの作成（Create Job）] ウィンドウで [展開方法の編集（Edit Deploy Method）] をクリックして、デバイスごとに展開先をファイルまたはデバイスに変更することもできます。Workflow 以外のモードを使用している場合は、Workflow 以外のモードでの設定の展開（515 ページ）を参照してください。Workflow モードを使用している場合は、展開ジョブの作成および編集 （524 ページ）を参照してください。

使用する方法は、組織が採用するプロセスおよび手順、および特定のデバイス タイプでサポートされているトランスポート プロトコルによって異なります。Configuration Engine（CNS）または Auto Update Server（AUS）を使用している場合は、それぞれの展開方法を使用してください。ダイナミック IP アドレスを使用するデバイスには、これらのいずれかを使用する必要があります。スタティック IP アドレスを使用するデバイスの場合、IOS、PIX、ASA、IPS、スタンドアロン FWSM の各デバイスには SSL（HTTPS）、および Catalyst シャーシ経由の FWSM には SSH を使用します。一部のデバイスに Token Management Server（TMS）を使用している場合は、Security Manager とともにその方法も使用できます。

以降のトピックでは、展開方法についてさらに詳しく説明します。

- デバイスへの直接展開 （491 ページ）
- 中間サーバを使用したデバイスへの展開 （492 ページ）
- ファイルへの展開 （493 ページ）

• アウトオブバンド変更の処理方法について （494 ページ）

デバイスへの直接展開

デバイスに直接展開することを選択した場合、Security Manager はそのデバイスのデバイスプロパティに定義されているトランスポートプロトコルを使用します（デバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択し、[全般（General）] をクリックします）。プロトコルは一般に、Security Manager 管理設定の [デバイス通信（Device Communication）] ページに定義されているデフォルトプロトコルです（[Device Communication] ページ （668 ページ）を参照）。表 100 : デフォルトの展開トランスポート プロトコル （491 ページ）には、デフォルトのトランスポートプロトコル設定の一部が一覧表示されます。

展開方法として [Device] を選択した場合、デバイスに AUS や Configuration Engine などの転送サーバを設定すると、展開に影響が及びます。中間転送サーバを使用している場合、設定展開はサーバを通過します。中間サーバの使用方法の詳細については、中間サーバを使用したデバイスへの展開 （492 ページ）を参照してください。

前回の展開以降にアウトオブバンド変更をデバイスに加えた場合には、展開にも影響が及ぶことがあります。詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

展開中、Security Manager は前回の展開以降に加えられた変更だけをデバイスに送信します。

注意 デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされます。

表 *100* : デフォルトの展開トランスポート プロトコル

デバイスタイプ	トランスポートプロトコル（Transport Protocol）	説明
ASA、IOS 12.3 以降のルータ、FWSM、PIX ファイアウォール、IPS センサー	SSL（HTTPS）（デフォルト）	Security Manager は、HTTPS とも呼ばれる Secure Socket Layer（SSL）プロトコルを使用して、設定をデバイスに展開します。Security Manager は、このプロトコルを使用して、設定ファイルを暗号化してからデバイスに送信します。

デバイスタイプ	トランスポートプロトコル（Transport Protocol）	説明
Catalyst 6500/7600 およびその他の Catalyst スイッチ	SSH	Security Manager は、Secure Shell（SSH; セキュアシェル）を使用して、設定をデバイスに展開します。これにより、セキュアでないチャネルでも強固な認証と安全な通信を確保できます。Security Manager は、SSHv1.5 と SSHv2 の両方をサポートします。デバイスに接続されると、Security Manager はどのバージョンを使用するかを決定し、そのバージョンを使用してダウンロードします。
IOS 12.2 ルータおよび 12.1 ルータ	Telnet	Security Manager は、Telnet プロトコルを使用して、設定をデバイスに展開します。

関連項目

- デバイス通信設定および証明書の管理　（576 ページ）
- デバイス OS バージョン不一致の処理　（495 ページ）

中間サーバを使用したデバイスへの展開

Auto Update Server（AUS）、Cisco Networking Services（CNS）Configuration Engine、Token Management Server（TMS）などの中間サーバを介して設定を展開する操作は、直接デバイスに展開する操作を若干変更したものです。展開方法を選択するときに、[Device] を選択します。Security Manager は、設定更新を中間サーバに送信します。この中間サーバで、デバイスがその更新を取得するか（AUS および CNS の場合）、またはユーザがその更新を eToken にダウンロードできます（TMS の場合）。

デバイス インターフェイスにダイナミック IP アドレスを使用している場合（つまり、IP アドレスを DHCP サーバから取得する場合）には、中間サーバを使用する必要があります。中間サーバは、スタティック IP アドレスでも使用できます。ただし、対話形式の CLI コマンドを使用する機能を設定する場合には、Configuration Engine ではダイナミック IP アドレスを持つ IOS デバイスを管理できません。次の機能に影響が及びます。

- 証明書登録：
  - **crypto pki trustpoint**
  - **crypto isakmp client configuration group**
  - **crypto key generate rsa**
- IPS シグニチャ設定（**ip ips signature-category**）

- IP Authproxy バナー（**ip auth-proxy-banner**）
- Catalyst デバイス インターフェイス スイッチポート（**interface switchport**）

中間サーバを使用するようにデバイスを設定した場合、Security Manager はその中間サーバを使用します。以降のトピックでは、中間サーバを使用する場合に必要な設定手順について説明します。

- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）

前回の展開以降にアウトオブバンド変更をデバイスに加えた場合には、展開に影響が及ぶことがあります。詳細については、アウトオブバンド変更の処理方法について （494ページ）を参照してください。

展開中、Security Manager はサーバのタイプに基づいて設定変更を送信します。

- PIX デバイスおよび ASA デバイスの Auto Update Server（スタンドアロンまたは Configuration Engine で稼働）：Security Manager は Auto Update Server にすべての設定を送信し、デバイスはサーバから設定を取得します。デルタ設定は送信されません。
- IOS デバイスの Configuration Engine：Security Manager は Configuration Engine にデルタ設定を送信し、デバイスはエンジンから設定を取得します。
- TMS：Security Manager は TMS サーバにデルタ設定を送信します。サーバから eToken に設定をダウンロードし、デバイス上にロードできます。

関連項目

- デバイス通信設定および証明書の管理 （576 ページ）
- [Device Communication] ページ （668 ページ）

ファイルへの展開

設定を構成ファイルに展開することを選択した場合、Security Manager は 2 つのファイルを作成します。デルタ設定用の *device_name* _delta.cfg と、完全な設定用の *device_name* _full.cfg です。展開スケジューリングから生成されたジョブによってファイルが作成された場合、その名前にはタイム スタンプが含まれています。設定ファイルは、TFTP を使用してデバイスにアップロードできるように、TFTP 形式になっています。

ヒント IPS デバイスの場合には、設定をファイルに展開できません。

ファイルに展開する場合は、ユーザ自身が設定をデバイスに転送します。Security Manager は、ユーザがこの転送を完了したものと想定するため、次回同じデバイスに展開すると、生成される差分コマンドは前回の展開の設定に基づくものになります。何らかの理由で前回の変更がデ

バイスに適用されなかった場合、新規デルタ設定ではデバイス設定がデバイスに展開されず、Security Manager に反映されません。

注意 Security Manager は、ユーザがデルタ設定を適用したことを想定している一方、デルタが展開されたかどうかを判断できないことも想定しています。このため、Security Manager はデバイスに直接実行された最新の展開に基づいた設定の内部ビューを維持します。デルタを適用すると、デルタの変更はアウトオブバンド変更と見なされます。次回のデバイスへの展開時に、アウトオブバンド変更設定によって展開がキャンセルされる場合があります。ファイルへの展開とデバイスへの展開を混在させる場合は、デバイスにファイルの展開を適用したあとにポリシーを再検出する必要があります。詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

ファイル展開用のデフォルトディレクトリを設定するには、[ツール（Tools）]>[Security Manager 管理（Security Manager Administration）] を選択し、[展開（Deployment）] を選択します（[Deployment] ページ （658 ページ）を参照）。デフォルトの展開方法に [File] を選択した場合は、そのデフォルトディレクトリも選択します。展開ジョブを作成するときに、そのジョブ用のこのディレクトリを変更できます。

設定をファイルに展開する処理は、デバイスがネットワークにまだ配置されていない場合（グリーンフィールド展開と呼ばれます）、独自のメカニズムで設定をデバイスに転送する場合、または遅延展開を採用する場合に便利です。ファイルに展開するとき、多数のデバイスを選択した場合や、大きな設定ファイルがあるデバイスをいくつか選択した場合には、展開ジョブが失敗することがあります。展開で障害が発生した場合は、選択されたデバイスの数を減らしてジョブを送信し直してください。

ヒント ファイルに展開するときは、展開中にデバイスとの対話を必要とするコマンドを使用しないでください。展開前に設定をプレビューして、そのようなコマンドがファイルにないことを確認することを推奨します。詳細については、設定のプレビュー （535 ページ）を参照してください。

アウトオブバンド変更の処理方法について

Security Manager は、アウトオブバンド変更を手動または Security Manager の管理外でデバイスに加えられた変更であると見なします。たとえば、デバイスに直接ログインし、CLI を介してコンフィギュレーションコマンドを入力した場合などが相当します。ところが、アウトオブバンド変更には、デバイスではなくファイルに設定を展開する際に Security Manager が作成するデルタ変更のアプリケーションも含まれます。

（ファイルではなく）デバイスに展開する際に、新規設定がデバイス上の現在の設定と比較されるようになっている展開方法を選択した場合は、[アウトオブバンド変更動作（Out of Band Change Behavior）] 設定でアウトオブバンド変更が検出されたときに、その変更をどのように処理するかを指定できます。ファイルへの展開では、設定値は適用されません。

新規デバイス設定を Security Manager Configuration Archive に格納されている最新のバージョンと比較する場合は、この設定値は無視されます。アウトオブバンド変更のデフォルトの処理方法は、[Tools] > [Security Manager Administration] > [Deployment] に設定されます。詳細については、[Deployment]ページ （658ページ）を参照してください。[デバイス参照設定の展開（Deploy to Device Reference Configuration）] および [アウトオブバンド変更の検出時（When Out of Band Changes Detected）] の設定を探します。

アウトオブバンド変更の処理に関するオプションは次のとおりです。

- [変更を上書きして警告を表示（Overwrite changes and show warning）]：設定が展開されると、Security Manager はデバイスの現在の設定をアップロードし、自身のデータベースに格納されている設定と比較します。デバイスに手動で変更が加えられていた場合、Security Manager は展開を続行し、展開の続行を通知する警告を表示します。アウトオブバンド変更は、デバイスから削除されます。
- [展開のキャンセル（Cancel deployment）]：設定が展開されると、Security Manager はデバイスの現在の設定をアップロードし、自身のデータベースに格納されている設定と比較します。デバイスに手動で変更が加えられていた場合、Security Manager は展開を取り消し、展開の取り消しを通知する警告を表示します。設定変更をデバイスに展開するには、アウトオブバンド変更を手動で削除するか、または Security Manager で同じ設定を行う必要があります。
- [変更を確認しない（Do not check for changes）]：Security Manager は、変更を確認せずに、変更をデバイスに展開します。警告が表示されずに、アウトオブバンド変更がデバイス設定から削除されます。

設定を展開する前に、デバイスにアウトオブバンド変更があるかどうかを検出し、そのような変更があれば Security Manager ポリシーに再作成するのか、Security Manager に変更の上書きを許可するのかを分析することを推奨します。詳細については、アウトオブバンド変更の検出および分析 （537 ページ）を参照してください。

関連項目

- デバイスへの直接展開 （491 ページ）
- 中間サーバを使用したデバイスへの展開 （492 ページ）
- ファイルへの展開 （493 ページ）

デバイス OS バージョン不一致の処理

変更を加えた設定ファイルを直接デバイスに展開する前に、Security Manager は通常、デバイスから現在実行中の設定ファイルをアップロードし、デバイスで実行されている OS バージョンを Security Manager データベースに格納されている OS バージョンと照合します（デバイスの設定ではなく、アーカイブされた設定が使用されように設定できます）。Security Manager は、OS バージョンが相互に一致するのか異なるのかに応じて処理を実行します。

Security Manager は設定を展開し、警告を表示する場合もあれば、設定を展開できない場合もあります。Security Manager が設定を展開するのは、次の場合です。

- デバイスに新しいマイナー バージョンがある場合。たとえば、Security Manager に示されている ASA 8.1(1) ではなく ASA 8.1(2) であるなど。
- デバイスに下位のマイナー バージョンがある場合。たとえば、ASA 8.1(2) ではなく ASA 8.1(1) であるなど。

デバイスが OS の新規メジャー バージョンを実行しているとき（たとえば、Security Manager に示されている ASA 7.2 ではなく ASA 8.0 など）や、デバイスが下位メジャー バージョン（8.0 ではなく 7.2）を実行している場合には、Security Manager は設定を展開しません。

次の表に、OS バージョンが相互に一致するのか異なるのかに応じて Security Manager が実行する処理を示します。表では、一例として ASA デバイスを使用していますが、処理はすべてのサポート対象デバイス タイプに適用されます。

表 *101 : OS* バージョンが一致するか異なるかに応じた展開処理

シナリオ	Security Manager データベースに格納された OS バージョン	デバイス上の OS バージョン	展開に使用される OS バージョン	操作
バージョンの一致	ASA 8.2(1)	ASA 8.2(1)	ASA 8.2(1)	何の警告もなく、展開が進みます。
デバイスに新しいマイナー OS バージョンがある。	ASA 8.1(1)	ASA 8.1(2)	ASA 8.1(2)	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを警告します。 Security Manager は、デバイスで稼働している OS バージョンに基づいて CLI を生成します。
デバイスに新しいマイナー OS バージョンがあるが、そのバージョンは Security Manager で直接サポートされていない。	ASA 8.0(2)	ASA 8.0(4)	ASA 8.0(3)	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを警告します。 Security Manager は、実行中の OS バージョンと下位互換性があるサポート対象の OS バージョンに基づいて、CLI を生成します。

シナリオ	Security Manager データベースに格納された OS バージョン	デバイス上の OS バージョン	展開に使用される OS バージョン	操作
デバイスに新規メジャーOSバージョンがある。	ASA 7.2(4)	ASA 8.2(1)	なし。展開に失敗。	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを示すエラーを報告します。 このミスマッチを修正するまで、Security Manager は処理を継続できません。インベントリからデバイスを削除し、再度追加してからデバイスポリシーを検出してください。
デバイスに古いマイナーOSバージョンがある。	ASA 8.1(2)	ASA 8.1(1)	ASA 8.1(1)	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを警告します。 Security Manager は、デバイスで稼働している OS バージョンに基づいて CLI を生成します。
デバイスに古いメジャーOSバージョンがある。	ASA 8.2(1)	ASA 7.2(4)	なし。展開に失敗。	Security Manager データベースの OS バージョンと異なる OS バージョンが、デバイスで検出されたことを示すエラーを報告します。 このミスマッチを修正するまで、Security Manager は処理を継続できません。インベントリからデバイスを削除し、再度追加してからデバイスポリシーを検出してください。

Deployment Manager および Configuration Archive の概要

Deployment Manager および Configuration Archive は、展開およびデバイス設定を管理するときに使用する主要なツールです。以降のトピックでは、これらのツールの概要を示します。

• Deployment Manager でできること （498 ページ）
• [Deployment Manager] ウィンドウ （499 ページ）

- [Deployment Schedules] タブ、Deployment Manager （505 ページ）
- [Configuration Archive] ウィンドウ （509 ページ）

Deployment Manager でできること

Deployment Manager では、展開ジョブおよび展開スケジュールを作成および管理します。次の利点があります。

- 設定のプレビューと比較：設定ファイルをデバイスに展開する前に、提示された設定ファイルをプレビューできます。また、提示された設定ファイルを、デバイスから前回インポートされたファイルまたはデバイスで現在実行中のファイルと比較することもできます。

デバイスへの展開が成功したあと、ダウンロードした設定コマンドのトランスクリプトとデバイスの応答を表示できます。詳細については、設定のプレビュー （535 ページ）を参照してください。

- 展開ジョブの中断：実行中の場合も含め展開ジョブを停止できます。ただし、実行中のジョブを中断しても、デバイスにすでに再設定された設定およびデバイスに現在再設定中の設定はロールバックされません。展開がまだ開始されていないデバイスだけが再設定できません。詳細については、 展開ジョブの中断 （549 ページ）を参照してください。
- 以前の設定へのロールバック：設定をデバイスに展開し、その後新しい設定に何か問題があることが明らかになった場合は、そのデバイスの以前の設定に戻って展開できます。詳細については、 Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）を参照してください。
- 展開ジョブの状態の表示：エラーに関する情報、提示された設定、ダウンロードのトランスクリプトなど、特定のデバイスへの展開に関する情報を表示できます。詳細については、 ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）を参照してください。
- 展開ジョブのスケジューリング：展開スケジュールを作成して、一定の間隔で展開ジョブを生成できます。Workflow モードでは、ジョブを展開するときに、将来の時刻に開始するように展開ジョブをスケジューリングすることもできます。ジョブをスケジューリングすると、デバイスでのトラフィックが少ない時間に展開を実施できます。詳細については、次の項を参照してください。
  - 展開スケジュールの作成または編集 （550 ページ）
  - Workflow モードでの展開ジョブの展開 （530 ページ）
- 展開ジョブ履歴のロギング（Workflow モード限定）：ジョブのトランザクションの履歴を表示できます。トランザクションには、ジョブの承認などさまざまなユーザが開始したジョブ状態の変更と、その状態変更に関連するコメントが表示されます。詳細については、 ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）を参照してください。

[Deployment Manager] ウィンドウ

[Deployment Manager] ウィンドウは、展開ジョブおよび展開スケジュールを管理するときに使用します。展開ジョブのリストを表示し、ジョブ詳細を参照し、設定をデバイスに展開および再展開できます。また、展開ジョブを中断し、選択したデバイスで以前の設定にロールバックし、スケジュールを作成して展開ジョブを自動的に生成できます。このほか、展開ジョブおよび展開スケジュールに加えた変更を追跡することもできます。

（注） Deployment Manager で使用できるボタンは、使用している Workflow モードによって異なります。

ナビゲーション パス

[メイン（Main）] ツールバーの [展開マネージャ（Deployment Manager）] ボタンをクリックするか、または[管理（Manage）] > [展開（Deployments）] を選択します。

関連項目

- 展開プロセスの概要 （482 ページ）
- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの展開ジョブの展開 （530 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）

フィールド リファレンス

表 *102 : [Deployment Manager]* ウィンドウ（*Workflow* モード）

要素	説明
[展開ジョブ（Deployment Job）] タブ このタブには、個々の展開ジョブが表示されます。上部ペインでジョブを選択すると、その詳細が下部ペインのタブに表示されます。 フィルター オプション（Filter Options） 4.14 以降、Cisco Security Manager には、名前（展開ジョブ名）、ステータス、変更者、およびデバイス名に基づいて展開ジョブを検索するためのフィルタオプションが用意されています。フィルタ条件を指定したら、[適用（Apply）] をクリックします。グリッドに検索結果が表示されます。テーブル内のジョブを選択すると、その詳細が下部ペインのタブに表示されます。	
名前	ジョブの名前。
直前のアクション	ジョブまたは状態が変更された日付と時刻。クライアントのタイム ゾーンではなく、サーバのタイム ゾーンに基づきます。
ステータス	各ジョブの状態。有効な状態は、Workflow モードによって異なります。状態については、次のトピックを参照してください。 • Workflow 以外のモードでのジョブの状態 （485 ページ） • Workflow モードでのジョブの状態 （487 ページ）
Changed By	ジョブを変更したユーザの名前。
説明	ジョブの説明。個別のダイアログボックスで説明を表示するには、アイコンをダブルクリックします。
ジョブ タイプ（Job Type）	スケジュールの点から見たジョブのタイプ。**one time** ジョブは定期的に繰り返されるジョブから作成されたものではありませんが、**recurring** ジョブは作成されたものです。
[Create] ボタン （Workflow モード限定）	Workflow モードでは、新規ジョブを作成するには、このボタンをクリックしします。[Create a Job] ダイアログボックスが開きます。 展開ジョブの作成および編集 （524 ページ）を参照してください。
[Open] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを開くには、このボタンをクリックします。[Edit a Job] ダイアログボックスが開きます。 展開ジョブの作成および編集 （524 ページ）を参照してください。

要素	説明
[Close] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを閉じ、ジョブを開いていた間に加えたすべての変更を保存するには、このボタンをクリックします。[Edit Open] 状態または [Submit Open] 状態であるときは、ジョブを閉じることができます。通常、ジョブを閉じる必要はありません。一般に、展開対象のジョブは送信、承認、展開、またはスケジューリングすることになるためです。ただし、Security Manager サーバが突然使用不可能になったり、ログイン セッションがタイムアウトしたりした場合は、ジョブが [Edit Open] 状態のままになることがあります。この場合、ジョブを選択し、[Close] をクリックして、手動でジョブを閉じることができます。
\[Submit\] ボタン[Submit ぼたん] （Workflow モード限定）	Workflow モードでは、承認のために選択したジョブを送信するには、このボタンをクリックします。ジョブは、[Edit] 状態または [Edit Open] 状態にある場合に送信できます。[Submit Deployment Job] ダイアログボックスが開きます。展開ジョブの送信 （528 ページ）を参照してください。 このボタンは、展開ジョブ アプルーバを割り当てて Workflow モードを使用している場合にだけアクティブになります。
[Reject] ボタン （Workflow モード限定）	Workflow モードでは、デバイス用に生成された設定に満足できない場合、このボタンをクリックして、選択したジョブを拒否します。展開ジョブ アプルーバを割り当てて Workflow モードを使用している場合にだけ、ジョブを拒否できます。ジョブを拒否したあと、そのジョブを開いて編集または廃棄できます。展開ジョブの承認と拒否 （529 ページ）を参照してください。 任意で、ジョブを拒否する理由を入力できます。
[Approve] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを承認するには、このボタンをクリックします。ジョブを承認したあと、そのジョブを展開できます。展開ジョブの承認と拒否 （529ページ）を参照してください。 任意で、ジョブを承認する理由を入力できます。
[Discard] ボタン （Workflow モード限定）	Workflow モードでは、選択したジョブを廃棄するには、このボタンをクリックします。[Deployed]、[Deployment Failed]、[Aborted] を除く任意の状態である場合に、ジョブを廃棄できます。いったん廃棄したジョブは、編集、送信、承認、および展開できません。ジョブが [Workflow 設定（Workflow settings）] ページの設定に従って自動的にシステムから削除されるか、または手動でシステムから削除するまで、ジョブ状態は「Discarded」として表示されます（詳細については、[Workflow] ページ （745 ページ）を参照してください）。 任意で、ジョブを廃棄する理由を入力できます。展開ジョブの廃棄（531 ページ）を参照してください。

要素	説明
[Deploy] ボタン （すべてのモード）	生成されたCLIコマンドをデバイスまたはファイルに展開するには、このボタンをクリックします。このボタンの動作は、Workflow モードによって異なります。 • （Workflow 以外のモード）展開ジョブを作成するには、このボタンをクリックします。まだ送信していない変更がある場合は、まず、その変更を送信するように求められます。[Deploy Saved Changes] ダイアログボックスが開き、どのデバイスをジョブに含めるかを選択できます。このボタンは、テーブルで選択されている展開ジョブには機能しないことに注意してください。その代わり、新規に展開ジョブを作成します。 Workflow 以外のモードでの設定の展開 （515 ページ）を参照してください。 • （Workflow モード）選択したジョブを展開するには、このボタンをクリックします。ジョブが [Approved] 状態である場合は、[Deploy Job] ダイアログボックスが開きます（ Workflow モードでの展開ジョブの展開 （530 ページ）を参照）。 ジョブが [Deployed]、[Failed]、[Aborted] のいずれかの状態である場合は、[Redeploy Job] ダイアログボックスが開きます。 デバイスへの設定の再展開 （547 ページ）を参照してください。
[Generate Report] ボタン （すべてのモード）	選択したジョブの展開ステータス レポートを作成するには、このボタンをクリックします。レポートはHTMLおよびPDF フォーマットで生成できます。ジョブは [Deployed]、[Failed]、[Rolled Back]、または [Aborted] のいずれかの状態である必要があります。 展開ステータスレポートには、ジョブの概要および完全な設定とデルタ設定、およびジョブのトランスクリプトが含まれます。ユーザはこのレポートを独自の目的で使用したり、Cisco TAC の問題のトラブルシューティングに使用したりできます。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成 （636 ページ）を参照してください。
[Refresh] ボタン （すべてのモード）	Security Manager サーバからジョブ情報をリロードするには、このボタンをクリックします。テーブルの下に [自動リフレッシュがオン（Auto Refresh is On）] というメッセージが表示された場合は、ジョブリストが定期的に自動リフレッシュされます。 （注） 自動リフレッシュ設定は、展開の管理設定で設定します。[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] の順に選択してください。

要素	説明
[Redeploy] ボタン （Workflow 以外のモード限定）	Workflow 以外のモードでは、選択したジョブを再展開するには、このボタンをクリックします。これにより、同じ CLI コマンドが生成されて、元のジョブで選択されていたのと同じデバイスまたはファイルに展開されます。[Redeploy Job dialog box] ダイアログボックスが開きます。デバイスへの設定の再展開 （547 ページ）を参照してください。 （Workflow モードでは、[Deploy] ボタンをクリックすると、選択したジョブの設定が再展開されます）
[Abort] ボタン （すべてのモード）	[Deploying]、[Scheduled]、[Rolling Back] のいずれかの状態である場合は、このボタンをクリックすると、選択したジョブが中断します。処理を確認するように求める警告が表示されます。展開ジョブの中断 （549 ページ）を参照してください。
[Rollback] ボタン （すべてのモード）	このボタンをクリックして、以前に展開した設定を選択したジョブのデバイスに展開します。[Deployment Rollback] ダイアログボックスが開きます（Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）を参照）。
[サマリー（Summary）] タブ	選択した展開ジョブの状態に関する要約情報を表示します。具体的には、ジョブの状態、展開ジョブの名前、ジョブに含まれているデバイスの数、正常に展開されたデバイスの数、展開時にエラーが発生したデバイスの数などです。

要素	説明
[Details] タブ	選択したジョブの詳細な情報を表示します。表には、ジョブに含まれている各デバイス、展開が正常に完了したか失敗したか、デバイスのジョブの一部である変更が含まれるチケット、およびデバイスの警告、エラー、失敗の数をまとめた一覧が表示されます。表でデバイスを選択すると、そのデバイスの結果が表示されます。 • [Config] 列のアイコンをダブルクリックすると、設定が表示されます（設定のプレビュー （535 ページ）を参照）。インベントリからデバイスを削除した場合は、設定およびトランスクリプトが使用できないことがあります。 • デバイスに展開していた場合は、[トランスクリプト（Transcripts）] カラムのアイコンをダブルクリックすると、デバイスに送信されるコマンドのトランスクリプトとデバイスの応答が表示されます。展開トランスクリプトの表示 （558 ページ）を参照してください。 • チケット管理が有効になっている場合、[最終チケット（Last Ticket(s)）] カラムには、デバイスの展開の一部である変更を含むチケットのチケット ID が表示されます。チケット ID をクリックして、作成者や最終更新日など、チケットに関する追加情報を表示できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。 • デバイスを選択すると、左下にある [Messages] ボックスに、展開に関して生成されたメッセージの概要が表示されます。項目を選択すると、右側にその説明が表示されます。ウィンドウを拡大しないと、[Description] ボックスが表示されないことがあります。問題を解決するために実行した処理があれば、その処理に関する情報も表示されます。
[履歴（History）] タブ（Workflow モード限定）	選択したジョブにこれまで加えられた変更のログを表示します。ログの内容は、状態の変更、変更を行ったユーザ、変更日時（Security Manager サーバの時間が基準）、およびユーザが入力した変更を説明するコメントです。
[Deployment Schedules] タブ このタブは、定期的な展開ジョブをスケジューリングする場合に使用します。このタブの詳細については、[Deployment Schedules] タブ、Deployment Manager （505 ページ）を参照してください。	

[Deployment Workflow Commentary] ダイアログボックス

Workflow モードを使用している場合に Deployment Manager で処理を実行すると、処理の説明を入力するように求められます。入力した説明は、ジョブまたはスケジュールの履歴に保持されます。

ダイアログボックスのタイトルは、実行している処理を示します。任意でコメントを入力し、[OK] をクリックして処理を実行します。

ナビゲーション パス

Workflow モードでは、Deployment Manager でジョブまたはスケジュールを選択し、適切なボタンをクリックして目的の処理を実行します。

[Deployment Schedules] タブ、Deployment Manager

[Deployment Manager] ウィンドウの [Deployment Schedules] タブは、定期的に繰り返される展開ジョブを作成する場合に使用します。スケジュールに指定した展開時刻になるたびに、スケジューリングしたジョブに基づいて、Security Manager が特定の展開ジョブを作成します。

ナビゲーション パス

[メイン（Main）] ツールバーの [Deployment Manager] ボタンをクリックするか、または **[管理（Manage）] > [展開（Deployments）]** を選択し、上部ペインにある [展開スケジュール（Deployment Schedules）] タブをクリックします。

関連項目

- 展開プロセスの概要 （482 ページ）
- 展開スケジュールの作成または編集 （550 ページ）
- 展開スケジュールの一時停止または再開 （554 ページ）

フィールド リファレンス

表 *103 : [Deployment Schedules]* タブ、*[Deployment Manager]* ウィンドウ

要素	説明
[Deployment Schedule] テーブル このテーブルには、展開ジョブ スケジュールが表示されます。テーブル内のスケジュールを選択すると、その詳細が下部ペインのタブに表示されます。 フィルター オプション（Filter Options） 4.14 以降、Cisco Security Manager には、名前（展開スケジュール名）、ステータス、およびデバイス名に基づいて展開スケジュールを検索するためのフィルタオプションが用意されています。フィルタ条件を指定したら、[適用（Apply）] をクリックします。グリッドに検索結果が表示されます。テーブル内のスケジュールを選択すると、その詳細が下部ペインのタブに表示されます。	
名前	ジョブ スケジュールの名前。このスケジュールから作成されたジョブが、この名前とタイム スタンプを使用します。
ステータス	スケジュールの状態。 • [Edit]：Workflow モードでは、スケジュールが作成中です。スケジュールを開き、その設定を変更できます。編集中のスケジュールからはジョブが作成されません。 • [Active]：このスケジュールに従って展開ジョブが作成されます。 • [Suspended]：スケジュールは一時停止されました。そのスケジュールで作成中のジョブはありません。スケジュールを再開するには、そのスケジュールを選択し、[再開（Resume）] をクリックします。
定例（Recurrence）	このスケジュールから展開ジョブが作成される頻度。
Next Run	次回このスケジュールから展開ジョブが作成される日付と時刻。
前回の実行	このスケジュールから最近作成された展開ジョブの日付と時刻。
Schedule End	スケジュールがアクティブではなくなった日付と時刻。スケジュールに終了日がない場合は、[Active Indefinitely] が示されます。
説明	ジョブ スケジュールの説明。説明を表示するには、アイコンをダブルクリックします。
[Create] ボタン	展開ジョブ スケジュールを作成するには、このボタンをクリックします。[Schedule] ダイアログボックスが開き、スケジュールを作成できます（[Schedule] ダイアログボックス （551 ページ）を参照）。

要素	説明
[Open] ボタン	選択したスケジュールを開くには、このボタンをクリックします。[Schedule] ダイアログボックスが開き、スケジュールを表示または変更できます（[Schedule] ダイアログボックス （551 ページ）を参照）。 Workflow以外のモードでは、スケジュールを変更しても、その状態は変更されません。Workflow モードでは、状態が [Edit] に変わり、承認のため再送信する必要があります。
[Close] ボタン （Workflow モード限定）	スケジュールを閉じ、スケジュールを開いていた間に加えたすべての変更を保存するには、このボタンをクリックします。[Edit Open] 状態または[Submit Open] 状態であるときは、スケジュールを閉じることができます。一般に、スケジュールを閉じる必要があるのは、スケジュールが開いたままの状態で Security Manager サーバが使用できなくなった場合だけです。
\[Submit\] ボタン[Submit ぼたん] （Workflow モード限定）	アプルーバを割り当てて Workflow モードを使用している場合は、承認のため、このボタンをクリックして、選択したスケジュールを送信します。[Edit] 状態または [Edit Open] 状態にある場合に、スケジュールを送信できます。任意で、送信の説明を入力できます。Workflowモードでは、電子メールが生成されてアプルーバに送信されます。
[Reject] ボタン （Workflow モード限定）	選択したスケジュールを拒否するには、このボタンをクリックします。任意で、拒否の説明を入力できます。Workflowモードでは、電子メールが生成されてアプルーバおよび送信者に送信されます。
[Approve] ボタン （Workflow モード限定）	選択したスケジュールを承認するには、このボタンをクリックします。任意で、承認の説明を入力できます。Workflowモードでは、電子メールが生成されてアプルーバおよび送信者に送信されます。
[Discard] ボタン	選択したスケジュールを廃棄するには、このボタンをクリックします。スケジュールは、そのスケジュールから作成されたアクティブな展開ジョブがある場合を除き、廃棄できます（ジョブが完了するまで待つか、またはジョブを中断してから、スケジュールを廃棄できます）。 任意で、廃棄の説明を入力できます。Workflow モードでは、電子メールが生成されてアプルーバおよび送信者に送信されます。

要素	説明
[Refresh] ボタン	Security Manager サーバからスケジュール情報をリロードするには、このボタンをクリックします。テーブルの下に [自動リフレッシュがオン（Auto Refresh is On）] というメッセージが表示された場合は、スケジュールリストが定期的に自動リフレッシュされます。 （注） 自動リフレッシュ設定は、展開の管理設定で設定します。[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] の順に選択してください。
[Suspend] ボタン	選択したスケジュールを一時停止するには、このボタンをクリックします。スケジュールを一時停止してもスケジュールは削除されませんが、そのスケジュールに基づいて展開ジョブを作成できなくなります。一時停止を説明するコメントの入力を要求されます。また、電子メールが生成されて、Workflow モードでアプルーバに送信されます。
[再開（Resume）] ボタン	一時停止したスケジュールを再アクティブ化するには、このボタンをクリックします。一時停止を説明するコメントの入力を要求されます。また、電子メールが生成されて、Workflow モードでアプルーバに送信されます。
[サマリー（Summary）] タブ	選択したスケジュールに関する要約情報を表示します。テーブルに表示されるフィールドのほか、要約情報にはスケジュールに含まれているデバイスの数、最後にスケジュールを変更したユーザの ID などがあります。
[Devices] タブ	選択したスケジュールに含まれているデバイスを表示します。ここに表示されるのは、スケジュールから展開ジョブが作成されたときに設定が展開されるデバイスです。デバイスリストを変更するには、[開く（Open）] をクリックし、[スケジュール（Schedule）] ダイアログボックスで [デバイスの追加（Add Devices）] をクリックします。
[履歴（History）] タブ	選択したスケジュールにこれまで加えられた変更のログを表示します。ログの内容は、状態の変更、変更を行ったユーザ、変更日時（Security Manager サーバの時間が基準）、およびユーザが入力した変更を説明するコメントです。

要素	説明
[Jobs] タブ	選択したスケジュールに基づいてこれまで作成された展開ジョブのリストを表示します。情報には、ジョブの名前、ジョブを作成した日付と時刻（クライアント時間ではなくサーバ時間に基づいた時間）、ジョブの状態などがあります。ジョブを選択し、[展開ジョブ（Deployment Job）] タブをクリックすると、選択したジョブが強調表示され、ジョブの詳細を表示できます。 ジョブの状態の詳細については、次の項を参照してください。 • Workflow モードでのジョブの状態 （487 ページ） • Workflow 以外のモードでのジョブの状態 （485 ページ）

[Configuration Archive] ウィンドウ

Configuration Archive は、Security Manager によって管理される各デバイスの設定バージョンを格納します。Cisco Security Manager からデバイスを削除すると、そのデバイスの設定はすべて Configuration Archive からも削除されます。

Configuration Archive は次の場合に使用できます。

- 選択したデバイスの設定展開のトランスクリプトを表示します。
- 設定バージョンを表示し、比較します。
- 展開された設定バージョン間での CLI の相違点を表示します。
- 設定がそのデバイスから作成されたものである場合に、以前の設定バージョンにロールバックします。設定をロールバックするのは、極端な状況にある場合だけとしてください。詳細については、次の項を参照してください。
  - 設定のロールバックについて （560 ページ）
  - ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- デバイスで現在実行中の設定をアーカイブに追加します。

デバイスの設定バージョンのリストをソートするには、ソート基準となる列見出しをクリックします。列見出しをクリックすると、行のソートが昇順と降順との間で切り替わります。表示されるフィールドを制御することもできます。そのためには、任意の列見出しを右クリックし、[Show Columns] コマンドの下で目的の列名を選択または選択解除します。

ナビゲーション パス

[管理（Manage）] > [Configuration Archive] を選択します。

関連項目

- [Configuration Archive] ページ （649 ページ）
- アーカイブされた設定バージョンの表示および比較 （555 ページ）
- 設定のロールバックについて （560 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （562 ページ）
- フェールオーバー デバイスのロールバックについて （562 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （563 ページ）
- IPS および IOS IPS のロールバックについて （564 ページ）
- デバイスの設定バージョンの Configuration Archive への追加 （555 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 *104 : [Configuration Archive]* ウィンドウ

要素	説明
Device Selector	デバイスインベントリのデバイスを一覧表示します。デバイスを選択すると、アーカイブで使用できるデバイスの設定バージョンが表示されます。次に挙げる情報が右ペインに表示されます。
バージョン ID（Version ID）	設定バージョンのバージョン番号。デフォルトでは、この列は表示されません。この列を表示するには、任意の列見出しを右クリックし、**[列の表示（Show Columns）] > [バージョンID（Version ID）]** を選択します。
作成日（Created On）	設定バージョンがアーカイブされた日付と時刻。
Created By	設定バージョンをアーカイブに追加する操作に関連付けられたユーザ ID またはシステム ID。 username1（username2）という形式で 2 つの名前がある場合、最初の名前が要求を開始したユーザーで、カッコ内の名前がシステム アイデンティティ ユーザーです。システムアイデンティティ信頼ユーザーの詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。
Archival Source	アーカイブ イベントの発生元（たとえば、ユーザ要求、展開、プロビジョニング、検出）。
Creation Comment	設定バージョンを作成した方法と理由に関する説明。

要素	説明
[Transcript] アイコン	ダブルクリックすると、デバイスに展開された設定バージョンのトランスクリプトが表示されます。 トランスクリプトとは、展開処理またはロールバック処理の間にキャプチャされた、Security Manager とデバイス間のトランザクション ログ ファイルです。この中には、展開要求またはロールバック要求が出た時点からサーバとデバイス間で送受信されたコマンドは含まれていますが、展開の初期検出フェーズである、Security Manager がデバイスから現在の設定を取得するときに行われた通信は含まれていません。
[表示（View）] ボタン	選択した設定を [Config Version Viewer] ウィンドウに表示するには、このボタンをクリックします（[Configuration Version Viewer] （556 ページ）を参照）。ここで、その設定を他の設定バージョンと比較することもできます。
[Rollback] ボタン	デバイス設定を選択した設定バージョンにロールバックするには、このボタンをクリックします。ただし、設定がそのデバイスから作成されたものである場合にかぎります。設定をロールバックするのは、極端な状況にある場合だけとしてください。詳細については、次の項を参照してください。 • 設定のロールバックについて （560 ページ） • ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
[Add from Device] ボタン	Security Manager を使用して、デバイスから現在実行中の設定を取得し、それを設定バージョンとしてアーカイブに追加するには、このボタンをクリックします。これは、デバイスの中に設定がデバイスの CLI で直接変更された可能性があるものがある場合に便利です。 設定バージョンの追加方法については、デバイスの設定バージョンの Configuration Archive への追加 （555 ページ）を参照してください。

展開および Configuration Archive の使用

ここでは、展開の管理と Configuration Archive の使用について説明します。

• ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）
• 展開ジョブを正常に完了するためのヒント （513 ページ）
• Workflow 以外のモードでの設定の展開 （515 ページ）
• Workflow モードでの設定の展開 （523 ページ）
• Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）

• Token Management Server への設定の展開 （534 ページ）
• 設定のプレビュー （535 ページ）
• アウトオブバンド変更の検出および分析 （537 ページ）
• デバイスへの設定の再展開 （547 ページ）
• 展開ジョブの中断 （549 ページ）
• 展開スケジュールの作成または編集 （550 ページ）
• 展開スケジュールの一時停止または再開 （554 ページ）
• デバイスの設定バージョンの Configuration Archive への追加 （555 ページ）
• アーカイブされた設定バージョンの表示および比較 （555 ページ）
• 展開トランスクリプトの表示 （558 ページ）

ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示

Deployment Manager では、展開ジョブおよび展開スケジュールのステータスおよび履歴情報の表示、さらに展開ジョブおよび展開スケジュールの作成および管理ができます。[Deployment Manager] ウィンドウを開くには、[管理（Manage）] > [展開（Deployments）] を選択します。

ジョブとスケジュールは、独立したタブに表示されます。ただし、展開スケジューリングに基づいてジョブを作成すると、そのジョブは定期的なジョブのリストに表示されます。ジョブまたはスケジュールのリストを表示するには、対応するタブをクリックします。リストでは、次の情報を参照できます。

- 展開ジョブ：上部ペインには、展開ジョブのリストが表示されます。ジョブを選択すると、さらに詳細な情報が下部ペインに表示されます。
  - [Summary] タブ：[Summary] タブには、ジョブの状態、正常に展開されたデバイスの数、展開時にエラーが発生したデバイスの数などが表示されます。
  - [Details] タブ：[Details] タブには、展開対象の各デバイスの状態の詳細が表示されます。
  - [History] タブ（Workflow モード限定）：[History] タブには、選択したジョブが作成されてから、そのジョブに対して実施されたトランザクションが表示されます。テーブルの各行には、実行された処理、処理を実行したユーザ、処理を実行した日付と時刻、ユーザが入力したコメントが表示されます。
- 展開スケジュール：上部ペインには、展開スケジュールのリストが表示されます。スケジュールを選択すると、さらに詳細な情報が下部ペインに表示されます。
  - [Summary] タブ：[Summary] タブには、スケジュール、スケジュールから次にジョブが作成される時間、スケジュールに基づいてジョブが最後に実行された時間、スケ

ジュールに含まれているデバイスの数、スケジュールを最後に変更したユーザのユーザ ID などが表示されます。

- [Devices] タブ：[Devices] タブには、スケジュールに含まれているデバイスのリストが表示されます。
- [History] タブ：[History] タブには、スケジュールの状態変更および関連するコメントが表示されます。処理ごとにどのユーザが実行したかを追跡できます。
- [Jobs] タブ：[Jobs] タブには、スケジュールから作成された展開ジョブとその状態を記載したリストが表示されます。これらのジョブは、[Deployment Jobs] タブでも参照できます。

[Deployment Manager] ウィンドウに表示される状態情報は、[Security Manager Administration Deployment] ページ（[Tools] > [Security Manager Administration] > [Deployment]）で自動リフレッシュをオフにしていないかぎり、自動的にリフレッシュされます。ジョブまたはスケジュールのテーブルの下にあるメッセージを参照すると、自動リフレッシュがオンになっているかどうかがわかります。オフの場合、状態情報をリフレッシュするには、[リフレッシュ（Refresh）] をクリックします。

関連項目

- 展開プロセスの概要 （482 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの展開ジョブの展開 （530 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）
- 設定のプレビュー （535 ページ）
- デバイスへの設定の再展開 （547 ページ）
- 展開ジョブの中断 （549 ページ）
- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- 展開スケジュールの作成または編集 （550 ページ）
- 展開スケジュールの一時停止または再開 （554 ページ）

展開ジョブを正常に完了するためのヒント

展開が正常に完了するかどうかは、展開のトラブルシューティング （584 ページ）に説明するように多くの要因で決まります。展開ジョブのデバイスを選択するときや、ジョブを開始するときに、ネットワーク通信およびデバイスの正常な機能に関する要因に加えて、次のヒントを念頭に置いておくと、展開の結果をよい方向に導くことができます。

- デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされ、デバイスは機能しません。
- ファイアウォール デバイス限定：ファイアウォール デバイスを（手動定義によるデバイスの追加 （116 ページ）の説明に従って）手動で追加した場合は、そのデバイスに展開する前に、そのデバイスの出荷時のデフォルト ポリシーを検出（インポート）することを強く推奨します。このようなポリシーを Security Manager に導入すると、初めてそのデバイスに展開するときに知らないうちにポリシーを削除してしまうミスを防ぐことができます。ファイアウォール デバイスの出荷時のデフォルト ポリシーの詳細については、ファイアウォールのデフォルト設定 （2333 ページ）を参照してください。ポリシーをインポートする方法の詳細については、 ポリシーの検出 （223 ページ）を参照してください。
- 展開にかかる時間は、展開ジョブに含まれるデバイスの数に応じて数分から 1 時間以上となる場合があります。
- VPN に含まれるデバイスのサブセットを変更すると、VPN が動作しなくなることがあります。展開ジョブを作成するときに VPN に含まれるデバイスのサブセットを選択した場合は、警告が表示され、VPN 内の他のデバイスを選択する機会が与えられます。 警告 - [Partial VPN Deployment] ダイアログボックス （519 ページ）を参照してください。
- 他の展開ジョブに含まれていて現在アクティブな状態（[Edit]、[Edit Open]、および [Approved]）であるデバイスは選択できません。他の展開ジョブに含まれていて現在 [Deployed]、[Failed]、[Discarded]、[Aborted] の状態であるデバイスは選択できます。
- Firewall Service Module（FWSM; ファイアウォール サービス モジュール）および Intrusion Detection System Service Module（IDSM; 侵入検知システム サービス モジュール）には、仮想デバイスが含まれています。Security Manager は、モジュールおよび仮想デバイスを独立したデバイスであると見なします。
- FWSM に加えた変更によっては、Catalyst Multiservice Function Card（MSFC; マルチサービス機能カード）の更新が必要になることもあります。このようなタイプの変更を加えた FWSM を選択した場合、Security Manager は展開ジョブに MSFC を含める必要があることを通知し、自動的に MSFC デバイスを選択します。ただし、MSFC がすでに別のアクティブな展開ジョブに含まれている場合は、現在の展開ジョブにその MSFC を含めることはできません。他の展開ジョブから MSFC を削除するか、他の展開ジョブを廃棄するか、または他の展開ジョブに FWSM を含める必要があります。
- Catalyst 6500/7600 デバイスへの展開の状態は、デバイスへの展開を示すほか、インターフェイス コンテキスト（子デバイス）に影響を与えるインターフェイス コマンドがポリシー変更に含まれているときには、そのインターフェイス コンテキストも示します。たとえば、スイッチが参加している VLAN に影響を与えるポリシー変更を展開するときや、インターフェイス コンテキストを追加または削除するなどしてインベントリを更新するときです。

関連項目

- 展開プロセスの概要 （482 ページ）

• Workflow 以外のモードでの設定の展開 （515 ページ）
• 展開ジョブの作成および編集 （524 ページ）
• デバイス通信設定および証明書の管理 （576 ページ）
• アウトオブバンド変更の検出および分析 （537 ページ）
• Workflow 以外のモードでのジョブの状態 （485 ページ）
• Workflow モードでのジョブの状態 （487 ページ）

Workflow 以外のモードでの設定の展開

設定を展開するとき、デバイスに設定を転送するには、直接転送する方法か、ネットワーク内の別の転送サーバ（AUS、CNS、または TMS など）に転送する方法があります。あるいは、Security Manager サーバのディレクトリに、設定ファイルとして作成することもできます。詳細については、 展開方法について （490 ページ）を参照してください。

（注） デバイスの RAVPN ポリシー（DAP、グループポリシーなど）で使用される Policy Object Manager を介して統合 ACL エントリに変更を加えた場合、デバイスとチケットは[保存した変更の展開（Deploy Saved Changes）] ウィンドウに表示されません。[他のデバイスを追加（Add other devices）] をクリックして、デバイスを手動で追加する必要があります。

ヒント 展開ジョブを作成する前に、 展開ジョブを正常に完了するためのヒント （513 ページ）を参照してください。この項には、展開ジョブを作成する場合に留意する必要のあるヒントと注意が記載されています。

注意 デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされます。

（注） 仮想センサーを使用している場合、IPS デバイスおよびそのデバイス上のすべての仮想センサーは、グループとして展開する必要があります。仮想センサーに変更を加えてから展開した場合、Security Manager は親デバイスとその関連するすべての仮想センサーを展開します。

はじめる前に

- デバイスがブートストラップされていることを確認します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （482 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開方法について （490 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- アウトオブバンド変更の処理方法について （494 ページ）

ステップ 1 Workflow 以外のモードでは、次のいずれかを実行します。

- **[ファイル（File）] > [送信して展開（Submit and Deploy）]** を選択するか、またはツールバーの [変更の送信と展開（Submit and Deploy Changes）] ボタンをクリックします。

（注） これらのオプションは、チケット管理が有効になっている場合は使用できません。

- **[ファイル（File）] > [展開（Deploy）]** を選択します。
- [メイン（Main）] ツールバーの [Deployment Manager] ボタンをクリックし、[展開ジョブ（Deployment Job）] タブがアクティブでない場合にはクリックします。[展開（Deploy）] をクリックします。

Security Manager は、前回の展開以降に加えられたすべてのポリシー変更を検証します。検証でエラーが発生した場合は、エラーを解決してから展開を再試行してください。警告メッセージまたは情報メッセージだけが表示される場合は、[OK] をクリックして [保存された変更の展開（Deploy Saved Changes）] ダイアログボックスに進みます。

ステップ 2 [Deploy Saved Changes] ダイアログボックスで、次の手順を実行します。

- 設定の展開先デバイスを選択します。デバイス セレクタには、ポリシーは変更されたが展開がまだ済んでいないデバイスがすべて表示されます。また、展開する変更デバイスは最初からすべて選択されています。

変更されたデバイスを含むすべてのデバイス グループが表示され、デバイス グループ フォルダを使用して、デバイスを選択または選択解除できます。複数のグループに表示されたデバイスを選択または選択解除すると、そのデバイスはすべてのグループで選択または選択解除されます。ただし、ジョブに含まれるデバイスが展開されるのは 1 回だけです。すべてのフォルダを開くには、[すべて展開（Expand All）] を右クリックして選択します。

[保存された変更の展開（Deploy Saved Changes）] ダイアログボックスには、選択したデバイスの展開に含まれる、変更に関連付けられた日付、時刻、およびユーザーが表示されます。この情報は、展開のために選択したデバイスに基づいて変化します。チケット管理を有効にしている場合、展開する変更に関連するチケットも表示されます。チケット ID をクリックしてチケットの詳細を表示し、設定されている場合は外部チケット管理システムに移動できます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。

アウトオブバンド変更が検出された場合、[OOB Changes] ダイアログボックスを閉じるときに、結果に基づいてデバイス名が色分けされます。緑はアウトオブバンド変更、赤は検出プロセス中のエラー、色に変更がない場合はアウトオブバンド変更がないことを示しています。

- ポリシー変更のないデバイスを展開ジョブに追加する場合は、[他のデバイスを追加（Add other devices）] をクリックして、他のデバイスを追加（Add other devices）] ダイアログボックスを開きます（[Add Other Devices] ダイアログボックス （553 ページ）を参照）。変更されていないデバイスを追加するのは、デバイスが手動で変更されたときに、そのデバイスを以前の設定（Security Manager データベースに格納されている設定）に戻す場合などがあります。
- （オプション）設定の展開方式を変更するには、[展開方式の編集（Edit Deploy Method）] をクリックして、[展開方式の編集（Edit Deploy Method）] ダイアログボックスを開きます（[Edit Deploy Method] ダイアログボックス （518 ページ）を参照）。展開方式にはシステム デフォルト（各組織で選択した方式）が存在するため、方式を変更する必要がない場合があります。選択できる方式は次のとおりです。
  - [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開 （491 ページ）または 中間サーバを使用したデバイスへの展開 （492 ページ）を参照してください。
  - [File]：Security Manager サーバ上の選択したディレクトリに設定ファイルを展開します。詳細については、 ファイルへの展開 （493 ページ）を参照してください。

展開を行う前に、次の作業を実行できます。

- 提示された設定を確認し、最後に展開された設定または現在実行中の設定と比較する。デバイスを右クリックして、[設定のプレビュー（Preview Config）] を選択します。詳細については、 設定のプレビュー （535 ページ）を参照してください。
- [OOBの変更を検出（Detect OOB Changes）] ボタンをクリックし、デバイスを分析してアウトオブバンド変更の有無を調べます。詳細については、 アウトオブバンド変更の検出および分析 （537 ページ）および [OOB (Out of Band) Changes] ダイアログボックス （541 ページ）を参照してください。

ステップ 3 [展開（Deploy）] をクリックして、選択したデバイスの展開ジョブを開始します。これにより、必要な設定ファイルが生成され、選択した展開方法に従って適用されます。

[Deployment Status Details] ダイアログボックスが開き、展開ステータスを参照できます。このダイアログボックスには、ジョブの概要情報、各デバイスへの展開ステータス、および展開に失敗した理由を示すメッセージが表示されます。

[Deployment Details] テーブルで、デバイスに対応する行を選択すると、特にそのデバイス向けの展開ステータス メッセージが表示されます。詳細については、[Deployment Status Details] ダイアログボックス （520 ページ）を参照してください。

デバイスへの展開が失敗した場合は、その失敗したデバイスに設定を再展開できます。詳細については、デバイスへの設定の再展開 （547 ページ）を参照してください。

[Edit Deploy Method] ダイアログボックス

[Edit Deploy Method] ダイアログボックスは、生成した設定を直接ネットワーク内のデバイスに展開するのか、Security Manager サーバ上のディレクトリに設定ファイルを作成するのかを指定する場合に使用します。

ナビゲーション パス

[適用（Deployment）]—[ジョブの作成（Create a job）] ダイアログボックス、または[ジョブの編集（Edit a job）]ダイアログボックス（Workflow モード）、または [保存した変更の展開（Deploy Saved Changes）] ダイアログボックス（Workflow 以外のモード）で、[展開方法の編集（Edit Deploy Method）] をクリックします。手順については、次を参照してください。

- 展開ジョブの作成および編集 （524 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）

関連項目

- 展開方法について （490 ページ）
- Workflow モードでの設定の展開 （523 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）

フィールド リファレンス

表 105 : [Edit Deploy Method] ダイアログボックス

要素	説明
デバイス	デバイスの名前。

要素	説明
方法	使用する展開方法。 • [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開 （491 ページ）または中間サーバを使用したデバイスへの展開 （492 ページ）を参照してください。 • [File]：Security Manager サーバ上のディレクトリに設定ファイルを展開します。[File] を選択する場合は、設定ファイルの展開先ディレクトリを [Destination] カラムで指定します。IPS デバイスではファイル展開を使用できません。詳細については、ファイルへの展開 （493 ページ）を参照してください。 （注） 複数のデバイスの展開方法を一度に設定するには、目的の行を選択して右クリックし、[選択した展開方法の編集（Edit Selected Deploy Method）] を選択します。[Edit Selected Deploy Method] ダイアログボックスが開き、ここで選択を行うことができます。
[接続先（Destination）]	[Method] フィールドで [File] を選択した場合は、設定ファイルを展開するディレクトリを入力します。使用可能なディレクトリのリストから選択するには、[参照（Browse）] をクリックします。
[Preview Config] ボタン	選択したデバイスに対して提示された設定変更を表示するには、このボタンをクリックします。最後に展開された設定または現在実行中の設定と比較できます。詳細については、設定のプレビュー （535 ページ）を参照してください。
Out of Band Change Behavior	CLI を使用してデバイスに直接変更を加えた場合に、Security Manager が実行する処理に対応するオプション ボタンをクリックします。アウトオブバンド変更を処理する方法および使用可能なオプションの意味の詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

警告 - [Partial VPN Deployment] ダイアログボックス

[Partial VPN Deployment] ダイアログボックスは、設定を展開する VPN に含まれる他のデバイスを選択する場合に使用します。

展開ジョブを作成し、そのジョブに VPN 内のデバイスが含まれる場合は、その VPN 内のすべてのデバイスを選択する必要があります。デバイスのサブセットを選択し、それらのデバイスにだけ展開しようとした場合は、このダイアログボックスが表示され、VPN に含まれる他のデバイスを選択できます。

ナビゲーション パス

- Workflow 以外のモード：[保存された変更内容の展開（Deploy Saved Changes）] ダイアログボックスで VPN 内のデバイスのサブセットを選択する場合は、[展開（Deploy）] をクリックすると、このダイアログボックスが表示されます。
- Workflow モード：[ジョブの作成または編集（Create or Edit a Job）] ダイアログボックスで VPN 内のデバイスのサブセットを選択する場合は、[OK] をクリックすると、このダイアログボックスが表示されます。

関連項目

- 展開ジョブの作成および編集 （524 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）

フィールド リファレンス

表 106 : [Partial VPN Deployment Warning] ダイアログボックス

要素	説明
VPN	VPN の名前。
Missing Devices	展開先として選択しなかった VPN 内のすべてのデバイス。
Is Device in Other Job	欠落しているデバイスが別の展開ジョブに含まれているかどうかを示します。
[Deploy to All Devices in VPN] ボタン	VPN 内のすべてのデバイスを展開するには、このボタンをクリックします。 VPN 内のすべてのデバイスに展開できるのは、そのいずれのデバイスも他の展開ジョブに含まれていない場合だけです。
[Deploy to Selected Devices] ボタン	[Create or Edit a Job] ダイアログボックスまたは [Deploy Saved Changes] ダイアログボックスで選択されているデバイスにだけ展開するには、このボタンをクリックします。

[Deployment Status Details] ダイアログボックス

選択したデバイスに設定が展開されているときには、[Deployment Status Details] ダイアログボックスが表示されます。このダイアログボックスには、ジョブの概要情報、各デバイスへの展開ステータス、および展開に失敗した理由を示すメッセージが表示されます。

[Deployment Details] テーブルで、デバイスに対応する行を選択すると、そのデバイスの展開ステータス メッセージが表示されます。

（注） [閉じる（Close）] をクリックして、このダイアログボックスを閉じ、展開を続けながら Security Manager での作業を続けることができます。

ナビゲーション パス

[保存した変更を展開する（Deploy Saved Changes）] ダイアログボックスから、[展開（Deploy）] をクリックします。

関連項目

- 展開プロセスの概要 （482 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- 展開ジョブを正常に完了するためのヒント （513 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- [Device Communication] ページ （668 ページ）

フィールド リファレンス

表 *107 : [Deployment Status Details]* ダイアログボックス

要素	説明
Deployment Status Details	
Progress Status Bar	正常に更新されたデバイスを視覚的に表現し、その割合を示したもの。
ステータス	展開の状態。有効な状態は、[Deploying]、[Aborted]、[Successful]、および [Failed] です。これらの状態の説明については、 Workflow モードでのジョブの状態 （487 ページ）を参照してください。
Deployment Job Name	展開ジョブの名前。
Devices To Be Deployed	展開ジョブに含まれるデバイスの合計数。
Devices Deployed Successfully	正常に更新されたデバイスの数。
Devices Deployed With Errors	更新に失敗したデバイスの数。
展開の詳細 この表には、展開ジョブに含まれるデバイスの一覧が表示されます。	

要素	説明
デバイス	デバイスの名前。
ステータス	デバイスへの展開の状態。これらの状態の説明については、Workflow 以外のモードでのジョブの状態 （485ページ）を参照してください。
[概要（Overview）]	デバイスの警告、エラー、および失敗の数。
方法	デバイスへの展開の方法。有効な方法は、[File] と [Device] です。
Config	デバイス設定ファイル。アイコンをダブルクリックすると、デバイスの設定がプレビューされます。詳細については、設定のプレビュー（535 ページ）を参照してください。
Transcript	（ファイルへの展開ではなく）デバイスに展開している場合、展開中に Security Manager がデバイスに発行したコマンドおよびデバイスからの応答。アイコンをダブルクリックすると、デバイスのトランスクリプトが表示されます。
Last Ticket(s)	デバイスの展開の一部である変更を含むチケット。チケット ID をクリックして、作成者や最終更新日など、チケットに関する追加情報を表示できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[Device Communication] ページ （668 ページ）を参照）。
メッセージ	重大度アイコンで示された、警告、エラー、および失敗のメッセージ。 項目を選択すると、右側の [Description] ボックスに詳細なメッセージが表示されます。右側の [Action] ボックスには、問題の修正方法が表示されます。
[Generate Report] ボタン	このジョブの展開ステータス レポートを作成するには、このボタンをクリックします。レポートは HTML および PDF フォーマットで生成できます。レポートには、ジョブの概要および完全な設定とデルタ設定、およびジョブのトランスクリプトが含まれます。ユーザはこのレポートを独自の目的で使用したり、Cisco TAC の問題のトラブルシューティングに使用したりできます。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成（636ページ）を参照してください。
[Refresh] ボタン	ステータス情報を更新するには、このボタンをクリックします。

要素	説明
[Abort] ボタン	展開ジョブを中断するには、このボタンをクリックします。中断可能な展開ジョブは、[Deploying]、[Scheduled]、または [Rolling Back] の状態にあるジョブだけです。ジョブを中断すると、保留中のデバイスへの設定ファイルの展開が停止しますが、展開が進行中のデバイス（コマンドがデバイスに現在書き込まれています）や、展開がすでに正常に完了したデバイスには影響が及びません。

Workflow モードでの設定の展開

Workflow モードで設定を展開する作業は、いくつかの手順からなるプロセスです。展開ジョブを作成し、承認を得てから、展開する必要があります。このプロセスにより、作業を何名かで分担していても、各人の作業を一元的に管理できます。

設定を展開するとき、デバイスに設定を転送するには、直接転送する方法か、ネットワーク内の別の転送サーバ（AUS、CNS、または TMS など）に転送する方法があります。あるいは、Security Manager サーバのディレクトリに、設定ファイルとして作成することもできます。詳細については、展開方法について （490 ページ）を参照してください。

ヒント　展開ジョブを作成する前に、展開ジョブを正常に完了するためのヒント （513 ページ）を参照してください。この項には、展開ジョブを作成する場合に留意する必要のあるヒントと注意が記載されています。

はじめる前に

- デバイスがブートストラップされていることを確認します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （482 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開方法について （490 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- アウトオブバンド変更の処理方法について （494 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 展開ジョブを作成します。[作成（Create）] をクリックし、ジョブのプロパティを入力します。手順については、展開ジョブの作成および編集 （524 ページ）を参照してください。

ジョブの作成後、そのジョブを送信するかどうかを選択できます。展開ジョブ アプルーバを使用しない場合は、ジョブを自動的に送信し、承認し、展開することもできます。その場合、このプロセスの他の手順を完了する必要はありません。

ステップ 3 （アプルーバを使用したワークフロー）ジョブを送信します。ジョブを送信しなかった場合は、[Deployment Manager] ウィンドウでそのジョブを選択し、[送信（Submit）] をクリックします。電子メールが、アプルーバに送信されます。詳細については、展開ジョブの送信 （528 ページ）を参照してください。

ステップ 4 （アプルーバを使用したワークフローまたは使用しないワークフロー）ジョブを承認します。作成時にジョブを承認しなかった場合は、[Deployment Manager] ウィンドウでそのジョブを選択し、[承認（Approve）] をクリックします。ジョブを承認する担当者が別にいる場合は、その担当者がこの手順を実行する必要があります。詳細については、展開ジョブの承認と拒否 （529 ページ）を参照してください。

ステップ 5 （アプルーバを使用したワークフローまたは使用しないワークフロー）ジョブを展開します。作成時にジョブを展開しなかった場合は、[Deployment Manager] ウィンドウでそのジョブを選択し、[展開（Deploy）] をクリックします。ジョブを開始する時刻として将来の時刻を指定したり、すぐにジョブを開始したりできます。設定は、ジョブのプロパティに従って展開されます。詳細については、Workflow モードでの展開ジョブの展開 （530 ページ）を参照してください。

（注） 展開ジョブは、展開する前であればいつでも廃棄できます。詳細については、展開ジョブの廃棄（531 ページ）を参照してください。

展開ジョブの作成および編集

Workflow モードでは、ポリシー設定をデバイスに展開する前に、展開ジョブを作成する必要があります。ジョブを作成するときは、設定を展開するデバイス、直接デバイスに展開するのか出力ファイルに展開するのか、およびいつジョブを実行するのかを選択します。

（注） デバイスの RAVPN ポリシー（DAP、グループポリシーなど）で使用される Policy Object Manager を介して統合 ACL エントリに変更を加えた場合、デバイスとチケットは [展開-ジョブの作成（Deployment- Create a Job）] ウィンドウに表示されません。[他のデバイスを追加（Add other devices）] をクリックして、デバイスを手動で追加する必要があります。

ヒント 展開ジョブを作成する前に、展開ジョブを正常に完了するためのヒント （513 ページ）を参照してください。この項には、展開ジョブを作成する場合に留意する必要のあるヒントと注意が記載されています。

注意 デバイスに展開する前に、そのデバイスで少なくとも 1 つのポリシーを設定する必要があります。ポリシーを 1 つも割り当てずにデバイスに展開すると、そのデバイスの現在の設定が空の設定で上書きされます。

はじめる前に

- デバイスがブートストラップされていることを確認します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （482 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開方法について （490 ページ）
- アウトオブバンド変更の処理方法について （494 ページ）
- Workflow モードでのジョブの状態 （487 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 次のいずれかを実行します。

- [作成（Create）] をクリックして、新規ジョブを作成します。
- 編集可能なジョブを選択し、[開く（Open）] をクリックしてジョブを編集します。すでに展開したジョブは編集できません。

[Create a Job] ダイアログボックスまたは [Edit a Job] ダイアログボックスが開きます。

ステップ 3 ダイアログボックスで、次の手順を実行してジョブの内容を定義します。

- [ジョブの名前と説明（Job Name and Description）]：デフォルトのジョブ名をそのまま使用するか、またはそのジョブが何であるかがよくわかる名前を入力します。ジョブ名を入力すると各ジョブを区別

できるため、ジョブの内容を反映する名前を割り当てることを推奨します。いったん作成したジョブの名前は変更できません。任意で、ジョブの説明を入力できます。

- 設定の展開先デバイスを選択します。デバイス セレクタには、ポリシーは変更されたが展開がまだ済んでいないデバイスがすべて表示されます。また、展開する変更デバイスは最初からすべて選択されています。

変更されたデバイスを含むすべてのデバイス グループが表示され、デバイス グループ フォルダを使用して、デバイスを選択または選択解除できます。複数のグループに表示されたデバイスを選択または選択解除すると、そのデバイスはすべてのグループで選択または選択解除されます。ただし、ジョブに含まれるデバイスが展開されるのは 1 回だけです。すべてのフォルダを開くには、[すべて展開（Expand All）] を右クリックして選択します。

アウトオブバンド変更が検出された場合、[OOB Changes] ダイアログボックスを閉じるときに、結果に基づいてデバイス名が色分けされます。緑はアウトオブバンド変更、赤は検出プロセス中のエラー、色に変更がない場合はアウトオブバンド変更がないことを示しています。

- ポリシー変更のないデバイスを展開ジョブに追加する場合は、[他のデバイスを追加（Add other devices）] をクリックして、[他のデバイスを追加（Add other devices）] ダイアログボックスを開きます（[Add Other Devices] ダイアログボックス （553 ページ）を参照）。変更されていないデバイスを追加するのは、デバイスが手動で変更されたときに、そのデバイスを以前の設定（Security Manager データベースに格納されている設定）に戻す場合などがあります。
- （任意）設定の展開方式を変更するには、[展開方式の編集（Edit Deploy Method）] をクリックして、[展開方式の編集（Edit Deploy Method）] ダイアログボックスを開きます（[Edit Deploy Method] ダイアログボックス （518 ページ）を参照）。展開方式にはシステム デフォルト（各組織で選択した方式）が存在するため、方式を変更する必要がない場合があります。選択できる方式は次のとおりです。
  - [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開 （491 ページ）または中間サーバを使用したデバイスへの展開 （492 ページ）を参照してください。
  - [File]：Security Manager サーバ上の選択したディレクトリに設定ファイルを展開します。詳細については、ファイルへの展開 （493 ページ）を参照してください。

展開を行う前に、次の作業を実行できます。

- 提示された設定を確認し、最後に展開された設定または現在実行中の設定と比較する。デバイスを右クリックして、[設定のプレビュー（Preview Config）] を選択します。詳細については、設定のプレビュー （535 ページ）を参照してください。
- [OOBの変更を検出（Detect OOB Changes）] ボタンをクリックし、デバイスを分析してアウトオブバンド変更の有無を調べます。詳細については、アウトオブバンド変更の検出および分析 （537 ページ）および [OOB (Out of Band) Changes] ダイアログボックス （541 ページ）を参照してください。

ステップ 4 ダイアログボックスを閉じたときのジョブの処理方法を選択します。使用できるオプションは、展開ジョブ アプルーバを割り当てて Workflow モードを使用しているかどうかによって異なります。

- **承認者なし**：別の承認者を使用しない場合は、次のオプションを使用できます。

- [ジョブを閉じる（Close the job）]：ジョブを閉じ、編集状態のままにします。ジョブにさらに変更を加えることがわかっている場合には、このオプションを選択します。
- [ジョブを承認する（Approve the job）]：ジョブを閉じて承認しますが、まだ展開しません。次を設定します。
- [コメント（Comments）]：（任意）ジョブの承認に関するコメント。
- [送信者（Submitter）]：承認のためにジョブを送信する担当者の電子メールアドレス。ジョブ状態変更の通知が、このアドレスに送信されます。このアドレスには当初、Security Manager へのログインに使用したユーザアカウントに関連付けられた電子メールアドレスが設定されます。このアドレスが正しいアドレスであると、通知を受信できます。
- [ジョブを展開する（Deploy the job）]：ジョブを閉じ、承認し、展開します。次を設定します。
- [オプション（Options）]：[今すぐ展開（Deploy Now）] または [スケジュール（Schedule）]。[Schedule] を選択した場合、他にいくつかフィールドが表示され、ジョブを実行する日付と時刻を指定できます。時間は 24 時間形式で、Security Manager サーバーのタイムゾーンに基づきます。必ずしも現在使用しているタイムゾーンと同じであるとはかぎりません。指定する時刻は、少なくとも 5 分先である必要があります。
- [コメント（Comments）]：（任意）ジョブの展開に関するコメント。
- [展開ステータス通知を送信する（Send Deployment Status Notification）]：ジョブステータスが変更されるたびに、Security Manager から電子メール通知を送信するかどうかを指定します。

このオプションを選択した場合は、通知を受信する担当者の電子メールアドレスを [Job Completion Recipients] フィールドに入力します。複数のアドレスを入力する場合は、各アドレスをカンマで区切ります。このフィールドには当初、デフォルトのアプルーバと自分の電子メール アドレスが入力されています。

- **承認者あり**：別の承認者を使用する場合は、次のオプションを設定できます。
  - [ジョブを送信する（Submit the job）]：承認のためにジョブを送信するかどうかを指定します。デフォルトでは、このチェックボックスはオンになっています。
  - [承認者の電子メール（Approver E-mail）]：承認のためにジョブを送信する場合は、承認者の電子メールアドレスを指定します。デフォルトのアプルーバ電子メール アドレスがフィールドに入力されていますが、このアドレスは変更できます。
  - [コメント（Comments）]：（任意）承認者に送信するコメント（ある場合）。
  - [送信者の電子メール（Submitter E-mail）]：送信者の電子メールアドレス。このフィールドには当初、ログインに使用したユーザアカウントに関連付けられた電子メールアドレスが入力されていますが、別のアドレスに変更できます。

ステップ 5 [OK] をクリック

ジョブの処理方法に関する選択内容によっては、さらにジョブの送信、承認、および展開が必要になることがあります。詳細については、次のトピックを参照してください。

- 展開ジョブの送信　（528 ページ）

• 展開ジョブの承認と拒否 （529 ページ）
• Workflow モードでの展開ジョブの展開 （530 ページ）

展開ジョブの送信

一部の組織では、ジョブを展開する前に、適切な権限を持つ別のユーザがジョブを承認する必要があります。この場合、展開ジョブのアプルーバによって Workflow モードがイネーブルになり、送信者はこのユーザにジョブを送信して確認してもらう必要があります。アプルーバはジョブを確認し、承認または拒否を行います。

展開ジョブアプルーバを割り当てずに Workflow モードを使用している場合は、自分自身でジョブを確認して承認できます。このモードでは、ジョブを送信しません。詳細については、展開ジョブの承認と拒否 （529 ページ）を参照してください。

（注） 展開ジョブの承認は、[Tools] > [Security Manager Administration] > [Workflow] からイネーブルおよびディセーブルにできます。詳細については、[Workflow] ページ （745 ページ）を参照してください。

この手順では、ジョブをすでに作成したものと想定しています。作成時にジョブを送信することもできます。そのためには、[ジョブの作成（Create a Job）] ダイアログボックスで [ジョブの送信（Submit the job）] チェックボックスをオンにします。

関連項目

- [Deployment Manager] ウィンドウ （499 ページ）
- Workflow モードでのジョブの状態 （487 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Status] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 送信するジョブを選択します。

ステップ 3 [送信（Submit）] をクリックします。

[Submit Deployment Job] ダイアログボックスが開きます。

ステップ 4 次の情報を入力します。

- [アプルーバ（Approver）]：ジョブ送信を通知する担当者の電子メールアドレス。デフォルトのアプルーバ電子メール アドレスがフィールドに入力されていますが、このアドレスは変更できます。
- [コメント（Comments）]：（任意）アプルーバに送信するコメント。

- [送信者（Submitter）]：展開ジョブを送信する担当者の電子メールアドレス。このフィールドには当初、Security Manager へのログインに使用したユーザ名に関連付けられた電子メールアドレスが入力されていますが、別の電子メール アドレスに変更できます。

ステップ 5 [OK] をクリック

ジョブ状態が [Submitted] に変わります。ジョブを展開するには、アプルーバがそのジョブを承認する必要があります。

展開ジョブの承認と拒否

一部の組織では、ジョブを展開する前に、適切な権限を持つ別のユーザがジョブを承認する必要があります。展開ジョブアプルーバを割り当てた Workflow モードでは、あるユーザーがジョブを送信し、別のユーザーがそのジョブをプレビューし、承認または拒否の判断を下します。

展開ジョブ アプルーバを割り当てない Workflow モードでは、ジョブを作成し、同時にジョブを承認できます。詳細については、展開ジョブの作成および編集 （524 ページ）を参照してください。

ジョブを拒否すると、そのジョブに含まれるデバイスはすぐに他のジョブに含めることができるようになります。拒否されたジョブは展開できませんが、開いて表示および編集できます。

（注） 展開ジョブの承認は、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ワークフロー（Workflow）]** からイネーブルおよびディセーブルにできます。詳細については、[Workflow] ページ （745 ページ）を参照してください。

関連項目

- [Deployment Manager] ウィンドウ （499 ページ）
- Workflow モードでのジョブの状態 （487 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 送信されるジョブを選択し、次のいずれかを実行します。

- [承認（Approve）] をクリックします。
- [却下（Reject）] をクリックします。

任意で処理のコメントを入力できます。入力したコメントは、ジョブの履歴に保持されます。コメントを送信すると、電子メール通知が送信され（電子メール通知を設定している場合）、ジョブ状態が [Approved]

または [Rejected] に適宜変わります。これでジョブを展開できます（Workflow モードでの展開ジョブの展開 （530 ページ）を参照）。

Workflow モードでの展開ジョブの展開

Workflowモードで作業している場合、設定をデバイスに展開するには、展開ジョブを作成し、その承認を得る必要があります。アプルーバを別途割り当てずに作業している場合は、自分自身でジョブを承認して展開できます。それ以外の場合、ジョブをアプルーバに送信する必要があります。

Workflowモードで展開ジョブを展開すると、それだけでジョブが開始されます。展開中、ジョブの内容は変更できません。

（注） 展開にかかる時間は、展開ジョブに含まれるデバイスの数に応じて数分から 1 時間以上となる場合があります。

はじめる前に

- デバイスがブートストラップされていることを確認します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。
- ジョブを作成します。詳細については、展開ジョブの作成および編集 （524 ページ）を参照してください。
- 展開ジョブ アプルーバを割り当てて Workflow モードを使用している場合は、ジョブを送信します。詳細については、展開ジョブの送信 （528 ページ）を参照してください。
- ジョブを承認します。詳細については、展開ジョブの承認と拒否 （529 ページ）を参照してください。

関連項目

- 展開プロセスの概要 （482 ページ）
- [Deployment Manager] ウィンドウ （499 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開方法について （490 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）

ステップ 1 [メイン（Main）] ツールバーで [Deployment Manager] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 展開するジョブを選択します。

ステップ 3 [展開（Deploy）] をクリックします。

[Deploy Job] ダイアログボックスが開きます。

ステップ 4 [Deploy Job] ダイアログボックスで、次の選択を行います。

- [オプション（Options）]：ジョブを実行する方法。将来のある時点でジョブを実行するには、[スケジュール（Schedule）] を選択します。ジョブを今すぐに実行するには、[今すぐ展開（Deploy Now）] を選択します。将来の時刻にジョブをスケジューリングする場合は、そのジョブで展開される変更は、ジョブの実行時ではなくジョブの作成時点で実施されていた変更に基づきます。

[Schedule] を選択した場合は、日付と時刻のフィールドが表示されます。

- カレンダー アイコンをクリックして、ジョブを実行する日付を選択します。
- [Time] フィールドに、ジョブを開始する時間を 24 時間形式で入力します。時間は、Security Manager サーバのタイム ゾーンのものである必要があります。現在使用中のタイム ゾーンと同じものになるとはかぎりません。指定する時刻は、少なくとも 5 分先である必要があります。
- [コメント（Comments）]：（任意）ジョブを展開する理由の説明。
- [展開ステータス通知の要求、ジョブ完了通知受信者（Require Deployment Status Notifications, Job Completion Recipients）]：ジョブ状態が変化したときに、Security Manager から電子メールを送信するかどうかを指定します。

ステータス通知の送信を選択した場合は、受信者の電子メールアドレスを入力します。このフィールドには当初、ログインに使用したユーザーアカウントに関連付けられている電子メールアドレスが含まれています。複数のアドレスを入力するには、コンマで区切ります。

ステップ 5 [OK] をクリック

[Deployment Manager] ウィンドウに戻ります。ジョブ状態が [Deploying] に変わります。展開が完了すると、ジョブ状態が [Deployed] に変わります。

展開ジョブの廃棄

Workflow モードでは、ジョブは [Deployed]、[Deployment Failed]、[Aborted] を除く任意の状態である場合に廃棄できます。ジョブが [Workflow Management] ページでの設定に従って自動的にシステムから削除されるか、または手動でシステムから削除するまで、ジョブ状態は [Discarded] として表示されます。

関連項目

- [Deployment Manager] ウィンドウ （499 ページ）
- Workflow モードでのジョブの状態 （487 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 廃棄するジョブを選択します。

ステップ 3 [破棄（Discard）] をクリックします。任意で、ジョブを廃棄する理由を入力できます。

Auto Update Server または CNS Configuration Engine を使用した設定の展開

組織が Auto Update Server（AUS）または Cisco Networking Services（CNS）Configuration Engine を使用してネットワーク デバイスへの設定の展開を管理している場合、Security Manager でこのような中間サーバを使用できます。このタイプの展開を実行するには、デバイス、AUS か Configuration Engine、および Security Manager を正しくセットアップする必要があります。この手順では、実行する必要のあるタスクについて説明します。

ヒント AUS を使用するために Security Manager が他のファイルをデバイスにダウンロードする必要がある場合、その AUS には設定を正常に展開できません。たとえば、リモート アクセス VPN ポリシーによっては、プラグイン、Anyconnect クライアント、および Cisco Secure Desktop 設定を設定できます。このようなファイルは AUS に送信されません。このようなタイプのポリシーを設定する場合は、AUS を使用しないでください。

関連項目

- 展開プロセスの概要 （482 ページ）
- デバイスを管理するための準備 （71 ページ）
- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開方法について （490 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）

ステップ 1 AUS または Configuration Engine をそれぞれの製品のマニュアルに従ってセットアップします。

ステップ 2 サーバを使用するようにデバイスを設定します。以降のトピックでは、サーバのタイプおよび目的のセットアップごとに設定手順を示します。

- PIX ファイアウォールおよび ASA デバイスでの AUS の設定 （81 ページ）

ステップ 3 デバイスを Security Manager に追加するときに、選択した方法で可能であればデバイスに AUS または Configuration Engine を選択します。AUS または Configuration Engine が Security Manager にまだ定義されていない場合は、ネットワーク デバイスを追加するときに Security Manager が AUS または Configuration Engine を識別するようにできます。詳細な手順については、次のトピックを参照してください。

- ネットワークからのデバイスの追加 （100 ページ）
- 設定ファイルからのデバイスの追加 （112 ページ）
- 手動定義によるデバイスの追加 （116 ページ）
- インベントリ ファイルからのデバイスの追加 （122 ページ）
- Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）

ヒント デバイスを Security Manager インベントリに追加すると、割り当てるサーバをデバイス プロパティで変更できます。デバイスを右クリックして、[デバイスプロパティ（Device Properties）] を選択します。デバイスを追加するときにサーバを特定できなかった場合は、デバイス プロパティを使用してサーバを設定します。

ステップ 4 デバイスで AUS を使用している場合は、Security Manager にそのデバイスの AUS ポリシーを設定します。次のいずれかを実行します。

- 単一のデバイスのポリシーを設定します。デバイスビューで、デバイスを選択し、次にデバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] を選択します。
- 同じ AUS を共有する多くのデバイスに割り当てることができる共有ポリシーを設定します。ポリシービューで、ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] を選択します。[AUS] を右クリックし、[新規AUSポリシー（New AUS Policy）] を選択してポリシーを作成するか、またはポリシーセレクタから既存のポリシーを選択してポリシーを変更します。[Assignments] タブを選択して、ポリシーを特定のデバイスに割り当てます。

このポリシーで特定するサーバは、デバイス プロパティで特定するサーバでもある必要があります。デバイス プロパティでは Security Manager が設定を送信するサーバを特定し、AUS ポリシーではデバイスが問い合わせるサーバを定義します。

ヒント AUS サーバを変更した場合、デバイスは新しい設定を受け取るまで現在の設定内に定義されている AUS サーバを引き続き使用することに留意してください。したがって、AUS ポリシーは変更しますが、設定の展開には前の AUS サーバを使用する必要があります。展開が正常に完了したあとで、新しいサーバを指し示すようにデバイス プロパティを変更します。

ステップ 5 Security Manager で、[デバイスへの展開（Deploy to Device）] 展開方式を使用して設定を展開します。Security Manager は、設定を AUS または Configuration Engine に送信し、そこでネットワーク デバイスがその設定を取得します。

使用する Workflow モードに応じて、次の手順を実行します。

- Workflow 以外のモードでの設定の展開 （515 ページ）

• Workflow モードでの設定の展開 （523 ページ）

Token Management Server への設定の展開

組織が Token Management Server（TMS）を使用して設定更新をルータに適用する必要がある場合は、TMS プロセスで Security Manager を使用できます。このタイプの展開を実行するには、デバイス、TMS、および Security Manager を正しくセットアップする必要があります。この手順では、実行する必要のあるタスクについて説明します。

関連項目

• 展開プロセスの概要 （482 ページ）
• デバイスを管理するための準備 （71 ページ）
• 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
• 展開方法について （490 ページ）
• デバイス通信設定および証明書の管理 （576 ページ）

ステップ 1 TMS を FTP サーバとしてセットアップします。Security Manager は、FTP を使用して設定ファイルを TMS に展開します。その TMS から設定ファイルを eToken にダウンロードし、暗号化できます。次に、eToken をルータの USB ポートに接続し、設定をダウンロードできます。詳細については、TMS 製品のマニュアルを参照してください。

ステップ 2 Security Manager で、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [トークンの管理（Token Management）]** を選択して、Security Manager への TMS サーバーを特定します。

デフォルトでは、Security Manager は Security Manager サーバを TMS として使用しますが、別のサーバを指定できます。ホスト名かIPアドレス、TMS のユーザ名とパスワード、設定ファイルのコピー先となるディレクトリ、および公開キー ファイルの場所を Security Manager に入力する必要があります。詳細については、[チケット管理（Ticket Management）] ページ （740 ページ）を参照してください。

ステップ 3 Cisco IOS ルータに使用するトランスポート プロトコルとして TMS を指定します。

このパラメータをすべての Cisco IOS ルータ用にグローバルに設定することも、特定のデバイス用に設定することもできます。

- グローバル：**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communication）]** を選択し、**[トランスポートプロトコル（IOSルータ12.3以降）（Transport Protocol (IOS Routers 12.3 and above)）]** で [TMS] を選択します。
- デバイス：デバイスセレクタでデバイスを右クリックし、[デバイスのプロパティ（Device Properties）] を選択します。[General] タブの [Device Communications Group] で、トランスポート プロトコルとして [TMS] を選択します。すべてのルータが TMS をサポートするわけではないため、デバイスによっては TMS を設定できないことがあります。

ステップ 4 Security Manager で、[デバイスへの展開（Deploy to Device）] 展開方式を使用して設定を展開します。Security Manager は、デルタ設定を TMS サーバに送信します。

使用する Workflow モードに応じて、次の手順を実行します。

- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）

ステップ 5 TMS を使用して、設定を eToken にダウンロードします。詳細については、TMS 製品のマニュアルを参照してください。

ステップ 6 設定を eToken からルータにダウンロードし、設定をデバイスに保存します。eToken をルータに接続し、次のコマンドを入力して設定をルータにダウンロードします。*usb_token_id* には、使用した USB ポートに応じて、**usbtoken0** または **usbtoken1** を指定します。デフォルトの PIN は 1234567890 です。

例：

```
router# crypto pki token
usb_token_id
login
PIN

router# config terminal

router(config)# crypto pki token default secondary config CCCD

router(config)# exit

router# write memory
```

ヒント CCCD は eToken のプライベート セクターで、ここに設定ファイルが保存されます。**crypto pki token default secondary config CCCD** コマンドを入力すると、eToken の CLI がルータの CLI とマージされます。

設定のプレビュー

デバイス設定をプレビューするには、さまざまな方法があります。デバイスセレクタからデバイスを選択してから **[ツール（Tools）] > [設定のプレビュー（Preview Configuration）]** を選択することも、いくつかのダイアログボックスで [設定のプレビュー（Preview Config）] ボタンをクリックすることもできます。

ヒント マップビューでデバイスを右クリックし、[設定のプレビュー（Preview Configuration）] を選択することもできます。

設定をプレビューすると、設定が [Config Version Viewer] ダイアログボックスに表示されます。提示された設定が左側に表示されます。デルタ設定を表示するのか（前回の展開以降の変更を表示します）、完全な設定を表示するのかを選択できます。右ペインでは、その設定を最後にデバイスに展開した設定または現在実行中の設定と比較することもできます。

提示される設定の内容は、その内容を参照している場所によって異なります。

- **[ツール（Tools）] > [設定のプレビュー（Preview Configuration）]** を使用した場合、またはデバイスセレクタでデバイスを右クリックし、[設定のプレビュー（Preview Configuration）] を選択した場合、提示された設定にはデータベースにまだ送信していない変更が含まれています。
- 展開ジョブの作成中に設定をプレビューした場合、提示された設定にはデータベースに送信した変更だけが含まれています。この設定に含まれている変更が、展開ジョブを開始した場合にデバイスに展開される変更です。

設定をプレビューすると、デバイスを設定するときに使用する実際のデバイス コマンドを表示できます。CLI に習熟している場合は、これにより、設定が想定どおりのものであることを容易に確認できます。CLI に習熟していない場合でも、プレビューされた情報を使用して、Cisco.com でオペレーティング システムのコマンド リファレンスを参照し、詳細な情報を探すことができます。

（注） デバイスでネットワークオブジェクトを設定した後で、Cisco Security Manager を介して ASA 8.2.3 デバイスを再検出すると、新しいオブジェクトが作成されます。プレビュー設定で生成されるこれらの新しいオブジェクトの CLI は無視してください。

次に、設定をプレビューするためのヒントを示します。

- 設定オプションの多くは、1 つ以上のインターフェイスに固有のものです。ポリシーにインターフェイス名を指定する必要がある場合、プレビューした設定にポリシーのコマンドが含まれるのは、[Interfaces] ポリシーにその指定したインターフェイスを定義している場合だけです。設定をプレビューする前に、[Interfaces] ポリシーを設定していることを確認してください。
- 仮想センサーの設定をプレビューした場合は、表示されるプレビューは仮想センサーではなく親デバイスのものとなります。仮想センサーの設定は親デバイスに保存されているためです。
- ポリシーにどのコマンドが設定されるかを確認するだけである場合は、ダミーのデバイスを追加し、そのデバイスのポリシーを設定することを検討してみてください。これにより、リアルデバイスで意図しない設定変更が実施されるのを容易に防ぐことができます。ダミーのデバイスを追加するには、手動定義によるデバイスの追加 （116ページ）で説明する手順を使用してください。
- 設定を表示するには、ポリシーを検証する必要があります。検証は、プレビューするデバイスだけでなく、すべてのデバイスを対象に実施されます。このため、目的のデバイスとは異なるデバイスに適用されるエラーおよび警告が表示されることがあります。エラーまたは警告が発生した場合は、[Preview Messages] ダイアログボックスが表示されます。ダイアログボックスには、すべてのメッセージがその重大度と有効な解決策を含めて表示されます。[OK] をクリックして、[Config Version Viewer] ダイアログボックスに進みます。[詳細（Details）] をクリックして、問題に関する詳細な情報を表示します。

次の表に、設定のプレビューに使用される [Config Version Viewer] ウィンドウのフィールドを示します。

表 *108 : [Config Version Viewer (Preview Configuration)]* ダイアログボックス

要素	説明
Proposed Config Type	表示する設定のタイプ。たとえば、完全な設定を表示することも、デルタ（最後に設定を展開してから加えられた変更）だけを表示することもできます。提示された設定は、左ペインに表示されます。
Compare to Version	提示された設定と比較する設定を選択します。選択した設定は、右ペインに表示されます。 • [None]：参照設定を空白のままにします。 • [Last Deployed]：最後にデバイスに展開した設定を表示し、その設定と提示された設定とを比較します。 • [Running Config]：デバイスで現在実行中の設定を表示し、その設定と提示された設定とを比較します。デバイスは、現在実行中の設定を取得できるようになっている必要があります。
[First Difference] ボタン	提示された設定と参照設定との間で指摘された最初の違いにカーソルを移動します。
[Previous Difference] ボタン	提示された設定と参照設定との間で指摘された 1 つ前の違いにカーソルを移動します。
[Current Difference] ボタン	現在選択されている差異をページの中央に移動します。
[Next Difference] ボタン	提示された設定と参照設定との間で指摘された 1 つあとの違いにカーソルを移動します。
[Last Difference] ボタン	提示された設定と参照設定との間で指摘された最後の違いにカーソルを移動します。
[Print] ボタン	設定を印刷します。

アウトオブバンド変更の検出および分析

設定をデバイスに展開すると、Security Manager は展開設定に基づいてアウトオブバンド変更を削除するか、または展開を取り消します（アウトオブバンド変更および展開時のその処理方法の詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください）。

Security Manager が展開中にアウトオブバンド変更を削除するという状況はよく発生します。ただし、Security Manager の管理外でそのような変更をデバイスに加えたのには妥当な理由が

あることもあります。このため、設定を展開する前に、アウトオブバンド変更についてデバイスを分析するようにすると効果的です。これにより、保持しておくべき設定変更をプロアクティブに再作成する機会が得られます。

（注） コンソールからデバイスを再起動すると、Config_mod 値が 0 になります。Config_mod パラメータ値は、検出または展開が完了するとすぐに保存されます。CSM で 5 分ごとにデバイスをポーリングして、config_mod パラメータ値の変更をチェックし、OOB を検出するのが理想的です。

前回のデバイスへの展開以降にデバイス設定に加えたアウトオブバンド変更があるかどうかを検出するには、さまざまな方法があります。（別のデバイス管理アプリケーションまたはCLIでの直接更新による）変更があった場合は、その変更をプレビューして、展開前にデバイスポリシーを更新するのか、展開を実施してそのようなアウトオブバンド変更を上書きするのかを判断できます（アウトオブバンド変更は、Cisco Security Manager では OOB 変更と呼ばれることもあります）。一部のシナリオでは、OOB の変更が検出されません。このような例外の処理については、アウトオブバンド変更検出の例外 （540 ページ）を参照してください。

ヒント アウトオブバンド変更を検出できるのは、IOS、ASA、PIX、FWSM の各デバイスとセキュリティコンテキストだけです。IPS デバイスでは検出できません。ただし、展開中にアウトオブバンド変更を処理するための設定は、IPS デバイスにも適用されます。その違いは、IPS デバイスでは展開前にこのような変更をプロアクティブに分析できないことです。

1つ以上のデバイスでアウトオブバンド変更があったかどうかを判断するには、デバイスビューで次のいずれかを実行します。

- **[ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out of Band Changes）]** を選択します。アウトオブバンド変更について評価するデバイスを選択するように求められます。デバイスまたはデバイスグループを選択し、[>>] をクリックして選択済みリストに移動し、[OK] をクリックします。デバイスの選択の詳細については、セレクタの使用 （60 ページ）を参照してください。
- 1 つ以上のデバイスまたはデバイスグループを選択し、右クリックして [アウトオブバンド変更の検出（Detect Out of Band Changes）] を選択します。選択したデバイスが変更について評価されます。
- 展開中に、展開に含めるデバイスを選択し、[OOB変更の検出（Detect OOB Changes）] ボタンをクリックします（このボタンは [保存した変更の展開（Deploy Saved Changes）] ダイアログボックスおよび [展開：ジョブの作成または編集（Deployment—Create or Edit a Job）] ダイアログボックスにあり、現在使用中の Workflow モードによって異なります）。選択したデバイスが変更について評価されます。

展開手順の詳細については、次の情報を参照してください。

- Workflow 以外のモードでの設定の展開 （515 ページ）

- 展開ジョブの作成および編集 （524 ページ）

検出プロセスを開始すると、[OOB (Out of Band) Changes] ダイアログボックス （541 ページ）が開き、その結果を参照できます。現在実行中の設定を取得し、Configuration Archive に格納されている最新の設定と比較することによって、選択した各デバイスが評価されます。Security Manager は、設定間の違いを評価する際、管理対象外のポリシー タイプを考慮しません。

ヒント　展開中の場合、現在実行中の設定は展開対象に提示している設定と比較されないため、アウトオブバンド変更を検出する場合は、提示された設定をプレビューして、Cisco Security Manager ポリシーに同じ変更をすでに実装しているか確認することを推奨します。展開のダイアログボックスでデバイスを右クリックし、[設定のプレビュー（Preview Config）] を選択します。提示された設定を現在実行中の設定と比較できます。詳細については、設定のプレビュー （535 ページ）を参照してください。

[OOB Changes] ダイアログボックスには、変更検出の結果が表示されます。デバイスにアウトオブバンド変更がある場合は、デバイスセレクタのデバイスのアイコンが緑色に変わります。[OOB Details] タブの左ペインでデバイスを選択すると、Configuration Archive に最新の設定に加えられた変更が表示されます。ウィンドウの一番下にあるボタンを使用すると、変更間を移動できます。一番下にある凡例では、変更の説明に使用されるカラーコーディングについて説明しています。

変更を評価するときは、次の点を考慮してください。

- 変更を保持する場合は、Security Manager の該当するポリシーを更新してポリシーを再作成します。preview config を使用すると、ポリシーに変更を加えて目的の結果を得ることができます。Security Manager で使用される命名ルールが異なることがあるため、ポリシーがまったく同じテキストであるかどうかではなく、同じ結果をもたらすものであるかどうかを検討してください。アウトオブバンド変更の検出では、意味の違いではなく、構文の違いが検出されることに留意してください。
- 別のアプリケーションを使用して特定のポリシーのタイプを設定する場合、Security Manager ではそのポリシー タイプを管理対象外にすることを検討してください。Security Manager は、管理対象外のポリシーに関連するコンフィギュレーション コマンドを無視します。詳細については、 [Policy Management] ページ （729 ページ）を参照してください。

（注）　config_mod パラメータ値は、デバイスの検出または展開が実行されるたびに保存されます。CSM では 5 分ごとにポーリングして、config_mod パラメータ値の変更をチェックし、OOB の変更が検出されます。コンソールから ASA デバイスをリロードすると、config_mod パラメータ値が 0 になり、そのデバイスは OOB 状態としてマークされます。

ヒント　展開中にアウトオブバンド変更を検出する場合、[OOB Changes] ダイアログボックスを閉じるときに、結果に基づいて展開のダイアログボックスのデバイス名が色分けされます。緑はアウトオブバンド変更、赤は検出プロセス中のエラー、色に変更がない場合はアウトオブバンド変更がないことを示しています。

アウトオブバンド変更検出の例外

変更が行われたアクティビティを承認していない場合、Cisco Security Manager データベースは更新されません。これにより、（OOB 機能が使用する）Cisco Security Manager 設定アーカイブと Cisco Security Manager データベースとの間に不一致が生じます。アクティビティを承認しない場合、Cisco Security Manager は、デバイスに適用されているアウトオブバンド（OOB）の変更を検出しません。その結果、OOB の変更が検出されたときに展開をキャンセルするように Cisco Security Manager を設定した場合でも、Cisco Security Manager は展開を停止しません（OOB の変更を上書きします）（アウトオブバンド変更の処理方法について （494 ページ）を参照）。このセクションでは、この例外とその対処方法について説明します。

ポリシーの再検出が開始されると、次のタスクが Cisco Security Manager（ワークフローモード）で実行されます。

ステップ 1　再検出後（Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ））、新しいデバイス設定が Cisco Security Manager 設定アーカイブに書き込まれます。

ステップ 2　ポリシーの再検出が実行されるアクティビティを承認しない場合、Cisco Security Manager データベースは新しいデバイス設定で更新されず、古い設定データを引き続き使用します。したがって、設定アーカイブと Cisco Security Manager データベースの間に不一致が生じます。これにより、デバイス上の OOB の変更が Cisco Security Manager によって上書きされる可能性があります。これは、OOB の変更が検出されたときに展開をキャンセルするように設定した場合でも発生します（アウトオブバンド変更の処理方法について （494 ページ）を参照）。

（注）　ポリシーの再検出アクティビティが承認されない場合、アウトオブバンド（OOB）の変更は、Cisco Security Manager データベースとデバイス上の設定との間では検出されません。これは、OOB の変更は、デバイスから検出された設定で更新された Cisco Security Manager 設定アーカイブを使用して検出されるためです（上記のステップ 1 （540 ページ））。一方、アクティビティが承認されていないため、Cisco Security Manager データベースにはデバイスの以前の設定が残っています。

次のタスク

さらに、アクティビティが承認される前に検出されたデバイスに対して 設定のプレビュー （535 ページ）を実行していると、設定のプレビューに正しい設定変更が表示されません。正しい相違を確認するには、最初にアクティビティを承認するか、別のアクティビティから設定をプレビューする必要があります。

アウトオブバンド変更検出の例外

これらの例外を克服するには、次の手順を実行します。

ステップ 1 再検出のための新しいアクティビティを作成します。

ステップ 2 ポリシーの再検出が完了したら、アクティビティを送信して承認します。アクティビティが承認されているかどうかを確認します。

ステップ 3 再検出されたデバイスの設定変更が期待どおりに表示されるかどうかを確認するには、デバイスに対して設定のプレビュー （535 ページ）を実行します。

ステップ 4 必要に応じて、変更を Cisco Security Manager からデバイスに展開します。

[OOB (Out of Band) Changes] ダイアログボックス

[OOB Changes] ダイアログボックスは、デバイスのアウトオブバンド変更を表示および分析する場合に使用します。アウトオブバンド変更とは、デバイスで現在実行中の設定と、Configuration Archive に格納されている最新のデバイスの設定との違いのことです。Security Manager は、設定間に違いがあるかどうかを評価する際、管理対象のポリシータイプだけを考慮することに注意してください。

ヒント 設定は、意味の違いではなく、構文の違いが比較されます。このため、機能の等しい設定がアウトオブバンド変更であると見なされることがあります。

ヒント 例として、セマンティクスを変更せずにデバイス設定で設定行を入れ替える単純なケースを考えてみましょう。この単純な例の場合: 1) Security Manager の行番号 100 にオブジェクトグループがあり、2) ASA 設定の 100 以外の行番号に同じオブジェクトグループが存在する場合、3) Security Manager は OOB として変更を検出して報告します。この単純な例を要約すると、この数個の設定行の順序の変更によってセマンティクスがまったく変わらないとしても、Security Manager は OOB 変更を報告します。

このダイアログボックスには、タブが 2 つあります。

- [OOBの詳細（OOB Detail）]：このタブには、詳細な結果と検出プロセスの経過が表示されます。そのフィールドについては次で説明します。
- [OOBの概要（OOB Summary）]：このタブには検出結果の概要が表示されます。選択したすべてのデバイスで検出プロセスが完了して初めて使用可能になります。情報はデバイス別になっています。タイムスタンプ（日付、時刻、タイムゾーン）のほか、追加、削除、および変更を示す差異データが、関連する設定の行番号とともに表示されます。このタブでテキストを選択し、Ctrl を押しながらクリックしてクリップボードにコピーし、別のアプリケーション（メモ帳など）に貼り付けることができます。

アウトオブバンド変更の検出および分析の詳細については、アウトオブバンド変更の検出および分析 （537 ページ）を参照してください。展開中のアウトオブバンド変更の処理の詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

バージョン 4.7 以降の Security Manager には、アウトオブバンドの変更を再同期するのに役立つツールがあります。この新しいツールの詳細については、OOB 再同期Tool （543 ページ）を参照してください。

ナビゲーション パス

アウトオブバンド変更検出プロセスを開始する方法がいくつかあります。**[ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out of Band Changes）]** コマンドを使用する方法もあれば、1 つ以上のデバイスを選択して右クリックし、[アウトオブバンド変更の検出（Detect Out of Band Changes）] を選択する方法もあります。このほか、次の手順での説明に従って、[保存した変更を展開する（Deploy Saved Changes）] ダイアログボックスおよび[展開（Deployment）]—[ジョブの作成（Create a job）] ダイアログボックス、または[ジョブの編集（Edit a job）]ダイアログボックスで [OOBの変更を検出（Detect OOB Changes）] ボタンをクリックする方法もあります。

- Workflow モードでの設定の展開 （523 ページ）
- 展開ジョブの作成および編集 （524 ページ）

関連項目

- 設定のプレビュー （535 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

フィールド リファレンス

表 109 : [OOB Changes] ダイアログボックス

要素	説明
[Selected Devices] リスト（左ペイン）	このリストには、アウトオブバンド変更について評価するために選択したすべてのデバイスが記載されています。デバイス グループがある場合には、デバイスはデバイス グループ別に編成されます。 デバイスを選択すると、右ペインにその結果が表示されます。 デバイスのアイコンは、検出プロセスの結果に基づいて色が変わります。 • 緑：アウトオブバンド変更があります。 • 赤：アウトオブバンド変更検出プロセスが何らかの理由で失敗しました。 • 色変更なし：アウトオブバンド変更はありません。

要素	説明
設定比較（右ペイン）	右ペインには、選択したデバイスの変更検出プロセスの結果が表示されます。メッセージを参照すると、OOB 検出が進行中であるのか、変更がないのか、変更検出を中断させるエラーが発生したのかがわかります。 変更がある場合、右ペインにはデバイスから取得した現在実行中の設定と、Configuration Archive に格納されている最新のデバイス設定の両方が表示されます。ウィンドウの一番下にある凡例は、変更を示すのに使用されるカラー コーディングについて説明しています。次のボタンを使用して、変更間を移動できます。
[First Difference] ボタン	設定間で指摘された最初の違いにカーソルを移動します。
[Previous Difference] ボタン	設定間で指摘された 1 つ前の違いにカーソルを移動します。
[Current Difference] ボタン	現在選択されている差異をページの中央に移動します。
[Next Difference] ボタン	設定間で指摘された 1 つあとの違いにカーソルを移動します。
[Last Difference] ボタン	設定間で指摘された最後の違いにカーソルを移動します。

OOB 再同期Tool

Security Manager 4.7 の新機能である OOB 再同期ツールは、アウトオブバンドデータの再同期または調整に役立ちます。OOB 再同期ツールは、Security Manager 4.6 およびそれ以前のバージョンで利用可能な OOB 検出ツールの拡張機能であり、4.7 でも継続されています。

ヒント　この分析の後、[再同期の概要（Re-Sync Summary）] タブがアクティブになります。OOB データが発生すると、結果的にデバイスの CLI を更新する必要があります。OOB データは次のような理由で発生します。1）（主に ACL の）緊急要件。不明な検証エラーが展開をブロックしているため、Security Manager を使用してワークフロープロセスを完了させる時間がない。2）同じデバイスを管理するために Security Manager 以外の管理アプリケーションを使用する。3）ASA の Security Manager による機能サポートが完全でない場合、一部の ASA 機能を CLI を使用して管理する必要がある。サードパーティツールを使用してデバイスに加えられた変更と、デバイスに加えられた CLI の変更を合計したものが OOB データとなります。

OOB 再同期ツールは、以前に確立したポリシー構造を保持しながら、デバイス上の OOB データを Security Manager インストールに取り込むプロセスを自動化することを目的としています。

OOB 再同期ツールがないと、展開中に OOB データが検出された場合、Security Manager（バージョン 4.6 以前）は次の管理オプションしか使用できません。

- OOB 変更を警告し、オーバーライドする（デフォルト）：Cisco Security Manager は展開中に OOB 変更を検出し、ユーザーに OOB 変更を警告しますが、そのまま処理を進めて OOB 変更を取り消しまたは消去します。
- 展開を停止：OOB 変更が検出されると、展開を中止します。
- OOB 変更をチェックしない：OOB 変更は展開中に検出されず、デバイスでオーバーライドされます。

OOB 再同期ツールでは次のオブジェクトがサポートされています。

- ネットワークオブジェクト/Object-group
- セキュリティグループ
- サービス オブジェクト グループ
- ユーザーグループ
- 時間範囲オブジェクト

（注） OOB 再同期ツールは、ルータの OOB 変更をサポートしていません。

OOB 再同期ツールは、すべてのオブジェクト/ACL を再同期しません。アクセスルールと統合アクセスルールは再同期しますが、IPv6 アクセスルールなどは再同期しません。次のリストに示すポリシーの詳細に注意してください。

- アクセスルール（統合）はサポートされています
- IPv4 アクセスルールはサポートされています
- IPv6 のみのアクセスルールはサポートされていません
- Ethertype ACL はサポートされていません。
- 標準 ACL はサポートされていません。

OOB 再同期ツールのワークフローは簡単です。

1. 次のいずれかの方法を使用して既存のツールを実行することで、OOB 変更を検出します。
   - **[Configuration Manager] > [ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out Of Band Changes）]**... 。
   - [Configuration Manager] > ツールバー > [OOB変更の検出（Detect OOB Changes）] アイコン
   - [Configuration Manager > [デバイスビュー（Device View）] > デバイスを右クリック > [アウトオブバンド変更の検出（Detect Out Of Band Changes）] をクリックします。
   - [保存した変更を展開する（Deploy Saved Changes）] ダイアログボックスで、[ODBの検出（Detect OOB）] をクリックします。

2. アウトオブバンド変更が検出されると、[OOBの詳細（OOB Details）] タブの [OOB （アウトオブバンド）変更（OOB (Out of Band) Changes）] ダイアログボックスの右側のペインに表示されます。[OOBの詳細（OOB Details）] タブには、変更のレポートと、ターゲットルール番号、共有ポリシー、セクション、影響を受けるデバイス、およびCLI が表示されます。

   また、アウトオブバンド変更が検出されると、 [OOB （アウトオブバンド）変更（OOB (Out of Band) Changes）] ダイアログボックスの右側のペインにある [再同期の概要（Re-Sync Summary）] タブがアクティブになります。

   既存の OOB 検出ツールによって OOB 変更が検出されたら、[評価（Evaluate）] をクリックします。その後、Security Manager は、デバイスで実行されている設定と Security Manager で使用可能な設定の違いをさらに分析します。この分析の後、[再同期の概要（Re-Sync Summary）] タブがアクティブになります。このタブで、Security Manager は、ACE、追加または削除されるオブジェクト、ルールの場所などの、追加の詳細を表示します。

（注） また、Security Manager は、デバイスビューとポリシービューの両方で、Policy Object Manager のオブジェクトについて、ポリシールールテーブルに注釈を付けます。

3. [再同期の概要（Re-Sync Summary）] タブがアクティブになると、レポートを生成し、OOB 機能でサポートされていない CLI があるかどうかを確認するオプションを選択できます。レポートを確認した後、[承認（Accept）] をクリックして変更の受け入れを選択できます。デバイスで ACL またはオブジェクトの変更の永続化操作が正常に行われた場合は、「成功」メッセージが表示されます。

（注） 共有ポリシーの一部であるアクセスルールを変更した場合、この特定のケースで、OOB 再同期ツールは実際に変更されたルールとそのすぐ上のルールの両方に注釈を付けます。これは次の場合に発生します。1）共有ポリシーの一部である少なくとも 2 つのアクセスルールを変更し、2）OOB 再同期ツールを実行し、3）変更を承認した。この場合、OOB 再同期ツールは、変更したルールに加えて、一部のルールの OOB 状態を報告します。ルール自体と共有ポリシーには悪影響がないことを理解することが重要です。

4. 左ペインの [OOBの詳細（OOB Detail）] タブで、.pdf 形式のレポートを要求できます。これを実行するには、[レポートの作成（Generate Report）] ボタンをクリックします。このレポートは必ず生成し、保存して必要に応じてトラブルシューティングに役立てることをお勧めします。

ヒント　次の例では、OOB再同期ツールを使用して、OOB再同期ツールでサポートされていないデバイスの変更と、サポートされているアクセスルールの変更を探すシナリオについて、簡単に説明します。このシナリオでは、IPv4 と IPv6 の両方を使用する ASA があるとします。**[ツール（Tools）] > [アウトオブバンド変更の検出（Detect Out of Band Changes）]** を使用してOOB 変更を見つけた場合、OOB 再同期ツールを使用する OOB 変更の再同期を選択する前に、IPv6 の変更を手動で調整する必要があります。

OOB 再同期ツールを使用する場合は、いくつかの注意事項があります。それらは次の表に記載しています。

表 *110* : 警告

インターフェイスロール	インターフェイスロールに関連付けられたアクセスルールと複数のインターフェイスルールは吸収されません。ただし、ルールには注釈が付けられ、ユーザーが OOB 再同期レポートから OOB ルールをコピーし、適切なルールの場所で「ルールのインポート」を実行して OOB CLI を吸収できるようにします。
Shared Policies	共有ポリシーに影響する OOB 変更は、他のデバイスに影響するため、再同期されません。ルールには、ユーザーによるルールのインポートに役立つように注釈が付けられます。
オブジェクト	OOB 再同期プロセスでは、常にオブジェクトのオーバーライドが作成されます。ただし、そのオブジェクトのオブジェクトオーバーライドが選択的に無効になっている場合、ユーザーがそのオブジェクトのデバイスオーバーライドを有効にするまで、再同期は許可されません。
サポートされていないアクセスリスト	統合アクセスリストの導入前に存在していた IPv6 専用アクセスリストは、再同期ではサポートされません Ether Type アクセスリストの再同期はサポートされていません
OOBアクセスグループ CLI	アクセスグループ CLI の OOB 変更は吸収できません。この警告に関する詳しい説明： • このような状況（アクセスグループ CLI での OOB 変更）では、評価を選択できません。つまり、OOB 変更の再同期を選択することはできません。 • 1）OOB 再同期ツールが再同期できる OOB 変更と、2）アクセスグループ CLI の変更の両方が含まれる場合、 OOB 変更の再同期を選択する前に、access-group コマンドに関する変更を解決する必要があります。

コメントの条件付き再同期	アクセスリスト CLI で作成されたアウトオブバンドに追加された ACL コメントは、ルールの再同期の一部として、再同期中に吸収されます。ただし、ACL コメント単独のランダムな OOB 変更は、再同期中に吸収されません。
ルール分割	ルールは、結合されたルール内で行われた OOB 変更の再同期中に分割されます。ユーザーは、フラット化されたルールで「ルールの結合」を実行して再同期し、可能であれば元のルールに復元する必要があります。

関連項目

- アウトオブバンド変更の検出および分析 （537 ページ）
- アウトオブバンド変更の処理方法について （494 ページ）

デバイスへの設定の再展開

必要に応じて、展開ジョブを再展開できます。これは、[Failed] 状態または [Aborted] 状態のジョブに特に有益です。ジョブに含まれるすべてのデバイスに再展開することも、特定のデバイス（展開が失敗したデバイスなど）を選択することもできます。

交換したデバイスへの設定の再展開に関するヒント

ハードウェア障害などのためにデバイスを交換する必要がある場合、そのデバイスの最後の展開ジョブを再展開することはできません。Security Manager では、そのデバイスが実際は新規のデバイスであることが認識されないためです。古いデバイスの設定を新規のデバイスに展開する場合、次の選択肢があります。

- 新規デバイスのモデルとオペレーティング システム バージョンが交換対象のデバイスとまったく同じである場合は、デバイスセレクタで古いデバイスを選択して右クリックし、[設定のプレビュー（Preview Configuration）] を選択し、完全な設定を新規デバイスにコピーして貼り付けることができます。ただし、この方法では、古いデバイスの証明書が新規デバイスに移行されません。自分自身でデバイスを再登録するか、または証明書を更新する必要があります。
- 新規デバイスが古いデバイスと同じものではない場合は、 Security Manager の機能セットを変更する変更 （157 ページ）で説明する手順に従ってください。

はじめる前に

- デバイスがブートストラップされていることを確認します。詳細については、デバイスを管理するための準備 （71 ページ）を参照してください。
- AUS、CNS、または TMS などの転送サーバに展開する場合は、サーバ、Security Manager 設定、およびデバイスが正しく設定されていることを確認します。

関連項目

- 展開プロセスの概要 （482 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）
- Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）
- Token Management Server への設定の展開 （534 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- 展開方法について （490 ページ）
- Workflow 以外のモードでのジョブの状態 （485 ページ）
- Workflow モードでのジョブの状態 （487 ページ）

ステップ 1 [メイン（Main）] ツールバーで [Deployment Manager] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 設定を再展開するデバイスが含まれているジョブを選択し、次のいずれかを実行します。

- Workflow 以外のモードでは、[再展開（Redeploy）] をクリックします。
- Workflow モードでは、[展開（Deploy）] をクリックします。

[Redeploy a Job] ダイアログボックスが開きます。ダイアログボックスには展開ジョブに含まれるデバイスが一覧表示され、デバイス名、使用される展開方法、前回の展開の状態、およびデバイスを更新した展開ジョブの名前が表示されます。

ステップ 3 [Redeploy a Job] ダイアログボックスで、次の作業を行います。

- [選択（Selection）] 列：[選択（Selection）] 列のチェックボックスにチェックマークを付けて、設定を再展開するデバイスを選択します。当初は失敗したすべてのデバイスが選択されています。
- [展開方法（Deployment Method）]、[接続先(Destination）]：（任意）個々のデバイスの設定を展開するのに使用する方法を変更できます。当初は、ジョブに使用されている方法が選択されています。選択できる方式は次のとおりです。
  - [デバイス（Device）]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。 詳細については、 デバイスへの直接展開 （491 ページ）または 中間サーバを使用したデバイスへの展開 （492 ページ）を参照してください。
  - [ファイル（File）]：Security Manager サーバー上のディレクトリに構成ファイルを展開します。[File] を選択する場合は、設定ファイルの展開先ディレクトリを [Destination] カラムで指定します。使用可能なディレクトリのリストから選択するには、[参照（Browse）] をクリックします。IPS デバイスではファイル展開を使用できません。詳細については、ファイルへの展開 （493 ページ）を参照してください。

（注） 複数のデバイスの展開方法を一度に設定するには、各デバイスを選択し、右クリックして、[選択した展開方法の編集（Edit Selected Deploy Method）] を選択します。[Edit Selected Deploy Method] ダイアログボックスが開き、ここで選択を行うことができます。

- [アウトオブバンド変更の動作（Out of Band Change Behavior）]：（任意）Security Manager 以外のユーザーによってデバイスに変更が加えられたことを検出した場合に、Security Manager がどのように応答するかを選択します（このような変更はアウトオブバンド変更と呼ばれます）。アウトオブバンド変更を処理する方法および使用可能なオプションの意味の詳細については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。

（注） 展開を進める前に、提示された設定を確認し、最後に展開された設定または現在実行中の設定と比較できます。デバイスの行を強調表示し、[設定のプレビュー（Preview Config）] をクリックします。詳細については、設定のプレビュー （535 ページ）を参照してください。

ステップ 4 [OK] をクリックします。

展開ジョブの中断

設定を展開しない場合または展開を延期する場合は、展開ジョブを停止できます。

中断可能な展開ジョブは、[Deploying]、[Scheduled]、または [Rolling Back] の状態にあるジョブだけです。ジョブを中断すると、保留中のデバイスへの設定の展開が停止しますが、展開が進行中のデバイス（コマンドがデバイスに現在書き込まれています）や、展開がすでに正常に完了したデバイスには影響が及びません。

ジョブを中断するには、次のいずれかを実行します。

- アクティブなジョブの稼働状態を表示しているときに、[Deployment Status] ダイアログボックスで [Abort] をクリックします。[Deployment Status Details] ダイアログボックス （520 ページ）を参照してください。
- **[管理（Manage）] > [展開（Deployments）]** を選択して [Deployment Manager] ウィンドウを開き、[展開ジョブ（Deployment Jobs）] タブでジョブを選択し、[中止（Abort）] をクリックします。

[Abort the Job] ダイアログボックスが開き、ジョブ中断の確認が求められます。[OK] をクリックして確認します。

ジョブを中断すると、保留中のデバイスの展開状態が [Aborted] に変わります。

展開を再開するには、ジョブを再展開します。詳細については、デバイスへの設定の再展開 （547 ページ）を参照してください。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）
- Workflow 以外のモードでのジョブの状態 （485 ページ）

- Workflow モードでのジョブの状態 （487 ページ）

展開スケジュールの作成または編集

展開スケジュールを作成して、一定の間隔で展開ジョブを作成できます。スケジュールを使用すると、選択したデバイスで設定を定期的に更新できるようになります。

ヒント　スケジュールにデバイスを含めると、デバイス設定に変更が加えられ、その変更がデータベースにコミットされた場合にだけ、スケジュールから生成された展開ジョブにデバイスが含められます。このため、スケジューリングされた展開にデバイスが含まれていなくても、その変更をまだ送信していない場合（または Workflow モードで独立したアプルーバを使用しているときに、変更を送信したものの、まだ承認が得られていない場合）には、デバイス設定をプレビューしたときに変更が表示されることがあります。

関連項目

- 展開プロセスの概要 （482 ページ）
- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）
- 展開スケジュールの一時停止または再開 （554 ページ）

ステップ 1　[メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。展開スケジュールがアクティブになっていない場合は、[展開スケジュール（Deployment Schedules）] タブをクリックします（[Deployment Schedules] タブ、Deployment Manager （505 ページ）を参照）。

ステップ 2　次のいずれかを実行します。

- 新規スケジュールを作成する場合は、[作成（Create）] をクリックします。
- 既存のスケジュールを編集する場合は、[展開スケジュール（Deployment Schedule）] 表でそのスケジュールを選択し、[開く（Open）] をクリックします。

[Schedule] ダイアログボックスが開きます（[Schedule] ダイアログボックス （551 ページ）を参照）。

ステップ 3　[Schedule] ダイアログボックスに少なくとも次の情報を入力します。

- スケジュールの名前。
- アプルーバを割り当てて Workflow モードを使用している場合は、アプルーバの電子メール アドレスが正しいことを確認します。また、自分の電子メールアドレスを（[Submitter] フィールドで）確認し、ジョブ状態が変わるたびに通知を受け取るかどうかを選択します。

- スケジュールを開始する最初の日付と時刻を定義し、スケジュールに基づいてどのくらいの頻度で展開ジョブを生成するかを選択します。また、スケジュールに終了日を設定し、その日以降は新規にジョブを作成しないようにするかどうかを決定します。
- [デバイスの追加（Add Devices）] をクリックし、展開ジョブに含めるデバイスをすべて選択します。デバイスを含めても、ユーザは引き続きそのデバイスに変更を加えることができ、他の展開ジョブまたは展開スケジュールにそのデバイスを含めることができます。

ユーザ ログイン クレデンシャルを使用してデバイスにアクセスするように Security Manager が設定されている場合は、スケジュール作成中にユーザ名とパスワードがキャプチャされます。パスワードを変更する場合は、スケジュールを作成し直す必要があります。

ステップ 4 [OK] をクリックスケジュールは、[Deployment Schedule] 表に追加されます。

ステップ 5 （Workflow モード限定）Workflow モードで作業している場合、さらに次の手順を完了する必要があります。

- 展開ジョブのアプルーバを使用している場合は、テーブルでスケジュールを選択し、[送信（Submit）] をクリックしてスケジュールをアプルーバに送信します。アプルーバの電子メール アドレスを確認し、アプルーバによるスケジュールの評価に役立つコメントを入力するように求められます。アプルーバがスケジュールを承認しないと、そのスケジュールはアクティブになりません。
- アプルーバを使用しない場合は、テーブルでスケジュールを選択し、[承認（Approve）] をクリックして自分自身でスケジュールを承認し、スケジュールをアクティブにします。

[Schedule] ダイアログボックス

[Schedule] ダイアログボックスは、定期的に繰り返される展開ジョブを作成する場合に使用します。

ナビゲーション パス

[管理（Manage）] > [展開（Deployments）] を選択して [Deployment Manager] ウィンドウを開き、上部ペインの [展開スケジュール（Deployment Schedules）] タブをクリックし、次のいずれかを実行します。

- [作成（Create）] をクリックして、新規スケジュールを作成します。
- スケジュールを選択し、[開く（Open）] をクリックしてそのプロパティを表示または変更します。

関連項目

- 展開スケジュールの作成または編集 （550 ページ）
- 展開スケジュールの一時停止または再開 （554 ページ）

フィールド リファレンス

表 *111 : [Schedule]* ダイアログボックス

要素	説明
Schedule Name Group このグループでは、ジョブの名前およびジョブの通知要件を定義します。	
名前	ジョブの名前。このスケジュールから個々の展開ジョブを作成すると、タイム スタンプがジョブ名に追加されます。
説明	ジョブの目的の説明。
Approver Email （Workflow 限定）	スケジュールを承認する担当者の電子メール アドレス。
説明 （Workflow 限定）	（任意）このスケジュールを保存すると、アプルーバがスケジュールを評価します。その評価に役立つ情報を指定します。
Submitter Email （Workflow 限定）	承認のためにこのスケジュールを送信している担当者の電子メール アドレス。このフィールドには当初、Security Manager へのログインに使用したユーザ アカウントに関連付けられた電子メール アドレスが入力されていますが、別のアドレスに変更できます。
Require Deployment Status Notifications （Workflow 限定）	ジョブ スケジューリングまたはそのスケジュールから作成されたジョブのジョブ状態が変わった場合に、電子メール メッセージを送信するかどうかを指定します。メッセージは、アプルーバと送信者に送信されます。
Recurrence Pattern Group このグループのフィールドには、ジョブ スケジュールを定義します。	
[開始日（Start Date）]	スケジュールの最初の日付。カレンダー アイコンをクリックして、カレンダーから日付を選択します。
Time (Start)	スケジュールを実行する日付の時刻。時間は 24 時間形式で、クライアントのタイム ゾーンではなくサーバのタイム ゾーンに基づいています。

要素	説明
定例（Recurrence）	このスケジュールに基づいて、どのくらいの頻度で展開ジョブを作成するかを指定します。 • [One time]：開始日として指定された日付の指定した開始時間にこのジョブを一度だけ実行します。 • [Hourly]：時間単位のスケジュールでこのジョブを実行します。展開ジョブの実行間隔を時間数で指定します。 • [Daily]：日次スケジュールでこのジョブを実行します。展開ジョブの実行間隔を日数で指定します。 • [Weekly]：指定した曜日にこのジョブを実行します。 • [Monthly]：月次スケジュールでこのジョブを実行します。ジョブを実行する日にちを選択し、展開ジョブの実行間隔を月数で指定します。
Run Indefinitely End Date and Time	スケジュールの有効期限日付と時刻。この時刻を過ぎると、展開ジョブは作成されません。スケジュールが期限切れにならないようにするには、[Run Indefinitely] を選択します。
Devices To Deploy Group この表には、展開ジョブに含まれるデバイスの一覧が表示されます。デバイスをリストに追加したり、リストからデバイスを削除したりするには、[デバイスの追加（Add Devices）] をクリックして、[他のデバイスの追加（Add Other Devices）] ダイアログボックスを開きます（[Add Other Devices] ダイアログボックス （553 ページ）を参照）。 ユーザ ログイン クレデンシャルを使用してデバイスにアクセスするように Security Manager が設定されている場合は、スケジュール作成中にユーザ名とパスワードがキャプチャされます。パスワードを変更する場合は、スケジュールを作成し直す必要があります。	

[Add Other Devices] ダイアログボックス

[Add Other Devices] ダイアログボックスは、展開ジョブまたは展開スケジューリングのデバイスを選択するときに使用します。リストには、実際にはポリシーが変更されていないデバイスも含まれることがあります。デバイスに手動で変更を加えたものの、デバイスを以前の設定（Security Manager データベースに格納されている設定）に戻す場合には、ジョブを作成するときに、ポリシー変更がないデバイスを追加することを推奨します。

- [使用可能なデバイス（Available Devices）] リストでジョブまたはスケジュールに含めるデバイスを選択し、[>>] をクリックしてそのデバイスを [選択されたデバイス（Selected Devices）] リストに移動します。
- デバイスを削除するには、[選択されたデバイス（Selected Devices）] リストでデバイスを選択して、[<<] をクリックします。

ナビゲーション パス

このダイアログボックスを開くには、次のいずれかを実行します。

- （Workflow 以外のモード）[保存した変更の展開（Deploy Saved Changes）] ダイアログボックスから、[他のデバイスの追加（Add other devices）] をクリックします。 Workflow 以外のモードでの設定の展開 （515 ページ）を参照してください。
- （Workflow モード）[展開：ジョブの作成または編集（Deployment: Create or Edit a Job）] ダイアログボックスから、[他のデバイスの追加（Add other devices）] をクリックします。展開ジョブの作成および編集 （524 ページ）を参照してください。
- （すべてのモード）[Schedule] ダイアログボックス （551 ページ）から、[デバイスの追加（Add Devices）] をクリックします。

関連項目

- 展開ジョブまたは展開スケジュールにデバイスを含める操作 （489 ページ）
- 展開スケジュールの作成または編集 （550 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）>

展開スケジュールの一時停止または再開

アクティブな展開スケジューリングを廃棄せずに一時停止し、あとでスケジュールに基づいてジョブの作成を再開するときに再アクティブ化できます。これにより、スケジュールを一時的に無効にできます。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）
- 展開スケジュールの作成または編集 （550 ページ）

ステップ 1 [メイン（Main）] ツールバーで [Deployment Manager] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。展開スケジュールがアクティブになっていない場合は、[展開スケジュール（Deployment Schedules）] タブをクリックします（[Deployment Schedules] タブ、Deployment Manager （505 ページ）を参照）。

ステップ 2 次のいずれかを実行します。

- アクティブなスケジュールを一時停止するには、そのスケジュールを選択し、[一時停止（Suspend）] をクリックします。

- 一時停止したスケジュールを再開するには、そのスケジュールを選択し、[再開（Resume）] をクリックします。

デバイスの設定バージョンの Configuration Archive への追加

Configuration Archive は、設定をデバイスにロールバックするときも含め、設定がデバイスまたはファイルに展開されるときには必ず新規設定バージョンで更新されます。

また、デバイスから直接設定を取得して、Configuration Archive に追加することもできます。これは、直接デバイス設定に変更が加えられたときに便利です（この変更はアウトオブバンド変更と呼ばれます）。

（注） AUS によって管理されるデバイス、およびダイナミック IP アドレスが設定されているデバイスからは、設定を取得できません。

この手順を使用すると、デバイスから設定を取得してアーカイブに追加できます。

関連項目

- アーカイブされた設定バージョンの表示および比較 （555 ページ）

ステップ 1 **[管理（Manage）] > [Configuration Archive]** を選択して、Configuration Archive を開きます（[Configuration Archive] ウィンドウ （509 ページ）を参照）。

ステップ 2 デバイス セレクタで、設定を取得するデバイスを選択します。アーカイブされた設定が右側のペインに表示されます。

ステップ 3 [デバイスから追加（Add from Device）] をクリックします。Security Manager がデバイスにログインし、現在実行中の設定を取得してアーカイブに追加します。

アーカイブされた設定バージョンの表示および比較

Configuration Archive では、デバイスの以前の設定を表示し、設定のバージョンを比較し、設定展開に関連するトランスクリプトを表示できます。Configuration Archive ウィンドウを開くには、**[管理（Manage）] > [Configuration Archive]** を選択します。

デバイスの設定バージョンを表示するには、デバイスセレクタでデバイスを選択します。アーカイブされたすべてのバージョンが右ペインに表示されます。次を実行できます。

- 設定を表示するには、その設定を選択し、[表示（View）] をクリックします。[Config Version Viewer] ダイアログボックスが開き、設定が左ペインに表示されます（ダイアログボックスの詳細については、[Configuration Version Viewer] （556 ページ）を参照してください）。

選択したバージョンに使用できる設定のタイプが複数ある場合は、[設定タイプ（Config Type）] フィールドを使用して、どのタイプを表示するかを選択できます。[フル（Full）] バージョンは設定がすべて含まれたもので、[デルタ（Delta）] バージョンはこのバージョンと、デバイスの前回の完全な設定との間で異なるコマンドだけが含まれたものです。デルタ設定には、ネガティブ コマンドが含まれることがあります。

- 設定を比較するには、その設定を選択し、[表示（View）] をクリックします。[Config Version Viewer] ウィンドウの [バージョンを比較（Compare with Version）] フィールドで比較する設定を選択します。2 つめのバージョンが右ペインに表示され、相違点がカラー コーディングで示されます。カラー コーディングについては、表示領域の下にあるキャプションを参照してください。
- 設定の展開に関連付けられたトランスクリプトを表示するには、次のいずれかを実行します。
  - [Configuration Archive] ウィンドウから、目的の設定の [Transcript] 列のアイコンをダブルクリックします。
  - [Config Version Viewer] ダイアログボックスの左ペインに設定を表示するときは、[トランスクリプトビュー（Transcript View）] をクリックします。

トランスクリプトとは、展開処理またはロールバック処理の間にキャプチャされた、Security Manager とデバイス間のトランザクション ログ ファイルです。この中には、展開要求またはロールバック要求が出た時点からサーバとデバイス間で送受信されたコマンドは含まれていますが、展開の初期検出フェーズである、Security Manager がデバイスから現在の設定を取得するときに行われた通信は含まれていません。ロールバックが失敗した場合、ロールバックまたは展開が失敗した段階によっては一部のトランスクリプトが生成されることがあります。トランスクリプトは、[Transcript Viewer] ウィンドウに表示されます（展開トランスクリプトの表示 （558 ページ）を参照）。

[Configuration Archive] 設定ページでは、アーカイブする設定バージョンの数を設定できます（[Configuration Archive] ページ （649 ページ）を参照）。

関連項目

- デバイスの設定バージョンの Configuration Archive への追加 （555 ページ）

[Configuration Version Viewer]

（Configuration Archive から開いた）[Config Version Viewer] ウィンドウは、デバイスの以前の設定を表示し、アーカイブされた他の設定と比較する場合に使用します。どのバージョンも、選択したデバイスのアーカイブにある他のバージョンと比較できます。選択したバージョンが左ペインに表示され、このウィンドウの右上にあるリストから比較対象の別のバージョンを選択できます。バージョンの表示および比較の詳細については、アーカイブされた設定バージョンの表示および比較 （555 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [Configuration Archive] を選択し、設定を表示するデバイスを選択します。次に、設定を選択し、[表示（View）] をクリックします。

関連項目

- [Configuration Archive] ウィンドウ （509 ページ）
- 展開トランスクリプトの表示 （558 ページ）
- アーカイブされた設定バージョンの表示および比較 （555 ページ）
- デバイスの設定バージョンの Configuration Archive への追加 （555 ページ）

フィールド リファレンス

表 *112 : [Configuration Version Viewer]* ウィンドウ（*Configuration Archive*）

要素	説明
バージョン ID（Version ID）	左ペインに表示する設定バージョン。 • [Previous]：現在選択しているバージョンよりも 1 つ前にあるバージョンを表示します。 • [Next]：現在選択しているバージョンよりも 1 つあとにあるバージョンを表示します。 • [Last]：リストの最後にあるバージョンを表示します。 • [Specific Date and Time]：指定の日付と時刻に作成されたバージョンを表示します。
Compare with version	バージョンを比較する場合は、左ペインで選択されているバージョンと比較する設定バージョン。設定は、右ペインに表示されます。相違点がまとめられ、カラー コーディングで示されます。カラー コーディングについては、ペインの下にあるキャプションを参照してください。

要素	説明
Config Type	表示できる設定のタイプ。設定のタイプは、デバイスのタイプによって異なります。タイプは [Full] または [Delta] となり、次の意味があります。 • [Full Configuration]：選択したデバイスの完全な設定で、Configuration Archive には完全な設定で保存されています。デバイスの完全な設定を比較できます。 • [Delta Configuration]：展開中に Security Manager が生成するファイルで、[Version ID] フィールドで選択されている設定と前回展開されたバージョンとの間に見られるポリシー変更を表します。 （注） アウトオブバンド変更（CLI での変更など）の場合、設定バージョンが生成され、[デバイスから追加（Add from Device）] を使用してそのバージョンを Configuration Archive に追加できますが、デルタ設定ファイルは生成されません。
[First Difference] ボタン	設定バージョン間で指摘された最初の違いにカーソルを移動します。
[Previous Difference] ボタン	設定バージョン間で指摘された 1 つ前の違いにカーソルを移動します。
[Current Difference] ボタン	カーソルを使用して、ウィンドウで現在選択している違いにフォーカスします。
[Next Difference] ボタン	設定バージョン間で指摘された 1 つあとの違いにカーソルを移動します。
[Last Difference] ボタン	設定バージョン間で指摘された最後の違いにカーソルを移動します。
[Transcript View] ボタン	[Transcript Viewer] ウィンドウを開くには、このボタンをクリックします。このウィンドウには、この設定に関連付けられたデバイス通信トランスクリプトが表示されます。
[Print] ボタン	設定を印刷するには、このボタンをクリックします。

展開トランスクリプトの表示

[Transcript Viewer] ウィンドウは、Security Manager とデバイスとの間で交換されたメッセージの記録を表示する場合に使用します。トランスクリプトとは、展開処理またはロールバック処理の間にキャプチャされた、Security Manager とデバイス間のトランザクション ログ ファイルです。この中には、展開要求またはロールバック要求が出た時点からサーバとデバイス間で送受信されたコマンドは含まれていますが、展開の初期検出フェーズである、Security Manager がデバイスから現在の設定を取得するときに行われた通信は含まれていません。詳細については、アーカイブされた設定バージョンの表示および比較 （555 ページ）を参照してください。

ナビゲーション パス

- Configuration Archive：[管理（Manage）] > [Configuration Archive] を選択して、Configuration Archive を開き、トランスクリプトを表示するデバイスを選択し、目的の設定バージョンの行にある [トランスクリプト（Transcript）] アイコンをダブルクリックします。

アーカイブされた設定を調べるときには、[Configuration Version Viewer] ウィンドウから [トランスクリプトの表示（Transcript View）] ボタンをクリックすることもできます（[Configuration Version Viewer] （556 ページ）を参照）。

- Deployment Manager：[管理（Manage）] > [展開（Deployments）] を選択して、Deployment Manager を開き、目的のデバイス展開が含まれている展開ジョブを選択します。次に、下部ペインで [詳細（Details）] タブを選択し、目的のデバイスの行にある [トランスクリプト（Transcript）] アイコンをダブルクリックします。

関連項目

- [Configuration Archive] ウィンドウ （509 ページ）
- [Deployment Manager] ウィンドウ （499 ページ）

フィールド リファレンス

表 *113 : [Transcript Viewer]* ウィンドウ

要素	説明
バージョン ID（Version ID）	トランスクリプトを表示する設定バージョン。 • [Previous]：現在選択しているバージョンよりも 1 つ前にあるバージョンのトランスクリプトを表示します。 • [Next]：現在選択しているバージョンよりも 1 つあとにあるバージョンのトランスクリプトを表示します。 • [Last]：リストの最後にあるバージョンのトランスクリプトを表示します。 • [Specific Date and Time]：指定の日付と時刻に作成されたバージョンのトランスクリプトを表示します。
Transcript Type	表示するトランスクリプトのタイプ。設定バージョンによっては、複数のトランスクリプトが関連付けられていることがあります。このフィールドを使用して、どのトランスクリプトを表示するかを選択します。

要素	説明
[Transcript] ウィンドウ	選択したトランスクリプトを表示します。テキストを選択し、クリップボードにコピーできます（Ctrl を押した状態で C を押します）。コピーしたテキストは、テキスト エディタに貼り付けることができます。
[表示（View）] ボタン	[Config Version Viewer] ウィンドウに関連する設定を表示するには、このボタンをクリックします（[Configuration Version Viewer]（556 ページ）を参照）。
[Print] ボタン	トランスクリプトを印刷するには、このボタンをクリックします。

設定のロールバック

新規設定をデバイスに展開したあと、その新規設定が正しく機能しないことがわかった場合は、設定を古いバージョンにロールバックできます。ただし、通常は、Security Manager で設定を修正し、修正された設定を展開するようにしてください。設定をロールバックすると、Security Manager に定義されている設定と、デバイスで実行中の設定が異なるという状況が発生します。設定をロールバックするのは、極端な状況にある場合だけとしてください。

以降のトピックは、設定のロールバックの理解を深めて、効果的に使用するのに役立ちます。

- 設定のロールバックについて （560 ページ）
- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- ファイルへの展開時のロールバックの実行 （571 ページ）

設定のロールバックについて

展開方法として [Device] を使用して設定をデバイスに展開した場合、設定を直接デバイスに展開しようと、中間サーバに展開しようと、その新規設定が正しく機能しないことがわかったときには、設定を古いバージョンにロールバックできます。ファイルに展開された設定にはロールバックできません。

注意 通常は、Security Manager で設定を修正し、修正された設定を展開するようにしてください。設定をロールバックすると、Security Manager に定義されている設定と、デバイスで実行中の設定が異なるという状況が発生します。ロールバックを実行したあとはデバイスのポリシーを再検出し、デバイスの設定と Security Manager に格納されている設定を一致させる必要があります。設定をロールバックするのは、極端な状況にある場合だけとしてください。

次のツールを使用して、設定をロールバックできます。

- Deployment Manager：最後の正常時の設定がファイルではなくデバイスに展開されたものであれば、展開をその設定にロールバックできます。Deployment Manager を開くには、**[管理（Manage）] > [展開（Deployments）]** を選択します。
- Configuration Archive：アーカイブされた設定がデバイスに展開されたものか、デバイスから作成されたものであれば、その設定に展開をロールバックできます。Configuration Archive を開くには、**[管理（Manage）] > [Configuration Archive]** を選択します。

設定をロールバックすると、Security Manager は次の処理を実行します。

- PIX ファイアウォール、ASA デバイス、および FWSM デバイスの場合、Cisco Security Manager はデバイスの SSL インターフェイスで **replace config** オプションを使用して、リロードと同等の操作を実行します（xlate はクリアされ、IPsec トンネルは終了するなど）。
- IOS 12.3(7)T 以降が稼働するデバイスの場合、Cisco Security Manager は **configure replace** コマンドを使用して、現在実行中の設定を設定ファイルの内容に置換します。このコマンドのサポートは、デバイスにインストールされている IOS バージョンによって異なります。
  - IOS 12.3(7)T 以降が稼働するデバイスの場合、Cisco Security Manager は **configure replace** コマンドを実行する前に、構成ファイルをスタートアップ コンフィギュレーションにコピーします。設定置換操作が失敗した場合、Cisco Security Manager は **reload** コマンドを発行し、スタートアップ コンフィギュレーションの内容を使用してオペレーティングシステムをリロードします。reload コマンドは、システムを再起動するため、一時的にネットワークが停止することがあります。
  - 12.3(7)T よりも前のバージョンが稼働するルータの場合、Cisco Security Manager は構成ファイルをスタートアップ コンフィギュレーションにコピーし、**reload** コマンドを発行してシステムを再起動します。この方法を使用している場合、Security Manager は [Configuration Archive] 設定ページ（[Configuration Archive] ページ （649 ページ）を参照）に指定されている TFTP サーバおよびディレクトリを使用します。
- ロールバックされた設定は、そのデバイスの Configuration Archive で別のアーカイブされたバージョンになります。

ヒント 設定のロールバックには、ユーザ アカウント ポリシーが含まれません。設定をロールバックしても、ユーザ アカウントの既存の状態は変わりません。これにより、ユーザはこれまでどおりデバイスにログインできます。

デバイス タイプおよび設定によっては、ロールバックに特殊な考慮事項が適用されます。詳細については、次の各項を参照してください。

- マルチ コンテキスト モードのデバイスのロールバックについて （562 ページ）
- フェールオーバー デバイスのロールバックについて （562 ページ）

• Catalyst 6500/7600 デバイスのロールバックについて （563 ページ）
• IPS および IOS IPS のロールバックについて （564 ページ）
• ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）
• ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

関連項目

• Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
• ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）

マルチ コンテキスト モードのデバイスのロールバックについて

ロールバックしようとしているシステム実行スペースの設定にセキュリティ コンテキストへの接続オプション（vlan config など）が指定され、かつロールバック対象として選択した設定とセキュリティ コンテキストで現在実行中の設定との間に不一致がある場合、Security Manager はセキュリティ コンテキストに接続できないことがあります。そのような場合は、システム実行スペースの設定をロールバックする前に、セキュリティコンテキストの設定をロールバックすることを推奨します。

マルチコンテキストモードで動作するデバイスのシステム実行スペースの設定をセキュリティ コンテキストのセットが異なる設定にロールバックした場合、ロールバック後、デバイス上のセキュリティ コンテキストが、Security Manager で管理されていてデバイス セレクタに表示されているセキュリティ コンテキストに一致しなくなることがあります。

関連項目

• Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
• ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
• ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）
• ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

フェールオーバー デバイスのロールバックについて

フェールオーバー ポリシーが含まれているセキュリティ コンテキストの設定をロールバックすると、Security Manager は当初システム実行スペースでフェールオーバーをディセーブルにし、両方のデバイスがアクティブになります。ロールバックの完了後、どちらのデバイスもそれぞれのフェールオーバー設定に戻ります。

ロールバック中にスイッチオーバーが発生した場合、またはアクティブ装置とスタンバイ装置との間で接続が失われた場合は、ロールバックの完了後、ブートストラップ設定をスタンバイ装置にコピーします。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログ ボックス （2579 ページ）を参照してください。

Security Manager は、次の条件が満たされた場合にのみ、ロールバックアクションを続行できます。

- プライマリユニットとセカンダリユニットの両方がアクティブ状態である必要があります。
- リンク上で構成されている場合、リンクが稼働している必要があります。
- LAN 上で構成されている場合は、インターフェースが稼働している必要があります。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

Catalyst 6500/7600 デバイスのロールバックについて

サービス モジュールへの接続オプション（vlan config など）を指定する Catalyst 6500/7600 デバイスに設定をロールバックするときに、ロールバック対象として選択した設定と現在実行中の設定との間に不一致がある場合、Security Manager はサービス モジュールに接続できないことがあります。設定を Catalyst 6500/7600 シャーシにロールバックする前に、サービス モジュールの設定をロールバックすることを推奨します。

したがって、Catalyst 6500/7600 デバイスでロールバックを実行するための正しい順序は次のようになります。

1. セキュリティ コンテキスト。
2. サービス モジュール。
3. シャーシ。

ロールバック操作の完了後、再検出を実行することを推奨します。

FWSM 展開をロールバックしている場合、デバイスの追加時にセキュリティ証明書を取得するようにシステムが設定されていると、ロールバック操作の完了後、証明書を取得することが必要になる場合があります。このためには、次のいずれかの方法を使用します。

- デバイス プロパティからデバイス単位で証明書を取得します。
- ロールバック後に自動的に証明書を取得するように Security Manager を設定します。このためには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communication）] を選択し、（[SSL証明書パラメータ（SSL Certificate Parameters）] の）[PIX/ASA/FWSMデバイス認証証明書（PIX/ASA/FWSM Device Authentication Certificates）] フィールドで [デバイスを追加時に取得（Retrieve while adding devices）] を選択します。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

IPS および IOS IPS のロールバックについて

（注） バージョン 4.17 以降、Cisco Security Manager は FWSM、IPS、および PIX デバイスをサポートしていません。さらに、このリリース以降、Cisco Security Manager は機能拡張を提供していません。

IPS デバイスおよび IOS IPS デバイスのロールバックには、特殊な考慮事項が適用されます。IPS デバイスおよび IOS IPS デバイスの場合、ロールバックにはセンサー更新またはシグニチャ更新のロールバックが含まれることがあります。このようになるのは、IPS デバイスおよび IOS IPS デバイスの場合、Security Manager は設定の管理をサポートするだけでなく、手動および自動によるアップグレードとシグニチャ更新という形でイメージ管理もサポートするためです。ロールバックを実施するときは、センサー更新やシグニチャ更新ではなく、設定をロールバックすることに留意してください。センサー更新とシグニチャ更新がダウングレードされるのは、どちらの更新もダウングレードしないと設定をロールバックできない場合だけです。

ロールバックは、Configuration Archive によって実施されます。IPS デバイスおよび IOS IPS デバイスの場合、現在の設定だけがアーカイブされます。あるデバイス バージョン（バージョン X など）の現在の設定が、別のデバイス バージョン（バージョン Y など）には有効でないことがあります。Security Manager は、バージョン X の設定がバージョン Y に有効であるかぎり、バージョン X の設定をバージョン Y のセンサーにロールバックします。

X の設定が Y に有効である場合、ロールバックが開始され、Security Manager は確認のダイアログボックスを表示します。X の設定が Y に有効ではない場合、Security Manager は警告ダイアログボックスを表示し、ロールバック中にセンサーをダウングレードするためのオプションを示します。ただし、このようなダウングレードがロールバックの完了に有用である場合にかぎります。

注意 IPS デバイスをダウングレードすると、IPS デバイスの一部の機能が削除されます。たとえば、エンジンをダウングレードすると、最新のシグニチャ更新を適用できなくなります。シグニチャ更新を最新の状態に維持せずに IPS デバイスを操作すると、IPS デバイスの有効性が減少します。

展開ジョブのロールバックの場合、警告ダイアログボックスには次のタイプの警告が 1 つ以上含まれています。

- Security Manager は、センサー バージョンをダウングレードしないとロールバックを実行できない IPS デバイスについて警告します。
- Security Manager は、シグニチャ レベルが変更された IOS IPS デバイスについて警告します。このようなデバイスの場合、設定の IPS 以外のセクションだけをロールバックできます。
- Security Manager は、レベルを 2 つ以上ダウングレードする必要がある IPS デバイスについて警告します。Security Manager では、このようなダウングレードは実行できません。このようなダウングレードには、Cisco IPS CLI を使用する必要があります。警告ダイアログボックスには、どのバージョンにデバイスを再イメージ化またはダウングレードする必要があるかが表示されます。

（注） IOS IPS デバイスはダウングレードをサポートしていないため、ロールバック中に IOS IPS デバイスをダウングレードするためのオプションは使用できません。

ロールバック中にセンサーをダウングレードするためのオプションがロールバックの完了に有用でない場合は、ロールバックが実行できないことと、ロールバックするデバイスでイメージを手動で再インストールする必要があることを通知するエラー メッセージが返されます。最近デバイスにインストールされた更新パッケージだけがダウングレードできるため、次のような場合にはダウングレードは有用ではありません。

- 複数の更新パッケージをデバイスにダウンロードする必要がある展開（シグニチャ更新）をロールバックする場合。
- 複数のアップグレードを実行したあとに続くロールバックの古い展開または設定を選択する場合。
- ダウングレードできないアップグレードをロールバックする場合。表 114 : センサーの有効なアップグレード タイプのダウングレード サポート （565 ページ）に示すように、メジャー、マイナー、およびほとんどのサービス パックのアップグレードはダウングレードできません。

設定のロールバックで Cisco IPS 5.1(4) よりも前のバージョンにダウングレードする必要がある場合、Security Manager は自動ダウングレードをサポートしません。指定のバージョンにデバイスを手動でダウングレードしてから、ロールバックを続行する必要があります。

表 *114* : センサーの有効なアップグレード タイプのダウングレード サポート

アップグレード タイプ	ダウングレード サポート
メジャー アップグレード	ダウングレードはサポートされません。
マイナー アップグレード	ダウングレードはサポートされません。
サービス パック更新	Cisco IPS 5.1(4) 以降からのダウングレードはサポートされません。

アップグレード タイプ	ダウングレード サポート
パッチ更新	ダウングレードがサポートされます。
シグニチャ アップデート	ダウングレードがサポートされます。
エンジン更新	ダウングレードがサポートされます。
再パッケージ（メジャー更新、マイナー更新、およびサービス パック更新に適用可能）。	5.1(4) よりも前のサービス パックの再パッケージはダウングレードできます。

注意 デバイスがダウングレードされている場合、そのデバイスで実施された Outbreak Prevention 更新が失われることがあります。

ロールバック中、デバイスに対するアウトオブバンド変更があるためにロールバックを実施できないことが検出された場合は、ロールバックが実施できないことを通知するエラー メッセージが返されます。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）

ロールバック後、競合を発生させる可能性があるコマンド

次のコマンドは、ロールバック後、競合を発生させる可能性があります。

- **http server enable** *port***http** *ip_address net_mask interface_name*

セキュリティ コンテキストだけに適用できます（システム実行スペースには適用できません）。

- **allocate-interface** {*physical_interface* | *subinterface* } **[map_name] [visible | invisible]**

context サブコマンドのシステム実行スペースだけに適用できます。

- **config-url** *diskX:/path/filename*

context サブコマンドのシステム実行スペースだけに適用できます。

- **join -failover-group** *group_number*

アクティブ/アクティブ フェールオーバーと context サブコマンドのシステム実行スペースだけに適用できます。フェールオーバー グループは、指定されていない場合、デフォルトではグループ 1 となります。

- **フェールオーバー**

システム実行スペースだけに適用できます。failover をイネーブルにすると、ピア間で設定同期がトリガーされます。

- **failover lan enable**

システム実行スペースだけに適用できます。このコマンドを省略した場合、PIX プラットフォームではシリアル ケーブル フェールオーバーを設定したことになり、ASA および FWSM ではフェールオーバー設定警告が不完全なものになります。

- **failover lan unit** {*primary* | *secondary* }

システム実行スペースだけに適用できます。このコマンドを指定していない場合、デフォルトでは両方の装置がセカンダリになります。誤った装置でロールバックが実行された場合、両方の装置がプライマリになり、どちらの装置が最初にアクティブになるかに影響を与えます。

- **failover group** *group_number*

システム実行スペースだけに適用できます。このコマンドは、アクティブ/アクティブ フェールオーバーをイネーブルにします。このコマンドを省略した場合は、アクティブ/スタンバイがイネーブルになります。

- **preempt** *delay*

システム実行スペースと failover group サブコマンドだけに適用できます。両方の装置が同時に起動するか、または指定の遅延内にプライマリが起動しない場合は、アクティブになるフェールオーバー グループが強制的に指定されます。

- **monitor-interface** *interface_name*

セキュリティ コンテキストだけに適用でき、重要なインターフェイスのヘルス モニタリングをイネーブルする場合に使用されます。このインターフェイスが「バウンス」されるか、または失敗した場合は、スイッチオーバーが発生することがあります。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド

ロールバック中にスイッチオーバーが発生し、2 つの装置が同期しなくなった場合は、次のコマンドを使用して復旧することが必要になることがあります。

- **failover active** *group_number*
- **failover reset** *group_number*
- **failover reload-standby**
- **clear configure failover**

これらのコマンドの詳細については、セキュリティ アプライアンスのコマンド リファレンスを参照してください。

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）

Deployment Manager を使用したデバイスへの設定のロールバック

設定をデバイスに展開し、その後新しい設定に何か問題があることが明らかになった場合は、そのデバイスの以前の設定に戻って展開できます。Configuration Archive に以前の設定がない場合は、以前の設定にロールバックできません。

設定は、ファイルではなくデバイスに展開された設定にだけロールバックできます。ファイルに展開された設定をロールバックする方法の詳細については、 ファイルへの展開時のロールバックの実行 （571 ページ）を参照してください。

また、Configuration Archive ツールを使用すると、デバイスからアーカイブされた設定にロールバックすることもできます。詳細については、ロールバックを使用したアーカイブ済み設定の展開 （569 ページ）を参照してください。

⚠

注意 設定をロールバックするのは、極端な状況にある場合だけとしてください。通常は、Security Manager で設定を修正し、修正された設定を展開するようにしてください。設定をロールバックすると、Security Manager に定義されている設定と、デバイスで実行中の設定が異なるという状況が発生します。ロールバックを実行したあとはデバイスのポリシーを再検出し、デバイスの設定と Security Manager に格納されている設定を一致させる必要があります。設定をロールバックするのは、極端な状況にある場合だけとしてください。処理を開始する前に、次のトピックを読んでください。

- 設定のロールバックについて （560 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （562 ページ）
- フェールオーバー デバイスのロールバックについて （562 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （563 ページ）
- IPS および IOS IPS のロールバックについて （564 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

はじめる前に

設定をロールバックする場合、そのアクションはアクティビティまたは設定セッションの一部としては実行されません。つまり、デバイスはロックされません。したがって、2 人のユーザがデバイスの設定を同時にロールバックできるため、予期しない問題が発生する可能性があります。設定をロールバックする前に、[Deployment Manager] ウィンドウにデバイスのアクティブな展開ジョブがないことを確認してください。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）
- Workflow 以外のモードでのジョブの状態 （485 ページ）
- Workflow モードでのジョブの状態 （487 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 展開ジョブ（[展開済み（Deployed）] 状態または [失敗（Failed）] 状態である必要があります）を選択し、[ロールバック（Rollback）] をクリックします。

[Rollback a Job] ダイアログボックスが開きます。ダイアログボックスには、ジョブに含まれているすべてのデバイスが表示されます。デバイスの名前、展開方法（ファイルまたはデバイス）、前回の展開の状態、デバイスを最後に更新した展開ジョブの名前なども表示されます。

ステップ 3 [Selection] 列のチェックボックスをオンにして、設定をロールバックするデバイスを選択します。デバイスへの展開を使用したデバイスだけを選択できます。デフォルトでは、[Succeeded] 状態のデバイスがすべて選択されます。

デバイスの行を強調表示し、[設定のプレビュー（Preview Config）] ボタンをクリックして、デバイスに展開する設定を表示できます。最後に展開された設定または現在実行中の設定と比較できます。詳細については、 設定のプレビュー （535 ページ）を参照してください。

ステップ 4 [OK] をクリックします。処理の確認が求められます。

ステップ 5 （任意）Security Manager に定義されている設定とデバイスで実行中の設定を一致させるには、デバイス ポリシーを再検出します（Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照）。

ロールバックを使用したアーカイブ済み設定の展開

Configuration Archive にある設定バージョンをその設定バージョンがアーカイブされているデバイスにロールバックできます。ただし、設定バージョンがデバイスに展開されたか、または設定がデバイスから作成された場合にかぎります。ロールバックされた設定は、そのデバイスのリストで別のアーカイブされたバージョンになります。ファイルに展開された設定をロールバックする方法の詳細については、 ファイルへの展開時のロールバックの実行 （571 ページ）を参照してください。

はじめる前に

ヒント　設定をロールバックする場合、そのアクションはアクティビティまたは設定セッションの一部としては実行されません。つまり、デバイスはロックされません。したがって、2人のユーザがデバイスの設定を同時にロールバックできるため、予期しない問題が発生する可能性があります。設定をロールバックする前に、Deployment Manager を参照して、デバイスのアクティブな展開ジョブがないことを確認してください（[管理（Manage）]> [展開（Deployments）] を選択）。

設定をロールバックするのは、極端な状況にある場合だけとしてください。設定をロールバックする前に、次のトピックを丁寧に読んでください。

- 設定のロールバックについて （560 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （562 ページ）
- フェールオーバー デバイスのロールバックについて （562 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （563 ページ）
- IPS および IOS IPS のロールバックについて （564 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）

関連項目

- Deployment Manager を使用したデバイスへの設定のロールバック （568 ページ）
- デバイスの設定バージョンの Configuration Archive への追加 （555 ページ）
- 展開の管理 （481 ページ）
- アーカイブされた設定バージョンの表示および比較 （555 ページ）

ステップ 1　**[管理（Manage）] > [Configuration Archive]** を選択して、Configuration Archive を開きます（[Configuration Archive] ウィンドウ （509 ページ）を参照）。

ステップ 2　デバイス セレクタで、別の設定バージョンにロールバックするデバイスを選択します。アーカイブされた設定が右側のペインに表示されます。

ステップ 3　ロールバックする設定バージョンを選択します。アーカイブされた設定がデバイスに展開されたものか、デバイスから作成されたものであれば、その設定にだけ展開をロールバックできます。ファイルに展開された設定にはロールバックできません。

ヒント　ロールバックの前に設定バージョンを表示するには、[表示（View）] をクリックします。

ステップ 4　選択した設定バージョンをデバイスに展開するには、[ロールバック（Rollback）] をクリックします。経過を表示するボックスが表示され、その後設定バージョンが正常に展開されると、通知メッセージが表示されます。

ステップ 5 （任意）Security Manager に定義されている設定とデバイスで実行中の設定を一致させるには、デバイス ポリシーを再検出します（Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照）。

ただし、通常はデバイスのポリシーを修正し、更新した設定を再展開する方が効率的です。これにより、変更内容およびデバイスの共有ポリシー設定が保持されます。このようにしないと、ポリシーを再検出した場合に、変更内容も共有ポリシー設定も削除されます。

ファイルへの展開時のロールバックの実行

デバイスではなくファイルに展開するときには、ロールバックを直接には実行できません。ファイルに展開しているときに、以前に保存した設定に戻すための手順は次のとおりです。

関連項目

- 設定のロールバックについて （560 ページ）
- マルチ コンテキスト モードのデバイスのロールバックについて （562 ページ）
- フェールオーバー デバイスのロールバックについて （562 ページ）
- Catalyst 6500/7600 デバイスのロールバックについて （563 ページ）
- IPS および IOS IPS のロールバックについて （564 ページ）
- ロールバック後、フェールオーバー設定ミスから復旧するためのコマンド （567 ページ）
- ロールバック後、競合を発生させる可能性があるコマンド （566 ページ）

ステップ 1 **[管理（Manage）] > [Configuration Archive]** を選択して、Configuration Archive を開きます（[Configuration Archive] ウィンドウ （509 ページ）を参照）。

ステップ 2 デバイス セレクタで、別の設定バージョンにロールバックするデバイスを選択します。アーカイブされた設定が右側のペインに表示されます。

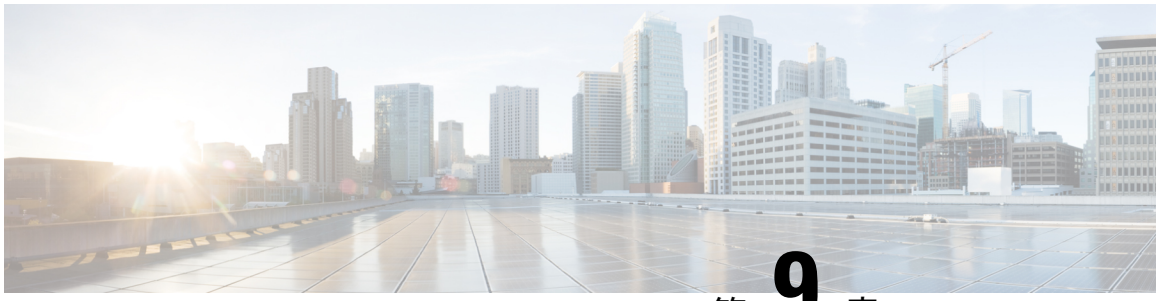
ステップ 3 ロールバックする設定バージョンを選択し、[表示（View）] をクリックします。

ステップ 4 [Configuration Version Viewer] ウィンドウで、[Config Type] を [Full] に設定します。

ステップ 5 左ペイン内をクリックし、Ctrl を押した状態で A を押し、続いて Ctrl を押した状態で C を押して、選択した設定を Windows クリップボードにコピーします。

ステップ 6 メモ帳などのテキスト エディタを開き、Ctrl を押した状態で V を押して、クリップボードの内容をテキスト ファイルに貼り付けます。

ステップ 7 ファイルを保存します。このファイルを使用して、手動でロールバックを実行できます。



第 9 章

デバイス通信および展開のトラブルシューティング

Security Manager がデバイスにログインする必要がある処理を行うときに、問題が発生する可能性が高くなります。このようなタイプの処理には、動作中デバイスを使用したポリシーの検出と展開や、デバイスから情報を取得する際の関連処理などがあります。

重要な点として、通信パスが Security Manager サーバからデバイスまでであること、つまり、Security Manager クライアントが動作しているワークステーションはデバイス通信に関連していないこと（サーバが同じマシン上にインストールされている場合を除きます）に注意してください。通信を正常に行うには、Security Manager サーバに、デバイスへのネットワーク パスと、デバイスに対して認証を行うための適切なクレデンシャルおよび証明書が必要です。

次の各項は、デバイス通信およびポリシー展開の一般的な問題のトラブルシューティングに役立ちます。

- デバイス接続のテスト （573 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- デバイス セレクタ内の赤い X マークの解決 （583 ページ）
- 展開のトラブルシューティング （584 ページ）

デバイス接続のテスト

Security Manager は、デバイスを管理するために、デバイスに接続してログインできる必要があります。この目的で Security Manager 内に定義したクレデンシャルおよびトランスポート方式を、Security Manager が使用できるかどうかをテストできます。

接続をテストできるのは、スタティック IP アドレスを持つデバイスだけです。トランスポート プロトコルとして Token Management Server（TMS）を使用するデバイスに対しては、接続をテストできません。

ネットワークまたはインベントリ ファイルからインベントリにデバイスを追加すると、Security Manager によって自動的に接続がテストされます。

デバイスの接続は、インベントリ内のデバイス、または手動で追加する新しいデバイスに対して、手動でテストできます。ここでは、すでにインベントリ内に存在するデバイスに対して接

続をテストする方法について説明します。デバイスを手動で追加する場合、[新規デバイス（New Device）] ウィザードの [デバイスのログイン情報（Device Credentials）] ページで [接続テスト（Test Connectivity）] をクリックして、次に示すテストを実行します。手動でのデバイスの追加方法については、 手動定義によるデバイスの追加 （116 ページ）を参照してください。

はじめる前に

Security Manager は、[Device Communication] ページの設定を使用して、接続タイムアウト、接続を再試行する頻度、トランスポートプロトコル、および使用するクレデンシャルを決定します。これらの設定を行うには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します。

関連項目

- デバイス ビューについて （87 ページ）
- デバイス プロパティの表示または変更 （136 ページ）
- [Device Communication] ページ （668 ページ）

ステップ 1 デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

ステップ 2 コンテンツテーブルから [ログイン情報（Credentials）] を選択します。

ステップ 3 [接続のテスト（Test Connectivity）] をクリックします。

[Device Connectivity Test] ダイアログボックスが開き、使用中のプロトコルなど、テストの経過が表示されます（[Device Connectivity Test] ダイアログボックス （575 ページ）を参照）。テストは実行中に中断できます。テストが完了したら、[詳細（Details）] をクリックして、次の情報を確認します。

- テストが成功した場合、 **show version** コマンドまたは **getVersion** コマンド（IPS センサーおよび Cisco IOS IPS センサーの場合）の出力が表示されます。テキストを選択し、Ctrl+C を押してテキストをクリップボードにコピーすると、あとで分析するために別のファイルに貼り付けることができます。
- テストが失敗した場合は、エラー情報が表示されます。次のような問題が一般的です。
  - ユーザ名またはパスワードが間違っている。
  - 間違ったプロトコルが選択されている。たとえば、選択されているプロトコルに応答するようにデバイスが設定されていない可能性があります。

- デバイスが接続を正しく受け入れるように設定されていない。サポートされているプロトコルが少なくとも 1 つ設定されていることを確認してください。
- デバイスに間違ったオペレーティング システムが指定されている（ASA デバイスに PIX を指定した場合など）。
- ACS 認証を使用していて、デバイスへの接続が完了している場合、Control 認可がなければ、Security Manager がバージョン情報の取得を試行するときにエラーが発生することがある。
- 一般的なネットワーク設定の問題が存在する。Security Manager の外部からデバイスへの接続をテストしてください。ハードウェアエラー、メディアエラー、ブーティングエラー、キューのオーバーフローを引き起こす超過トラフィック、デバイス上の重複する MAC または IP アドレス、物理的な不一致（リンク、デュプレックス、速度の不一致など）、または論理的な不一致（VLAN や VTP の不一致、ATM ネットワークの設定の誤りなど）がないかどうかを調べます。

[Device Connectivity Test] ダイアログボックス

[Device Connectivity Test] ダイアログボックスを使用して、Security Manager が設定済みのクレデンシャルを使用してデバイスに接続できるかどうかを確認します。

ナビゲーション パス

デバイス接続テストを開始するには、次のいずれかの領域の [ログイン情報（Credentials）] ページから [接続のテスト（Test Connectivity）] をクリックします。

- 手動でデバイスを追加するときの New Device ウィザード。 手動定義によるデバイスの追加 （116 ページ）を参照してください。
- [Device Properties]。このページを開くには、デバイスセレクタ内のデバイスをダブルクリックするか、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択します。

ネットワークからデバイスを追加するときの [ログイン情報（Credentials）] ページで [次へ（Next）] または [完了（Finish）] をクリックすると、接続テストが自動的に実行されます。

関連項目

- デバイス接続のテスト （573 ページ）
- [Device Credentials] ページ （143 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

フィールド リファレンス

表 115 : [Device Connectivity Test] ダイアログボックス

要素	説明
接続プロトコル（Connectivity Protocol）	デバイスへのログインに使用されているトランスポート プロトコル。Security Managerは、デバイスのデバイス プロパティで指定されているプロトコルを使用します。通常は、[Device Communications] ページ（[Device Communication] ページ （668 ページ）を参照）で設定されているデフォルト プロトコルです。
Connectivity Status	テストのステータスと、テスト開始後の経過時間が表示されます。
[Details] ボタン	このボタンをクリックすると、テスト結果の詳細情報が表示されます。 • [合格したテスト（Passed tests）]：**show version** コマンドの出力（PIX ファイアウォール、適応型セキュリティアプライアンス（ASA）、ファイアウォール サービス モジュール（FWSM）、Cisco IOS ルータ、および VPN サービスモジュール（VPNSM）の場合）または **getVersion** コマンドの出力（IPS センサーおよびCisco IOS IPS センサーの場合）の詳細が表示されます。コマンド出力をコピーして、分析のためにファイルに貼り付けることができます。 • [Failed tests]：詳細なエラー メッセージです。
[Abort] ボタン	完了前に接続テストを停止します。

デバイス通信設定および証明書の管理

デバイスインベントリおよびポリシーをデバイスから直接検出する場合、またはファイルではなくデバイスに設定を展開する場合は、デバイスで使用されるトランスポートプロトコルを使用するように Security Manager を設定する必要があります。一部のデバイス タイプは、1 つのトランスポートプロトコルしかサポートしていません。この場合、選択を行う必要はありません。使用するプロトコルを選択できるデバイスもあります（Cisco IOS ルータなど）。

Security Managerには、各デバイス タイプで最もよく使用されるプロトコルであるトランスポート プロトコルのデフォルト設定が用意されています。これらの設定を変更するには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します（[Device Communication] ページ （668 ページ）を参照）。

ほとんどのユーザの場合、管理が必要となる通信設定は、SSL（HTTPS）通信に使用される証明書と、SSH接続に使用される公開キーです。デバイスの証明書およびキーは更新できます。この場合、Security Manager で古いコピーが保持されます。

次の各項では、証明書およびキーの管理と、デバイス通信のトラブルシューティングの方法について説明します。

- SSL 証明書：[Device Communication] ページで、デバイスから取得した証明書で自動的に証明書を置換するように Security Manager を設定できます。SSL 証明書ストアを手動で管理する場合は、HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （578 ページ）を参照してください。次のトピックでは、証明書エラーに関する詳細を説明します。
  - デバイス検出時にセキュリティ証明書が拒否される （579 ページ）
  - デバイス検出中の無効な証明書のエラー （580 ページ）
  - IPS 証明書の管理 （2310 ページ）

ヒント Security Manager を使用して管理するすべての PIX ファイアウォールおよび適応型セキュリティ アプライアンスに、3DES/AES のライセンスがあることを確認してください。デバイスの通信要件について （71 ページ）を参照してください。

- SSH 公開キー：デフォルトでは、Security Manager により、公開キーが SSH 接続中に取得された新しい公開キーに置換されます。SSH 通信に関する問題が発生した場合は、SSH 接続の問題のトラブルシューティング （581 ページ）を参照してください。
- デバイス通信の一般的なトラブルシューティング：発生する可能性のあるその他の問題については、デバイス通信障害のトラブルシューティング （581 ページ）を参照してください。

複数証明書認証のサポート

バージョン 4.13 以降、Cisco Security Manager は、VPN 接続の複数証明書認証に関する ASA 9.7.1 の機能をサポートします。ASA のリリース 9.7.1 では、VPN クライアントのお客様に対する複数証明書認証のサポートが導入されました。その結果、クライアントは 2 つのクライアント証明書を使用してリモート VPN ユーザーを認証できるようになりました。2 つのクライアント証明書は、1 つのユーザー証明書と 1 つのマシン証明書の組み合わせ、または 2 つのユーザー証明書の組み合わせにすることができます。セキュリティを考慮して、2 つのマシン証明書による認証はサポートされていません。複数証明書認証は、SSL VPN と IPsec VPN の両方で機能します。

Cisco Security Manager 4.13 で複数証明書認証のサポートを有効にするには、AAA 認証方式を適切に指定し（[AAA] タブ（[Connection Profiles]） （1721 ページ）を参照）、DAP ポリシーを設定する必要があります（[DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）] （1881 ページ）を参照）。

HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加

（注） このトピックで説明されている方法に加えて、IPS デバイスでは IPS Certificates ユーティリティを使用して、Cisco Security Manager の証明書データストアにある証明書を管理できます。詳細については、IPS 証明書の管理 （2310 ページ）を参照してください。

IPS、PIX、ASA、または FWSM の各デバイスとの通信、あるいは Cisco IOS ルータとの通信にトランスポート プロトコルとして SSL（HTTPS）を使用する場合は、デバイスの追加時にデバイス認証証明書を自動的に取得するように Security Manager を設定できます（[Device Communication] ページ （668 ページ）を参照）。

ヒント HTTPS 通信を正常に行うには、適切な証明書が必要です。適切な証明書がないと、Security Manager はデバイスと通信できず、設定は展開されません。自己署名証明書を使用している場合は、Security Manager が間違った証明書を使用してデバイスにアクセスしようとすると、デバイスによって新しい証明書が作成されることがあります。このため、常にデバイスから証明書を取得するように Security Manager を設定しておくことを推奨します。

ネットワーク セキュリティのレベルを上げるために、証明書を自動取得するように Security Manager を設定せずに、手動で証明書を追加することもできます。[デバイス通信（Device Communication）]ページで、デバイスタイプのデバイス認証を [証明書を手動で追加（Manually add certificates）] として設定します。

デバイスの証明書を手動で更新するには、デバイスから証明書を取得する方法が最も簡単です。デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。[ログイン情報（Credentials）] をクリックして [ログイン情報（Credentials）] ページを開き、[認証証明書のサムプリント（Authentication Certificate Thumbprint）] フィールドの右側にある [デバイスから取得（Retrieve From Device）] をクリックします。Security Manager により証明書が取得され、ユーザは証明書を受け入れるように要求されます。設定の展開中に証明書の問題が発生した場合には、この操作を行う必要があることがあります（証明書を自分で入力してこのフィールドに貼り付けることもできます）。

また、Security Manager からデバイスにログインせずに、証明書のサムプリントを手動で入力またはコピー アンド ペーストすることもできます。手動で追加した証明書を必要とするようにデバイス タイプを設定した場合、そのデバイスの SSL 証明書サムプリントを手動で入力するには、次の手順を使用します。

ヒント Cisco Security Manager では、**[メガメニュー（Megamenu）] > [サーバー管理（Server Administration）] > [サーバー（Server）] > [セキュリティ（Security）] > [単一サーバー管理（Single Server Management）] > [証明書セットアップ（Certificate Setup）]** で 2048 ビットの自己署名証明書を生成できます。

ヒント [メガメニュー（Megamenu）]にアクセスするには、サーバーのデスクトップにある [Cisco Security Manager] アイコンをダブルクリックしてログオンします。[メガメニュー（Megamenu）]にアクセスする別の方法は次のとおりです。Windows > [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Security Manager] > [Cisco Security Manager] > [ログオン（log on）]。この 2 番目のナビゲーションパスは、Windows Server のインストール時の個人用設定の内容によって若干異なる場合があります。

はじめる前に

デバイスの証明書サムプリント（16 進ストリング）を取得します。

ヒント サムプリントをすぐに使用できない場合、ネットワークからデバイスを追加したときに表示されるエラーメッセージから、またはエクスポート ファイルから、サムプリントをコピーできます。

ステップ 1 **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択し、目次から [デバイス通信（Device Communication）] を選択して [デバイス通信（Device Communication）] ページを開きます（ [Device Communication] ページ （668 ページ）を参照）。

ステップ 2 [証明書の追加（Add Certificate）] をクリックして、[証明書の追加（Add Certificate）] ダイアログボックスを開きます（ [Add Certificate] ダイアログボックス （672 ページ）を参照）。

ステップ 3 デバイスの DNS ホスト名または IP アドレス、証明書サムプリントを 16 進形式で入力し、[OK] をクリックします。サムプリントが証明書ストアに追加されます。

ヒント 既存のサムプリントを消去するには、[Certificate Thumbprint] フィールドを空のままにしておきます。

デバイス検出時にセキュリティ証明書が拒否される

デバイスを検出しようとするとエラーが発生し、デバイスから取得したセキュリティ証明書が拒否されたことがエラーメッセージに示される場合、証明書を更新する必要があります。これには、次のいずれかの方法を使用できます。

- IPS デバイスの場合にのみ、**[管理（Manage）] > [IPS] > [IPS証明書（IPS Certificates）]** を選択して、証明書を同期します。また、証明書の再生成が必要になる場合があります。詳細については、 IPS 証明書の管理 （2310 ページ）を参照してください。
- 次のいずれかの操作を実行して、証明書に必要なサムプリントを手動で入力します。
  - **[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバイス通信（Device Communication）]** を選択します。[証明書の追加（Add Certificate）] をクリックし、デバイスの IP アドレスを入力してから、エラーメッセー

ジに表示されたサムプリントをコピーして [証明書サムプリント（Certificate Thumbprint）] フィールドに貼り付けます。

- デバイスを右クリックし、**[デバイスのプロパティ（Device Properties）] > [資格情報（Credentials）]** を選択します。エラー メッセージに表示されたサムプリントをコピーして、[Authentication Certificate Thumbprint] フィールドに貼り付けます。

[Add New Device] または [Add From Configuration File] オプションを使用して新しいデバイスを追加するとき、および再検出を実行するときは、サムプリントを手動で入力する必要があります。[Add New Device From Network] または [Add Device From File] オプションを使用して新しいデバイスを追加するときには、この操作は不要です。

- デバイスの追加時に証明書を自動的に取得するようにSSL証明書を設定します。IPS、ルータ、およびASA/PIX/FWSMデバイスには、それぞれ異なる設定を選択できます。これらの設定を行うには、**[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバイス通信（Device Communication）]** を選択し、[SSL証明書パラメータ（SSL Certificate Parameters）] グループを参照します。

関連項目

- HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （578 ページ）
- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイスを管理するための準備 （71 ページ）
- [Device Communication] ページ （668 ページ）
- [Device Credentials] ページ （143 ページ）

デバイス検出中の無効な証明書のエラー

デバイスと Security Manager の時刻設定が同期していない場合、（インベントリにデバイスを追加したり、インベントリ内にすでに存在するデバイス上のポリシーを再検出して）デバイス上のポリシーを検出しようとすると、証明書がまだ有効になっていないというエラー メッセージが表示されることがあります。

Security Manager サーバの設定時刻がデバイスの設定時刻よりも遅れている場合、有効期間の開始時刻が Security Manager の時刻設定よりも進んでいると、Security Manager はデバイス証明書を検証できません。設定されているタイム ゾーンがデバイスと Security Manager で同じであっても、夏時間（サマータイム）の設定が異なっていると、無効な証明書のエラーが発生します。この問題を解決するには、タイム ゾーンが同じであるかどうかにかかわらず、夏時間の時刻設定がデバイスと Security Manager で同じになっていることを確認します。夏時間の設定後に、デバイスのクロックを Security Manager と同期して、どちらにも同じ時刻が表示されるようにします。

最善の結果を得るために、デバイスと Security Manager で同じタイム ゾーンを設定し、証明書の検出後に、必要に応じてあとからタイム ゾーンを変更することを推奨します。

関連項目

- HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （578 ページ）
- IPS 証明書の管理 （2310 ページ）
- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイスを管理するための準備 （71 ページ）

SSH 接続の問題のトラブルシューティング

トランスポート プロトコルとして SSH を使用するデバイスの場合、Security Manager は、各デバイスで使用する適切な SSH バージョン（1.5 または 2）を自動的に検出します。SSH バージョン 2 の接続中、Security Manager は暗号化アルゴリズムまたは暗号をデバイスと自動的にネゴシエートします。また、キーが変更された場合、Security Manager はデバイスの SSH 公開キーを自動的に上書きします。このため、通常は SSH 接続の問題が発生することはありません。

実際に SSH 接続の問題が発生した場合は、次の修正策を考慮してください。

- デバイスの公開キーが変更され、キーの問題が原因で SSH 接続が失敗する場合は、Security Manager サーバ上の Program Files/CSCOpx/MDC/be/tmp/.shh/known_hosts ファイルからデバイスのキーを削除してから、操作を再試行します。
- Security Manager は、デフォルトの暗号化アルゴリズムとして Triple Data Encryption Standard（3DES; トリプルデータ暗号規格）を使用します。このアルゴリズムが使用中のデバイスに適していない場合は、デバイスの設定を変更するか、DCS.ssh.encipher プロパティで適切なアルゴリズムを指定するように Program Files/MDC/athena/config/DCS.properties ファイルを更新します（不明な点があれば、Cisco TAC にお問い合わせください）。このファイルを変更した場合は、Security Manager デーモン マネージャを再起動する必要があります。

関連項目

- デバイスを管理するための準備 （71 ページ）
- [Device Communication] ページ （668 ページ）
- [Device Credentials] ページ （143 ページ）

デバイス通信障害のトラブルシューティング

Security Manager がデバイスと通信できない場合（デバイスのログイン、検出、展開、その他の処理で失敗するなど）、次の領域を確認し、問題を特定して解決してください。

- デバイスが動作していることを確認します。
- どのトランスポート プロトコルが選択されているかを確認します。デバイスで受け入れるように設定されているプロトコルを選択する必要があります。ほとんどのデバイスの場合、プロトコルは [デバイスプロパティ（Device Properties）] の [全般（General）] ページ

（[ツール（Tools）] > [デバイスプロパティ（Device Properties）] > [全般（General）] を選択）で選択します。IPS デバイスの場合は、デバイス プロパティの [Credentials] ページで [IPS RDEP] モードが選択されています。

K8 または K9 暗号イメージを持たない IOS デバイスの場合は、プロトコルとして Telnet を選択する必要があります。

デバイスを追加する方法によっては、デフォルト以外のトランスポートプロトコルを選択することもできます。デバイスクラスに対してデフォルトのトランスポートプロトコルを設定するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communications）] を選択します。

- [Device Properties General] ページで、ホスト名、ドメイン名、および IP アドレスが正しいことを確認します。デバイスのホスト名、アカウント、およびクレデンシャルのポリシーによって、デバイスで設定される実際の名前およびクレデンシャルが定義されます。ただし、ポリシーはデバイス通信には使用されません。デバイス通信に使用しているクレデンシャルに影響を与えるポリシーを変更した場合は、デバイスプロパティも手動で更新する必要があります。
- Security Manager サーバから DNS 名を解決できることを確認します。サーバ上の DNS 設定を修正する必要があることもあります。
- Security Manager でデバイスのクレデンシャルを調べて、クレデンシャルが正しいこと、およびサーバとデバイスの間にルートが存在することを確認します。デバイスを右クリックし、[デバイスプロパティ（Device Properties）] を選択します。次に [クレデンシャル（Credentials）] タブを選択して、[テスト接続（Test Connectivity）] ボタンをクリックします。接続が失敗した場合は、エラーメッセージを確認して、接続の問題かクレデンシャルの問題かを判断します。必要に応じて、デバイスプロパティ内のクレデンシャルを更新します。

デバイスを追加する方法でクレデンシャルが必要とされる場合は、新しいデバイスを追加するときに、New Device ウィザードでクレデンシャルが定義されます。次の点を考慮してください。

- SSH 接続および Telnet 接続にはプライマリ クレデンシャルが使用される。
- HTTP 接続および SSL 接続には、HTTP/HTTPS クレデンシャルが使用されます。ただし、[プライマリクレデンシャルを使用（Use Primary Credentials）] を選択した場合は例外で、これらの接続にもプライマリクレデンシャルが使用されます。
- バージョン 4.11 以降、Security Manager は、MD5 アルゴリズムを使用するデバイス SSL 証明書をサポートしていません。デバイスの SSL が MD5 アルゴリズムを使用している場合、デバイスを Security Manager に追加しようとすると、Security Manager にエラーが表示されます。このエラーは、セキュリティの脆弱性を理由として、JRE がデフォルトで MD5 アルゴリズムを無効にするために発生します。これを解決するには、デバイスの SSL 証明書により高度な暗号化アルゴリズムを使用する必要があります。
- バージョン 4.19 以降、Cisco Security Manager は、DES アルゴリズムを使用したデバイス SSL 証明書をサポートしていません。デバイスの SSL が DES アルゴリズムを使用してい

る場合、デバイスを Security Manager に追加しようとすると、Security Manager にエラーが表示されます。このエラーは、セキュリティの脆弱性を理由として、JRE がデフォルトで DES アルゴリズムを無効にするために発生します。これを解決するには、デバイスの SSL 証明書により高度な暗号化アルゴリズムを使用するか、以下の手順に従う必要があります。

- Security Manager サーバーサービスを停止します。
- 必ず MDC\vms\jre\lib\security\java.security プロパティのバックアップを取ってください。
- プロパティで、「jdk.tls.disabledAlgorithms=SSLv3, DES, MD5withRSA, DH keySize <1024, \ EC keySize < 224, RC4_40, 3DES_EDE_CBC」を見つけ、リストから「DES」を削除します。
- Security Manager サーバーサービスを再度開始します。

関連項目

- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイスの通信要件について （71 ページ）
- デバイスを管理するための準備 （71 ページ）
- [Device Credentials] ページ （143 ページ）

デバイス セレクタ内の赤い X マークの解決

デバイス ビューのデバイス セレクタ内でデバイスに赤い X マークが付いている場合は、3.2.0 以前の Security Manager リリースからのアップグレード中に、そのデバイスに対する Auto Update Server（AUS）または Configuration Engine サーバの割り当てが失われたことを意味しています。AUS と Configuration Engine は、3.1.x からのアップグレード中に移行されません。アップグレード後に次の手順を使用して、これらによって管理されるデバイスを再び割り当てる必要があります。

ステップ 1 デバイス ビューで、次のいずれかを実行します。

- デバイスセレクタから、赤い X アイコンの付いたデバイスを右クリックし、[サーバー情報の更新（Update Server Info）] を選択します。
- デバイス選択ツリー内の赤い X アイコンをクリックします。アップグレード プロセス後に、AUS および Configuration Engine の情報が移行されなかったという警告メッセージが表示されます。[はい（Yes）] をクリックして、これらのサーバーを手動で追加します。

[Device Server Assignment] ダイアログボックスが開きます。

ステップ 2 [使用可能なデバイス（Available Devices）] リストから、同じ AUS または Configuration Engine サーバーを使用するすべてのデバイスを選択し、[>>] をクリックして選択済みリストに移動します。[Available Devices] リストには、赤い X マークの付いた AUS または Configuration Engine により管理されるすべてのデバイスが含まれます。

ステップ 3 [Server] リストから、選択されたデバイスを管理する AUS または Configuration Engine を選択します。目的のサーバが表示されていない場合は、[Server Properties] ダイアログボックス （132 ページ）を使用して、[+サーバーの追加...（+ Add Server...）] を選択して、インベントリにそのサーバーを追加します。

AUS または Configuration Engine サーバをインベントリに追加する方法については、 Auto Update Server または Configuration Engine の追加、編集、または削除 （130 ページ）を参照してください。

ステップ 4 赤い X マークの付いたデバイスがなくなるまで、このプロセスを繰り返します。

展開のトラブルシューティング

展開プロセスは、Security Manager の使用中に問題が発生する可能性が高い領域の 1 つです。展開には、展開ジョブの成否を決めるさまざまなプロセスが多数関連しています。

- Security Manager 自体。
- ネットワークの安定性と可用性（リモート管理されるデバイスへのリンクを含む）。
- Security Manager が展開しようとするコマンドに影響を与えるネットワーク デバイスで使用中のオペレーティング システム バージョン固有のバグ（Security Manager は、これらのバグの影響を受けます）。
- デバイスでイネーブルにしたライセンス。多くのセキュリティ コマンドでは、固有のデバイス ライセンスが必要となるためです。
- デバイスでサポートされている特定の機能。Security Manager が常に事前にこれらを判別できるとはかぎりません。たとえば、デバイスに特定の最小 RAM がある場合にかぎってこれらの機能がサポートされるプラットフォームもあれば、特定のインターフェイス カードに対してだけ使用可能なインターフェイス設定もあります。
- 中間アプリケーション（AUS、Configuration Engine、TMS サーバなど）の正常な動作。

展開が失敗する場合は、展開ステータス ウィンドウ内のメッセージをよく調べてください。さらに、次の各項で、発生する可能性のあるいくつかの問題について説明します。

- Security Manager のデバイス メッセージへの応答方法の変更 （585 ページ）
- ASA 8.3+ デバイスのメモリ違反展開エラー （587 ページ）
- 展開後に Security Manager がデバイスと通信できない （588 ページ）
- ルーティング プロセスを組み込む VPN の更新 （589 ページ）
- ルータ ポリシーおよび VPN ポリシーを使用した展開方式の混合 （589 ページ）
- ルータへの展開の失敗 （591 ページ）

• Catalyst スイッチおよびサービス モジュールへの展開の失敗 （592 ページ）
• AUS により管理されるデバイスへの展開が失敗する （595 ページ）
• Configuration Engine により管理されるデバイスのセットアップのトラブルシューティング （595 ページ）

Security Manager のデバイス メッセージへの応答方法の変更

Security Manager には、デバイス設定時に表示される可能性のある多くの応答メッセージに対する、組み込みの応答があります。Security Manager でエラーとして処理されるメッセージが、無視してよいメッセージ、または通知メッセージとして処理してよいメッセージであることがあります。エラーが無視されるように展開ジョブを設定することもできますが、プロパティ ファイルを使用して、特定のメッセージを別の方法で処理するように Security Manager を更新することもできます。

エラーが無視されるようにプロパティ ファイルを設定するだけでは必ずしも十分ではないことを理解してください。[エラー時のダウンロードを許可する（Allow Download on Error）] チェックボックス（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] ページにある）がデフォルトで選択されていないため、展開が失敗する可能性があります。次の表に、展開中にエラーが発生した場合、[エラー時のダウンロードを許可する（Allow Download on Error）] オプションが選択されている場合と選択されていない場合、および [変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] オプションが選択されている場合と選択されていない場合の Security Manager の動作について説明します。

表 *116 : PIX* ファイアウォール、*ASA*、および *Cisco IOS* ルータでの *SSL* および *SSH* に対する展開デバイス エラー処理

Allow Download on Error	エラー発生	警告表現を使用してエラーを無視	展開ステータス	メモリ書き込みの実行
オン	対応	×	失敗しました（Failed）	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。
オン	対応	対応	[成功 (Success)]	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。
オン	非対応	該当なし	[成功 (Success)]	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。

Allow Download on Error	エラー発生	警告表現を使用してエラーを無視	展開ステータス	メモリ書き込みの実行
オフ	対応	×	Failed（「Deploy not Completed」メッセージ）	番号
オフ	対応	対応	SSL（ASA、PIX、IOS デバイス）：Failed SSH（IOS デバイス）：Success	SSL：なし。 SSH（IOS デバイス）：[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。
オフ	非対応	該当なし	[成功 (Success)]	[変更をデバイスに永続的に保存する（Save Changes Permanently on Device）] が選択されているかどうかに基づく。

（注） SSL プロトコルを使用する Cisco IOS ルータでは、コマンド構文エラーでデバイスでの展開が停止されます。設定関連のエラーが発生しても、展開は停止されません。

Security Manager でのメッセージの処理方法を変更するには、インストール ディレクトリ（通常は c:\Program Files）の \CSCOpx\MDC\athena\config フォルダ内の DCS.properties ファイルを更新する必要があります。メモ帳などのテキストエディタを使用して、ファイルを更新します。

無視してよいメッセージを判断するには、次の手順を使用して、エラーの原因となった展開ジョブのトランスクリプトを調べるのが最も簡単です。

関連項目

- ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）

ステップ 1 [メイン（Main）] ツールバーで [展開マネージャ（Deployment Manager）] ボタンをクリックします。

[Deployment Manager] ウィンドウが表示されます。[展開ジョブ（Deployment Jobs）] タブがアクティブでない場合は、このタブをクリックします。

ステップ 2 エラー メッセージのあるジョブを選択します。

ステップ 3 [展開の詳細（Deployment Details）] タブの [トランスクリプト（Transcript）] ボタンをクリックして、トランスクリプトを開きます。

ステップ 4 無視してよいエラー テキストを特定します。

ステップ 5 DCS.properties ファイル内で適切な警告表現プロパティを見つけます。たとえば、PIX デバイスの場合、プロパティの名前は **dev.pix.warningExpressions** ですが、IOS デバイスの場合、プロパティの名前は **dev.ios.warningExpressions**です。

ヒント 逆に、プレフィックス Error が付かないデバイス応答をエラー メッセージとして表示することもできます。このためには、メッセージを [エラー表現（Error Expressions）] リスト（dev.pix.ErrorExpressions など）に追加します。

ステップ 6 エラーテキストを警告表現リストに追加します。警告メッセージは、汎用の正規表現ストリングにする必要があります。最後の表現を除いて、すべての表現を「$\」で区切る必要があります。たとえば、「Enter a public key as a hexadecimal number」というメッセージを無視する場合は、次の文字列を入力します。

.*Enter a public key as a hexadecimal number .*$

ステップ 7 CiscoWorks Daemon Manager を再起動します。

ASA 8.3+ デバイスのメモリ違反展開エラー

ASA ソフトウェア リリース 8.3+ では、旧バージョンの ASA ソフトウェアに比べ、必要なデバイス メモリが大幅に増加しています。最小メモリ要件を満たしていない ASA デバイスをアップグレードすると、アップグレードプロセスで問題が通知され、デバイスは、最小メモリ要件が満たされるまで syslog メッセージを定期的に送信します。

最小メモリ要件を満たしていない ASA デバイスは正常に動作できないため、インベントリへのデバイスの追加、およびインベントリからのポリシーの検出がユーザに許可されていても、Security Manager は設定をこれらのデバイスに展開しません。ただし、メモリを追加する前にポリシーをデバイスに展開しようとすると、デバイスが最小メモリ要件を満たしていないことを示す展開エラーが発生し、展開は失敗します。

エラーを解決する最善の方法は、メモリをデバイスに追加することです。ASA デバイスおよびメモリアップグレードの可能性の詳細については、https://www.cisco.com/c/ja_jp/products/security/asa-firepower-services/index.html を参照してください。

また、ASA ソフトウェア バージョンをダウングレードすることもできます。この場合は、インベントリからデバイスを削除してから再びインベントリに追加したあと、ポリシーを検出する必要があります。

未参照のオブジェクトを削除しようとしたときのエラー

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）] ページで [未参照のオブジェクトグループをデバイスから削除（Remove Unreferenced Object Groups from Device）] オプションを有効にすると、Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないオブジェクトを展開中に削除します。Security Manager によって検出または管理されていないポリシーがそのようなオブジェクトを使用している場合、Security Manager は展開中にそのオブジェクトを削除しようとします。このような場合、オブジェクトが使用されているためオブジェクトを削除

できなかったことを示すトランスクリプトエラーが表示されて、展開が失敗します。正常に展開するには、[未参照のオブジェクトグループのデバイスからの削除を無効化（disable the Remove Unreferenced Object Groups from Device）] オプションを無効にします。

展開後に Security Manager がデバイスと通信できない

Security Manager で設定可能な、デバイスへのアクセスを妨げるようなポリシーが数多くあります。これがセキュリティのポイントであり、望ましくないホストがネットワークやネットワーク デバイスに侵入できないようにします。

ただし、間違って Security Manager サーバがデバイスからロックアウトされてしまうと、Security Manager が設定をデバイスに展開できなくなったり、デバイスを管理できなくなることがあります。展開後に Security Manager がデバイスにアクセスできなくなっていることが判明した場合は、デバイスが動作中であること、またはデバイスが正常に機能していることを確認してから、次のポリシーをよく調べて、ポリシーがロックアウトの原因となっていないかどうかを確認します。

- **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] または [ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]**：これらのポリシーを使用する場合は、ルールが Security Manager サーバーからの管理トラフィックを許可する必要があります。少なくとも、HTTP、HTTPS、SSH、および Telnet を許可することを検討してください。Security Manager に対する必要なアクセスを定義する共有ポリシーを作成して、すべてのデバイスにそれを適用することを検討してください。これらのポリシー内にルールを作成した場合、明示的に許可されていないトラフィックはすべて拒否されるという暗黙のルールがポリシーの最後に追加されます。
- [NATポリシー（NAT policies）]：デバイス上で変換対象の元のアドレスとしてローカルアドレスを使用していないことを確認します。このアドレスを変換すると、Security Manager とデバイス間で送信される管理トラフィックが変換されて、中断されることがあります。
- [ルータ上のデバイスアクセスポリシー（Device Access policies on routers）]：デバイスへのデバイスアクセスポリシーの割り当てを解除して再展開したあと、Security Manager がデバイスとの接続を解除することがあります。デバイス アクセス ポリシーを使用して、デバイスにアクセスするためのイネーブルパスワードを定義できます。このポリシーの割り当てを解除して再展開すると、パスワードがデバイスから削除されます。この場合は通常、デバイスによってパスワードがデフォルトに戻されます。ただし、Security Manager に認識されない追加パスワード（ライン コンソール パスワードなど）がデバイスに含まれる場合もあります。この追加パスワードが存在する場合は、デフォルトパスワードではなくこのパスワードに戻されます。この場合、Security Manager はこのデバイスを設定できません。このため、デバイス アクセス ポリシーを使用してデバイス上にイネーブル パスワードやイネーブル シークレット パスワードを設定する場合は、ポリシーの割り当てを解除してから、次の展開までに新しいポリシーを割り当ててください。
- [サイト間VPN（Site-to-Site VPNs）]：VPN 内のスポークとの通信を失った場合、Security Manager サーバーがハブの保護対象ネットワーク内からスポーク上の外部インターフェイスと通信するときに、問題が発生する可能性があります。ハブデバイスを Security Manager

に追加するときは、ハブの保護対象ネットワークの外側にある管理 IP アドレスを定義することを推奨します。

- **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [許可ホスト（Allowed Hosts）]**：IPS デバイスの場合、[許可ホスト（Allowed Hosts）] ポリシーでは、センサーに接続できるホストを指定します。このポリシーには、Security Manager サーバを含める必要があります。

関連項目

- デバイス通信障害のトラブルシューティング （581 ページ）
- デバイス通信設定および証明書の管理 （576 ページ）
- IPS 証明書の管理 （2310 ページ）
- デバイスの通信要件について （71 ページ）

ルーティング プロセスを組み込む VPN の更新

問題：（Site-to-Site VPN Manager またはルーティングポリシーを使用して）VPN トポロジによって使用されているルーティングプロセスへの変更を定義および展開した場合、行った変更は、デバイスで設定されている CLI コマンドには反映されません。

解決策：ルーティングプロセスを組み込む VPN トポロジ（GRE 完全メッシュなど）を検出した場合、Security Manager は、Site-to-Site VPN Manager に GRE Modes ポリシーおよび関連するルーティングポリシーを移入します。ただし、Security Manager でこれらのポリシーの 1 つに対して行われた変更が他のポリシーに自動的に反映されることはないため、展開後に予期しない結果が起こることがあります。したがって、Site-to-Site VPN Manager で保護対象の IGP に変更を行った場合は、[プラットフォーム（Platform）] > [デバイスでのルーティング（Routing in Device）] ビューを選択してデバイスのルーティングポリシーに必要な変更を行ってください。同様に、ルーティング ポリシーを直接変更した場合も、Site-to-Site VPN Manager で必要な変更を行ってください。

関連項目

- サイト間 VPN の管理：基本 （1379 ページ）
- ルータの管理 （3001 ページ）
- ファイアウォール デバイスの管理 （2331 ページ）

ルータ ポリシーおよび VPN ポリシーを使用した展開方式の混合

ルータ プラットフォーム ポリシーおよび VPN ポリシーを、設定ファイルにすでに展開したあとで動作中のデバイスに展開すると、予期しない結果が発生することがあります。

この問題は、ルータ プラットフォーム ポリシーと VPN ポリシーを使用した展開方式（デバイスへの展開およびファイルへの展開）を混合して使用すると、発生することがあります。Security Manager では、これらのポリシー タイプに対する使用可能なすべての CLI コマンドが管理されるわけではないため、設定されたコマンドのスナップショットが維持され、他のすべてのコマンド（Security Manager でサポートされていないコマンドや、Security Manager で設定されていないポリシー内のサポート対象コマンドを含む）はデバイスでその状態のまま残ります。

展開が終わるたびに、Security Manager では、各デバイスに展開されたポリシーのスナップショットが作成されます。このスナップショットは、次の展開時に、デバイスに展開される設定変更リストを生成するために使用されます。デバイス 1 つにつき、一度に 1 つだけスナップショットが維持されます。

この例に示すように、ルータ プラットフォーム ポリシーと VPN ポリシーを使用した展開方式を混合すると、予期しない結果が発生することがあります。

1. 動作中のデバイスに対してルータ プラットフォーム ポリシー A を設定します。展開が完了すると、Security Manager によって、ポリシー A を持つそのデバイスのスナップショットが作成されます。
2. 次に、ポリシー A に置き換わるポリシー B を設定します。ただし、ポリシー B は、デバイスではなくファイルに展開します。この展開が完了すると、Security Manager によって、ポリシー A を持つ以前のスナップショットに置き換わるポリシー B を持つスナップショットが作成されます。ただし、ポリシー B をデバイスに展開していないため、ポリシー A を無効にするために必要な CLI コマンドは展開されていません。ポリシー A はデバイス上に展開されたままです。
3. 設定ファイル内の変更をデバイスにコピーせずに、再びデバイスに展開します。ポリシー A を持つスナップショットはもう存在しないため、Security Manager は、デバイスからポリシー A を無効にするために必要なコマンドを生成できません。

ポリシー A はルータ プラットフォーム ポリシーであるため、次のいずれの結果になる可能性があります。

- 最後の展開のポリシーによってポリシー A が上書きされる。
- デバイスで両方のポリシーが定義されることになる。
- 2 つのポリシーが共存できないため、展開が失敗する。

このため、動作中のデバイスでの作業中にファイルに展開する場合は、設定変更をファイルからデバイスにコピーしてから、デバイスへの追加の展開を実行することを強く推奨します。

関連項目

- サイト間 VPN の管理：基本 （1379 ページ）
- ルータの管理 （3001 ページ）

ルータへの展開の失敗

次に、設定を Cisco IOS ルータに展開するときに発生する可能性のある問題を示します。

インターフェイス設定の展開に失敗

問題：ルータへのインターフェイス設定の展開が失敗します。

解決策：Security Manager は、インターフェイスポリシーをサポートするための適切なタイプのインターフェイスカードまたは共有ポートアダプタ（SPA）がルータにインストールされているか、または適切なライセンスが設定されているかどうかを検証できません。インターフェイス ポリシーを変更せずにインターフェイス カードを追加または削除すると、展開エラーが発生することがあります。ベストプラクティスとして、Security Manager が適切なインターフェイス機能を検出できるように、インターフェイス モジュールまたは SPA を変更するたびに必ずルータからインベントリを検出することを推奨します。

レイヤ 2 インターフェイス定義の展開

問題：インターフェイスポリシーにレイヤ2インターフェイスの定義が含まれていると、展開に失敗します。

解決策：レイヤ2インターフェイスは、IP アドレスなどのレイヤ3インターフェイス定義をサポートしていません。レイヤ2インターフェイスにレイヤ3を定義していないことを確認してください。

VPN トラフィックが暗号化されずに送信される

問題：VPN を介して暗号化して送信する必要のあるトラフィックが、暗号化されずに送信されます。

解決策：VPN トラフィックに対して NAT を実行していないことを確認してください。VPN トラフィックに対してアドレス変換を実行すると、トラフィックが暗号化されなくなり、VPN トンネル経由で送信されなくなります。ダイナミック NAT ルールを定義する際は、IPSec に対して NAT を実行する場合でも、[Do Not Translate VPN Traffic] チェックボックスが選択されていることを確認してください（このオプションを設定しても、重複するネットワークから到着したアドレスの変換は行われます）。

このオプションは、サイト間 VPN に対してだけ使用できます。リモートアクセス VPN の場合は、VPN トラフィックを含むフローを明示的に拒否する ACL オブジェクトを作成し、この ACL を NAT ポリシー内にダイナミック ルールの一部として定義する必要があります。詳細については、[NAT] ページ - [Dynamic Rules] （1319 ページ）を参照してください。

ADSL または PVC ポリシーを展開できない

問題：ADSL または PVC ポリシーの展開が失敗します。

解決策：ポリシー定義で適切な ATM インターフェイス カード タイプを選択していることを確認してください。Security Manager は、適切なカード タイプが不明な場合、ポリシー定義を正しく検証できません。これにより、展開が失敗することがあります。

DHCP トラフィックが送信されない

問題：DHCP ポリシーをデバイスに展開した後も、DHCP トラフィックが送信されません。

解決策：デバイス上のアクセスルールによりブートストラッププロトコル（BootP）トラフィックがブロックされていないかどうかを確認してください。このようなルールが設定されていると、DHCP トラフィックは送信されません。

NAC がルータ上に実装されない

問題：NAC ポリシーがルータに展開されているにもかかわらず、ネットワーク アドミッション コントロールがルータ上に実装されません。

解決策：ルータ上のデフォルト ACL で、EAP over UDP トラフィックの NAC ポリシーで定義されているポートを経由する UDP トラフィックが許可されていることを確認してください。これは、NAC が Cisco Trust Agent（CTA）とネットワーク アクセス デバイス（NAD）の間の通信に使用するプロトコルです。CTA は、インストールされているエンドポイント デバイスのポスチャ クレデンシャルを提供する NAC クライアントであり、NAD は、検証のためにポスチャ クレデンシャルを AAA サーバに中継するデバイス（この場合はルータ）です。EAP over UDP トラフィックに使用されるデフォルト ポートは 21862 ですが、このポートは NAC ポリシーの一部として変更できます。デフォルト ACL により UDP トラフィックがブロックされている場合、EAP over UDP トラフィックも同様にブロックされるため、NAC は実装されません。

「Error Writing to Server」または「HTTP Response Code 500」メッセージとともに展開が失敗する

問題：Cisco IOS ルータへの展開が失敗し、「Error Writing to Server」または「Http Response Code 500」というエラーメッセージが表示されます。

解決策：SSL をトランスポートプロトコルとして使用して設定を Cisco IOS ルータに展開する場合、設定は複数の設定バルクに分割されます。この設定バルクのサイズは、プラットフォームによって異なります。Security Manager が、そのデバイスで設定されている SSL チャンクサイズを超える設定バルクを展開しようとすると、展開は失敗し、「Error Writing to Server」または「Http Response Code 500」というエラーメッセージが表示されます。

これを解決するには、次の手順を実行します。

1. Security Manager サーバで、インストール先ディレクトリ（通常は C:\Program Files）\CSCOpx\MDC\athena\config フォルダから DCS.properties ファイルを開きます。
2. **DCS.IOS.ssl.maxChunkSize=**<*value of the configuration bulk*> を見つけます。
3. 設定バルクの値を小さくします。
4. CiscoWorks Daemon Manager を再起動します。

Catalyst スイッチおよびサービス モジュールへの展開の失敗

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、拡張機能はサポートしていません。

次に、Catalyst スイッチおよび Catalyst 6500/7600 サービス モジュールに設定を展開するときに発生する可能性のある問題を示します。

インターフェイス設定の展開に失敗

問題：Catalyst 6500/7600 デバイスへのインターフェイス設定の展開が失敗します。

解決策：一部のインターフェイス設定（速度、デュプレックス、MTU 設定など）は特定のカードタイプに固有のものであり、展開の前に検証されません。展開が正常に行われるように、特定のカード タイプには適切な値を入力してください。

インターフェイス ポリシーの変更後に FWSM セキュリティ コンテキストの展開が失敗する

問題：セキュリティコンテキストとともに FWSM を追加し、そのポリシーを検出します。設定にはインターフェイス エイリアス（allocate interface コマンド）が含まれます。コンテキストのインターフェイス ポリシーを変更したあと、展開が失敗します。

解決策：FWSM に直接接続し、システム実行領域設定から、マッピングされているすべてのインターフェイス名を削除します。また、他のすべてのコンテキストで、マッピングされている名前へのインターフェイス参照を、インターフェイスの VLAN ID で置き換えます。これにより、Security Manager インベントリから FWSM を削除し、再検出できるようになります。

複数のコンテキストを持つ FWSM への展開が失敗する

問題：複数のセキュリティコンテキストを持つ FWSM に展開しようとすると、展開が失敗したり、FWSM のパフォーマンスが一時的に低下したりすることがあります。

解決策：問題は、Security Manager が設定を 1 つのデバイス上にある複数のセキュリティコンテキストに同時に展開しようとしている点です。設定変更によっては、これによりデバイスでエラーが発生して、展開が失敗することがあります。マルチ コンテキスト モードで FWSM を使用する場合は、Security Manager でマルチ コンテキストの FWSM に設定を展開する方法の変更 （594 ページ）の説明に従って、一度に 1 つずつコンテキストが設定され、設定がシリアルにデバイスに展開されるように、Security Manager を設定します。

内部 VLAN への展開の失敗

問題：Security Manager がデバイスの内部 VLAN リストの範囲に含まれる ID で VLAN を作成しようとすると、展開が失敗します。

解決策：Security Manager は内部 VLAN を検出できません。このため、デバイスの内部 VLAN リストの範囲外にある VLAN ID をユーザーが定義する必要があります。デバイスで **show vlan internal usage** コマンドを使用して、内部 VLAN のリストを表示します。

IDSM データ ポート VLAN の動作モードの変更時に展開が失敗する

問題：データポート VLAN の動作モードを [Trunk（トランク）]（IPS）から [Capture（キャプチャ）]（IDS）に変更しようとすると、展開が失敗し、次のエラーメッセージが表示されます。

Command Rejected: Remove trunk allowed vlan configuration from data port 2 before configuring capture allowed-vlans

解決策：一部のソフトウェアリリース（12.2(18)SFX4 など）には、正常な変更を妨げるバグがあります。この問題を解決するには、デバイスをリロードしてください。

多数の ACL が含まれる FWSM 設定で展開が失敗する

問題：設定に多数の ACL が含まれている場合、FWSM デバイスへの展開が失敗します。

解決策：これは、ACL コンパイル中に CPU 使用率が高くなったために発生する可能性があります。これを解決するには、次の手順を実行して、CPU 使用率のしきい値制限を再設定します。

1. Security Manager サーバで、インストール先ディレクトリ（通常は C:\Program Files）\CSCOpx\MDC\athena\config フォルダから DCS.properties ファイルを開きます。
2. **DCS.FWSM.checkThreshold=False** プロパティを見つけます。
3. 値を true に変更します（**DCS.FWSM.checkThreshold=True**）。
4. CiscoWorks Daemon Manager を再起動します。
5. 設定を再びデバイスに展開します。

値を true に設定したあと、検出および展開によって CPU 使用率が確認されます。CPU 使用率が DCS.FWSM.minThresholdLimit プロパティ内に設定されている値の範囲を超えていると、エラー メッセージが生成されます。デフォルト値は 85 です。

Security Manager でマルチ コンテキストの FWSM に設定を展開する方法の変更

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、拡張機能はサポートしていません。

FWSM で複数のセキュリティ コンテキストをホストするために、マルチ コンテキスト モードで動作するように Firewall Services Module（FWSM; ファイアウォール サービス モジュール）を設定した場合は、設定がシリアルに FWSM に展開されるように Security Manager を設定する必要があります。FWSM には、複数のコンテキストが同時に更新された場合に正常な展開を妨げる可能性のある、いくつかの制限があります。このため、シリアル展開を使用しない場合、展開が失敗することがあります。また、シリアル展開を使用しないと、展開中の FWSM のパフォーマンスが低下することもあります。

Security Manager でマルチ コンテキストの FWSM に設定を展開する方法を変更するには、DCS.properties ファイルを更新する必要があります。個々のセキュリティ コンテキストを追加するのではなく、FWSM 管理コンテキストを使用して FWSM コンテキストをインベントリに追加する必要があります。

次に、FWSM 展開をシリアルに行うためのエンドツーエンド プロセスについて説明します。

ステップ 1 通常は、管理コンテキストの管理 IP アドレスを使用して FWSM セキュリティ コンテキストを追加してください。コンテキストの管理は、管理コンテキストを介して行います。

各コンテキストの管理 IP アドレスを使用して FWSM のセキュリティコンテキストを個別に追加することも可能ですが、Security Manager は、個別に追加されたこれらのコンテキストを、同じ物理デバイス上でホ

スティングされるコンテキストとして認識できません。この場合、Security Manager ではコンテキストへのシリアル展開を実行できません。

セキュリティ コンテキスト管理 IP を使用して追加した FWSM セキュリティ コンテキストがある場合は、インベントリからコンテキストおよびFWSMを削除してから、管理コンテキストを使用してそれらを追加します（すべてのポリシーを検出します）。デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。

ヒント これらのコンテキストに対する未展開の変更を保持する必要がある場合、まず変更を展開して、デバイスの設定が完了していることを確認します。コンテキスト展開は、一度に 1 つずつ行ってください。

ステップ 2 Security Manager サーバーで Windows にログインし、インストールディレクトリ（通常は c:\Program Files）の \CSCOpx\MDC\athena\config フォルダ内の **DCS.properties** ファイルを編集します。メモ帳などのテキスト エディタを使用して、ファイルを更新します。

ステップ 3 DCS.properties ファイル内の DCS.doSerialAccessForFWSMVCs プロパティを見つけて、true に設定します。

DCS.doSerialAccessForFWSMVCs=true

ステップ 4 CiscoWorks Daemon Manager を再起動します。

AUS により管理されるデバイスへの展開が失敗する

Auto Update Server（AUS）を起動してから、完全に動作可能になる前に展開を実行すると、AUS により管理される複数のデバイスに展開するとき、展開が失敗することがあります。次の操作の実行後は、AUS が起動するまでに時間がかかります。

- 新規インストールまたはアップグレード
- 手動による再起動（停電後など）
- 手動による Cisco Security Manager Daemon Manager サービスの再起動

AUS が完全に動作可能になったかどうかを確認するには、Windows サービスのステータスを確認します。このためには、**[スタート（Start）] > [コントロールパネル（Control Panel）] > [管理サービス（Administrative Services）] > [サービス（Services）]** を選択してから、CiscoWorks AUS Database Engine サービスのステータスを確認します。このサービスがすでに開始されていれば、展開を再試行してください。

Configuration Engine により管理されるデバイスのセットアップのトラブルシューティング

次の質問と回答で、Cisco Configuration Engine（CNS）により管理されるデバイスのセットアップ時に発生する可能性のある問題と、その解決方法について説明します。

質問：Configuration Engine の展開が失敗するのはなぜですか。

回答：Configuration Engine のすべてのバージョンが互換性をもって機能するわけではありません。Configuration Engine をデバイス インベントリに追加するとき、Security Manager では Configuration Engine 上で動作しているソフトウェア バージョンを確認できないため、サポートされていないバージョンをユーザがインベントリに追加してしまう可能性があります。この場合、展開しようとすると、予期しないエラーが発生することがあります。サポートされている Configuration Engine バージョンを実行していることを確認してください（バージョン情報については、http://www.cisco.com/en/US/products/ps6498/prod_release_notes_list.html にあるこのバージョンの Security Manager のリリースノートを参照してください）。

質問：Configuration Engine の Web ページで IOS デバイスをクリックすると、InvalidParameterException が発生するのはなぜですか。

回答：これは想定された動作です。IOS デバイスの場合、Security Manager は展開ジョブを使用して、設定を Configuration Engine の IOS デバイスに関連付けるのではなく、設定を Configuration Engine に展開します。このため、Configuration Engine の Web ページでデバイス名をクリックしても、関連付けられた設定は表示されません。ASA/PIX デバイスの場合、Security Manager は設定を Configuration Engine のデバイスに関連付けます。このため、デバイス名をクリックすると、関連付けられた設定が表示されます。

質問：「com.cisco.netmgmt.ce.websvc.exec.ExecServiceException: [002-01003]]deviceName does not exists?」というエラーが発生するのはなぜですか。

回答：このエラーは、デバイスがまだ Configuration Engine に追加されていないことを示します。Security Manager でロールバックも展開も（いずれもデバイスが自動的に追加されます）実行しておらず、手動でも Configuration Engine にデバイスを追加していない場合、このエラーが表示されます。

質問：「com.cisco.netmgmt.ce.websvc.config.ConfigServiceException: [002-01003]]Device device id is not connected」というエラーが発生するのはなぜですか。

回答：回答は、実行しているセットアップのタイプによって異なります。

- イベントモードセットアップ：Security Manager の [デバイスのプロパティ（Device Properties）] ウィンドウで定義されている Configuration Engine デバイス ID が、ルータで設定されているデバイス ID と一致していることを確認してください（**cns id string** コマンドを使用）。
- Call Home モード セットアップ：このモードでは、デバイスは Configuration Engine に接続されません。このため、Configuration Engine を使用してデバイス設定を取得することが必要となる Security Manager 操作はいずれもサポートされません。これには、検出、プレビュー設定、表示実行設定、および接続テスト（IOS デバイスの場合はロールバックも）が含まれます。

質問：Configuration Engine により管理される ASA/PIX デバイスへの展開が正常に行われないのはなぜですか。

回答：いくつかの原因が考えられます。

- 設定に無効なコマンドが含まれている。このことをテストするには、Configuration Engine で ASA/PIX デバイスに関連付けられている設定をコピーして、デバイスに直接貼り付けます。

- **auto-update server** コマンドに無効なユーザー名およびパスワードが含まれている。
- 設定を ASA/PIX デバイスにポーリングするための待機時間が足りなかった。次回のポーリングサイクルがいつ開始されるかを確認するには、**show auto** コマンドを使用します。
- 以前に同じ ASA/PIX デバイスに対して Configuration Engine サーバを使用していて、現在の作業を開始する前に Configuration Engine サーバからそのデバイスを削除しなかった場合、新しい設定をユーザがデバイスに展開する前に、デバイスがサーバから以前の設定を取得した可能性があります。
- 上記のいずれによっても問題が解決しない場合は、ASA/PIX デバイスで Configuration Engine デバッグ モードを有効にし、次のポーリング サイクル終了後にログでエラーを確認します。

質問：Configuration Engine により管理される ASA/PIX デバイスへの展開が最初は成功したのに、2 回め以降は成功しないのはなぜですか。

回答：最初の展開でプッシュされた設定に自動更新機能に対する不適切な CLI コマンドが含まれていた場合、このようなエラーが発生することがあります。次の点をチェックします。

- **auto-update** コマンドで Configuration Engine サーバーのユーザー名およびパスワードが適切に定義されてることを確認します。
- デバイス CLI を使用して自動更新サーバーを設定する際に **name** コマンドを使用した場合、必要な **name** コマンドを含む FlexConfig を定義したことを確認します。このコマンドは Security Manager で直接サポートされていないため、FlexConfig が必要となります。このため、このコマンドが検出されても、完全な設定には表示されません。Security Manager を使用して AUS ポリシーを設定する場合は、**name** コマンドは必要ありません。

質問：ASA/PIX デバイスで Configuration Engine をデバッグするにはどうすればよいですか。

回答：次の CLI コマンドを入力します。

```
logging monitor debug
terminal monitor
logging on
```

Configuration Engine サーバ上の PIX ログで関連情報を確認することもできます。

質問：IOS デバイスで Configuration Engine をデバッグするにはどうすればよいですか。

回答：次の CLI コマンドを入力します。

```
debug cns all
debug kron exec-cli
terminal monitor
```

イベント モードの場合は、Configuration Engine サーバ上のイベント ログで関連情報を確認することもできます。Call Home モードの場合は、Configuration Engine サーバ上の config server ログを確認してください。

質問：Configuration Engine を介した IOS デバイスの検出およびその設定の取得に失敗したのはなぜですか。

回答：デバッグモードで、次のエラーが表示されているかどうかを確認します。

*Feb 23 21:42:15.677: CNS exec decode: Unknown hostname cnsServer-lnx.cisco.com ... 474F6860: 72726F72 2D6D6573 73616765 3E584D4C error-message>XML 474F6870: 5F504152 53455F45 52524F52 3C2F6572 _PARSE_ERROR

次のことを確認してください。

- CNS コマンドで完全修飾ホスト名（ホスト名およびドメイン名）が使用されている。
- デバイスに **ip domain name** コマンドが含まれている。
- デバイスに、**ip host** コマンドと、Configuration Engine の完全修飾ホスト名およびその IP アドレスが含まれている。

質問：イベントモードルータが Configuration Engine の [デバイスの検出（Discover Device）] ページに表示されない、または Configuration Engine の Web ページに緑色で表示されるのはなぜですか。

回答：次のことを確認してください。

- ルータと Configuration Engine サーバで相互に ping が実行できることを確認します。
- 次のいずれかのコマンドを使用して、Configuration Engine サーバでイベント ゲートウェイが動作していることを確認します。

プレーンテキストモードのステータス：**/etc/init.d/EvtGateway**

SSL 暗号化モードのステータス：**/etc/init.d/EvtGatewayCrypto**

- **cns event** コマンドをクリアしてから、ポート番号を指定せずにコマンドを再入力します。

第 10 章

Cisco Security Manager サーバーの管理

ここでは、Security Manager 製品の一般的な操作に関連するシステム管理作業について説明します。

- Security Manager サーバの管理および運用の概要 （599 ページ）
- Security Manager サーバのクラスタの管理 （600 ページ）
- Security Manager のライセンス ファイルのインストール （618 ページ）
- 証明書信頼管理 （620 ページ）
- 監査レポートの使用 （622 ページ）
- 別のユーザの作業の引き継ぎ （628 ページ）
- 管理ユーザまたは他のユーザのパスワード変更 （628 ページ）
- Security Manager データベースのバックアップおよび復元 （629 ページ）
- Cisco Technical Assistance Center 用データの生成 （633 ページ）

Security Manager サーバの管理および運用の概要

Cisco Security Manager は、ソフトウェア アプリケーションの 1 つとして、CiscoWorks Common Services アプリケーションにより提供されるフレームワークで動作します。基本的なサーバ制御機能の多くは、Common Services によって提供されます。たとえば、Security Manager に複数サーバ セットアップを作成するには、Common Services でそのセットアップを作成する必要があります。また、Common Services には、ローカル ユーザ アカウントの作成と管理、データベースのバックアップと復元、システム機能に関する各種レポートの生成を行うためのツールや、その他多くの基本的な機能に対応するツールも備わっています。

Common Services アプリケーションにアクセスするには、次のいずれかを実行します。

- Security Manager クライアントが現在開いている場合は、**[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）]** を選択し、コンテンツテーブルから [サーバーセキュリティ（Server Security）] を選択します。[Server Security] ページには、Common Services の特定のページにリンクするボタンおよび特定のページを開くボタンが含まれています。任意のボタンをクリックして、Common Services の目的のページにナビゲートできます。

- Web ブラウザを使用し、URL https://*servername* を使用して Security Manager サーバーにリンクします（*servername* はサーバーの IP アドレスまたは DNS 名です）。この URL によって Security Manager ホームページが開きます。[サーバー管理（Server Administration）] または [CiscoWorks] リンクをクリックして、Common Services を開きます。

（注） Windows Server 2012（Standard または Datacenter）64 ビットで Internet Explorer 10.x を使用している場合は、特別な考慮事項が適用されます。これは、Cisco Security Manager のバージョン 4.7 で新たにサポートされます。次のナビゲーション パスを使用する場合は、この考慮事項に注意する必要があります。Windows の [スタート] > [Cisco Security Manager クライアント（Cisco Security Manager Client）] >（ログイン）> [Configuration Manager] > [ツール（Tools）] > [Security Manager管理...（Security Manager Administration...）] > [サーバーセキュリティ（Server Security）]。[サーバーセキュリティ（Server Security）] ページは通常どおり開きますが、そのページではボタン（[ローカルユーザセットアップ（Local User Setup）] など）を使用して、Common Services 内でサーバーセキュリティツールを相互起動することはできません。この問題を回避するには、Internet Explorer 10.x のイントラネット設定のセキュリティレベルを下げます。

Common Services で実行可能な操作の詳細については、Common Services オンライン ヘルプを参照してください。

（注） Common Services の **[ソフトウェアセンター（Software Center）] > [ソフトウェアの更新（Software Update）]** 機能は、Cisco Security Manager ではサポートされていません。

Security Manager サーバのクラスタの管理

Security Manager サーバ クラスタは、ネットワークを管理するために使用される 2 つ以上の Security Manager サーバです。一般的に、そのサーバ間の関係は維持することが求められます。クラスタ内のサーバー間に体系的な関係はありませんが、クラスタのような関係を維持するために使用できるいくつかのテクニックがあります。この章の各項では、Security Manager サーバのグループをクラスタとして管理する方法を説明します。

ここでは、次の内容について説明します。

- Security Manager サーバ クラスタの管理 （601 ページ）
- デバイス インベントリのエクスポート （605 ページ）
- 共有ポリシーのエクスポート （612 ページ）
- ポリシーまたはデバイスのインポート （615 ページ）

Security Manager サーバ クラスタの管理

単一の Cisco Security Manager サーバーで多数のデバイスを管理できます。また一方で、ネットワークの管理に 2 つ以上の Security Manager サーバを使用する理由はさまざまです。次に例を示します。

- 管理対象のデバイスが非常に多い、大規模なネットワークの場合、単一のサーバからすべてのデバイスを管理しようとすると、パフォーマンスが許容できなくなる可能性があります。
- 地理的な理由から、管理対象デバイスにより近いサーバを用意した方が改善されると判断する場合。たとえば、世界各地に主要サイトがある場合は、各主要サイトに分けてサーバを置くと、管理を簡易化し、パフォーマンスを向上できます。また、管理対象デバイスに設定を展開する場合を例にすると、バンガロールにあるデバイスへの設定の展開は、サンフランシスコにある Security Manager サーバよりも、バンガロールにある Security Manager サーバの方がはるかに速く展開することができます。単純に物理的なネットワークの距離がとても近いためです。
- 管理されたテクノロジーに基づいて、デバイス管理をセグメント化する場合。たとえば、1 台のサーバでサイト間 VPN を管理し、もう 1 台のサーバで ASA ファイアウォールとリモート アクセス VPN ポリシーを管理し、さらに 3 台目のサーバで IPS を管理する場合があります。
- 分かれた複数の IT 組織がネットワークのそれぞれ別の部分を管理している場合。デバイス レベルでアクセス コントロールを微調整するように ACS を設定できますが、それよりも IT 組織ごとに別個の Security Manager サーバを用意する方が簡易化できます。

2 つ以上の Security Manager サーバをインストールする場合の主な課題は次のとおりです。

- 単一のサーバを 2 つ以上のサーバに分ける：現在、単一の Security Manager サーバを使用していて、複数のサーバの必要性がある場合。1 つの Security Manager サーバを 2 つ以上のサーバに分ける方法については、Security Manager サーバの分割 （601 ページ）を参照してください。
- 同一セットの共有ポリシーの維持：複数のサーバを使用して同じデバイス タイプを管理する場合は、デバイスに割り当てる共有ポリシーを同一に保つことができます。たとえば、同一セットの必須およびデフォルトのアクセス ルールをすべての ASA デバイスで継承させることができます。

同じ共有ポリシーのセットをサーバのクラスタ内で自動的に管理するプロセスは存在しません。代わりに、手動でメイン サーバからポリシーをエクスポートし、その他のサーバにインポートする必要があります。詳細については、Cisco Security Manager サーバー間での共有ポリシーの同期 （603 ページ）を参照してください。

Security Manager サーバの分割

単一の Security Manager サーバを 2 つ以上のサーバに切り替える必要がある場合は、元のサーバで管理しているデバイスのサブセットを新しいサーバに移動することによって、サーバを分

けることができます。特定の 1 つのネットワーク デバイスは単一の Security Manager サーバから管理する必要があるため、移動したデバイスを元のサーバから削除することに留意してください。

ヒント　すべてのサーバーで同じリリースの Security Manager ソフトウェアを使用します。

関連項目

- Security Manager サーバ クラスタの管理 （601 ページ）
- Cisco Security Manager サーバー間での共有ポリシーの同期 （603 ページ）
- 共有ポリシーのエクスポート （612 ページ）

ステップ 1　『Installation Guide for Cisco Security Manager』の説明に従って、新しい Security Manager サーバーをインストールします。

サーバが正しく機能していること、またサーバに移動しようとしているデバイスに対して十分なデバイス数でライセンスをインストールしたことを確認します。Professional ライセンスを必要とするデバイス タイプを管理する場合は、必ずそのライセンスを使用します。ライセンスのインストールの詳細については、Security Manager のライセンス ファイルのインストール （618 ページ）を参照してください。

ステップ 2　元のサーバ上の移動対象デバイスのポリシーで、新しいサーバの IP アドレスからのアクセスが許可されていることを確認します。たとえば、ASA およびルータ上のアクセス ルール、および IPS デバイス上の Allowed Hosts ポリシーを検討します。

ステップ 3　元のサーバで、移動しているデバイスに対するすべての設定変更が送信済みおよび展開済みであることを確認します。スタッフにその変更を送信して展開するように依頼する必要があります。Security Manager 内でこのステータスを確認する簡単な方法はありません。

この手順では、保留中で未確定の変更がないことを確認します。構成の展開については、Workflow モードに基づいた次のトピックを参照してください。

- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）

ステップ 4　**[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** を選択して、元の Security Manager サーバーから割り当てられたポリシーとポリシーオブジェクトを持つデバイスをエクスポートします。デバイスのエクスポート時に [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）] を選択して、ポリシー情報が含まれるようにします。ファイルタイプは **dev** にする必要があります。詳細については、Security Manager クライアントからのデバイス インベントリのエクスポート （605 ページ）を参照してください。

新規 Security Manager サーバごとに独自のデバイスを含む個別のエクスポート ファイルを作成します。

ヒント　この時点では、元のサーバ内のエクスポートされたデバイスに対してポリシーの変更を行わないでください。また、これらのデバイスに設定を展開しないでください。分割を行う前に元のサーバのデバイスに変更を行う必要性が見つかった場合は、新しいエクスポート ファイルを作成します。

ステップ 5　新しい Security Manager サーバーそれぞれで、**[ファイル（File）] > [インポート（Import）]** を選択して、エクスポートされた情報を新しいサーバーにインポートします。詳細については、ポリシーまたはデバイスのインポート （615 ページ）を参照してください。

ヒント　インポート時にデバイスグループは維持されません。すべてのデバイスが、All グループに配置されます。手動で目的のデバイス グループ構成を再作成し、デバイスを適切なグループに追加する必要があります。

ステップ 6　新しい Security Manager サーバごとに新しくインポートされたデバイスを管理できることを確認します。たとえば、変更されていないデバイスに対しても展開を実行して、新しいサーバーがすべてのデバイスに正常に接続して設定を展開できるようにすることができます。

ヒント　ポリシーまたはデバイスのインポート （615 ページ）で説明されているように、デバイスを設定するための変更が適用される前に、ポリシーを送信する必要があります。展開を行う前にポリシーを送信します。

ステップ 7　元のサーバを使用して、移動対象デバイスのいずれかをモニタしていた場合（つまり、Event Viewer およびオプションの Report Manager を使用していた場合）、新しいサーバに syslog メッセージが送信されるように、また新しいサーバからの接続を許可するように関連ポリシーを更新します。元のサーバのイベントデータまたはレポート データはいずれも、新しいサーバには転送されません。

Security Manager のモニタをイネーブルにするようにデバイスを設定する方法については、次の項を参照してください。

- イベント管理のための ASA と FWSM デバイスの設定 （3506 ページ）
- イベント管理のための IPS デバイスの設定 （3508 ページ）

ステップ 8　元の Security Manager サーバで、**[ファイル（File）] > [デバイスの削除（Delete Devices）]** を選択して、移動したデバイスを元のサーバーから削除します。デバイスの削除の詳細については、Security Manager インベントリからのデバイスの削除 （162 ページ）を参照してください。

Cisco Security Manager サーバー間での共有ポリシーの同期

複数の Security Manager サーバーがある場合、サーバー間で共有ポリシーを手動で同期できます。共有ポリシーを同期すると、これらの共有ポリシーで使用されるポリシーオブジェクトも同期されます。

ヒント

- 単一の Security Manager サーバーを「プライマリ」サーバー（正式なバージョンの共有ポリシーを含むサーバー）として識別するプログラムを使用した方法はありません。どのサーバーをプライマリとして使用するか決め、そのサーバーだけで共有ポリシーを編集することを定める必要があります。

- すべてのサーバーで同じリリースの Security Manager ソフトウェアを使用します。
- 特定のタイプのポリシーオブジェクトは、それらのオブジェクトが共有ポリシーで使用されていない場合でも、サーバー間で同期できます。同期するネットワーク/ホスト、サービス、またはポート リスト オブジェクトがある場合は、ポリシー オブジェクトのインポートおよびエクスポート （318 ページ）に説明されているコマンドを使用できます。
- 共有ポリシーおよびポリシーオブジェクトのインポート時には、常に同じ名前の既存の共有ポリシーまたはポリシーオブジェクトがインポートされた情報によって置換されます。そのため、ポリシーとオブジェクトをインポートするサーバー上でユーザーが独自の共有ポリシーとオブジェクトを作成できるようにする場合は、ポリシーとオブジェクトの命名規則を作成して、新しくインポートされたポリシーとオブジェクトによってユーザーポリシーとオブジェクトが誤って上書きされないようにすることが重要です。

関連項目

- Security Manager サーバ クラスタの管理 （601 ページ）
- Security Manager サーバの分割 （601 ページ）
- Security Manager クライアントからのデバイス インベントリのエクスポート （605 ページ）

ステップ 1 元のサーバで、共有ポリシーおよびポリシー オブジェクトに対するすべての設定変更が送信済みであることを確認します。スタッフにその変更を送信して承認が行われるように依頼する必要があります。Security Manager 内でこのステータスを確認する簡単な方法はありません。

共有ポリシーをエクスポートする場合、新しい変更がポリシーに割り当てられたデバイスに展開されていることを確認する必要はありません。デバイスの割り当てと展開のステータスは、エクスポートされた情報には含まれません。

ステップ 2 [ファイル（File）] > [エクスポート（Export）] > [ポリシー（Policies）] を選択して、共有ポリシーと共有ポリシーで使用されるポリシーオブジェクトをエクスポートします。エクスポート処理では、拡張子 **pol** を持つファイルが作成されます。

ヒント エクスポートするポリシーは選択できません。選択できるのはポリシータイプだけです。選択したタイプのすべての共有ポリシーがエクスポートされます。

詳細については、共有ポリシーのエクスポート （612 ページ）を参照してください。

ステップ 3 他の Security Manager サーバーのそれぞれで、[ファイル（File）] > [インポート（Import）] を選択して、エクスポートされた共有ポリシー情報をサーバーにインポートします。詳細については、ポリシーまたはデバイスのインポート （615 ページ）を参照してください。

ヒント インポートされるものと同じ名前の共有ポリシーまたはオブジェクトがあれば置換されます。ユーザーがポリシーまたはオブジェクトをすでにロックしている場合、ポリシーまたはオブジェクトのインポートは失敗します。ポリシーまたはデバイスのインポート （615 ページ）で説明されているように、デバイスを設定するための変更が適用される前に、ポリシーを送信する必要があります。

ステップ 4 共有ポリシーをすべてインポートしない場合、他のサーバ上ではインポートする予定のなかった共有ポリシーを削除します。これは手動の処理です。

デバイス インベントリのエクスポート

デバイスインベントリをエクスポートすると、インベントリを他のネットワーク管理アプリケーションにインポートしたり、独自のレポートを生成する目的で出力を操作したりできます。デバイス インベントリをエクスポートするには、相互に関連のない 2 つの方法があります。

- **[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** コマンドを使用する：このコマンドを使用して、デバイスとその設定ポリシー全体を含む単純なカンマ区切り値（CSV）ファイルまたは圧縮された .dev ファイルを作成できます。CSV ファイルは、CiscoWorks Common Services Device Credential Repository（DCR）、Cisco Security Monitoring, Analysis and Response System（CS-MARS）、Cisco Prime Security Manager（PRSM）、または他の Cisco Security Manager のインストールへのインポートに適した形式です。つまり、スプレッドシートやテキストエディタのプログラムでファイルを開いて表示できます。.dev ファイルは、他の Security Manager サーバへのインポート専用です。詳細については、Security Manager クライアントからのデバイス インベントリのエクスポート （605 ページ）を参照してください。
- Perl スクリプト CSMgrDeviceExport を使用する：この Perl スクリプトでは、Security Manager クライアントを起動せずにインベントリをエクスポートできます。出力を画面または Comma-Separated Value（CSV; カンマ区切り値）ファイルに転送できます。詳細については、コマンドラインからのデバイス インベントリのエクスポート （611 ページ）を参照してください。

（注） 各デバイス設定の最新の 5 つのバージョンのみエクスポートされます。

Security Manager クライアントからのデバイス インベントリのエクスポート

デバイスインベントリをさまざまな形式でエクスポートできます。主な選択肢は次のとおりです。

- [CSVとしてエクスポート（Export as CSV）]（カンマ区切り値）：次のいずれかの形式でインベントリ情報を含む単純な CSV ファイルを作成できます。CSM（Cisco Security Manager で使用）、Device Credential Repository（DCR、CiscoWorks Common Services の場合）、および CS-MARS シードファイル（Cisco Security Monitoring、Analysis and Response System で使用）。スプレッドシート アプリケーションまたはテキストエディタで CSV ファイルを開き、他の Cisco Security Manager サーバーを含む、その形式をサポートするアプリケーションでそのファイルを使用できます。ただし、この形式にはポリシー情報が含まれないため、他の Security Manager サーバで使用する場合は、デバイスの追加時にポリシーを見つける必要があります。

- CSV形式の詳細については、インベントリのインポートまたはエクスポートでサポートされている CSV 形式 （609 ページ）を参照してください。
- CSV ファイルからデバイスをインポートする方法については、 インベントリ ファイルからのデバイスの追加 （122 ページ）を参照してください。

- [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）]：デバイスで使用されるすべてのデバイスのプロパティ、ポリシー、およびポリシーオブジェクトとともにデバイスインベントリをエクスポートします。エクスポートされた情報には、次の内容が含まれています。

（注） *.pol または *.dev ファイルのインポートは、各ファイルのエクスポート時に使用されたものと同じバージョンの Cisco Security Manager でのみサポートされます。あるバージョンの Cisco Security Manager からエクスポートして、別のバージョンを実行しているサーバーにインポートすることはできません。

- ポリシーで使用されるすべてのポリシーオブジェクト、およびオブジェクトのデバイスレベルのオーバーライドを含む、デバイスに割り当てられたすべてのローカルポリシーと共有ポリシー。共有ポリシーの割り当ては維持されます。
- デバイス プロパティおよびデバイス インベントリ。
- デバイスの Configuration Archive データ。
- デバイスの履歴スナップショット。
- デバイス証明書。
- IPS デバイス ライセンスおよび証明書情報。適用されたシグネチャはエクスポートされません（デバイスをインポートする場合は、同じシグネチャパッケージをサーバーに登録する必要があります）。IPS 更新設定は含まれていません。インポート後に再作成する必要があります。
- デバイスが参加している VPN トポロジ。ただし、VPN トポロジは、そのトポロジに参加しているすべてのデバイスがエクスポートに含まれる場合のみエクスポートされます。エクストラネット VPN は常にエクスポートされます。

したがって、エクスポート ファイルには、選択したデバイスのポリシー設定全体が含まれます。作成されたファイルは拡張子 .dev を持ち、他の Security Manager サーバからは読み取り専用にすることができます（ファイルの内容は圧縮されており、解読不能であるため、ユーザのポリシー情報のセキュリティが保持されます）。

.dev ファイルを別の Cisco Security Manager サーバーにインポートする方法については、ポリシーまたはデバイスのインポート （615 ページ）を参照してください。

エクスポートサイズの制限

Cisco Security Manager データベースに多数のデバイス、または多数のポリシーやポリシーオブジェクトが含まれている場合は、エラーを防ぐために、一度にエクスポートするデバイスの数を制限する必要があります。次のガイドラインを使用して、一度に正常にエクスポートできるデバイスの数を見積もることができます。

例 1：データベース内に 1000 以上のデバイス、デバイスごとに約 1500 以上のポリシー、データベース内に約 25,000 のオブジェクトがある場合。

- 一度にエクスポートできるデバイスの最大数（デバイスのみ）= 250
- 一度にエクスポートされるデバイスの最大数（ポリシーやオブジェクトと同時）= 100 ～ 150

例 2：データベース内に 1000 未満のデバイス、デバイスごとに約 1500 以上のポリシー、データベース内に約 10,000 ～ 15,000 のオブジェクトがある場合。

- 一度にエクスポートできるデバイスの最大数（デバイスのみ）= 250 ～ 300
- 一度にエクスポートされるデバイスの最大数（ポリシーやオブジェクトと同時）= 200

ヒント

- [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）] オプションを選択すると、Cisco Security Manager サーバーまたはローカルの Cisco Security Manager クライアントにエクスポートできます。CSV ファイルをエクスポートする場合は、Cisco Security Manager サーバーにのみエクスポートできます。ローカル Cisco Security Manager クライアントにエクスポートまたはインポートする機能は、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）]** から制御できます。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。
- エクスポートされたデバイスは、インベントリから削除されません。別の Cisco Security Manager サーバーからデバイスを管理する場合は、該当デバイスを別のサーバーに正常にインポートした後でデバイスを削除します。
- AUS または Configuration Engine を使用して構成を管理するデバイスを選択する場合は、エクスポートするデバイスのリストでサーバーも選択する必要があります。AUS または Configuration Engine の情報は、CS-MARS 形式にはエクスポートできません。
- 管理対象外のデバイスをエクスポートできます。
- ポリシーとともにデバイスをエクスポートする場合、送信済みかつ承認済みのポリシーおよびポリシーオブジェクトのみエクスポートファイルに含まれます。ポリシーおよびポリシーオブジェクトとともにデバイスをエクスポートする前に、必要なすべての送信と承認が行われていることを確認します。
- イベントデータとレポートデータ（つまり、イベントビューアまたは Report Manager で使用できるデータ）を含むエクスポートファイルのタイプはありません。したがって、別の Cisco Security Manager サーバーに移動する目的でデバイスをエクスポートしている場合、すでに収集されているそのデバイスに関するイベントおよびレポートデータは、新しいサーバーでは使用できません。

- デバイスグループ情報を含むエクスポートファイルのタイプはありません。デバイスをインポートしたあとに、手動でデバイス グループを再作成し、そのグループにデバイスを割り当てる必要があります。
- セキュリティコンテキストまたは仮想センサーを選択するときは、ホストデバイスも選択してください。また、デバイスが VPN に参加している場合は、デバイス、ポリシー、およびポリシー オブジェクトのエクスポート時に VPN 内のすべてのデバイスを選択するようにします。
- IPS または IOS IPS デバイスを選択する場合は、すでに IPS シグニチャの更新をデバイスに適用済みであることを確認します。基本センサーパッケージ（Sig0）を使用して IPS または IOS IPS デバイスをエクスポートできますが、インポートはできません。インポートエラー「Sig0 パッケージがありません（missing Sig0 package）」が表示されます。
- 別のデバイスに含まれているデバイス タイプのうち、Catalyst 6500/7600 内の任意のモジュール、ルータ内の AIM モジュールまたは NME モジュールを選択すると、ホスティング デバイスも自動的にエクスポートされます。ASA デバイスとその IPS モジュールを別々にエクスポートできます。
- アクティビティ セッションまたは設定セッションの承認中は、デバイスとそのポリシー（.dev 形式）をエクスポートできません。デバイスとそのポリシーをエクスポートするには、先にすべての承認が完了している必要があります。アプルーバのいる Workflow モードでは、アプルーバに問い合わせ、承認をただちに完了させるように依頼します。Workflow 以外のモードまたはアプルーバのいない Workflow モードでは、変更が送信されると承認が自動的に行われるため、数分待ってからエクスポートを再試行します。
- デバイスとそのポリシー（.dev 形式）のエクスポート中は、ポリシーの変更を承認できません。エクスポートファイルが作成されるとすぐにコマンドが終了し、ユーザは再びポリシーの変更を承認できるようになります。このことは、Workflow 以外のモードまたはアプルーバのいない Workflow モードの場合、エクスポート処理中に送信ができないということになります。
- デバイス、ポリシー、およびポリシー オブジェクトをエクスポートするには、ポリシーとオブジェクトのタイプに対するポリシー変更とオブジェクト変更の権限、およびデバイス変更の権限が必要です。これらの権限は、認可制御に ACS を使用するときに、個別のポリシー、オブジェクト、およびデバイスに割り当てることができます。システム管理者、ネットワーク管理者、またはセキュリティ管理者の権限を持つと、それに必要な権限が与えられます。

デバイスを CSV にエクスポートする場合は、[デバイスの変更（Modify Devices）] 権限のみが必要です。

関連項目

- セレクタ内の項目のフィルタリング （60 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）
- [Customize Desktop] ページ （654 ページ）

ステップ 1 デバイスビューで、**[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** を選択して、[インベントリのエクスポート（Export Inventory）] ダイアログボックスを開きます。

ステップ 2 [CSVとしてエクスポート（Export as CSV）] または [デバイス、ポリシー、およびオブジェクトのエクスポート（Export Devices, Policies, and Objects）] を選択します。これらのオプションについては、上記に説明があります。

ステップ 3 エクスポートファイルに含めるデバイスを選択し、[>>] をクリックして [選択済みデバイス（Selected Devices）] リストに追加します。フォルダを選択して、フォルダ内のすべてのデバイスを選択できます。

デバイスを選択するためのリストには、デバイス変更の権限があるデバイスだけが表示されます。

（注） Cisco Security Manager データベースに多数のデバイス、または多数のポリシーやポリシーオブジェクトが含まれている場合は、エラーを防ぐために、一度にエクスポートするデバイスの数を制限する必要があります。詳細については、前述の「**エクスポートサイズの制限**」を参照してください。

ステップ 4 [参照（Browse）] をクリックして、エクスポートファイルの作成先となるフォルダを選択し、エクスポートファイルの名前を入力します。[ファイルタイプ（File Type）] で、作成するファイルタイプを選択します。CSV ファイルの作成時はこの選択が重要ですが、.dev ファイルの作成時には 1 つのオプションを使用できます。

[保存（Save）] をクリックして [インベントリのエクスポート（Export Inventory）] ダイアログボックスに戻ります。[Export Inventory To] フィールドが、エクスポート ファイル情報で更新されます。

ステップ 5 [OK] をクリックして、エクスポートファイルを作成します。

エクスポートの完了時間、およびエクスポートにエラーがあったかどうかを示すメッセージが表示されます。[OK] をクリックすると、エクスポート中に問題が発生した場合は、ダイアログボックスが開き、メッセージが表示されます。ダイアログボックスに [詳細（Details）] ボタンがある場合は、メッセージを選択して [詳細（Details）] をクリックすると、さらに読みやすい形式のメッセージを確認できます。

インベントリのインポートまたはエクスポートでサポートされている CSV 形式

CSV（カンマ区切り値）ファイルにデバイスをエクスポートする場合（**[ファイル（File）] > [エクスポート（Export）] > [デバイス（Devices）]** を選択して [CSVとしてエクスポート（Export as CSV）] を選択）、または CSV ファイルからデバイスをインポートする場合（**[ファイル（File）] > [新規デバイス（New Device）]** を選択して New Device ウィザードの [ファイル（File）] から [デバイスの追加（Add Device）] を選択）には、次のいずれかの CSV ファイル形式を選択できます。

- **Device Credential Repository（DCR）**：CiscoWorks Common Services 用のデバイス管理システム。この形式の詳細については、次の URL で、Common Services のマニュアルのサンプルバージョン 3.0 CSV ファイルの説明を参照してください。
  http://www.cisco.com/en/US/docs/net_mgmt/ciscoworks_common_services_software/3.3/user/guide/dcr.html#wp1193611

- **CS-MARS シードファイル**：Cisco Security Monitoring、Analysis and Response System。この形式の詳細については、次の URL で、CS-MARS のマニュアルを参照してください。http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/device/configuration/guide/chDvcOver.html#wp162016
- **Cisco Security Manager**：Cisco Security Manager 形式。DCR バージョン 3.0 形式に複数のフィールドを追加した形式です。インベントリを別の Security Manager サーバにインポートしている場合は、この形式を選択すると、デバイスでポリシーを検出せずにインベントリをインポートできます。

（注） ファイルにデバイスの os_type および os_version が指定されていない場合は、デバイスを追加するときにデバイスから直接ポリシーを検出する必要があります。

各行の末尾に表示される追加のフィールドは次のとおりです。

- os_type。オペレーティング システム タイプ。PIX、ASA、IOS、FWSM、IPS のいずれかになります。このフィールドは、すべてのデバイス タイプに必須です。
- os_version。ターゲット オペレーティング システム バージョン。[Add New Device] を選択したときに New Device ウィザードのリストに示されるバージョン番号のいずれかになります。許容できるバージョン番号はデバイス モデルによって異なるため、CSV ファイルを手作業で作成している場合は、このリストに慎重に目を通してください。この方法を使用したデバイスの追加の詳細については、手動定義によるデバイスの追加 （116 ページ）を参照してください。このフィールドは、すべてのデバイス タイプに必須です。
- fw_os_mode。ファイアウォール デバイスが実行されているモード。TRANSPARENT、ROUTER、MIXED のいずれかになります。このフィールドは、ASA、PIX、および FWSM デバイスに必須です。
- fw_os_context。ファイアウォール デバイスが実行されているコンテキスト。SINGLE または MULTI になります。このフィールドは、ASA、PIX、および FWSM デバイスに必須です。
- anc_os_type。Cisco IOS-IPS デバイスの補助的なオペレーティング システム タイプ。存在する場合は IPS となります。このフィールドは、IOS IPS デバイスに必須です。
- anc_os_version。補助的なターゲット オペレーティング システム バージョンで、IPS ターゲット オペレーティング システム バージョンです。存在する場合は、サポートされている IOS-IPS バージョンのいずれかになります。このフィールドは、IOS IPS デバイスに必須です。

これらの CSV ファイルは、そのファイル形式をサポートする任意のプログラムで使用できます。ユーザ自身で CSV ファイルを作成し、そのファイルを使用して Security Manager にインベントリをインポートすることもできます。

関連項目

- Security Manager クライアントからのデバイス インベントリのエクスポート （605 ページ）
- ポリシーまたはデバイスのインポート （615 ページ）
- インベントリ ファイルからのデバイスの追加 （122 ページ）

コマンドラインからのデバイス インベントリのエクスポート

Security Manager には、Security Manager クライアントを起動せずにデバイス インベントリをエクスポートするのに使用できる Perl スクリプトが用意されています。このスクリプトを使用すると、組織で必要になるさまざまなオフライン レポート タスクを自動化できます。出力を Comma-Separated Value（CSV; カンマ区切り値）ファイルにパイプできます。また、出力をキャプチャして操作することもできます。

ヒント このコマンドでは、デバイスのインポートまたは「ファイルからの」デバイスの追加に使用できるファイルは生成されません。このコマンドは、インベントリ情報をエクスポートするので、統合されたエクスポート機能のように見えますが、コマンドの有効性は、独自のオフラインレポートプロセス要件を備えた組織でのレポートの用途に限定されます。

Perl コマンドは $NMSROOT\bin（通常は C:\Program Files\CSCSpx\bin）にあります。コマンドの構文は次のとおりです。

perl [*path*]**CSMgrDeviceExport.pl -u** *username* [**-p** *password*] [**-s** {**Dhdoirtg**}] [**-h**] [> *filename.csv*]

構文

perl [*path*] **CSMgrDeviceExport.pl**	Perl スクリプト コマンド。システム パス変数内に CSMgrDeviceExport.pl ファイルへのパスが定義されていない場合は、そのパスを追加します。
-u *username*	Security Manager のユーザ名。エクスポートされるデータは、このユーザに割り当てられた権限によって制限されます。ユーザには、デバイス表示の権限が必要です。
-p *password*	（オプション）ユーザーのパスワード。コマンドにパスワードを含めていない場合、パスワードの入力を求められます。

-s {Dhdoirtg}	（オプション）出力に含めるために選択されているフィールド。-s オプションを指定しない場合は、すべてのフィールドが含められます。次の 1 つ以上を指定できます。 • D：表示名。 • h：ホスト名。 • d：ドメイン名。 • o：オペレーティング システム（OS）タイプ。 • I：イメージ名。 • r：実行中の OS バージョン。 • t：ターゲット OS バージョン。 • g：デバイス グループ。
-h	（オプション）コマンドラインのヘルプを表示します。このオプションを指定すると、他のすべてのオプションは無視されます。
> *filename.csv*	（オプション）出力を指定のファイルに渡します。ファイルを指定しない場合、出力は画面に表示されます。

出力形式（Output Format）

出力は標準の Comma-Separated Value（CSV; カンマ区切り値）形式であるため、スプレッドシートプログラムで開いたり、独自のスクリプトで処理したりできます。最初の行はカラムの見出しです。カラムは左から右に、上記の -s オプションで説明したフィールドの順に並んでいます。

特定のフィールドに値がない場合、そのフィールドは出力でブランクになります。

デバイス グループ出力フィールドは二重引用符で囲まれ、複数のグループ名が含まれることがあります。グループ名には、グループのパス構造が含まれています。たとえば、次の出力はデバイスが 2 つのグループの一部であることを示します。[Department] フォルダの East Coast グループと、[New] フォルダの NewGroup グループです。グループは、セミコロンで区切られています。

```
"/Department/East Coast; /New/NewGroup"
```

スクリプトが生成したエラー メッセージがあれば、出力ファイルに書き込まれます。

共有ポリシーのエクスポート

他の Security Manager サーバにインポートするために使用する共有ポリシーおよびポリシー オブジェクトをエクスポートできます。この機能は、Cisco Security Manager サーバー間での共有

ポリシーの同期（603ページ）で説明されているように、サーバーのグループ間で同じポリシーを維持するのに役立ちます。

（注） *.pol または *.dev ファイルのインポートは、各ファイルのエクスポート時に使用されたものと同じバージョンの Cisco Security Manager でのみサポートされます。あるバージョンの Cisco Security Manager からエクスポートして、別のバージョンを実行しているサーバーにインポートすることはできません。

ヒント

- Security Manager サーバーまたはローカルの Security Manager クライアントにインポートできます。ローカル Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。
- 共有ポリシーおよびポリシー オブジェクトは、送信されて承認済みのものだけがエクスポート ファイルに含まれます。ポリシーをエクスポートする前に、必要なすべての送信と承認が行われていることを確認します。
- 共有ポリシーによって参照されるすべてのポリシーオブジェクトもエクスポートされます。ただし、ポリシーオブジェクトが参照されていない場合はエクスポートされません。ネットワーク/ホスト、サービス、およびポート リストのオブジェクトを直接エクスポートするために使用できる個別のコマンドがあります。詳細については、ポリシーオブジェクトのインポートおよびエクスポート （318 ページ）を参照してください。
- アクティビティ セッションまたは設定セッションの承認中は、ポリシーをエクスポートできません。ポリシーをエクスポートするには、先にすべての承認が完了している必要があります。アプルーバのいる Workflow モードでは、アプルーバに問い合わせ、承認をただちに完了させるように依頼します。Workflow 以外のモードまたはアプルーバのいない Workflow モードでは、変更が送信されると承認が自動的に行われるため、数分待ってからエクスポートを再試行します。
- ポリシーのエクスポート中は、ポリシーの変更を承認できません。エクスポート ファイルが作成されるとすぐにコマンドが終了し、ユーザは再びポリシーの変更を承認できるようになります。このことは、Workflow 以外のモードまたはアプルーバのいない Workflow モードの場合、エクスポート処理中に送信ができないということになります。
- ポリシーとそのポリシーオブジェクトをエクスポートするには、そのポリシーとオブジェクトタイプに対するポリシー変更とオブジェクト変更の権限が必要です。これらの権限は、認可制御に ACS を使用するときに、個別のポリシー、オブジェクト、およびデバイスに割り当てることができます。システム管理者、ネットワーク管理者、またはセキュリティ管理者の権限を持つと、それに必要な権限が与えられます。

（注） バージョン 4.21 以降、Cisco Security Manager は Cisco Identity Services Engine（ISE）を介した TACACS+ 認証のみをサポートします。これは、ACS のサポートが終了しているためです。

関連項目

- Security Manager サーバ クラスタの管理 （601 ページ）
- Security Manager サーバの分割 （601 ページ）
- Cisco Security Manager サーバー間での共有ポリシーの同期 （603 ページ）
- Security Manager クライアントからのデバイス インベントリのエクスポート （605 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）
- [Customize Desktop] ページ （654 ページ）

ステップ 1 Configuration Manager で、[ファイル（File）] > [エクスポート（Export）] > [ポリシー（Policies）] を選択して、[共有ポリシーのエクスポート（Export Shared Policies）] ダイアログボックスを開きます。

ダイアログボックスが開く前に、Security Manager によって、定義済みの共有ポリシーが評価およびロードされている必要があります。

ステップ 2 次のいずれかの方法を使用して、エクスポートする共有ポリシーを選択します。

ヒント 複数の方法を使用してポリシーを選択できます。たとえば、特定の日付以降に変更されたすべての共有ポリシーを選択したり、特定のタイプの共有ポリシーすべてを選択したりすることが可能で、選択したポリシーを同じファイルにエクスポートできます。

- 特定の日付以降に変更されたすべての共有ポリシーを選択するには、その日付を [変更日（Modified）] フィールドに入力し、[変更日（Modified）] フィールドの横にある [選択>>（Select >>）] をクリックします。日付を *MMM DD YYYY* 形式で入力するか、[カレンダー（Calendar）] をクリックして目的の日付を選択します。
- すべての共有ポリシーを選択するには、[すべて（すべて）] フォルダを選択し、[すべての共有ポリシーを参照（Browse All Shared Policies）] で [選択>>（Select >>）] をクリックします。
- 特定のタイプの共有ポリシーすべてを選択するには、共有ポリシーのタイプを選択し、[すべての共有ポリシーを参照（Browse All Shared Policies）] で [選択>>（Select >>）] をクリックします。フォルダを選択して、選択したリストにフォルダ内のすべてのタイプを移動できます。
- エクスポートする特定の共有ポリシーを指定するには、[すべての共有ポリシーを参照（Browse All Shared Policies）] リストからエクスポートする共有ポリシーのタイプを選択し、エクスポートするタイプの共有ポリシーの横にあるチェックボックスをオンにして、[選択>>（Select >>）] をクリックします。それらを [選択済みのポリシー（Selected Policies）] リストに移動します。特定の共有ポリシー

を選択しない場合、選択したタイプのすべてのポリシーが [選択済みのポリシー（Selected Policies）] リストに追加されます。

（注） 共有ポリシーが定義されているポリシー タイプだけが表示されます。

[選択済みのポリシー（Selected Policies）] リストからポリシーを削除するには、ポリシーを選択して [<<削除（<< Remove）] ボタンをクリックします。[選択済みのポリシー（Selected Policies）] リストのすべてのエントリを削除対象に指定するには、[すべて選択（Select All）] チェックボックスを使用します。

ステップ 3 [共有ポリシーのエクスポート先（Export Shared Policies To）] フィールドの横にある [参照（Browse）] をクリックして、エクスポートファイルを作成するフォルダを選択し、ファイルの名前を入力します。ファイル タイプは、.pol としてあらかじめ選択されているため、変更できません。

[OK] をクリックして、ファイル名と場所を保存します。

ステップ 4 [共有ポリシーのエクスポート（Export Shared Policies）] ダイアログボックスの [OK] をクリックして、エクスポートを開始します。エクスポートが完了すると、エクスポートした共有ポリシーの数が通知され、警告やエラーがある場合は、ダイアログボックスが開いて問題が表示されます。

ポリシーまたはデバイスのインポート （615 ページ）で説明したように、これで、別の Security Manager サーバにポリシーをインポートできます。

ポリシーまたはデバイスのインポート

共有ポリシー（.pol）ファイル、または別の Security Manager サーバからエクスポートされたデバイス インベントリとポリシー（.dev）ファイルをインポートできます。

（注） *.pol または *.dev ファイルのインポートは、各ファイルのエクスポート時に使用されたものと同じバージョンの Cisco Security Manager でのみサポートされます。あるバージョンの Cisco Security Manager からエクスポートして、別のバージョンを実行しているサーバーにインポートすることはできません。

ヒント

- Security Manager サーバーまたはローカルの Security Manager クライアントからインポートできます。ローカルの Cisco Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。
- デバイスのインポート時、サーバには、インポートしているデバイスの数およびタイプに対応する十分な Security Manager ライセンスが必要です。Professional ライセンスを必要とするデバイス タイプをインポートする前に、そのライセンスをインストールするようにします。ライセンスのインストールの詳細については、Security Manager のライセンス ファイルのインストール （618 ページ）を参照してください。

- ポリシーをインポートするときは、デバイスまたは共有ポリシーのインポート中に、Security Manager 管理の [ポリシー管理（Policy Management）] ページで管理用に選択されたポリシータイプのみが表示されます。ただし、すべてのポリシーがインポートされます。以前管理用に選択を解除したポリシー タイプを選択すると、そのインポートされたポリシーは、インポートされた設定とともに表示されます。選択的なポリシー管理の詳細については、ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ （221 ページ）を参照してください。

- 共有ポリシーおよびポリシーオブジェクトのインポート時、サーバ上のポリシーまたはオブジェクトがインポートするものと同じ名前の場合は、インポートされるポリシーまたはオブジェクトによって置換されます。ポリシーまたはオブジェクトにロックがある場合、そのポリシーまたはオブジェクトのインポートは失敗します。メッセージには、失敗の原因がロックの問題であることが示されます。問題を回避するには、インポートを実行する前に、すべてのユーザーが共有ポリシーまたはポリシーオブジェクトへの変更を送信して承認していることを確認してください。

- デバイスをインポートすると、デバイスに割り当てられている共有ポリシーとポリシーオブジェクトもインポートされます。これらのポリシーとオブジェクトは、共有ポリシーのインポート時に使用されたのと同じ条件で、既存のポリシーとオブジェクトを置き換えます。

- ポリシー、およびそのポリシーオブジェクトをインポートするには、そのポリシーとオブジェクトタイプに対するポリシー変更とオブジェクト変更の権限が必要です。デバイスをインポートする場合、デバイスの変更権限も持っている必要があります。これらの権限は、認可制御に ACS を使用するときに、個別のポリシー、オブジェクト、およびデバイスに割り当てることができます。システム管理者、ネットワーク管理者、またはセキュリティ管理者の権限を持つと、それに必要な権限が与えられます。

- ファイルは、同じリリースの Security Manager を実行しているサーバーからエクスポートされた場合にのみインポートできます。

- デバイスがすでにインベントリにある場合には、そのデバイスをインポートできません。したがって、インポート ファイルからデバイス ポリシーを更新できません。デバイスを再インポートする場合は、あらかじめインベントリからそのデバイスを削除します。

- AUS または Configuration Engine サーバを使用して設定の展開を管理するデバイスをインポートする場合、そのサーバがインポート ファイルに含まれているか、または Security Manager サーバですでに定義されている必要があります（いずれか一方）。インベントリにすでに定義されている AUS または Configuration Engine がインポート ファイルに含まれている場合は、重複する表示名のエラーが発生します。AUS または Configuration Engine サーバーが割り当てられているデバイスをインポートしようとすると、「サーバーの選択が無効です」というエラーが発生しますが、サーバーがインポートファイルに含まれていないか、インベントリで定義されていません。

- 管理対象外デバイスをインポートできます。

- IPS デバイスのインポート時、サーバは、インポートされるデバイスと同じシグニチャ レベルである必要があります。たとえば、2 つの IPS デバイスがあり、一方がシグニチャ レベル 481 で、もう一方が 530 で稼働していて、これらのデバイスをインポートする場合、

サーバには 481 と 530 の両方がインストールされている必要があります。IPS デバイスをインポートする前に、IPS 更新の確認とダウンロード （2304 ページ）に説明されているようにシグニチャ パッケージのダウンロードが必要な場合があります。

- この手順では、.pol ファイルまたは .dev ファイルのインポート方法について説明します。CSV ファイルからデバイス インベントリをインポートする場合、手順の説明は インベントリ ファイルからのデバイスの追加 （122 ページ）にあります。これらの手順は異なります。

関連項目

- Security Manager サーバ クラスタの管理 （601 ページ）
- Security Manager サーバの分割 （601 ページ）
- Cisco Security Manager サーバー間での共有ポリシーの同期 （603 ページ）
- Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）
- [Customize Desktop] ページ （654 ページ）

ステップ 1 Configuration Manager で、[ファイル（File）] > [インポート（Import）] を選択して [インポート（Import）] ダイアログボックスを開きます。

ステップ 2 [参照（Browse）] をクリックしてファイルを選択します。[Select a File] ダイアログボックスの [Files of Type] リストから目的のファイル タイプ（.pol または .dev）を選択するようにします。

ファイルを選択したら、[OK] をクリックします。

ステップ 3 [インポート（Import）] ダイアログボックスで、[OK] をクリックします。

インポートされるポリシーまたはポリシー オブジェクトによる同じ名前のポリシーおよびオブジェクトの置換が警告されます。必要な認可権限（システム管理者または管理変更）がある場合は、[共有ポリシーとインポートしたオブジェクトの警告をすべて表示する（Display a warning on all shared policies and imported objects）] を選択解除するオプションがあります。選択した場合は、共有ポリシーおよびインポートされたオブジェクトのバナーにより、インポート中に共有ポリシーが作成された可能性があること、およびインポート中に特定のオブジェクトが実際に作成されたことがユーザに警告されます。この警告は、ユーザがポリシーまたはオブジェクトを変更する場合に、この変更がそのあとに行われるポリシーのインポートによって上書きされる可能性があるという注意を促します。警告を表示するかどうかを選択し、[はい（Yes）] をクリックします。

ヒント 警告を表示するかどうかをあとで変更する場合は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ポリシー管理（Policy Management）] ページで [共有ポリシーとインポートしたオブジェクトの警告をすべて表示する（Display a warning on all shared policies and imported objects）] オプションを変更できます。

情報がインポートされ、その結果が通知されます。エラーが発生した場合、インポートは行われず、エラーを説明するダイアログボックスが開きます。最も一般的なエラーには、デバイスをインポートするときのデバイスの表示名の重複、インポートされるものと同じ名前を持つ共有ポリシーまたはポリシーオブジェクトのロックなどがあります。

- 表示名の重複問題を解決するには、インベントリからデバイスを削除するか、そのデバイスの名前を変更する必要があります。デバイスを選択してインポートすることはできません。すべてインポートするかインポートしないかのいずれかです。

（注） 重複するデバイス名がすべて表示されるわけではありません。AUS または Configuration Engine を使用して設定の展開を管理している場合、インポートされる AUS 名および設定名は、管理対象デバイス名より先に評価されます。したがって、最初に出るエラーを修正したあとに、新たな重複表示名のエラーが表示されることがあります。

- ロックの問題を解決するには、ユーザがポリシーの変更を送信したら、その変更を承認させるようにする必要があります。デバイスのインポート時、インポートを再試行する前にインポートされたデバイスの削除が必要な場合があります。

ヒント デバイスのインポート時、デバイスがデバイス ビューのデバイス リストに表示されるまで時間がかかる場合があります。また、インポート時にデバイス グループは維持されません。すべてのデバイスが、All グループに配置されます。手動で目的のデバイス グループ構成を再作成し、デバイスを適切なグループに追加する必要があります。

ステップ 4 ポリシーの変更はアクティビティ セッションまたは設定セッションで実行されるため、インポートされるポリシーおよびポリシー オブジェクトは、まだ Security Manager データベースにコミットされていません。変更を送信および承認する必要があります。Workflow モードに基づいて、次のように行います。

- Workflow 以外のモード：[ファイル（File）] > [送信（Submit）] を選択します。
- 承認者のいない Workflow モード：[アクティビティ（Activities）] > [アクティビティの承認（Approve Activity）] を選択します。
- 承認者のいる Workflow モード：[アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）] を選択します。アクティビティは、変更をコミットする前に承認する必要があります。

インポートに問題がある場合は、アクティビティ セッションまたは設定セッションを廃棄できます。ただし、デバイスのインポート時、デバイスがアクティビティ セッションまたは設定セッション以外で追加されます。したがって、アクティビティまたは設定セッションを破棄すると、デバイスポリシーと VPN トポロジが破棄されますが、デバイスはインベントリに残ります。Security Manager インベントリからのデバイスの削除 （162 ページ）に説明されているように、デバイスを削除する必要もあります。

Security Manager のライセンス ファイルのインストール

ご使用の Security Manager ソフトウェア ライセンスの条件に従って、使用可能な機能や管理できるデバイス数を含めて多くの事柄が決まります。ライセンスの目的で、IP アドレスを使用する物理デバイス、セキュリティ コンテキスト、仮想センサー、または Catalyst セキュリティ サービス モジュールが、デバイスとしてカウントされます。フェールオーバー ペアは 1 つのデバイスとしてカウントされます。PIX ファイアウォール、FWSM、および ASA デバイスが（複数のセキュリティ コンテキストをホストするように）マルチ コンテキスト モードで設定されている場合は、セキュリティ コンテキストだけがデバイスとしてカウントされ、ホスティング デバイスは個別のデバイスとしてカウントされません。

Standard、Professional、および Upgrade の 3 つのライセンス タイプが入手可能です。また、デバイス数が最大 50 に制限される 90 日間の無償評価期間があります。入手可能なライセンスタイプと、サポートされているさまざまなアップグレードパス、および購入可能な Cisco Software Application Support サービス契約の詳細については、http://www.cisco.com/en/US/products/ps6498/prod_bulletins_list.html でこのバージョンの Security Manager の製品速報を参照してください。『Installation Guide for Cisco Security Manager』も参照してください。

割り当てられた時間（評価版ライセンスの場合）、またはご使用のライセンスで管理可能なデバイス数を超過すると、ライセンス制限が発生します。評価版ライセンスの権限は、Professional 版ライセンスの権限と同じです。製品を継続して使用できるように、90 日以内にできるだけ早く必要なデバイス数に対して Security Manager を登録することが重要です。アプリケーションを起動するたびに、評価版ライセンスの残りの日数が通知され、評価期間中にアップグレードするように求められます。評価期間終了後は、ライセンスをアップグレードしないとログインできなくなります。

非評価ライセンスについては、ご使用の設定ライセンスで許可された数よりも多くのデバイスがデータベースに含まれる場合、Security Manager クライアントを使用してアプリケーションにログインできません。ログイン中にライセンスを追加するように求められ、適切なライセンスを追加するまでログインを完了できません。

ヒント　セキュリティコンテキストを検出したアクティビティを送信していないで、それらが現在デバイスセレクタに表示されていなくても、デバイスの数には検出されたすべてのセキュリティコンテキストと仮想センサーが含まれます。インベントリ内のデバイス数がライセンスで許可されるデバイス数よりも少ないのに、デバイス カウント エラー メッセージが表示される場合は、検出されたデバイスの数を決定するためにすべてのアクティビティを送信してください。管理対象でないデバイスは削除してください。

はじめる前に

- 基本ライセンスまたはアップグレードライセンスと、その他の必要なライセンスを取得します。Cisco.com ユーザ ID が必要です。また、Cisco.com でソフトウェアのコピーを登録する必要があります。登録時に、出荷ソフトウェア パッケージ内の Software License Claim Certificate に対応付けられている Product Authorization Key（PAK; 製品認証キー）を指定する必要があります。
  - Cisco.com ユーザとして登録済みの場合は、http://www.cisco.com/go/license にアクセスしてください。
  - Cisco.com ユーザとして登録されていない場合は、http://tools.cisco.com/RPF/register/register.do にアクセスしてください。

登録後に、基本ソフトウェアライセンスが、登録時に指定した電子メールアドレスに送られます。Security Manager の PAK とライセンスを受信するのに加えて、購入したデバイス カウント パックごとに PAK が 1 つ追加されます。

これらのライセンス ファイルを、Security Manager サーバまたはローカル Security Manager クライアント上のフォルダにコピーします。Security Manager サーバにライセンス ファイルをコピーする場合、ライセンス ファイルは、Security Manager サーバのローカル ディスクに格納する必要があります。サーバに対応付けらたドライブを使用することはできません。Windows ではこの制限が課されますが、これにより Security Manager のパフォーマンスとセキュリティが向上します。

（注） ローカルの Security Manager クライアントにあるライセンスファイルをインストールするには、クライアント側のファイル参照を有効にする必要があります（[Customize Desktop] ページ （654 ページ） を参照）。

ヒント ライセンスファイルを、Security Manager サーバー上にある製品のインストールフォルダ内の etc/licenses/CSM フォルダに格納しないでください。このフォルダに格納した場合、ライセンスを追加しようとするとエラーが発生します。ファイルは、製品フォルダ以外のフォルダに格納してください。

- Common Services にライセンス ファイルは必要ありません。
- Auto Update Server にライセンス ファイルは必要ありません。

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツ テーブルから [ライセンス（Licensing）] を選択します。

ステップ 2 タブがアクティブになっていない場合は、[CSM] をクリックします。このタブの各フィールドの説明については、[CSM] タブ、[Licensing] ページ （720 ページ） を参照してください。

ステップ 3 [ライセンスのインストール（Install a License）] をクリックして、[ライセンスのインストール（Install a License）] ダイアログボックスを開きます。

[Install a License] ダイアログボックスには、ライセンスを取得するための Cisco.com へのリンクが含まれています（まだライセンスを取得していない場合）。[参照（Browse）] をクリックしてライセンスファイルを選択し、[ライセンスのインストール（Install a License）] ダイアログボックスで [OK] をクリックしてライセンスをインストールします。

すべてのライセンスのインストールが完了するまで、このプロセスを繰り返します。

証明書信頼管理

Cisco Security Manager は、HTTPS 経由で Cisco.com から ASA イメージと IPS パッケージをダウンロードします。信頼を確立するために証明書を使用します。バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、両方のタイプのダウンロードで Cisco.com 証明書の処理を改善するのに役立ちます。

- ASA イメージのダウンロード。ASA イメージダウンロードの証明書信頼管理に関する詳細なドキュメントについては、[Image Manager] ページ （695 ページ）を参照するか、または**[ツール（Tools）] > [Security Manager管理...（Security Manager Administration...）] > [Image Manager] > [ヘルプ（Help）]** に移動します。
- IPS パッケージのダウンロード。IPS パッケージダウンロードの証明書信頼管理に関する詳細なドキュメントについては、[Edit Update Server Settings] ダイアログボックス （712 ページ）を参照するか、または**[ツール（Tools）] > [Security Manager管理...（Security Manager Administration...）] > [IPS アップデート（IPS Updates）] > [サーバーグループの更新（Update Server group）] > [設定の編集（Edit Settings）] > [ヘルプ（Help）]** に移動します。

証明書信頼管理機能

Security Manager の証明書信頼管理機能には、次の特性があります。

- ブラウザのように動作します。ユーザが意識的に信頼しているものに信頼を与えます。
- これにより、証明書を表示し、自分の裁量でそれを受け入れることができます。
- 証明書を積極的に検証して、受け入れるか拒否するかを判断するのに役立ちます。たとえば、証明書が自己署名されている（信頼できる認証局によって発行されていない）かどうかを確認したり、期限が切れているか、まだ有効でないか、取り消されているかを確認します。
- 証明書を受け入れると、その証明書が Security Manager サーバーに保存されます。
- 透明性と制御を提供します。証明書の取得と追加、証明書の表示、および保存されている証明書の削除ができます。
- Cisco.com との通信中に、ライブサーバー証明書と保存されている証明書を比較し、完全に一致した場合にのみ続行します。ルート証明書だけでなく、完全な証明書チェーンが一致するかどうかを比較します。不一致がある場合、新しい証明書を表示して受け入れるまで、現在の操作は中止されます。
- 証明書の失効と有効性について Security Manager サーバーを毎日チェックし、サーバーから失効した証明書または無効な証明書を削除します。これは、証明書にある CRL 配布ポイント/URL とのライブコンタクトによって行います。デフォルトの固定スケジュールでは、この毎日のチェックは午前 2 時に実行されます。

ダウンロード要件

Cisco.com からイメージをダウンロードするには、最新のイメージメタデータロケータ証明書とダウンロードサイトの最新の証明書 URL の両方を取得、表示、および受け入れる必要があります。Security Manager インターフェイスには、主要拠点のユーザを支援するためのメッセージがあり、詳細なドキュメントは[Image Manager] ページ （695 ページ）および[Edit Update Server Settings] ダイアログボックス （712 ページ）を参照することで入手できます。

トラブルシューティング

証明書の失効と有効性を毎日チェックしている間、CRL 失効リストは Security Manager サーバーに保存されません。そのため、接続が失われた場合、毎日のチェックでは証明書の失効の可能性を検出できません。この問題は、接続が復元された後に解決されます。

ASAイメージのダウンロード中またはIPSアップデートパッケージの確認中にエラーが発生した場合、最もあり得る原因は次のとおりです。

- サイトの証明書が Security Manager サーバーで見つからない
- サイトから受け取った証明書と保存されている証明書が一致しない
- サイトの証明書の有効期限が切れている

上記の 3 つの場合すべてで、操作は中止され、エラーの原因と失敗したサイトの URL を示すメッセージが表示されます。回復するには、証明書機能のユーザインターフェイス ([ツール（Tools）] > [Security Manager管理...（ Security Manager Administration...）] > [Image Managerまたはツール（Image Manager or Tools）] > [Security Manager管理...（Security Manager Administration...）] > [IPSアップデート（IPS Updates）] > [サーバーグループの更新（Update Server group）] > [設定の編集（Edit Settings）] に移動し、次にサイトから新しい証明書を取得、表示、および受け入れて、ダウンロードを再試行します。

IPS アップデートのチェック中にエラーが発生した場合は、IPS パッケージのメタデータ情報の取得に使用された Cisco.com サイトの証明書と、IPS パッケージの実際のダウンロードサイトの証明書の両方を受け入れていることを確認してください。ジョブの実行ステータスを通知する電子メールを常に設定することをお勧めします。それにより、エラーから回復するための推奨されるアクションを電子メールで表示できます。電子メールメッセージから失敗したダウンロード URL をコピーして、証明書を取得します。

証明書が保存されるため、以前のバージョンから Security Manager 4.4 にアップグレードすると、Cisco.com とのすべての通信が失敗します。この問題を解決するには、イメージメタデータロケータとダウンロードサイトの URL から証明書を取得する必要があります。

ユーザーインターフェイスに保存されている証明書テーブルに特定の証明書の追加が表示されない場合は、証明書の失効と有効性の毎日のチェックで、失効または有効期限切れにより証明書が削除されていないかどうかを確認します。これを行うには、tomcat ログで証明書失効チェックタスクを探します。このログにより、保存されていた証明書が削除された正確な理由を確認できます。

監査レポートの使用

Security Manager で状態が変更されると、監査ログ内に監査エントリが作成されます。このエントリを表示するには、[管理（Manage）] > [監査レポート（Audit Report）] を選択します。ここでは、監査レポートについて詳しく説明します。

- 監査レポートについて （623 ページ）
- 監査レポートの生成 （623 ページ）

- 監査ログ エントリのページ （627 ページ）

監査レポートについて

Security Manager で状態が変更されると、監査ログ内に監査エントリが作成されます。このエントリを表示するには、[管理（Manage）] > [監査レポート（Audit Report）] を選択します。

次の状態変更が行われると、イベントが生成され、監査エントリが作成されます。

- 実行時環境に対する変更：
  - システム変更（ログイン試行（成功または失敗）、ログアウト、計画的なバックアップなど）
  - 認可の問題（試行の失敗やセキュリティ違反など）
  - マップの変更（バックグラウンド マップ ビューの保存、削除、変更など）
  - 管理上の変更（ワークフロー モードの変更など）
- Security Manager オブジェクトの状態の変更：
  - アクティビティの変更（アクティビティの作成、編集、送信、承認など）
  - 展開の変更（展開ジョブの作成、編集、送信など）
- 管理対象デバイスの状態の変更：
  - オブジェクトの変更（ポリシー オブジェクトの変更など）
  - インベントリの変更（インベントリ内のデバイスの追加、削除、変更など）
  - ポリシーの変更（ポリシーの作成、復元、変更、削除など）
  - VPN の作成、修正、または削除などの VPN の変更

監査レポートを表示するとき、目的のレコードだけが選択されるように検索基準を指定することにより、エントリのサブセットを表示できます。

関連項目

- 監査レポートについて （623 ページ）
- 監査ログ エントリのページ （627 ページ）

監査レポートの生成

監査ログを確認して、Security Manager システムで発生したイベントを分析できます。この情報は、ユーザーがデバイスに加えた変更を追跡したり、重要な他のシステムイベントを識別し

たりするのに役立ちます。[Audit Report] ウィンドウに、興味のある特定の監査ログ エントリを表示するために役立つ拡張的な検索基準が表示されます。

ヒント CiscoWorks Common Services を使用して監査ログを表示することもできます。[Common Servicesサーバー管理（Common Services Server Administration）] ページから [サーバー（Server）]>[レポート（Reports）] を選択し、コンテンツテーブルから [監査ログ（Audit Log）] を選択します。[レポートの生成（Generate Report）] をクリックすると、1 日ごとに 1 つのログリストが表示されます。目的のログのリンクをクリックすると、そのログが開きます。これらのログは、Program Files/CSCOpx/MDC/Logs/audit/ ディレクトリに格納されています。Common Services へのログインの詳細については、Cisco Security Management Suite サーバへのログイン （16 ページ）を参照してください。

関連項目

- 監査レポートについて （623 ページ）

ステップ 1 [管理（Manage）] > [監査レポート（Audit Report）] を選択して、[監査レポート（Audit Report）] ウィンドウを開きます。

ステップ 2 レポートを重要な領域に関連した特定のレコードセットに限定するには、該当する検索条件を左側ペインに入力して、[検索（Search）] をクリックします。検索フィールドの詳細については、[Audit Report] ウィンドウの使用 （624 ページ）を参照してください。

次に、検索基準の例について説明します。

- デバイス router1 が Security Manager 管理から削除された日時を調べるには、[アクションで検索（Search by action）] セレクタから [デバイス（Devices）] > [削除（Delete）] を選択します。[オブジェクトの名前の全体または一部で検索（Search by all or part of the object name）] フィールドに、デバイスの表示名（router1）を入力します。
- システムでログイン試行失敗が発生したかどうかを調べるには、[アクションで検索（Search by action）] セレクタから [システム（System）] > [許可（Authorization）] > [ログイン（Login）] > [失敗（Failed）] を選択します。

ステップ 3 レポート内のエントリの内容を表示するには、そのエントリをダブルクリックします。この処理によりダイアログボックスが開き、エントリに関連するメッセージが表示されます。このダイアログボックス内で、上矢印ボタンと下矢印ボタンを使用して、レポート全体をスクロールできます。

[Audit Report] ウィンドウの使用

[Audit Report] ウィンドウを使用して、Security Manager の状態変更のレコードを表示します。

[Audit Report] ページには、2 つのペインが含まれます。左側のペインを使用して、監査レポートを生成するためのパラメータを定義します。右側のペインには、監査エントリまたはメッ

セージごとに1行ずつ使用して監査レポートが表示されます。監査レポートの内容は、左側のペインで定義したパラメータによって異なります。このため、表に示されたすべてのカラムが生成済みの監査レポートに表示されるとはかぎりません。

ナビゲーション パス

[管理（Manage）] > [監査レポート（Audit Report）] を選択します。

関連項目

- 監査レポートについて （623 ページ）
- 監査レポートの生成 （623 ページ）

フィールド リファレンス

表 *117 : [Audit Report]* ウィンドウ

要素	説明
検索基準（左側のペイン） [Audit Report] ウィンドウの左側には、レポートの検索基準が表示されます。デフォルトのレポートには、昨日から今日にかけてのすべての状態変更が、新しい順に上から表示されます。	
Search by action	監査レポートに含める 1 つ以上の処理ソース。何も選択しない場合、レポートは処理に基づいてフィルタリングされません。すべての処理ソースを含める場合は、[All] を選択できます。
Search by date	レポートに含める期間。開始日から終了日までに発生した処理が表示されます。カレンダーアイコンをクリックして、日付を選択します。 このフィルタのデフォルト（リセット位置）では、昨日から今日までのアクションが含められます。
Search for activity by state	このフィールドは他の検索フィールドとは異なり、主にWorkflowモードで使用されます。このフィールドを使用して、レポートに含める 1 つ以上のアクティビティを選択できます。アクティビティは、ドロップダウンリストの下の表示ボックスに示されます。ドロップダウンリストを使用すると、レポートするアクティビティを簡単に見つけることができます。 この検索メカニズムを使用するには、レポートするアクティビティのアクティビティ状態を選択してから、アクティビティを選択します。複数のアクティビティを選択するには、Ctrl を押しながらそれらのアクティビティをクリックします。 アクティビティに基づいてフィルタリングしない場合は、[No Activity] を選択します。

要素	説明
Search by message warning level	メッセージ警告レベル。レポートには、選択した重大度のメッセージだけが表示されます。複数のレベルを選択するには、Ctrl を押しながらそれらのレベルをクリックします。
Search by user name	レポートに含める処理実行者のユーザ名。Security Manager システムにより生成された処理を表示するには、ユーザ名 System を入力します。
Search by a phrase in the message body	監査レポートエントリのメッセージ内に表示するテキスト文字列。最大 1025 文字を入力できます。 メッセージはレポート表には表示されません。エントリに関連するメッセージを表示するには、そのエントリをダブルクリックします。
Search by all or part of the object name	監査エントリが生成されたオブジェクトの名前に表示するテキスト文字列。最大 1025 文字を入力できます。
[Search] ボタン	このボタンをクリックすると、右側のペイン内にレポートが生成されます。
リセット ボタン	このボタンをクリックすると、検索条件がリセットされ、選択した値または項目がすべて削除されます。
監査レポート（右側のペイン） [Audit Report] ウィンドウの右側には、監査レポートが含まれます。それぞれの行が 1 つの監査エントリを表しています。行をダブルクリックすると、[Audit Message Details] ダイアログボックスが開きます。このダイアログボックスでは、より読みやすいレイアウトで情報が表示され、エントリに関連付けられた特定のメッセージが表示されます。[Audit Message Details] ダイアログボックス内から、レポートのエントリ全体をスクロールできます。	
Message Level	メッセージ警告レベル：[Information]、[Warning]、[Success]、[Failure]、および [Internal System Error]。
日付	処理が行われた日時。
ソース	監査エントリの送信元：[Objects]、[License]、[Admin]、[Firewall]、[Policy Manager]、[Devices]、[Topology]、[VPN]、[Config Archive]、[Deployment]、[System]、および [Activity]。
操作	実行された処理：[Add]、[Assign]、[Create]、[Delete]、[Open]、[Purge]、[Unassign]、および [Update]。

要素	説明
オブジェクト	処理のオブジェクトの ID。たとえば、カテゴリがデバイスの場合、オブジェクト ID はデバイス名または IP アドレスとなります。カテゴリが展開の場合、オブジェクト ID はジョブ名やジョブ ID などになります。特定のオブジェクト名がないこともよくあります。
ユーザー名	処理実行者のユーザ名。
アクティビティ	処理が行われたアクティビティの名前（ある場合）。
# of rows per page	各ページに表示する行数。
[<] 矢印	このボタンをクリックすると、監査レポートの直前のページに戻ります。
[>] 矢印	このボタンをクリックすると、監査レポートの次のページに進みます。

監査ログ エントリのページ

Security Manager は、ログ エントリの経過時間に基づいて、自動的に監査ログを削除します。ログのサイズを自分で管理する必要はありません。ただし、デフォルトを変更して、ログの最大サイズを拡大または縮小することにより、データベースの全体的なサイズを管理することはできます。

監査ログのデフォルト設定を変更するには、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ログ（Logs）] を選択します（[Logs] ページ （726 ページ）を参照）。ログのサイズは、エントリの最大経過日数と、ログ内の全体的な最大エントリ数によって制御されます。これらの設定は同時に機能し、ログが常に最大エントリ数を超えないように、また最大日数を経過したエントリが含まれないように、エントリは定期的に削除されます。ログの最大サイズを縮小する場合は、[今すぐ消去（Purge Now）] をクリックして、通常の削除サイクルよりも前に超過エントリを削除します。

（注） [Purge Now] ボタンは、データベースから監査レポートを削除するだけです。<install_dir>\CSCOpx\MDC\log\audit フォルダの *.csv ファイルは削除されません。これらの *.csv ファイルは、直接削除できます。

また、ログ内に取り込まれるイベントの重大度レベルを変更することによっても、ログのサイズを制御できます。たとえば、重大なイベントだけを取り込むようにすれば、ログのサイズが小さく保たれます。ただし、情報のレベルを縮小すると、ログの価値も低下する可能性があります。

関連項目

- 監査レポートについて （623 ページ）
- 監査レポートの生成 （623 ページ）
- [Audit Report] ウィンドウの使用 （624 ページ）

別のユーザの作業の引き継ぎ

管理権限を持つユーザは、Workflow 以外のモードで別のユーザの作業を引き継ぐことができます。あるユーザがデバイスおよびポリシーに対する操作を実行していて、デバイスおよびポリシーがロックされ、別のユーザが同じデバイスおよびポリシーへのアクセスを必要としている場合、別のユーザの作業を引き継ぐと便利です。

ステップ 1 [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ユーザセッションの引き継ぎ（Take Over User Session）] を選択して、[ユーザセッションの引き継ぎ（Take Over User Session）] ページを開きます（[Take Over User Session] ページ （739 ページ）を参照）。

ステップ 2 引き継ぐユーザ セッションを選択します。

ステップ 3 [セッションの引き継ぎ（Take over session）] をクリックします。選択されたユーザが行った変更が転送されます。まだコミットされていない変更はすべて廃棄されます。

選択されたユーザが変更の引き継ぎ時にログインしている場合、ユーザに警告メッセージが表示され、進行中の変更が失われて、ユーザがログアウトされます。

管理ユーザまたは他のユーザのパスワード変更

管理ユーザは、すべての Security Manager 機能にアクセスできる事前定義ユーザです。製品をインストールするときに、管理ユーザのパスワードを設定します。パスワードを忘れた場合は、次の手順を使用してパスワードを変更します。この手順は、他のユーザアカウントのパスワードをリセットする場合にも使用できます。

ステップ 1 Security Manager サーバ上の Windows にログインし、Windows コマンドライン ウィンドウを開きます。

ステップ 2 次のコマンドを使用して、デーモン マネージャ サービスを停止します。

net stop crmdmgtd

ヒント デーモン マネージャの停止と起動は、[Services] コントロール パネルを使用して行うこともできます。

ステップ 3 ユーザー名として admin を指定して、ResetPasswd.pl を実行します。この例では、製品が次のデフォルトディレクトリにインストールされていることを想定しています。別のディレクトリを使用した場合は、ディレクトリ パスを変更してください。

C:\Program Files\CSCOpx\bin\perl ResetPasswd.pl admin

新しいパスワードを入力するように求められます。

ヒント　別のユーザーのパスワードを変更する場合は、**admin** をそのユーザー名に置き換えてください。

ステップ 4 次のコマンドを使用して、デーモン マネージャ サービスを開始します。

net start crmdmgtd

Security Manager データベースのバックアップおよび復元

作業の復元が必要な場合に備えて、Security Manager データベースを定期的にバックアップする必要があります。

ヒント　Security Manager データベース バックアップには、Event Manager サービスで使用されるイベント データ ストアは含まれません。イベント管理データをバックアップする場合は、イベント データ ストアのアーカイブまたはバックアップと復元 （3516 ページ）を参照してください。

ここでは、Security Manager データベースのバックアップおよび復元の方法について説明します。

- サーバ データベースのバックアップ （629 ページ）
- サーバ データベースの復元 （632 ページ）

サーバ データベースのバックアップ

Security Manager では、CiscoWorks Common Services 機能を使用してデータベースのバックアップおよび復元を行います。Security Manager クライアントで、[ツール（Tools）] > [バックアップ（Backup）] を選択して、バックアップスケジュールを作成するための [CiscoWorks Common Services のバックアップ（CiscoWorks Common Services Backup）] ページを開きます。必要な場合にデータベースを復元できるように、定期的にデータベースをバックアップしておく必要があります。

バックアップが完了すると、Security Manager によりバックアップが圧縮されます。[CiscoWorks Common Services backup] ページで電子メール アドレスを設定した場合、バックアップおよび圧縮のプロセスが完了したことを示す通知を受け取ります。ファイル圧縮で問題が発生する場合、またはバックアップを圧縮しない場合は、バックアップ圧縮をオフに切り替えることができます。%NMSROOT%\conf フォルダ（通常は C:\Program Files\CSCOpx\conf）の backup.properties ファイルを編集し、バックアップ圧縮プロパティを VMS_FILEBACKUP_COMPRESS=NO のように変更します（YES の代わりに NO を指定します）。

ヒント　バックアップには、設定データベースおよびレポート データベースが含まれますが、イベント保管領域は含まれません。backup.properties ファイル内の SKIP_RPT_DB_BACKUP プロパティ値を YES に変更することで、レポート データベースを除外できます。YES を指定した場合でも、バックアップには、レポート スケジュールで生成されるレポートが含まれます。イベント データ ストアのバックアップについては、イベント データ ストアのアーカイブまたはバックアップと復元 （3516 ページ）を参照してください。

データのバックアップおよび復元中、Common Services と Security Manager の両方のプロセスがシャットダウンされてから再起動されます。Security Manager の再起動が完了するまでには数分かかる可能性があるため、再起動の完了前にユーザがクライアントを起動してしまうことがあります。この場合、デバイスポリシーのウィンドウに「error loading page」というメッセージが表示されることがあります。

古いバックアップを復元する前に、現在のシステムのバックアップを作成することを強く推奨します。

旧バージョンの Security Manager のバックアップに保留中のデータが含まれている場合、そのデータはまだデータベースにコミットされていないデータであるため、そのバージョンからバックアップを復元することはできません。新しいバージョンの Cisco Security Manager にアップグレードする前に、コミットされていない変更をコミットまたは廃棄してから、データベースのバックアップを作成することを推奨します。次の手順を使用すると、保留中のデータをコミットまたは廃棄する場合に便利です。

- **ワークフロー以外のモードで、次の手順を実行します。**
  - 変更をコミットするには、[ファイル（File）] > [送信（Submit）] を選択します。
  - コミットされていない変更を廃棄するには、[ファイル（File）] > [廃棄（Discard）] を選択します。

保留中のデータを持つユーザが複数存在する場合、それらのユーザの変更もコミットまたは廃棄する必要があります。別のユーザーの変更をコミットまたは廃棄する必要がある場合は、そのユーザーのセッションを引き継ぐことができます。セッションを引き継ぐには、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [ユーザーセッションの引き継ぎ（Take Over User Session）] を選択し、[セッションの引き継ぎ（Take Over Session）] をクリックします。

- **ワークフロー モードで、次の手順を実行します。**
  - 変更をコミットして承認するには、[管理（Manage）]>[アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウからアクティビティを選択し、[承認（Approve）] をクリックします。Activity Approver を使用している場合は、[送信（Submit）] をクリックして、Approver にアクティビティを承認してもらいます。
  - コミットされていない変更を廃棄するには、[管理（Manage）] > [アクティビティ（Activities）] を選択します。[Activity Manager] ウィンドウからアクティビティを選

択し、[廃棄（Discard）] をクリックします。廃棄できるのは、Edit または Edit Open の状態にあるアクティビティだけです。

また、Windows コマンド プロンプトから次のコマンドを使用してデータベースをバックアップすることもできます。

[*path*]**perl** [*path*]**backup.pl** *backup_directory* [*log_filename* [**email=***email_address* [*number_of_generations* [**compress**]]]]

構文

[*path*]**perl** [*path*]**backup.pl**	Perl スクリプト コマンド。システム パス変数内に perl コマンドおよび backup.pl ファイルへのパスが定義されていない場合は、そのパスを追加します。両方とも、通常のパスは C:\Progra~1\CSCOpx\bin\ です。
backup_directory	バックアップを作成するディレクトリ。C:\Backups などです。
log_filename	（オプション）バックアップ中に生成されたメッセージのログファイル。現在のディレクトリ以外の場所にバックアップを作成する場合は、そのパスを追加します。C:\BackupLogs などです。 名前を指定しない場合、ログは %NMSROOT%\log\dbbackup.log となります。
email=*email_address*	（オプション）通知が送信される電子メールアドレス。電子メールアドレスは指定しないが、後続のパラメータを指定する必要がある場合、等号またはアドレスを指定せずに **email** を入力します。 CiscoWorks Common Services で SMTP を設定して、通知をイネーブルにする必要があります。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）を参照してください。
number_of_generations	（オプション）バックアップディレクトリに保存するバックアップ世代の最大数。最大数に達すると、古いバックアップが削除されます。デフォルトは 0 で、保存される世代数に制限はありません。
compress	（オプション）バックアップファイルを圧縮するかどうかを指定します。このキーワードを入力しないと、backup.properties ファイル内に VMS_FILEBACKUP_COMPRESS=NO が指定されている場合、バックアップは圧縮されません。指定されていない場合は、このキーワードを入力しなくてもバックアップは圧縮されます。バックアップは圧縮することを推奨します。

例

次のコマンドでは、現在のディレクトリに perl コマンドと backup.pl コマンドが含まれていることを想定しています。バックアップ ディレクトリ内に圧縮されたバックアップおよびログ

ファイルが作成され、admin@domain.com に通知が送信されます。圧縮パラメータを含めるには、バックアップ世代を指定する必要があります。ログ ファイル パラメータのあとに何らかのパラメータを指定した場合、その前にあるすべてのパラメータの値を含める必要があります。

```
perl backup.pl C:\backups C:\backups\backup.log email=admin@domain.com 0 compress
```

ヒント　進行中のバックアップを中止する場合は、他のバックアップを実行する前に、Security Manager のインストール ディレクトリ（通常は C:\Progra~1\CSCOpx）にある backup.LOCK ファイルを削除する必要があります。

サーバ データベースの復元

コマンドラインからスクリプトを実行することにより、データベースを復元できます。データの復元中に、CiscoWorks をシャットダウンしてから再起動する必要があります。ここでは、サーバ上のバックアップ データベースを復元する方法について説明します。バックアップおよび復元のための機能は 1 つだけであり、CiscoWorks サーバにインストールされているすべてのアプリケーションをバックアップおよび復元できます。個々のアプリケーションをバックアップまたは復元することはできません。

複数のサーバにアプリケーションをインストールした場合は、インストールされているアプリケーションに適したデータが含まれるデータベース バックアップを復元する必要があります。

ヒント　以前のリリースのアプリケーションから作成したバックアップは、このバージョンのアプリケーションへのダイレクト ローカル インライン アップグレードがサポートされているバージョンからのバックアップであれば、復元できます。アップグレードがサポートされているバージョンの詳細については、この製品リリースの『Installation Guide for Cisco Security Manager』を参照してください。

ステップ 1　コマンドラインで次のように入力して、すべてのプロセスを停止します。

net stop crmdmgtd

ステップ 2　次のように入力して、データベースを復元します。

*$NMSROOT***bin\perl** *$NMSROOT***bin\restorebackup.pl** [**-t** *temporary_directory*] [**-gen** *generationNumber*] **-d** *backup_directory* [**-h**]

引数の説明

- *$NMSROOT* —The full pathname of the Common Services installation directory (the default is C:\Program Files\CSCOpx)
- **-t** *temporary_directory*：（任意）復元プログラムで一時ファイルを保存するために使用されるディレクトリまたはフォルダ。デフォルトでは、このディレクトリは *$NMSROOT* \tempBackupData です。

- **-gen** *generationNumber*：（任意）復元するバックアップ世代番号。デフォルトでは、最新の世代です。世代 1 ～ 5 が存在する場合、5 が最新の世代となります。
- **-d** *backup_directory*：復元するバックアップが含まれるバックアップディレクトリ。
- **-h**：（任意）ヘルプを表示します。-d BackupDirectory とともに使用すると、適切な構文と、使用可能なスイートおよび世代がヘルプに表示されます。

たとえば、c:\var\backup ディレクトリから最新のバージョンを復元する場合は、次のコマンドを入力します。

C:\Progra~1\CSCOpx\bin\perl C:\Progra~1\CSCOpx\bin\restorebackup.pl -d C:\var\backup

ヒント　RME データが含まれるデータベースを復元する場合は、インベントリ データを収集するかどうか尋ねられることがあります。このデータの収集には時間がかかることがあります。No で応答して、インベントリをスケジュールするようにRMEを設定できます。RME で、[デバイス（Devices）] > [インベントリ（Inventory）] を選択します。

ステップ 3　ログファイル *NMSROOT***log\restorebackup.log** を調べて、データベースが復元されたことを確認します。

ステップ 4　次のように入力して、システムを再起動します。

net start crmdmgtd

ステップ 5　Security Manager サービス パックのインストール前にバックアップされたデータベースを復元する場合は、データベースの復元後にサービス パックを再適用する必要があります。

Cisco Technical Assistance Center 用データの生成

Cisco Technical Assistance Center（TAC）の担当者は、アプリケーションの使用中に発生する問題の識別や解決に役立てるため、さまざまなデータを送信するようにユーザに依頼することがあります。次の項を参考に必要な情報を生成できます。ただし、これらのタスクを実行するのは、TAC の指示がある場合だけにしてください。問題の解決にその情報が必ずしも必要であるとは限らないためです。

- Cisco Technical Assistance Center 用の診断ファイルの作成　（633 ページ）
- 展開ステータス レポートまたは検出ステータス レポートの生成 （636 ページ）
- Cisco Technical Assistance Center 用の差分データベース バックアップの生成 （637 ページ）

Cisco Technical Assistance Center 用の診断ファイルの作成

問題レポートの提出時に、Cisco Technical Assistance Center（TAC）の担当者により、診断ファイルの形式でシステム設定情報の提出を求められることがあります。診断ファイルは、TAC による問題の診断に役立ちます。診断ファイルの提出は、担当者から求められた場合だけでかまいません。

診断ファイルを作成する前に、レポートに記載の問題の原因となったアクションを実行してください。必要に応じて、[デバッグオプション（Debug Options）] ページ（[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デバッグオプション（Debug Options）]）で設定を変更することにより、診断ファイルの詳細レベルを調整できます。[Debug Options] ページ （656 ページ）を参照してください。

バージョン 4.7 以降、Cisco Security Manager は、新しい軽量のバリアントで診断をサポートします。このバリアント「Light Diagnostics」は基本的な情報のみを収集します。その結果、診断ファイルのサイズが小さくなり、その生成が速くなります。既存のバリアント「General Diagnostics」は、4.7 でも 4.6 以前のバージョンの場合と同じものです。

General Diagnostics ファイル

General Diagnostics ファイル（CSMDiagnostics.zip）には、次のファイルと情報が含まれています。

- コンフィギュレーション ファイル
- Apache 構成ファイルおよびログファイル
- Tomcat 構成ファイルおよびログファイル
- インストール、監査および操作のログファイル
- CiscoWorks Common Services レジストリサブツリー（[HKEY_LOCAL_MACHINE][SOFTWARE][Cisco][MDC]）
- Windows のシステム イベント ログ ファイルおよびアプリケーション イベント ログ ファイル
- ホスト環境情報（オペレーティングシステムのバージョンとインストール済みサービス パック、RAM の大きさ、すべてのボリュームのディスク容量、コンピュータ名、および仮想メモリサイズ）

GUI を使用して CSMDiagnostics.zip を作成するには、次の手順に従います。

1. Security Manager クライアントを使用して、**[ツール（Tools）] > [Security Manager Diagnostics...] > [General Diagnostics...]** を選択します。ダイアログボックスが開きます。
2. [OK] をクリックして、ファイル生成を開始します。ダイアログボックスに経過が表示されます。
3. ファイルが生成されたら、[閉じる（Close）] をクリックします。

CLI を使用して CSMDiagnostics.zip を作成するには、次の手順に従います。

1. Security Manager サーバーでコマンドラインウィンドウを開きます。
2. **~MDC\bin\CSMDiagnostics** プログラムを実行します。
3. CSMDiagnostics.zip ファイルは <*installation_location*>/MDC/etc フォルダに格納されます。<*installation_location*> は、CiscoWorks Common Services をインストールしたドライブおよ

びディレクトリです。<*installation_location*> のデフォルト値は C:\Program Files (x86)\CSCOpx です。

4. 必要に応じて、CSMDiagnostics.zip を格納する別のフォルダを指定することもできます。たとえば、**CSMDiagnostics D:\temp** のように指定できます。

5. CSMDiagnostics.zip は、作成後に移動するか名前を変更する必要があります。このファイルは 2 回目の生成時に上書きされ、1 つ前のバージョン（「_old」が追加されます）のみが保存されるためです。

（注） CLI を使用して CSMDiagnostics.zip を作成する場合は、コマンドが完了してからウィンドウを閉じる必要があります。そうしないと、その後 **CSMDiagnostics** を実行しても正常に動作しません。誤ってウィンドウを閉じた場合は、C:\Program Files\CSCOpx\MDC\etc\mdcsupporttemp フォルダを削除してから、コマンドを再試行してください。

Light Diagnostics ファイル

Light Diagnostics ファイル（CSMDiagnostics_light.zip）には、General Diagnostics ファイル（CSMDiagnostics.zip）のサブセットが含まれているため、サイズが小さく、速く生成されます。

GUI を使用して CSMDiagnostics_light.zip を作成するには、次の手順に従います。

1. Security Manager クライアントを使用して、**[ツール（Tools）] > [Security Manager Diagnostics...] > [Light Diagnostics...]** を選択します。ダイアログボックスが開きます。

2. [OK] をクリックして、ファイル生成を開始します。ダイアログボックスに経過が表示されます。

3. ファイルが生成されたら、[閉じる（Close）] をクリックします。

CLI を使用して CSMDiagnostics_light.zip を作成するには、次の手順に従います。

1. Security Manager サーバーでコマンドラインウィンドウを開きます。

2. <*installation_location*>\MDC\diagnostics\script>rundiag.bat コマンドを実行します。<*installation_location*> は、CiscoWorks Common Services をインストールしたドライブおよびディレクトリです。<*installation_location*> のデフォルト値は C:\Program Files (x86)\CSCOpx です。

3. 次の 3 つのパラメータを含むコマンドを、示されている順序で実行してください。

3.1. Installation Folder：Security Manager がインストールされているフォルダ。これを変更または修正することはできません。パスにエラーがあると、診断ファイルの生成に失敗します。例: C:\PROGRA~2\CSCOpx\MDC

3.2. Destination Folder：生成後に診断ファイルが格納されるフォルダ。ファイルを保存する任意のパスとフォルダを指定できます。ファイルをデフォルトのパスに保存する場合は、デフォルトのパスを明示的に指定する必要があります。パスを指定しないと、生成時にエラーが発生します。例: C:\PROGRA~2\Light_Diagnostics

3.3. スペースのない文字列「LightDiagnostics」。この文字列ではアルファベットの大文字と小文字が区別されません。大文字または小文字を使用できますが、スペースは使用しないでください。この文字列を指定しなかった場合、General Diagnostics（つまり、Light Diagnostics ではない）ログの一部が宛先フォルダに自動的に収集されます。

1. 完全なコマンド画面の例:

C:\Program Files (x86)\CSCOpx\MDC\diagnostics\script>rundiag.bat C:\PROGRA~2\CSCOpx\MDC C:\PROGRA~2\Light_Diagnostics LightDiagnostics

展開ステータス レポートまたは検出ステータス レポートの生成

展開ジョブおよびポリシー検出ジョブについて、ステータス レポートを生成できます。展開または検出に伴う問題が発生した場合は、これらのレポートは、Cisco Technical Support（TAC）の担当者による問題の解決に役立ちます。主にレポートはトラブルシューティングのためのものですが、個人で使用するためのレポートを生成することもできます。

ステータス レポートは、ご使用のワークステーション上に Adobe Acrobat（PDF）ファイルとして生成されます（PDF ファイルを保存する場所を選択するように指示されます）。レポートには、ジョブの概要、およびそのジョブのデバイス別の概要が含まれます。展開ステータス レポートには、完全な設定とデルタ設定、および Security Manager とデバイス間通信のトランスクリプトも含まれます。

次の方法で展開レポートまたは検出レポートを生成できます。

- **展開ステータス レポート**
  - 展開ジョブが成功または失敗して完了した場合は、[展開ステータス（Deployment Status）] ダイアログボックスにある [レポートの生成（Generate Report）] ボタンをクリックします。[Deployment Status Details] ダイアログボックス （520 ページ）を参照してください。
  - 以前完了したジョブの場合は、Deployment Manager でジョブを選択して、[レポートの生成（Generate Report）] ボタンをクリックします。[Deployment Manager] ウィンドウ （499 ページ）を参照してください。
- **検出ステータス レポート**
  - 検出ジョブ（デバイスの追加時、またはインベントリにすでに存在するデバイスのポリシーを再検出する際に発生するジョブ）の実行中に、[検出ステータス（Discovery Status）] ダイアログボックスにある [レポートの生成（Generate Report）] ボタンをクリックします。[Discovery Status] ダイアログボックス （238 ページ）を参照してください。

- 以前完了したジョブの場合は、[ポリシー検出ステータス（Policy Discovery Status）] ダイアログボックスでジョブを選択して、[レポートの生成（Generate Report）] ボタンをクリックします。 [Policy Discovery Status] ページ （240 ページ） を参照してください。

Cisco Technical Assistance Center 用の差分データベース バックアップの生成

注意 この項では、差分データベース バックアップの作成方法について説明します。差分バックアップは不完全なものであり、これをフル バックアップの代わりとしては使用できません。差分バックアップは、トラブルシューティングでの使用に限定されます。Cisco Technical Assistance（TAC）の担当者が指示した場合にかぎり、生成するようにしてください。

差分データベースバックアップには、定期バックアップと同じ特徴がありますが、それよりも限定されたデータ セットです。差分バックアップを作成する場合は、Configuration Archive のデータを含めるかどうか確認され、含める場合は、（デバイス単位に）アーカイブのバージョンをいくつ分含めるか確認されます（定期バックアップには Configuration Archive 全体が含まれます）。定期バックアップの説明については、サーバ データベースのバックアップ （629 ページ）を参照してください。

ヒント 差分バックアップでは、サーバデータベースのバックアップ（629 ページ）に説明されているように、backup.properties ファイルの設定に基づいてレポート データベースを含めたり、除外したりします。

データのバックアップおよび復元中、Common Services と Security Manager の両方のプロセスがシャットダウンされてから再起動されます。Security Manager の再起動が完了するまでには数分かかる可能性があるため、再起動の完了前にユーザがクライアントを起動してしまうことがあります。この場合、デバイスポリシーのウィンドウに「error loading page」というメッセージが表示されることがあります。差分バックアップを復元しようとする場合、システムにより、それが差分バックアップであることが指摘されるため、ユーザは差分バックアップの復元を行うことを確認する必要がある点に注意してください。

差分バックアップを生成するには、Security Manager サーバ上の Windows コマンド プロンプトで次のコマンドを使用します。

[*path*]**perl** [*path*]**partial_backup.pl** *backup_directory* [*log_filename* [**email**=*email_address* [*number_of_generations* [**compress**]]]]

構文

[*path*]**perl** [*path*]**partial_backup.pl**	Perl スクリプト コマンド。システムパス変数内に perl コマンドおよび partial_backup.pl ファイルへのパスが定義されていない場合は、そのパスを含めます。両方とも、通常のパスは C:\Progra~1\CSCOpx\bin\ です。
backup_directory	バックアップを作成するディレクトリ。C:\Backups などです。
log_filename	（オプション）バックアップ中に生成されたメッセージのログファイル。現在のディレクトリ以外の場所にバックアップを作成する場合は、そのパスを追加します。C:\BackupLogs などです。 名前を指定しない場合、ログは %NMSROOT%\log\dbbackup.log となります。
email=*email_address*	（オプション）通知が送信される電子メールアドレス。電子メールアドレスは指定しないが、後続のパラメータを指定する必要がある場合、等号またはアドレスを指定せずに **email** を入力します。 CiscoWorks Common Services で SMTP を設定して、通知をイネーブルにする必要があります。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）を参照してください。
number_of_generations	（オプション）バックアップディレクトリに保存するバックアップ世代の最大数。最大数に達すると、古いバックアップが削除されます。デフォルトは 0 で、保存される世代数に制限はありません。
compress	（オプション）バックアップファイルを圧縮するかどうかを指定します。このキーワードを入力しないと、backup.properties ファイル内に VMS_FILEBACKUP_COMPRESS=NO が指定されている場合、バックアップは圧縮されません。指定されていない場合は、このキーワードを入力しなくてもバックアップは圧縮されます。バックアップは圧縮することを推奨します。

例

次のコマンドでは、現在のディレクトリに perl コマンドと partial_backup.pl コマンドが含まれていることを想定しています。バックアップディレクトリ内に圧縮された差分バックアップおよびログ ファイルが作成され、admin@domain.com に通知が送信されます。圧縮パラメータを含めるには、バックアップ世代を指定する必要があります。ログ ファイル パラメータのあとに何らかのパラメータを指定した場合、その前にあるすべてのパラメータの値を含める必要があります。また、Configuration Archive を含めるかどうか確認されることも留意してください。含める場合は、バックアップに含めるアーカイブ バージョンの数が確認されます。この例では、デバイス単位に 5 つのアーカイブ バージョンをバックアップに含めます。

```
perl partial_backup.pl C:\backups C:\backups\pbackup.log email=admin@domain.com 0 compress
Root: c:\backups
```

```
Do you also want to take config-archive backup(Yes/No): Yes
How many previous config-archive you want to restore: 5
```

第 11 章

Security Manager の管理設定値の設定

Security Manager には、数多くのシステム機能に対してデフォルト設定が用意されています。組織のニーズに合わない場合は、これらの設定を変更できます。これらの設定を表示および変更するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択します。次に、ウィンドウの左側にあるコンテンツテーブルから項目を選択して、その項目に関するデフォルト設定を表示できます。

ほとんどのページで、設定を変更する場合は、[Save] をクリックして変更を保存する必要があります。間違えた場合は、[リセット（Reset）] をクリックして、以前に保存した値に戻すことができます。また、[デフォルトを復元（Restore Defaults）] をクリックして、Security Manager のデフォルト設定に戻すこともできます。

[Security Manager管理（Security Manager Administration）] ウィンドウには、システムのデフォルトが含まれたページ以外に、システム管理アクティビティに関連する項目（別のユーザの作業を引き継ぐ、サーバーセキュリティ作業を実行するために Common Services 内のページにアクセスするなど）が含まれています。

次の項では、[Security Manager Administration] ウィンドウで使用できる各ページ上で使用可能な設定とアクションについて説明します。

- [API設定（API Settings）] ページ （642 ページ）
- [自動リンク設定（AutoL-ink Settings）] ページ （643 ページ）
- [ACLヒットカウント設定（ACL Hit Count Settings）] ページ （644 ページ）
- [CCO設定（CCO Settings）] ページ （645 ページ）
- [Configuration Archive] ページ （649 ページ）
- [CS-MARS] ページ （650 ページ）
- [CSM Mobile] ページ （653 ページ）
- [Customize Desktop] ページ （654 ページ）
- [Debug Options] ページ （656 ページ）
- [Deployment] ページ （658 ページ）
- [Device Communication] ページ （668 ページ）
- [Device Groups] ページ （673 ページ）
- [Discovery] ページ （674 ページ）
- [Event Management] ページ （677 ページ）

- [Health and Performance Monitor] ページ （690 ページ）
- [Report Manager] ページ （692 ページ）
- [Identity Settings] ページ （693 ページ）
- [Image Manager] ページ （695 ページ）
- [IPインテリジェンス設定（IP Intelligence Settings）] ページ （696 ページ）
- [イベント通知設定（Eventing Notification Settings）] ページ （701 ページ）
- [IPS Updates] ページ （705 ページ）
- [ISE設定（ISE Settings）] ページ （718 ページ）
- Licensing ページ （719 ページ）
- [Logs] ページ （726 ページ）
- [Policy Management] ページ （729 ページ）
- [Policy Objects] ページ （732 ページ）
- [プロセスモニタリングの設定（Process Monitoring Settings）] ページ （733 ページ）
- [シングルサインオンの設定（Single Sign-on Configuration）] ページ （735 ページ）
- [Rule Expiration] ページ （736 ページ）
- [Server Security] ページ （737 ページ）
- [Take Over User Session] ページ （739 ページ）
- [チケット管理（Ticket Management）] ページ （740 ページ）
- [Token Management] ページ （742 ページ）
- [VPN Policy Defaults] ページ （743 ページ）
- [Workflow] ページ （745 ページ）
- [ウォール設定（Wall Settings）] ページ （747 ページ）

[API設定（API Settings）] ページ

Cisco Security Manager の [API設定（API Settings）] ページでは、API サービスを有効または無効にして、サービスの設定を変更できます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [API] を選択します。

フィールド リファレンス

表 118 : [API設定（API Settings）] ページ

要素	説明
API サービスの有効化	API サービスを有効にするか無効にするかを指定します。

要素	説明
結果セットのページサイズ（Result Set Page Size）	許容値は 100 から 1000 までです。
アクティブクライアントセッション数（Active client sessions）	許容値は 1 から 10 までです。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[自動リンク設定（AutoL-ink Settings）] ページ

Security Manager のマップ ビューでは、VPN およびレイヤ 3 ネットワーク トポロジのグラフィカル ビューが提供されます。管理対象デバイスを表すデバイス ノード、および管理対象外のオブジェクト（デバイス、クラウド、ネットワークなど）を表すマップ オブジェクトを使用して、ネットワークの調査に使用するトポロジマップを作成できます。自動リンク設定を使用すると、5つのプライベート ネットワークまたは予約済みネットワークのいずれかをマップ ビューから除外できます。たとえば、Security Manager を使用して実行する管理タスクとは関係ないテスト ネットワークを除外する必要がある場合があります。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [自動リンク（AutoLink）] を選択します。

関連項目

- マップにおけるレイヤ 3 リンクの追加と管理 （2072 ページ）
- マップでのネットワークの表示 （2065 ページ）

フィールド リファレンス

表 119 : [AutoLink] ページ

要素	説明
Enable AutoLink for 10.0.0.0/8 Enable AutoLink for 172.16.0.0/12 Enable AutoLink for 192.168.0.0/16	作成したマップで、これらのプライベート ネットワークを自動的に含めるか、または除外する（選択解除する）かを指定します。

要素	説明
Enable AutoLink for 127.0.0.0/8	作成したマップで、このループバック ネットワークを自動的に含めるか、または除外する（選択解除する）かを指定します。
Enable AutoLink for 224.0.0.0/4	作成したマップで、マルチキャスト ネットワークを自動的に含めるか、または除外する（選択解除する）かを指定します。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[ACLヒットカウント設定（ACL Hit Count Settings）] ページ

Security Manager の [ACLヒットカウント設定（ACL Hit Count Settings）] ページでは、ヒットカウントの設定を構成および変更できます。この機能は、ASA および ASASM デバイスの Security Manager バージョン 4.9 以降で使用できます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Managerの管理（Cisco Security Manager Administration）] をクリックし、コンテンツテーブルから [ACLヒットカウント設定（ACL Hit Count Settings）] を選択します。

フィールド リファレンス

表 *120 :* ヒットカウント設定

要素	説明
[ヒットカウント履歴の持続制限（ACE単位）（Hit Count History Persist Limit (per ACE)）]	[ヒットカウント履歴の持続制限（ACE単位）（Hit Count History Persist Limit (per ACE)）] は、データベース内の特定の ACE に関して保存できるヒットカウント履歴の詳細情報に対する制限です。デフォルト値は 5 で、入力可能な最大値は 10 です。
[消去スケジューラの処理時間（Purge Scheduler Process Time）]	[消去スケジューラの処理時間（Purge Scheduler Process Time）] は、ヒットカウントスケジューラによって、毎日指定された時刻にヒットカウント消去ジョブをスケジュールするために使用されます。ドロップダウンリストから時刻を選択します。デフォルトは [12 AM] です。

（注） 画面間を移動した後に ACL ポリシーページに移動すると、すべての ACL ルールについて、[HitCount] および [LastHitTime] の値にそれぞれ [0] および [なし（Never）] が表示されます。実際の [HitCount] および [LastHitTime] の値を取得するには、ACL ポリシーページの [ヒットカウントの更新（Refresh Hit Count）] ボタンをクリックします。値はデータベースから取得され、すべての ACL ルールに表示されます。

[CCO設定（CCO Settings）] ページ

[CCO設定（CCO Settings）] ページを使用して、Cisco.com への接続に使用する設定を構成します。

証明書の信頼管理にも [CCO設定（CCO Settings）] ページを使用します（Security Manager は、HTTPS 経由で Cisco.com から ASA イメージをダウンロードし、信頼を確立するために証明書を使用します）。[Image Manager] ページの証明書信頼管理機能は、Security Manager 4.4 の新機能です。この機能は、ASA イメージのダウンロードに向けた Cisco.com 証明書の処理を改善するのに役立ちます。

- この機能を使用して証明書を表示できます。証明書を受け入れるかどうか慎重に検討してください。
- 証明書を受け入れると、証明書は Security Manager サーバーに保存されます。
- [Image Manager] ページの概要テーブルにすべての証明書が表示され、そのテーブルを使用して証明書を表示または削除できます。

ヒント 下のテーブルの [証明書の取得（Retrieve Certificate）] を必ず確認してください。

証明書信頼管理機能の詳細については、証明書信頼管理 （620 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [CCO設定（CCO Settings）] を選択します。

フィールド リファレンス

表 *121 : [CCO*設定（*CCO Settings***）*]* ページ**

要素	説明
[IPS更新設定を使用（Use IPS Updates Settings）]	オンにすると、このページの他の設定が無効になり、デフォルトが優先されるようになります（[IPSの更新（IPS Updates）] ページの Cisco.com ログイン情報が適用されます）。 **注意** オンにした場合、[IPSの更新（IPS Updates）] ページの Cisco.com ログイン情報が正しく設定されていることを確認してください。ページ上の [更新元：（Update From:）] のデフォルト値は [ローカルサーバー（Local Server）] です。証明書の設定を表示するには、[Cisco.com] を選択する必要があります。証明書の設定が不適切または不完全な場合、Cisco.com への接続が妨げられ、このエリアでの Cisco.com 関連のすべての操作が失敗します。
ユーザー名	Security Manager が Cisco.com にログインするときに使用するユーザー名。
パスワード 確認（Confirm）	ユーザー名のパスワード。両方のフィールドにパスワードを入力します。
プロキシ サーバーの設定	
[プロキシの有効化（Enable Proxy）]	Image Manager が Web プロキシサーバー経由で Cisco.com に接続できるようにします。[プロキシの有効化（Enable Proxy）] を選択すると、他のプロキシフィールド（[IP] または [ホスト名（Hostname）]、[ポート（Port）]、[ユーザー名（Username）]、および[パスワード（Password）] など）が有効になり、Web プロキシへの接続に使用されます。
テスト接続（Test Connection）	Cisco.com の接続とログイン情報をテストするために使用されます。
証明書	

要素	説明
[連絡先URL（Contact URL）]	• 選択すると、[イメージメタデータロケータ（Image Meta-data Locator）] が使用されます。これは、イメージに関するメタデータ情報の取得に使用される Cisco.com の URL です。メタデータ情報は、特定の製品に該当するイメージ、名前、サイズ、チェックサム、および各イメージをダウンロードする URL で構成されます。 • 選択すると [その他（Other）] が使用されます。任意の有効な HTTPS URL を入力できます。この URL は、主に、イメージに関するメタデータ情報から取得したイメージをダウンロードするための HTTPS URL を対象としています。この URL は、前の段落で説明したイメージメタデータロケータの URL とは異なる場合があります。証明書も異なる場合があります。 **注意** [その他（Other）] を選択した場合は、明示的に "https://dl.cisco.com" を追加する必要があります（引用符は不要）。[その他（Other）] ボタンの隣のテキストフィールドに入力します。これを追加しないと、Cisco.com に接続できなくなり、このエリアでの Cisco.com 関連のすべての操作が失敗します。

要素	説明
[証明書の取得（Retrieve Certificate）]	選択した [連絡先URL（Contact URL）] に接続して証明書を取得するために使用されます。証明書を取得すると、[証明書の検証（Certificate Verification）] ダイアログが開きます。証明書の簡単な概要、つまり、証明書の発行対象、発行者、証明書の有効期間が表示されます。さらに、次の選択肢が表示されます。 • [証明書の表示（View Certificate）]：証明書ビューアを開いて、証明書のすべての詳細（認証局、バージョン、シリアル番号、サムプリント、その他の詳細）を表示できます。ルート発行認証局までの完全な証明書チェーン情報が表示されます。 • [承認（Accept）]：証明書を承認して、Cisco Security Manager に追加します。 • [拒否（Reject）]：証明書を拒否します。アクションは実行されません。 • [キャンセル（Cancel）]：アクションを実行せずに [証明書の検証（Certificate Verification）] ダイアログを閉じます。 次の推奨される証明書を表示して承認する必要があります。 • https://www.cisco.com/ • https://www.dl3.cisco.com • https://www.cloudsso.cisco.com • https://www.api.cisco.com
証明書	Security Manager インストールの各証明書について、[情報カテゴリ（Subject）]、[発行者（Issued By）]、および [承認者（Accepted By）] を表示するテーブル。
表示（View）	[証明書（Certificate）] テーブルで選択した証明書の証明書ビューアを開きます。
削除（Remove）	[証明書（Certificate）] テーブルで選択した証明書を削除します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Configuration Archive] ページ

[Configuration Archive] ページを使用して、Configuration Archive ツールのデフォルト設定（保存する設定バージョンの数、Cisco IOS ソフトウェア デバイス設定のロールバックに使用する TFTP サーバなど）を定義します。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [設定アーカイブ（Configuration Archive）] を選択します。

関連項目

- [Configuration Archive] ウィンドウ （509 ページ）
- 設定のロールバック （560 ページ）

フィールド リファレンス

表 *122 : [Configuration Archive]* ページ

要素	説明
[デバイスごとの最大バージョン数（Max. Versions per Device）] [Purge Now] ボタン Enable Configuration Archive Versions Auto Purge	各管理対象デバイスで維持する設定バージョン数（1 ～ 100）。この数を減らした場合は、[今すぐ消去（Purge Now）] をクリックして、余分なバージョンをすぐに削除できます。 このオプションを使用してファイルを消去すると、**C:\Program Files (x86)\CSCOpx\MDC\tomcat\vms\athena\transcript** フォルダから、追加の設定バージョンに対応するトランスクリプトファイルが削除されます。ただし、消去後は、削除されたバージョンに関連するトランスクリプトファイル（対応する展開ジョブにも関連）は表示できません。トランスクリプトファイルを表示しようとすると、それらが削除されているため、「**Unable to Display Transcript（トランスクリプトを表示できません）**」というエラーが表示されます。 。 [設定アーカイブバージョンの自動消去を有効にする（Enable Configuration Archive Versions Auto Purge）] オプションを指定している場合、Security Manager は、通常のクリーンアップサイクル中に余分なバージョンを自動的に削除します。

要素	説明
TFTP Server for Rollback	TFTP ファイル転送に使用するサーバの完全修飾 DNS ホスト名または IP アドレス。TFTP は、設定を更新できなかった場合に、**configure replace** コマンドを使用して IOS をロールバックするときに使用されます。このとき、システムのリロードは発生しません。Security Manager サーバーを使用するには、**localhost** を入力します。 TFTP サーバは、Security Manager サーバ上でデフォルトでイネーブルになっています。リモート TFTP サーバを指定する場合は、TFTP サービスを適切に提供するように、そのサーバを設定する必要があります。
TFTP Root Directory	Security Manager サーバを TFTP サーバとして使用している場合の、設定ファイル転送用のルート ディレクトリ。[参照（Browse）] をクリックして、Security Manager サーバー上のディレクトリを選択します。 Security Manager サーバ以外のサーバを TFTP ホストとして指定する場合、Security Manager は、その TFTP サーバのルート ディレクトリを常に使用します。リモート TFTP サーバのルート以外のディレクトリは指定できません。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[CS-MARS] ページ

[CS-MARS] ページを使用して、Cisco Security Monitoring, Analysis and Response System サーバを登録します。このサーバは、Security Manager を使用してデバイスをモニタします。CS-MARS サーバーを登録すると、Security Manager で設定されているデバイスのファイアウォール アクセス ルールまたは IPS シグニチャルールに基づいて CS-MARS でキャプチャされたメッセージとイベントを表示できます。CS-MARS サーバを登録しないと、ユーザは CS-MARS から収集されたイベントを表示できません。

ヒント CS-MARS Global Controller を使用している場合は、個別の Local Controller ではなく Global Controller を追加します。Global Controller を追加することによって、各 Local Controller を追加しなくても、Security Manager でデバイスの正しい Local Controller を識別できます。これにより、Security Manager における CS-MARS の設定が簡素化されます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [CS-MARS] を選択します。

関連項目

- Security Manager での CS-MARS サーバの登録 （3730 ページ）

フィールド リファレンス

表 *123 : [CS-MARS]* ページ

要素	説明
CS-MARS Devices	Security Manager に登録する CS-MARS サーバ。 • サーバを追加するには、[Add]（+）ボタンをクリックし、[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス （652 ページ）に入力します。 • サーバを編集するには、サーバを選択し、[Edit]（鉛筆）ボタンをクリックします。 • サーバを削除するには、そのサーバを選択し、[Delete]（ゴミ箱）ボタンをクリックします。サーバを削除すると、そのサーバを使用するすべてのデバイスのデバイス プロパティが更新され、そのサーバ接続が削除されます。リスト上の別のCS-MARSサーバもデバイスをモニタしている場合は、別のサーバを指し示すようにデバイスのプロパティが更新されます。
When Launching CS-MARS Allow User to Save Credentials	Security Manager が、イベント情報の取得時に CS-MARS にログインするために使用するクレデンシャルのタイプ： • [ユーザーのプロンプト（Prompt users）]：ユーザーは、CS-MARS からイベント情報を取得しようとするときに、CS-MARS にログインするように要求されます。このオプションを選択する場合は、[ユーザーによるクレデンシャルの保存を許可（Allow User to Save Credentials）] も選択する必要があります。選択すると、ユーザーのクレデンシャルを保存するオプションがユーザーに表示されるため、ユーザーは、次回イベントステータスを要求したときにCS-MARSに再度ログインする必要がなくなります。 • [CS-Managerクレデンシャルを使用（Use CS-Manager Credentials）]：ユーザーは、CS-MARS からイベント情報を取得しようとするときに、Security Manager へのログインに使用しているのと同じユーザー名とパスワードを使用して CS-MARS にログインします。
[Save] ボタン	変更を保存して適用します。

要素	説明
リセット ボタン	変更を前回保存した値にリセットします。

[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス

[New CS-MARS Device] または [Edit CS-MARS Device] ダイアログボックスを使用して、Security Manager に CS-MARS サーバを登録します。ユーザーは、デバイスをモニターしている CS-MARS サーバーから、デバイスのファイアウォールまたは IPS ポリシーのメッセージやイベントステータスを取得できます。詳細については、Security Manager での CS-MARS サーバの登録（3730 ページ）を参照してください。

ナビゲーション パス

[CS-MARS] ページ （650 ページ）で、[Add] ボタンをクリックして新しいサーバを追加するか、またはサーバを選択して [Edit] ボタンをクリックします。

フィールド リファレンス

表 *124 : [Add CS-MARS Device]/[Edit CS-MARS Device]* ダイアログボックス

要素	説明
CS-MARS Hostname/IP	CS-MARS サーバの IP アドレスまたは完全修飾 DNS ホスト名。 ヒント CS-MARS Global Controller を追加する場合は、その Global Controller によってモニタされる Local Controller は追加しないでください。Security Manager によって、特定のデバイスをモニタしている Local Controller が自動的に識別されます。Global Controller を追加することによって、CS-MARS の設定が簡素化されます。
ユーザ名 パスワード ユーザー タイプ（User Type）	CS-MARS サーバが適切なソフトウェア バージョンを実行していることを検証し、その他の基本情報を取得するために、サーバにログインするときのユーザ名とパスワード。また、Security Manager では、このアカウントを使用して、特定のデバイスをモニタしている CS-MARS サーバも識別します。 CS-MARS Local Controller の場合は、グローバル ユーザ アカウントまたはローカル ユーザ アカウントを入力できます。Global Controller の場合は、グローバル アカウントを入力する必要があります。アカウントのタイプを [User Type] フィールドで指定します。

要素	説明
Certificate Thumbprint [Retrieve From Device] ボタン	CS-MARS サーバ証明書（デバイス固有の 16 進ストリング）。[デバイスから取得（Retrieve From Device）] をクリックして、Security Manager が証明書を CS-MARS サーバーから取得するようにします。 証明書は、正常に取得されると表示されます。証明書を確認した後に、[承認（Accept）] をクリックして、Security Manager サーバーにその証明書を保存します。Security Manager から CS-MARS サーバを使用するには、正しい証明書を取得している必要があります。

[CSM Mobile] ページ

[Security Manager管理（Security Manager Administration）] ウィンドウの [CSM Mobile] ページを使用して、Cisco Security Manager の CSM Mobile 機能をイネーブルまたはディセーブルにします。CSM Mobile 機能がイネーブルになっている場合、ユーザは次のリンクに移動して、モバイルデバイスからデバイスの正常性と概要の情報にアクセスできます。ここで、<SecManServer> は Security Manager サーバーの DNS 名または IP アドレスです。

https://<*SecManServer*> /mobile/

または

https://<*SecManServer*> /mobile

提供される情報のタイプの詳細については、ダッシュボードの概要（3674 ページ）を参照してください。

CSM Mobile の詳細については、CSM Mobile （3692 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [CSM Mobile] を選択します。

フィールド リファレンス

表 125 : [CSM Mobile] ページ

要素	説明
CSM モバイル機能の有効化（Enable CSM Mobile Feature）	CSM Mobile機能をイネーブルまたはディセーブルにできます。この機能をディセーブルにすると、モバイルデバイスからデバイスの正常性の概要情報にアクセスできなくなります。

要素	説明
[Save] ボタン	変更を保存して適用します。 サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。
リセット ボタン	変更を前回保存した値にリセットします。

[Customize Desktop] ページ

[デスクトップのカスタマイズ（Customize Desktop）]ページを使用して、Security Managerアプリケーションが、指定した時間アイドル状態であったあとに自動的に閉じられるかどうかを制御し、特定の状況におけるアクションを確認するようにユーザに要求するかどうかをリセットします。また特定のファイル操作を Security Manager クライアントで実行できるかどうかを制御します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デスクトップのカスタマイズ（Customize Desktop）] を選択します。

関連項目

- Security Manager のライセンス ファイルのインストール （618 ページ）
- ポリシーまたはデバイスのインポート （615 ページ）
- コマンドラインからのデバイス インベントリのエクスポート （611 ページ）
- 共有ポリシーのエクスポート （612 ページ）
- IPS ライセンス ファイルの選択 （725 ページ）

フィールド リファレンス

表 126 : [Customize Desktop] ページ

要素	説明
[警告の「Do Not Ask」のリセット（Reset "Do Not Ask" on Warnings）] ボタン	このボタンをクリックして、「Are you sure...?」ポップアップ警告を再設定します。一部のアクションを実行すると、結果に関する警告が表示され、警告が再度表示されないようにするオプションが提示されます。これらの警告のいずれかに対して [Do Not Ask Me Again] を選択している場合、このボタンをクリックすると、警告が再度イネーブルになります。

要素	説明
Enable Idle Timeout Idle Timeout (minutes)	指定した期間、Security Manager クライアント アプリケーションを使用しなかった場合に、クライアントを自動的に終了するかどうかを指定します。タイムアウトはすべてのアプリケーションにわたって適用され、1 つのアプリケーションで操作するとすべてのアプリケーションのタイマーがリセットされます。 このオプションを選択する場合は、クライアントを閉じるまでに経過する必要がある時間を分単位で [Idle Timeout] フィールドに入力します。デフォルトでは、クライアントは、非活動状態が 120 分続いたあとに閉じられます。
Enable Client side file browser	Security Manager クライアントでファイル操作を許可するかどうか。このオプションが選択されている場合、次のファイル操作を実行するときに、クライアント ファイル システムとサーバ ファイル システムを選択できます。 • Security Manager のライセンス ファイルのインストール • IPS ライセンスファイルのインストール • デバイス インベントリ ファイルのインポート/エクスポート • 共有ポリシーのインポート/エクスポート • 次のファイル オブジェクトの作成 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • AnyConnect Profile • AnyConnect Image • Hostscan Image このオプションは、デフォルトで有効です。
[グローバル検索（Global Search）]	
グローバル検索の有効化	グローバル検索機能を有効にするか無効にするか。この機能はデフォルトでイネーブルになっています。 ヒント　パフォーマンスを向上させるために、デバイスの一括検出または再検出を実行する前にグローバル検索を無効にすることができます。検出が完了した後、またはユーザーがシステムを使用する可能性が最も低いときに、グローバル検索を再度有効にしてインデックスを再作成できます。

要素	説明
インデックスの再作成	このボタンをクリックして、検索インデックスを再生成します。インデックスの再作成中は、グローバル検索機能を使用できません。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Debug Options] ページ

[Debug Options] ページを使用して、デバッグ ログに含めるメッセージの重大度を設定し、収集するその他のデバッグ情報を指定します。

デバッグ レベルは、Cisco Technical Assistance Center（TAC）から変更を指示された場合にだけ変更してください。これにより、より詳細な情報を CSMDiagnostics.zip ファイルに含めることができるようになります。

該当するサブコンポーネントのメッセージ レベルを変更したあと、システムの問題を引き起こすアクションを再実行します。問題が発生した後、次の順番で選択して、CSMDiagnostics.zip ファイル（または CSMDiagnostics_light.zip ファイル）を作成します。**[ツール（Tools）] > [Cisco Security Managerの診断...（Security Manager Diagnostics,,,）] > [一般的な診断...（General Diagnostics...）]**（または **[ツール（Tools）] > [Cisco Security Managerの診断...（Security Manager Diagnostics...）] > [Light Diagnostics...]**。次に、デバッグ オプションをデフォルト レベルにリセットして、Security Manager サーバが、余分なデバッグ情報の収集が原因でダウンしないようにします。CSMDiagnostics.zip ファイルの生成の詳細については、Cisco Technical Assistance Center 用の診断ファイルの作成 （633 ページ）を参照してください。

デフォルトでは、重大度がエラーであるか、より高いメッセージがログに含められます。重大度（重大度の高い順）：

- [Severe]：システムが使用できなくなる問題。
- [Error]：Security Manager によって復元できない問題。
- [Warning]：Security Manager による復元が可能な、予期しない状況。
- [Info]：情報メッセージ。
- [Debug]：内部ステータス情報。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [デバッグオプション（Debug Options）] を選択します。

フィールド リファレンス

表 *127 : [Debug Options]* ページ

要素	説明
Capture Discovery/Deployment Debugging Snapshots to File	Security Managerが、設定の生成、展開、および検出が実行されたときに、これらの機能に関するデータ ファイルを生成するかどうかを指定します。一時的なデータ ファイルが、サーバ上の Security Managerインストール フォルダ内の MDC\temp ディレクトリに格納されます。これらのファイルをデバッグに使用できます。 展開または検出に関する問題が発生した場合に、この設定をイネーブルにします。 （注） このチェックボックスをオンにすると、Security Manager の応答時間が遅くなります。このオプションは、限られた状況でだけイネーブルにします。 これらのファイルをデバッグのために Cisco TAC に送信する場合は、パスワードなどの機密データが含まれている可能性があるため、暗号化します。 （注） 検出（または）展開の進行中は、Cisco Security Manager インストールフォルダの MDC\temp ディレクトリにあるスナップショットファイルを削除しないでください。スナップショットファイルは、Cisco Security Manager がアイドル状態のときに削除できます。また、デフォルトのファイルを削除していないことを確認してください。
Deployment Debug Level	展開関連のアクション（デバイス通信など）のメッセージの重大度。
Event Manager Debug Level	Event Manager サブシステムのメッセージの重大度。
Health and Performance Monitor のデバッグレベル（Health and Performance Monitor Debug Level）	Health and Performance Monitor サブシステムのメッセージ重大度レベル。
Image Managerのデバッグレベル（Image Manager Debug Level）	Image Manager サブシステムのメッセージの重大度。
Firewall Services Debug Level	ファイアウォール関連ポリシーのメッセージの重大度。
IOS Platform Debug Level	Cisco IOS ソフトウェア プラットフォーム ポリシーのメッセージの重大度。

要素	説明
PIX Platform Debug Level	PIX、ASA、および FWSM プラットフォーム ポリシーのメッセージの重大度。
Report Manager Debug Level	Report Manager サブシステムのメッセージの重大度。
VPN Services Debug Level	VPN サービス ポリシーのメッセージの重大度。
APIのデバッグレベル（API Debug Level）	アプリケーション プログラミング インターフェイス サブシステムのメッセージ重大度レベル。
[Save] ボタン	変更内容を保存します。
リセット ボタン	すべてのフィールドを以前の値に復元します。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Deployment] ページ

[Deployment] ページを使用して、Security Manager がデバイスに設定を展開するデフォルトの方式を定義します。展開ジョブの作成時に、これらの設定の一部をオーバーライドできます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [展開（Deployment）] を選択します。

関連項目

- 展開の管理 （481 ページ）
- ポリシー オブジェクトの管理 （287 ページ）

フィールド リファレンス

表 *128 : [Deployment]* ページ

要素	説明
一般的なパラメータ	

要素	説明
スナップショットパージ設定 Purge Debugging Files Older Than (days)	システムがデバッグ ファイルを保持する最大日数。デバッグ ファイルは自動的に削除されます。この日数を減らした場合、[今すぐパージする（Purge Now）] をクリックして、指定した日数よりも古いすべてのデバッグファイルをすぐに削除できます。 （注） パージする場合、Security Manager は、[デバッグオプション（Debug Options）] ページの [検出/展開デバッグスナップショットのファイルへのキャプチャ（Capture Discovery/Deployment Debugging Snapshots to File）] チェックボックスが有効になった後に作成されたデバッグファイルのみを考慮します。
Default Deployment Method ディレクトリ	デバイスに設定を展開するためのデフォルト方式として使用する方式。 • [Device]：設定をデバイスに直接展開するか、またはデバイスに指定された転送メカニズムに展開します。詳細については、デバイスへの直接展開 （491 ページ）を参照してください。 • [File]：Security Manager サーバ上のディレクトリに設定ファイルを展開します。[File] を選択する場合は、設定ファイルの展開先ディレクトリを [Destination] カラムで指定します。ファイルをデフォルトとして選択しても、IPS デバイスには設定が適用されません。IPS デバイスについては、デバイス展開だけを使用できます。詳細については、ファイルへの展開 （493 ページ）を参照してください。 展開ジョブを作成するときに、この方式をオーバーライドできます。

要素	説明
When Out of Band Changes Detected	Security Manager が、設定がデバイスに最後に展開されたあとに、デバイスの CLI で変更が直接行われたことを検出したときに、対応するかどうかを指定します。アウトオブバンド変更の検出は、ファイルではなくデバイスに展開するときにだけ正しく機能し、デバイスから参照設定を取得するように設定された展開方式に対してだけ適用されます（参照設定の設定値については、後述の説明を参照してください）。 この設定によって、デフォルトのアクションが指定されます。デフォルトのアクションは、展開ジョブの作成時にオーバーライドできます。次のいずれかを選択できます。 • [変更を上書きして警告を表示（Overwrite changes and show warning）]（デフォルト）：デバイスに対して手動で変更を行った場合、Security Manager は、展開を続行し、変更を上書きし、このアクションを通知する警告を表示します。 • [展開をキャンセル（Cancel deployment）]：デバイスに対して手動で変更を行った場合、Security Manager は展開をキャンセルし、このアクションを通知する警告を表示します。 • [変更を確認しない（Do not check for changes）]：Security Manager は、変更内容を確認せずにデバイスに展開し、ローカルの変更を上書きします。 アウトオブバンド変更の処理の詳細な説明については、アウトオブバンド変更の処理方法について （494 ページ）を参照してください。 （注） フェールオーバーが設定されていないデバイスの場合、帯域外の変更が検出されたときに [展開をキャンセル（Cancel Deployment）] オプションを選択すると、ブートストラップ設定によって展開が失敗する可能性があります。展開を成功させるには、Security Manager でデバイスを検出する前にフェールオーバーを設定する必要があります。
Deploy to File Reference Configuration	Security Manager サーバ上のファイルに設定を展開するときに、Security Manager が、デバイスの以前の設定と新しいポリシーを比較するために使用する設定。 • [Archive]（デフォルト）：最後にアーカイブされた設定。 • [Device]：現在実行中のデバイスの設定。デバイスから取得されます。 設定を比較したあとで、Security Manager によって、展開する適切な CLI が生成されます。

要素	説明
Deploy to Device Reference Configuration	デバイス（または転送サーバ）に設定を直接展開するときに、Security Manager が、デバイスの以前の設定と新しいポリシーを比較するために使用する設定。 • [Archive]：最後にアーカイブされた設定。 • [Device]（デフォルト）：現在実行中のデバイスの設定。デバイスから取得されます。 設定を比較したあとで、Security Manager によって、展開する適切な CLI が生成されます。
Allow Download on Error	軽微なデバイス設定エラーがある場合でも、デバイスへの展開を継続するかどうかを指定します。
Save Changes Permanently on Device	設定をデバイスに展開したあとに（**write memory** コマンドを使用して）、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するかどうか。これは、PIX、FWSM、ASA、または Cisco IOS の各デバイスに適用されます。このチェックボックスをオフにすると、スタートアップ コンフィギュレーションは変更されません。これは、デバイスが何らかの理由でリロードされると設定の変更内容が失われることを意味します。
Preselect Devices with Undeployed Changes	展開ジョブの作成時に確認する、変更されたデバイスのリストで、変更されたすべてのデバイスを選択済みとするかどうかを指定します。このオプションの選択を解除すると、ユーザは、デバイスを手動で選択して展開ジョブに含める必要があります。
Enable Auto Refresh in Deployment Main Panel	展開ジョブおよびスケジュール ステータス情報が、[Deployment Manager] ウィンドウで自動的にリフレッシュされるかどうかを指定します。このオプションの選択を解除すると、[Refresh] ボタンをクリックして、情報を手動でリフレッシュする必要があります。
Remove Unreferenced SSL VPN Files on Device （ASA のみ）	SSL VPN 設定に関連するファイルが、デバイスの SSL VPN 設定によって現在は参照されていない場合に、Security Manager がこれらのファイルを削除するかどうか。このオプションの選択を解除すると、使用されていないファイルは、展開後にデバイス上に残ります。

要素	説明
Mask Passwords and Keys When Viewing Configs and Transcripts Mask Passwords and Keys When Deploying to File	Security Manager が、次の項目をマスクして、読み取られないようにする条件（ある場合）：ユーザ、イネーブル モード、Telnet、およびコンソールのパスワード。SNMP コミュニティ ストリング。TACACS+、事前共有キー、RADIUS サーバ、ISAKMP、フェールオーバー、Web VPN 属性、ロギング ポリシー属性、AAA、AUS、OSPF、RIP、NTP、ロギング FTP サーバ、ポイントツーポイント プロトコル、ストレージ キー、シングル サインオン サーバ、ロード バランシング、HTTP/HTTPS プロキシ、および IPSEC 共有キーなどのキー。 • [Mask Passwords and Keys When Viewing Configs and Transcripts]：このオプションは、クレデンシャルの画面表示だけに影響します。これにより、未認可ユーザによるクレデンシャルの表示を防ぐことができます。このオプションを選択しない場合でも、デバイスがクレデンシャルを処理する方法によっては、完全なトランスクリプトのクレデンシャルが引き続きマスクされる場合があります。 • [Mask Passwords and Keys When Deploying to File]：このオプションは、ファイルに展開される設定ファイルの内容に影響し、設定ファイルが実際のデバイスに展開できなくなります。このオプションは、これらの設定を現実のデバイスに実際に展開する必要がない場合にだけ選択します。このオプションを選択しても、クレデンシャルが表示されるときにマスクされるかどうかに影響はありません。
新規または変更された Flexconfig のみを展開する	FlexConfig の作成または変更後に FlexConfig を 1 回だけ展開するか、展開ごとにすべての FlexConfig を展開するか。このオプションは、デフォルトで選択されます。 （注） 展開ごとに展開する必要がある FlexConfig がある場合は、このオプションを無効にする必要があります。この設定を変更した後は、展開後に 1 回限りの FlexConfig を削除して管理する必要があります。
ACL パラメータ	

要素	説明
Optimize the Deployment of Access Rules For （IPv4 および IPv6 のアクセス ルール）。	ファイアウォール ルールが展開される方法。次のいずれかを選択できます。 • [Speed]（デフォルト）：新しい ACL と古い ACL 間のデルタ（差分）だけを送信することで、展開速度を高速化します。これは推奨オプションです。この方法では、ACL 行番号を利用することで、特定の位置にある ACE を選択して追加、更新、または削除します。ACL 全体の再送信は実行されません。編集されている ACL は使用中であるため、ACE が削除され、新しい位置に追加されるまでの間に、一部のトラフィックが不適切に処理される可能性がわずかにあります。この ACL 行番号機能は、Cisco IOS、PIX、および ASA のほとんどのバージョンでサポートされており、FWSM の場合は FWSM 3.1(1) から使用できるようになりました。 • [Traffic]：この方法によって、ACL がシームレスに切り替えられ、トラフィックの中断が回避されます。ただし、展開タスクに時間がかかり、一時 ACL が削除されるまではより多くのデバイス メモリが使用されます。最初に、一時コピーが、展開するための ACL で構成されます。この一時 ACL が、ターゲット インターフェイスにバインドされます。次に、古い ACL が元の名前を使用して再作成されますが、その内容は新しい ACL になります。この ACL も、ターゲット インターフェイスにバインドされます。この時点で、一時 ACL が削除されます。 （注） FWSM デバイスの場合は、[Let FWSM Decide When to Compile Access Lists] オプションも選択している場合にだけ、このオプションが処理に影響します。
Firewall Access-List Names （IPv4 および IPv6 のアクセス ルール）。	アクセス ルールに Security Manager での名前がない場合に、ACL 名がデバイスに展開される方法。 • [Reuse existing names]：参照設定で設定されている ACL 名を再利用します（通常は、デバイスからの名前）。 • [Reset to CS-Manager generated names]：Security Manager が自動生成した ACL 名に名前をリセットします。

要素	説明
Enable ACL Sharing for Firewall Rules （IPv4 および IPv6 のアクセス ルール）。	Security Manager が、アクセス ルール ポリシー用の単一アクセス コントロール リスト（ACL）を複数のインターフェイスと共有するかどうかを指定します。このオプションを選択しない場合、Security Manager は IPv4 および IPv6 のアクセス ルール ポリシーを適用する各インターフェイス固有の ACL を作成します。ACL の共有は、アクセス ルール ポリシーによって作成された ACL の場合にだけ行われます。 このオプションを選択すると、Security Manager は、各インターフェイスのアクセス ルール ポリシーを評価し、ポリシーの実行に必要な最小数を展開する一方で、ACL 命名要件を維持します。たとえば、1 つのインターフェイスロールを使用して 4 つのインターフェイスに同じルールを割り当てる場合は、[ファイアウォールアクセスリスト名（Firewall Access-List Names）] プロパティの [CS-Managerが生成した名前にリセット（Reset to CS-Manager generated names）] を指定し、アクセス制御設定ポリシーでインターフェイスの ACL 名は指定せずに、1 つの ACL だけを展開し、各インターフェイスでその ACL を使用するようにします。 このオプションを選択する場合は、次の点に注意してください。 • インターフェイスで、別のインターフェイスの名前が付いた ACL が使用される場合があります。 • アクセス コントロール設定ポリシーで ACL の名前を指定すると、その名前の ACL は、別のインターフェイスによって使用されている名前と同じ場合でも作成されます。このポリシーで指定された名前は、他のいずれの設定よりも優先されます。 • [ファイアウォールアクセルリスト名（Firewall Access-List Names）] プロパティの [既存の名前を再利用（Reuse Existing Names）] を選択すると、既存の名前は保存されます（アクセス制御設定ポリシーで名前をオーバーライドした場合を除く）。つまり、重複する ACL がデバイスにすでに存在する場合は、異なる名前で ACL が重複して作成されます。 • ヒット カウント統計は、インターフェイスではなく ACL に基づくため、共有 ACL により、その ACL を共有するすべてのインターフェイスから結合された統計情報が提供されます。 • ACL の共有は、FWSM など、デバイスにメモリの制約がある場合に有用です。

要素	説明
Let FWSM Decide When to Compile Access Lists （IPv4 のアクセス ルールのみ）。	Firewall Services Module（FWSM; ファイアウォール サービス モジュール）で、アクセス リストをコンパイルするタイミングを自動的に決定するかどうかを指定します。このオプションを選択すると、展開が高速化される可能性がありますが、トラフィックが中断し、システムが ACL コンパイルのエラー メッセージを報告できなくなる場合があります。このオプションを選択すると、[Optimize the Deployment of Access Rules For Traffic] 設定を使用して、トラフィックの中断の可能性を低減できます。 選択を解除すると、Security Manager は、ACL コンパイルを制御して、トラフィックの中断を回避し、デバイスにおけるピーク時のメモリ使用率を最小限に抑えます。 **注意** このオプションは、展開の問題が発生し、かつ自分が上級ユーザである場合を除き、選択しないでください。
Remove Unreferenced Access-lists on Device （IPv4 および IPv6 のアクセス ルール）。	展開時に、Security Manager が管理する他の CLI コマンドで使用されていないアクセスリストをデバイスから削除するかどうかを指定します。 （注） このオプションを有効にすると、Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないアクセスリストを、展開中に削除します。Security Manager によって検出または管理されていないポリシーがそのようなアクセスリストを使用している場合、Security Manager は展開中にそのオブジェクトを削除しようとします。これは、FlexConfig で使用され、Security Manager によって管理される他のポリシーでは使用されないアクセスリストにも適用されます。 **警告** [管理設定（Administrative Settings）] から [デバイスで参照されていないアクセスリストを削除（Remove Unreferenced Access-lists on Device）] オプションを有効にすると、Cisco Security Manager は、Security Manager によって管理または検出されたポリシーで使用されていないアクセスリストを自動的に削除します。ただし、グループポリシーの VPN フィルタが使用されている場合、[デバイスで参照されていないアクセスリストを削除（Remove Unreferenced Access-lists on Device）] オプションが有効になっていない場合でも、Security Manager は参照されていないアクセスリストを削除します。
Generate ACL Remarks During Deployment （IPv4 および IPv6 のアクセス ルール）。	展開時に、ACL の警告メッセージおよび備考を表示するかどうかを指定します。

要素	説明
Preserve Sections for Access Rules	アクセスルールを編成するセクション名を展開するかどうかを指定します。このオプションにより、デバイスが検出または再検出された場合にセクション名が失われません。
Generate CSM Rule Number	Cisco Security Manager ユーザーインターフェイスで使用されるルール番号を展開するかどうかを指定します。このオプションは、デバイス設定内のアクセスルールをルールテーブル内の位置に関連付けるのに役立ちます。
オブジェクト グループ パラメータ	
Remove Unreferenced Object Groups from Device (PIX, ASA, FWSM, IOS 12.4(20)T+) （IPv4 オブジェクトおよび IPv6 オブジェクト）。	Security Manager が、Security Manager が管理する他の CLI コマンドで使用されていないオブジェクトグループを、展開中にデバイスから削除するかどうかを指定します。オブジェクトグループには、ネットワーク/ホスト、サービス、およびIDユーザーグループが含まれます。 （注） このオプションを有効にすると、Security Managerは、Security Managerによって管理または検出されたポリシーで使用されていないオブジェクトを、展開中に削除します。Security Managerによって検出または管理されていないポリシーがそのようなオブジェクトを使用している場合、Security Managerは展開中にそのオブジェクトを削除しようとします。このような場合、オブジェクトを削除できなかったことを示すトランスクリプトエラーが表示されて、展開が失敗します。 ヒント ASA 8.3+ デバイス上のオブジェクト NAT 設定を含む、ネットワーク/ホスト オブジェクトは、参照されないとは見なされません。

要素	説明
Create Object Groups for Policy Objects (PIX, ASA, FWSM, IOS 12.4(20)T+) Create Object Groups for Multiple Sources, Destinations or Services in a Rule (PIX, ASA, FWSM, IOS 12.4(20)T+) Optimize Network Object Groups During Deployment (PIX, ASA, FWSM, IOS 12.4(20)T+) （IPv4 オブジェクトおよび IPv6 オブジェクト）。	Security Manager が、ネットワークオブジェクトやサービス グループ オブジェクトなどのオブジェクトグループを作成して、ユーザー グループ オブジェクトを識別し、指定されたデバイスの規則テーブルセル内のカンマ区切りの値を置換するかどうかを指定します。選択を解除すると、Security Manager は、オブジェクトグループをフラット化して、これらのデバイスの IP アドレス、送信元と宛先、ユーザ、ポート、およびプロトコルを表示します。 **ヒント** これらのオプションは、常にオブジェクトとして作成されるホスト、ネットワーク、またはアドレス範囲ネットワーク/ホストの各オブジェクト、あるいはサービス オブジェクト（サービス グループ オブジェクトではありません）には適用されません。複数の FQDN ネットワーク オブジェクトを単一のネットワーク オブジェクトにグループ化できます。 このオプションを選択すると、次のオプションも選択できます。 • [ルール内の複数の送信元、宛先、またはサービスのオブジェクトグループを作成（Create Object Groups for Multiple Sources, Destinations or Services in a Rule）]：ネットワークオブジェクトおよびサービスオブジェクトを自動的に作成して、ユーザー グループ オブジェクトを識別し、規則テーブルセル内の、複数のルールが結合された結果であるカンマ区切りの複数の値を置換するかどうかを指定します。オブジェクトは展開中に作成され、「CSM_INLINE...」の形式で、たとえば「CSM_INLINE_src_rule_8589960758」のようになります。詳細については、ルールの結合 （785 ページ）を参照してください。 • [Optimize Network Object Groups During Deployment]：ネットワーク オブジェクト グループをより簡潔にして、最適化するかどうかを指定します。ポリシー オブジェクトの簡潔化の詳細については、ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化 （802 ページ）を参照してください。
IPS パラメータ	
Generate transcripts for IPS Auto-Update Jobs	
Attach transcripts to email for IPS Auto-Update Jobs	

要素	説明
Remove Unreferenced Signature and Event Action Variables from IPS Device (IPS Parameters object group)	次回の展開中に、センサー（IPS デバイス）設定から未使用の変数を削除するかどうかを指定します。IPS のイベントおよびシグニチャ変数は、Security Manager のポリシーオブジェクトとして定義されています。 デフォルトでは無効になっています（チェックボックスはデフォルトでオフになっています）。つまり、参照されていない変数を削除しません。 次の変数に適用されます。 IPv4 と IPv6 の両方に適用されます。 • signature source と destination addresses • シグネチャ エンジン パラメータの signature service port 変数 • イベントアクションフィルタの victim and attacker addresses • network information target addresses 次の変数には適用されません。 • signature source port • OS identification address • signature destination port
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Device Communication] ページ

[Device Communication] ページを使用して、デバイスと通信する場合のデフォルト設定を定義します。これらの設定は、主に、デバイスインベントリ、ポリシー検出、および設定の展開に影響します。デバイスのデバイスプロパティにおける個々のデバイスに関する転送設定をオーバーライドできます。

トランスポートプロトコルの設定を変更する場合は、使用しているデバイスが、それらの接続タイプを受け入れるように適切に設定されていることを確認してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択します。

関連項目

- デバイス インベントリへのデバイスの追加 （94 ページ）
- デバイス インベントリの管理 （87 ページ）
- デバイスを管理するための準備 （71 ページ）
- デバイス プロパティの表示または変更 （136 ページ）

フィールド リファレンス

表 *129 : [Device Communication]* ページ

要素	説明
Device Connection Parameters	
Device Connection Timeout	Security Manager がデバイスとの接続を何秒の間に確立する必要があるか。この秒数を超過すると、タイムアウトします。
再試行回数（Retry Count）	Security Manager がデバイスへの接続の確立を何回試行するか。この試行回数を超過すると、接続を実行できないと判断されます。デフォルト値は 3 です。
Socket Read Timeout	SSH セッションと Telnet セッションの場合に、接続が失われたと結論付ける前に、Security Manager が着信データを待機する最大の秒数。
Transport Protocol (IPS)	IPS 機能を備えた IPS センサーとルータのデフォルト トランスポート プロトコル。デフォルトは HTTPS です。
Transport Protocol (IOS Routers 12.3 and above)	Cisco IOS ソフトウェア Release 12.3 以上を実行するルータのデフォルト トランスポート プロトコル。デフォルトは HTTPS です。
Transport Protocol (Catalyst Switch/7600)	Catalyst 6500/7600 デバイスおよびその他のすべての Catalyst スイッチのデフォルト トランスポート プロトコル（これらのデバイス上で実行されている Cisco IOS ソフトウェア バージョンは関係ありません）。デフォルトは SSH です。
Transport Protocol (IOS Routers 12.2, 12.1)	Cisco IOS ソフトウェア Release 12.1 および 12.2 を実行するルータのデフォルト トランスポート プロトコル。デフォルトは Telnet です。

要素	説明
Connect to Device Using	Security Manager がデバイスにアクセスするときに使用するクレデンシャルのタイプ。詳細については、デバイス クレデンシャルについて（91 ページ）を参照してください。 • [Security Managerのユーザ ログイン クレデンシャル（Security Manager User Login Credentials）]：Security Manager は、ユーザが Security Manager にログインしたときに入力したクレデンシャルを使用して、デバイスに接続します。[Device Credentials] ページで各デバイスに設定されたクレデンシャルに関係なく、同じクレデンシャル セットがすべてのデバイスに使用されます。 • [Security Managerデバイスのクレデンシャル（Security Manager Device Credentials）]：Security Manager は、[デバイスプロパティのクレデンシャル（Device Properties Credentials）] ページで指定したクレデンシャルを使用して、デバイスに接続します。これがデフォルトです。 **注意** IPS センサーへの接続が含まれる場合は、[Security Manager User Login Credentials] ではなく [Security Manager Device Credentials] を使用する必要があります。Security Manager が IPS センサーに接続するとき、Security Manager にユーザがログインしているかどうかにかかわらず、デバイス クレデンシャルを使用する必要があります。
SSL Certificate Parameters	

要素	説明
Device Authentication Certificates (IPS) Device Authentication Certificates (Router) PIX/ ASA/ FWSM Device Authentication Certificates [Add Certificate] ボタン	SSL（HTTPS）通信用のデバイス認証証明書の処理方法。さまざまなデバイス タイプごとに異なる動作を設定できますが、次の設定は同じ意味を持ちます。 • [デバイスの追加時に取得（Retrieve while adding devices）]：Security Managerは、ユーザがネットワークまたはエクスポートファイルからデバイスを追加するときに、これらのデバイスの証明書を自動的に取得します。 • [証明書を手動で追加（Manually add certificates）]：Security Managerは、デバイスから証明書を自動的に受け取りません。[証明書の追加（Add Certificate）] をクリックして、[Add Certificate] ダイアログボックスを開きます（[Add Certificate] ダイアログボックス （672ページ）を参照）。このダイアログボックスで、ネットワークまたはエクスポートファイルからのデバイスの追加を試行する前に、サムプリントを手動で追加できます。[Device Properties Credentials] ページで手動による作成に成功したデバイスの証明書を追加することもできます。詳細については、HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （578ページ）を参照してください。 • [証明書認証を使用しない（Do not use certificate authentication）]：Security Manager は、デバイス認証証明書を無視します。このオプションを使用すると、第三者によるデバイス検証の妨害に対してシステムが脆弱になります。このオプションは使用しないことを推奨します。
Accept Device SSL Certificate after Rollback	SSL を使用するデバイスの場合、デバイス上の設定をロールバックするときに、IPS デバイス、ファイアウォールデバイス、FWSM、ASA、または Cisco IOS ルータにインストールされている証明書をデバイスから取得するかどうかを指定します。

要素	説明
HTTPS Port Number	デバイスが、Security Manager（および、これらのプロトコルを使用するその他の管理アプリケーション）とのセキュアな通信に使用するデフォルトのポート番号。この値によって、デバイスの HTTP ポリシーで設定した HTTPS ポート番号がオーバーライドされます。 （注） ローカル HTTP ポリシーを共有ポリシーとして設定し、その HTTP ポリシーを複数のデバイスに割り当てると、このポリシーが割り当てられているすべてのデバイスに関して、[Device Properties Credentials] ページで設定されたポート番号が、このポリシーの HTTPS ポート番号設定で上書きされます。 この HTTPS ポート番号は、Cisco Web ブラウザのユーザ インターフェイスを介してデバイスへのアクセスを提供する以外に、Cisco Router and Security Device Manager（SDM）などのデバイス管理アプリケーションや、デバイスと通信するモニタリング ツールで使用されます。 （注） セキュリティ アプライアンスでは、同じインターフェイス上のデバイス マネージャ管理セッションの SSL VPN 接続と HTTPS 接続の両方を同時にサポートできます。HTTPS と SSL VPN は両方とも、デフォルトでポート 443 を使用します。このため、HTTPS と SSL VPN の両方を同じインターフェイスでイネーブルにする場合は、HTTPS または WebVPN に対して異なるポート番号を指定する必要があります。代替方法は、SSL VPN と HTTPS を異なるインターフェイスに設定することです。
Overwrite SSH Keys	Security Manager が、デバイスの SSH キーがデバイス上で変更された場合に、そのキーを上書きできるかどうかを指定します。SSH 接続の場合、通信を正常に実行するには正しいキーが必要です。 このチェックボックスは、慎重に検討し、より高いレベルのセキュリティが必要な場合にだけ、オフにしてください。キーがデバイス上で変更されると、Security Manager はそのデバイスと通信しなくなります。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Add Certificate] ダイアログボックス

[Add Certificate] ダイアログボックスを使用して、SSL トランスポート プロトコルを使用するデバイス（ファイアウォール デバイス、FWSM、ASA、IPS デバイス、および Cisco IOS デバ

イス）にデバイス証明書を手動で追加します。デバイス証明書を手動で追加すると、侵入者が不正な証明書サムプリントを追加できなくなるため、最高レベルのセキュリティがもたらされます。デバイス証明書は、デバイス認証に使用されるデータベースに格納されます。

SSL 証明書の手動による追加の詳細については、HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （578 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイス通信（Device Communication）] を選択し、[証明書の追加（Add Certificate）] をクリックします。

フィールド リファレンス

表 *130 : [Add Certificate]* ダイアログボックス

要素	説明
ホスト名またはIPアドレス	証明書を追加するデバイスのホスト名または IP アドレス。
Certificate Thumbprint	デバイス固有の16進数文字列である、証明書サムプリント。

[Device Groups] ページ

[Device Groups] ページを使用して、デバイス インベントリで定義されているデバイス グループおよびグループ タイプを管理します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デバイスグループ（Device Groups）] を選択します。

関連項目

- デバイスのグループ化について （164 ページ）
- デバイス グループの使用 （164 ページ）

フィールド リファレンス

表 *131 : [Device Groups]* ページ

要素	説明
Groups	デバイス グループとグループ タイプを表示します。 グループ名またはタイプ名を変更するには、グループまたはタイプを選択し、もう一度クリックしてテキストを編集可能にします。新しい名前を入力し、Enter を押します。
[Add Type] ボタン	新しいグループ タイプを作成するには、このボタンをクリックします。タイプはデフォルト名で追加されます。名前を上書き入力し、Enter を押します。
[Add Group to Type] ボタン	デバイス グループを選択したデバイス グループまたはグループ タイプに追加するには、このボタンをクリックします。
[Delete] ボタン（ゴミ箱）	選択したデバイス グループまたはグループ タイプとその中に含まれているすべてのデバイス グループを削除するには、このボタンをクリックします。デバイス グループまたはグループ タイプを削除しても、その中に含まれているデバイスは削除されません。
[Save] ボタン	変更内容を保存します。
リセット ボタン	すべてのフィールドを以前の値に復元します。

[Discovery] ページ

[Discovery] ページを使用して、Security Manager が、インベントリおよびポリシーの検出時に特定のタイプのオブジェクトまたはイベントを処理する方法を定義します。Security Manager が検出タスクを保持する時間を制御することもできます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [検出（Discovery）] を選択します。

フィールド リファレンス

表 *132 : [Discovery]* ページ

要素	説明
Prepend Device Name when Generating Security Context Names	セキュリティコンテキストが含まれているデバイスの名前を、そのセキュリティコンテキスト名の先頭に追加するかどうかを指定します。たとえば、セキュリティ コンテキストが admin という名前で、表示名が 10.100.15.16 であるデバイスに含まれている場合、デバイス セレクタに表示される名前は 10.100.15.16_admin になります。 デバイス名をプリペンドしない場合は、セキュリティ コンテキスト名がそのままインベントリに表示されます。Security Manager では、親デバイスに関連するフォルダにセキュリティ コンテキストが配置されないため、デバイスに関連するコンテキストを簡単に確認する唯一の方法が、デバイス名のプリペンドです。 デバイス名をプリペンドしない場合、Security Manager は、同じ名前のデバイスを区別するために番号のサフィックスを追加します。たとえば、admin コンテキストが複数のファイアウォールに存在する場合、デバイス セレクタでは admin_01、admin_02、というように表示されます。
Purge Discovery Tasks Older Than	検出タスクおよびデバイスインポート タスクを保存する日数。入力した日数よりも古いタスクは削除されます。
Reuse Policy Objects for Inline Values	Security Manager ですでに定義されているネットワーク/ホスト オブジェクト、アイデンティティ ユーザ グループ オブジェクトなど、名前の付いているポリシー オブジェクトを、CLI のインライン値に置き換えるかどうかを指定します。ポリシー オブジェクトの詳細については、ポリシー オブジェクトの管理 （287 ページ）を参照してください。 **ヒント** このオプションは通常、ネットワーク/ホストオブジェクトに適用されますが、完全修飾ドメイン名（FQDN）はインライン値として指定できないため、FQDN ネットワーク/ホストオブジェクトには適用されません。

要素	説明
Allow Device Override for Discovered Policy Objects	オーバーライドが可能なオブジェクトタイプについて、ユーザーが、検出されたポリシーオブジェクトの親オブジェクトの値をデバイスレベルでオーバーライドできるようにするかどうかを指定します。たとえば、このオプションを選択すると、デバイスに Security Manager の ACL ポリシー オブジェクトと同じ名前の ACL があるデバイス上でポリシー検出を実行した場合、検出されたポリシー オブジェクトの名前が再利用されますが、このオブジェクトのデバイス レベルのオーバーライドが作成されます。このオプションの選択を解除すると、新しいポリシー オブジェクトが、名前に番号が付加されて作成されます。 **ヒント** ネットワーク/ホストやサービスなど、サブタイプを持つオブジェクトの場合、オーバーライドはタイプ内に限定されます。たとえば、同じ名前のネットワーク/ホスト グループが検出されると、ネットワーク/ホスト グループのオーバーライドが作成されますが、同じ名前のネットワーク/ホスト アドレス範囲が検出されても、オーバーライドは作成されません。代わりに、新たに検出されたオブジェクトの名前に番号が付加されます。 詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。
On Error, Rollback Discovery for Entire Device	Security Manager が、ポリシー検出時に、単一ポリシーで 1 つのエラーが発生した場合でも、検出されたすべてのポリシーをロールバックするかどうかを指定します。選択を解除すると、Security Manager は、正常に検出されたポリシーを保持し、エラーが発生したポリシーだけを廃棄します。ポリシー検出の詳細については、ポリシーの検出 （223 ページ）を参照してください。
Auto-Expand Object Groups with Prefixes	デバイス インポート プロセス時に、リストに表示されているプレフィックスを使用して、ネットワーク グループやアイデンティティ ユーザ グループなどのオブジェクト グループを拡張します。複数のプレフィックスはカンマで区切ります。この拡張によって、オブジェクト グループの要素が、検出されたポリシーにおける個別の項目として表示されます。詳細については、検出中のオブジェクト グループの展開 （806 ページ）を参照してください。 **ヒント** このオプションは、**object network** コマンドまたは **object service** コマンドを使用して ASA 8.3+ デバイスから作成されたポリシー オブジェクトには適用されません。これらのコマンドによって、ホスト、ネットワーク、FQDN、またはアドレス範囲ネットワーク/ホストの各オブジェクトや、サービス オブジェクトが作成されます。
[Save] ボタン	変更内容を保存します。

要素	説明
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Event Management] ページ

[Event Management] ページを使用して、イベント管理をイネーブルにします。イベント管理では、Event Viewer を使用して、ASA イベント、FWSM イベント、および IPS イベントを表示できます。イベント収集に必要な設定値を設定することもできます。

Event Manager サービスは Report Manager アプリケーションにも必要です。Report Manager アプリケーションでは、このサービスによって収集された情報を集約したレポートを参照できます。

ヒント　このページで [イベント管理の有効化（Enable Event Management）] オプションが選択されているにもかかわらず、[起動（Launch）] > [イベントビューア（Event Viewer）] を選択したときに Event Viewer が使用不可能であるというメッセージが表示される場合には、Event Manager サービスをもう一度開始してみてください。まず、[Enable] オプションの選択を解除し、[Save] をクリックします。サービスが停止するまで待ちます。次に、[Enable] オプションを選択し、[Save] をクリックし、サービスが再び開始されるまで待機します。その後、Event Viewer を再度開いてみます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] をクリックし、コンテンツテーブルから [イベント管理（Event Management）] を選択します。

フィールド リファレンス

表 133 : [Event Management] ページ

要素	説明
Event Management Options	

要素	説明
Enable Event Management	Event Manager サービスをイネーブルにするかどうかを指定します。このサービスを使用すると、Security Manager はイベント情報を収集できます。この機能をディセーブルにすると、Event Viewer アプリケーションまたは Report Manager アプリケーションを使用できません。 **ヒント** この設定を変更し、[保存（Save）] をクリックすると、Event Manager サービスを起動または停止してもよいかどうかの確認を求められます。[Yes] をクリックするとすぐにサービスが開始または停止し、進捗インジケータが表示されて変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。
Event Data Store Location	イベント情報の収集に使用するディレクトリ。これはプライマリ イベント ストアと呼ばれます。[参照（Browse）] をクリックして、Security Manager サーバー上のディレクトリを選択します。 まだ存在していないディレクトリを指定する場合は、Windows エクスプローラで作成します。Security Manager からディレクトリを作成することはできません。 **ヒント** Event Manager サービスを使用して起動したあとに場所を変更した場合、古いイベントのクエリーは実行できなくなります。
Event Data Store Disk Size	イベント データを格納するために割り当てるディスク スペースの容量（GB 単位）。拡張ストアのサイズが指定した容量の 90 % に達すると、増分に応じて（循環的に）ストアからイベントが削除されるようになります。この設定を変更する場合は、次のことを考慮してください。 • イベント データによってすでに使用されているディスク スペース容量よりもサイズを少なくすると、新たに設定したサイズになるまで、古いものから順にイベントが削除されます。 • イベントデータに現在使用されているスペース量の視覚的表示を確認できます。Event Viewer を開き（**[起動（Launch）] > [Event Viewer]**）、次にイベントビューアで **[ビュー（Views）] > [イベントストアディスク使用状況の表示（Show Event Store Disk Usage）]** を選択します。

要素	説明
Event Syslog Capture Port	syslogイベントキャプチャをイネーブルにするポート。デフォルトは514です。 Security Managerサーバおよび介在するファイアウォールで、イベントを収集するために、Security Managerのこのポート上で着信トラフィックが許可されていることを確認してください。管理対象デバイスは、Security Managerサーバ上のこのポートにsyslog情報を送信するように設定されている必要があります。 **ヒント** このポートを変更した場合は、Security Managerにイベントを送信するすべてのASAデバイスおよびFWSMデバイスと、それらのセキュリティコンテキストのSyslog Serversポリシーも変更する必要があります。詳細については、[Syslog Servers] ページ （2671 ページ）を参照してください。
Event Data Pagination Size	各クエリー応答の各ページに含めることができる最大イベント数。デフォルトは20000ですが、サポートされている値のリストから異なるサイズを選択できます。 （注） Security Manager 4.10では、ページあたりのイベントの最大数が100000に増えました。
Extended Store Management Options	
Auto Copy Events to Extended Store	イベントを格納する拡張保管場所を定義するかどうかを指定します。通常のイベント保管場所から拡張保管場所にイベントをコピーして、引き続き使用できるようにします。Event Viewerで履歴イベントのクエリーを実行すると、必要に応じて、拡張保管場所にあるイベントが自動取得されます。 **ヒント** この拡張サービスを開始して拡張保管場所に変更を加えてもよいかどうかの確認が求められます。

要素	説明
Extended Data Store Location	イベントの拡張データ ストアの場所。サーバ上のドライブとして表示される、DASプロトコルを使用する直接接続ストレージを指定できます。たとえば、ファイバ チャネルを介して接続された SAN ストレージなどです。CIFS ストレージはサポートされていません。[参照（Browse）] をクリックして、目的のドライブとディレクトリを選択します。 **ヒント** • 拡張保管場所を選択して変更を保存すると、Security Managerは、その場所にアクセスできるかどうか、また書き込み権限があるかどうかをチェックします。プライマリ保管場所は参照として使用され、プライマリ保管場所にあって、拡張保管場所にはないデータがあった場合、そのデータは拡張保管場所にコピーされます。すでに拡張保管場所にあるデータは評価されず、そのまま残りますが、あとで削除して新しいデータ用のスペースを確保できます。 • 拡張データ ストアの場所を変更した場合、変更前の拡張データ ストアの場所だけに存在するイベント（プライマリ ロケーションからすでに削除されていて照会できないイベント）に対してクエリーを実行することはできません。このようなイベントを保持するには、以前の場所から新しい場所にデータをコピーしてください。
Extended Data Store Disk Size	イベントの拡張保管場所に割り当てるスペース量（GB 単位）。拡張ストアのサイズが指定した容量の90%に達すると、増分に応じて（循環的に）ストアからイベントが削除されるようになります。サイズは、イベントデータのプライマリ保管場所のサイズ以上にする必要があります。 イベントデータに現在使用されているスペース量の視覚的表示を確認できます。Event Viewerを開き（**[起動（Launch）] > [Event Viewer]**）、次にイベントビューアで **[ビュー（Views）] > [イベントストアディスク使用状況の表示（Show Event Store Disk Usage）]** を選択します。

要素	説明
Error Notification Email IDs	拡張保管場所の使用で問題が発生した場合に、通知を受信する電子メールアドレス。カンマで複数のアドレスを区切ります。通知が正常に送信されるように、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）で説明しているように SMTP サーバも設定する必要があります。 メッセージには、問題、原因、および推奨アクションが示されます。たとえば、頻繁に拡張ストレージが到達不能になる場合、データのコピーが繰り返し失敗する場合、または拡張保管領域にコピーできるようになる前にプライマリ保管領域からパーティションが削除された場合（頻繁にストレージが到達不能になるか、コピーに永続的な問題があると発生する可能性がある）などに通知を受信します。
フェールオーバーデバイスの Syslog	
フェールオーバースタンバイデバイスからの Syslog の処理（Process Syslogs from Failover Standby Device）	スタンバイ ASA からの syslog メッセージの処理をイネーブルまたはディセーブルにします。イネーブルにすると、スタンバイ ASA またはフェールオーバー ASA によって生成された syslog メッセージが、[イベントモニタリング（Event Monitoring）] ウィンドウの [デバイス ID（Device Identifier）] 列に表示されます。 （注） デフォルトでは、スタンバイ ASA からの syslog メッセージの処理は無効になっています。
Syslogリレーサービス（Syslog Relay Service） （注） バージョン 4.13 以降、Cisco Security Manager は Event Viewer で IPv6 経由の syslog をサポートしますが、syslog リレーサービスは IPv6 経由の syslog ではサポートされません。	
Syslogリレーサービスの有効化（Enable Syslog Relay Service）	Syslog リレーサービスをイネーブルまたはディセーブルにします。[Syslogリレーサービスの有効化（Enable Syslog Relay Service）] チェックボックスをオンにして、Syslog リレーサービスの構成に必要なフィールドを有効にします。

要素	説明
Syslogリレーキャプチャポート（Syslog Relay Capture Port）	Syslog リレーサービスが syslog をリッスンする UDP ポートを指定します。デフォルトは 514 です。 Syslog リレーサービスが有効になっている場合、デバイスはSyslog リレーキャプチャポートに Syslog を送信して、ローカルコレクタとリモートコレクタに転送できるようにする必要があります。Syslog リレーサービスがオフになっている場合、デバイスはSyslogをイベント Syslog キャプチャポートに送信する必要があります。 （注） Syslog リレーキャプチャポートとイベント Syslog キャプチャポートを同じにすることはできません。Syslog リレーサービスを有効にするときに、デバイスが現在 Syslog をイベント Syslog キャプチャ ポートに送信するように設定されている場合は、代わりにそのポート番号を Syslog リレーキャプチャポートに使用してから、イベント Syslog キャプチャポートを別のポートに変更する必要があります。 Security Manager サーバおよび介在するファイアウォールで、イベントを収集するために、Security Manager のこのポート上で着信トラフィックが許可されていることを確認してください。管理対象デバイスは、Security Manager サーバ上のこのポートに syslog 情報を送信するように設定されている必要があります。 ヒント このポートを変更した場合は、Security Manager にイベントを送信するすべての ASA デバイスおよび FWSM デバイスと、それらのセキュリティ コンテキストの Syslog Servers ポリシーも変更する必要があります。詳細については、[Syslog Servers] ページ （2671 ページ）を参照してください。
ローカルイベントコレクタへのリレー（Relay to Local Event Collector）	ローカルイベントコレクタの syslog リレーを有効または無効にします。
リモートコレクタ1へのリレー（Relay to Remote Collector 1）	リモートコレクタ 1 の syslog リレーを有効または無効にします。
コレクタ1のIPアドレス（Collector 1 IP address）	リモートコレクタ 1 の syslog 送信先 IP アドレスを指定します。
コレクタ1 Syslogキャプチャポート（Collector 1 Syslog Capture Port）	リモートコレクタ 1 がリレーされた syslog をリッスンする UDP ポートを指定します。

要素	説明
リモートコレクタ2へのリレー（Relay to Remote Collector 2）	リモートコレクタ 2 の syslog リレーを有効または無効にします。
コレクタ2のIPアドレス（Collector 2 IP address）	リモートコレクタ 2 の syslog 送信先 IP アドレスを指定します。
コレクタ2 Syslogキャプチャポート（Collector 2 Syslog Capture Port）	リモートコレクタ 2 がリレーされた syslog をリッスンする UDP ポートを指定します。

要素	説明
デバイス フィルタ	特定のコレクタについて、syslog をリレーする必要があるデバイスをフィルタできます。この機能を使用すると、あるデバイスセットの syslog を 1 つのコレクタに送信し、別のデバイスセットの syslog を別のコレクタに送信するように構成できます。 **1.** デバイスをフィルタリングする対象のタブ（ローカルコレクタ、リモートコレクタ 1、またはリモートコレクタ 2）を選択します。 **2.** このコレクタに対して syslog をリレーするデバイスを指定するには、[リレーを許可（Permit Relay）] を選択します。逆に、このコレクタに対する syslog リレーを無効にするデバイスを指定する場合は、[リレーを許可（Permit Relay）] チェックボックスをオフにします。[リレーを許可（Permit Relay）] チェックボックスがオンになっていない場合、フィルタに追加したデバイスの syslog はリレーされません。一方、他のすべてのデバイスの syslog はリレーされます。 （注） 有効になっている各コレクタについて、すべてのデバイスからの syslog リレーがデフォルトで有効になっています。 （注） クラスタをフィルタリストに追加すると、クラスタ管理プールの IP アドレスがフィルタ構成の一部として含まれます。 **3.** フィルタに追加するデバイスまたはデバイスグループを [使用可能なデバイス（Available Devices）] リストから選択し、[>>] をクリックして [選択されたデバイス（Selected Devices）] リストに移動します。デバイスの選択の詳細については、セレクタの使用（60 ページ）を参照してください。 **4.** Security Manager の管理対象外デバイスを追加するには、[特別なデバイスの追加（Add Special Device）] フィールドにデバイスの IP アドレスを入力し、下部の [>>] をクリックして、デバイスを [選択されたデバイス（Selected Devices] リストに移動します。
再起動（Restart）	Syslog リレーサービスを再起動します。
CPUスロットル設定（CPU Throttle Settings）	Syslog リレーサービスに使われる CPU 負荷を制御できる [CPUスロットリングポリシー（CPU Throttling Policy] ダイアログボックスを開きます。詳細については、[CPU スロットリング ポリシー] ダイアログボックス （686 ページ）を参照してください。

要素	説明
統計情報の表示（View Statistics）	[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスを開いて、syslog リレーサービスプロセスの平均CPUとメモリ使用量、およびさまざまなコレクタのトラフィックレートを表示できます。詳細については、[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス （688 ページ）を参照してください。
[Save] ボタン	変更を保存して適用します。 ほとんどの場合、Event Viewer 設定に関連する変更を反映するには、Event Manager サービスを一時的に停止し、再起動することが必要となります。サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。 Syslog リレーサービス設定の変更を反映するには、Syslog リレーサービスを一時的に停止してから再起動する必要があります。サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

Syslog リレーサーバーのトラブルシューティング

Syslog リレーサービスが有効になっている場合、デバイスはSyslog リレーキャプチャポートにSyslogを送信して、ローカルコレクタとリモートコレクタに転送できるようにする必要があります。Syslog リレーサービスがオフになっている場合、デバイスは Syslog をイベント Syslog キャプチャポートに送信する必要があります。

Syslog リレーサーバーは、デバイスイベントと Security Manager イベント マネージャ アプリケーション間の中間接続として機能します。デバイスイベントのパケットを受信し、ローカルコレクタとリモートコレクタに転送します。

IP によるデバイス管理

IP を介して（IPv4 または IPv6 を使用して）Security Manager でデバイスを管理するには、デバイス管理インターフェイスに適切な IP 情報が必要です。

たとえば、次のサンプル設定を参照してください。

```
!
interface Management1/1
management-only
nameif management
```

security-level 100

ip address 10.197.87.95 255.255.255.0

ipv6 address 2016::b2aa:77ff:fe7c:a068/64

ipv6 enable

この設定では、デバイス管理 IP アドレスに IPv4 と IPv6 の両方の管理アドレスがあります。したがって、IPv4 または IPv6 を介してデバイスを管理できます。

問題：

デバイスが Security Manager の IPv6 管理アドレスを介して管理されている場合、Security Manager とデバイス間の通信は、IPv4 アドレスではなく IPv6 アドレスのみを介して行われます。

ただし、Event Syslog サーバーは引き続き Event Syslog パケットを IPv4 アドレスにのみ送信するため、このシナリオでは、Security Manager は受信した IPv4 Event Syslog パケットに対応するデバイスをマッピングできません。

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）] > [Syslogリレーサービス（Syslog Relay Service）] で、Syslog リレーサービスのローカルコレクタまたはリモートコレクタにフィルタデバイスを追加すると、Security Manager は、IPv6 管理アドレスではなくデバイス管理 IPv4 アドレスを抽出しようとします。

ただし、デバイスには IPv4 管理インターフェイスが設定されていません。したがって、Security Manager は次のエラーを表示します。

デバイスの選択 – デバイスの IPv4 アドレスが見つかりません（Device selection – Ipv4 address not found for device(s)）

ソリューション：

[デバイスビュー（Device View）] > [ポリシー（Policies）] > [インターフェイス（Interfaces）] に移動して、IPv4 アドレスを使用してデバイス管理インターフェイスを設定します。

[CPU スロットリング ポリシー] ダイアログボックス

[CPUスロットリングポリシー（CPU Throttling Policy] ダイアログボックスを使用して、Syslog リレーサービスに使われる CPU 負荷を制御するための設定を指定します。

CPU スロットリングをイネーブルにした後で、[最大CPU使用率平均の時間（Average Max CPU Usage Time）] フィールドで選択されている期間中の syslog リレーサービスの平均 CPU 使用率が [最大CPU使用率（Maximum CPU Usage）] しきい値より大きい場合、[転送の中止期間（Stop Forwarding For）] で指定された期間、CPU スロットリングが [次への転送を中止（Stop Forwarding To）] で指定されたコレクタに対して実行されます。

（注） [Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスを使用して、スロットルポリシーのためにコレクタごとにドロップされた syslog パケットの数を確認できます（[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス （688 ページ）を参照）。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択して、[CPUスロットル設定（CPU Throttle Settings）] をクリックします。

フィールド リファレンス

表 *134 : [CPU* スロットリング ポリシー*]* ダイアログボックス

要素	説明
CPUスロットリングを有効にする（Enable CPU Throttling）	syslog リレーサービスに対するスロットリングをイネーブルにするかどうかを指定します。デフォルトでは、syslog リレーサービスに対する CPU スロットリングはディセーブルになっています。
最大CPU使用率（Maximum CPU Usage）	Syslog リレーサービス用の最大 CPU 使用率を、合計 CPU 容量のパーセンテージとして指定します。これは、CPU スロットリングが開始されるしきい値です。
最大CPU使用率平均の時間 (分)（Average Max CPU Usage Time (Minutes)）	syslog リレーサービスによる CPU 使用率が計算される時間を分単位で指定します。オプションは、1 分、5 分、および 15 分です。この平均値は、最大 CPU 使用率の値と比較されて、スロットルを実行する必要があるかどうかが判断されます。
[次への転送を中止（Stop Forwarding To）]	スロットリングが行われているときに syslog の転送を停止するコレクタを指定します。
転送の中止期間（Stop Forwarding For）	しきい値に達したときにスロットルをイネーブルにする時間を分単位で指定します。指定された時間が経過した後も、CPU 使用率が最大 CPU 使用率のしきい値を超えている場合、スロットリングは引き続きイネーブルです。
電子メール通知の有効化	syslog リレーサービスがスロットルモードを開始または終了したときに電子メール通知を送信するかどうかを指定します。電子メール通知は、デフォルトではディセーブルです。 電子メールを送信するには、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）の説明に従って SMTP サーバを設定する必要があります。
通知電子メールID（Notification Email IDs）	[通知電子メールID（Notification Email IDs）] フィールドに、有効なアドレスを 1 つ以上入力します。複数のアドレスはコンマで区切ります。

要素	説明
電子メールの送信	通知メールを送信する頻度を指定します。 • [毎回（Every time）]：このオプションを選択すると、syslog リレーサービスがスロットルモードを開始または終了するたびに通知が送信されます。転送の中止期間タイマーが経過した後も CPU 使用率が最大 CPU 使用率のしきい値を超えている場合、スロットリングは継続され、追加の通知が送信されます。 • [指定した期間ごと（Every）]：このオプションを選択すると、syslog リレーサービスが特定の期間にスロットルモードを開始または終了したときに、最大 1 つの通知が送信されます。このオプションを選択する場合は、分数または時間数を入力して期間を指定し、ドロップダウンリストから対応するオプション（分/時間）を選択します。

[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス

[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスを使用して、syslog リレーサービスプロセスの平均 CPU とメモリ使用量、およびさまざまなコレクタのトラフィックレートを表示します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [イベント管理（Event Management）] を選択して、[統計情報の表示（View Statistics）] をクリックします。

フィールド リファレンス

表 135 : [Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックス

要素	説明
ログリレーサービス（Log Relay Service）	
平均メモリ使用量（過去1分間）（Memory Usage Average (last 1 min.)）	過去 1 分間に平均して syslog リレーサービスによって使用されたメモリの量を示します。

要素	説明
平均CPU使用率（過去1分間）（CPU Usage Average (last 1 min.)）	過去 1 分間に平均して syslog リレーサービスによって使用された CPU 容量の割合を示します。 ヒント　平均CPU使用率が高すぎる場合は、syslog リレーサービスの CPU スロットリングを有効にすることを検討してください（[CPU スロットリング ポリシー] ダイアログボックス （686 ページ）を参照）。
受信syslogパケットの総数（Total sylog packets received）	サービスの開始以降、syslog リレーサービスによって受信された syslog パケットの総数を示します。
開始以降に受信した1秒あたりの平均syslog数（Average syslog received per second since start）	サービスの開始以降、syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
過去1分間に受信した1秒あたりの平均syslog数（Average syslog received per second for last 1 minute）	過去 1 分間に syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
過去5分間に受信した1秒あたりの平均syslog数（Average syslog received per second for last 5 minute）	過去 5 分間に syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
過去15分間に受信した1秒あたりの平均syslog数（Average syslog received per second for last 15 minute）	過去 15 分間に syslog リレーサービスによって受信された 1 秒あたりの syslog パケットの平均数を示します。
スロットルポリシーがアクティブな期間（分単位）（Period (in mins.) for which throttle policy is active）	syslog リレーサービスの CPU スロットルポリシーがアクティブであった時間を分単位で示します。詳細については、[CPU スロットリング ポリシー] ダイアログボックス （686ページ）を参照してください。
ローカルコレクタ/リモートコレクタ 1/リモートコレクタ 2	
正常に送信されたsyslogパケットの総数（Total syslog packets sent successfully）	サービスの開始以降、syslog リレーサービスによって送信された syslog パケットの総数を示します。
ドロップされたsyslogパケットの総数（フィルタポリシー）（Total syslog packets dropped (filter policy)）	サービスの開始以降、定義されたフィルタポリシーに従って syslog リレーサービスによってドロップされた syslog パケットの総数を示します。
ドロップされたsyslogパケットの総数（スロットルポリシー）（Total syslog packets dropped (throttle policy)）	サービスの開始以降、スロットルポリシーに従って syslog リレーサービスによってドロップされた syslog パケットの総数を示します。

要素	説明
送信中に失敗したsyslogパケットの総数（Total syslog packets failed during transmit）	サービスの開始試行、syslog リレーサービスで転送できなかった syslog パケットの総数を示します。
開始以降に送信した1秒あたりの平均syslog数（Average syslog sent per second since start）	サービスの開始以降、syslog リレーサービスによって送信された 1 秒あたりの syslog パケットの平均数を示します。
過去1分間に送信した1秒あたりの平均syslog数（Average syslog sent per second for last 1 minute）	過去 1 分間に、syslog リレーサービスによって 1 秒あたりに送信された syslog パケットの平均数を示します。
過去5分間に送信した1秒あたりの平均syslog数（Average syslog sent per second for last 5 minute）	過去 5 分間に、syslog リレーサービスによって 1 秒あたりに送信された syslog パケットの平均数を示します。
過去15分間に送信した1秒あたりの平均syslog数（Average syslog sent per second for last 15 minute）	過去 15 分間に、syslog リレーサービスによって 1 秒あたりに送信された syslog パケットの平均数を示します。
更新	[Syslogリレー統計（Syslog Relay Statistics）] ダイアログボックスに表示される統計を更新します。

[Health and Performance Monitor] ページ

[Cisco Security Manager管理（Cisco Security Manager Administration）] ウィンドウの [Health and Performance Monitor] ページを使用して、ネットワーク全体の Health and Performance Monitoring を有効にします。Health and Performance Monitor（HPM）はスタンドアロン アプリケーションであり、デバイスステータスやトラフィック情報をネットワークレベルで可視化することにより、ASA デバイス、IPS デバイス、および VPN サービスの主要な正常性データとパフォーマンスデータを監視できます。

ヒント　Health and Performance Monitor の起動を試みたときにアプリケーションが使用できないというメッセージが表示された場合でも、このページで [Health and Performance Monitorの有効化（Enable Health and Performance Monitor）] オプションを選択している場合は、Health and Performance Monitoring を再起動してみてください。まず、[Enable] オプションの選択を解除し、[Save] をクリックします。サービスが停止するまで待ちます。次に、[Enable] オプションを選択し、[Save] をクリックし、サービスが再び開始されるまで待機します。その後、HPM アプリケーションを再度開いてみてください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] をクリックし、目次から [Health and Performance Monitor] を選択します。

フィールド リファレンス

表 136 : [Health and Performance Monitor] ページ

要素	説明
Health and Performance Monitorの有効化（Enable Health and Performance Monitor）	Cisco Security Manager がイベント情報を収集できるようにする Health and Performance Monitoring サービスを有効化または無効化できます。この機能を無効にすると、HPM アプリケーションを使用できません。 **ヒント** この設定を変更し、[保存（Save）] をクリックすると、Health and Performance Monitoring サービスの起動または停止の確認を求められます。[Yes] をクリックするとすぐにサービスが開始または停止し、進捗インジケータが表示されて変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。
OOB 通知設定 **（注）** 電子メール通知を受信するには、SMTP サーバーが Cisco Security Manager サーバーで設定されている必要があります。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）を参照してください。 Cisco Security Manager は、アウトオブバンド（OOB）変更を手動で、または Cisco Security Manager の管理外でデバイスに加えられた変更であると見なします。たとえば、（監視対象）デバイスに直接ログインし、CLI を介してコンフィギュレーション コマンドを入力した場合です。HPM アプリケーションによって監視されるデバイスの場合、Cisco Security Manager は、HPM によって定期的に検出される OOB の変更を監視します。アウトオブバンド変更が検出された場合、HPM は [デバイスステータスビュー（Device Status View）] ページに表示されるアラートを生成し、設定済みの受信者に電子メールを送信します。 **（注）** 更新時間中に Cisco Security Manager が再起動した場合、OOB の変更が検出され、電子メール通知が送信された後、Cisco Security Manager の起動後に同じ電子メールが再度送信される可能性があります。	

要素	説明
OOB電子メール通知の有効化（Enable OOB Email Notification）	アウトオブバンド変更に関する電子メール通知を有効化または無効化できます。 （注） 電子メール通知が無効になっている場合、[デバイスステータスビュー（Device Status View）] ページにはアラートのみが表示されます。 （注） HPM が OOB の変更を検出し、Configuration Manager と同期すると、監視対象のデバイスごとに個別の電子メールアラート通知が送信されます。重複を防ぐために、OOB 変更ごとに送信される電子メールは追跡され、5 分に 1 回ファイルに保存されます。 ヒント デフォルトの追跡時間は、Cisco Security Manager プロパティファイルで5分に設定されています。時間は必要に応じて更新できます。
受信者の電子メール（Recipient E-mail(s)）	OOB の変更を通知する必要がある受信者を指定します。
[Save] ボタン	変更を保存して適用します。 ほとんどの場合、Health and Performance Monitoring サービスを一時的に停止して、再起動する必要があります。サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。
リセット ボタン	変更を前回保存した値にリセットします。

[Report Manager] ページ

[Security Manager管理（Security Manager Administration）] ウィンドウの [Report Manager] ページを使用して、Cisco Security Manager の Report Manager 機能をイネーブルまたはディセーブルにします。Report Manager は、デバイス、およびリモートアクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示できるスタンドアロンアプリケーションです。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] をクリックし、コンテンツテーブルから [Report Manager] を選択します。

フィールド リファレンス

表 *137 : [*ヘルスとパフォーマンスのモニタリング（*Health and Performance Monitoring***）*]* ページ**

要素	説明
Report Manager を有効にする（Report Manager）	Report Manager サービスをイネーブルまたはディセーブルにすることができます。この機能をディセーブルにすると、Report Manager アプリケーションを使用できません。 ヒント この設定を変更し、[保存（Save）]をクリックすると、Report Manager サービスを起動または停止してもよいかどうかの確認を求められます。[Yes] をクリックするとすぐにサービスが開始または停止し、進捗インジケータが表示されて変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。
[Save] ボタン	変更を保存して適用します。 サービスがイネーブルであるかどうかを変更した場合は、それに応じてサービスが停止または起動します。進捗インジケータが表示されます。
リセット ボタン	変更を前回保存した値にリセットします。

[Identity Settings] ページ

[Identity Settings] ページを使用して、NetBIOS ドメインが ASA デバイスの ID 認証ファイアウォール ポリシーを使用するように、Active Directory（AD）サーバ グループを設定します。これらの設定によって、ID認証ポリシーのユーザまたはユーザ グループ、またはアイデンティティ ユーザ グループ ポリシー オブジェクトを選択するときに、検索機能を使用できるようになります。

ヒント ASA で [Identity Options] ポリシーを設定することで、エントリを追加することもできます。ポリシーを保存するときに、アイデンティティ設定管理ページを更新するかどうかを確認します。1 つのドメインに対して異なるサーバ グループを使用するように複数の ASA を設定できますが、設定ページでのドメインと AD サーバの組み合わせは 1 つであることに注意してください。ユーザー名のルックアップでは、設定している個々の ASA にどのサーバーグループが設定されているかに関係なく、常に ID 設定管理ページで定義された AD サーバーが選択されます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ID設定（Identity Settings）] を選択します。

関連項目

- アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）
- ポリシーでのアイデンティティ ユーザの選択 （835 ページ）

フィールド リファレンス

表 *138 : [Identity Settings]* ページ

要素	説明
ドメイン - AD サーバー グループ マッピング テーブル。	テーブルの各行によって、NetBIOS ドメインが ASA デバイスの ID 認証ファイアウォール ポリシーを使用するように、Active Directory（AD）サーバ グループが定義されます。 • エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[AD ドメイン サーバーの追加（Add AD Domain Server）] ダイアログボックスに入力します。 [Domain AD Server] ダイアログボックス （821 ページ）を参照してください。ドメイン名を入力し、LDAP AD サーバーを指定する AAA サーバー グループ オブジェクトを選択する必要があります。 • エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。 • Security Manager がサーバーグループで定義されたサーバーに正常に接続できるかどうかをテストするには、行を選択して [テスト（Test）] をクリックします。
デフォルト ドメイン	ファイアウォール ポリシーまたはアイデンティティ ユーザ グループ ポリシー オブジェクトのユーザ名またはグループ名を指定するときにドメインを入力しなかった場合に使用する NetBIOS ドメイン。 デフォルトは LOCAL であり、これは名前が ASA 自体で定義されることを意味します（ローカルユーザーとして、またはドメイン名に関連付けられた LDAP サーバーグループ以外の手段で認証された VPN ユーザーとして）。 LOCAL 以外は、[Domain-AD Server Group Mapping] テーブルで設定されたドメインだけがこのリストに表示されます。 **ヒント** この設定は、user-identity default-domain コマンドで設定されたデフォルト ドメインとは関係ありません。この設定は、ドメイン名を必ずしも含めなくてもユーザー名を入力できるようにする便利な設定です。ユーザー名を最も頻繁に入力するドメインを選択します。

要素	説明
ルートクエリの経由元	ユーザまたはユーザ グループを選択するときに検索機能を使用する場合、Security Manager から AD サーバにクエリーを送信する必要があります。クエリが Security Manager クライアント（クライアントを実行しているワークステーション）からのものか、サーバーからのものかを選択します。 デフォルトでは、LDAP クエリはクライアントから送信されます。
ドメインのないユーザー文字列の場合	デフォルト ドメインに LOCAL 以外を選択した場合、ドメイン名なしで入力されたユーザ名またはユーザ グループ名の処理方法を指定します。 • [ADからユーザー/ユーザーグループを自動判断（Auto determine user/user-group from AD）]：デフォルトドメインに関連付けられている AD サーバーをチェックして、名前がユーザーかユーザーグループかを判断し、適切な文字列（Default-Domain\user または Default-Domain\\user-group）を追加します。名前が見つからない場合は、ドメイン名と 1 つか 2 つの \ 文字を手動で入力して、その名前がユーザーのものかグループのものかを示す必要があります。 • [Default-Domain/userに変更（Change it to Default-Domain/use）]：入力された名前がユーザーグループ名ではなくユーザー名であると想定し、デフォルトドメイン（Default-Domain\user）を追加します。 ヒント 入力する場合は、名前の前に \ または \\ を付けると、デフォルトドメインが自動的に追加されます。そのため、[Change it to Default-Domain/user] オプションを選択した場合でも、最初に \\ を入力すれば、ドメインを入力せずにグループ名を入力できます。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Image Manager] ページ

[Image Manager] ページを使用して、Cisco Security Manager 内の Image Manager の管理設定を制御します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [Image Manager] を選択します。

フィールド リファレンス

表 139 : [Image Manager] ページ

要素	説明
CCO設定の編集（Edit CCO Settings）	[CCO設定の編集（Edit CCO Settings）] リンクを使用して、[CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （645 ページ）を参照してください。
より古いジョブを削除（Purge Jobs Older Than）	Image Manager ジョブを削除する前に保持する期間（日数）を入力します。デフォルトは365 日です。[今すぐ削除（Purge Now）] を選択して、以前の Image Manager ジョブの仕様をすぐにクリアします。
リポジトリを含める（Include Repository）	オンにすると、イメージリポジトリは Cisco Security Manager バックアップの一部になります。デフォルトではイメージは除外されます。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[IPインテリジェンス設定（IP Intelligence Settings）] ページ

[IPインテリジェンス設定（IP Intelligence Settings）] ページを使用して、Cisco Security Manager 内の IP インテリジェンス機能の管理設定を制御します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [IPインテリジェンス設定（IP Intelligence Settings）] を選択します。

フィールド リファレンス

表 *140 : [IP*インテリジェンス設定（*IP Intelligence Settings***）*]* ページ**

要素	説明
CCO設定の編集（Edit CCO Settings）	GeoIP データベースを自動更新するには、Cisco.com に接続するためのログイン情報が必要です。[CCO設定の編集（Edit CCO Settings）] リンクを使用して、ログイン情報が設定されている [CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページでプロキシサーバーの設定を設定することもできます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （645 ページ）を参照してください。
逆引き DNS（FQDN）	
逆引きDNS（FQDN）ルックアップサービスの有効化（Enable Reverse DNS (FQDN) Lookup Service）	逆引きDNS（FQDN）ルックアップサービスを有効にするか無効にするかを指定します。IP インテリジェンスツールを使用して IPv4 アドレスの完全修飾ドメイン名（FQDN）を特定できるようにする場合は、このサービスを有効にします。
CSMサーバーのDNSサーバーを使用（Use CSM Server's DNS Server）	逆引き DNS ルックアップ要求に Cisco Security Manager サーバーで定義された DNS サーバーを使用するには、このオプションを選択します。
カスタムDNSサーバーを使用（Use custom DNS servers）	逆引き DNS ルックアップ要求に使用する DNS サーバーを手動で指定するには、このオプションを選択します。表示されるフィールドには、最大 3 つの DNS サーバーアドレスを入力できます。 （注） Cisco Security Manager は、仮想マシンの内部に構成された外部 DNS サーバーの使用をサポートしていません。
ロードバランシングの有効化（Enable Load Balancing）	複数の DNS サーバーが使用可能な場合に、DNS サーバー間で逆引き DNS ルックアップ要求を分散するかどうかを指定します。
デフォルトのブロッキング範囲（Default Blocking Ranges）	デフォルトで逆引き DNS ルックアップから除外される IP アドレスの範囲を一覧表示します。 0.0.0.0、255.255.255.255、127.0.0.1、169.254.0.0 ～ 169.254.255.255、224.0.0.0 ～ 239.255.255.255

要素	説明
ユーザー定義のブロッキング範囲（User-defined Blocking Ranges）	逆引き DNS ルックアップ要求から除外する必要がある追加の IPアドレスまたはアドレスの範囲を指定します。[編集（Edit）]（鉛筆）ボタンをクリックして [IPv4ブロック範囲アドレスの編集（Edit IPv4 Blocking Range Addresses）] ダイアログボックスを開き、除外する IPv4 アドレスまたはアドレスの範囲を指定できます。複数のエントリを指定する場合は、カンマ「,」で区切ります。
GeoIP	
GeoIPルックアップサービスの有効化（Enable GeoIP Lookup Service）	GeoIP ルックアップサービスを有効にするか無効にするかを指定します。IP インテリジェンスツールを使用して IPv4 アドレスの地理的位置情報を取得できるようにする場合は、このサービスを有効にします。 （注） GeoIP 情報を IP インテリジェンスデータに含めるには、Cisco.com から地理的位置データベースをダウンロードする必要があります。また、バックアップから Cisco Security Manager データベースを復元した後、Cisco.com から地理的位置データベースをダウンロードする必要があります。バージョン 4.9 以降、Cisco Security Manager では、cisco.com からアップデートをダウンロードする前に、シスコ エンドユーザー ライセンス契約（EULA）を読んで同意することが義務付けられています。
GeoIP手動アップロード（GeoIP Manual Upload） [GeoIP手動アップロード（GeoIP Manual Upload）] フィールドを使用して、Cisco.com からダウンロードした MaxMind GeoLite City 更新パッケージを使用して、Cisco Security Manager の地理的位置データベースを更新します。 （注） 新しい更新パッケージは、Cisco.com で毎月提供されます。	
GeoIPデータベースアーティファクトの場所（GeoIP Database Artifact Location）	[参照（Browse）] をクリックし、Cisco.com からダウンロードした MaxMind GeoLite City 更新パッケージに移動して選択します。次に、[アップロード（Upload）] をクリックして、選択したデータベースを Cisco Security Manager にアップロードします。 （注） MaxMind 社またはその他のソースから直接取得した位置情報の更新は、Cisco Security Manager ではサポートされていません。

要素	説明
GeoIP Maxmindデータベースの更新設定（GeoIP Maxmind Database Update Settings） MaxMind GeoLite City 更新パッケージは、Cisco.com で毎月更新されます。[GeoIP Maxmind データベースの更新設定（GeoIP Maxmind Database Update Settings）] を使用して、更新パッケージを Cisco.com から自動的にダウンロードし、スケジュールされた更新を設定します。 （注） 地理的位置データベースを自動更新するには、Cisco.com に接続するためのログイン情報が必要です。[CCO設定の編集（Edit CCO Settings）] リンクを使用して、ログイン情報が設定されている [CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （645 ページ）を参照してください。	
即時データベース更新を実行する（Run immediate database update）	[今すぐ更新（Update Now）] をクリックして、Cisco.com にある最新の更新パッケージを使用して、Cisco Security Manager の地理的位置データベースを更新します。
スケジュールされた更新の有効化（Enable scheduled update）	地理的位置データベースの自動更新を定期的なスケジュールで有効にするか無効にするかを指定します。スケジュールされた更新を有効にしたら、[設定の編集（Edit Settings）] をクリックして、更新を実行するスケジュールを指定します。 [毎週（Weekly）] オプションを使用して、自動更新を実行する曜日を指定できます。[毎月（Monthly）] オプションを使用して、自動更新を実行する日付を指定できます。いずれのオプションでも、更新の実行時刻を指定できます。 ヒント 地理的位置データベースは、毎月第 1 火曜日に MaxMind 社によって更新されます。新しい更新パッケージは、通常、MaxMind 社が発行してから約 1 週間後に Cisco.com で入手可能になるため、毎月 15 日以降に更新スケジュールを設定することを推奨します。ただし、更新されたデータベースが Cisco.com で利用可能になる時刻にできるだけ近い時刻に Cisco Security Manager で利用可能にする場合は、更新をより頻繁に実行するようにスケジュールできます。 （注） バージョン 4.9 以降、Cisco Security Manager では、cisco.com からアップデートをダウンロードする前に、シスコ エンド ユーザー ライセンス契約（EULA）を読んで同意することが義務付けられています。
デフォルトのブロッキング範囲（Default Blocking Ranges）	デフォルトで GeoIP ルックアップから除外される IP アドレスの範囲を一覧表示します。 0.0.0.0、255.255.255.255、127.0.0.1、10.0.0.0 ～ 10.255.255.255、169.254.0.0 ～ 169.254.255.255、172.16.0.0 ～ 172.31.255.255、192.168.0.0 ～ 192.168.255.255、224.0.0.0 ～ 239.255.255.255

要素	説明
ユーザー定義のブロッキング範囲（User-defined Blocking Ranges）	GeoIP ルックアップ要求から除外する必要がある追加の IP アドレスまたはアドレスの範囲を指定します。[編集（Edit）]（鉛筆）ボタンをクリックして [IPv4ブロック範囲アドレスの編集（Edit IPv4 Blocking Range Addresses）] ダイアログボックスを開き、除外する IPv4 アドレスまたはアドレスの範囲を指定できます。複数のエントリを指定する場合は、カンマ「,」で区切ります。
[Whois]	
Whoisルックアップサービスの有効化（Enable Whois Lookup Service）	Whois ルックアップサービスを有効にするか無効にするかを指定します。IP インテリジェンスツールを使用して IPv4 アドレスの WHOIS 情報を取得できるようにする場合は、このサービスを有効にします。
外部プロキシの有効化（Enable External Proxy）	Whois リクエストに対して外部プロキシの使用を有効にするか無効にするかを指定します。プロキシサーバーの設定は、[CCO設定（CCO Settings）] ページで指定します。 **ヒント** [CCO設定の編集（Edit CCO Settings）] リンクを使用して、プロキシサーバー設定が設定されている [CCO設定（CCO Settings）] ページに迅速に移動できます。[CCO設定（CCO Settings）] ページの詳細については、[CCO設定（CCO Settings）] ページ （645 ページ）を参照してください。
デフォルトのブロッキング範囲（Default Blocking Ranges）	デフォルトで Whois ルックアップから除外される IP アドレスの範囲を一覧表示します。 0.0.0.0、255.255.255.255、127.0.0.1、10.0.0.0 ～ 10.255.255.255、169.254.0.0 ～ 169.254.255.255、172.16.0.0 ～ 172.31.255.255、192.168.0.0 ～ 192.168.255.255、224.0.0.0 ～ 239.255.255.255
ユーザー定義のブロッキング範囲（User-defined Blocking Ranges）	Whois ルックアップ要求から除外する必要がある追加の IP アドレスまたはアドレスの範囲を指定します。[編集（Edit）]（鉛筆）ボタンをクリックして [IPv4ブロック範囲アドレスの編集（Edit IPv4 Blocking Range Addresses）] ダイアログボックスを開き、除外する IPv4 アドレスまたはアドレスの範囲を指定できます。複数のエントリを指定する場合は、カンマ「,」で区切ります。

要素	説明
統計情報の表示（View Statistics）	IP インテリジェンス機能の統計を表示する [IPインテリジェンス統計（IP Intelligence Statistics）] ダイアログボックスを開きます。[IPインテリジェンス統計（IP Intelligence Statistics）] ダイアログボックスに表示される情報は次のとおりです。 • 過去 5 分間および過去 15 分間の IP インテリジェンス ルックアップ リクエストの平均数 • すべての IP インテリジェンス サービス リクエストの平均ルックアップ時間 • 現在有効になっている個々のサービスの平均ルックアップ時間 • 現在有効になっている個々のサービスに対して成功および失敗したルックアップの数 • 現在有効になっている個々のサービスのキャッシュヒット率 • GeoIP 更新のアップロード情報：更新の最終更新時刻、ステータス、およびバージョン情報 [更新（Refresh）] をクリックして、[IPインテリジェンス統計（IP Intelligence Statistics）] ダイアログボックスのデータを更新します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[イベント通知設定（Eventing Notification Settings）] ページ

[イベント通知設定（Eventing Notification Settings）] ページを使用して、IPS イベントおよび重要な ASA イベントの電子メール通知を受信します。電子メール通知を受信する時間間隔を設定できます。

イベントは、.zip ファイル形式内の .CSV ファイルの形式で送信されます。デフォルトでは、電子メール通知はディセーブルになっています。電子メール通知を有効にすると、IPS イベントの通知のみが有効になります。重要なイベントの電子メール通知を受信するには、重要なイベント用の追加設定をイネーブルにする必要があります。

（注） Security Manager により通知が正常に送信されるように、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）で説明しているように SMTP サーバーを設定する必要があります。

ヒント Security Manager Event Viewer アプリケーションまたはダッシュボードを使用して、すべてのイベントを表示および監視することもできます。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント通知設定（Eventing Notification Settings）] を選択します。

フィールド リファレンス

表 *141 : [イベント通知設定（Eventing Notification Settings）] ページ*

要素	説明
イベント電子メール通知の有効化（Enable Eventing Email Notification）	電子メールによる IPS イベントの通知を有効にする場合に選択します。
通知間隔（Notification Interval）（15 ～ 60 分）	Security Manager が IPS イベントまたは重要なイベントの電子メール通知を送信する間隔を入力します。 （注） Security Manager が設定された時間間隔中に 50000 を超えるイベントを受信した場合、最初の 50000 件のイベントのみが選択され、電子メールで送信されます。
通知設定（IPS）	
電子メールID（IPS イベント用）（Email IDs (for IPS Events)）	電子メールアドレスを 1 つ以上入力します（コンマ区切り）。
イベント重大度の選択（Select Severity of Events）	IPS シグニチャによってレポートされる重大度レベル（[高（High）]、[中（Medium）]、[低（Low）]、または [情報（Informational）]）。デフォルトでは、[高（High）] と [中（Medium）] の重大度が選択されています。

要素	説明
通知の内容	要約通知と詳細通知のどちらを電子メールで送信するかを指定します。[詳細な通知（Detailed Notifications）] を選択した場合は、電子メール通知に含める必要がある情報のフィールドを選択します。一部のフィールドは、デフォルトで選択されています。
フィールド	
イベント ID（Event ID）	内部で各イベントに割り当てられる一意の連続番号。
重大度	ファイアウォールまたは IPS の重大度の値。
デバイス	イベントの送信元。通常はデバイス ID です。 Not Available と識別されたデバイスは、Security Manager インベントリから削除されています。
アプリケーション	イベントを発生させているアプリケーションの名前。
Receive Time	イベントが Security Manager によって受信された時刻。
イベント時間	デバイスによりイベントが生成された時間。
センサーのローカル時刻（Sensor Local Time）	イベントが発生したセンサーの現地時刻。
Sig ID	Sig ID 値は、アラート発信者がアクティビティを特定するために使用されます。この値により、アクティビティにあらかじめ定義されているシグニチャを識別できます。
サブシグニチャ ID（Sub Sig. ID）ID	このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャIDによって、広範なシグニチャのより詳細なバージョンが識別されます。
シグニチャ名（Sig. Name）名前	証明書に割り当てられる名前を示します。
シグニチャ詳細（Sig. Detail）詳細（Details）	レポートされたシグニチャの詳細。トリガーされて、アラートの生成を引き起こしたシグニチャです。
シグニチャバージョン（Sig. Version）バージョン	アラートの生成に使用されたシグニチャ定義のバージョン。
Attacker IP	攻撃パケットを送信するホストの IP アドレス。
Attacker Port	攻撃者ホストによって使用されるポート。これは、攻撃パケットの発信元のポートです。

要素	説明
攻撃者の所在（Attacker Locality）	攻撃者のアドレスが、侵入検知デバイスの設定で指定された特定のネットワークの内側に存在するか、外側に存在するかを識別します。
攻撃対象IP（Victim IP）	攻撃されているホストの IP アドレス。
攻撃対象のポート	攻撃されているホスト（攻撃パケットの受信者）のポート。これは、攻撃パケットの送信先のポートです。
攻撃対象の OS	攻撃されているホストの OS。
攻撃対象の所在地	攻撃対象のアドレスが、侵入検知デバイスの設定で指定された特定のネットワークの内側に存在するか、外側に存在するかを識別します。
サマリーカウント（Summary Count）	サマリーアラートであり、特性が共通する 1 つ以上のアラートを表したものです。数値は、「initialAlert」属性値との一致により、最後のサマリーアラート以降にシグニチャが発行された回数を示します。
初期アラート（Initial Alert）	このフィールドはサマリーアラートに適用され、特性が共通する 1 つ以上のアラートを表したものです。値 initialAlertは、特性（sigid/subsigid）が同じでサマリーアラートではない最後の evIdsAlert のイベント ID です。
Summary Type	サマリーアラートのすべてのアラートに共通する特性を定義します。
最後（Is Final）	サマリーアラートに適用され、特性が共通する 1 つ以上のアラートを表したものです。このアラートが、 initialAlert 属性に同じ値を含む最後のイベントアラートであるかどうかを示します。
インターフェイス	IPS インターフェイスの名前。
VLAN	アラートをトリガーしたアクティビティにかかわるパケットに関連付けられた VLAN 番号。
仮想センサー	イベントに関連付けられた仮想センサーの名前。
[実施アクション（Action Taken）]	フローに対して実行されるアクション。たとえば、終了や拒否。
アラート詳細（Alert Details）	アラートに関する詳細。
Risk Rating	イベントに関連付けられたリスクを計算した値。
Threat Rating	イベントの脅威レーティング（ある場合）。

要素	説明
レピュテーション	-10.0 ～ +10.0 で示される攻撃者のレピュテーションスコア。スコアが低い（負の値が大きい）ほど、ホストが悪意のあるホストである可能性が高くなります。
レピュテーションの詳細（Reputation Details）	攻撃者の拒否（Deny Attacker）：リスクレーティングを算出した結果、内部オーバーライドを超えたために、攻撃者拒否アクションが発生した（または発生することになっていた）のかどうかを示す true または false。
プロトコル	Level-3 プロトコルまたは Level-4 プロトコル。
通知設定 （Notification Settings）（重要なイベントのみ）	
有効 電子メール ID（Email IDs）	重要なイベントについて電子メール通知を送信するかどうか。このオプションを選択した場合は、1 つ以上の電子メール アドレスも入力します（カンマ区切り）。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[IPS Updates] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[IPS Updates] ページを使用して、シグニチャ、マイナーなバージョン更新、およびサービス パックに関して、センサーを最新の状態に保持するための管理タスクを実行します。[IPS Updates] ページを使用して、次のことを実行できます。

- 更新ステータスをモニタする。
- 取得可能な更新を確認し、それらをダウンロードする。
- IPS 更新サーバを設定する。
- 自動更新の設定値を設定する。

（注） Security Manager バージョン 4.9 以降、IPS の最新のセンサーおよびシグネチャパッケージのみが CCO からダウンロードできます。古いパッケージは、CCO からダウンロードできません。

ヒント

- IPS 更新を手動で適用するには、[ツール（Tools）] > [IPS更新の適用（Apply IPS Update）] を選択します。詳細については、IPS 更新の手動適用 （2307 ページ）を参照してください。
- 後にシグニチャの更新を適用する必要はなかったと判断した場合は、デバイスで [シグネチャ（Signatures）] ポリシーを選択し、[更新レベルの表示（View Update Level）] ボタンをクリックしてから [Revert] をクリックすることで、直前の更新レベルに戻すことができます。

バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理 （620 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPSの更新（IPS Updates）] を選択します。

関連項目

- IPS 更新サーバの設定 （2303 ページ）
- IPS 更新の確認とダウンロード （2304 ページ）
- IPS 更新の自動化 （2305 ページ）
- Cisco IOS IPS のシグニチャ カテゴリの選択 （2321 ページ）

フィールド リファレンス

表 *142 : [IPS Updates]* ページ

要素	説明
[Update Status] グループ [Refresh] ボタン	次の項目を表示します。[更新（Refresh）] をクリックして、情報を更新してください。 • [Latest Available]：Cisco.com または最後に更新を確認したときのローカル HTTP サーバで取得可能な最新のシグニチャおよびセンサーの更新。 • [Latest Downloaded]：Security Manager にダウンロードされた、最新のシグニチャおよびセンサーの更新。 • [Latest Applied]：Security Manager でデバイスに適用された、最新のシグニチャおよびセンサーの更新。 • [Latest Deployed]：Security Manager でデバイスに展開された、最新のシグニチャおよびセンサーの更新。 • [Last Check On]：Cisco.com の確認を最後に実行した時間。 • [Last Download On]：最後の更新が Security Manager にダウンロードされた時間。 • [Last Deployed On]：いずれかのデバイスに最後の更新が展開された時間。

要素	説明
[Check for Updates] ボタン [Download Latest Updates] ボタン	これらのボタンによって、更新が確認されるか、または Security Manager サーバにまだダウンロードされていないシグニチャおよびセンサー更新が IPS 更新サーバからダウンロードされます。更新の確認またはダウンロードの前に、IPS 更新サーバーを設定する必要があります（[サーバーの更新（Update Server）] グループで [設定の編集（Edit Settings）] をクリックします）。 これらのボタンのいずれかをクリックすると、ダイアログボックスが開き、操作の結果が表示されます。ユーザが [Download] ボタンをクリックすると、Security Manager は IPS 更新サーバにログインして更新を確認し、更新をダウンロードします。Cisco.com からのダウンロードに失敗する場合は、使用しているアカウントで強化暗号化ソフトウェアをダウンロードできることを確認してください。詳細については、[Edit Update Server Settings] ダイアログボックス （712 ページ）の [User Name] の説明を参照してください。 **ヒント** サーバーを設定し、次に更新を確認しようとしたときに、サーバーを設定していないと通知された場合は、このページの一番下にある [保存（Save）] をクリックして、再試行してください。 （注） バージョン 4.9 以降、Cisco Security Manager では、cisco.com からアップデートをダウンロードする前に、シスコ エンドユーザー ライセンス契約（EULA）を読んで同意することが義務付けられています。
[Update Server] グループ	Cisco.com、または IPS 更新パッケージが格納されているローカル サーバへのアクセスに使用する設定を表示します。これらのフィールドには、Update サーバが Cisco.com とローカルに設定された HTTP サーバのいずれであるか、ローカル サーバを使用する場合はローカル サーバの名前、サーバにログインするためのユーザ アカウント、およびプロキシ サーバの名前（ある場合）が示されます。IPS 更新サーバーを設定または変更するには、[設定の編集（Edit Settings）] をクリックして [サーバー設定の更新の編集（Edit Update Server Settings）] ダイアログボックスを開きます（[Edit Update Server Settings] ダイアログボックス （712 ページ）を参照）。 詳細については、IPS 更新サーバの設定 （2303 ページ）を参照してください。 バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理 （620 ページ）を参照してください。
シグニチャフィルタ設定グループ	IPS シグネチャアップデートを選択的にダウンロードできます。[設定の編集（Edit Settings）] をクリックして、[シグネチャダウンロードフィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログ ボックスを開きます（[シグネチャ ダウンロードフィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックス （716 ページ） を参照）。

要素	説明
[Auto Update Settings] グループ	自動更新に固有の設定が含まれています。詳細については、IPS 更新の自動化 （2305 ページ）を参照してください。
Auto Update Mode	自動更新を実行するかどうか、およびどの程度実行するかを設定します。次のオプションがあります。 • Download, Apply, and Deploy Updates • Disable Auto Update • 更新の確認（Check for Updates） • Download Updates • Download and Apply Updates デフォルトでは、自動更新はディセーブルになっています。その他のオプションは、次のオプションを 1 つ以上組み合わせたものとなります。 • [Check for Updates]：Security Manager は、IPS 更新サーバに接続して更新を取得できるかどうかを確認し、電子メール通知が設定されている場合は、電子メールを送信します。ファイルはダウンロードされません。 • [Download Updates]：Security Manager は最新の更新を IPS 更新サーバからダウンロードし、電子メール通知が設定されている場合は、電子メールを送信します。 • [Apply Updates]：Security Manager は、ダウンロードされた更新パッケージに基づいて、[Apply Update To] リストで選択されているデバイスの設定を変更します。[Deploy Updates] も選択している場合を除き、これらの更新は個別に展開する必要があります。 • [Deploy Updates]：Security Manager は、展開ジョブを開始して、適用可能な更新パッケージを、[Apply Update To] リストで選択されているデバイスに送信します。デバイスは、シグニチャ更新の成功に必要なライセンスを取得している必要があります。

要素	説明
スケジュールの更新 [Edit Update Schedule] ボタン	[Auto Update Mode] フィールドで選択されたアクションのスケジュール。このスケジュールを変更するには、[更新スケジュールの編集（Edit Update Schedule）] をクリックし、[IPS更新スケジュールの編集（Edit IPS Updates Schedule）] ダイアログボックスでスケジュールを定義します。Security Managerが毎時間、毎日、毎週、または毎月のスケジュールに基づいて更新を実行することを指定したり、1 回かぎりのイベントを指定したりできます。開始時間を入力する場合は、24 時間制の *hh:mm* 形式を使用してください。 （注） Security Manager サーバーの時刻から 10 分以内に更新が行われるようにスケジュールすると、[次の更新（Next Update）] フィールドに明日の日付が表示され、それに応じてジョブが実行されます。これは、最初の実行を保証するために設計された安全機能です。 ヒント 自動ダウンロードを時間外にスケジュールして、デバイス検出などの他のユーザ操作と競合しないようにすることを推奨します。 ヒント 通常のユーザ操作には、管理者アカウント以外のアカウントを使用することをお勧めします。
Notify Email	自動更新の通知が送信される電子メール アドレス。複数のアドレスを入力する場合は、それらのアドレスをカンマで区切ります。通知は、更新が次の状態になると送信されます。 • ダウンロードが可能になった。 • ダウンロードされた。 • ダウンロードされ、適用された。 • ダウンロードされ、適用され、展開された。

要素	説明
Apply Update To タイプ（Type） [Edit Row] ボタン Devices to be Auto Updated	このセレクタには、Security Manager で定義されたローカル シグニチャ ポリシーおよび共有シグニチャ ポリシーを持つIPSデバイスが含まれています。セレクタのカラムは、ローカル デバイス ポリシーまたは共有ポリシーが、次の更新タイプに関して選択されているかどうかを示します。 • [Signature]：シグニチャ更新レベルの自動更新の場合。 • [Minor]：マイナー更新およびサービス パックの場合。 • [S.P.]：サービス パック更新の場合。 共有ポリシーの場合、一部がグレー表示になっているチェックボックスは、このポリシーを使用するデバイスの全部ではなく一部が選択されていることを示します。自動更新イベント中に、共有ポリシーに割り当てられているデバイスを変更すると、その共有ポリシーはグレー表示され、古い割り当てだけがこのページに表示されます。更新を実行したあとに、この割り当てリストは共有ポリシーのデバイス割り当てと同期されます。次の自動更新が実行される前に、このデバイス リストをプロアクティブに更新するには、ポリシーを選択して編集します（自動更新設定を選択します）。これで、デバイス割り当てリストが訂正されます。 （注） また、共有ポリシーの場合：デフォルトの仮想センサー（vs0）に割り当てられた共有ポリシーのみを選択できます。別の仮想センサーの共有ポリシーを選択しようとしても、変更は適用されず、エラーメッセージは受け取りません。 [Type] フィールドを使用して、ローカル ポリシーと共有ポリシーの表示を切り替えます。表示を変更しても、自動更新の選択内容は変更されません。 自動更新用のローカルまたは共有ポリシーを選択するには、このセレクタで選択し、セレクタの下にある [行の編集（Edit Row）] ボタンをクリックします。これにより、[Edit Auto Update Settings] ダイアログボックスが開きます。このダイアログボックスで、ポリシーの更新タイプを選択できます。いずれかの自動更新タイプをポリシーに選択すると、影響を受けるデバイスが、セレクタの右にある [自動更新されるデバイス（Devices to be Auto Updated）] リストに一覧表示されます。
[Save] ボタン	変更内容を保存します。
リセットボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Edit Update Server Settings] ダイアログボックス

[Edit Update Server Settings] ダイアログボックスを使用して、IPS 更新の取得に使用するサーバを設定します。必要に応じて、Update サーバと通信するためのプロキシ サーバを設定できます。

また、証明書の信頼管理には [更新サーバー設定の編集（Edit Update Server Settings）] ダイアログボックスを使用します（Security Manager は、HTTPS 経由で Cisco.com から IPS パッケージをダウンロードし、信頼を確立するために証明書を使用します）。[Image Manager] ページの証明書信頼管理機能は、Security Manager 4.4 の新機能です。この機能は、IPS パッケージのダウンロードに向けた Cisco.com 証明書の処理を改善するのに役立ちます。

- この機能を使用して証明書を表示できます。証明書を受け入れるかどうか慎重に検討してください。
- 証明書を受け入れると、証明書は Security Manager サーバーに保存されます。
- [Image Manager] ページの概要テーブルにすべての証明書が表示され、そのテーブルを使用して証明書を表示または削除できます。

ヒント　下のテーブルの [証明書の取得（Retrieve Certificate）] を必ず確認してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [IPS のアップデート（IPS Updates）] を選択し、[更新サーバー（Update Server）] グループで [設定の編集（Edit Settings）] をクリックします。

フィールド リファレンス

表 *143 : [Edit Update Server Settings]* ダイアログボックス

要素	説明
Update From	IPS 更新を Cisco.com から取得するか、ローカル HTTP/HTTPS サーバから取得するかを指定します。ダイアログボックスのフィールドは、選択に応じて変わります。 ローカルを選択した場合は、IPS 更新サーバとして使用するように HTTP または HTTPS サーバを設定する必要があります。 **注意**　[更新元：（Update From:）] のデフォルト値は [ローカルサーバー（Local Server）] です。証明書の設定を表示するには、[Cisco.com] を選択する必要があります。証明書の設定が不適切または不完全な場合、Cisco.com への接続が妨げられ、このエリアでの Cisco.com 関連のすべての操作が失敗します。

要素	説明
IP Address/ Host Name （ローカル サーバのみ）	ローカル IPS 更新 Web サーバのホスト名または IP アドレス。
Web サーバ ポート（Web Server Port） （ローカル サーバのみ）	ローカルサーバが接続要求をリスニングするポート番号。デフォルトは 80 です。
ユーザー名	IPS 更新サーバにログインするユーザ名。ユーザ ログインが不要なローカル サーバを設定する場合は、このフィールドを空白のままにしておきます。 Cisco.com ユーザ名を指定する場合、Cisco.com 上のユーザ アカウントは、強化暗号化ソフトウェアをダウンロードできる必要があります。アカウントが必要な権限を持っているかどうか不明な場合は、このアカウントを使用して Cisco.com にログインし、IPS 更新ファイルをダウンロードしてみます（http://www.cisco.com/cgi-bin/tablebuild.pl/ips5-system）。アカウントが適切な権限を持っていない場合は、必要な条件を読んで同意するように要求されます。適格要件を満たしている場合は、これらの条件を受け入れることができます。そうでない場合は、シスコの営業担当者にお問い合わせください。
パスワード 確認（Confirm）	両方のフィールドに入力される、指定したユーザ名のパスワード。パスワードが不要なローカル サーバを設定する場合は、これらのフィールドを空白のままにしておきます。
Path to Update Files （ローカル サーバのみ）	ローカル サーバ上の IPS 更新ファイルの場所へのパス。たとえば、更新ファイルに http://local-server-ip:port/update_files_path/ でアクセスできる場合、update_files_path をこのフィールドに入力します。
Connect Using HTTPS （ローカル サーバのみ）	ローカル IPS 更新サーバに接続する場合に、SSL を使用するかどうかを指定します。
Certificate Thumbprint	ローカル サーバ上の証明書から証明書サムプリントが計算されたあとに、この証明書サムプリントを表示します。
Retrieve From Server	ダイアログボックスで指定されたローカル サーバに接続し、所定のローカル サーバから証明書を取得し、[Certificate Thumbprint] フィールドに表示される証明書サムプリントを計算するために使用します。

要素	説明
[連絡先URL（Contact URL）]	• 選択すると、[イメージメタデータロケータ（Image Meta-data Locator）] が使用されます。これは、イメージに関するメタデータ情報の取得に使用される Cisco.com の URL です。メタデータ情報は、特定の製品に該当するイメージ、名前、サイズ、チェックサム、および各イメージをダウンロードする URL で構成されます。 • 選択すると [その他（Other）] が使用されます。任意の有効な HTTPS URL を入力できます。この URL は、主に、イメージに関するメタデータ情報から取得したイメージをダウンロードするための HTTPS URL を対象としています。この URL は、前の段落で説明したイメージメタデータロケータの URL とは異なる場合があります。証明書も異なる場合があります。 **注意** [その他（Other）] を選択した場合は、明示的に "https://dl.cisco.com" を追加する必要があります（引用符は不要）。[その他（Other）] ボタンの隣のテキストフィールドに入力します。これを追加しないと、Cisco.com に接続できなくなり、このエリアでの Cisco.com 関連のすべての操作が失敗します。
[証明書の取得（Retrieve Certificate）]	選択した [連絡先URL（Contact URL）] に接続して証明書を取得するために使用されます。証明書を取得すると、[証明書の検証（Certificate Verification）] ダイアログが開きます。証明書の簡単な概要、つまり、証明書の発行対象、発行者、証明書の有効期間が表示されます。さらに、次の選択肢が表示されます。 • [証明書の表示（View Certificate）]：証明書ビューアを開いて、証明書のすべての詳細（認証局、バージョン、シリアル番号、サムプリント、その他の詳細）を表示できます。ルート発行認証局までの完全な証明書チェーン情報が表示されます。 • [承認（Accept）]：証明書を承認して、Cisco Security Manager に追加します。 • [拒否（Reject）]：証明書を拒否します。アクションは実行されません。 • [キャンセル（Cancel）]：アクションを実行せずに [証明書の検証（Certificate Verification）] ダイアログを閉じます。
証明書	Security Manager インストールの各証明書について、[情報カテゴリ（Subject）]、[発行者（Issued By）]、および [承認者（Accepted By）] を表示するテーブル。

要素	説明
表示（View）	[証明書（Certificate）] テーブルで選択した証明書の証明書ビューアを開きます。
削除（Remove）	[証明書（Certificate）] テーブルで選択した証明書を削除します。
Proxy Server Group	
Enable Proxy Server	プロキシ サーバが、Cisco.com またはローカル サーバに接続するために必要であるかどうかを指定します。
IP Address/ Host Name	プロキシ サーバのホスト名または IP アドレス。 基本的なダイジェスト NT LAN Manager（NTLM）V1 または NTLM V2 認証を使用するように、プロキシ サーバを設定できます。NTLM V2 が、最もセキュアなスキームです。
[ポート（Port）]	プロキシサーバが接続要求をリッスンするポート番号。デフォルトは 80 です。
ユーザー名	プロキシ サーバにログインするユーザ名。プロキシ サーバでユーザ ログインが必要ない場合は、このフィールドを空白のままにしておきます。
パスワード 確認（Confirm）	両方のフィールドに入力される、指定したユーザ名のパスワード。プロキシサーバでパスワードが必要ない場合は、これらのフィールドを空白のままにしておきます。

[Edit Auto Update Settings] ダイアログボックス

[Edit Auto Update Settings] ダイアログボックスを使用して、[IPS Updates] ページの [Apply Update To] テーブルで選択したデバイスまたはポリシーの自動更新オプションを設定します。自動更新の設定については、IPS 更新の自動化 （2305 ページ）を参照してください。

ナビゲーション パス

[IPS Updates] ページ（[IPS Updates] ページ （705 ページ）を参照）の [Apply Update To] テーブルで、デバイスまたはポリシーを選択し、[Edit Row] ボタンをクリックします。

フィールド リファレンス

表 *144 : [Edit Auto Update Settings]* ダイアログボックス

要素	説明
自動更新 （IPS センサーおよび共有ポリシーだけ）	選択したデバイスまたは共有ポリシーに適用する、センサー更新のタイプ。マイナー更新とサービス パックの両方を適用したり、サービス パックだけを適用したりできます。または、[None] を選択して、センサーの更新が自動的に適用されないようにできます。
Auto Update Signature Update Level	自動シグニチャ更新にデバイスまたはポリシーを選択するかどうかを指定します。

[シグネチャダウンロードフィルタ設定の編集（EditSignatureDownload Filter Settings）] ダイアログボックス

[シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックスでは、IPS シグネチャの更新を選択的にダウンロードできます。これは、手動ダウンロードと自動ダウンロードの両方に適用されます。

（注） フィルタ処理は、IPS センサーパッケージまたは IPS エンジンパッケージには適用されません。IPS シグネチャパッケージのみに適用されます。Cisco.com またはローカルサーバー上の使用可能なすべてのセンサーパッケージが、シグニチャダウンロードの一部としてダウンロードされます。

選択的ダウンロードの利点は、必要なものだけをダウンロードできるため、ダウンロード時間が短縮され、ディスクストレージスペースが削減され、トラブルシューティングが迅速化されることです。

[シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックスでは、次の 4 タイプのシグネチャダウンロードを使用できます。

- [フィルタなし（No filter）]
- [[E4、E3、E2、またはE1を選択]で始まるエンジンバージョンのすべてのシグネチャをダウンロード（Download all signatures for engine versions starting with [choose E4, E3, E2, or E1]）]
- [[1000 などのシグネチャバージョンを入力] で始まるすべてのシグネチャバージョンをダウンロード（Download all signature versions starting with [enter a signature version such as 1000]）]
- [単一のシグネチャバージョン番号 [1000 などのシグネチャ番号を入力] をダウンロード（Download a single signature version number [enter a signature number such as 1000]）]

デフォルトのシグネチャ設定では、E4 以降のエンジンバージョンのシグネチャがすべてダウンロードされます。

ヒント　このデフォルト値は、Security Manager 4.3 の新規インストールでも以前のバージョンからのアップグレードでも同じです。

ナビゲーション パス

[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] を選択し、目次で [IPS の更新（IPS Updates）] を選択します。その後、[シグネチャフィルタ設定（Signature Filter Settings）] グループの [設定の編集（Edit Settings）] をクリックします。

関連項目

- IPS 更新サーバの設定　（2303 ページ）
- IPS 更新の確認とダウンロード　（2304 ページ）
- IPS 更新の自動化　（2305 ページ）

フィールド リファレンス

表 *145 : [シグネチャ ダウンロード フィルタ設定の編集（Edit Signature Download Filter Settings）] ダイアログボックス*

要素	説明
[フィルタタイプ（Filter Type）] : [フィルタなし（No filter）]	使用可能なすべてのエンジン用の使用可能なすべてのシグネチャがダウンロードされます。
[フィルタタイプ（Filter Type）] : [で始まるエンジンバージョンのすべてのシグネチャをダウンロード（Download all signatures for engine versions starting with）]	選択したエンジン（E4、E3、E2、または E1）用の使用可能なすべてのシグネチャがダウンロードされます。
[フィルタタイプ（Filter Type）] : [で始まるすべてのシグネチャバージョンをダウンロード（Download all signature versions starting with）]	入力した ID で始まる使用可能なすべてのシグネチャがダウンロードされます。
[フィルタタイプ（Filter Type）] : [単一のシグネチャバージョン番号をダウンロード（Download single signature version number）]	入力した ID を持つ単一のシグネチャがダウンロードされます。

[ISE設定（ISE Settings）] ページ

[ISE 設定（ISE Settings）] ページを使用して、Cisco Security Manager と TrustSec ファイアウォールポリシーで使用する Cisco Identity Services Engine（ISE）間の通信を設定します。

（注） Cisco Security Manager は、セキュリティグループの名前とタグを取得して解決するために、1 つの ISE アプライアンス/サーバーとの通信のみサポートします。

PCI に準拠するために、Cisco Security Manager 4.15 および 4.16 では、TLS 1.0 と TLS 1.1 がそれぞれ無効になりました。したがって、4.16 以降では、Cisco Security Manager は TLS 1.2 バージョンのみを使用していました。

ただし、ISE 1.3 サーバーおよびその下位バージョンは TLS 1.2 をサポートしていません。これは、リリース 4.15 以降の Cisco Security Manager でのレガシー ISE 設定に影響します。この非互換性により、ISE サーバーと Cisco Security Manager の統合が妨げられます。

Cisco Security Manager 4.15、4.16、または 4.17 バージョンで ISE サーバー（バージョン 1.3 以前）を使用して、ISE 1.3 以前のバージョンを Cisco Security Manager と正常に統合する必要がある場合は、リリース 4.17 用の『Cisco Security Manager User Guide』を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ISE設定（ISE Settings）] を選択します。

関連項目

- Trustsec ファイアウォールポリシーの管理 （845 ページ）
- セキュリティ グループ オブジェクトの作成 （863 ページ）
- ポリシーでのセキュリティグループの選択 （865 ページ）

フィールド リファレンス

表 *146 : [Identity Settings]* ページ

要素	説明
ISE 機能の有効化（Enable ISE feature）	ISE との通信をイネーブルにするかどうかを指定します。
ユーザー名	Security Manager が、ISE にログインするときに使用するユーザ名。
パスワード	ユーザー名のパスワード。

要素	説明
ISEサーバー（IPアドレス/ホスト名）（ISE Server (IP Address/Hostname)）	ISE の DNS ホスト名または IP アドレス
ISEバージョン（ISE Version）	バージョン 4.18 以降、Cisco Security Manager は ISE バージョン 2.3 の統合のみをサポートします。
接続のテスト	[接続のテスト（Test Connectivity）] をクリックして、入力した設定で Security Manager が ISE と通信できることを確認します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

Licensing ページ

[Licensing] ページを使用して、Security Manager アプリケーションおよび IPS デバイス用のライセンスを管理します。詳細については、IPS ライセンスの管理 （2299 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ライセンス（Licensing）] を選択します。

フィールド リファレンス

表 147 : Licensing ページ

要素	説明
[CSM] タブ	Security Manager アプリケーションのライセンス設定。このタブの各フィールドの説明については、[CSM] タブ、[Licensing] ページ （720 ページ）を参照してください。
[IPS] タブ	Security Manager によって管理される IPS デバイスのライセンス設定。このタブの各フィールドの説明については、[IPS] タブ、[Licensing] ページ （720 ページ）を参照してください。

[CSM] タブ、[Licensing] ページ

[Licensing] ページの [CSM] タブを使用して、インストール済みの Security Manager ライセンスのリストを表示し、新しいライセンスをインストールします。詳細については、Security Manager のライセンス ファイルのインストール （618 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ライセンス（Licensing）] を選択し、[CSM] をクリックします。

フィールド リファレンス

表 *148 : [CSM]* タブ、*[Licensing]* ページ

要素	説明
ライセンス情報	製品に登録されているライセンスに関する情報（エディション、ライセンスタイプ、有効期限、ライセンス対象デバイスの数、使用中のデバイス数、および使用されているデバイス数のパーセンテージ）を表示します。
ライセンスのインストール	インストールしたライセンスおよびそのインストール日のリスト。
Install a License button	このボタンをクリックして、ライセンスファイルをインストールします。開いているこのダイアログボックスには、Cisco.com へのリンクが含まれています。ライセンスをまだ取得していない場合は、Cisco.com でライセンスを取得できます。ライセンス ファイルは、Security Manager サーバ上のローカル ドライブにコピーしてからインストールする必要があります。

[IPS] タブ、[Licensing] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、拡張機能はサポートしていません。

[Licensing] ページの [IPS] タブを使用して、インストール済みの IPS デバイス ライセンスのリストを表示したり、新しいライセンスまたは更新されたライセンスをインストールしたり、ライセンスを再展開したりします。このライセンス リストには、現在のライセンス、ライセンスを取得していないデバイス、ライセンスの有効期限が切れているデバイス、およびライセンスが無効なデバイスが表示されます。また、このページの設定を使用して、ライセンスが指定された日数以内に期限切れになるすべての IPS デバイスのレポートを送信できます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ライセンス（Licensing）] を選択し、[IPS] をクリックします。

関連項目

- IPS ライセンス ファイルの更新 （2299 ページ）
- IPS ライセンス ファイルの再展開 （2301 ページ）
- IPS ライセンス ファイル更新の自動化 （2301 ページ）
- [License Update Status Details] ダイアログボックス （725 ページ）
- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

フィールド リファレンス

表 149 : [IPS] タブ、[Licensing] ページ

要素	説明
IPS License Table	情報を最後にリフレッシュした時点での、デバイスインベントリ内のすべての IPS デバイスおよびそのライセンス ステータスを表示します。[更新（Refresh）]ボタンをクリックして、デバイスから最新の情報を取得します。 情報には、デバイスのシリアル番号（ライセンスの登録に使用）、ライセンス ステータス、およびライセンスの有効期限が含まれます。このリストには、現在のライセンスだけでなく、ライセンスを取得していないデバイス、ライセンスの有効期限が切れているデバイス、およびライセンスが無効なデバイスも表示されます。 **ヒント** このリストには、Cisco IOS IPS デバイスは含まれていません。Security Manager は、IPS を実行しているルータのライセンス管理には使用できません。

要素	説明
[Update Selected via CCO] ボタン	このボタンをクリックして Cisco.com に接続し、新しいライセンスを取得して、選択したデバイスのライセンスファイルを更新します。このボタンをクリックすると、ダイアログボックスが表示され、Cisco.com から更新可能なデバイスが示されます。選択したすべてのデバイスが表示されるとはかぎりません。[OK] をクリックして、更新を実行します。正常に更新するために、更新されたファイルがデバイスに自動的に適用されます。 この方法でライセンスを更新するには、選択したデバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。 ヒント　ライセンスが格納されたシスコのソフトウェアライセンスサーバ（SWIFT）は、同じサーバから 3 分間に 10 ライセンス以上の要求があると、その要求をブロックする場合があります。そのため、手動でライセンス更新を実行するときは、一度に選択するデバイスを 8 つ以下にしてください。
[Redeploy Selected Licenses] ボタン	このボタンをクリックして、選択したデバイスにライセンスを再展開します。ライセンスの再展開は、更新されたライセンス ファイルを取得し、そのファイルが自動更新時にデバイスに正常に適用されなかった場合に必要となる場合があります。 このボタンをクリックすると、ダイアログボックスが開き、再展開するライセンスのデバイスが表示されます。[OK] をクリックして、更新を実行します。正常に更新するために、更新されたファイルがデバイスに自動的に適用されます。
[Update from License File] ボタン	このボタンをクリックし、Security Manager サーバからライセンス ファイルを選択して、ライセンスを更新します。このボタンをクリックすると、ダイアログボックスが開き、そこでライセンスファイルを指定できます。[参照（Browse）]をクリックして、ファイルを選択します。ファイルは、Cisco Security Manager サーバー上のローカルドライブに存在する必要があります。[OK] をクリックすると、更新されたファイルがデバイスに自動的に適用されます。
[名前を付けてエクスポート（Export As）] ボタン	リストから 1 つ以上の IPS デバイスを選択し、[名前を付けてエクスポート（Export As）]ボタンをクリックして、ライセンスを Portable Document Format（PDF）またはカンマ区切り値（CSV）ファイルにエクスポートします。Security Manager サーバ上のフォルダを選択し、ファイル名を指定するように要求されます。リストからデバイスを選択しない場合、使用可能なすべてのデバイスのライセンスがエクスポートされます。

要素	説明
[Refresh License] ボタン	選択したデバイスの IPS ライセンステーブルのデータをリフレッシュするには、このボタンをクリックします。更新された情報がデバイスから取得されます。デバイスを選択しないと、すべてのデバイスのデータがリフレッシュされるため、リストに含まれるデバイスの数によっては長時間かかる場合があります。
Download and apply licenses Days before the expiration date	IPS ライセンスを Cisco.com から自動的にダウンロードし、それらのライセンスをデバイスに自動的に適用するかどうかを指定します。自動更新を設定するには、IPS デバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。 このオプションを選択した場合は、ライセンスの有効期限が切れるまでの日数も指定して、その間にライセンスをダウンロードして適用できるようにします。Security Manager は、ライセンスのないデバイス、ライセンスの有効期限が切れたデバイス、またはライセンスは有効だが、ここで指定した日数以内に期限切れになるデバイスだけを評価します。有効期限が現在のライセンスより長いか、または異なるライセンス情報を持つ、有効なライセンスのみが適用されます。
Discover devices daily at	自動ライセンス更新を選択した場合に、Security Manager がデバイスに接続して現在のライセンスのステータスを確認し、指定した日数以内に期限切れになるデバイスがあるかどうかを評価する時刻を指定します。1 つ以上のデバイスが有効期限切れの条件を満たしている場合にだけ、Cisco.com に接続します。
Email License Update Results 電子メール通知	有効期限切れのアラートとライセンス更新ジョブの結果を通知する電子メールを送信するかどうかを指定します。このオプションを選択した場合は、1 つ以上の電子メール アドレスも入力します（カンマ区切り）。
ライセンス有効期限ステータスの電子メール送信（Email License Expiration Status） 電子メール通知	ライセンスが指定された日数以内に期限切れになる IPS デバイスの PDF レポートを送信するかどうかを指定します。このオプションを選択した場合は、次のようになります。 • Cisco Security Manager が PDF レポートを送信するデバイスライセンスの有効期限までの日数（100 以下）を入力します。 • Cisco Security Manager がライセンスの有効期限をチェックする日時を選択します。 • ライセンス有効期限ステータス PDF レポートの送信先となる 1 つ以上の電子メールアドレス（カンマ区切り）を入力します。
[Save] ボタン	自動ライセンス更新と電子メール通知設定の変更を保存します。

ライセンスを更新または再展開する IPS デバイスの確認

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[ライセンス（Licensing）] > [IPS] タブでデバイスを選択し（[IPS] タブ、[Licensing] ページ（720 ページ）を参照）、Cisco.com（CCO）からライセンスを更新したり、ライセンスを再展開したりしようとすると、更新されるデバイスのリストが最初に表示されます。ダイアログボックスの名前は、実行するアクションによって異なります。

- [CCO経由でのライセンスの更新（Updating Licenses via CCO）] ダイアログボックス：Cisco.com から更新するために選択した IPS デバイスを確認します。このデバイス リストには、Cisco.com からライセンスを更新できる IPS デバイスが表示されます。選択したすべてのデバイスが表示されるとはかぎりません。

この方法でライセンスを更新するには、選択したデバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。

ヒント ライセンスが格納されたシスコのソフトウェア ライセンス サーバ（SWIFT）は、同じサーバから 3 分間に 10 ライセンス以上の要求があると、その要求をブロックする場合があります。そのため、手動でライセンス更新を実行するときは、一度に選択するデバイスを 8 つ以下にしてください。

- [ライセンスの再展開（Redeploying Licenses）] ダイアログボックス：ライセンスを再展開するために選択した IPS デバイスを確認します。ライセンスをデバイスに再展開する場合は、そのライセンスが展開済みである必要があります。Security Manager は、すでに IPS デバイスと関連付けられているファイルを使用して、ライセンスを再展開します。

[OK] をクリックすると、[ライセンス更新ステータスの詳細（License Update Status Details）] ダイアログボックスが開き、ライセンス再展開タスクのステータスを表示できます。 [License Update Status Details] ダイアログボックス （725 ページ）を参照してください。

ナビゲーション パス

これらのダイアログボックスを開くには、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ライセンス（Licensing）] > [IPS]** タブで 1 つ以上のデバイスを選択し、[CCO経由で選択内容を更新（Update Selected via CCO）] または [選択したライセンスの再展開（Redeploy Selected Licenses）] をクリックします。

IPS ライセンス ファイルの選択

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、拡張機能はサポートしていません。

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [ライセンス（Licensing）] > [IPS] タブで 1 つ以上のデバイスを選択し、[ライセンスファイルからの更新（Update from License File）] をクリックすると、[ファイルからライセンスを更新（Updating Licenses from File）] ダイアログボックスで使用するライセンスファイルを選択するように要求されます。

ライセンスファイルは Security Manager サーバーのローカルドライブに保存することが可能で、Security Manager のバージョン 4.5 以降は、クライアントのローカルドライブに保存できます。

[参照（Browse）] をクリックしてライセンスファイルを選択します。Ctrl を押しながらクリックして複数のライセンス ファイルを選択したり、Shift を押しながらクリックしてファイルの範囲を選択したりできます。

（注） Security Manager サーバーがインストールされているマシンとは別のマシンに Security Manager クライアントをインストールした場合は、クライアントマシンまたはサーバーマシンのどちらからライセンスファイルを選択するかを選択できます。クライアントとサーバーの両方が同じマシンにインストールされている場合、Security Manager では、ライセンスファイルをサーバーのみから選択できます。

使用するライセンスファイルを選択したら、[OK] をクリックして、それらのファイルを IPS デバイスに適用します。

（注） ライセンスファイルをクライアントマシンに保存する場合は、[デスクトップのカスタマイズ（Customize Desktop）] ページで [クライアント側のファイルブラウザを有効にする（Enable Client side file browser）] を選択する必要があります（[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）]）。

[License Update Status Details] ダイアログボックス

[License Update Status Details] ダイアログボックスを使用して、IPS ライセンス更新タスクのステータスを表示します。このダイアログボックスは、[Licensing] ページの [IPS] タブから更新タスクを起動するたびに開きます。詳細については、[IPS] タブ、[Licensing] ページ （720 ページ）を参照してください。

フィールド リファレンス

表 *150 : [License Update Status Details]* ダイアログボックス

要素	説明
進行状況バー	現在のデバイス上でライセンス更新タスクが何%完了したかを示します。
ステータス	更新タスクの現在の状態。
Devices to be updated	このタスク中に更新されるデバイスの総数。
Devices updated successfully	エラーが発生することなく更新されたデバイスの数。
Devices updated with errors	更新中にエラーが発生したデバイスの数。
Device list	更新されるデバイス。デバイス名、更新のステータス、および更新に関する概要情報が含まれます。デバイスを選択し、要約リストの下にあるメッセージリストで、そのデバイスの更新中に生成されたメッセージを確認します。
Messages list	ライセンス更新中に、選択したデバイスに関して生成されたメッセージ。メッセージを選択すると、リストの右側のフィールドに詳細情報が表示されます。
説明	[Message list] で選択されたメッセージに関する詳細情報。
操作	説明されている問題を解決するために実行する必要がある手順。
[Abort] ボタン	ライセンス更新タスクを中断します。

[Logs] ページ

[Logs]ページを使用して、監査ログおよび操作ログのデフォルト設定値を設定します。監査ログによって、Security Manager で発生したすべての状態変更の記録が保持されます。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ログ（Logs）] を選択します。

関連項目

- [Audit Report] ウィンドウの使用 （624 ページ）
- 監査レポートについて （623 ページ）
- 監査レポートの生成 （623 ページ）

• 監査ログ エントリのページ （627 ページ）

フィールド リファレンス

表 *151 : [Logs]* ページ

要素	説明
手動削除	
監査ログをDBに保持する期間（日）（Keep Audit Log in DB For (days)）	削除する前にデータベースに保存する必要がある監査ログエントリの最大日数。
最後の監査ログをDBに保持する（エントリ）（Keep Audit Log in DB For Last (entries)）	データベースに保存される監査ログエントリの最大数。エントリが、[Keep Audit Log For] フィールドで指定した日数よりも古くなると、ログに含まれているエントリがこの最大エントリ数より少ない場合でも、そのエントリは削除されます。
Purge Now	データベースから古いエントリを削除するには、[今すぐ削除（Purge Now）] をクリックします。[過去（日）の監査ログをDBに保持する（Keep audit log in DB for Last (days)）] フィールドおよび[最後の監査ログをDBに保持する（エントリ）（Keep audit log in DB for Last (entries)）] フィールドに入力された値に基づいて、最大数の監査ログエントリが削除されます。 たとえば、[最後の監査ログをDBに保持する期間（日）（Keep audit log in DB for Last (days)）] の値が 5 で、[最後のの監査ログをDBに保持する（エントリ）（Keep audit log in DB for Last (entries)）] の値が 5000 で、過去 5 日間のログエントリが 5000 を超える場合、Cisco Security Manager は過去の 5000 エントリを保持し、古いエントリ（過去 5 日間のエントリも対象）を削除します。 （注） [Purge Now] ボタンは、データベースから監査レポートを削除するだけです。<install_dir>\CSCOpx\MDC\log\audit フォルダの *.csv ファイルは削除されません。これらの *.csv ファイルは、直接削除できます。
監査ログファイルの保存期間（日）（Keep Audit Log File For (days)）	監査ログファイルをシステムに保持する日数。

要素	説明
Purge Now	指定した古い監査ログファイルをすぐに削除するには、このボタンをクリックします。 （注） [今すぐ削除（Purge Now）] ボタンは、<install_dir>\MDC\log\CSDL 監査ログフォルダから CSDL 監査ログファイルを削除し、<install_dir>\MDC\log\audit フォルダから監査ログファイルを削除します。
操作ログファイルの保存期間（日）（Keep Operation Log Files For (days)）	操作ログが、削除されるまで Security Manager によって保持される日数。これらのログは、デバッグのために使用されます。
[Purge Now] ボタン	指定した古い監査ログファイルをすぐ削除するには、このボタンをクリックします。
スケジュールされた削除	
監査ログデータベースエントリのスケジュールされた削除の有効化（Enable Scheduled Purging for Audit Log Database Entries）	古いログエントリの削除をスケジュールするには、このチェックボックスをオンします。このチェックボックスをオンすると、スケジュールオプションが有効になります。
監査ログをDBに保持する期間（日）（Keep Audit Log in DB For (days)）	削除する前にデータベースに保存する必要がある監査ログエントリの最大日数。
最後の監査ログをDBに保持する（エントリ）（Keep Audit Log in DB For Last (entries)）	データベースに保存される監査ログエントリの最大数。エントリが、[Keep Audit Log For] フィールドで指定した日数よりも古くなると、ログに含まれているエントリがこの最大エントリ数より少ない場合でも、そのエントリは削除されます。
監査ログファイルのスケジュールされた削除の有効化（Enable Scheduled Purging for Audit Log Files）	システムの監査ログの削除をスケジュールするには、このチェックボックスをオンします。
監査ログファイルの保存期間（日）（Keep Audit Log File For (days)）	監査ログファイルをシステムに保持する日数。
操作ログファイルのスケジュールされた削除の有効化（Enable Scheduled Purging for Operation Log Files）	システムの操作ログの削除をスケジュールするには、このチェックボックスをオンにします。

要素	説明
操作ログファイルの保存期間（日）（Keep Operation Log Files For (days)）	操作ログが、削除されるまで Security Manager によって保持される日数。これらのログは、デバッグのために使用されます。
ログ レベル（Log Level）	操作ログで収集する必要がある、重大度に基づく情報レベル。各レベルでは、異なる量のデータが収集されます。たとえば、情報レベルでは、ほとんどのデータが収集され、重大レベルでは、収集されるデータが最も少なくなります。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Policy Management] ページ

[Policy Management] ページを使用して、Security Manager で管理するルータおよびファイアウォールのポリシータイプを選択します。これらの選択内容は、ルータおよびファイアウォールデバイスに適用されますが、IPS デバイスには適用されません。デフォルトでは、すべてのポリシーが管理対象として選択されています。

管理対象外のポリシーは、デバイス ビューとポリシー ビューの両方から削除されます。管理対象外のポリシー（ローカルまたは共有）は、Security Manager データベースから削除されます。唯一の例外は、インターフェイス ポリシーです。インターフェイス ポリシーは、Security Manager に引き続き表示されますが、読み取り専用ポリシーのマークが付けられます。ファイアウォール デバイスの場合、インターフェイスおよびフェールオーバーの設定は、1 つのユニットと見なされ、両方が管理対象となるか、または管理対象外となります。

ポリシータイプを管理する方法および管理対象外とする方法（これらの設定を変更する前後に実行する必要がある内容を含む）の詳細については、ルータおよびファイアウォール デバイスのポリシー管理のカスタマイズ （221 ページ）を参照してください。

注意 AUS または CNS を使用して設定を ASA または PIX デバイスに展開する場合は、デバイスが AUS または CNS から完全な設定をダウンロードする点に注意してください。そのため、Security Manager で管理されているポリシーを減らすと、実際にはデバイスから設定が削除されます。管理対象の一部の ASA/PIX ポリシーを選択解除し、Security Manager とともに他のアプリケーションを使用してデバイスを設定する場合は、AUS または CNS を使用しないでください。

ナビゲーション パス

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ポリシー管理（Policy Management）] を選択します。

フィールド リファレンス

表 *152 : [Policy Management]* ページ

要素	説明
Policies to Manage	ポリシー タイプは、フォルダで整理されます。個別に処理されるルータとファイアウォール（すべての ASA、PIX、および FWSM デバイスを含む）別に整理され、次に、カテゴリ（[NAT]、[Interfaces]、および [Platform]）別に整理されます。必要に応じてポリシータイプを選択または選択解除し、[保存（Save）] をクリックします。ポリシーのグループのチェックボックスをオフにすると、そのグループのすべてのポリシーの選択が解除されます。デフォルトでは、すべてのポリシーが選択されています。 （注） バージョン 4.18 以降、Cisco Security Manager は、Cisco Umbrella サーバーで設定される ASA 9.10(1) デバイスのサポートを提供します。

要素	説明
Display a warning on all shared policies and imported objects	すべての共有ポリシーと、[ファイル（File）]>[インポート（Import）] コマンドでインポートされたオブジェクトに、メッセージを追加するかどうかを指定します。このオプションを選択すると、次のものにメッセージが表示されます。 • すべての共有ポリシー（インポートされたかローカルで作成されたかを問いません）。 • [ファイル（File）]>[インポート（Import）] コマンドを使用してデバイスまたは共有ポリシーをインポートすることで作成されたポリシーオブジェクト。PolicyObjectImportExport.pl コマンド（ポリシー オブジェクトのインポートおよびエクスポート （318ページ）を参照）によって作成され、インポートされたポリシーオブジェクトは含まれません。 共有ポリシーを定期的にインポートすると、インポートされたポリシーおよびオブジェクトによって同名のポリシーおよびオブジェクトが置換されて、ローカルで行った変更が削除されます。このメッセージは、ポリシーがインポートされる可能性があることをユーザに通知し、編集しないポリシーオブジェクトをユーザが識別するために役立ちます。 **ヒント** ポリシーまたはデバイスをインポートするとき、このオプションの設定を選択するように要求されます。そのため、ポリシーまたはデバイスをインポートするユーザは、必要な認可を受けていれば、このページにアクセスすることなくこの設定を変更できます。この変更は、インポートの実行者が変更を送信（必要に応じて承認）したあとにだけ、有効になります。詳細については、ポリシーまたはデバイスのインポート （615ページ）を参照してください。
[Save] ボタン	変更内容を保存します。 ポリシーを管理対象外とする場合、そのポリシーが割り当てられているデバイスのリストが表示されます。Security Manager は、ポリシーの割り当てを解除するために、すべてのデバイスから必要なロックを取得できる必要があります。そうでない場合、ポリシーを管理対象外とする前に、手動でポリシーの割り当てを解除（またはロックを削除）する必要があります。 前に管理対象外であったポリシーを管理対象にする場合は、影響を受けるすべてのデバイスを再検出して、既存の設定値を Security Manager に含める必要があります。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Policy Objects] ページ

[Policy Objects] ページを使用して、ポリシー オブジェクトの作成に関するシステム デフォルトを定義します。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ポリシーオブジェクト（Policy Objects）] を選択します。

関連項目

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- ポリシー オブジェクトの管理 （287 ページ）

フィールド リファレンス

表 *153 : [Policy Objects]* ページ

要素	説明
When Redundant Objects Detected	既存のオブジェクトと同じ定義を持つポリシー オブジェクトを作成しようとしたときに、Security Manager で実行するアクション： • [Ignore]：同一の定義を持つオブジェクトを自由に作成できます。すべての競合は無視されます。 • [Warn]：既存のオブジェクトと同じオブジェクトを作成しようとすると、警告が表示されます。必要な場合は、オブジェクトの作成に進むことができます。 • [Enforce]：既存のオブジェクトと同じオブジェクトを作成することが禁止されます。エラー メッセージが表示されます。

要素	説明
Default Source Ports	サービス オブジェクトのデフォルト送信元ポート範囲として使用するポート範囲値。次のいずれかを選択できます。 • [Use all ports]：1 ～ 65535 のすべてのポートが含まれます。 • [Use secure ports]：1024 ～ 65535 のすべてのポートが含まれます。 デフォルトの送信元ポートを変更した場合は、影響を受ける可能性がある、以前展開されていたすべてのデバイスに手動で再展開する必要があります。これらの変更内容は、データをリフレッシュするまで、開いているアクティビティには反映されない場合があります。 ポート リスト オブジェクトの詳細については、ポート リスト オブジェクトの設定 （420 ページ）を参照してください。
Enable AutoComplete Dropdown Box	ユーザがサービスを作成するときに、ユーザの入力に一致するサービス名およびポート リスト名を Security Manager が表示するかどうかを指定します。これにより、すでに定義している名前から簡単に選択できるようになります。オートコンプリートの選択を解除すると、正確なサービス名およびポート リスト名を覚えておき、自分で入力する必要があります。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[プロセスモニタリングの設定（Process Monitoring Settings）] ページ

[プロセスモニタリングの設定（Process Monitoring Settings）] ページを使用して、プロセスモニタリングを有効にします。このページで、特定のプロセスのモニタリングを有効または無効にしたり、モニタリング間隔や電子メールアドレスなどの通知設定を行ったりすることができます。この設定により、プロセスが停止したときに、指定された受信者に電子メール通知が送信されます。

はじめる前に

電子メールアラートを受信できるようにするため、CS Web コンソールで SMTP サーバーと送信者メールを設定します。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [プロセスモニタリングの設定（Process Monitoring Settings）] を選択します。

フィールド リファレンス

表 *154 : [プロセスモニタリングの設定（Process Monitoring Settings）] ページ*

要素	説明
[プロセスモニタリングの有効化（Enable Process Monitoring）]	選択すると、Security Manager でモニタリングするプロセスを指定できます。続いて他のプロセスモニタリングの設定を行う必要があります。 デフォルトでは、プロセスモニタリング機能は Cisco Security Manager サーバーで無効になっています。 （注） プロセスモニタリングを有効または無効にすると、Windows レジストリが変更され、システムアラートが生成される場合があります。
[モニタリング間隔（分単位）（Monitor Interval (in Minutes)）]	プロセスをモニタリングする間隔を指定します。有効な値は 1 ～ 60 分です。デフォルトのモニタリング間隔は 5 分です。 （注） モニタリング間隔が変更されると、進行中のモニタリングタスクが停止し、新しいモニタリングタスクが更新された間隔で開始されます。
[通知受信者の電子メール（Notification Recipient(s) E-mail(s)）]	通知受信者の電子メールIDを入力します。複数の電子メールIDをカンマで区切って入力できます。通知受信者は、モニタリングされているプロセスが停止したときに通知される受信者です。
[最大メールアラート数（Maximum Mail Alerts）]	Security Manager の実行時に受信者に送信される電子メールの最大数を入力します。この項目のデフォルト値は 10 です。
[プロセスリスト（Process List）]	モニタリングするプロセスを 1 つ以上選択します。選択したプロセスのいずれかが停止すると、指定された受信者に通知メールが送信されます。 （注） [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] で、[イベント管理（Event Management）]、[正常性およびパフォーマンスのモニタリング（Health and Performance Monitor）]、[Report Manager] が無効になっている場合、[プロセスモニタリングの設定（Process Monitoring Settings）] ページで VmsEventServer、CsmHPMServer、および CsmReportServer の各プロセスが有効になっていても、電子メール通知は送信されません。

要素	説明
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[シングルサインオンの設定（Single Sign-on Configuration）] ページ

[Cisco Security Manager管理（Security Manager Administration）] ウィンドウの [シングルサインオンの設定（Single Sign-on Configuration）] ページを使用して、Cisco Prime Security Manager または FireSIGHT Management Center のクロス起動に使用する「シングルサインオン」（SSO）共有キーを有効にして設定します。

（注） シングルサインオンを使用することで、ユーザーは、Prime Security Manager や FireSIGHT Management Center に個別にログインすることなく、Cisco Security Manager から Prime Security Manager または FireSIGHT Management Center をクロス起動できます。ただし、Prime Security Manager や FireSIGHT Management Center をクロス起動するために SSO は必要ありません。

ヒント Cisco Prime Security Manager は、ASA CX モジュールの管理に使用されます。FireSIGHT Management Center は、ASA FirePOWER モジュールの管理に使用されます。

関連項目

- ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）
- Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）
- PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有 （3708 ページ）

ナビゲーション パス

1. **[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）]** を選択し、目次から [シングルサインオンの設定（Single Sign-on Configuration）] を選択します。

2. [Prime Security Managerの有効化（Enable for Prime Security Manager）] チェックボックスまたは [FireSIGHT Management Centerの有効化（Enable for FireSIGHT Management Center）] チェックボックスを選択します。

フィールド リファレンス

表 *155 : [シングルサインオンの設定（Single Sign-on Configuration）] ページ*

要素	説明
Prime Security Managerの有効化（Enable for Prime Security Manager）	[チェックボックス] Prime Security Manager の SSO 機能を有効または無効にできます。無効の場合、共有キーが保持されます。
FireSIGHT Management Centerの有効化（Enable for FireSIGHT Management Center）	[チェックボックス] FireSIGHT Management Center の SSO 機能を有効または無効にできます。無効の場合、共有キーが保持されます。
シングルサインオンの共有キー（Shared Key for Single Sign-on）	このセクションの機能を使用して、Prime Security Manager または FireSIGHT Management Center をクロス起動するための暗号化キーを生成および表示します。 [生成（Generate）] ボタンをクリックして、128 ビットの AES キーをランダムに生成します。このキーは、[SSO共有キー（SSO Shared Key）] フィールドに 32 桁の 16 進数文字列として表示されます。 （注） このキーは、Prime Security Manager または FireSIGHT Management Center でシングルサインオンクロス起動を設定するときに指定する必要があります。また、許可された各 Cisco Security Manager ユーザーは、Prime Security Manager データベースまたは FireSIGHT Management Center ユーザーデータベースで、Cisco Security Manager ユーザーデータベースと同じユーザー名で設定する必要があります（パスワードは異なる場合があります）。 ヒント PRSM での SSO の設定については、ASA CX および Cisco Prime Security Manager のユーザーガイド [英語]（Cisco ASA CX Context-Aware Security End-User Guides）の「Configuring Single Sign-On for Cisco Security Manager」を参照してください。

[Rule Expiration] ページ

[Rule Expiration] ページを使用して、ポリシールールの有効期限のデフォルト値を定義します。一部のタイプのポリシールール（アクセス ルールなど）のポリシーを作成するときに、その

ルールの有効期限を設定できます。また、Security Manager は、有効期限が近づくと電子メールで通知できます。

電子メール通知をイネーブルにするように、SMTP サーバを設定する必要があります。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [有効期限（Expiration）] を選択します。

フィールド リファレンス

表 156 : [Rule Expiration] ページ

要素	説明
Notify Email	ルールの有効期限の通知を受信する、デフォルトの電子メール アドレス。ユーザは、個々のルールを設定するときにこのアドレスをオーバーライドできます。
Notify Before Expiration	Security Manager が電子メール メッセージを送信する、ルールの有効期限が切れる前のデフォルト日数。ユーザは、個々のルールを設定するときにこの値をオーバーライドできます。
送信者（Sender）	Security Manager が電子メール通知を送信するために使用する電子メール アドレス。
Email Format	電子メール メッセージの形式： • [Text]：電子メールは、HTML 形式およびプレーン テキスト形式で送信されます。 • [XML]：電子メールは、XML マークアップを使用して送信されます。このオプションは、通知に対する処理および応答を自動的に行うプログラムを記述する場合に適しています。
[Save] ボタン	変更内容を保存します。
リセット ボタン	すべてのフィールドを以前の値に復元します。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Server Security] ページ

[Server Security] ページを使用して、CiscoWorks Common Services アプリケーションの特定のページを開きます。これらのページでは、Security Manager サーバでのさまざまなセキュリティ

機能を設定できます。CiscoWorks Common Services によって、ユーザ アクセス コントロールやシステム セキュリティなど、Security Manager サーバの基本的な機能が制御されます。

Security Manager にログインするときに、ユーザ名とパスワードが、（インストール時に AAA プロバイダーとして設定したシステムに応じて）CiscoWorks または Cisco Secure Access Control Server（ACS）データベースに格納されているアカウント情報と比較されます。クレデンシャルの認証後、割り当てられているロールに応じたアクセスを実行できます。

Common Services ロールが、Security Manager におけるユーザー機能に変換される方法など、Security Manager のロールおよび権限の詳細については、『Installation Guide for Cisco Security Manager』を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager 管理（Security Manager Administration）] を選択し、目次から [サーバーセキュリティ（Server Security）] を選択します。

フィールド リファレンス

表 *157 : [Server Security]* ページ

要素	説明
[AAA Setup] ボタン	Common Services を開き、[AAA Mode Setup] ページを表示します。このページで、AAA をフォールバック サインオン方式として設定できます。AAA の詳細については、[AAA モードのセットアップ（AAA Mode Setup）] ページの [ヘルプ（Help）] をクリックして参照してください。
[Certificate Setup] ボタン	Common Services を開き、[Self-Signed Certificate Setup] ページを表示します。CiscoWorks を使用すると、自己署名セキュリティ証明書を作成できます。この証明書を使用して、クライアントブラウザと管理サーバ間の SSL 接続をイネーブルにできます。自己署名証明書の詳細については、[証明書のセットアップ（Certificate Setup）] ページの [ヘルプ（Help）] をクリックして参照してください。
[Single Sign On] ボタン	Common Services を開き、[Single Sign-On Setup] ページを表示します。Single Sign-On（SSO; シングル サインオン）を使用すると、ブラウザ セッションを使用して、複数の CiscoWorks サーバに透過的にナビゲートできます。各サーバで認証を受ける必要はありません。複数の CiscoWorks サーバ間の通信は、証明書と共有秘密キーによって対処されるトラスト モードでイネーブルになります。SSO のセットアップの詳細については、[シングルサイノン（Single Sign-On）] ページの [ヘルプ（Help）] をクリックして参照してください。

要素	説明
[Local User Setup]	Common Services を開き、[Local User Setup] ページを表示します。このページでは、ユーザを追加および削除したり、ユーザ設定を編集したり、ロールや権限を割り当てたりできます。詳細については、[ローカルユーザーのセットアップ（Local User Setup）] ページの [ヘルプ（Help）] をクリックし、『Installation Guide for Cisco Security Manager』を参照してください。
[System Identity Setup]	Common Services を開き、[System Identity Setup] ページを表示します。複数の CiscoWorks サーバ間の通信は、証明書と共有秘密キーによって対処されるトラスト モードでイネーブルになります。システム ID を設定すると、複数サーバ セットアップの一部であるサーバ上に信頼ユーザを作成できます。システム ID の設定の詳細については、[システム ID のセットアップ（System Identity Setup）] ページの [ヘルプ（Help）] をクリックして参照してください。
[ネイティブ RBAC パラメータ（Native RBAC Parameters）]	
[ローカル ユーザー データベースで使用できないユーザー ID のログオンを許可（Allow logon for user ids not available in Local User Database）]	Active Directory、TACACS+、または RADIUS などの外部認証サーバーと統合された Security Manager インストールの場合、ユーザー名が Security Manager ユーザーリストで定義されていなくてもユーザーがログインできるかどうかを指定します。オンにすると、ユーザーはロール管理セットアップで指定されたデフォルトのロールを使用してログインできます。デフォルトのロールが設定されていない場合、ユーザーはログインを許可されません。

[Take Over User Session] ページ

[ユーザセッションの引き継ぎ（Take Over User Session）] ページを使用して、別のユーザの設定セッションを引き継ぎます。管理権限を持つユーザは、Workflow 以外のモードで別のユーザの作業を引き継ぐことができます。デバイスおよびポリシーが、ユーザによって操作されているためにロックされているが、別のユーザが同じデバイスおよびポリシーへのアクセスを必要としている場合、セッションの引き継ぎが役立ちます。ただし、別のユーザのセッションを引き継ぐと、現在のセッションは廃棄されるため、セッションを引き継ぐ前に、変更内容を必ず送信してください。

テーブルには、現在の設定セッションがすべて表示され、ユーザ名とセッションの状態、およびユーザが現在ログインしているかログアウトしているかが示されます。引き継ぐ設定セッションを選択し、[セッションの引き継ぎ（Take over session）] をクリックします。セッションは、ユーザがセッション中に保存した変更内容を含め、現在の状態で転送されます。

選択したユーザが、セッションを引き継ぐときにログインしている場合、そのユーザは、警告メッセージを受信し、進行中の保存していない変更内容は失われ、ログアウトされます。

詳細については、別のユーザの作業の引き継ぎ （628 ページ）を参照してください。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ユーザセッションの引き継ぎ（Take Over User Session）] を選択します。

[チケット管理（Ticket Management）] ページ

[チケット管理（Ticket Management）] ページを使用して、チケット管理をイネーブルにし、外部の変更管理システムと統合するためのチケット発行システムの URL を設定し、チケット情報の消去設定を構成します。

チケット管理がイネーブルになっている場合、すべてのイメージ管理インストールジョブにはチケットが割り当てられている必要があります。それ以外の場合、ジョブは実行されません。

ナビゲーション パス

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [チケット管理（Ticket Management）] を選択します。

関連項目

- ワークフロー モードの変更　（36 ページ）
- Workflow モードの比較　（29 ページ）

フィールド リファレンス

表 *158 : [チケット管理（Ticket Management）] ページ*

要素	説明
チケットの有効化（Enable Ticketing）	チケット管理をイネーブルにするかどうかを指定します。
システム生成のデフォルトのチケット名（System Generated Default Ticket Name）	デフォルトでは、このチェック ボックスはオンになっています。チケット名にシステム生成のデフォルト名を付加しない場合は、チェックボックスをオフにします。アクティビティ作成ダイアログのチケット名フィールドは空白のままです。
チケットシステムURL（Ticketing System URL）	

要素	説明
チケットシステムURL（Ticketing System URL）	外部変更管理システムの起動に使用する URL。このフィールドが設定されている場合、チケット ID は、指定された URL を起動するハイパーリンクです。URL の形式は、チケット ID がURL の一部として組み込まれるテンプレートになっている必要があります。テンプレート形式では、実際のチケット ID の代わりに {0} を使用します。 たとえば、チケット ID が *TKT12345* のチケットの外部チケット管理システムを起動する URL が http://ticketsystem/displayticket?ticketid=TKT12345 である場合、使用するテンプレート URL は **http://ticketsystem/displayticket?ticketid={0}** となります。 チケットを作成すると、指定したチケット ID がハイパーリンクの {0} の代わりに使用されます。
生成	クリックすると、チケットシステム URL の作成に使用できる [テンプレートURLの生成（Generate Template URL）] ダイアログボックスが表示されます。 上記の例を使用すると、[チケット ID（Ticket ID）] フィールドに **TKT12345** と入力し、[チケット URL（Ticket URL）] フィールドに **http://ticketsystem/displayticket?ticketid=TKT12345** と入力します。[OK] をクリックすると、適切なテンプレート URL が作成され、[チケットシステムURL（Ticketing System URL）] フィールドに入力されます。
[チケット履歴（Ticket History）] チケット履歴の設定は、非ワークフローモードでのみ使用できます。ワークフローモードでは、消去設定はアクティビティの設定を介して制御されます（[Workflow] ページ （745 ページ）を参照）。	
次より古いチケット（変更レポートを含む）を消去（Purge Tickets (including change report) Older than）	チケット情報を Ticket Manager テーブルに保持する日数。デフォルトは 30 です。1 ～ 120 日まで指定できます。 [今すぐ消去（Purge Now）] をクリックすると、指定した日数よりも古いすべてのチケットが削除されます。
次より古い変更レポートを消去（Purge Change Report older than）	変更レポートが保持される日数。デフォルトは30です。[次より古いチケット（変更レポートを含む）を消去（Purge Tickets (including change report) Older than）] 設定よりも小さい値を指定できます。 [今すぐ消去（Purge Now）] をクリックすると、指定した日数よりも古いすべての変更レポートが削除されます。
[Save] ボタン	変更内容を保存します。

要素	説明
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[Token Management] ページ

[Token Management] ページを使用して、Token Management System（TMS）を通信プロトコルとして使用している Cisco IOS ルータに設定を展開するために使用する TMS サーバを指定します。Security Manager は、このページ上の設定を使用して、TMS サーバに接続します。

Security Manager は、FTP を使用して、デルタ設定ファイルを TMS サーバに展開します。TMS サーバから eToken に設定ファイルをダウンロードし、暗号化できます。

Cisco IOS ルータで TMS を使用するには、TMS をトランスポート プロトコルとして指定する必要があります。すべてのルータの場合は [Device Communication] ページ（[Device Communication] ページ （668 ページ）を参照）で指定し、特定のルータの場合はそのデバイス プロパティ（[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ （137 ページ）を参照）で指定できます。TMS サーバを FTP サーバとして設定する必要もあります。設定しないと、展開は失敗します。

ナビゲーション パス

[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [トークン管理（Token Management）] を選択します。

関連項目

- Token Management Server への設定の展開 （534 ページ）
- 展開方法について （490 ページ）

フィールド リファレンス

表 159 : [Token Management] ページ

要素	説明
[Server Name] または [IP Address]	TMS サーバの DNS ホスト名または IP アドレス。
ユーザー名	Security Manager が、TMS サーバにログインするときに使用するユーザ名。
Password Confirm Password	ユーザー名のパスワード。両方のフィールドにパスワードを入力します。

要素	説明
Directory in the TMS Server for Config Files	展開された設定ファイルがダウンロードされる、TMS サーバ上のディレクトリ。ルート FTP ディレクトリ（「.」）が、TMS サーバー上のデフォルトの FTP ロケーションです。
Public Key File Location	TMS サーバからコピーされた、Security Manager サーバ上の公開キー ファイルと秘密キー ファイルの場所。Security Manager は、この公開キーを使用して、TMS サーバに送信されるデータを暗号化します。次に、サーバはその秘密キーを使用してデータを復号化します。Security Manager には、サーバ上のデフォルトの秘密キーと一致する、デフォルトの公開キーが用意されています。 （注） 必要に応じて、TMS サーバを使用して、公開キーと秘密キーの新しいペアを生成できます。生成した場合は、新しい公開キーを Security Manager サーバにコピーする必要があります。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[VPN Policy Defaults] ページ

[VPN Policy Defaults] ページを使用して、Security Manager が各 IPsec テクノロジーに使用するデフォルトの VPN ポリシーを表示または割り当てます。ポリシーをデフォルトとして選択する前に、そのポリシーを共有ポリシーとして作成し、データベースに送信し、承認を受ける必要があります。このページからポリシーを作成することはできません。これらのデフォルトを設定する方法の詳細については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。

VPN トポロジに関連する各タブでは、各ポリシー タイプのドロップダウン リストに、選択可能な既存の共有ポリシーが示されます。ポリシーを選択して [コンテンツを表示（View Content）] ボタンをクリックすると、そのポリシーの定義を参照できます。場合によっては変更できますが、その変更は保存できません。

Security Manager は、VPN ポリシーのデフォルトを使用して、ポリシーの一貫性を維持すると同時に、VPN 設定を簡素化します。Security Manager は、必須ポリシー用に出荷時のデフォルト ポリシーを提供します。これにより、VPN が機能するために VPN トポロジ内のデバイスで設定する必要がある設定値が提供されます。必須ポリシーは、割り当てられている IPsec テクノロジーによって変わります。デフォルトの設定値を持つ出荷時のデフォルト ポリシーを使用すると、VPN トポロジの作成後すぐにデバイスに展開できます。デフォルト設定は、オプションのポリシーには提供されません。出荷時のデフォルト設定を使用する代わりに、異なるデフォルト設定を提供するために共有ポリシーを作成する必要がある場合があります。

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [VPNポリシーのデフォルト（VPN Policy Defaults）] を選択します。

関連項目

- 新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て （1463 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （1703 ページ）

フィールド リファレンス

表 *160 : [VPN Policy Defaults]* ページ

要素	説明
[DMVPN] タブ	ダイナミック マルチポイント VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[Large Scale DMVPN] タブ	大規模ダイナミック マルチポイント VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[Easy VPN] タブ	Easy VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[IPsec/GRE] タブ	IPsec/GRE VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[GRE Dynamic IP] タブ	GRE ダイナミック IP VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[Regular IPsec] タブ	通常の IPsec VPN テクノロジー用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。
[通常の IPSec VTI（Regular IPsec VTI）] タブ	通常の、トンネルベースの IPsec VPN テクノロジー用のデフォルトポリシーを設定できるポリシータイプが一覧表示されます。
GET VPN	Group Encrypted Transport（GET）VPN テクノロジー用のデフォルトポリシーを設定できるポリシータイプが一覧表示されます。
リモート アクセス VPN	IPsec リモート アクセス VPN 用のデフォルト ポリシーを設定できるポリシー タイプが一覧表示されます。

要素	説明
[S2S Endpoints] タブ	サイト間VPNにおける内部インターフェイスと外部インターフェイスのデフォルトのエンドポイントを定義するインターフェイスロール。

[Workflow] ページ

[Workflow] ページを使用して、Security Manager が適用するワークフロー モードを選択します。また、アクティビティおよび展開ジョブの通知とログのデフォルト設定を定義します。

ワークフローモードを変更する前に、次の項で、モードの相違、およびモード変更による影響を確認してください。

- Workflow モードの作業 （27 ページ）
- Workflow 以外のモードの作業 （28 ページ）
- Workflow モードの比較 （29 ページ）
- ワークフロー モードの変更 （36 ページ）

ナビゲーション パス

[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ワークフロー（Workflow）] を選択します。

関連項目

- アクティビティの管理 （177 ページ）
- 展開の管理 （481 ページ）

フィールド リファレンス

表 161 : [Workflow] ページ

要素	説明
Workflow Control	
Enable Workflow	Workflow モードをイネーブルにするかどうかを指定します。Workflow モードをイネーブルにすると、アクティビティおよび展開ジョブのアプルーバを設定するかどうかを選択できます。

要素	説明
Require Activity Approval	アクティビティが、割り当てられたアプルーバによって明示的に承認される必要があるかどうかを指定します。アプルーバの有無による処理の違いについては、アクティビティの承認 （179 ページ）を参照してください。
提出者はアクティビティを承認できる（Submitter can Approve Activity）	アクティビティは提出者によって承認されます。
[展開とインストールイメージに承認が必要（Require Deployment & Install Image Approval）]	展開ジョブおよびインストールイメージジョブが、割り当てられたアプルーバによって明示的に承認される必要があるかどうかを指定します。アプルーバの有無による処理の違いについては、展開について （481 ページ）を参照してください。
提出者は展開ジョブを承認できる（Submitter can Approve Deployment Jobs）	展開ジョブは送信者が承認できます。
システム生成のデフォルトのアクティビティ名（System Generated Default Activity Name）	デフォルトでは、このチェックボックスはオンになっています。アクティビティ名にシステム生成のデフォルト名を付加しない場合は、チェックボックスをオフにします。アクティビティ作成ダイアログのアクティビティ名フィールドは空白のままになります。
電子メールの通知	
送信者（Sender）	Security Manager が電子メール通知を送信するために使用する電子メール アドレス。
Activity Approver	アクティビティの承認担当者のデフォルトの電子メール アドレス。ユーザは、承認のためにアクティビティを送信するときに、このアドレスをオーバーライドできます。詳細については、承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） （202 ページ）を参照してください。
Job/Schedule Approver	展開ジョブまたはスケジュールの承認担当者のデフォルトの電子メール アドレス。ユーザは、承認のためにジョブまたはスケジュールを送信するときに、このアドレスをオーバーライドできます。詳細については、展開ジョブの送信 （528 ページ）を参照してください。

要素	説明
Require Deployment Status Notification Include Job Deployer Job Completion Notification	展開ジョブのステータスが変更されるたびに、電子メール通知を送信するかどうかを指定します。このオプションを選択した場合は、通知を受信する電子メール アドレスを [Job Completion Notification] フィールドに入力します。カンマで複数のアドレスを区切ります。 [Include Job Deployer] を選択して、ジョブを展開した担当者の電子メール アドレスを通知電子メール メッセージに含めることもできます。
Workflow History	
Keep Activity for	アクティビティ情報を [Activity] テーブルで保持する日数。デフォルトは 30 です。1 ～ 180 日を指定できます。 [今すぐ消去（Purge Now）] をクリックして、指定した日数よりも古いすべてのアクティビティを削除します。 （注） Workflow 以外のモードでチケット発行が有効になっている場合、消去設定はチケットの設定を介して制御されます（[チケット管理（Ticket Management）] ページ（740 ページ）を参照）。
Keep Job for	展開ジョブ情報を [Deployment Job] テーブルで保持する日数。デフォルトは 30 です。1 ～ 180 日を指定できます。 [今すぐ消去（Purge Now）] をクリックして、指定した日数よりも古いすべてのジョブを削除します。
Keep job per schedule for	展開ジョブ情報を、各ジョブ スケジュールの [Deployment Job] テーブルで保持する日数。この設定は、スケジュールを使用して開始されたジョブだけに適用されます。デフォルトは 30 です。1 ～ 180 日を指定できます。 [今すぐ消去（Purge Now）] をクリックして、指定した日数よりも古いすべてのジョブを削除します。
[Save] ボタン	変更内容を保存します。
リセット ボタン	変更を以前に適用した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

[ウォール設定（Wall Settings）] ページ

Security Manager の [ウォール設定（Wall Settings）] ページでは、ウォール機能を有効または無効にできます。

「ウォール」機能は、「ShoutBox」機能とも呼ばれます。この機能を使用して、同じ Security Manager サーバーにログインしているすべてのユーザーにメッセージを送信できます。ただし、まず [ウォール設定（Wall Settings）] ページで機能を有効にする必要があります。

（注） 管理者ユーザーのみがウォール機能を有効または無効にする権限を持っていますが、すべてのユーザーはメッセージを送信する権限を持っています。

たとえば、ウォール機能を使用して、Security Manager のインストールでいくつかの変更を行いながら、他のユーザーと対話することができます。対話の内容は、多くの場合、行われている変更や、変更に対して実行される特定の即時アクションに関するものです。送信されるメッセージは、ログインしているすべてのユーザーにブロードキャストされます。ウォール機能を使用すると、ユーザーは、ログイン時に他のユーザーが表示できる基本的なプロファイル情報を入力できます。ウォール機能の重要な用途の 1 つは、現在ログインしているすべてのユーザーのリストを表示することです（ユーザーは、アイドルタイムアウトの後、または Security Manager クライアントを介してログアウトした後、[ウォール（Wall）] ウィンドウから削除されます）。

ウォール機能を使用して、*.pdf、*.xls、またはその他のファイルを添付送信することはできません。

ナビゲーション パス

[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] をクリックし、コンテンツテーブルから [ウォール設定（Wall Settings）] を選択します。

フィールド リファレンス

表 *162 : [ウォール設定（Wall Settings）] ページ*

要素	説明
ユーザーが他のユーザーにメッセージを送信できるようにします。	ウォール機能を有効にするか無効にするかを指定します。
[Save] ボタン	変更を保存して適用します。
リセット ボタン	変更を前回保存した値にリセットします。
[Restore Defaults] ボタン	値を Security Manager のデフォルトにリセットします。

ウォール機能が有効になっている場合、[ツール（Tool）] > [壁...（Wall...）] をクリックするか、Configuration Manager で [ウォール（Wall）] アイコンをクリックして、[ウォール（Wall）] ウィンドウを開くことができます。

Health and Performance Monitor または Image Manager で [ウォール（Wall）] アイコンをクリックして、[ウォール（Wall）] ウィンドウを開くこともできます。イベントビューアまたはReport Manager で [ウォール（Wall）] ウィンドウを開くことはできません。

ヘルプアイコンをクリックすると、[ウォール（Wall）] で詳細なウォール機能のヘルプを利用できます。

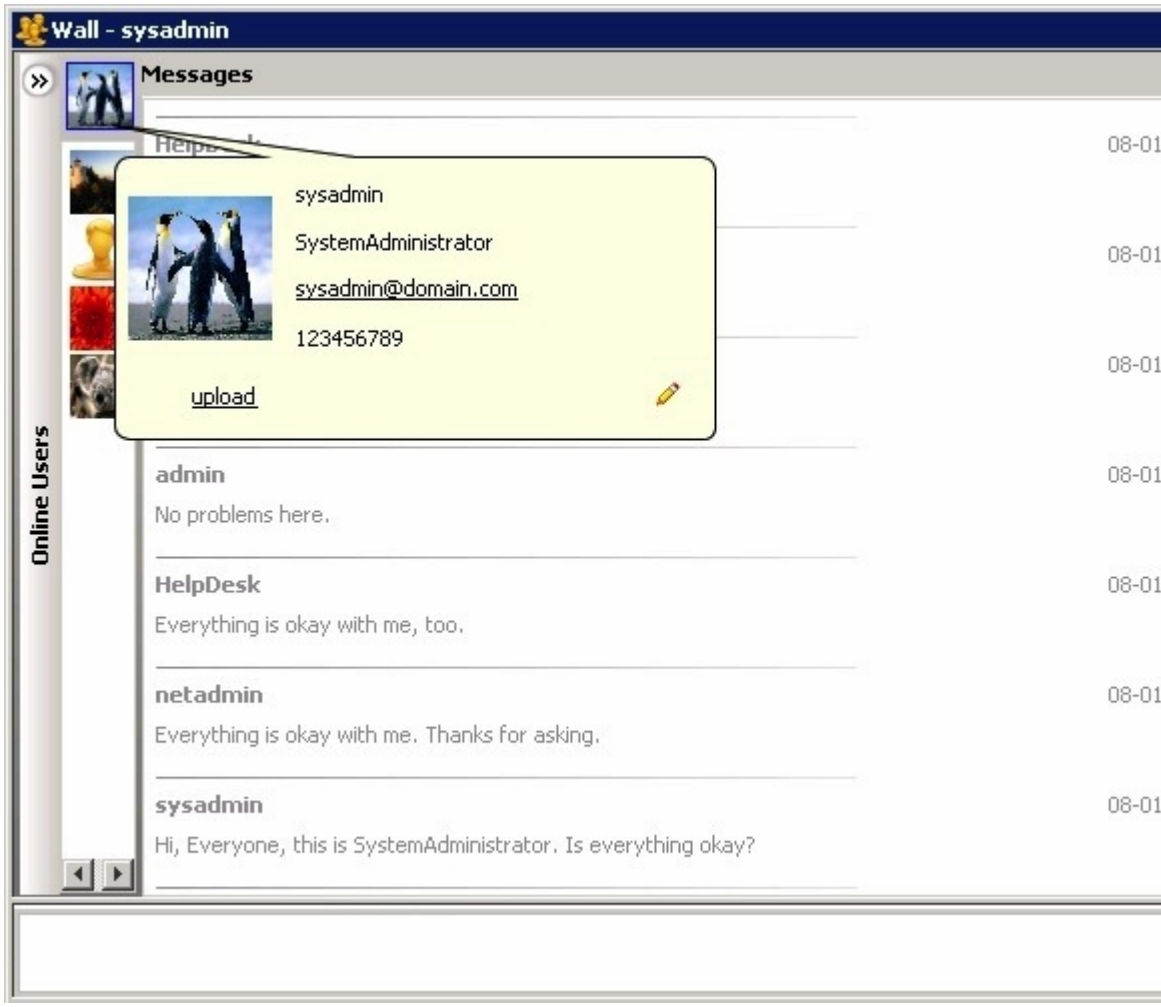
[ウォール（Wall）] ウィンドウには、次の要素が含まれています。

- 左側ペイン。同じ Security Manager サーバーにログインしているユーザーと展開/折りたたみボタンを表示します。
- 右側ペイン。ページの大部分を占めており、ユーザーが送信したメッセージのテキストが含まれます。右側ペインには、ウォールアラートを有効または無効にするボタンと、クリックして詳細なヘルプを表示できるヘルプアイコンもあります。

[ウォール（Wall）] ウィンドウの概要	
メッセージの表示	メッセージは、[ウォール（Wall）] ウィンドウの右側ペインに表示されます。常に最新のメッセージが最上部に表示されます。メッセージからテキストを選択してコピーすることができます。 メッセージパネルには最大 280 文字を入力することが可能で、この文字数に達すると、ビープ音で警告されます。
Message Log	過去のメッセージのログを表示できます。メッセージログには 100 件のメッセージが保持されます。[ウォール（Wall）] ウィンドウを起動すると、メッセージが表示されます。
プロファイル画像	プロフィール用の写真をアップロードできます。JPG、PNG、BMP、GIF などの有効な画像タイプがサポートされています。 写真をアップロードするには、ユーザー プロファイル ウィンドウの [アップロード（upload）] リンクを使用します。ユーザー プロファイル ウィンドウを開くには、[ウォール（Wall）] ウィンドウでユーザー名またはユーザーの写真をクリックします。 ユーザープロファイル ウィンドウには、プロファイル情報の編集機能とプロファイル情報の保存機能を切り替えるアイコンもあります。

ユーザー プロファイル ウィンドウ	ユーザー プロファイル ウィンドウを開くには、[ウォール（Wall）] ウィンドウでユーザー名またはユーザーの写真をクリックします。ユーザー プロファイル ウィンドウには、次の情報が含まれています。 • プロファイル名（最大 20 文字） • 職名（最大 15 文字） • 電子メール（最大 15 文字） • 電話 対応するメールリンクをクリックしてメールを送信します。
通知アラート	新しいメッセージを受信した時点で [ウォール（Wall）] ウィンドウがフォーカスされていない場合、新しい通知アラートポップアップが表示されます。通知をクリックするだけで [ウォール（Wall）] ウィンドウを起動できます。 通知アラートポップアップが表示されると、[ウォール（Wall）] ウィンドウのアイコンも点滅し、メッセージ数が表示されます。 アラートポップアップまたは [ウォール（Wall）] ウィンドウに表示される設定オプションから、通知アラートをオフにすることができます。

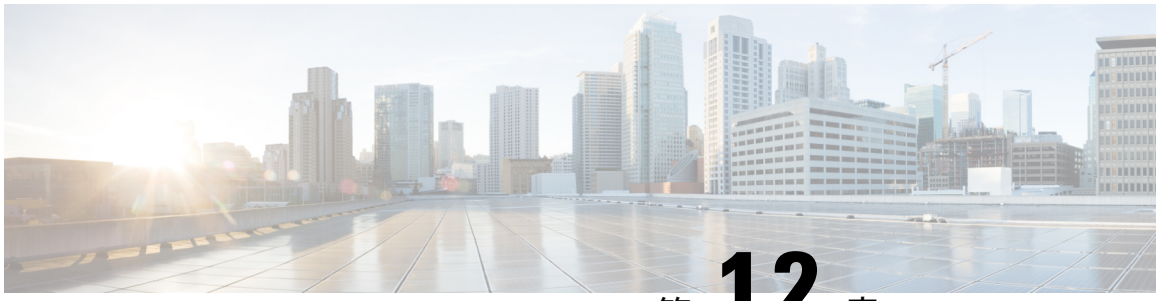
図 *16 : [*ウォール（*Wall*）*]* ウィンドウ



第 II 部

ファイアウォール サービスおよび NAT

- ファイアウォール サービスの概要 （755 ページ）
- ID 認証ファイアウォール ポリシーの管理 （809 ページ）
- Trustsec ファイアウォールポリシーの管理 （845 ページ）
- ファイアウォール AAA ルールの管理 （869 ページ）
- ファイアウォール アクセス ルールの管理 （913 ページ）
- ファイアウォール インスペクション ルールの管理 （977 ページ）
- ファイアウォール Web フィルタ ルールの管理 （1135 ページ）
- ファイアウォールの Botnet Traffic Filter ルールの管理 （1163 ページ）
- ScanSafe Web Security の使用 （1185 ページ）
- ゾーンベースのファイアウォール ルールの管理 （1195 ページ）
- トラフィック ゾーンの管理 （1287 ページ）
- トランスペアレント ファイアウォール ルールの管理 （1297 ページ）
- ネットワーク アドレス変換の設定 （1307 ページ）



第 12 章

ファイアウォール サービスの概要

Firewall ポリシー フォルダ（デバイス ビューまたはポリシー ビュー）には、ファイアウォールに関連するポリシーが含まれています。これらのポリシーは、Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）、PIX ファイアウォール（PIX）、Catalyst Firewall Services Module（FWSM; ファイアウォール サービス モジュール）、および Cisco IOS ソフトウェアを実行しているセキュリティ ルータに展開できます。これらのポリシーを使用すると、デバイスを介したネットワーク アクセスを制御できます。

この章は次のトピックで構成されています。

- ファイアウォール サービスの概要 （755 ページ）
- ルール テーブルの管理 （763 ページ）

ファイアウォール サービスの概要

Firewall ポリシーフォルダ（デバイスビューまたはポリシービュー）には、ファイアウォールに関連するポリシーが含まれています。これらのポリシーは、適応型セキュリティアプライアンス（ASA）、PIX ファイアウォール（PIX）、Catalyst Firewall Services Module（FWSM）に展開できます。

（注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービスルータ、組み込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。

これらのポリシーは、デバイスへのアクセス（つまり、デバイスの設定を変更したり **show** コマンドを使用したりするためにデバイスにログインすること）ではなく、デバイスを介したアクセスの制御に焦点を置いたものです。次に、使用可能なファイアウォール ポリシーについて概説し、詳細な情報を示す項へのポインタを示します。

- AAA ルール：AAA ファイアウォールまたは認証プロキシのルールです。これにより、ユーザが（ユーザ名とパスワードを使用した）認証および認可（任意）を受けて初めて、デバイスを介したネットワーク接続がユーザに許可されるように設定できます。また、ア

カウンティング、セキュリティ、またはリソース割り当て情報を作成することもできます。詳細については、AAA ルールについて （869 ページ）を参照してください。

- アクセス規則：従来的なインターフェイスベースの拡張アクセス コントロール規則です。パケットは、送信元アドレス、宛先アドレス、送信元インターフェイス、およびサービスに基づいて許可または拒否されます。これらのルールは、in 方向と out 方向のどちらにも適用できます。詳細については、アクセス ルールについて （913 ページ）を参照してください。
- インスペクション ルール：従来的な Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）であり、アプリケーション レイヤ プロトコル セッション情報に基づいて不正な TCP/UDP パケットをフィルタで除外し、選択したサービスの戻りトラフィックをイネーブルにします。詳細については、インスペクション ルールについて （977 ページ）を参照してください。
- Web フィルタ ルール：要求された URL に基づいて Web トラフィックをフィルタリングするタイプのインスペクション ルールです。これにより、望ましくない Web サイトへの接続を阻止できます。詳細については、Web フィルタ ルールについて （1135 ページ）を参照してください。
- ゾーンベースのファイアウォール ルール：インターフェイスではなくゾーンに基づいてルールを設定する場合、これらのルールで、IOS デバイス上のアクセス ルール、インスペクション ルール、および Web フィルタ ルールを置き換えます。ゾーンとは、同じセキュリティ ロールを実行する定義済みのインターフェイス グループのことです（Inside や Outside など）。ゾーン ルールを使用すると、他のタイプのルールを使用するよりもコンパクトなデバイス設定を作成できます。詳細については、ゾーンベースのファイアウォール ルールについて （1197 ページ）を参照してください。
- ボットネット トラフィック フィルタ ルール：これらのルールを使用すると、既知の不正なアドレスに送信されたボットネット トラフィックを見つけることができます。ボットネットは、無警戒なコンピュータ上に悪意のあるソフトウェアをインストールし、これらのコンピュータをプロキシとして使用して悪意のあるアクションを実行します。詳細については、ファイアウォールの Botnet Traffic Filter ルールの管理 （1163 ページ）を参照してください。
- トランスペアレント ルール：トランスペアレント インターフェイスまたはブリッジド インターフェイス上の非 IP のレイヤ 2 トラフィックに適用される Ethertype アクセス コントロール ルールです。詳細については、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください。

ほとんどのファイアウォール ルール ポリシーは、ルール テーブル内で設定します。これらのテーブルを使用すると、ほとんどのセルのインライン編集、セクションを使用したルール編成、およびルールの順序変更を行うことができます。共有ルール ポリシーを作成すると、多数のデバイス（異なるオペレーティング システムを実行しているデバイスを含む）にそれを適用できます。Security Manager により適切なデバイス コマンドが自動的に作成されて、個々のデバイスの特性に基づいてポリシーが設定され、デバイスに適用されない設定はフィルタで除外されます。ルール テーブルの使用方法の詳細については、ルール テーブルの管理 （763 ページ）を参照してください。

また、ほとんどのファイアウォール ルール ポリシーで使用される強力な機能に、継承という考え方があります。共有ポリシーを作成するとき、デバイスにポリシーを割り当てるのではなく、デバイスにポリシーを継承させるという選択もできます。このため、一方で一連の共有ルールをすべてのデバイスに適用し、他方で固有のルールを該当のデバイスだけに適用することができます。継承の詳細については、次の項を参照してください。

- ルールの継承について （213 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）

ここでは、ファイアウォール サービス ポリシーの概要について説明します。

- ファイアウォール ルールの処理順序について （757 ページ）
- NAT がファイアウォール ルールに与える影響について （758 ページ）
- Security Manager によって保持される ACL 名 （759 ページ）

ファイアウォール ルールの処理順序について

ファイアウォール ルール ポリシーを設定する際は、ルールが処理される論理順序を覚えておく必要があります。たとえば、あるアクセスルールで特定タイプのすべてのトラフィックをドロップする場合は、そのタイプのトラフィックに適用されるルールを他のファイアウォール ポリシー内に作成しても意味がありません。そのようなルールがトリガーされることはないためです。逆に、特定タイプのインスペクションまたは Web フィルタリングをトラフィックに適用する場合は、そのトラフィックがデバイスに入ることを、このアクセス ルールが最初に許可するように設定する必要があります。

ファイアウォール ルールの一般的な論理処理順序は、次のとおりです。

- AAA ルール：（認可の有無に関係なく）認証が必要な場合、ユーザはテストに合格する必要があります。合格しない場合、トラフィックはドロップされます。
- アクセスルール（イン方向）：トラフィックがアクセスルールを通過する必要があります。AAA ルールを使用する場合、ユーザーのセッションに対してユーザー単位の一時的なアクセスルールを設定できます。これらのユーザ単位のルールは、Security Manager ではなく AAA サーバで設定します。

  ASA 8.3 以降のデバイスでは、グローバル アクセス ルールはインターフェイス固有のアクセス ルールのあとに処理されます。詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください。
- 検査ルール（イン方向）、Web フィルタルール（イン方向）、ボットネットルール、サービスポリシールール（IPS、QoS、接続）：これらのすべてがトラフィックに適用されます。方向を設定できないデバイスの場合は、すべてのルールが In 方向であると見なされます。

- ゾーンベースのファイアウォール ルール：IOS デバイスに対してゾーンベースのルールを設定した場合、これらのルールがインスペクション ルールと Web フィルタ ルールを置き換えます（ボットネット ルールは IOS デバイスに適用されません）。
- 次に、ルーティング プロトコルがトラフィックに適用されます。トラフィックをルーティングできない場合、そのトラフィックはドロップされます（ルーティング ポリシーは、各種デバイス タイプ用の Platform フォルダの中にあり、ファイアウォール ポリシーとは見なされません）。
- ScanSafe Web セキュリティ ポリシー、検査ルール（アウト方向）、Web フィルタ ルール（アウト方向）：IOS デバイスに限り、アウト方向で作成した ScanSafe ポリシー、検査ルールまたは Web フィルタ ルールが適用されるようになりました。
- アクセス規則（Out 方向）：最後に、トラフィックは Out 方向のアクセス規則を通過する必要があります。

トランスペアレント ルールはこの概要には該当しません。トランスペアレント ルールは非 IP のレイヤ 2 トラフィックだけに適用されるため、あるトランスペアレント ルールがパケットに適用されると、その他のファイアウォール ルールは適用されません。また逆に、他のルールが適用されると、そのトランスペアレント ルールは適用されません。

関連項目

- AAA ルールについて （869 ページ）
- アクセス ルールについて （913 ページ）
- インスペクション ルールについて （977 ページ）
- Web フィルタ ルールについて （1135 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ファイアウォールの Botnet Traffic Filter ルールの管理 （1163 ページ）
- トランスペアレント ファイアウォール ルールの設定 （1297 ページ）

NAT がファイアウォール ルールに与える影響について

ファイアウォール規則をサポートしているデバイスでは、ネットワーク アドレス変換（NAT）を設定することもできます。NAT は、パケット内の実際のアドレスを、宛先ネットワーク上のマップされているルーティング可能なアドレスと置き換えます。

NAT をインターフェイスで実行するように設定した場合、そのインターフェイスで同様に設定されているファイアウォール ルールで、元の（NAT 実行前の）アドレスではなく、変換されたアドレスに基づいてトラフィックが評価される必要があります（ASA 8.3+ デバイスの場合を除く）。

ASA ソフトウェア リリース 8.3 以降を実行しているデバイスでは、トラフィックを評価する際に、元の（実際の）IP アドレスが使用されます（IPSec VPN トラフィック ポリシーの場合を除

く）。このため、ファイアウォール ルール、ACL ポリシー オブジェクト、または IOS、QoS、および接続ルール プラットフォーム サービス ポリシーを設定する場合は、必ず元のアドレスを使用してください。

NAT の詳細については、次の項を参照してください。

- ASA、PIX、FWSM デバイス： ネットワーク アドレス変換について （1307 ページ）
- IOS デバイス： Cisco IOS ルータにおける NAT ポリシー （1313 ページ）

Security Manager によって保持される ACL 名

Security Manager は、ユーザー定義のアクセス制御リスト（ACL）名を、デバイスで設定されているとおりに保持しようとします。次の場合、Security Manager は、デバイスで設定されている ACL 名を保持できます。

- ACL 名が Security Manager で指定されている場合。

アクセスルールポリシーの場合、**[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]** または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセス制御（IPv6 Access Control）]** で ACL 名を指定できます。特定の名前を単一のインターフェイスおよび方向に対して指定できますが、その名前は、同じ ACL を使用する他のすべてのインターフェイスおよび方向に使用されます。デバイスで他のポリシーに割り当てる ACL ポリシー オブジェクトと同じ名前を使用することはできません。また、IPv4 ACL と IPv6 ACL に同じ名前を使用することはできません。

（注） Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。ただし、以前の ASA バージョンでは、IPv6 アクセスルールの別のページが引き続きデバイスビューで提供されますが、ポリシービューでは、AAA ルール、アクセスルール、およびインスペクションルールのポリシータイプの IPv4 および統合バージョンが提供されます。

- ポリシーで ACL ポリシー オブジェクトを使用する場合、そのポリシー オブジェクトの名前が ACL 名に使用されます。検出中に作成された ACL ポリシーでは、可能なかぎり、デバイスで定義されている ACL の名前が使用されます。動作は管理設定によって異なります。
  - **[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [検出（Discovery）]** の順に選択して [ポリシーオブジェクトでデバイスのオーバーライドを許可（Allow Device Override for Policy Objects）] を選択すると、同じ名前で内容が異なるポリシーオブジェクトが Security Manager に存在していれば、その名前が再利用され、デバイスレベルのオーバーライドが作成されます。

- そのオプションを選択しない場合は、同じ名前に番号を追加して（ACLobject_1 など）ポリシー オブジェクトが作成されます。これはデフォルトの動作です。

- **[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [展開（Deployment）]** の順に選択して表示される [ファイアウォールアクセスリスト名（Firewall Access List Names）] 設定で [既存の名前を再利用（Reuse Existing Names）] を選択した場合、ACL を生成するファイアウォールルールに対して、デバイスで定義されている名前が再利用されます。
- ACL が共有されない場合（Security Manager で ACL の内容を変更した場合も同じ）。
- ACL は共有されるが、その ACL を共有する各ポリシーが Security Manager で同様には定義されていない場合。ACL の内容を変更すると、1 つの ACL が名前を保持し、その他の ACL には生成された名前が割り当てられます。

（注） ASA デバイス、またはバージョン 6.3(x) を実行していない PIX デバイスでは、ACL 名が NAT ポリシー スタティック ルールで使用されていて、さらにオブジェクトグループを含んでいる場合、その ACL 名は Security Manager により再利用されません。ACL は、送信元として定義されているオブジェクトグループの内容とともに展開されます。これは、デバイスでは ACL 内のすべての ACE の送信元がすべて同じである必要があるためです。

ヒント

- ACL ポリシー オブジェクトの名前が、デバイスですでに定義されている ACL でも使用される名前と同じであり、既存の ACL が Security Manager でサポートされないコマンドに対応している場合は、展開エラーが発生し、別の名前を選択するよう要求されます。このエラーが発生した場合は、ポリシー オブジェクトの名前を変更します。
- IOS デバイスでは、<number>_<number> という名前の ACL は無効です。Security Manager により、展開前にサフィックスが取り除かれます。つまり、同じ番号のプレフィックスを使用して IOS デバイスを複数の ACL オブジェクトに割り当てることはできません。ただし、番号付きサフィックスを持つ名前の ACL は許可されます（ACLname_1 など）。
- 番号付き ACL では、IOS デバイスに対する適切な番号範囲を使用する必要があります。標準 ACL は、1 ～ 99 または 1300 ～ 1999 の範囲にする必要があります。拡張 ACL は、100 ～ 199 または 2000 ～ 2699 の範囲にする必要があります。
- IOS デバイスの ACL 名の開始文字をアンダースコア（_）にすることはできません。
- ユーザ定義の名前を保持しないポリシーには、SSL VPN ポリシー、トランスペアレント ファイアウォール ルール、および AAA ルール（IOS デバイスの場合）があります。

ここでは、ACL 命名に関する追加情報を提供します。

- ACL 命名ルール （761 ページ）
- ユーザー定義の ACL ポリシーの名前付けの競合の解決 （763 ページ）

• ポリシー間での ACL 名前競合の解決 （763 ページ）

ACL 命名ルール

ACL の名前が Security Manager により生成される場合、その名前は、定義しているルールまたはプラットフォームのタイプと、それを固有にしている設定から導出されます。新しく作成された ACL には、次の表に示す命名ルールに基づいて名前が割り当てられます。

ヒント　展開中、既存の ACL を編集できない場合は、サフィックス *.n*（n は整数）が付加されることがあります。たとえば、acl_mdc_outside_10 という名前の ACL がすでにデバイスに存在している場合、この古い ACL を削除せずに新しい ACL を展開すると、acl_mdc_outside_10.1 という名前の新しい ACL が作成されます。

表 *163 : ACL* 命名ルール

ポリシー タイプ	命名ルール
アクセス ACL	• インバウンド：CSM_FW_ACL_InterfaceName • アウトバウンド：CSM_FW_ACL_OUT_InterfaceName
IPv6 アクセス ACL	• インバウンド：CSM_IPV6_FW_ACL_InterfaceName • アウトバウンド：CSM_IPV6_FW_ACL_OUT_InterfaceName （注）　Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。ただし、以前の ASA バージョンでは、IPv6 アクセスルールの別のページが引き続きデバイスビューで提供されますが、ポリシービューでは、AAA ルール、アクセスルール、およびインスペクションルールのポリシータイプの IPv4 および統合バージョンが提供されます。
インスペクション ルール	• ASA 7.0+/PIX 7.0+：CSM_CMAP_ACL_n（n は 1 から始まる整数）。 • IOS デバイスの場合、番号付き ACL。
NAT0 ACL	• インバウンド：CSM_nat0_InterfaceName_in • アウトバウンド：CSM_nat0_InterfaceName

ポリシー タイプ	命名ルール
NAT ACL	• インバウンド：CSM_nat_InterfaceName_poolID_in • アウトバウンド：CSM_nat_InterfaceName_poolID （注） PIX 6.3(x) デバイスの場合、ACL 名には、add _dns（dns）、_nrseq（norandomseq）、_emb##（初期接続制限）、_tcp##（tcp の最大接続制限）、および _udp##（udp の最大接続制限）が追加されます。
NAT ポリシー スタティック変換ルール ACL	• PIX 6.3(x) デバイス： • IP の場合：CSM_static_globalIP_LocalInterfaceName_globalInterfaceName • その他のプロトコルの場合：CSM_static_globalIP_LocalInterfaceName_globalInterfaceName_protocol _globalPort • 他の OS バージョンを実行しているデバイスの場合、localIP 文字列が追加されます。 • IP の場合：CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName • その他のプロトコルの場合：CSM_static_localIP_globalIP_LocalInterfaceName_globalInterfaceName_protocol _globalPort
AAA ACL	PIX/ASA/FWSM の場合：CSM_AAA_{AUTHO | ATHEN | ACCT}_InterfaceName _ServerGroupName IOS デバイスの認証プロキシ： • NAC を使用しないインターフェイス：CSM_AUTH-PROXY_InterfaceName_traffic type_ACL。ここで、InterfaceName はルールが適用されるインターフェイスです。traffic type は、HTTP、Telnet、または FTP です。 • 同じインターフェイス上の AuthProxy および NAC：CSM_ADMISSION_ID_ACL。ここで、ID は Security Manager 内の NAC が適用されるインターフェイス ロールの内部識別子です。
Web フィルタ ルール ACL	ASA 7.0+/PIX 7.0+：デバイスはフィルタ コマンドに一致します。 IOS デバイスの場合、番号付き ACL。

ユーザー定義の ACL ポリシーの名前付けの競合の解決

Cisco Security Manager は、「CSM_」で始まる ACL 名を生成します。デバイスで ACL を定義するときは、同じ命名パターンを使用しないでください。デバイスで「CSM_」プレフィックスを使用して ACL 名を宣言すると、Cisco Security Manager でのデバイス設定の検出中に、それらの ACL 名は Security Manager で生成された名前に置き換えられ、それぞれの設定のデルタが次の展開でデバイスに適用されます。

たとえば、Cisco Security Manager には、着信ファイアウォール インターフェイスの ACL 命名パターンとして CSM_FW_ACL_InterfaceName があります。デバイスの ACL 名の宣言に CSM パターン（CSM_xyz など）を使用すると、Security Manager はその名前を「CSM_FW_ACL_InterfaceName」に変更します。

（注） このルールはファイアウォール アクセス リストに対して有効であり、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [展開（Deployment）] で [既存の名前を再利用する（Reuse existing names）] 設定が選択されている場合でも、デルタが生成されてデバイスに適用されます。

ポリシー間での ACL 名前競合の解決

ACL は共有されるが、その ACL を共有するポリシーが Security Manager で同様には定義されていない場合、1 つのポリシーが ACL の元の名前を使用し、その他のポリシーは Security Manager により生成された新しい名前を使用します。元の名前を使用するポリシーを決定する際の優先順位は、次のとおりです。

- アクセス リスト ACL
- AAA ACL
- スタティック ACL
- NAT0 ACL
- NAT ACL

たとえば、アクセス ACL と NAT0 ACL が同じ ACL を再利用しようとする場合は、アクセス ACL がデバイスで設定されている元の名前を使用し、NAT0 ACL は Security Manager によって名前変更されます。

ルール テーブルの管理

ここでは、多くのファイアウォール ルール、NAT、およびその他のポリシーに関連する、ルール テーブルの基本的な使用方法について説明します。

- ルール テーブルの使用 （764 ページ）
- ルールの追加および削除 （766 ページ）

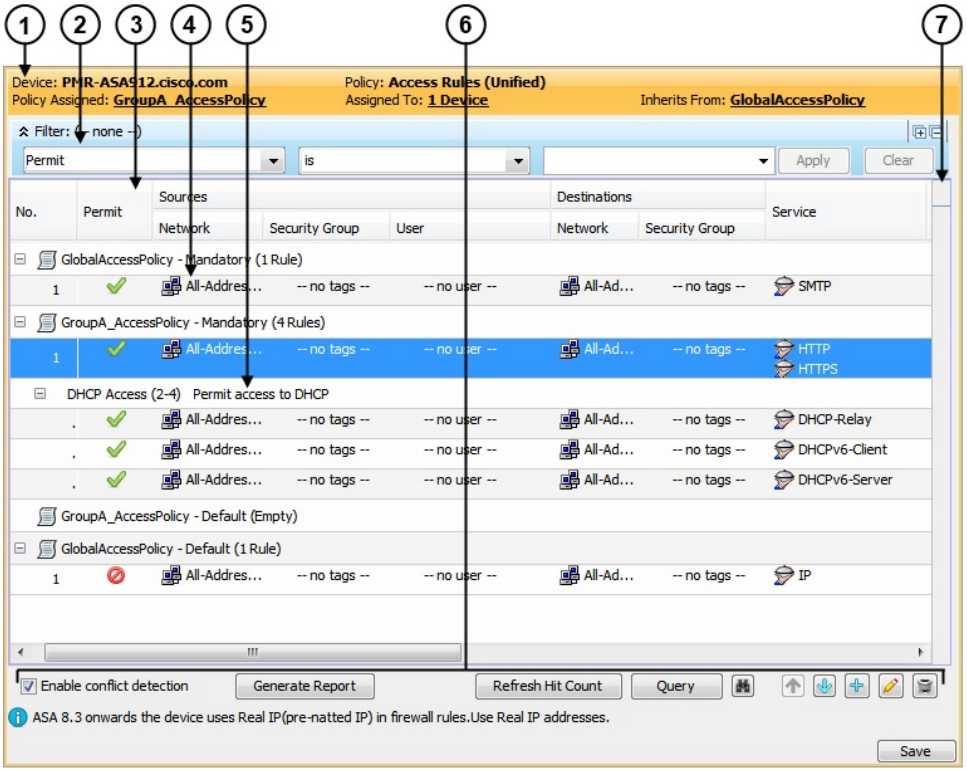
- ルールの編集 （767 ページ）
- ルール テーブルの項目の検索と置換 （777 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）
- ルールの結合 （785 ページ）
- ポリシー クエリー レポートの生成 （793 ページ）
- ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化 （802 ページ）
- 検出中のオブジェクト グループの展開 （806 ページ）

ルール テーブルの使用

Security Manager のルール テーブルには、ポリシーを構成するルール セット（アクセス ルールなど）が表示されます。これらのタイプのテーブルは、特定のポリシー グループだけで使用されますが、多くのファイアウォール サービス ルール ポリシーで使用されます。ポリシー内のルールの順序が重要な場合は、ルール テーブルが使用されます。

下の図で、ルールテーブルに含まれる機能について説明します。

図 *17* : ルール テーブルの例



次に、ルール テーブルの機能について、番号付きのコールアウトで説明します。

- **デバイスおよびポリシーの識別バナー（1）**：このバナーに、ポリシーの共有および継承の情報が示され、いくつかのアクションを実行できることが示されます。詳細については、ポリシー バナーの使用 （258 ページ）を参照してください。
- **テーブルフィルタ（2）**：大きなテーブルの中でルールを簡単に見つけられるように、ルールをフィルタリングできます。詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
- **テーブルのカラム見出し（3）**：カラムごとのソート、カラムの移動、カラムの表示/非表示の切り替えを実行できます。詳細については、テーブル カラムおよびカラム見出しの機能 （66 ページ）を参照してください。
- **ルール、作業領域（4）**：テーブルの本文に、ポリシーに含まれているルールが表示されます。
- **ユーザー定義のセクション（5）**：便宜上、ルールをセクション単位にグループ化できます。詳細については、セクションを使用したルール テーブルの編成 （783 ページ）を参照してください。
- **テーブルボタン（6）**：次の操作を実行する場合は、テーブルの下にあるボタンを使用します。

- 自動競合検出を有効にします（アクセスルールのみ）。詳細については、自動競合検出の使用 （950 ページ）を参照してください。

競合検出が有効になっている場合は、[レポートの生成（Generate Report）] ボタンをクリックして、競合の HTML レポートを作成し、出力したり、別のツールにエクスポートしたりできます。

最初に [アクセスルール（Access Rules）] ページを開くと、[レポートの生成（Generate Report）] ボタンが進行状況バーに置き換えられます。競合分析が完了すると、他の競合検出機能とともに [レポートの生成（Generate Report）] ボタンが使用できるようになります。

- テーブルに表示されるヒットカウント情報の更新。詳細については、ヒットカウントの詳細の表示 （960 ページ）および [Hit Count Selection Summary] ダイアログボックス （939 ページ）を参照してください。
- ポリシークエリの実行。実行すると、ルールを評価して、効果のないルールを特定できます。 ポリシー クエリー レポートの生成 （793 ページ）を参照してください。
- ルール内の項目の検索と置換（双眼鏡アイコンが付いたボタン）：詳細については、ルール テーブルの項目の検索と置換 （777 ページ）を参照してください。
- ルールの移動と並べ替え（上矢印および下矢印）：詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。
- テーブルにルールを追加（+アイコン）：詳細については、ルールの追加および削除 （766 ページ）を参照してください。
- 選択したルールの編集（鉛筆アイコン）：詳細については、ルールの編集 （767 ページ）を参照してください。
- 選択したルールの削除（ゴミ箱アイコン）：詳細については、 ルールの追加および削除 （766 ページ）を参照してください。
- **競合ナビゲーションバー（7）**：競合ナビゲーションバーを使用して、ルールテーブル内の競合するルールに移動します。詳細については、自動競合検出の使用 （950 ページ）を参照してください。

ルールの追加および削除

ルール テーブルを使用するポリシーを操作するとき、ファイアウォール ルール ポリシーの多くと同様に、いくつかの方法を使用してポリシーにルールを追加できます。

- [行の追加（Add Row）] ボタン（+ アイコン）：テーブルの下の [行の追加（Add Row）] ボタンをクリックすることが、新しいルールを追加するための標準的な方法です。このボタンをクリックすると、そのポリシータイプに固有のルールを追加するためのダイアログボックスが開きます。行またはセクション見出しを選択すると、選択した行の後ろに新しいルールが追加されます。選択しない場合、新しいルールは適切なスコープ（通常はローカル スコープ）の末尾に追加されます。

- 行を右クリックして [行の追加（Add Row）] を選択：行を選択して [行の追加（Add Row）] ボタンをクリックするのと同じです。
- コピーアンドペースト：既存のルールと類似する新しいルールを作成するには、そのルールを選択し、右クリックして [コピー（Copy）] を選択します。次に、ルールを挿入する位置の前の行を選択し、右クリックして [貼り付け（Paste）] を選択します。これにより複製されたルールが作成されるので、それを選択して編集できます（ルールの編集 （767 ページ）を参照）。
- カットアンドペースト：カットアンドペーストはコピーアンドペーストと似ていますが、[カット（Cut）] コマンドを選択すると既存のルールは削除されます。カット アンド ペーストの代わりに、ルールを移動することを考慮してください（ルールの移動とルール順序の重要性 （781 ページ）を参照）。

ルールが不要になったときは、そのルールを選択して [行の削除（Delete Row）] ボタン（ゴミ箱アイコン）をクリックすると、そのルールを削除できます。

ヒント ルールを削除する代わりに、まずルールをディセーブルにすることを考慮してください。ルールをディセーブルにすると、（設定を再展開したときに）そのルールはデバイスから削除されますが、Security Manager から削除されることはありません。あとで結局そのルールが必要であるとわかった場合は、ルールをイネーブルにして、設定を再展開するだけで済みます。ルールを削除した場合は、作成し直す必要があります（元に戻す機能はありません）。このため、ルールを削除するポリシーを進めるのは、ルールを一定時間ディセーブルにしてからにしてください。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

関連項目

- ルール テーブルの使用 （764 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）

ルールの編集

ルールテーブルを使用するルールポリシー内の既存のルールを編集するには、ルールを選択して [行の編集（Edit Row）] ボタンをクリックするか、右クリックして [行の編集（Edit Row）] を選択します。これにより、選択したルールのすべての側面を編集できます。

ヒント ローカル デバイス ルール ポリシーからの継承ルールについては、いずれの側面も編集できません。継承ルールはポリシー ビューで編集します。

ほとんどのルール テーブルでは、ルール全部を編集せずに、右クリック メニューに表示されるコマンドを使用して特定の属性やテーブル セルを編集することもできます。

セルを編集できるかどうかは、その内容を編集することが適切かどうかによって制限されます。たとえば、インスペクション ルールには、ルールの設定に基づいて多くの制限があります。

- [All Interfaces] にルールを適用した場合、送信元アドレス、宛先アドレス、インターフェイス、またはルールの方向はいずれも編集できません。
- （送信元と宛先の間のインスペクションを制限するためのオプションを選択せずに）トラフィック一致基準に [Default Inspection Traffic] を選択した場合、または [Custom Destination Ports] を選択した場合、送信元アドレスや宛先アドレスは編集できません。
- [Destination Address and Port (IOS)] を選択した場合、送信元アドレスは編集できません。

次のセルレベル コマンドが使用可能ですが、ルール テーブルを使用するすべてのポリシーで、複数の行の編集機能がサポートされているわけではありません。

- [<属性タイプ>の追加（Add <Attribute Type>）]：複数の行を選択して、[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、[サービス（Services）]、または [インターフェース（Interface）] セルを右クリックすると、[追加（Add）] コマンドを選択して、選択したセル内の既存のデータにエントリを追加できます。[追加（Add）] コマンドの完全な名前には、属性の名前が含まれます（[送信元の追加（Add Source）] など）。
- [<属性タイプ>の編集（Edit <Attribute Type>）]：ほとんどの属性で、内容を編集できます。編集すると、セルの内容が置き換わります。単一のセルを編集することも、複数の行を選択して、すべての行で同じタイプのセルの内容を一度に編集することもできます。[編集（Edit）] コマンドの完全な名前には、属性の名前が含まれます（[インターフェースの編集（Edit Interfaces）] など）。
- [<エントリ>の編集（Edit <Entry>）]：[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、[サービス（Services）]、または [インターフェース（Interface）] を編集するときに、セル内のエントリを選択し、そのエントリだけを編集できる場合もあります。たとえば、[Sources] セルに 3 つのネットワーク/ホスト オブジェクトと 1 つの IP アドレスが含まれる場合、そのいずれかを選択してエントリを編集できます。[Edit] コマンドには、エントリの名前が含まれます（[Edit HostObject] など）。
- [<エントリ>の削除（Remove <Entry>）]：[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、[サービス（Services）]、または [インターフェース（Interface）] を編集するときに、セル内のエントリを選択し、そのエントリを削除できる場合もあります。セル内の最後のエントリは削除できません。削除するとルールが無効になります。[Remove] コマンドには、エントリの名前が含まれます（[Remove IP] など）。
- [セルコンテンツからオブジェクトを作成（**Create <Object Type> Object from Cell Contents**）]：[送信元（Source）]、[ユーザー（User）]、[宛先（Destination）]、および [サービス（Services）] セルで、[作成（Create）] コマンドを選択して適切なタイプのポリシーオブジェクトを作成できます。また、セル内のエントリを選択して、選択した項目だけからポリシー オブジェクトを作成することもできます。[Create] コマンドには、作成できるポリシー オブジェクト タイプ、およびオブジェクトの送信元である項目の名前（セル内のすべての要素のセル コンテンツ、または選択したセルのエントリの名前）が含まれ

ます。ネットワーク/ホストオブジェクトを作成すると、必ずネットワーク/ホストグループ オブジェクトを作成することになります。

- [<属性タイプ>コンテンツの表示、<エントリ>コンテンツの表示（Show <Attribute Type> Contents; Show <Entry> Contents）]：[表示（Show）] コマンドを使用すると、セル内に定義されている実際のデータを参照できます。結果は、現在のビューによって異なります。
  - デバイスビュー、マップビュー、またはインポートルール：特定のデバイスに対してルールが適用される実際の IP アドレス、完全修飾ドメイン名（FQDN）、サービス、またはインターフェイスが表示されます。たとえば、ルールでネットワーク/ホストオブジェクトが使用されている場合は、それらのオブジェクトによって定義されている特定の IP アドレスまたは FQDN が表示されます。ルールでインターフェイス オブジェクトが使用されている場合は、オブジェクトによって識別される、デバイスに定義されている特定のインターフェイスが表示されます（ある場合）。

ネットワーク/ホスト オブジェクトの IP アドレスは、IP アドレスに基づいて昇順にソートされ、その後サブネット マスクに基づいて降順にソートされます。

サービス オブジェクトは、プロトコル、送信元ポート、および宛先ポートに基づいてソートされます。

インターフェイス オブジェクトは、アルファベット順に表示されます。インターフェイスがインターフェイス オブジェクト内のパターンと一致するために選択されている場合は、そのパターンが最初に表示され、そのあとに一致するインターフェイスがカッコで囲まれて表示されます。たとえば、「* (Ethernet1)」は、デバイス上の Ethernet1 インターフェイスが * パターンと一致（すべてのインターフェイスと一致）しているために選択されています。

- ポリシー ビュー：ポリシー オブジェクトに定義されているパターンとポリシーに定義されているエントリが表示されます。エントリはアルファベット順にソートされ、数字や特殊文字を先頭に含むエントリが先頭に表示されます。

関連項目

- ルール テーブルの使用 （764 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）

ルール テーブルの [Address] セルの追加または編集

[Add Sources or Destinations]/[Edit Sources or Destinations] ダイアログボックス、または NAT テーブルの [Address] ダイアログボックスを使用して、送信元または宛先を含むルール テーブル内の送信元エントリまたは宛先エントリを編集します。ファイアウォール ルールのセルの編集に関する詳細については、 ルールの編集 （767 ページ）を参照してください。

次のアドレス タイプを自由に組み合わせて入力し、トラフィックの送信元または宛先を定義できます。ポリシーのタイプによって、IPv4 または IPv6 のいずれのアドレスが必要であるかが決まります。アドレス タイプを混在させることはできません。項目をカンマで区切って複数の値を入力できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

- ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから新しいオブジェクトを作成することもできます。

（注） Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を指定するには、FQDN ネットワーク/ホスト オブジェクトまたは FQDN オブジェクトを含むグループ オブジェクトを使用する必要があります。FQDN を直接入力することはできません。すべてのポリシー タイプで FQDN が許可されるわけではありません。ポリシーで許可されていない場合は、FQDN オブジェクトを含むオブジェクトを指定できません。

- ホスト IP アドレス（10.10.10.100（IPv4）または 2001:DB8::200C:417A（IPv6）など）。
- IPv4 ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。
- IPv6 ネットワーク アドレスとプレフィックス長。形式は、2001:DB8::/32。
- IP アドレスの範囲（10.10.10.100-10.10.10.200（IPv4）または 2001:DB8::1-2001:DB8::100（IPv6）など）。
- （IPv4 のみ）10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。
- インターフェイス ロール オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します（オブジェクト タイプとして [インターフェイス ロール（Interface Role）] を選択する必要があります）。インターフェイス ロールを使用する場合は、選択したインターフェイスの IPv4 または IPv6 のアドレスを指定した場合と同様にルールが動作します。デバイスに割り当てられる IP アドレスを把握できないため、DHCP を経由してアドレスを取得するインターフェイスの場合に有効です。詳細については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

インターフェイス ロールを送信元として選択した場合、ダイアログボックスにタブが表示され、ホストまたはネットワークとインターフェイス ロールが区別されます。

ナビゲーション パス

送信元、宛先、またはその他のアドレス セルを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内のアドレスセルを右クリックし、[ソースの編集（Edit Sources）] または [宛先の編集（Edit Destinations）] あるいは類似のコマンドを選択します。選択したセルの内容が入力したデータに置き換えられます。
- アドレスセル内のエントリを選択し、[<エントリ>の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。
- 複数のルールを選択し、[送信元（Sources）] または [宛先（Destination）] セルを右クリックして [送信元の追加（Add Sources）] または [宛先の追加（Add Destinations）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。

ルールテーブルの [ユーザー（User）] セルの追加または編集

ヒント　ユーザーセルは、ASA 8.4(2 以降) にのみ適用されます。他のデバイスタイプまたは OS バージョンについては、セルでの設定内容はすべて無視されます。

[ユーザーの追加（Add Users）] または [ユーザーの編集（Edit Users）] ダイアログボックスを使用して、ユーザー アイデンティティ グループを含むルールテーブルのユーザーエントリを編集します。ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集（767 ページ）を参照してください。

次の任意の組み合わせを入力して、Active Directory（AD）ユーザーまたはユーザーグループ名に基づいてトラフィックを識別できます。アイデンティティ ユーザー グループを設定する場合、それらは送信元トラフィックにのみ適用されます。ルールに一致するトラフィックの場合、送信元アドレスとアイデンティティ ユーザ グループの両方が一致する必要があります。つまり、ルールは、宛先に向けられた際に送信元フィールドに定義された特定のネットワークまたはホスト上のユーザから送信されたトラフィックに適用されます。詳細については、アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）を参照してください。

送信元アドレスに関係なくルールをユーザーに適用するには、送信元セルに「any」を指定します。

項目をカンマで区切って複数の値を入力できます。サポートされるフォーマットは次のとおりです。

- アイデンティティ ユーザー グループ オブジェクト
- 個別のユーザ：NETBIOS_DOMAIN\user
- ユーザ グループ（\ を二重にします）：NETBIOS_DOMAIN\\user_group

[選択（Select）] をクリックしてリストからオブジェクト、ユーザー、またはユーザーグループを選択するか、新しいオブジェクトを作成します。詳細については、ポリシーでのアイデンティティ ユーザの選択 （835 ページ）およびアイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）を参照してください。

ナビゲーション パス

[User] セルを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内の [ユーザー（User）] セルを右クリックし、[ユーザーの編集（Edit Users）] を選択します。選択したセルの内容が入力したデータに置き換えられます。
- [ユーザー（User）] セル内のエントリを選択し、[<Entry> の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。
- 複数のルールを選択し、[ユーザー（User）] セルを右クリックして [ユーザーの追加（Add User）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。

ルール テーブルの [Services] セルの追加または編集

[Edit Services] ダイアログボックスを使用して、対象となるトラフィックのタイプを定義するサービスを編集します。項目をカンマで区切って複数の値を入力できます。

サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。また、[選択（Select）] をクリックして、リストからサービスを選択するか、新しいサービスを作成することもできます。

サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。

ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集 （767 ページ）を参照してください。

ナビゲーション パス

サービスを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内の [サービス（Services）] セルを右クリックし、[サービスの編集（Edit Services）] を選択します。選択したセルの内容が入力したデータに置き換えられます。
- [サービス（Services）] セル内のエントリを選択し、[<Entry> の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。
- 複数のルールを選択し、[サービス（Services）] セルを右クリックして [サービスの追加（Add Services）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。

ヒント インスペクション ルールでは、[Traffic Match] カラムにサービスが表示されます。ただし、サービスが表示されるのは、トラフィックが送信元、宛先、およびポートと一致するルールの場合だけです。

ルール テーブルの [Interfaces] セルまたは [Zones] セルの追加または編集

[Add or Edit Interfaces] または [Add or Edit Zones] ダイアログボックスを使用して、ルールが定義されているインターフェイスまたはゾーンを編集します。ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集 （767 ページ）を参照してください。

- インターフェイスを編集する際は、特定のインターフェイス名またはインターフェイス ロールを自由に組み合わせて入力できます。項目をカンマで区切って複数の値を入力できます。名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイスおよびロールを選択するか、新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。

ポリシーをデバイスに展開すると、インターフェイス ロールが実際のインターフェイス名で置き換えられます。これは、そのデバイスで実際に設定されているインターフェイスだけです。ルールによって実際に選択されるインターフェイスを表示するには、[インターフェイス（Interfaces）] セルを右クリックして [インターフェイスの表示（Show Interfaces）] を選択します。

- ゾーンの編集時には、インターフェイス ロールを 1 つだけ選択できます。個々のインターフェイスは選択できません。ゾーン ベースのファイアウォール ルールにゾーンを作成するには、インターフェイス ロールを使用します。ゾーンに属するインターフェイスを表示するには、[ゾーン（Zones）] セルを右クリックして [ゾーンコンテンツの表示（Show Zone Contents）] を選択します。

インターフェイス ロールおよびインターフェイスの選択に関する詳細については、次の項を参照してください。

- インターフェイス ロール オブジェクトについて （381 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）

ナビゲーション パス

インターフェイスまたはゾーンを含むルール ポリシー内で、次のいずれかを実行します。

- ルールテーブル内の [インターフェイス（Interfaces）] または [ゾーン（Zones）] セルを右クリックし、[インターフェイスの編集（Edit Interfaces）]、[ゾーンの編集（Edit Zones）]、または類似のコマンドを選択します。選択したセルの内容が入力したデータに置き換えられます。
- [インターフェイス（Interfaces）] セル内のエントリを選択し、[<エントリ>の編集（Edit <Entry>）] を選択します。選択したエントリが入力したデータに置き換えられます。ゾーン内のエントリを編集することはできません。
- 複数のルールを選択し、[インターフェイス（Interfaces）] セルを右クリックして [インターフェイスの追加（Add Interfaces）] を選択します。セルにすでに入力されているデータに、入力したデータが付加されます。エントリをゾーンに追加することはできません。

ルール テーブルの [Category] セルの編集

[Edit Category] ダイアログボックスを使用して、ルールに割り当てられているカテゴリを変更します。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集 （767 ページ）を参照してください。

ナビゲーション パス

カテゴリを含むルールポリシー内の [カテゴリ（Category）] セルを右クリックし、[カテゴリの編集（Edit Category）] を選択します。

ルール テーブルの [Description] セルの編集

[Edit Description] ダイアログボックスを使用して、ルールの説明を編集します。説明を使用すると、ルールの目的を明確にできます。最大 1024 文字です。ルールのセルの編集に関する詳細については、ルールの編集 （767 ページ）を参照してください。

ナビゲーション パス

説明を含むルールポリシー内の [説明（Description）] セルを右クリックし、[説明の編集（Edit Description）] を選択します。

ルール テーブルのセルの内容の表示

[Show Contents] ダイアログボックスを使用して、送信元、ユーザ、宛先、サービス、インターフェイス、またはゾーンのセルや、それらの要素を定義するアドレス、アイデンティティ ユーザ グループ、インターフェイス、サービス、またはポリシー オブジェクトを含むルール テーブル内のその他のセルで定義されている実際の変換済みデータを表示します。ダイアログボックスのタイトルは、調べるセルまたはエントリを示しています。この情報を使用して、デバイスに展開されたルールが実際に適用されるアドレス、サービス、またはインターフェイスを判別します。セルの内容の編集または表示に関する詳細については、ルールの編集 （767 ページ）を参照してください。

ダイアログボックスに表示される内容は、現在のビューによって異なります。

- デバイス ビュー、マップ ビュー：特定のデバイスに対してルールが適用される実際の IP アドレス、ユーザ、サービス、またはインターフェイスが表示されます。たとえば、ルールでネットワーク/ホスト オブジェクトが使用されている場合は、それらのオブジェクトによって定義されている特定の IP アドレスまたは Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）が表示されます。ルールでインターフェイス オブジェクトが使用されている場合は、オブジェクトによって識別される、デバイスに定義されている特定のインターフェイスが表示されます（ある場合）。
  - ネットワーク/ホスト オブジェクトの IP アドレスは、IP アドレスに基づいて昇順にソートされ、その後サブネット マスクに基づいて降順にソートされます。
  - サービス オブジェクトは、プロトコル、送信元ポート、および宛先ポートに基づいてソートされます。

- インターフェイス オブジェクトは、アルファベット順に表示されます。インターフェイスがインターフェイス オブジェクト内のパターンと一致するために選択されている場合は、そのパターンが最初に表示され、そのあとに一致するインターフェイスがカッコで囲まれて表示されます。たとえば、「*(Ethernet1)」は、デバイス上の Ethernet1 インターフェイスが * パターンと一致（すべてのインターフェイスと一致）しているために選択されています。

- ポリシー ビュー：ポリシー オブジェクトに定義されているパターンとポリシーに定義されているエントリが表示されます。エントリはアルファベット順にソートされ、数字や特殊文字を先頭に含むエントリが先頭に表示されます。

コンテンツのフィルタリング

[コンテンツの表示（Show Contents）] ダイアログボックスの結果の上にリストフィルタフィールドが表示されます。リストフィルタフィールドを使用すると、指定したテキスト文字列を含むエントリをすばやく見つけることができます。

図 *18*：リストフィルタフィールド

1	フィルタパラメータボタン	2	クリアボタン

[コンテンツの表示（Show Contents）] リストで特定のテキスト文字列を検索するには、次のように操作します。

- リストフィルタフィールドをクリックしてテキストカーソルを置き、入力を開始します。

これらは「ライブフィルタ」フィールドです。つまり、各文字を入力すると、現在のテキスト文字列を含まないエントリがリストまたはテーブルから除外されます。

リストフィルタフィールドをクリアするには、次のように操作します。

- フィールドの右側にあるクリアボタンをクリックします。

このボタンは、フィールドへの入力を開始すると表示されます(文字を強調表示して、キーボードの Delete キーまたは Backspace キーを押すこともできます)。

リストフィルタフィールドをクリアすると、リスト内のすべてのエントリが再び表示されます。

大文字と小文字を区別するか区別しないかを選択し、ワイルドカードまたは正規表現を許可し、返される文字列のどこに文字が配置されている必要があるかを指定することにより、フィルタ結果を調整できます。

リストフィルタ条件を変更するには、次のように操作します。

1. リストフィルタフィールドの左側にあるフィルタ パラメーターボタン（虫眼鏡）をクリックして、パラメーターメニューを開きます。
2. オプションを選択します。

メニューは 3 つのセクションで構成されています。

- [大文字と小文字を区別する（Case sensitive）]および[大文字と小文字を区別しない（Case insensitive）]：いずれかを選択します。[大文字と小文字を区別する（Case sensitive）]を選択した場合、見つかったテキストは、入力した文字だけでなく、大文字と小文字も入力されたものと一致する必要があります。
- [ワイルドカードを使用する（Use wildcards）] および [正規表現を使用する（Use regular expression）]：いずれかを選択します。次のワイルドカードが認識されます。
- *****（アスタリスク）：文字列内のその位置にある 0 個以上の文字に一致します。
- **+**（プラス記号）：文字列内のその位置にある 1 個以上の文字に一致します。
- **?**（疑問符）：文字列内のその位置にある 1 文字に一致します。
- [最初から一致（Match from start）]、[完全一致（Match exactly）]、および [一部が一致（Match anywhere）]：1 つを選択します。[最初から一致（Match from start）]とは、入力した文字列がエントリの先頭で見つかる必要があることを意味します。ただし、より大きな文字セットの一部でも可能です。[完全一致（Match exactly）] では、入力した文字列がカラムエントリ全体と完全に一致する必要があります。 [一部が一致（Match anywhere）] とは、文字列がエントリ内のどこかで見つかることを意味し、より大きな文字セットの一部でも可能です。
- 別のパラメータを変更するには、手順 1 と 2 を繰り返します。

ナビゲーション パス

送信元、ユーザ、宛先、サービス、インターフェイス、またはゾーンや、ネットワーク、アイデンティティユーザグループ、インターフェイス、またはサービスを指定するその他のフィールドを含むルールポリシー内で、次のいずれかを実行します。また、ルールを操作する（ルールのインポートなど）ツールを使用する際にも、内容を表示できます。

- これらのセルの 1 つを右クリックし、[<Attribute Type>のコンテンツを表示（Show <Attribute Type> Contents）]（attribute type はセル名）を選択します。データには、セル内に定義されているすべてのエントリが含まれます。
- これらのセルの 1 つのエントリを右クリックし、[<Entry>のコンテンツを表示（Show <Entry> Contents）] を選択します。コマンド名には、選択したエントリの名前が含まれます。表示されるデータは、選択したエントリだけに対応するデータです。

ヒント　インスペクション ルールでは、[Traffic Match] カラムにサービスが表示されます。ただし、サービスが表示されるのは、トラフィックが送信元、宛先、およびポートと一致するルールの場合だけです。

ルール テーブルの項目の検索と置換

ルールテーブルを使用するポリシー内で、いくつかのセルの項目を検索し、選択的に置換できます。検索できるセルは、ポリシーによって異なります。パターンマッチングに基づいて項目を検索する場合、ワイルドカード文字を使用できます。たとえば、関連するいくつかのネットワークを、それらに定義されている新しいネットワーク/ホスト ポリシー オブジェクトで置き換えることができます。

検索と置換を使用するには、ルールテーブルを使用するポリシーの一番下にある [検索と置換（Find and Replace）]（双眼鏡アイコン）ボタンをクリックして、[Find and Replace] ダイアログボックス （778 ページ）を開きます。Firewall フォルダでは、これに AAA 規則、アクセス規則、IPv6 アクセス規則、インスペクション規則、ゾーン ベースのファイアウォール規則、および Web フィルタ規則（ASA/PIX/FWSM デバイスのみ）が含まれます。ASA/PIX/FWSM デバイスでは、NAT 変換ルール ポリシー（ただし、コンテキストと動作モードのすべての組み合わせに当てはまるとはかぎりません）と IOS、QoS、および接続ルールのプラットフォーム サービス ポリシーも含まれます。

項目を検索するときは、項目のタイプおよび検索するカラムを選択し、検索する文字列を入力します。また任意で、置換に使用する文字列を入力します。次の項目タイプを検索および置換できます。

- [ネットワーク（Network）]：ネットワーク/ホストオブジェクト名またはホストやネットワークの IP アドレス。
- [User]：Active Directory（AD）ユーザ名（NetBIOS_DOMAIN\user）、ユーザ グループ名（NetBIOS_DOMAIN\\user_group）、またはアイデンティティ ユーザ グループ オブジェクト名。
- [Service]：サービス オブジェクト名またはプロトコルとポート。たとえば、TCP/80。検索は意味ではなく構文によるものです。つまり、TCP/80 を検索し、ルールで HTTP が使用されている場合、検索結果には TCP/80 は含まれません。
- [Interface Role]：インターフェイス名またはインターフェイス ロール オブジェクト名。

（注） アクセス ルールでは、グローバル インターフェイス名を使用してグローバル ルールを検索できます。ただし、グローバル ルールとインターフェイス固有のルールを変換する方法はありません。グローバルルールはグローバルインターフェイス名を使用して検索できますが、インターフェイス名を「Global」という名前で置換しようとすると、実際には Global という名前のポリシーオブジェクトを使用する、インターフェイス固有のアクセス ルールが作成されます。

- [Text]：[Description] フィールドのテキスト文字列。

次に、検索と置換に関連する操作の例をいくつか示します。

- 10.100.0.0/16 の範囲内のすべてのネットワークに対して network10.100 という名前の新しいネットワーク/ホスト オブジェクトを作成すると、すべての従属ネットワーク指定を検索および置換できます。たとえば、^10.100* を検索すると、10.100.10.0/24 のようなアドレスすべてを検索できます。[全単語のみ検索（Find Whole Words Only）] および [ワイルドカードを許可（Allow Wildcard）] オプションを選択して、置換文字列として「network10.100」と入力します。[Find Whole Words Only] を選択したため、置換される文字列は、10.100 の部分だけでなく 10.100.10.0/24 文字列全体です。
- （ネットワーク/ホスト オブジェクトの代わりに）IP アドレスを使用するすべてのルールを検索する場合は、*.*.*.* を検索すると、すべてのホストまたはネットワーク IP アドレスが検索されます。次に、[Find and Replace] ダイアログボックスが開いている間に、選択的にセルを編集できます。
- 名前に「side」が含まれるすべてのインターフェイス ロール オブジェクト（inside や outside など）を、External という名前のインターフェイス ロール オブジェクトで置換する場合は、[全単語のみ検索（Find Whole Words Only）] オプションと [ワイルドカードを許可（Allow Wildcard）] オプションを選択して *side を検索し、[置換（Replace）] フィールドに External を入力します。

関連項目

- ルールの編集 （767 ページ）

[Find and Replace] ダイアログボックス

[Find and Replace] ダイアログボックスを使用して、ルール テーブルのセル内の項目を検索し、任意で置換します。検索できる項目のタイプは、表示されているポリシーによって異なります。

ナビゲーション パス

ルールテーブルを使用するポリシーの一番下にある [検索と置換（Find and Replace）]（双眼鏡アイコン）ボタンをクリックします。Firewall フォルダでは、これに AAA 規則、アクセス規則、IPv6 アクセス規則、インスペクション規則、ゾーン ベースのファイアウォール規則、お

よびWebフィルタ規則（ASA/PIX/FWSMデバイスのみ）が含まれます。ASA/PIX/FWSMデバイスでは、NAT変換ルール ポリシー（ただし、コンテキストと動作モードのすべての組み合わせに当てはまるとはかぎりません）とIOS、QoS、および接続ルールのプラットフォーム サービス ポリシーも含まれます。

関連項目

- ルール テーブルの項目の検索と置換 （777 ページ）
- ルールの編集 （767 ページ）

フィールド リファレンス

表 *164 : [Find and Replace]* ページ

要素	説明
タイプ	検索する項目のタイプ。タイプを選択し、検索するカラムを選択します。[All Columns] を選択すると、検索されたカラムは、[All Columns] 項目とともに一覧表示されます（検索では、テーブル内のすべてのカラムが考慮されるわけではありません）。 • [ネットワーク（Network）]：ネットワーク/ホストオブジェクト名またはホストやネットワークのIPアドレス。 • [User]：Active Directory（AD）ユーザ名（NetBIOS_DOMAIN\user）、ユーザ グループ名（NetBIOS_DOMAIN\\user_group）、またはアイデンティティ ユーザ グループ オブジェクト名。 • [Service]：サービス オブジェクト名またはプロトコルとポート。たとえば、TCP/80。検索は意味ではなく構文によるものです。つまり、TCP/80を検索し、ルールでHTTPが使用されている場合、検索結果にはTCP/80は含まれません。 • [Interface Role]：インターフェイス名またはインターフェイス ロール オブジェクト名。 （注） アクセス ルールでは、グローバル インターフェイス名を使用してグローバル ルールを検索できます。ただし、グローバル ルールとインターフェイス固有のルールを変換する方法はありません。グローバルルールはグローバルインターフェイス名を使用して検索できますが、インターフェイス名を「Global」という名前で置換しようとすると、実際にはGlobalという名前のポリシーオブジェクトを使用する、インターフェイス固有のアクセスルールが作成されます。 • [Text]：[Description] フィールドのテキスト文字列。

要素	説明
検索（Find）	検索文字列。ポリシーオブジェクトを検索する場合は、[選択（Select）] をクリックして、リストからオブジェクトを選択します。
置換（Replace）	（任意）検索文字列を置換するために使用する文字列。置換される文字列は、検索オプションで制御します。検索文字列をポリシーオブジェクト名で置換する場合は、[選択（Select）] をクリックして、リストからオブジェクトを選択します。 検索文字列を複数の項目で置換できます。複数の項目はカンマで区切ります。たとえば、TCP サービスを検索し、それを TCP, UDP で置き換えます。 [置換（Replace）] フィールドに何も入力せずに [置換（Replace）] ボタンをクリックすると、項目を削除できます。 テーブルで編集が許可されていない場合は、このフィールドがグレー表示されます。
方向	現在選択されている行またはセルを基準にした検索の方向（[up] または [down]）。テーブルの終わりに達すると、引き続きテーブルの一番上から検索されます。
Match Case	テキスト検索の場合、[Find] フィールドで使用した大文字と小文字の違いを一致させるかどうか。
Find Whole Words Only	検索で単語全体（スペースまたは句読点で区切られた文字列）だけを検索して選択するかどうか。たとえば、SanJose を単語全体で検索すると、SanJose は検出されますが、SanJose1 は検出されません。 このオプションを [Allow Wildcard] オプションとともに使用すると、部分文字列を検索できます。ただし、検出された文字列を置換すると、部分文字列ではなく単語全体が置換されます。たとえば、^10.100* を検索すると、10.100.10.0/24 のようなすべてのアドレスが検出され、それらが network10.100 ポリシー オブジェクトで置換されます。[Whole Words] を選択することにより、検索対象の部分だけでなくアドレス全体がネットワーク/ホストオブジェクトで置換されます。 テキスト検索の場合、このオプションと [Allow Wildcards] オプションは相互に排他的です。

要素	説明
Allow Wildcards	検索文字列または置換文字列でワイルドカード文字を使用するかどうか。このオプションを選択しない場合、すべての文字が文字どおりに処理されます。 Java 正規表現を使用して、次の例外を含む表現を作成できます。 • ピリオド（.）：ピリオドはリテラル ピリオドであり、暗黙的にエスケープされます。 • 疑問符（?）：疑問符は単一文字を表します。 • アスタリスク（*）：アスタリスクは、1 つ以上の文字と一致します。0 文字とは一致しません。 • プラス記号（+）：プラス記号はアスタリスクと同じ意味で、1 つ以上の文字と一致します。
[Find Next] ボタン	検索文字列の次のオカレンスを検索する場合は、このボタンをクリックします。
[Replace] ボタン	見つかった文字列を置換文字列で置換する場合、このボタンをクリックします。
[Replace All] ボタン	検索文字列を自動的に検索し、テーブル全体にわたってそれを置換する場合は、このボタンをクリックします。

ルールの移動とルール順序の重要性

ルール テーブルを使用するルール ポリシーは、順序付けられたリストです。つまり、ルールの上から下への順序が重要であり、ポリシーに影響を与えます。

デバイスは、ルール ポリシーに照らしてパケットを分析するとき、上から下に順にルールを検索します。パケットに一致した最初のルールが、そのパケットに適用されるルールです。それ以降のルールはすべて無視されます。このため、特定の送信元または宛先の HTML トラフィックに関連する具体的なルールの前に、IP トラフィックに関連する一般的なルールを配置すると、具体的なルールの方が適用されないことがあります。

アクセス制御ルールの場合は、自動競合検出ツールを使用して、どのような場合に、ルール順序によってルールがトラフィックに適用されなくなるかを特定できます（詳細については、自動競合検出の使用 （950 ページ）を参照してください）。その他のルール ポリシーの場合は、テーブルをよく調べて、ルール順序に関連する問題を特定してください。

ルールの順序を並べ替える必要があると判断した場合は、移動する必要のあるルールを選択し、適宜、[上の行へ（Up Row）]（上矢印）または [下の行へ（Down Row）]（下矢印）ボタンをクリックします。これらのボタンがルール テーブルの下に表示されない場合、ルール順序は問題ではないため、その順序を並べ替えることはできません。

セクションを使用してルールを編成した場合は、セクション内でだけルールを移動できます。セクション外部のルールを移動する場合、そのセクションの上または下に移動できます。セクションでの作業の詳細については、セクションを使用したルール テーブルの編成 （783 ページ）を参照してください。

ヒント　ポリシー内でインターフェイスに固有のルールとグローバル ルールを組み合わせる場合は、移動するアクセス ルールに特殊なルールが適用されます。詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください。

関連項目

- ルール テーブルの使用 （764 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）

ルールのイネーブル化とディセーブル化

ルール テーブルを使用するポリシー（ほとんどのファイアウォール サービス ルール ポリシーなど）内で、個々のルールをイネーブル化およびディセーブル化できます。変更は、設定をデバイスに再展開すると有効になります。

ルールがディセーブルになっている場合、テーブルでそのルールにハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。

ディセーブルなルールは便宜的に Security Manager のルール ポリシー内に保持されます。ルールが必要になった場合は、ルールを再作成しなくとも簡単にイネーブルにできます。このため、不要になったと思われるルールは、すぐに削除してしまわずに、ディセーブルにすることを推奨します。

ルールがイネーブルかディセーブルかを変更するには、ルールを選択して右クリックし、[有効化（Enable）] または [無効化（Disable）] を必要に応じて選択します。

関連項目

- ルール テーブルの使用 （764 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）

セクションを使用したルール テーブルの編成

ルールテーブルを使用するポリシーは、セクション単位に編成できます。次の2つのタイプのセクションがあります。

- スコープ：ポリシーと継承ポリシーの継承関係を定義します。このセクションは、ポリシーを継承すると自動的に作成されます。詳細については、ルールの継承について （213 ページ）を参照してください。
- ユーザ定義セクション：ポリシーの評価および編集が簡単になるようにルールを編成する際に役立つ便利なグループです。このタイプのセクションは、多数のルールが含まれるポリシーに対して最も効果を発揮します。

セクション内のすべてのルールは順序付けられている必要があります。ルールをランダムにグループ化することはできません。連続しないルールどうしを関連付けて指定するには、それらのルールに同じカテゴリを割り当てることができます。

ユーザ定義セクションは、インデントされたセクション見出しによって、テーブル内の他のルールから目立つように表示されます。見出しには、左から順に、セクションを開いたり閉じたりするための +/- アイコン、セクションに割り当てたカテゴリ（ある場合）を識別する色の帯、セクション名、セクションに含まれる最初と最後のルール番号（4-8 など）、および入力したセクションの説明（ある場合）が表示されます。

（注） セクション内のルールの番号付けを表示するには、ルール番号の列のサイズを変更する必要がある可能性があります。

ユーザ定義セクションを作成するかどうかは、ユーザの自由です。これらのタイプのセクションを作成することが有益だと判断した場合は、次の情報に示すセクションの作成方法と使用方法を参照してください。

- 新しいセクションを作成するには、セクションを挿入する行を右クリックし、[新しいセクションに含める（Include in New Section）] を選択します（Shift を押しながらクリックして、ルールのブロックを選択することもできます）。セクションの名前、説明、およびカテゴリを入力するように要求されます（必須の要素は名前だけです）。
- 既存のルールをセクションに移動するには、1つ以上の連続するルールを選択し、右クリックして [<セクション名> セクションに含める（Include in Section <name of section>）] を選択します。このコマンドは、選択した行が既存のセクションの隣にある場合にだけ表示されます。セクションに追加する行が現在そのセクションの隣にない場合は、セクションの隣に来るまでルールを移動するか、ルールをカットしてセクションにペーストします。
- セクションの移動はできません。このため、セクションの外側のルールをセクション周りに移動する必要があります。セクション内にはないが、セクションの隣にあるルールを移動すると、ルールはそのセクションを飛び越えます。
- ルールをセクションの外部に移動したり、セクションを通過して移動したりすることはできません。セクションとは、ルールを移動できる範囲の境界を定義するものです。ルール

をセクションの外側に移動して Local スコープセクションに戻すには、1 つ以上の連続するルールを選択し、右クリックして [<name of section> セクションから削除する（Remove from Section <name of section>）] を選択します。このコマンドを使用するには、ルールがセクションの開始位置または終了位置にある必要があります。そうでない場合、ルールが開始位置または終了位置に来るまでルールを移動するか、ルールをカット アンド ペーストしてセクションの外側に移動できます。

- 新しいルールをセクションに追加するには、目的の位置のすぐ前にあるルールを選択し、[Add Row] ボタンをクリックします。ルールをセクションの開始位置に挿入するには、セクション見出しを選択します。

ルールを（セクションの外部だが）セクションの後ろに作成するには、ルールをセクション内の最後のルールとして作成してから、セクションから削除します。または、ルールをセクションのすぐ上に作成し、下矢印ボタンをクリックします。

- セクション見出しを右クリックして [セクションの編集（Edit Section）] を選択することにより、セクションの名前、説明、またはカテゴリを変更できます。
- セクションを削除すると、セクションに含まれているすべてのルールは保持されて、Local スコープセクションに再び移されます。削除されるルールはありません。セクションを削除するには、セクション見出しを右クリックし、[セクションの削除（Delete Section）] を選択します。
- Combine Rules ツールを使用する場合、結果として結合されたルールではセクションが考慮されます。セクション内にあるルールは、そのセクション内の他のルールとだけ結合できます。

関連項目

- ルール テーブルの使用 （764 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）

[Add Rule Section]/[Edit Rule Section] ダイアログボックス

[Add and Edit Rule Section] ダイアログボックスを使用して、ルール テーブルでユーザ定義セクション見出しを追加または編集します。セクションを使用してルールテーブルを編成する方法の詳細については、セクションを使用したルール テーブルの編成 （783 ページ）を参照してください。

ナビゲーション パス

次のいずれかを実行します。

- ルールテーブル内の 1 つ以上のルールを選択し、右クリックして [新しいセクションに含める（Include in New Section）] を選択します。
- セクション見出しを右クリックし、[セクションの編集（Edit Section）] を選択します。

フィールド リファレンス

表 *165 : [Add Rule Section]/[Edit Rule Section]* ダイアログボックス

要素	説明
名前	セクションの名前。
説明	セクションの説明。最大 1024 文字です。
カテゴリ	セクションに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

ルールの結合

アクセス ルール ポリシーおよび AAA ルール ポリシーは時間とともに拡大し、多数のルールを含むことがあります。これらのポリシーの大きさによっては、ポリシーの管理が困難になることがあります。この問題を軽減するために、ルール結合ツールを使用できます。これにより、ポリシーがトラフィックを処理する方法を変更することなく、ポリシー内のルールの数を減らすことができます。

ヒント ルールを結合すると、特定のセキュリティ ポリシーを実装するために必要なアクセス ルールの数を大幅に圧縮できます。たとえば、あるポリシーでアクセス ルールが 3,300 個必要な場合、ホストとサービスを効率的にグループ化すると、必要なルールを 40 個に減らすことができます。ただし、Rule Combiner は IPv6 アクセス ルールで使用できません。また、ユーザまたはユーザ グループを指定するルールでも、直接とアイデンティティ ユーザ グループ オブジェクトのどちらでも使用できません。FQDN ネットワーク/ホスト オブジェクトを使用するルールで、このツールを使用できます。

（送信元としての）信頼できる各種ホストに対する特定範囲のサービスを（宛先としての）各種パブリック サーバに対して許可するような、複数のルールが存在するとします。この状況で 10 個のルールを適用する場合は、その 10 個のルールを 1 つのルールに結合できます。これにより、サービスの集まり（AllowedServices など）、ホスト（TrustedHosts など）、およびサーバ（PublicServers など）に対して新しいポリシー オブジェクトを作成できます。ルール結合中に新しいオブジェクトを作成するには、新しく結合したセルを右クリックし、[ネットワーク（またはサービス）オブジェクトをセルコンテンツから作成する（Create Network (or Service) Object from Cell Contents）] を選択します。

たとえば、インターフェイス FastEthernet0 に次の 2 つのルールがあるとします。

- Permit TCP for source 10.100.10.1 to destination 10.100.12.1
- Permit TCP for source 10.100.10.1 to destination 10.100.13.1

この 2 つを結合して、permit TCP for source 10.100.10.1 to destination 10.100.12.1, 10.100.13.1 という 1 つのルールにできます。

ルールを結合するには、多次元のソートが使用されます。たとえば、アクセス ルールの場合、次のようになります。

1. ルールは送信元によってソートされるため、送信元が同じルールはまとめて配置されます。
2. 送信元が同じルールは宛先によってソートされるため、送信元も宛先も同じルールはまとめて配置されます。
3. 送信元も宛先も同じルールは 1 つのルールに結合され、サービスが連結されます。
4. 隣接するルールは、送信元およびサービスが同じかどうかチェックされます。同じであった場合、1 つのルールに結合され、宛先が連結されます。
5. 隣接するルールは、宛先およびサービスが同じかどうかチェックされます。同じであった場合、1 つのルールに結合され、送信元が連結されます。

今度は、宛先と（送信元の代わりに）サービスに基づいてソートが繰り返されます。

ヒント セクションの異なるルールが結合されることはありません。ルールを整理するために作成したセクションによって、可能な結合の範囲が制限されます。また、インターフェイス固有のアクセス ルールとグローバル アクセス ルールが結合されることはありません。グローバル ルールの詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください。

関連項目

- ファイアウォール AAA ルールの管理 （869 ページ）
- ファイアウォール アクセス ルールの管理 （913 ページ）

ステップ 1 **Firewall** フォルダから、結合するルールのポリシーを選択します。次のタイプのポリシーに対してルールを結合できます。

- AAA ルール
- アクセス ルール

ステップ 2 ツールで可能な結合が特定のルール グループに制限されるようにする場合は、それらのルールを選択します。Shift および Ctrl を押しながらクリックすると、複数のルールを選択できます。セクション見出しを選択すると、セクション内のすべてのルールを選択できます。スコープ見出し（[Local] など）を選択する

と、スコープ内のすべてのルールを選択できます。ツールを制限しない場合は、テーブルから何も選択しないでください。次の点を考慮してください。

- デバイス ビューでは、ローカル ルールに対する結合だけを保存できます。ツールは共有ルールおよび継承ルールに対して実行できますが、結果を保存することはできません。ルールを選択しない場合、デフォルトですべてのローカル スコープ ルールが考慮されます。
- 共有ポリシー内のルールを結合するには、ポリシー ビューでツールを実行する必要があります。ルールを選択しない場合、デフォルトですべての必須ルールが考慮されます。

結果を保存できない場合にツールを実行しようとすると、警告されます。

ステップ 3 ルールテーブル内の任意の場所を右クリックし、[ルールの結合（Combine Rules）] を選択して [Combine Rules Selection Summary] ダイアログボックス （787 ページ）を開きます。組み合わせを制限する特定のルールを選択した場合は、選択したルールの 1 つで右クリックしてください。そうしないと、ルールの選択が解除されます。

ステップ 4 ルールで結合を考慮するカラムを選択します。カラムを選択しない場合、結合されたルールの設定が、結合対象のカラム内の設定と同じである必要があります。

また、選択したルールの結合を考慮するように選択したり、ポリシー内のすべてのルールの結合を考慮するように選択することもできます。

ヒント カラム タイプが表示されていない場合、結合されたルールの内容が、[Description] セルを除くセルの内容と同じである必要があります。セルの内容が異なるルールどうしは結合されません。

ステップ 5 [OK] をクリックすると、結合が生成され、[ルールの結合結果（Rule Combiner Results）] ダイアログボックスに結果が表示されます。

結果を分析し、結合を保存するかどうかを評価します。全部を保存するか、何も保存しないかのどちらかです。保存する結合を選択することはできません。

結果の評価の詳細については、Rule Combiner 結果の解釈 （789 ページ）を参照してください。例については、 Rule Combiner 結果の例 （791 ページ）を参照してください。

ステップ 6 [OK] をクリックすると、ルールテーブル内の元のルールが、結合されたルールに置き換わります。

[Combine Rules Selection Summary] ダイアログボックス

[Combine Rules Selection Summary] ダイアログボックスを使用して、ファイアウォール ルール ポリシー内のルールを結合するために使用するパラメータを定義します。[OK] をクリックすると、結合の結果が [Rule Combiner結果（Rule Combiner Results）] ダイアログボックスに表示されます。このダイアログボックスで、 Rule Combiner 結果の解釈 （789 ページ）の説明に従い、結果の保存または破棄を選択できます。

ナビゲーション パス

[AAA Rules] ページ （880 ページ）と [Access Rules] ページ （924 ページ）からルールを結合できます。テーブルの一番下にある [ツール（Tools）] をクリックし、[ルールの結合（Combine Rules）] を選択します。

フィールド リファレンス

表 *166 : [Combine Rules Selection Summary]* ダイアログボックス

要素	説明
Policy Selected	選択したポリシーおよびスコープが表示されます。[Local] は、ローカル デバイス ルールを表します。それ以外の場合、フィールドには共有ポリシーの名前と、そのポリシー内で選択されているスコープ（ある場合）が示されます。
Rules to be combined	ツールで結合を考慮するルール： • [All Rules]：選択したポリシー内のすべてのルールの結合が考慮されます。 • [Selected Rules]：ツールの起動前にポリシー内で選択したルールだけの結合が考慮されます。 ツールの実行前のルールの選択に関する詳細については、ルールの結合（785 ページ）を参照してください。

Choose which columns to combine	ルールテーブル内の結合可能なカラム。2つのルールを結合するには、選択していないカラムの内容がいずれも同一である必要があります（結合可能カラムとして一覧表示されていないカラムも含む。ただし、[Description] カラムを除く）。結合できるカラムは、次のとおりです。
	• ソース
	• ユーザー（User）
	• [接続先（Destination）]
	• サービス
	• インターフェイス
	• [セキュリティ送信先（Security Sources）]
	• [セキュリティ宛先（Security Destinations）]
	• AAA ルールの場合、他に次のカラムも結合できます。
	  • 操作
	  • Auth Proxy

Rule Combiner 結果の解釈

[Rule Combiner Results] ダイアログボックスを使用して、ルール結合の結果を評価できます（ルールの結合 （785 ページ）を参照）。このダイアログボックスには結果が要約され、[OK] をクリックすると作成される新しいルールが表示されます。

変更されるルールのセルの枠は赤色になります。上半分のテーブルで結合済みのルールを選択すると、そのルールを作成するために結合されたルールが下半分のテーブルに表示されます。

このウィンドウで、結果の要素を改良できます。

- 複数の要素を持つ [送信元（Source）]、[宛先（Destination）]、[サービス（Service）] セルを右クリックし、[ネットワーク（またはサービス）オブジェクトをセルコンテンツから作成する（Create Network (or Service) Object from Cell Contents）] を選択すると、結合されたセルの内容を含む新しいポリシーオブジェクトを作成できます。セルの内容が新しいオブジェクトに置き換わります。

また、展開された設定内にネットワーク オブジェクト グループを自動的に作成して、ルール テーブル セル内のカンマ区切りの値を置き換えることもできます。ネットワーク オブジェクトは展開中に作成されます。これがルール ポリシーの内容に影響することはありません。このオプションをイネーブルにするには、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [展開（Deployment）] を選択して [Deployment] ページ （658 ページ）を開き、[ルール内の複数の送信元、宛先、またはサービスのオブジェクト グループを作成（Create Object Groups for Multiple Sources, Destinations, or Services in a Rule）] を選択します。

- [説明（Description）] を右クリックし、[説明の編集（Edit Description）] を選択して説明を変更します。結合済みのルールの説明は、改行で区切られた古いルールの各説明を連結したものです。

例については、 Rule Combiner 結果の例 （791 ページ）を参照してください。

ヒント

- 結合された結果は、[OK] をクリックするまでポリシーに適用されません。結合の結果に満足しない場合は、[キャンセル（Cancel）] をクリックして、より小さなルール グループを選択して Combine Rules ツールのスコープを制限することを考慮します。

[OK] をクリックしたあとで、その変更の受け入れを取り消すには、次の 2 つのオプションがあります。1 つめは、ポリシー ページで [保存（Save）] をクリックしないようにし、別のポリシーを選択して、ポリシーの変更を保存するように要求されたら [いいえ（No）] をクリックします。すでに [保存（Save）] をクリックした場合でも、（たとえば、[ファイル（File）] > [廃棄（Discard）] を選択して）アクティビティまたは設定セッションを廃棄することにより、変更を元に戻すことができます。ただし、これを行うと、他のポリシーに対して行った他の変更内容もすべて廃棄されます。変更を送信したあと、またはアクティビティが承認されたあとは、変更を元に戻すことはできません。

- 保存が許可されていないポリシーに対してルールを結合する場合でも、Combine Rules ツールは実行できます。たとえば、デバイス ビューでは共有ポリシーまたは継承ポリシーの結

合済みルールを保存できません。結果を保存できない場合は、ツールの実行前に警告が表示されます。

- セクションの異なるルールが結合されることはありません。ルールを整理するために作成したセクションによって、可能な結合の範囲が制限されます。また、インターフェイス固有のアクセス ルールとグローバル アクセス ルールが結合されることはありません。グローバル ルールの詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください。

ナビゲーション パス

[AAA Rules] ページ （880 ページ）と [Access Rules] ページ （924 ページ）からルールを結合できます。テーブルの一番下にある [ツール（Tools）] をクリックして [ルールの結合（Combine Rules）] を選択し、[Combine Rules Selection Summary] ダイアログボックス （787 ページ）を入力して [OK] をクリックします。

フィールド リファレンス

表 *167* : 結合されたルールの結果の要約

要素	説明
Result Summary	何らかの結合を行うことができる場合、結合の結果の要約が示され、元のルールの数、結合後に残るルールの数、変更されるルールの数、および変更されないルールの数が示されます。
[Resulting Rules] テーブル	ポリシー内に現存するルールを置換するルール。[OK] をクリックした場合、これらのルールがポリシーの一部となります。カラムは、関連付けられたポリシー内のカラム（[AAA Rules] ページ （880 ページ）または [Access Rules] ページ （924 ページ）を参照）に、[Rule State] カラムが追加されたものです。 [Rule State] カラムには、ルールのステータスが示されます。 • [Modified]、[Combined]：新しいルールは、1 つ以上のルールを結合した結果、または既存のルールを変更した結果として生成されたものです。セルの枠が赤い場合、内容が結合されたセルであることを示します。 • [Unchanged]：ルールは他のルールと結合できなかったため、変更されていません。 • [Not Selected]：可能な結合に対してルールを選択していません。 ルールが多数存在する場合、テーブルの下のボタンを使用して、変更のあるルール全部をスクロールできます。変更されていないルールおよび選択されていないルールはスキップされます。

要素	説明
[Original rules] テーブル（下半分のテーブル）	ダイアログボックスの下半分のテーブルに、上半分のテーブルで選択したルールを作成するために結合された元のルールが表示されます。
[Detail Report] ボタン	このボタンをクリックすると、結果の HTML レポートが作成されます。レポートには結果が要約され、結果のルールの詳細と、新しいルールを作成するために結合されたルールも表示されます。 結合されたルールのセル内に多数のエントリがある場合、このレポートを使用すると、結果を簡単に解釈できます。あとで使用できるようにレポートを印刷または保存することもできます。

Rule Combiner 結果の例

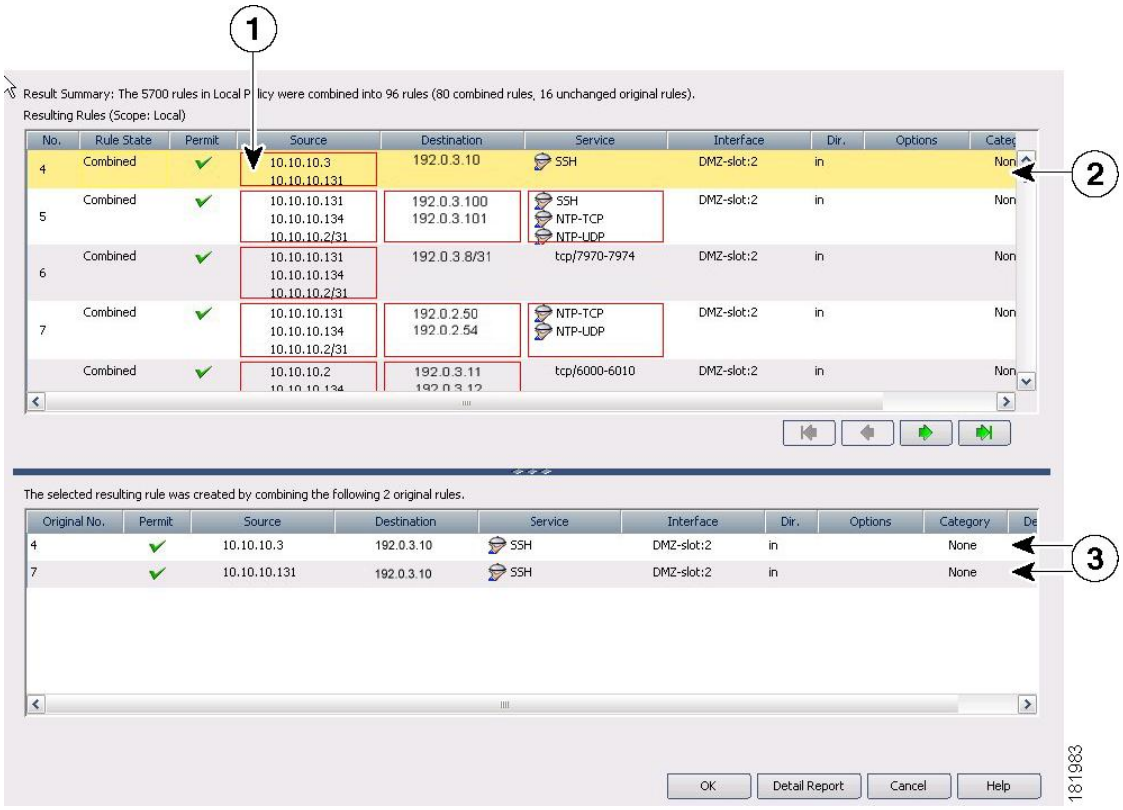
ルールの結合 （785 ページ）で説明されているように Combine Rules ツールを実行すると、結合の結果が [Rule Combiner Results] ダイアログボックスに表示されます（Rule Combiner 結果の解釈 （789 ページ）を参照）。

次の図に、ルールの結合の例を示します。

新しいルールが上半分のテーブルに表示されます。新しいルールが変更済みルールまたは結合済みルールとして示され、変更されたセルの枠は赤色になります。上半分のテーブルで新しいルールを選択すると、下半分のテーブルに、新しいルールを作成するために結合された古いルールが表示されます。この例では、2 つの古いルールは、宛先、サービス、およびインターフェイスが同じです。また、2 つの異なる送信元が連結されて、新しいルールを構成しています。

レポートの一番上に、結果が要約されます。この例では、5700 個のルールが 96 個に縮小されました。

図 *19 : Rule Combiner* の結果例



1	結合されたセル	3	元のルール
2	新しく結合されたルール		

関連項目

- ファイアウォール AAA ルールの管理 （869 ページ）
- ファイアウォール アクセス ルールの管理 （913 ページ）

IPv4 ルールから統合ルールへの変換

Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Security Manager 4.4 および ASA 9.0+ では、これらのポリシーとポリシーオブジェクトが結合または統合されました。ただし、以前の ASA バージョンでは、IPv6 アクセス ルールの別のページが引き続きデバイス ビューで提供されますが、ポリシー ビューでは、AAA、アクセス、および検査ルールのポリシー タイプの IPv4 および統合バージョンが提供されます。

個別の IPv4 および IPv6 ファイアウォールルールを「統合」ルールに変換するユーティリティが Security Manager 4.4 で提供され、ASA を以前のバージョンから 9.0 以降にアップグレードするときに使用できます。

ナビゲーション パス

ファイアウォールルール統合ユーティリティにアクセスするには、次の手順を実行します。

- （ポリシービュー）ポリシータイプセレクタからファイアウォール IPv4 ルールタイプを選択し、[ポリシー（Policies）] ペインで目的のポリシーを右クリックします。 [< ルールタイプ >ルール（統合）に変換（Convert to <rule-type > Rules (Unified)）] を選択します。

関連項目

- [AAA Rules] ページ （880 ページ）
- [Access Rules] ページ （924 ページ）
- [Inspection Rules] ページ （986 ページ）

上記のようにユーティリティを開きます。 [ポリシーの変換（Convert Policy）] ダイアログボックスで新しい統合ポリシーの名前を指定して、[OK] をクリックします。

処理後、新しい統合ルールポリシーが表示されます。このポリシーを ASA 9.0 以降のデバイスに割り当てることができるようになりました。

ポリシー クエリー レポートの生成

ほとんどのファイアウォール ルール ポリシーでは、ルールの評価に役立つポリシー クエリー レポートを生成できます。ポリシー クエリー レポートを使用すると、新しいルールを作成して特定の送信元、ユーザ、宛先、インターフェイス、サービス、またはゾーンに適用する前に、これらの項目に対してすでに存在しているルールを判別できます。

また、ルールの使用を禁止しているブロッキングルールや、削除できる冗長なルールがあるかどうかも、ある程度は判別できます。ただし、アクセスルールを評価する場合は、これらの問題を判別するためのより強力なルール分析ツールを使用する方が得策です。

ポリシークエリーを作成する場合は、ルールの作成時にトラフィックを説明するのと同様の方法で、関連するトラフィックを説明します。クエリーの作成方法は基本的に、ルールの作成方法と同じです。しかし、ルールの説明をより広範にして、取得するトラフィック セットの幅を広げた方が、単一のルールまたはかぎられた数のルールではなく、関連するルールのセットを確認できます。作成するクエリーは、検出する目的の情報によって決まります。

クエリーの可能なレベルは、現在のビューによって異なります。

- デバイス ビューまたはマップ ビュー：クエリーは、選択したデバイスに制限されます。ただし、サポートされているすべてのルールタイプにわたってクエリーを実行できます。これにより、同じトラフィックに適用されるさまざまなタイプのルールを比較できます。

- ポリシー ビュー：クエリーは、選択したポリシーに制限されます。そのポリシー内で定義されているルールだけが表示されます。他のポリシー タイプを照会することはできません。他のポリシーを調べている間に共有ポリシーを照会する場合は、共有ポリシーに割り当てられているデバイスを選択し、デバイス ビューでデバイスからポリシーを照会します。

関連項目

- [AAA Rules] ページ （880 ページ）
- [Access Rules] ページ （924 ページ）
- [Inspection Rules] ページ （986 ページ）
- [Inspection Rules] ページ （986 ページ）
- [Zone-based Firewall Rules] ページ （1272 ページ）

ステップ 1 [ファイアウォール（Firewall）] フォルダから、照会するポリシーを選択します。次のいずれかのタイプのポリシーを照会できます。

- AAA ルール
- アクセル ルール
- インスペクション ルール
- Web フィルタ ルール（PIX/ASA/FWSM）
- ゾーン ベースのルール

ステップ 2 テーブルの下の [クエリ（Query）] ボタンをクリックし、[デバイスまたはポリシーのクエリ（Querying Device or Policy）] ダイアログボックスを開きます。

ステップ 3 照会するルールを定義するパラメータを入力します。クエリーを設定するときに、少なくとも 1 つのルール タイプ（イネーブル、ディセーブル、または両方、許可、拒否、または両方、および必須、デフォルト、または両方）を選択する必要があります。クエリー パラメータの詳細については、[Querying Device or Policy] ダイアログボックス （795 ページ）を参照してください。

ポリシー ビューで、照会するルールのタイプを変更することはできません。デバイス ビューで、ルール タイプの結合を照会することはできません。

ステップ 4 [OK] をクリックすると、基準と一致したルールが [ポリシークエリ結果（Policy Query Results）] ダイアログボックスに表示されます。このレポートの解釈については、 ポリシー クエリー結果の解釈 （799 ページ）を参照してください。

ポリシー クエリー レポートの例については、 [Policy Query Result] の例 （801 ページ）を参照してください。

[Querying Device or Policy] ダイアログボックス

[Querying Device] または [Querying Policy] ダイアログボックスを使用して、クエリーのパラメータを設定します。クエリー結果に、パラメータと一致したルールが表示されます。ダイアログボックスのタイトルは、照会する内容を示しています。

- デバイス ビューまたはマップ ビューでは、選択したデバイスに対して定義されているルールを照会します。
- ポリシー ビューでは、選択したポリシーの中だけのルールを照会します。

これらのポリシー タイプから、AAA ルール、アクセル ルール、インスペクション ルール、Web フィルタ ルール（ASA/PIX/FWSM の場合）、およびゾーン ベースのファイアウォール ルールを照会できます。

クエリーを設定するときに、少なくとも 1 つのルール タイプ（イネーブル、ディセーブル、または両方、許可、拒否、または両方、および必須、デフォルト、または両方）を選択する必要があります。

（注） インスペクション ルールでは、インターフェイス値として Global を入力した場合、一致が完了しても、一致ステータス結果は部分一致として表示されます。

結果は、[Policy Query Results] ダイアログボックス（ポリシー クエリー結果の解釈 （799 ページ）を参照）に表示されます。

ナビゲーション パス

ポリシー クエリー レポートを生成するには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、Firewall フォルダから、サポートされているファイアウォール ルール ポリシーのいずれかを選択して、テーブルの下にある [クエリ（Query）] ボタンをクリックします。
- （ポリシービュー）Firewall フォルダから、サポートされているファイアウォール ルール ポリシーのいずれかを選択し、共有ポリシーセレクタから特定のポリシーを選択して、テーブルの下にある [クエリ（Query）] をクリックします。
- （マップ ビュー）デバイスを右クリックし、[Edit Firewall Policies] メニューから、サポートされているファイアウォール ルール ポリシーを選択します。[クエリ（Query）] ボタンをクリックします。

関連項目

- ポリシー クエリー レポートの生成 （793 ページ）
- [Policy Query Result] の例 （801 ページ）

フィールド リファレンス

表 *168 : [Querying Device or Policy]* ダイアログボックス

要素	説明
Rule Types	照会するルールのタイプ。ポリシー ビューで照会する場合は、選択内容を変更できません。デバイス ビューで照会する場合は、次のいずれかのタイプのルールを選択できます。クエリーのスコープは、選択したデバイスに制限されます。 • AAA ルール • アクセル ルール • インスペクション ルール • Web フィルタ ルール • ゾーン ベースのルール
Enabled and/or Disabled Rules	イネーブルなルール、ディセーブルなルール、またはその両方を照会するか。
Mandatory and/or Default Rules	必須セクション内のルール、デフォルト セクション内のルール、または両方のセクション内のルールを照会するか。
一致（Match）	トラフィックを許可するルール、否定するルール、またはその両方を照会するか。

要素	説明
ソース 宛先	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 （注） フィールドをブランクのままにした場合、クエリーはそのフィールドに対する任意のアドレスと一致します。 次のアドレス タイプを自由に組み合わせて入力し、トラフィックの送信元または宛先を定義できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。 ヒント 将来のポリシー クエリー要求を容易にするために、IP アドレスのリストとともにオブジェクトを作成できます。

要素	説明
ユーザー（User）	（ASA 8.4(2) 以降のみ）ルールの Active Directory（AD）ユーザー名、ユーザーグループ、またはアイデンティティ ユーザー グループ オブジェクト（使用する場合）。項目をカンマで区切って複数の値を入力できます。 （注） フィールドをブランクのままにした場合、クエリーは[User]フィールドに何も入っていないルールにのみ一致します。 次の値を組み合わせて入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。 [選択（Select）]をクリックしてリストからオブジェクト、ユーザー、またはユーザーグループを選択するか、新しいオブジェクトを作成します。 詳細については、以下を参照してください。 • ポリシーでのアイデンティティ ユーザの選択 （835 ページ） • アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ） • アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）
サービス	対象となるトラフィックのタイプを定義するサービス。項目をカンマで区切って複数の値を入力できます。 （注） フィールドをブランクのままにした場合、クエリーは任意のサービスと一致します。 サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。 ヒント 将来のポリシー クエリー要求を容易にするために、サービスのリストとともにオブジェクトを作成できます。

要素	説明
インターフェイス	ルールが定義されているインターフェイス。インターフェイスまたはインターフェイス ロール名の任意の組み合わせを、カンマで区切って入力できます。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。 （注） フィールドをブランクのままにした場合、クエリーは任意のインターフェイスまたはインターフェイス ロールと一致します。
Query for Global Rules	アクセス ルールまたはインスペクション ルールを照会するとき、クエリーでグローバル ルールも考慮する必要があるかどうか。
From Zone To Zone	ゾーン ベースのファイアウォール ルールの場合、ルールに定義されているゾーン。ゾーン名（インターフェイスロール）を入力するか、[選択（Select）] をクリックしてリストからゾーンを選択します。
アクション（Actions）	ゾーン ベースのファイアウォール ルールの場合、ルールに定義されているアクション。
Check if Matching Rules Are Shadowed by Rules Above	ポリシー クエリー結果に競合検出情報を含めるかどうか。このオプションを選択すると、パフォーマンスおよびコストの結果に影響を及ぼす可能性があります。

ポリシー クエリー結果の解釈

[Policy Query Results] ダイアログボックスを使用して、[Query Device or Policy] ダイアログボックスで定義したポリシー クエリーの結果を参照します。結果レポートは、[Querying Device or Policy] ダイアログボックス （795 ページ）でクエリパラメータを定義して [OK] をクリックすると開きます。手順については、ポリシー クエリー レポートの生成 （793 ページ）を参照してください。レポート例については、[Policy Query Result] の例 （801 ページ）を参照してください。

ヒント クエリ結果テーブルで、行をダブルクリックするか、右クリックして [ルールに移動（Go to Rule）] を選択して、ルールを編集できる [ルールポリシー（rules policy）] ページでルールを選択します。ポリシー セレクタで適切なルール ポリシーがまだ選択されていない場合は、これを 2 回行って、実際にルールを選択する必要があることがあります。

レポートを解釈するには、次のレポート セクションを考慮してください。

- [クエリパラメータ（Query Parameters）]：レポートの最上部分で、クエリに対して入力したパラメータを指定します。パラメータを変更する場合は、[クエリの編集（Edit Query）] をクリックして [Querying Device or Policy] ダイアログボックス （795 ページ）を開きます。ここで、変更を行い、レポートを再生成できます。

- [結果（Results）]テーブル：このテーブルには、クエリと一致するすべてのルールが一覧表示されます。複数タイプのルールをクエリした場合、[表示（Display）]フィールドで、調査するルールタイプを選択します。このテーブル内のカラムは、そのタイプのルールのカラムに、次のカラムが追加されたものです。
  - [Match Status]：ルールをクエリーと一致させる方法を示します。

[完全一致（Complete Match）]：ルールはすべてのクエリパラメータと一致します。

[部分一致（Partial Match）]：すべての検索条件が重なるか、一致したルールのスーパーセットです。たとえば、送信元アドレス 10.100.20.0/24、宛先アドレス 10.200.100.0/24、および IP のサービスでルールが定義されている場合、クエリで送信元 10.100.20.0/24 を検索すると、クエリ結果はルールの定義の一部だけを表すため、一致ステータスは部分一致として表示されます。

[影響なし（No Effect）]：ルールが他の一致ルールによりブロックされているか、影響しない競合が存在しています。たとえば、A と B の 2 つの一致ルールがあるとします。ルール A の送信元アドレス、宛先アドレス、およびサービスがルールBのそれらと等しいか、それらを含む場合、ルールBはルールAによってブロックされます。したがって、ルールBはトラフィックには影響しません。

別の例として、グローバルな必須ルールによってサービスが許可されるが、デバイス（ローカル）レベルでのルールによってサービスが拒否されるとします。ルールは最初に一致したものから順に認識されるため、必須のグローバルスコープで一致が検出されると、それ以降は他のルールはチェックされません。ローカルルールは無効です。つまり、サービスは拒否されず、許可されます。適切な結果を得るためには、ポリシーを編集する必要があります。

- [Scope]：ルールが共有ルールかローカル ルールか、必須ルールかデフォルト ルールかを示します。

- [詳細（Details）] テーブル：[詳細（details）] テーブルには、[結果（results）] テーブルで選択されているルールの詳細なクエリ致情報が表示されます。左側のフォルダは、詳細情報を参照できる属性を表しています。詳細を表示するフォルダを選択します。

詳細には、定義したパラメータであるクエリー値と、パラメータと一致するルール内の項目が表示されます。一致の関係は次のいずれかです。

- [Identical]：パラメータは、ルール内の値と同じです。
- [Contains]：パラメータは、ルール内の値を含むスーパーセットです。たとえば、クエリーパラメータがネットワーク/ホスト オブジェクトであり、オブジェクト定義の一部である IP アドレスがルールで使用されている場合などです。
- [Is contained by]：パラメータは、ルールの値の中でネストされているサブセットです。
- [Overlaps]：クエリーパラメータでは、ルール内で使用されている複数のポリシーオブジェクトにまたがる結果が表示されます。たとえば、サービス クエリーパラメータが tcp/70-90 であり、tcp/80-100 として定義されているサービスが結果に表示される場合などです。

関連項目

- [AAA Rules] ページ （880 ページ）
- [Access Rules] ページ （924 ページ）
- [Inspection Rules] ページ （986 ページ）
- [Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （1138 ページ）
- [Zone-based Firewall Rules] ページ （1272 ページ）

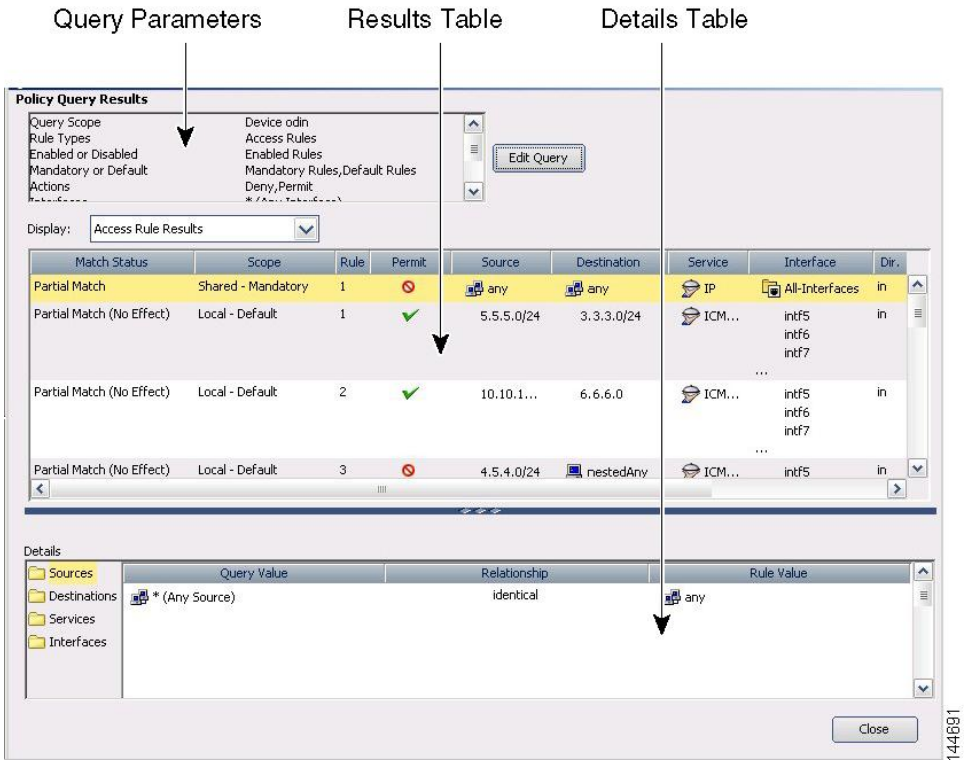
[Policy Query Result] の例

次に、アクセスルールに関するポリシークエリレポートの例を示します。基準によって送信先、宛先、サービス、およびインターフェイスのパラメータは制限されませんが、クエリーはイネーブルなルールに制限されます。共有ルールとローカル ルールの両方が含められます。

[Query Parameters] セクションに、レポートのクエリー基準が表示されます。この例では、結果テーブル内の最初の行が選択されています。また、ウィンドウの下半分の詳細テーブルに、そのルールの詳細情報が表示されています。この例では、詳細テーブルで送信元フォルダが選択されており、ルールの値 **any** が、クエリパラメータ ***** と完全に一致する（任意の送信元アドレスに相当する）ことが結果に示されています。

このレポートの解釈の詳細については、 ポリシー クエリー結果の解釈 （799 ページ）を参照してください。

図 *20 : [Policy Query Results]*



関連項目

- ポリシー クエリー レポートの生成 （793 ページ）
- [AAA Rules] ページ （880 ページ）
- [Access Rules] ページ （924 ページ）
- [Inspection Rules] ページ （986 ページ）
- [Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （1138 ページ）
- [Zone-based Firewall Rules] ページ （1272 ページ）

ファイアウォールルールの展開時のネットワークオブジェクトグループの最適化

ファイアウォール ルール ポリシーを ASA、PIX、FWSM、または IOS 12.4(20)T 以降のデバイスに展開すると、関連付けられたネットワーク オブジェクト グループをデバイス上に作成するときに、ルールで使用するネットワーク/ホスト ポリシー オブジェクトを評価して最適化するように Security Manager を設定できます。最適化によって、隣接するネットワークがマージされ、冗長なネットワーク エントリが削除されます。これにより、実行時のアクセス リスト

データ構造と設定のサイズが縮小されます。メモリ制約のある一部の FWSM および PIX デバイスでは、これによるメリットがあります。

たとえば、次のエントリを含みアクセスルール内で使用される **test** という名前のネットワーク/ホストオブジェクトについて考えてみます。

```
192.168.1.0/24
192.168.1.23
10.1.1.0
10.1.1.1
10.1.1.2/31
```

最適化をイネーブルにした場合、ポリシーを展開すると、結果のオブジェクト グループ設定が生成されます。説明に、グループが最適化されたことが示されることに注意してください。

```
object-group network test
 description (Optimized by CS-Manager)
 network-object 10.1.1.0 255.255.255.252
 network-object 192.168.1.0 255.255.255.0
```

最適化をイネーブルにしない場合、グループ設定は次のようになります。

```
object-group network test
 network-object 192.168.1.0 255.255.255.0
 network-object 192.168.1.23 255.255.255.255
 network-object 10.1.1.0 255.255.255.255
 network-object 10.1.1.1 255.255.255.255
 network-object 10.1.1.2 255.255.255.254
```

この最適化によってネットワーク/ホスト オブジェクトの定義が変更されることも、新しいネットワーク/ホスト ポリシー オブジェクトが作成されることもありません。デバイス上でポリシーを再検出すると、変更されていない既存のポリシー オブジェクトが使用されます。

（注） ネットワーク/ホスト オブジェクトに別のネットワーク/ホスト オブジェクトが含まれる場合、それらのオブジェクトは結合されません。それぞれのネットワーク/ホスト オブジェクトが個別に最適化されます。また、Security Manager は、連続しないサブネット マスクを使用するネットワーク/ホスト オブジェクト オブジェクトを最適化できません。

最適化を設定するには、[Deployment] ページ （658 ページ）で [展開中にネットワークオブジェクトグループを最適化する（Optimize Network Object-Groups During Deployment）] オプションを選択します（**[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）]** を選択してコンテンツテーブルから [展開（Deployment）] を選択）。デフォルトでは、展開中にネットワーク オブジェクト グループは最適化されません。

（注）

CSM 4.17 SP1 および CSM 4.18 を設定せずに CSM 4.19 にアップグレードした場合、object-group service を含むファイアウォールの展開は、次のオブジェクトに対して失敗します。

- service-object gre
- service-object 41
- service-object ah

展開の失敗を回避するには、CSM サーバーの DB 側で次の SQL クエリを実行する必要があります。

```
$SIG{INT} = 'IGNORE';
use CRM;
use DBI;
use lib "$ENV{NMSROOT}/lib/perl/install";
use InstallUtility;
require "$ENV{NMSROOT}/cgi-bin/dbadmin/pdbadmin/dbAdminCommon.pl";
my $DROP_CONNECTION_FLAG = false;

checkDMisRunning();
&resolveGreSubTypeEntries();

sub checkDMisRunning
{
 my $d = '\\';
    my ($rc, $dmIsRunning, $line, @lines);
    $rc = open IN, "$ENV{NMSROOT}${d}bin${d}pdshow 2>&1 |";
    if (!$rc)
    {
        print "ERROR: *** Could not execute pdshow ***\n";
        print "ERROR: *** probable cause: daemon manger is corrupted ***";
        exit(-1);
    }

    @lines = <IN>;

    $dmIsRunning = 1;
    for $line (@lines)
    {

        if ($line =~ m/ERROR:\s+connect\s+to\s+dmgtd.*on\s+port\s+.+failed:/)
        {
   $dmIsRunning = 0;
            last;
        }
 }
    close IN;

    if ($dmIsRunning)
    {
        print "Daemon manager is  running ..\n";
     }
 else
 {
    print "Daemon manager is not running ..\n";
  print "Deamon manager should be running to execute this file\n";
  exit(-1);
  }
}
```

```
sub resolveGreSubTypeEntries
{

  $dsn="vms";
  $node_dbh = &dbinternal::connect("dsn=$dsn");

  if ($node_dbh)
  {
   print "\n*****************************************\n";
   print "\nScript Execution Starts \n" ;
   print "\n*****************************************\n";
   my $select_query = "select count(*) from BB_MAIN where OBJECTID =1106 and name='gre'
 and subtype!='SO'";
   my $select_query_prep = $node_dbh->prepare($select_query) || die "Error preparing
query" . $node_dbh->errstr;
   $select_query_prep->execute || die "Error executing query" . $select_query_prep->errstr;

   my @node_results;
      $impactedcount = 0;
   while (@node_results = $select_query_prep->fetchrow_array())
   {
         my $size = @node_results;
      for (my $j=0; $j < $size; $j++)
        {
     $impactedcount = $node_results[$j];
          }
      }
   if($impactedcount > 0){
       my $updateQuery = "update BB_MAIN set subtype='SO' where OBJECTID=1106";
       my $prep = $node_dbh->prepare($updateQuery) || die "Error preparing query" .
$node_dbh->errstr;
       $prep->execute || die "Error executing query" . $prep->errstr;
   }
   print "\n*****************************************\n";
   print "\nScript Execution Completed! \n" ;
   print "\n*****************************************\n";
     }

  return 0;

}
```

スクリプトを ~CSCOpx/bin ディレクトリにコピーし、次のコマンドを実行します。

```
C:\PROGRA~2\CSCOpx\bin\perl
C:\PROGRA~2\CSCOpx\bin\resolveDBEntriesCSCvj54910.pl#!/usr/bin/perl
```

検出中のオブジェクト グループの展開

オブジェクト グループを使用するデバイスからポリシーを検出するとき、グループからポリシー オブジェクトを作成するのではなく、それらのオブジェクト グループを構成する項目に展開するように設定できます。

たとえば、CSM_INLINE_55 という名前のオブジェクト グループにホスト 10.100.10.15、10.100.10.18、および10.100.10.25が含まれる場合、オブジェクトを展開することによりアクセス コントロール リストをインポートすると、CSM_INLINE_55 という名前のネットワーク/ホスト ポリシー オブジェクトではなく、3つすべてのアドレスが送信元セル（または該当する場合は宛先セル）に含まれるルールが作成されます。

展開を設定するには、展開するグループのプレフィックスを識別できるようなオブジェクト グループの命名方式が必要となります。デフォルトでは、プレフィックス CSM_INLINE で始まるすべてのオブジェクト グループが展開されます。[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] を選択し、目次で [検出（Discovery）] を選択することにより、[Discovery] ページ （674 ページ）の [これらのプレフィックスを持つオブジェクト グループを自動展開する（Auto-Expand Object Groups with These Prefixes）] フィールドでこれらのプレフィックスを設定します。

第 13 章

ID 認証ファイアウォール ポリシーの管理

ID 認証ファイアウォールポリシーを使用すると、ユーザー ID またはホストの完全修飾ドメイン名に基づいてトラフィックを制御できます。たとえば、すべてのトラフィックを許可または禁止する代わりに、あるユーザーグループに対しては特定のタイプのトラフィックを選択的に許可し、別のユーザーグループに対しては許可しないようにできます。完全修飾ドメイン名を使用すると、特定のサーバーへの HTTP アクセスを禁止し、他の全サーバーへの HTTP トラフィックを許可できます。

アイデンティティ認識は複数の既存のファイアウォール ルールに組み込まれます。固有の ID 認証ファイアウォール ポリシーはありません。この章では、ID認証ファイアウォールポリシーと、ID 認証をサポートするさまざまなポリシーに ID 認証ファイアウォールポリシーを実装する方法について説明します。

この章は次のトピックで構成されています。

- ID 認証ファイアウォールポリシーの概要 （809 ページ）
- ID 認証ファイアウォール ポリシーの設定 （817 ページ）
- アイデンティティ ファイアウォール ポリシーの監視 （844 ページ）

ID 認証ファイアウォールポリシーの概要

従来のファイアウォールポリシーでは、送信元と宛先の IP アドレス、ポート、およびサービスに基づいて決定が行われます。ASA におけるアイデンティティ ファイアウォールは、以下のいずれか、または両方に基づいたより細かな制御を実現します。

- ユーザー ID：送信元 IP アドレス単独ではなくユーザー名とユーザーグループ名に基づいてアクセスルールとセキュリティポリシーを設定できます。ASA は、IP アドレスと Windows Active Directory のログイン情報の関連付けに基づいてセキュリティポリシーを適用し、ネットワーク IP アドレスではなくマッピングされたユーザー名に基づいてイベントを報告します。

アイデンティティ ファイアウォールは、実際のアイデンティティマッピングを提供する外部 Active Directory（AD）エージェントと連携する Microsoft Active Directory と統合されます。ASA では、特定の IP アドレスに対する現在のユーザーのアイデンティティ情報を取得する情報元として Windows Active Directory を使用し、Active Directory ユーザーのトランスペアレント認

証を実現します。AD エージェントのセットアップおよび設定の詳細については、Cisco.com（http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html）の*Active Directory* エージェントインストール/セットアップガイド [英語] を参照してください。

- FQDN ネットワークオブジェクト：ホストの IP アドレスではなく、完全修飾ドメイン名（FQDN）をルールで使用できるため、ホストのアドレスが変更された場合（DHCP を介してアドレスを取得する場合など）、ルールは引き続き適用されます。

アイデンティティに基づくファイアウォールサービスは、送信元または宛先 IP アドレスの代わりに、送信元および FQDN としてユーザーまたはグループを指定できるようにすることで、既存のアクセス制御メカニズムとセキュリティポリシー メカニズムを強化します。アイデンティティに基づくセキュリティ ポリシーは、従来の IP アドレス ベースのルール間の制約を受けることなくインターリーブできます。

アイデンティティ ファイアウォールの主な利点には、次のようなものがあります。

- セキュリティ ポリシーからのネットワーク トポロジの分離。ユーザーが接続するネットワークの場所に関係なく、ルールがユーザーに適用されます。
- セキュリティポリシー作成の簡略化。
- ネットワークリソースに対するユーザーアクティビティを容易に検出可能。
- ユーザー アクティビティ モニタリングの簡略化。

ここでは、次の内容について説明します。

- ユーザー ID の取得　（810 ページ）
- ID 認証ファイアウォール ポリシーの要件　（811 ページ）
- ID 認証サービスを提供するためのファイアウォールの設定　（816 ページ）

ユーザー ID の取得

ファイアウォールポリシーで Active Directory ユーザ名またはユーザグループ名を指定する場合、ASA は最終的にその名前を IP アドレスにマッピングして、パケットを処理する必要があります。ASA はこの情報に次の 2 つのプライマリ ソースを使用します。

- ユーザ グループ メンバーシップ：ルールでユーザグループを指定すると、ASA は設定された Active Directory（AD）サーバーに接続して、グループメンバーシップを取得します。
- ユーザから IP アドレスへのマッピング：標準（VPN 以外）ネットワーク上のネットワーク ドメインにログインするユーザに対して、AD エージェントは、AD サーバーとの通信で、ログイン情報を取得し、ユーザから IP アドレスへのマッピングテーブルを作成します。この情報は ASA に提供されます。

ユーザベースのアイデンティティ ファイアウォール ポリシーを構成する前に、必要な AD サーバーとエージェントをインストールして構成する必要があります。さまざまな導入シナリオの説明については、http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_

guides_list.htmlにある ASDM または CLI の ASA コンフィギュレーション ガイドを参照してください。

ユーザ名は、次のタイプのトラフィックに対して取得され、特に記載がない限り、AD ドメインが含まれます。

- 標準トラフィック。
- IPsec IKEv1 および IKEv2、AnyConnect クライアント、および L2TP VPN を含むリモートアクセス VPN。VPN に LDAP 認証を使用し、VPN とアイデンティティ ファイアウォールのドメインに同じサーバーグループを使用する場合、ユーザは認証に使用されるドメインに関連付けられます。他のすべての承認メカニズムでは、VPN を介して取得されたユーザは、ローカルドメインに存在すると見なされます。ASA は、これらのユーザを AD エージェントに報告します。AD エージェントは、AD エージェントに登録されている他の ASA またはクライアントにそれらのユーザを配布します。

（注） クライアントレス SSL VPN では、ユーザ名は取得されません。

- IPv4 カットスループロキシ。IPv6カットスループロキシの場合、ユーザ名は取得されません。認証時にユーザ名にドメイン名が含まれている場合、そのユーザはドメイン名に関連付けられます。それ以外の場合、ドメインは、アイデンティティ オプション ポリシーで設定されているデフォルト メインとなります。カットスルー プロキシの設定 （839 ページ） を参照してください。

ID 認証ファイアウォール ポリシーの要件

ID 認識ファイアウォールポリシーは、すべてのタイプのデバイスおよびオペレーティングシステムでサポートされているわけではありません。次の表では、これらのタイプのポリシーをネットワークに実装するための要件と、いくつかの制限について説明します。

表 *169 : ID* 認証ファイアウォール ポリシーの要件

要件	説明
ファイアウォールデバイス	ASA ソフトウェアバージョン 8.4(2) 以降を実行しているが、8.5(1) を実行している ASA-SM を含まない ASA。単一または複数のコンテキスト構成。 **ヒント** ASA にはオンボード暗号化アクセラレーションが必要です。デバイスに必要な機能があるかどうかを確認するには、デバイスコンソールにログインし、**show version** コマンドを実行します。出力に「暗号化ハードウェアデバイス（Encryption hardware device）」が含まれている必要があります。 1 つの Active Directory エージェントに最大 100 の ASA を登録できます。

要件	説明
Active Directory（AD）	ユーザーとユーザーグループを定義するには、Active Directory を使用する必要があります。ASA は、LDAP プロトコルを実行する AD サーバーから直接ユーザーグループ情報を取得します。他のタイプの LDAP サーバーは使用できません。 サポートされる AD サーバーのタイプと、その設定要件の詳細については、Cisco.com（https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-guides-list.html）の*Active Directory* エージェントのインストールおよびセットアップガイド [英語] を参照してください。 **ヒント** 複数の AD サーバーを設定できますが、それぞれがすべてのドメイン間で一意の IP アドレスを持つ必要があります。他のタイプの LDAP サーバーはサポートされていません。
AD エージェント	ASA と AD サーバー間の仲介として機能するように、オフボックス AD エージェントを設定する必要があります。AD エージェントは、ユーザーと IP アドレスのアクティブなマッピングを保持します。 デフォルトでは、5505 を除き、ASA はブート時またはリロード時にこのリストを取得し、AD エージェントは収集された新しいマッピングを送信します。5505 はアイデンティティ基準を含むトラフィック一致ルールに対応し、必要に応じて AD エージェントを照会します。これはアイデンティティ オプション ポリシーを使用して変更できますが、このデフォルトの動作を使用することをお勧めします。 AD エージェントは RADIUS プロトコルを使用します。 AD エージェントのセットアップおよび設定の詳細については、Cisco.com（http://www.cisco.com/en/US/products/ps6120/prod_installation_guides_list.html）の *Active Directory* エージェントインストール/セットアップガイド [英語] を参照してください。
クライアント システム	デバイスを介してトラフィックを渡すユーザーは、次のクライアントプラットフォームのいずれかを使用する必要があります。 • Windows XP SP3 • Windows Vista • Windows 7 • その他のシステムで、明示的にサポートされるプラットフォームと同じ方法で Active Directory を使用するもの。

要件	説明
IPv6	IPv6 は、次の例外を除いてサポートされています。 • IPv6 上の NetBIOS はサポートされていません。 • ユーザーワークステーションでの複数の IPv6 アドレスはサポートされていません。Windows 64 ビットのシステムでは、通信を開始するときに一時的な IPv6 アドレスを使用する場合があります。ユーザーが 1 つの IPv6 アドレスを使用して AD エージェントに登録し、別のアドレスを使用して通信を開始した場合、ユーザーの ID 認識ファイアウォールルールは適用されず、代わりに 2 番目の IPv6 アドレスに一致するルールが適用されます。 。 これらの一時アドレスの使用を無効にするためのオプションが 2 つあります。 • ネットワーク内のすべてのネットワーキングデバイスのすべてのインターフェイスで、IPv6 ルーティング アドバタイズメントを無効にする。 • 各 Windows マシンでコマンド ウィンドウを開き、次のコマンドを入力してワークステーションをリブートする。 **netsh interface ipv6 set privacy state=disable** **netsh interface ipv6 set global randomizeidentifiers=disabled**

要件	説明
NetBIOS ログアウト プローブ （オプション）	NetBIOS ログアウト プローブをイネーブルにすると、ASA は NetBIOS を使用して、非アクティブ ユーザをデータベースから削除できるように、このユーザをログオフするかどうか判断できます。プローブは、UDP でカプセル化された NetBIOS トラフィックを使用します。したがって、アクセスルールが、ASA、AD エージェント、およびユーザーワークステーション間のネットワーク上で次のトラフィックを確実に許可するようにする必要があります。 • クエリパケット：任意の UDP ソースポートから UDP ポート 137（UDP/137）。 • クエリ応答：UDP/137 ソースから任意の UDP ポート。 さらに、NetBIOS応答パケットにユーザ名が提供されるよう、ワークステーションを設定する必要があります。Windows ワークステーションの場合、メッセンジャーサービスを有効にしてWINSを構成する必要があります。メッセンジャーサービスがオンになっていない場合、ユーザーがログオンしていてもログオンしていなくても、ワークステーションからの応答は同じです。 **ヒント** • NetBIOS ログアウトプローブは、VPN またはカットスルー プロキシ ユーザーでは使用されません。 • ASA には非アクティブ ユーザのタイムアウト設定があります。これは、データベースからユーザを削除するためにも使用されます。このタイマーはすべてのユーザ タイプに適用されます。したがって、データベースから非アクティブ ユーザを削除するために、NetBIOS プローブの実装は不要です。

要件	説明
DNS の設定 （完全修飾ドメイン名の使用に必要）	Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）のネットワーク/ホストオブジェクトをファイアウォールルールに使用する場合は、ドメインネームシステム（DNS）を [DNS] ページ （2616 ページ）の説明のように設定する必要があります。これらの設定により、名前を検索して関連する IP アドレスを判別するために使用される DNS サーバーが識別されます。最終的には、すべての処理がこの IP アドレスに基づいて行われます。 FQDN を使用するように DNS を設定する場合は、次の点を考慮してください。 • DNS 応答はスプーフィングされる可能性があり、ネットワークにセキュリティホールが開く可能性があります。信頼できる DNS サーバーのみを指定します。ネットワーク内の DNS サーバーのみを指定するのが理想的です。 • 一部のホストは、常に変化する複数の IP アドレスを使用する場合があるため、ASA が任意の時点ですべての有効な IP アドレスを持つとは限りません。 • 存続時間の値が短いホスト名では、DNS ルックアップを頻繁に行う必要があります。これは、ASA のパフォーマンスに影響を与える可能性があります。 • 複数のホスト名を同じ IP アドレスに解決できます。最終的に、ファイアウォールルールは IP アドレスに基づいて適用されます。つまり、2 つの名前が同じアドレスに割り当てられ、使用中のルールで、これらの名前に別々のサービスが指定されている場合、実際に提供されるサービスは、最初に一致したルールに指定されたものになります。 ルールにすべてのバージョンの FQDN ホスト名を指定しなくても済むような、別の方法を検討してください。複数の名前が常に同じホストを指していることがわかっている場合は、最も一般的に使用される名前に対してルールを設定して、その名前のすべての同義語にルールが適用されるようにすることができます。

要件	説明

上限	ユーザー、ユーザーグループ、およびユーザーあたりの IP アドレスの数には制限があります。これらの制限を超えると、追加のトラフィックに対して ID 認識処理が実行されません。
	• IP アドレスの制限：1 人のユーザーを、すべてのドメインで最大 8 つの IP アドレスに関連付けることができます。
	• ユーザーグループの制限：ポリシーは、最大 256 のユーザーグループに適用できます。ユーザーは複数のユーザーグループに属することができます。
	• ユーザの制限：ポリシーは次のユーザ数まで適用できます。この数は、デバイスで定義されているすべてのコンテキストの合計です。
	  • ASA 5505：1024 ユーザー。
	  • その他の ASA 5500 シリーズ：64,000 ユーザー。

ID 認証サービスを提供するためのファイアウォールの設定

ID 認証ファイアウォールサービスをネットワークに提供するには、複数のポリシーを設定して、ファイアウォールでユーザーベースまたは完全修飾ドメイン名（FQDN）ベースのルールを処理できるようにする必要があります。ASA は、ネットワーク内の他のサーバーに依存して、ID 認証ポリシーを実装するために必要なユーザー、ユーザーグループ、および FQDN 名前解決サービスを提供します。

必要な構成は、使用する ID 認証の側面によって異なります。

- ユーザー、ユーザーグループの解決：ファイアウォールルールでアイデンティティ ユーザー グループ オブジェクトを使用するには、いくつかのオブジェクトとポリシーを設定して、ユーザーとユーザーグループの情報を提供する Active Directory サーバーを識別する必要があります。
- FQDN 解決：ファイアウォールルールで FQDN ネットワーク/ホストオブジェクトを使用するには、FQDN を IP アドレスに解決するように DNS サーバーを設定する必要があります。

この手順では、ID 認証ポリシーを実装するプロセス全体について説明します。

はじめる前に

ご使用のネットワークが、ID 認証ファイアウォール ポリシーの要件 （811 ページ）に説明がある要件に適合している必要があります。次の手順では、すでに Active Directory（AD）を使用しており、AD エージェントをインストールして設定し、これらのサービスが正しく動作していることを前提としています。

ステップ 1 AD ユーザーとユーザーグループの解決を有効にします。

a) AD サーバーとエージェントを識別し、サーバーグループの NetBIOS ドメインを設定するために必要なポリシーオブジェクトを作成します。詳細については、Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。

b) デフォルト以外の設定が必要な場合はアイデンティティ オプションを変更してください。これらのオプションを使用して NetBIOS ログアウト プローブをイネーブルにし、さまざまなタイマー処理やエラー処理を設定します。詳細については、アイデンティティ オプションの設定 （828 ページ）を参照してください。

c) （AD で定義されたユーザーグループに加えて）ASA で定義されたユーザーグループを作成する場合は、必要なアイデンティティ ユーザー グループ ポリシーオブジェクトを作成します。アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）を参照してください。

ステップ 2 FQDN ネットワーク/ホストオブジェクトの解決を有効にします。

a) DefaultDNS グループに DNS サーバを設定します。FQDN を IP アドレスに解決するには、DNS が必要です。DNS の設定手順については、[DNS] ページ （2616 ページ）を参照してください。

b) ネットワーク/ホストオブジェクトの作成 （394 ページ）の説明に従って、FQDN ネットワーク/ホストオブジェクトを作成します。

ステップ 3 FQDN オブジェクト、ユーザ名、ユーザ グループ名、またはアイデンティティ ユーザ グループ オブジェクトを使用するファイアウォール ルールを設定します。アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）を参照してください。

ステップ 4 アイデンティティ ファイアウォール システムを監視します。アイデンティティ ファイアウォール ポリシーの監視 （844 ページ） を参照してください。

ID 認証ファイアウォール ポリシーの設定

アイデンティティ認識は複数の既存のファイアウォール ルールに組み込まれます。固有の ID 認証ファイアウォール ポリシーはありません。この項では、アイデンティティ認識をファイアウォール ポリシーに統合するためのさまざまな手順について説明します。

ここでは、次の内容について説明します。

- ID 認証ファイアウォール サービスのイネーブル化 （818 ページ）
- アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）
- ポリシーでのアイデンティティ ユーザの選択 （835 ページ）
- アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）
- カットスルー プロキシの設定 （839 ページ）
- ユーザ統計の収集 （842 ページ）
- アイデンティティ ベースのルールを使用した VPN トラフィックのフィルタリング （843 ページ）

ID 認証ファイアウォール サービスのイネーブル化

アイデンティティ オプション ポリシーを使用して、アイデンティティ認識型ファイアウォールサービスを有効にします。ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [アイデンティティオプション（Identity Options）] を選択します。
- （ポリシービュー）ポリシーセレクタから [アイデンティティオプション（ASA）（Identity Options (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ポリシーには次のタブがあります。

- [AD設定（AD Setup）]：ネットワークのユーザおよびユーザグループを定義する Active Directory サーバーと、情報の収集に使用する AD エージェントを設定し、それを ASA に提供します。Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。
- [詳細設定（Advanced）]：ユーザ アイデンティティ サービスをイネーブルまたはディセーブルにし、エラー処理、NetBIOS ログアウトプローブ、アイドルタイムアウト、および AD エージェント通信設定用のオプションを設定します。アイデンティティ オプションの設定 （828 ページ） を参照してください。

Active Directory サーバおよびエージェントの識別

[Identity Options] ポリシーの [AD Setup] タブを使用して、ユーザ ID 情報に使用する Active Directory サーバとエージェントを識別します。ユーザ指定（アイデンティティユーザ グループ オブジェクトなど）を含む ID 認証ファイアウォール ポリシーをイネーブルにするには、1 つ以上の AD サーバと AD エージェントを設定する必要があります。

（注） ID 認証ファイアウォールには ASA ソフトウェア 8.4(2+) が必要です。

はじめる前に

設定では AAA サーバ グループ ポリシー オブジェクトを使用します。このオブジェクトには AAA サーバ オブジェクトが組み込まれます。これらのオブジェクトは Policy Object Manager（[Manage] > [Policy Objects]）から作成するか、この手順の実行（設定ウィザードを使用するか、オブジェクト セレクタ ダイアログボックスで [Add Object]（+）ボタンをクリックする）によって作成します。

オブジェクトは、次の要件を満たす必要があります。

- AD サーバ：LDAP プロトコルを使用する必要があります。LDAP サーバ タイプとして Microsoft を選択していると、ユーザ グループの検索のベース ディレクトリを識別し、検索時間を短縮する LDAP グループ ベース DN を指定することもできます。[Auto Detect] を選択した場合、Microsoft AD サーバがアイデンティティ ファイアウォールの設定で使用で

きる LDAP サーバの唯一のタイプであっても、グループ ベース DN は設定できません。Security Manager と Active Directory の通信については、次の制限に従う必要もあります。

- [Enable LDAP over SSL] オプションを選択しない。
- [SASL Kerberos Authentication] オプションを選択しない。シンプルおよび SASL MD5 認証メカニズムのみがサポートされます。ユーザ名とパスワードが平文で送信されるシンプルなメカニズムは、SASL オプションのいずれかを選択していない場合に使用されます。

- AD エージェント：RADIUS プロトコルを使用する必要があります。AAA サーバー グループ オブジェクトで、[AD エージェントモード（AD Agent Mode）] オプションを選択します。

このポリシーを設定する前に、AD エージェントをインストールおよび設定しておく必要があります。サーバ グループには AD エージェントを最大 2 つ設定できます。2 番目のエージェントは、最初のエージェントがクエリーへの応答を停止した場合にのみ使用されます。この 2 つのエージェント以降に定義されたエージェントはすべて無視されます。

http://www.cisco.com/go/asa から AD エージェントソフトウェアを入手します。AD エージェントのセットアップおよび設定の詳細については、Cisco.com の『*Installation and Setup Guide for the Active Directory Agent*』を参照してください。

関連項目

- ID 認証ファイアウォール ポリシーの要件 （811 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- AAA サーバ オブジェクトの作成 （330 ページ）
- [AAA Server] ダイアログボックス - LDAP 設定 （339 ページ）
- AAA サーバ グループ オブジェクトの作成 （349 ページ）
- アイデンティティ オプションの設定 （828 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [アイデンティティオプション（Identity Options）] を選択します。[AD Setup] タブを選択します。
- （ポリシー ビュー）ポリシーセレクタから [アイデンティティオプション（ASA）（Identity Options (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[AD Setup] タブを選択します。

ステップ 2 AD Setup のガイドを利用する場合は、[アイデンティティの設定（Configure Identity）] ボタンをクリックして Identity Configuration ウィザードを開始してください。このウィザードによって、ドメイン用の AD サーバと、AD エージェントを設定するプロセスが実行され、必要な AAA サーバおよび AAA サーバ グループ オブジェクトを作成できます。

ウィザードでは次の手順を実行します。

- AD サーバ設定：ドメイン用の AD サーバを設定します。 Identity Configuration ウィザードの Active Directory Settings （822 ページ）を参照してください。
- AD エージェント設定：ASA 用の AD エージェントを設定します。 Identity Configuration ウィザードの Active Directory エージェント （825 ページ）を参照してください。
- プレビュー：作成されるオブジェクトを表示します。 Identity Configuration ウィザードの Preview （827 ページ）を参照してください。

ヒント このウィザードを複数回使用すると、さまざまな NetBIOS ドメインを設定できます。ただし、このウィザードでは常に AD エージェント情報の入力を求められます。AD エージェントにはドメイン単位に別個のグループを設定するのではなく、単一グループを設定するため、すでに行った AD エージェントの設定が選択によって上書きされます。そのため、ウィザードを実行するたびに、必ず AD エージェントに同じ AAA サーバーグループを選択してください。

ステップ 3 ウィザードを使用しない場合は、AD サーバを設定します。AD サーバは、ID 認証ファイアウォール ポリシーで使用する AD ユーザ グループについてのユーザ メンバーシップ情報を取得するために使用されます。

テーブルにはネットワーク用の AD サーバがリストされます。個々の NetBIOS ドメイン名にエントリを追加する必要があります。各行には AAA サーバ グループが定義され、ドメインに対応する AD LDAP サーバの識別と、AD サーバ グループが使用できない場合に、ドメインの ID 認証ファイアウォール ルールをアクティブにするかどうかの判断に使用されます。

次を実行できます。

- エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[AD ドメインサーバーの追加（Add AD Domain Server）] ダイアログボックスに入力します。 [Domain AD Server] ダイアログボックス （821 ページ）を参照してください。
- エントリを編集するには、エントリを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- エントリを削除するには、エントリを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

ステップ 4 ウィザードを使用しない場合は、AD エージェントを設定します。AD エージェントはユーザのログオン/ログアウトと IP アドレス マッピングを AD サーバから入手します。次に、ASA は AD エージェントから情報を取得します。

[Active Directoryエージェントグループ（Active Directory Agent Group）] で、AD エージェントのリストを定義する AAA サーバー グループ オブジェクトの名前を入力します。あるいは [選択（Select）] をクリックしてオブジェクトを選択するか、グループオブジェクトを新しく作成します。

ステップ 5 [デフォルトドメイン（Default Domain）] で、デバイスのデフォルトドメインとして設定するドメインを選択します。ドメインをデフォルト ドメインとして選択する前に、そのドメインを AD サーバに追加する必要があります。

デフォルトは LOCAL です。これは、デバイスに定義されたユーザ グループまたはアイデンティティ サービス用に設定された AD サーバ以外の方法を使用して認証を行う VPN ユーザに適用されます。この設定はカットスルー プロキシを設定する場合にも使用されます（カットスルー プロキシの設定 （839 ページ）を参照）。

ステップ 6 [保存（Save）] をクリックして変更を保存します。

管理設定の [Identity Settings] ページを、ドメインから AD サーバへのマッピングを使用して更新するかどうかの問い合わせがあります。ID設定によって、ファイアウォール ポリシーまたはアイデンティティ ユーザ グループ オブジェクトでユーザまたはユーザ オブジェクトを指定する際に、どのサーバを使用して [Find] 機能を使用するかが決まります。ID 管理設定は、ASA の設定には影響を与えません。

[Domain AD Server] ダイアログボックス

NetBIOS ドメインに Active Directory サーバを定義するには、[Add Domain AD Server] または [Edit Domain AD Server] ダイアログボックスを使用します。NetBIOS ドメインにユーザ グループのファイアウォール ルールを設定すると、ユーザ メンバーシップはドメインに定義した AD サーバを照会することによって決まります。

ナビゲーション パス

次のいずれかを実行します。

- [Identity Options] ページの [AD Setup] タブで、ドメイン テーブルの [Add] または [Edit] ボタンをクリックします。Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。
- ID 設定の Security Manager 管理ページで、設定テーブルの [Add] または [Edit] ボタンをクリックします。これらの設定は、ファイアウォール ルールまたはアイデンティティ ユーザ グループ オブジェクトの設定で、[Find] を使用してユーザ名またはユーザ グループ名を検索する際に、どのサーバを使用するかを決定します。[Identity Settings] ページ （693 ページ）を参照してください。

フィールド リファレンス

表 170 : [Domain AD Server] ダイアログボックス

要素	説明
ドメイン	この AD サーバ グループの NetBIOS ドメイン。ドメイン名は最大 32 文字まで指定できます。通常はすべて大文字です。たとえば、ユーザ指定が DOMAIN\user1 の場合、DOMAIN は NetBIOS ドメイン名になります。

要素	説明
AD Server Group	AAA サーバ グループ ポリシー オブジェクトの名前。この名前によって、このドメインの AD サーバが指定されます。オブジェクトで LDAP プロトコルを使用する必要があります。 [選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。
Disable Rules When Server Is Down （アイデンティティ オプション ポリシーのみ）	ドメイン コントローラが停止している場合、このドメインのすべての ID 認証ファイアウォール ルールをディセーブルにするかどうかを指定します。このオプションを選択した場合、ドメインのすべてのユーザは、サーバが使用可能になるまでディセーブルとマークされます。
Update Administrative Settings （アイデンティティ オプション ポリシーのみ）	ドメインとサーバのマッピングを [Security Manager Administration] の [Identity Settings] ページに追加するかどうかを指定します。この管理ページによって、ファイアウォール ポリシーまたはアイデンティティ ユーザ グループ オブジェクトに、ユーザまたはユーザ グループを追加する場合、これらの検索時にどの AD サーバを照会するかが決定されます。詳細については、[Identity Settings] ページ （693 ページ）を参照してください。

Identity Configuration ウィザードの Active Directory Settings

NetBIOS ドメインの Active Directory（AD）サーバを識別するには、Identity Configuration ウィザードの [Active Directory Settings] ページを使用します。これらの設定は、ユーザ ID 対応のファイアウォール ポリシーをドメイン内のユーザでイネーブルにするために必要です。

ナビゲーション パス

次のいずれかを実行します。

- [アイデンティティオプション（Identity Options）] ページの [ADセットアップ（AD Setup）] タブで [アイデンティティの設定（Configure Identity）] ボタンをクリックします。Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。
- アイデンティティ オプションのポリシーがまだ設定されていない場合は、[User] フィールドの [Select] ボタンをクリックし、アイデンティティを設定するかどうかの質問には [Yes] をクリックすると、AAA ルール ポリシー、アクセス ルール ポリシー、またはインスペクション ルール ポリシーからこのウィザードを開始できます。

フィールド リファレンス

表 *171 : Identity Configuration* ウィザードの *Active Directory Settings*

要素	説明
NetBIOS ドメイン（NetBIOS Domain）	この AD サーバ グループの NetBIOS ドメイン。ドメイン名は最大 32 文字まで指定できます。通常はすべて大文字です。たとえば、ユーザ指定が DOMAIN\user1 の場合、DOMAIN は NetBIOS ドメイン名になります。
Select Existing AD Server Group	必要な AD サーバを識別する AAA サーバ グループ ポリシー オブジェクトがすでに存在している場合はこのオプションを選択します。オブジェクトで LDAP プロトコルを使用する必要があります。 [グループ名（Group Name）] フィールドの横にある [選択（Select）] をクリックし、オブジェクトを選択します。
Create New AD Server Group	AAA サーバ グループ ポリシー オブジェクトがまだ存在していないか、ウィザードでオブジェクトを新たに作成する場合にこのオプションを選択します。 オブジェクトに含まれるグループおよびサーバを識別するように、残りのオプションを設定します。
[Create AD Server Group] プロパティ	
グループ名（Group Name） （ウィザードでグループを作成する場合）	作成する AAA サーバ グループ オブジェクトの名前。名前には最大 16 文字を使用できます。
AD Server Name/IP	次のいずれかです。 • AD サーバを定義する既存の AAA サーバ オブジェクトの名前。[選択（Select）] をクリックして、リストからオブジェクトを選択します。 オブジェクトを選択すると、残りのプロパティを設定できなくなります。 • AD サーバの IP アドレス。

要素	説明
ユーザー名	認証済みバインディングに使用されるLDAP階層内のユーザまたはディレクトリ オブジェクトの名前（最大 128 文字）。認証済みバインディングは、一部の LDAP サーバ（Microsoft Active Directory サーバなど）によって、他の LDAP 操作の実行前に要求されます。このフィールドには、デバイスの認証特性が記述されます。これらの特性は、管理者特権を持つユーザーの特性に対応している必要があります。 この文字列では、大文字と小文字が区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。 通常は、DOMAIN\Administrator などのユーザ名です。従来型のフォーマット（cn=Administrator、OU=Employees、DN=example、DN=com など）を使用してもかまいません。
パスワード 確認（Confirm）	LDAPサーバにアクセスするための、大文字と小文字が区別される英数字のパスワード（最大 64 文字）。スペースは使用できません。
インターフェイス	すべての発信パケットに対して、そのIPアドレスが使用されるインターフェイス（送信元インターフェイスと呼ばれます）。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。 **ヒント** • インターフェイスの名前を入力する場合、このAAAオブジェクトを使用するポリシーが、この名前のインターフェイスを含むデバイスに割り当てられるようにします。 • インターフェイス ロールの名前を入力する場合、ロールが複数のインターフェイスではなく、1つのインターフェイスを表すようにします。 • AAA サーバ グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。複数のサーバを指定する場合は、すべて同じインターフェイスにする必要があります。
Add Another AD Server	サーバを別に作成する場合にのみ、このボタンをクリックしてください。 このボタンをクリックすると、サーバ フィールドの情報が保存されてフィールドがクリアされ、次のサーバの情報を追加できるようになります。サーバは、シングルコンテキスト モードでは16台まで、マルチコンテキスト モードでは 4 台まで追加できます。

Identity Configuration ウィザードの Active Directory エージェント

NetBIOS ドメインの Active Directory（AD）エージェントを識別するには、Identity Configuration ウィザードの [Active Directory Agent Settings] ページを使用します。これらの設定は、ユーザ ID 対応のファイアウォール ポリシーをドメイン内のユーザでイネーブルにするために必要です。

ヒント ASA に単一の AD エージェント グループを設定できます。NetBIOS ドメインごとにに別のグループを設定しないでください。したがって、アイデンティティ オプションのポリシーに正しい AD エージェント グループをすでに設定している場合は、このウィザードページで同じグループを選択してください。ポリシーで定義されているグループがこのページで選択した内容に置き換えられます。

ナビゲーション パス

次のいずれかを実行します。

- [アイデンティティオプション（Identity Options）]ページの [ADセットアップ（AD Setup）] タブで [アイデンティティの設定（Configure Identity）] ボタンをクリックし、次のページに進みます。 [Identity Settings] ページ （693 ページ）を参照してください。
- アイデンティティ オプションのポリシーがまだ設定されていない場合は、[User] フィールドの [Select] ボタンをクリックし、アイデンティティを設定するかどうかの質問には [Yes] をクリックすると、AAA ルール ポリシー、アクセス ルール ポリシー、またはインスペクション ルール ポリシーからこのウィザードを開始できます。

フィールド リファレンス

表 *172 : Identity Configuration* ウィザードの *Active Directory Agent Settings*

要素	説明
Select Existing AD Agent Group	必要な AD エージェントを識別する AAA サーバ グループ ポリシー オブジェクトがすでに存在している場合はこのオプションを選択します。このオブジェクトは RADIUS プロトコルを使用し、[ADエージェント モード（AD Agent Mode）] オプションを選択している必要があります。 [グループ名（Group Name）] フィールドの横にある [選択（Select）] をクリックし、オブジェクトを選択します。
Create New AD Agent Group	AAA サーバ グループ ポリシー オブジェクトがまだ存在していないか、ウィザードでオブジェクトを新たに作成する場合にこのオプションを選択します。 オブジェクトに含まれるグループおよびサーバを識別するように、残りのオプションを設定します。

要素	説明
[Create AD Agent Group] プロパティ	
グループ名（Group Name） （ウィザードでグループを作成する場合）	作成する AAA サーバ グループ オブジェクトの名前。名前には最大 16 文字を使用できます。
AD Agent Name/IP	次のいずれかです。 • AD エージェントを定義する既存の AAA サーバ オブジェクトの名前。[選択（Select）] をクリックして、リストからオブジェクトを選択します。 オブジェクトを選択すると、残りのプロパティを設定できなくなります。 • AD エージェントの IP アドレス。
秘密キー（Secret Key） 確認（Confirm）	ネットワーク デバイス（クライアント）と AAA サーバ間でデータを暗号化するために使用される共有秘密キー。キーでは、127 文字以下の英数字で、大文字と小文字を区別します。特殊文字も使用可能です。 このフィールドで定義したキーは、RADIUS サーバのキーと一致している必要があります。確認フィールドでもう一度キーを入力します。 キーを定義しない場合、AAA サーバとその AAA クライアント間のすべてのトラフィックは暗号化されずに送信されます。
インターフェイス	すべての発信パケットに対して、そのIPアドレスが使用されるインターフェイス（送信元インターフェイスと呼ばれます）。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは[選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。 **ヒント** • インターフェイスの名前を入力する場合、この AAA オブジェクトを使用するポリシーが、この名前のインターフェイスを含むデバイスに割り当てられるようにします。 • インターフェイス ロールの名前を入力する場合、ロールが複数のインターフェイスではなく、1 つのインターフェイスを表すようにします。 • AAA サーバ グループ内の AAA サーバに対して定義できる送信元インターフェイスは 1 つだけです。複数のサーバを指定する場合は、すべて同じインターフェイスにする必要があります。

要素	説明
Add Secondary AD Agent	エージェントを別に作成する場合にのみ、このボタンをクリックしてください。このエージェントは、最初のエージェントが使用できなくなった場合に使用されます。 このボタンをクリックすると、エージェント フィールドの情報が保存されてプレビュー ページに追加され、フィールドがクリアされて 2 番目のエージェントの情報を追加できるようになります。

Identity Configuration ウィザードの Preview

Identity Configuration ウィザードに入力した情報を確認するには、このウィザードの [Preview] ページを使用します。

プレビューには NetBIOS ドメインの Active Directory 設定に作成または使用されるオブジェクトの情報がまとめられています。

- AD サーバ グループには、このドメインで使用される AD サーバの AAA サーバ グループ オブジェクト名が示されます。テーブルには各 AD サーバを定義する AAA サーバ オブジェクトが示されます。
- AD エージェントには、AD エージェントの AAA サーバ グループ オブジェクト名が示されます。プライマリ エージェントとセカンダリ エージェントには、エージェントを定義する AAA サーバ オブジェクトが示されます。

ウィザードで作成されるオブジェクトの場合、名前は AAA サーバーオブジェクト用に自動的に生成され、**ldap_** または **radius_** がプレフィックスとしてサーバーの IP アドレスに追加されます。

変更する場合、[戻る（Back）] をクリックします。変更しない場合は、[終了（Finish）] をクリックして設定を保存します。

ヒント　ウィザードを完了すると、新たに作成されたオブジェクトのプロパティを編集して、ウィザードがデフォルト設定として残した設定値を設定できます。

ナビゲーション パス

次のいずれかを実行します。

- [アイデンティティオプション（Identity Options）] ページの [ADセットアップ（AD Setup）] タブで [アイデンティティの設定（Configure Identity）] ボタンをクリックし、次のページに進みます。Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。
- アイデンティティ オプションのポリシーがまだ設定されていない場合は、[User] フィールドの [Select] ボタンをクリックし、アイデンティティを設定するかどうかの質問には [Yes]

をクリックすると、AAA ルール ポリシー、アクセス ルール ポリシー、またはインスペクション ルール ポリシーからこのウィザードを開始できます。

アイデンティティ オプションの設定

アイデンティティ オプション ポリシーの [Advanced] タブを使用して、ユーザ ID サービスをイネーブルまたはディセーブルにし、エラー処理、NetBIOS ログアウト プローブ、アイドル タイムアウト、および AD エージェント通信設定用のオプションを設定します。このタブに含まれるオプションにはデフォルト値があるため、実際のネットワーク用に設定を微調整する必要がある場合にのみ、値を変更します。

ナビゲーション パス

- （デバイス ビュー）ASA デバイスを選択し、ポリシー セレクタから [アイデンティティ オプション（Identity Options）] を選択します。[Advanced] タブを選択します。
- （ポリシー ビュー）ポリシー セレクタから [アイデンティティ オプション（ASA）（Identity Options (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[Advanced] タブを選択します。

関連項目

- Active Directory サーバおよびエージェントの識別 （818 ページ）
- ID 認証ファイアウォール ポリシーの要件 （811 ページ）

フィールド リファレンス

表 *173 :* アイデンティティ オプションの *[Advanced]* タブ

要素	説明
Enable User Identity	[AD設定（AD Setup）] タブに AD エージェントと AD サーバーが設定されている場合、これらからユーザ ID 情報を入手するためにデバイスをイネーブルにするかどうかを指定します。デフォルトではイネーブルになっています。 このオプションを変更して展開すると、この変更には新しい設定に基づいた次の効果があります。 • ディセーブル：ユーザ マッピング データベースに対する IP アドレス全体が消去され、有効なユーザ固有のルールがないすべてのユーザが解放されます。ADエージェントおよびサーバは更新に対するクエリーを受信しなくなり、有効なユーザ ID ベースのすべてのルールは、トラフィックに影響を与えなくなります。 • イネーブル：有効なユーザがADエージェントとの通信を介して段階的に再作成されます。VPNユーザの再認証が必要な場合があります。AD エージェントと AD サーバへのクエリーが再開されます。
エラー状態	
Disable Rules When Active Directory Agent Is Down	AD エージェントへの接続が使用できない場合に、ユーザ ID を含むすべてのルールをディセーブルにするかどうかを指定します。このオプションを選択すると、ユーザから IP アドレスへのマッピングはすべてディセーブルとマークされ、ユーザの詳細情報を含むルールがすべてトラフィックに適用されなくなります。デフォルトでは、このオプションはディセーブルです。
Remove User IP When NetBIOS Probe Fails	ユーザの NetBIOS プローブが何らかの理由で失敗した（プローブがネットワーク内でブロックされているか、ユーザが活動していないためにプローブに失敗した）場合に、ユーザの IP アドレスマッピングをデータベースから削除するかどうかを指定します。ユーザはワークステーションにログインし直す必要があります。NetBIOS ログアウト プローブをこのページでイネーブルにした場合にのみ、このオプションに効果があります。デフォルトでは、このオプションはディセーブルです。

要素	説明
[ユーザのMACアドレスが不整合の場合にユーザIPを削除する（Remove User IP When User's MAC Address is Inconsistent）]	ユーザがマッピングされたIPアドレスからの要求ごとに、そのMedia Access Control（MAC; メディア アクセス コントロール）アドレスと前のパケットの MAC アドレスとを確認するかどうかを指定します。 このオプションを選択し、MAC アドレスがパケット間で変化した場合、ユーザと IP アドレスのマッピングはデータベースから削除され、後続のパケットはドロップされます。ユーザは Active Directory への再認証が必要です。MACの不一致によってユーザとIPのマッピングが削除された場合は、ADエージェントに通知されます。デフォルトでは、このオプションは有効になっています。 MAC の確認は、ASA に直接接続されたネットワーク上の IP アドレスからのパケットだけに対して行われます。VPN ユーザは確認されません。
Track User Not Found	「ユーザが見つからない」トラッキングをイネーブルにするかどうかを指定します。デフォルトでは、このオプションはディセーブルです。
NetBIOS ログアウト プローブ	
Enable (NetBIOS Logout Probe)	NetBIOS ログアウト プローブをイネーブルにするかどうかを指定します。 このプローブを使用すると、ユーザがネットワークからログアウトしたかどうかを事前に判断できます。これにより、アイドル タイムアウトがこの目的で使用される唯一のメカニズムである場合よりも、デバイスによるユーザから IP アドレスへのマッピングの削除が迅速にできるようになります。デフォルトでは、プローブはディセーブルになっていて、ユーザは Idle Timeout の値よりも長い期間アイドルになっている場合にのみ削除されます。 ユーザが検査されるのは、ユーザの状態がアクティブで、1つ以上の有効なルールで使用されている場合に限ります。VPN ユーザとカットスルー プロキシ ユーザは検査されません。NetBIOS ログアウト プローブによってユーザと IP のマッピングが削除された場合は、AD エージェントに通知されます。 以下のオプションの設定の詳細については、ID認証ファイアウォール ポリシーの要件 （811 ページ）を参照してください。
Probe Timer	ユーザがアイドルであるかどうかにかかわらず、有効なユーザに NetBIOS プローブを送信する頻度。デフォルトは 15 分で、指定できる範囲は 1 ～ 65535 分です。

要素	説明
再試行間隔（Retry Interval）	IP アドレスからの応答がない場合にプローブを再試行する頻度と、プローブを再試行する回数。デフォルトは 3 秒と再試行回数 3 回です。範囲は 1 ～ 65535 秒と、再試行回数 1 ～ 256 回です。 最後の再試行から応答がない場合に [NetBIOSプローブが失敗した場合にユーザIPを削除する（Remove User IP When NetBIOS Probe Fails）] オプションを選択すると、ユーザから IP アドレスへのマッピングが削除されます。このオプションを選択しないと、アドレスは次のインターバルで確認されます。
ユーザー名	NetBIOS 応答があった場合に、戻されたユーザ名に基づいて応答を処理する方法を指定します。 • [いずれかが一致（Match Any）]（デフォルト）：応答内の任意のユーザ名が、IP アドレスのデータベース内のユーザ名と一致します。応答に複数の名前があり（複数のユーザがワークステーションにログインしている）、応答内のユーザがデータベース内のユーザと一致する場合、プローブは成功したと見なされ、そのマッピングが保持されます。 • [ユーザ不要（User Not Needed）]：NetBIOS 応答内のユーザ名は無視されます。クエリの応答だけで、ユーザから IP アドレスへのマッピングを保持することができます。このオプションは、Messenger サービスがワークステーションでオンになっていない場合に有効です。この場合、NetBIOS の応答にはユーザ名は含まれません。このオプションは、複数のユーザーがワークステーションにログインする場合にも役立ちます。 • [完全一致（Exact Match）]：NetBIOS 応答内には 1 つのユーザ名のみが含まれ、ユーザから IP アドレスへのマッピングデータベース内のユーザ名と完全に一致する必要があります。ユーザが複数含まれていたり、ユーザ名が一致しなかったりすると、マッピングはデータベースから削除され、IP アドレスは非アクティブとしてマークされます。
Users	
アイドル タイムアウト	データベース内のユーザから IP アドレスへのマッピングを削除する前に、ユーザがアイドル状態でいられる期間を分単位で指定します。マッピングが削除されると、ユーザはマッピングを更新するためにログインし直す必要があります（Ctrl+Alt+Delete を使用してワークステーションをロックし、もう一度ログインするなど）。デフォルトは 60 分で、指定できる範囲は 1 ～ 65535 分です。 このオプションの選択を解除すると、アイドル タイムアウトの確認をディセーブルにすることができます。この場合、ユーザから IP へのマッピングはアイドル状態のため削除されません。 VPN ユーザとカットスルー プロキシ ユーザはこのタイマーの対象となりません。アイドル タイムアウトによってユーザと IP アドレスのマッピングが削除された場合は、AD エージェントに通知されません。

要素	説明
Active Directory Agent	
Hello タイマー（Hello Timer）	Hello パケットを AD エージェントに送信する頻度。ASA は hello パケットを使用して、ASA レプリケーション ステータスとドメイン ステータスを入手します。ASA が最後の再試行後に応答を受け取らなかった場合、AD エージェントはダウンしていると見なされ、ASA はバックアップの AD エージェントに切り替えられます（エージェントを設定している場合）。 デフォルトでは、hello パケットは 30 秒おきに送信され、応答がない場合は最大 5 回まで再試行が行われます。範囲は 10 ～ 65535 秒と、再試行回数 1 ～ 65535 回です。
Poll Groups Timer	ファイアウォール ルールに指定したユーザ メンバーシップのリストを入手するために Active Directory サーバがクエリーを送信する間隔を指定します。ASA は、グループを使用している場合に限り、グループ内のメンバーシップについてサーバに対してクエリーを実行します。AD サーバに定義されたすべてのグループに対するクエリーは実行しません。デフォルトは 8 時間で、指定できる範囲は 1 ～ 65535 時間です。 **ヒント** グループ メンバーシップが変更された場合、その変更は、このタイマーの期限が切れて、ASA が更新情報を AD サーバにポーリングするまでルール処理に反映されません。したがって、ASA でグループ メンバーシップを更新する必要性と、ポーリングの量を削減しようとする要求とのバランスをとりながら、ネットワーク内のグループ メンバーシップに対する変更頻度に基づいてタイマーを設定する必要があります。

要素	説明
Retrieve User Information	ASA がユーザと IP アドレスのマッピングを AD エージェントから取得する方法を指定します。 • [フルダウンロード（Full Download）]（ASA 5505 以外のデバイスのデフォルト）：ブート時に、ASA はユーザから IP アドレスへの完全マッピングデータベースを AD エージェントから取得し、ユーザがネットワークにログインおよびログアウトしたときに差分更新を入手します。 このオプションは、ネットワークにあるユーザが 1024 よりも少ない場合にのみ、5505 で使用されます。5505 ではユーザから IP へのマッピングの数が 1024 以内に制限されているためです。5505 では、デフォルトのオンデマンド設定は、ごく少数のユーザがデバイス経由でトラフィックを通過させる場合にのみ適用されます。 • [オンデマンド（On Demand）]（ASA 5505 デバイスのデフォルト）：ASA は、新しいパケットが接続を必要とし、マッピングが存在しない場合にのみ、ユーザから IP へのマッピングについて、AD エージェントに対してクエリを実行します。このオプションではメモリがあまり使用されませんが、マッピングの取得で遅延が生じる可能性があります。パケットは、当初従来型の送信元 IP アドレスと宛先 IP アドレス、およびサービス情報を基に評価され、誤ったアクションが生じる可能性があります。企業の環境か悪意のある攻撃により、大量のユーザが同時にログインした場合、遅延が増大する可能性があります。

アイデンティティ ユーザ グループ オブジェクトの作成

アイデンティティ ユーザ グループ オブジェクトを作成すると、個々のユーザ、ユーザ グループ、またはユーザとグループの組み合わせを識別できます。これらのユーザとグループは、Active Directory（AD）に定義されている必要があります。他のタイプのユーザは定義できません。

ヒント アイデンティティ ユーザ グループは ASA で定義されます。AD に定義済みのグループを複製するために、これらのグループを作成する必要はありません。AD グループはファイアウォール ルール内に直接指定できます。アイデンティティ ユーザ グループ オブジェクトは、それ以外では AD に存在しないユーザとユーザ グループの集合を定義するためのみに必要です。

事前に定義されているアイデンティティ ユーザ グループは 2 種類あります。これらのグループは、カットスルー プロキシの設定 （839 ページ）で説明されているカットスルー プロキシの設定で使用されます。

- all-auth-users：認証済みユーザと関連付けられているすべての IP アドレスと一致します。

- all-unauth-users：認証済みユーザーと関連付けられていない IP アドレスのみを照合します。

ヒント

- これらのオブジェクトの使用は、ASA 8.4(2+) のみでサポートされます。
- これらのオブジェクトを使用できるようにするには、ASA にアイデンティティ オプションのポリシーを設定する必要があります。
- このオブジェクトタイプを使用するポリシーまたはオブジェクトを定義するときに、アイデンティティ ユーザ グループを作成できます。詳細については、ポリシーでのアイデンティティ ユーザの選択 （835 ページ）を参照してください。

関連項目

- アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）
- ID 認証ファイアウォール ポリシーの要件 （811 ページ）
- [Identity Settings] ページ （693 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [アイデンティティユーザーグループ（Identity User Group）] を選択します。

ステップ 3 作業領域を右クリックして [新規オブジェクト（New Object）] を選択し、[アイデンティティユーザーグループの追加（Identity User Group）] ダイアログボックスを開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 [グループ内のメンバー（Members in Group）] リストにアイテムを追加したり、このリストからアイテムを削除したりして、オブジェクトに定義されているユーザーとユーザーグループを識別します。

リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なアイデンティティユーザーグループ（Available Identity User Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。
- [ユーザー/ユーザーグループの検索（Search User/User Group）] で、ID 設定の管理オプションでドメインに対して設定されている Active Directory サーバーからユーザーまたはユーザーグループを選択します。ユーザまたはユーザ グループを選択する前に設定を行っておく必要があります。この設定で Security Manager が使用する AD サーバを認識します。

ユーザまたはユーザ グループを検索するには、NetBIOS ドメインを選択し、ユーザまたはユーザ グループを検索しているかどうかを指定して、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。検索文字列が名前内の任意の場所（名前、ミドルネームのイニシャル、姓）、

ユーザ ID、CN、（ユーザ グループの場合）ユーザ グループ名に含まれている場合、名前は一致していると見なされます。

ユーザーまたはグループを追加するには、リストで選択し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。

- [カンマで区切られたアイデンティティユーザーまたはユーザーグループの入力（Type in comma separated identity user or user group）] に有効な名前を入力し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。複数の名前はカンマで区切ります。これらは、メンバー リストに別々の行として追加されます。

次の形式を使用して、名前を入力できます。

- 個別のユーザ：NETBIOS_DOMAIN\user
- ユーザ グループ（\ を二重にします）：NETBIOS_DOMAIN\\user_group

ドメイン名が含まれていない場合、Security Manager Administration の [Identity Settings] ページで選択したオプションに基づいてドメイン名が付加されます。名前の前に \ または \\ を付けると、[Identity Settings] ページで定義されたデフォルト ドメインが自動的に追加されます。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ポリシーでのアイデンティティ ユーザの選択

アイデンティティ ユーザの指定を許可するポリシーまたはポリシー オブジェクトで、[User] フィールドの横にある [Select] ボタンをクリックして、アイデンティティ ユーザ グループ オブジェクトを選択して情報入力するか、直接情報を入力できます。

[アイデンティティユーザーグループセレクタ（Identity User Group Selector）] ダイアログボックスで [グループ内のメンバー（Members in Group）] リストに入力することにより、[ユーザー（User）] フィールドの内容を定義できます。リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なアイデンティティユーザーグループ（Available Identity User Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。目的のオブジェクトが存在しない場合は、リストの下にある [追加（Add）]（+）ボタンをクリックして新しいオブジェクトを作成できます。オブジェクトを選択し [編集（Edit）]（鉛筆）ボタンをクリックして、オブジェクトを変更するか、内容を確認できます。

事前に定義されているアイデンティティ ユーザ グループは 2 種類あります。これらのグループは、カットスルー プロキシの設定 （839 ページ）で説明されているカットスルー プロキシの設定で使用されます。

- all-auth-users：認証済みユーザと関連付けられているすべての IP アドレスと一致します。
- all-unauth-users：認証済みユーザーと関連付けられていない IP アドレスのみを照合します。
- [ユーザー/ユーザーグループの検索（Search User/User Group）] で、ID 設定の管理オプションでドメインに対して設定されている Active Directory サーバーからユーザーまたはユーザーグループを選択します。ユーザまたはユーザ グループを選択する前に設定を行っておく必要があります。この設定で Security Manager が使用する AD サーバを認識します。

ユーザまたはユーザ グループを検索するには、NetBIOS ドメインを選択し、ユーザまたはユーザ グループを検索しているかどうかを指定して、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。検索文字列が名前内の任意の場所（名前、ミドルネームのイニシャル、姓）、ユーザ ID、CN、（ユーザ グループの場合）ユーザ グループ名に含まれている場合、名前は一致していると見なされます。

ユーザーまたはグループを追加するには、リストで選択し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。

- [カンマで区切られたアイデンティティユーザーまたはユーザーグループの入力（Type in comma separated identity user or user group）] に有効な名前を入力し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。複数の名前はカンマで区切ります。これらは、メンバー リストに別々の行として追加されます。

次の形式を使用して、名前を入力できます。

- 個別のユーザ：NETBIOS_DOMAIN\user
- ユーザ グループ（\ を二重にします）：NETBIOS_DOMAIN\\user_group

ドメイン名が含まれていない場合、[Identity Settings] ページ （693 ページ）で説明しているように、[Security Manager Administration] の [Identity Settings] ページで選択したオプションに基づいてドメイン名が付加されます。名前の前に \ または \\ を付けると、[Identity Settings] ページで定義されたデフォルト ドメインが自動的に追加されます。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

アイデンティティ ベースのファイアウォール ルールの設定

アイデンティティ認識は、ファイアウォール サービスを提供するために使用される ACL 内のアクセス コントロール エントリまたはルールと統合されます。この機能は ACL と統合されるため、アイデンティティ ベースのルールをファイアウォール ポリシーに追加する方法は、すべてのタイプのファイアウォール ポリシーで同じになります。この項では、アイデンティティ

ベースのルールを既存のポリシーに取り込む一般的な方法を説明し、アイデンティティ ベースのルールを許可するポリシーごとの設定について、詳細な情報を提供します。

アイデンティティ ベースのルールを追加する際のガイドライン

アイデンティティ ベースのルールを追加する際の一般的なガイドラインと推奨事項は以下のとおりです。

- FQDN（完全修飾ドメイン名）のネットワーク/ホスト オブジェクトは、送信元フィールドと宛先フィールドの両方に使用できます。これらのオブジェクトの設定の詳細については、ネットワーク/ホスト オブジェクトの作成 （394 ページ）を参照してください。
- Active Directory（AD）ユーザ名またはユーザ グループ名を指定するユーザ、ユーザ グループ、アイデンティティ ユーザ グループ オブジェクトは、別個のフィールド [User] で定義されます。1 つ以上のユーザー名、ユーザーグループ名、またはアイデンティティ ユーザー グループ オブジェクトを使用してルールを設定した場合、指定により送信元アドレスの設定のみが変更されます。宛先フィールドに指定されたアドレスには適用されません。これらのアイデンティティ ユーザ グループ オブジェクトの設定の詳細については、アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）を参照してください。

ルールを主に、指定したユーザまたはユーザ グループに基づいて動作するようにする場合でも、送信元アドレスはルール内に設定する必要があります。送信元指定とユーザ指定は、その組み合わせでルールの有効範囲をコントロールします。送信元フィールドの値に基づいて、ルールは次のように動作します。

- **Source = any**：ルールをユーザー指定にのみ基づいて適用する場合、送信元として「any」を使用します。これらのルールは、ユーザがトラフィックを送信するワークステーションの IP アドレスに関係なくユーザ指定と一致します。
- **Source = その他**：送信元アドレスとして「any」以外を指定した場合は、ユーザーが送信元アドレス指定と一致する IP アドレスからトラフィックを送信した場合にのみ、ルールが適用されます。送信元のネットワークに基づいてさまざまなサービスを提供する場合は、この方法を使用します。

たとえば、内部に信頼されたネットワークがある場合、特定のユーザ グループ内のユーザには、そこから機密性の高い宛先へのアクセスを許可しても、そのユーザが信頼されるネットワークの外部にいる場合はアクセスを拒否することができます。この場合は、信頼されたネットワークを送信元、信頼されたユーザ グループをユーザ、機密性の高いサーバを宛先として指定した許可ルールを作成します。また、送信元と宛先だけを指定した特定の拒否ルールを作成したり、デフォルトのすべて拒否ルールによって、一致しないトラフィックをキャプチャすることもできます。

- ユーザ アイデンティティの影響をまったく受けないトラフィック クラスがあるかどうか確認します。たとえば、DNS トラフィックはすべてのユーザに許可されます。こうしたタイプのルールをアイデンティティ ベースのルールよりも上位に配置すると、デバイスがアイデンティティ ベースのルールの評価を必要とする前にトラフィックの照合を迅速に許可することができます。

- ルールのトラブルシューティング時は、最終的に IP アドレスに基づいてルールが適用されることに注意してください。FQDN ルールの照合は DNS 検索に基づいて行われます。ホストの IP アドレスは、正常に終了した検索と、検索が次に更新されるときとで変化することがあります。ユーザについては、IP アドレスのマッピングはネットワークに設定された AD エージェントから取得されるか、ASA 自身によって行われる認証によって取得されます。
- FQDN 指定とユーザ指定は完全に独立したものです。それぞれを個別に使用できます。

アイデンティティ ベースのルールを許可するファイアウォール ポリシー

アイデンティティベースのルールは ASA 8.4.2 以降だけで可能です。以下のポリシーにより、アイデンティティ ベースのルールを設定できます。

- AAA ルール：[ファイアウォール（Firewall）] > [AAA ルール（AAA Rules）] を選択します。ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）を参照してください。

ヒント AAA ルールは、カットスルー プロキシの設定に使用できます。このプロキシにより、IP アドレスのマッピングが無効になり、ネットワーク アクセスが拒否されたユーザが、マッピングの問題を解決するために ASA に直接認証処理を行うことができるようになります。カットスルー プロキシの設定 （839 ページ）を参照してください。

- アクセスルール：[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] を選択します。アクセス ルールの設定 （920 ページ）を参照してください。
- インスペクションルール：[ファイアウォール（Firewall）] > [インスペクションルール（Inspection Rules）] を選択します。インスペクション ルールの設定 （983 ページ）を参照してください。
- 拡張 ACL ポリシー オブジェクトを使用するポリシー：複数のファイアウォール ポリシーが拡張 ACL ポリシー オブジェクトを使用して、ルール テーブルを直接ポリシーに取り込む代わりにトラフィック照合基準を定義できます。FQDN オブジェクトまたはユーザ指定を組み込むために拡張 ACL ポリシー オブジェクトを設定できます（拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）を参照）。これらのアイデンティティ ベースの拡張 ACL オブジェクトは、次のポリシーで使用できます。
  - ボットネット トラフィック フィルタ ルール：[ファイアウォール（Firewall）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）] を選択します。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170 ページ）を参照してください。アイデンティティ ベースの ACL は、イネーブル ルールおよびドロップ ルールのトラフィック分類として使用できます。
  - IPS ルール、QoS ルール、および接続ルール（サービスポリシールール）：[プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、

QoS、および接続ルール（IPS, QoS, and Connection Rules）] を選択します。[サービス ポリシールール（Service Policy Rules）] ページ （2946 ページ）を参照してください。

このポリシーのトラフィック照合基準は、トラフィック フロー ポリシー オブジェクトに組み込まれる拡張 ACL ポリシー オブジェクトに基づいて行われます。アイデンティティ ベースのトラフィック分類を組み込むトラフィック フロー オブジェクトに、ACL を指定するオプションをいずれか選択する必要があります。アイデンティティ ベースの ACL はすべてのサービス タイプに使用できます。詳細については、トラフィック フロー オブジェクトの設定 （2965 ページ）を参照してください。

このポリシーで使用できるサービスの 1 つであるユーザ統計は、アイデンティティ ベースのファイアウォール ユーザのアカウンティング情報の収集用に特別に設計されたものです。ユーザ統計の収集 （842 ページ）を参照してください。

- リモート アクセス グループ ポリシーでの VPN フィルタ：VPN フィルタ ACL が VPN トラフィックに適用されます。VPN フィルタは、リモート アクセス接続ポリシーで使用する ASA グループ ポリシー オブジェクトの [Connection Settings] ページに設定できます。ASA グループ ポリシーの接続設定 （1967 ページ）およびアイデンティティ ベースのルールを使用した VPN トラフィックのフィルタリング （843 ページ）を参照してください。

アイデンティティ ベースのルールまたはオブジェクトを許可しないポリシー

ポリシーには、ネットワーク/ホスト オブジェクトまたは拡張 ACL オブジェクトを指定できるタイプがありますが、このタイプのオブジェクトやアイデンティティ ユーザ グループ オブジェクトを使用する FQDN ネットワーク/ホスト オブジェクトまたは ACL を許可しないポリシーもあります。こうしたタイプのオブジェクトを使用できない例を、いくつか次に示します。

- ルート マップを含むルーティング ポリシー。
- Network Address Translation（NAT; ネットワーク アドレス変換）。
- WCCP（Web キャッシュ コントロール プロトコル）。
- VPN 設定のクリプト マップ。
- リモート アクセス VPN 設定のダイナミック アクセス ポリシー。

カットスルー プロキシの設定

ID 認証ファイアウォール ポリシーを使用する場合、ユーザから IP アドレスへのマッピングは、さまざまな機能、主にネットワーク内の AD エージェントから取得されます。マッピングは定期的に更新されますが、ユーザから IP アドレスへのマッピングが同期されていないために、ファイアウォール ルールによって正規のユーザがブロックされる場合があります。

この状態に備えるためカットスルー プロキシを設定できます。カットスルー プロキシを使用すると、ユーザがブロックされても ASA に直接サインオンできます。ASA は、ユーザの現在の IP アドレスを正しく反映するようにユーザから IP へのマッピングを更新します。HTTP パ

ケット/HTTPS パケットを受信して認証するインターフェイスを含むすべてのコンテキストに新しいマッピングが転送されます。

AAA ルールはカットスルー プロキシの設定に使用できます。設定の選択項目は、1 つ以上の NetBIOS ドメインがネットワーク内にあるかどうかに基づき、2 種類が用意されています。

- 単一ドメイン：認証用に通常の AAA ルールを設定し、このドメインに対して Active Directory サーバを識別する LDAP サーバ グループを指定します。送信元には「any」を使用し、宛先には ASA の IP アドレスを使用します。サービスには HTTP と HTTPS を含めることができます。次に、サーバーへの認証を必要とする場合、ユーザーは次の標準認証 URL のいずれかを入力します。interface_ip はインターフェイスの IP アドレスで、対話型認証テーブルでプロトコルにデフォルト以外のポートを指定した場合、port はポート番号（任意）です。**http://***interface_ip* [**:***port*]**/netaccess/connstatus.html** or **https://***interface_ip* [**:***port*]**/netaccess/connstatus.html**。

ヒント　ユーザから IP へのマッピングは、選択した AD サーバ グループに設定されたドメインと同じドメインの下に置かれます。別の方法を認証に使用した場合、マッピングは LOCAL ドメインの下に置かれます。

- 複数ドメイン：特定の AAA サーバ グループではなくユーザ ID オプションを使用する 2 種類の認証ルールを設定します。次の手順で、このステップについて説明します。この設定は単一ドメイン ネットワークでも機能します。単一ドメインの場合と同じ URL を使用して ASA への認証を行います。

ユーザ ID オプションを使用する場合、認証は次のように処理されます。

- ユーザがログイン クレデンシャルに DOMAIN\username 形式でドメインを組み込んでいると、ASA はそのドメインを使用して、アイデンティティ オプションのポリシー内のドメイン マッピングに基づいてどの AD サーバを認証に使用するか決定します。AAA サーバがドメインにマップされていない場合、認証の試行は拒否されます。
- ログイン クレデンシャルに識別可能なドメイン名が含まれていない場合（\ 文字がユーザ名ストリングに含まれていない場合）、ASA はアイデンティティ オプションのポリシーで選択されたデフォルトのドメインに割り当てられている AD サーバを使用します。AAA サーバがデフォルトのドメインにマップされていない場合、認証の試行は拒否されます。

ヒント　カットスルー プロキシは IPv4 アドレスでのみ機能します。IPv6 はサポートされていません。

関連項目

- ID 認証ファイアウォール ポリシーの要件　（811 ページ）
- ID 認証サービスを提供するためのファイアウォールの設定　（816 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定　（873 ページ）

- ユーザの認証方法について （871 ページ）

ステップ 1 Active Directory サーバおよびエージェントの識別 （818 ページ）の説明のとおり、すべての NetBIOS ドメインと、そのネットワーク用の AD サーバ グループ、および AD エージェント グループを指定するようにアイデンティティ オプション ポリシーを設定します。

ステップ 2 次のいずれかを実行して、 [AAA Rules] ページ （880 ページ）を開きます。

- （デバイスビュー）：ポリシーセレクタから **[ファイアウォール（Firewall）] > [AAAルール（AAA Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）]>[AAAルール（AAA Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 3 [行の追加（Add Row）] ボタンを使用して次のルールを作成します。[Add AAA Rules] ダイアログボックスの詳細については、 [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）を参照してください。

ヒント 次のルールに示すものよりも詳細な送信元指定、宛先指定、サービス指定を使用できます。

ルール 1：認証済みユーザに再認証を強制しない。

- [認証アクション（Authentication Action）] オプションおよび [ユーザーID（User-Identity）] オプションを選択します。
- Action = Deny。AAA 認証ルールの場合、「deny」ではユーザーは認証を要求されませんが、ユーザーのトラフィックがドロップされるわけではありません。
- Sources = any。
- Users = all-auth-users。

ユーザーの場合、**all-auth-users** は、Active Directory で認証済みで、IP マッピングが存在するユーザーを意味します。

- Destination = any。
- Services = IP。
- AAA Server Group =（選択なし）。
- Interface =（選択、通常はインターフェイス内）。

ルール 2：まだ認証されていないユーザを認証する。

- [認証アクション（Authentication Action）] オプションおよび [ユーザーID（User-Identity）] オプションを選択します。
- Action = Permit。このアクションには認証と照合を行うユーザが必要です。
- User = all-unauth-users。

この場合、**all-unauth-users** は Active Directory で認証されていないすべてのユーザーを意味します。

- その他のオプションは最初のルールと同じです。

ユーザ統計の収集

アイデンティティ ベースのファイアウォール ポリシーに関するユーザ統計のアカウンティング情報を収集できます。これらの統計情報は、ユーザ名またはユーザ グループ メンバーシップに基づいてファイアウォール ポリシーが適用されるユーザに対して保持されます。

関連項目

- ID 認証ファイアウォール ポリシーの要件 （811 ページ）
- ID 認証サービスを提供するためのファイアウォールの設定 （816 ページ）
- [サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）
- トラフィック フロー オブジェクトの設定 （2965 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを追加する行を選択して、テーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックし、Insert Service Policy Rule ウィザードを開始します。

ステップ 3 ウィザードのステップ 1 で、ルールをグローバルにするか、特定のインターフェイスまたはインターフェイス ロールに適用するかを選択します。ユーザのトラフィックがどのインターフェイスを通過するかに関係なく、ユーザの統計を収集する場合は [Global] を選択します。

[次へ（Next）] をクリックします。

ステップ 4 ステップ 2 で、統計情報の収集対象となるトラフィックを定義するトラフィック クラスを選択します。すべてのトラフィックで統計情報を収集する場合は、class-default を選択します。対象がすべてのトラフィックではない場合は、[Traffic Class] を使用してトラフィック照合属性を定義するトラフィック フロー オブジェクトを選択します。

[次へ（Next）] をクリックします。

ステップ 5 ステップ 3 で、[ユーザー統計（User Statistics）] タブを選択します。

- [ユーザー統計アカウンティングの有効化（Enable user statistics accounting）] を選択します。
- 収集する情報のタイプを選択します。
  - **Account for sent drop count**
  - **Account for sent packet, sent drop and received packet count**

ステップ 6 [終了（Finish）] をクリックしてルールを保存します。

アイデンティティベースのルールを使用したVPNトラフィックのフィルタリング

ASA 上のリモート アクセス VPN をサポートしている場合、ユーザ依存のアクセスを設定します。アイデンティティ ベースのルールは、リモート ユーザ アクセスの検証後、トラフィックをフィルタリングするために使用することもできます。

VPN 用のアイデンティティ ベースのルールを作成する前に、VPN ユーザ名のルールについて理解し、このルールが正しいドメイン名を使用していることを確認する必要があります。

- 認可に Active Directory LDAP サーバ グループを使用していて、ドメイン グループ/サーバ グループをアイデンティティ オプションのポリシーに設定した場合、ユーザ名はNetBIOS ドメインに関連付けられます。
- 他の許可メカニズムの場合、VPN ユーザのドメイン名は LOCAL になります。

これらのことを考慮して、アイデンティティ ベースの ACL ルールで VPN 上のトラフィックをフィルタリングするために使用できる方法は次の 2 種類です。

- ASA グループ ポリシー オブジェクトに VPN フィルタを適用します。このフィルタはグループ内のすべてのユーザに適用されます。VPN フィルタは、リモート アクセス接続ポリシーで使用する ASA グループ ポリシー オブジェクトの [Connection Settings] ページに設定できます。 ASA グループ ポリシーの接続設定 （1967 ページ）を参照してください。
- デフォルトでは、VPN トラフィックがインターフェイス アクセス ルールをバイパスします。この動作は、すべての VPN トラフィックがインターフェイス アクセス ルールも経由するように変更できます。この方法を採用した場合、インターフェイス ルールは VPN トラフィックに依存することに注意してください。VPN トラフィックがインターフェイス アクセス ルールを経由するようにするには、RA VPNグローバル設定ポリシーの [ISAKMP/IPsec] タブで [Sysopt上でのIPsecの有効化（Enable IPsec over Sysopt）] オプションの選択を解除してください。 VPN グローバル ISAKMP/IPsec 設定 （1520 ページ） を参照してください。

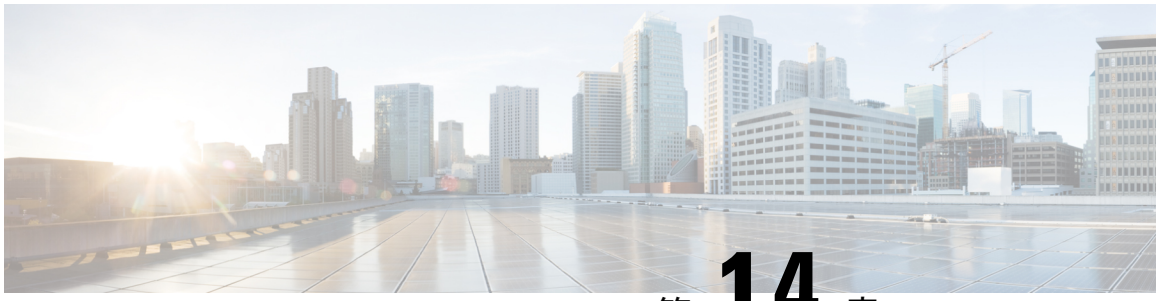
アイデンティティ ファイアウォール ポリシーの監視

Event Viewer を使用して、他のタイプのポリシーやイベントと同じ方法で ID 認証ファイアウォール ポリシーを監視できます。次に、アイデンティティ ポリシーを効率的に監視するためのヒントをいくつか示します。Event Viewer 使用の一般情報については、イベントの表示（3473 ページ）を参照してください。

- アイデンティティ ファイアウォールに特に関連した syslog メッセージのグループは 746001 ～ 746019 です。これらのメッセージの説明については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html で、ご使用の ASA ソフトウェアバージョンの Syslog メッセージ [英語] を参照してください。

特に重要なのは、次のメッセージです。

- **746004 と 746011**：これらの syslog は、ユーザーグループまたはユーザーへの参照数がサポートされる数を超えたことを示します。ポリシーの変更を検討する必要があります。これらの制約事項の詳細については、ID 認証ファイアウォール ポリシーの要件 （811 ページ）を参照してください。
- **746003**：IP アドレスへのユーザーグループまたはユーザーマッピングのダウンロードに失敗しました。メッセージには、失敗の理由についての説明があります。
- **746005**：AD エージェントに到達できませんでした。このエージェントが正しく機能し、ASA とエージェントの間にネットワーク パスが存在することを確認してください。
- **746010**：メッセージに示された理由によって、インポートしたユーザーまたはユーザーグループへの更新が失敗しました。
- **746016**：メッセージに示された理由によって、完全修飾ドメイン名（FQDN）への DNS 探索が失敗しました。
- 複数の既存の syslog メッセージにユーザ名または FQDN 情報が含まれるようになりました。Event Viewer には [Destination User Identity] 情報と [FQDN and Source User Identity] 情報を表示する 2 つのカラムがあります。更新されたメッセージは次のとおりです。
  - 302005、302006、302013、302014、302016 ～ 302018、302020、302021。
  - 305005、305006、305009 ～ 305013。
  - 304001 ～ 304002 には ID 情報が含まれていますが解析されません。
- [Event Type] にフィルタを作成し、[Identity Firewall Events] フォルダを選択することで、すべてのアイデンティティ関連の syslog メッセージをフィルタリングできます。
- Event Viewer からの Security Manager ポリシーの検索 （3541 ページ）の説明のとおり、イベントで Go to Policy コマンドを使用する場合は、ID 情報が検索基準に含まれます。ID 情報は、106100 には含まれていないことに注意してください。そのためこのメッセージのポリシー検索は、ユーザ ID の影響を受けません。



第 14 章

Trustsec ファイアウォールポリシーの管理

Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤とするアクセス コントロール ソリューションです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec ソリューションでは、実行デバイスはユーザー属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。

Cisco ASA に Cisco TrustSec が統合され、セキュリティグループに基づいてポリシーが適用されます。Cisco TrustSec ドメイン内のアクセス ポリシーは、トポロジには依存しません。ネットワーク IP アドレスではなく、送信元および宛先のデバイスのロールに基づいています。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

セキュリティグループ認識は複数の既存のファイアウォールルールに組み込まれます。固有の TrustSec ファイアウォールポリシーはありません。この章では、TrustSec ファイアウォールポリシーと、セキュリティグループ認識をサポートするさまざまなポリシーに TrustSec ファイアウォールポリシーを実装する方法について説明します。

この章は次のトピックで構成されています。

- TrustSec ファイアウォールポリシーの概要　（845 ページ）
- TrustSec ファイアウォールポリシーの構成　（853 ページ）
- TrustSec ファイアウォールポリシーのモニタリング　（867 ページ）

TrustSec ファイアウォールポリシーの概要

従来、ファイアウォールなどのセキュリティ機能は、事前定義されている IP アドレス、サブネット、およびプロトコルに基づいてアクセスコントロールを実行していました。しかし、企業のボーダレス ネットワークへの移行に伴い、ユーザーと組織の接続に使用されるテクノロジーおよびデータとネットワークを保護するためのセキュリティ要件が大幅に向上していま

す。エンド ポイントは、ますます遊動的となり、ユーザは通常さまざまなエンド ポイント（ラップトップとデスクトップ、スマートフォン、タブレットなど）を使用します。つまり、ユーザ属性とエンドポイント属性の組み合わせにより、ファイアウォール機能または専用ファイアウォールを持つスイッチやルータなどの実行デバイスがアクセス コントロール判断のために信頼して使用できる既存の 6 タプル ベースのルール以外の主要な特性が提供されます。

その結果、お客様のネットワークで、ネットワークのアクセスレイヤ、分散レイヤ、コアレイヤおよびデータセンターなどのセキュリティソリューションを有効にするために、エンドポイント属性またはクライアント アイデンティティ属性の可用性と伝達がますます重要な要件となっています。

Cisco TrustSec は、既存の ID 認証インフラストラクチャを基盤とするアクセス コントロール ソリューションです。ネットワーク デバイス間のデータ機密性保持を目的としており、セキュリティ アクセス サービスを 1 つのプラットフォーム上で統合します。Cisco TrustSec ソリューションでは、実行デバイスはユーザー属性とエンドポイント属性の組み合わせを使用して、ロールベースおよびアイデンティティベースのアクセス コントロールを決定します。

ご使用の環境に Cisco TrustSec を実装する利点は、次のとおりです。

- デバイスからの適切でより安全なアクセスにより、拡大する複雑なモバイル ワークフォースを提供します。
- 有線または無線ネットワークへの接続元を包括的に確認できるため、セキュリティ リスクが低減されます。
- 物理またはクラウドベースの IT リソースにアクセスするネットワーク ユーザーのアクティビティに対する非常に優れた制御が実現されます。
- 中央集中化、非常にセキュアなアクセス ポリシー管理、およびスケーラブルな実行メカニズムにより、総所有コストが削減されます。

Cisco TrustSec の詳細については、http://www.cisco.com/go/trustsecを参照してください。

ここでは、次の内容について説明します。

- Cisco TrustSec の SGT および SXP サポートについて （846 ページ）
- Cisco TrustSec ソリューションのロール （847 ページ）
- セキュリティ グループ ポリシーの適用 （848 ページ）
- 送信者および受信者のロールについて （851 ページ）
- ASA と Cisco TrustSec を統合するための前提条件 （852 ページ）

Cisco TrustSec の SGT および SXP サポートについて

Cisco TrustSec ソリューションでは、セキュリティ グループ アクセスは、トポロジ認識ネットワークをロールベースのネットワークに変換するため、ロールベース アクセス コントロール（RBAC）に基づいて実施されるエンドツーエンドポリシーがイネーブルになります。認証時に取得されたデバイスおよびユーザー クレデンシャルは、パケットをセキュリティ グループ

ごとに分類するために使用されます。Cisco TrustSec クラウドに着信するすべてのパケットは、セキュリティ グループ タグ（SGT）でタグ付けされます。タギングは、信頼できる中継がパケットの送信元のアイデンティティを識別し、データ パスでセキュリティ ポリシーを適用するのに役立ちます。

SGT は、SGT を使用してセキュリティ グループ ACL を定義する場合に、ドメイン全体の特権レベルを示すことができます。SGT は、RADIUS ベンダー固有属性で発生する IEEE 802.1X 認証、Web 認証、または MAC 認証バイパス（MAB）を使用してデバイスに割り当てられます。SGT は、特定の IP アドレスまたはスイッチ インターフェイスにスタティックに割り当てることができます。SGT は、認証の成功後にスイッチまたはアクセス ポイントにダイナミックに渡されます。

セキュリティ グループ交換プロトコル（SXP）は、SGT およびセキュリティ グループ ACL をサポートしているハードウェアに対する SGT 対応ハードウェア サポートがないネットワーク デバイスに IP-to-SGT マッピング データベースを伝搬できるよう Cisco TrustSec 向けに開発されたプロトコルです。コントロール プレーン プロトコルの SXP は、IP-SGT マッピングを認証ポイント（レガシー アクセス レイヤ スイッチなど）からネットワークのアップストリーム デバイスに渡します。

SXP 接続はポイントツーポイントであり、基礎となる転送プロトコルとして TCP を使用します。SXP は接続を開始するために既知の TCP ポート番号 64999 を使用します。また、SXP 接続は、送信元および宛先 IP アドレスによって一意に識別されます。

Cisco TrustSec ソリューションのロール

アイデンティティおよびポリシーベースのアクセス実施を提供するために、Cisco TrustSec ソリューションには、次の機能があります。

- **アクセス要求側（AR）**：アクセス要求側は、ネットワークの保護されたリソースへのアクセスを要求するエンドポイントのデバイスです。これらのデバイスはアーキテクチャのプライマリ対象であり、そのアクセス権限はアイデンティティ クレデンシャルによって異なります。

アクセス要求側には、PC、ラップトップ、携帯電話、プリンタ、カメラ、MACsec 対応 IP フォンなどのエンドポイント デバイスが含まれます。

- **ポリシーデシジョンポイント（PDP）**：ポリシーデシジョンポイントはアクセス制御を判断します。PDP は 802.1x、MAB、Web 認証などの機能を提供します。PDP は VLAN、DACL および Security Group Access（SGACL/SXP/SGT）による許可および適用をサポートします。

Cisco TrustSec ソリューションでは、Cisco Identity Services Engine（ISE）が PDP として機能します。Cisco ISE はアイデンティティおよびアクセス コントロール ポリシーの機能を提供します。

- **ポリシー情報ポイント（PIP）**：ポリシー情報ポイントは、ポリシーデシジョンポイントに外部情報（たとえば、評価、場所、および LDAP 属性）を提供する送信元です。

ポリシー情報ポイントには、Session Directory、IPS センサー、Communication Manager などのデバイスが含まれます。

- **ポリシー管理ポイント（PAP）**：ポリシー管理ポイントはポリシーを定義し、許可システムに挿入します。PAP は、ユーザ アイデンティティ マッピングおよびサーバ リソース マッピングに Cisco TrustSec タグを提供することによって、アイデンティティ リポジトリとして機能します。

Cisco TrustSec ソリューションでは、Cisco Secure Access Control System（802.1x および SGT サポートと統合されたポリシー サーバ）が PAP として機能します。

- **ポリシー エンフォースメント ポイント（PEP）**：ポリシー エンフォースメント ポイントは、各 AR の PDP による決定（ポリシールールおよびアクション）を実行するエンティティです。PEPデバイスは、ネットワーク全体に存在するプライマリ通信パスを介してアイデンティティ情報を学習します。PEPデバイスは、エンドポイントエージェント、許可サーバ、ピア実行デバイス、ネットワーク フローなど、さまざまな送信元から各 ARのアイデンティティ属性を学習します。同様に、PEPデバイスはSXPを使用して、ネットワーク全体で相互信頼できるピア デバイスに IP-SGT マッピングを伝搬します。

ポリシーエンフォースメントポイントには、Catalyst Switches、ルータ、ファイアウォール（具体的にはASA）、サーバー、VPNデバイス、SANデバイスなどのネットワーク デバイスが含まれます。

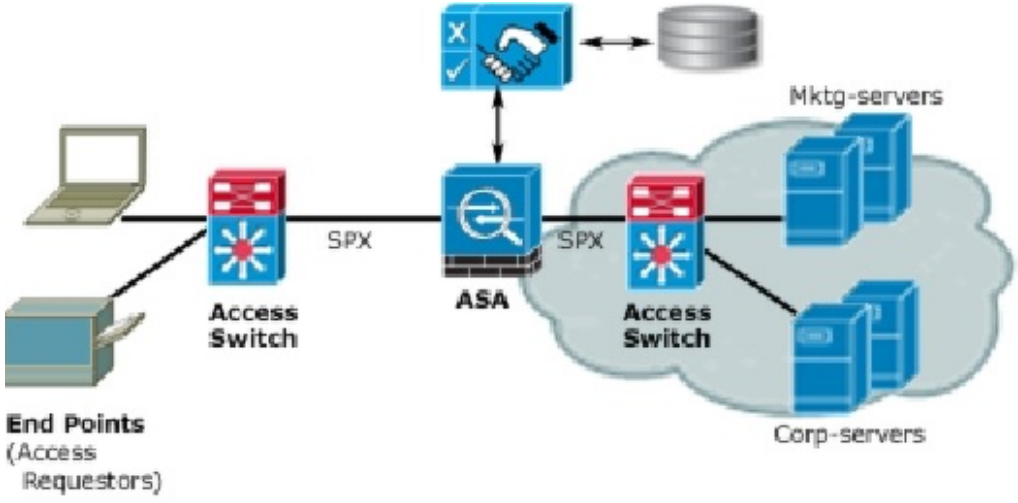
セキュリティ グループ ポリシーの適用

セキュリティ ポリシーの適用はセキュリティ グループの名前に基づきます。ファイアウォールで設定された従来の IP ベースのポリシーと比較して、アイデンティティベースのポリシーは、ユーザーおよびデバイス アイデンティティに基づいて設定されます。たとえば、mktg-contractor が mktg-server にアクセスできるとします。mktg-corp-user は、mktg-server および corp-server にアクセスできます。

このタイプの導入の利点を次に示します。

- ユーザーグループとリソースが 1 つのオブジェクト（SGT）を使用して定義されます（簡易ポリシー管理）。
- ユーザ アイデンティティとリソース アイデンティティは、Cisco Trustsec 対応スイッチ インフラストラクチャ全体で保持されます。

図 *21* : セキュリティ グループ名に基づくポリシー適用の導入



Cisco TrustSec を実装すると、サーバーのセグメンテーションをサポートするセキュリティ ポリシーを設定できます。また、Cisco TrustSec の実装には次のような特徴があります。

- 簡易ポリシー管理用に、サーバーのプールに SGT を割り当てることができます。
- SGT 情報は、Cisco Trustsec 対応スイッチのインフラストラクチャ内に保持されます。
- ASA は、Cisco TrustSec ドメイン全体にポリシーを適用するために IP-SGT マッピングを利用できます。
- サーバーの 802.1x 許可が必須であるため、導入を簡略化できます。

ASA によるセキュリティ グループベースのポリシーの適用

（注） ユーザーベースのセキュリティ ポリシーおよびセキュリティ グループベースのポリシーは、ASA で共存できます。セキュリティ ポリシーでは、ネットワーク属性、ユーザーベースの属性、およびセキュリティ グループベースの属性の任意の組み合わせを設定できます。

Cisco TrustSec と連携するように ASA を設定するには、ISE から Protected Access Credential（PAC）ファイルをインポートする必要があります。

PAC ファイルを ASA にインポートすると、ISE との安全な通信チャネルが確立されます。チャネルが確立されると、ASA は、ISE を使用して PAC セキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします（具体的には、セキュリティ グループ テーブル）。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。

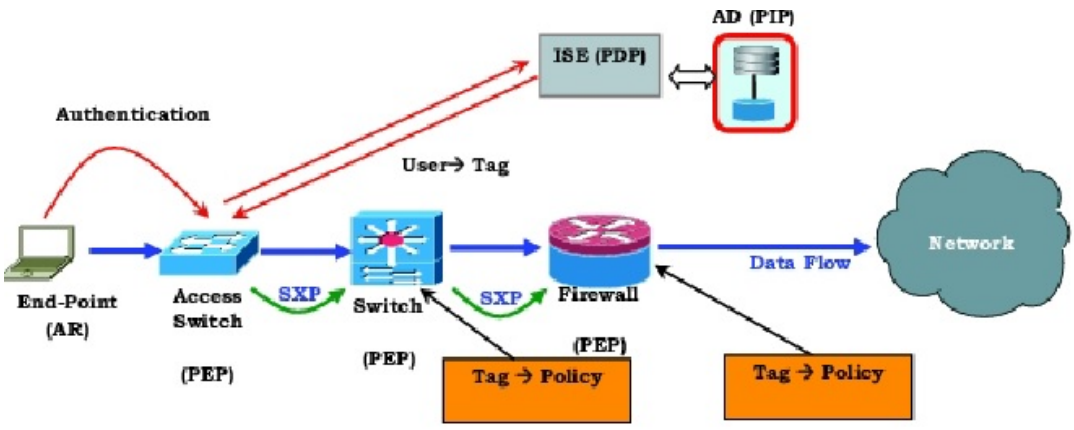
（注） バージョン 4.23 以降、Cisco Security Manager は、ACL および AAA ポリシーでの ISE サーバーからの 20 を超えるセキュリティグループタグ（SGT）の取得をサポートしています。[SGT] フィールドおよび[ユーザー（User）] フィールドの検索テキストボックスで下線を使用することにより、下線が含まれているユーザー名を検索する手間を減らすこともできます。

（注） Cisco Identity Services Engine の詳細については、http://www.cisco.com/en/US/products/ps11640/index.html を参照してください。

ASA は、最初にセキュリティ グループ テーブルをダウンロードするときに、テーブル内のすべてのエントリを順を追って調べ、そこで設定されているセキュリティ ポリシーに含まれるすべてのセキュリティ グループの名前を解決します。次に、ASA は、それらのセキュリティ ポリシーをローカルでアクティブ化します。ASA がセキュリティ グループの名前を解決できない場合、不明なセキュリティ グループ名に対して syslog メッセージを生成します。

次の図に、セキュリティ ポリシーが Cisco TrustSec で適用される仕組みを示します。

図 *22*：セキュリティ ポリシーの適用



1. エンドポイント デバイスは、アクセス レイヤ デバイスに直接アクセスするか、またはリモート アクセスを介してアクセスし、Cisco TrustSec で認証します。
2. アクセス レイヤ デバイスは 802.1X や Web 認証などの認証方式を使用して ISE のエンドポイント デバイスを認証します。エンドポイント デバイスは、ロールおよびグループ メンバーシップを渡して、デバイスを適切なセキュリティ グループに分類します。
3. アクセス レイヤ デバイスは SXP を使用して、アップストリーム デバイスに IP-SGT マッピングを伝搬します。
4. ASA はパケットを受信すると、SXP から渡された IP-SGT マッピングを使用して、送信元および宛先 IP アドレスの SGT を調べます。

マッピングが新規の場合、ASA はそのマッピングをローカル IP-SGT マネージャ データベースに記録します。コントロール プレーンで実行される IP-SGT マネージャ データベースは、各 IPv4 または IPv6 アドレスの IP-SGT マッピングを追跡します。データベースでは、マッピングが学習された送信元が記録されます。SXP 接続のピア IP アドレスがマッピングの送信元として使用されます。各 IP-SGT マッピングには、送信元が複数存在する可能性があります。

ASA が送信者として設定されている場合、ADSA は SXP ピアに IP-SGT マッピングを送信します。 送信者および受信者のロールについて （851 ページ）を参照してください。

- ASA で SGT またはセキュリティ グループの名前を使用してセキュリティ ポリシーが設定されている場合、ASA はそのポリシーを適用します。（ASA では、SGT またはセキュリティ グループの名前を含むセキュリティ ポリシーを作成できます。セキュリティ グループの名前に基づいてポリシーを適用するには、ASA はセキュリティ グループ テーブルで SGT にセキュリティ グループの名前をマッピングする必要があります）。

ASA がセキュリティ グループ テーブルでセキュリティグループの名前を見つけることができず、その名前がセキュリティポリシーに含まれている場合、ASAは、セキュリティグループの名前を不明と見なし、syslog メッセージを生成します。ISE からのセキュリティ グループ テーブルの更新とセキュリティ グループの名前の学習後、ASA はセキュリティ グループの名前がわかっていることを示す syslog メッセージを生成します。

送信者および受信者のロールについて

セキュリティグループ交換プロトコル（SXP）では、他のネットワークデバイスとの間でIP-SGTマッピングを送受信するために使用されます。SXP を使用すると、セキュリティ デバイスとファイアウォールが、ハードウェアをアップグレードまたは変更する必要なく、アクセス スイッチからのアイデンティティ情報を学習できます。また、SXPを使用して、アップストリーム デバイス（データセンター デバイスなど）からの IP-SGT マッピングをダウンストリーム デバイスに渡すこともできます。

SXP ピアへの SXP 接続を設定する場合は、その接続について、アイデンティティ情報を交換できるように、デバイスを送信者または受信者として指定する必要があります。

- 送信者モード：アクティブな IP-SGT マッピングをポリシー適用のためにすべてアップストリームデバイスに転送できるように、デバイスを設定します。
- 受信者モード：ダウンストリームデバイス（SGT 対応スイッチ）からの IP-SGT マッピングを受信し、ポリシー定義の作成でこの情報を使用できるように、デバイスを設定します。

SXP接続の一方の端が送信者として設定されている場合、もう一方の端は受信者として設定する必要があります。逆の場合も同様です。SXP接続の両端の両方のデバイスに同じロール（両方とも送信者または両方とも受信者）が設定されている場合、SXP接続が失敗し、デバイスはシステムログメッセージを生成します。

デバイスを SXP 接続の送信者および受信者の両方として設定すると、SXP ループが発生する可能性があります。つまり、SXP データが最初にそのデータを送信した SXP ピアで受信される可能性があります。

SXP の設定の一部として、SXP 調整タイマーを設定します。SXP ピアが SXP 接続を終了すると、デバイスはホールドダウンタイマーを開始します。受信者デバイスとして指定された SXP ピアのみが接続を終了できます。ホールドダウンタイマーの実行中に SXP ピアが接続されると、デバイスは調整タイマーを開始します。次に、デバイスは、IP-SGT マッピングデータベースを更新して、最新のマッピングを学習します。

ASA と Cisco TrustSec を統合するための前提条件

Cisco TrustSec と統合するように ASA を設定する前に、次の前提条件を満たす必要があります。

- ISE に ASA を登録する。
- ISE で ASA のセキュリティグループを作成する。
- ASA にインポートする PAC ファイルを ISE で生成する。

ISE への ASA の登録

ASA が PAC ファイルを正常にインポートするには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。

1. ISE にログインします。
2. [管理（Administration）] > [ネットワークデバイス（Network Devices）] > [ネットワークデバイス（Network Devices）] の順に選択します。
3. [Add] をクリックします。
4. ASA の IP アドレスを入力します。
5. ISE が Cisco TrustSec ソリューションでユーザ認証に使用されている場合は、[Authentication Settings] エリアに共有秘密を入力します。ASA で AAA サーバーを設定する場合は、ISE でここで作成した共有秘密を指定します。ASA の AAA サーバーはこの共有秘密を使用して、ISE と通信します。
6. ASA のデバイス名、デバイス ID、パスワード、およびダウンロード間隔を指定します。これらのタスクを実行する方法の詳細については、ISE のマニュアルを参照してください。

ISE でのセキュリティ グループの作成

ISE と通信するように ASA を設定する場合は、AAA サーバーを指定します。AAA サーバーを ASA で設定する場合は、サーバー グループを指定する必要があります。

セキュリティ グループは、RADIUS プロトコルを使用するように設定する必要があります。

1. ISE にログインします。
2. [ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [結果（Results）] > [セキュリティグループアクセス（Security Group Access）] > [セキュリティグループ（Security Groups）] を選択します。

3. ASA のセキュリティ グループを追加します。（セキュリティ グループは、グローバルであり、ASA に固有ではありません）。

   ISE は、タグを使用して [Security Groups] でエントリを作成します。

4. [セキュリティグループアクセス（Security Group Access）] セクションで、 ASA のデバイス ID クレデンシャルおよびパスワードを設定します。

PAC の生成

PAC ファイルを生成する前に、ISE に ASA を登録する必要があります。

1. ISE にログインします。
2. [管理（Administration）] > [ネットワーク リソース（Network Resources）] > [ネットワークデバイス（Network Devices）] の順に選択します。
3. デバイスのリストから、ASA デバイスを選択します。
4. [Security Group Access (SGA)] で、[Generate PAC] をクリックします。
5. PAC ファイルを暗号化するには、パスワードを入力します。

PAC ファイルを暗号化するために入力するパスワード（または暗号キー）は、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

ISE は PAC ファイルを生成します。ASA は、フラッシュ、または TFTP、FTP、HTTP、HTTPS、SMB を介してリモートサーバーから PAC をインポートできます。（PAC は、インポート前に ASA フラッシュに配置されている必要はありません）。

TrustSec ファイアウォールポリシーの構成

セキュリティグループ認識は複数の既存のファイアウォールルールに組み込まれます。固有の TrustSec ファイアウォールポリシーはありません。また、サポートするツールが更新され、TrustSec ファイアウォールポリシーで機能するようになりました。たとえば、[検索と置換（Find and Replace）] ツールを使用して、特定のセキュリティグループを含むルールを検索できます。

この項では、セキュリティグループ認識をファイアウォールポリシーに統合するためのさまざまな手順について説明します。

ここでは、次の内容について説明します。

- Cisco TrustSec サービスの設定 （854 ページ）
- セキュリティ グループ オブジェクトの作成 （863 ページ）
- ポリシーでのセキュリティグループの選択 （865 ページ）
- TrustSec ベースのファイアウォールルールの設定 （866 ページ）

Cisco TrustSec サービスの設定

この手順では、Cisco Security Manager および必要なセキュリティデバイスで Cisco TrustSec の有効化と設定の方法について説明します。

はじめる前に

Cisco TrustSec と統合するために ASA を設定する前に、 ASA と Cisco TrustSec を統合するための前提条件 （852 ページ） で説明されている前提条件を満たす必要があります。

Cisco TrustSec を設定するには、次のタスクを実行します。

ステップ 1 Cisco Security Manager と Cisco Identity Services Engine（ISE）間の通信を設定します。 [ISE設定（ISE Settings）] ページ （718 ページ） を参照してください。

（注） Cisco Security Manager は、セキュリティグループの名前とタグを取得して解決するために、1 つの ISE アプライアンス/サーバーとの通信のみサポートします。

ステップ 2 Security Exchange Protocol（SXP）を有効にしてデフォルト値を設定します。 Cisco TrustSec の SGT および SXP サポートについて （846 ページ） を参照してください。

ステップ 3 Cisco TrustSec アーキテクチャの SXP 接続ピアを追加します。 SXP 接続ピアの定義 （859 ページ） を参照してください。

ステップ 4 （ASA 9.3.1 以降のデバイスのみ）セキュリティ グループ タギング オプションを設定します。 [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （2396 ページ） を参照してください。

ステップ 5 （ASA 9.3.1 以降のデバイスのみ）VPN セッションのセキュリティ グループ タギングを設定します。 ASA グループ ポリシーの SSL VPN フル クライアント設定 （1945 ページ） を参照してください。

ステップ 6 セキュリティ ポリシーを設定します。 TrustSec ベースのファイアウォールルールの設定 （866 ページ） を参照してください

ステップ 7 TrustSec ファイアウォールシステムを監視します。 TrustSec ファイアウォールポリシーのモニタリング （867 ページ） を参照してください。

Security Exchange Protocol（SXP）の設定

[SXP 設定（SXP Settings）] ページを使用して、セキュリティデバイスで Security Exchange Protocol（SXP）を有効にし、デバイスの SXP 設定を行います。

（注） 特定のデバイスタイプのポリシービューまたはデバイスビューからそのページにアクセスするかどうかにかかわらず、すべての設定は [SXP 設定（SXP Settings）] ページで使用できます。特定のデバイスでサポートされていない設定を行うと、検証警告を受信し、そのデバイスでサポートされていない CLI は生成されません。

ナビゲーション パス

- （デバイスビュー）セキュリティデバイスを選択し、ポリシーセレクタから [TrustSec] > [SXP設定（SXP Settings）] を選択します。
- (ポリシービュー) ポリシーセレクターから [TrustSec] > [SXP設定（SXP Settings）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ASA と Cisco TrustSec を統合するための前提条件 （852 ページ）
- SXP 接続ピアの定義 （859 ページ）

フィールド リファレンス

表 *174 : [SXP*設定（*SXP Settings***）*]* ページ**

要素	説明
SGT 交換プロトコル（SXP）の有効化	デバイスでセキュリティ交換プロトコルを有効にするかどうか。デフォルトではディセーブルになっています。
再試行タイマー	SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔。0～64000 秒の範囲で、再試行タイマー値を秒数で入力します。0 秒を指定すると、タイマーの期限が切れず、デバイスは SXP ピアへの接続を試行しません。デフォルトでは、タイマー値は 120 秒です。 デバイスは、接続に成功するまで、新しい SXP ピアへの接続の試みを続けます。 確立されていない SXP 接続が存在する限り、再試行タイマーがトリガーされます。 再試行タイマーが期限切れになると、デバイスは接続データベースを順に検索し、データベースにオフまたは「保留中」状態の接続が含まれている場合、 デバイスは再試行タイマーを再開します。

要素	説明
調整タイマー	調整タイマー値（1 ～ 64000 秒の範囲）。デフォルトでは、タイマー値は 120 秒です。 SXP ピアが SXP 接続を終了すると、セキュリティデバイスはホールドダウンタイマーを開始します。ホールドダウンタイマーの実行中に SXP ピアが再接続されると、デバイスは調整タイマーを開始します。次に、デバイスは SXP マッピングデータベースを更新して、最新のマッピングを学習します。 調整タイマーの期限が切れると、デバイスは、SXP マッピングデータベースをスキャンして、古いマッピングエントリ（前回の接続セッションで学習されたエントリ）を識別します。デバイスは、これらの接続を廃止としてマークします。調整タイマーが期限切れになると、デバイスは SXP マッピングデータベースから廃止エントリを削除します。 （注） 復帰期間を 0 秒に設定すると、タイマーが無効になり、前回の接続のすべてのエントリが削除されます。
ネットワーク マップ	ネットワークマップ引数は、SGT にバインドされ、SXP リスナーにエクスポートできる、0 ～ 65,535 のサブネット IP ホストの最大数を指定します。デフォルトは 0（実行される拡張なし）です。
Server Group Name （IOS-XE には適用されません）	デバイス用 ISE で作成したセキュリティグループの名前を入力または選択します。 （注） サーバーグループを選択する場合、AAA サーバーグループを追加することもできます。 ここで指定するサーバーグループ名は、デバイス用 ISE で作成したセキュリティグループの名前と一致している必要があります。これら 2 つのグループ名が一致しない場合、デバイスは ISE と通信できません。この情報が不明な場合は、ISE 管理者にお問い合わせください。
CTS サーバー設定（IOS/IOS-XE のみ）	
ログバインディング変更	IP から SGT へのバインディング変更のロギングを有効にすると、IP から SGT へのバインディング変更（追加、削除、変更）が発生するたびに SXP の syslog（sev 5 syslog）が生成されるかどうか。これらの変更は SXP 接続で学習されて伝播されます。このロギング機能は、デフォルトではディセーブルになっています。

要素	説明
キャッシングの有効化 キャッシュ NV ストレージ （IOS-XE には適用されません）	DRAM および NVRAM への TrustSec 許可および環境データ情報のキャッシュを有効にするかどうか。 DRAM キャッシュの更新を不揮発性ストレージに書き込み、デバイスの起動時に DRAM キャッシュが不揮発性ストレージから最初に読み込まれるようにするには、[キャッシュNVストレージ（Cache NV Storage）] リストから目的のファイルシステムを選択します。次のオプションがあります。 • flash • flash0 • flash1 • flash2 • disk0 • disk1 • disk2
CTS SGT 番号	1 ～ 65533 の番号を入力して、このデバイスのセキュリティグループタグ（SGT）番号を手動で割り当てます。
サーバーのデッドタイム （IOS-XE には適用されません）	いったん停止中としてマークされたグループ内のサーバを、どのくらいの期間、サービス用に選択してはいけないかを指定します。デフォルトは 20 秒です。指定できる範囲は 1 ～ 864000 です。

要素	説明
ロード バランシング（Load Balance） （IOS-XE には適用されません）	RADIUS サーバーグループのロードバランシングを設定するかどうか。ロードバランスが有効になっている場合、次のオプションを指定できます。 バッチサイズ：バッチごとに割り当てられるトランザクションの数。デフォルトの transactions は 25 です。 （注） バッチ サイズを変更すると、CPU の負荷やネットワークのスループットに影響する可能性があります。バッチ サイズが大きくなるほど、CPU の負荷が減少し、ネットワークのスループットが増加します。ただし、バッチ サイズが大きくても、使用可能なすべてのサーバー リソースが使い果たされることはありません。バッチサイズが小さくなるほど、CPU の負荷が増加し、ネットワークのスループットが減少します。デフォルト バッチ サイズの 25 の使用を推奨します。これは、CPU の負荷に悪影響を及ぼさない、高スループットに最適化されているためです。 優先サーバを無視：セッション全体を通じて同じサーバーを使用しないようにデバイスに指示します。
SGT ロールベース マップテーブル （ASA 9.3(1)+、IOS15.2(2)T+、および IOS-XE3.5.x（15.2(1)S）+ のみ）	SGT ロールベースマップテーブルを使用して、セキュリティグループタグ（SGT）番号を個々の IP アドレスまたはホストオブジェクトに手動でマッピングします。 次を実行できます。 • エントリを追加するには、[行の追加（+）（Add Row(+)] ボタンをクリックし、[接続ピアの追加（Add Connection Peer）] ダイアログボックスに入力します。 [SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックス （858 ページ）を参照してください。 • エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。

[SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックス

[SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックスを使用して、セキュリティグループタグ（SGT）番号を個々の IP アドレスまたはホストオブジェクトに手動でマッピングします。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [TrustSec] > [SXP設定（SXP Settings）] を選択します。
  - エントリを追加するには、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の追加（+）（Add Row (+)）] ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- (ポリシービュー) ポリシーセレクターから [TrustSec] > [SXP設定（SXP Settings）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
  - エントリを追加するには、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の追加（+）（Add Row (+)）] ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[SGTロールベースマップ（SGT Rolebased Map）] テーブルの下にある [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- 送信者および受信者のロールについて （851 ページ）
- ASA と Cisco TrustSec を統合するための前提条件 （852 ページ）

フィールド リファレンス

表 *175 : [SGTロールの追加/編集（Add/Edit SGT Role）] ダイアログボックス*

要素	説明
IPアドレス	セキュリティグループタグ（SGT）番号を手動で割り当てるホストの IPv4 アドレス。 ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。
CTS SGT 番号	指定したホスト/IP アドレスに割り当てるセキュリティグループタグ（SGT）番号。ASA 9.3(1)+ で有効なセキュリティタグ番号は 2 ～ 65519 です。

SXP 接続ピアの定義

セキュリティ グループ交換プロトコル（SXP）は、SGT およびセキュリティ グループ ACL をサポートしているハードウェアに対する SGT 対応ハードウェア サポートがないネットワーク デバイスに IP-to-SGT マッピング データベースを伝搬できるよう Cisco TrustSec 向けに開発さ

れたプロトコルです。コントロール プレーン プロトコルの SXP は、IP-SGT マッピングを認証ポイント（レガシー アクセス レイヤ スイッチなど）からネットワークのアップストリーム デバイスに渡します。ピア間の SXP 接続はポイントツーポイントであり、基礎となるトランスポート プロトコルとして TCP を使用します。

関連項目

- ASA と Cisco TrustSec を統合するための前提条件 （852 ページ）
- 送信者および受信者のロールについて （851 ページ）
- Security Exchange Protocol（SXP）の設定 （854 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [TrustSec（TrustSec）] > [SXP接続ピア（SXP Connection Peers）] を選択します。
- (ポリシー ビュー) ポリシー セレクターから [TrustSec] > [SXP 接続ピア] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [デフォルトソース（Default Source）] フィールドに、SXP 接続のデフォルトローカル IP アドレスを入力します。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。

（注） ピア IP アドレスが到達可能な発信インターフェイスの IP アドレスとして、デバイスが SXP 接続のローカル IP アドレスを指定します。設定されたローカルアドレスが発信インターフェイスの IP アドレスと異なる場合、デバイスは SXP ピアに接続できず、システムログメッセージを生成します。

ステップ 3 [デフォルトパスワード（Default password）] と [確認（Confirm）] に、SXP ピアによる TCP MD5 認証用のデフォルトパスワードを入力します。デフォルトでは、SXP 接続にパスワードは設定されていません。

パスワードは、162 文字までの暗号化された文字列または 80 文字までの ASCII キー ストリングとして指定できます。

ステップ 4 SXP ピアの設定：

次を実行できます。

- エントリを追加するには、[行の追加（+）（Add Row(+)] ボタンをクリックし、[接続ピアの追加（Add Connection Peer）] ダイアログボックスに入力します。[接続ピアの追加（Add Connection Peer）]/[接続ピアの編集（Edit Connection Peer）] ダイアログボックス （861 ページ）を参照してください。
- エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。
- エントリを削除するには、エントリを選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。

ステップ 5 [保存（Save）] をクリックして変更を保存します。

[接続ピアの追加（Add Connection Peer）]/[接続ピアの編集（Edit Connection Peer）] ダイアログボックス

[接続ピアの追加（Add Connection Peer）]/[接続ピアの編集（Edit Connection Peer）] ダイアログボックスを使用して、SXP 接続の設定を定義します。

（注） ポリシービューまたは特定のデバイスタイプのデバイスビューのどちらから [接続ピアの追加/編集（Add/Edit Connection Peer）] ダイアログボックスにアクセスしても、このダイアログボックスですべての設定を使用できます。特定のデバイスでサポートされていない設定を行うと、検証警告を受信し、そのデバイスでサポートされていない CLI は生成されません。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [TrustSec（TrustSec）] > [SXP接続ピア（SXP Connection Peers）] を選択します。
  - エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。
- (ポリシー ビュー) ポリシー セレクターから [TrustSec] > [SXP 接続ピア] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
  - エントリを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。
  - エントリを編集するには、エントリを選択し、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。

関連項目

- 送信者および受信者のロールについて （851 ページ）
- ASA と Cisco TrustSec を統合するための前提条件 （852 ページ）

フィールド リファレンス

表 176 : [接続ピアの追加（Add Connection Peer）] ダイアログボックス

要素	説明
ピア IP アドレス（Peer IP Address）	SXP ピアの IPv4 アドレスまたは IPv6 アドレス。ピア IP アドレスは、発信インターフェイスからアクセスできる必要があります。 ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。
送信元 IP アドレス	（任意）SXP 接続のローカル IPv4 または IPv6 アドレス。送信元 IP アドレスの指定は任意ですが、選択することにより設定ミスを防ぐことができます。 ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力できます。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。 （注） 送信元 IP アドレスとピア IP アドレスを同じアドレスで設定することはできません。また、一方のフィールドで IPv4 アドレスを使用し、もう一方のフィールドで IPv6 アドレスを使用することはできません。
パスワード	SXP 接続に認証キーを使用するかどうかを指定します。次の値から選択します。 • default：SXP 接続用に設定されたデフォルト パスワードを使用します。 SXP 接続ピアの定義 （859 ページ）を参照してください。 • none：SXP 接続にパスワードを使用しません。
[モード（Mode）]	SXP 接続のモード。次の値から選択します。 • local：ローカル SXP デバイスを使用します。 • peer：ピア SXP デバイスを使用します。

要素	説明
ロール	SXP接続で、デバイスがスピーカまたはリスナーのいずれとして機能するかを指定します。 • [リスナー（Listener）]：デバイスはダウンストリームデバイスから IP-SGT マッピングを受信できます。 • [スピーカ（Speaker）]： デバイスは IP-SGT マッピングをアップストリームデバイスに転送できます。 送信者および受信者のロールについて （851 ページ）を参照してください。
最小保留時間（Hold Time (Min)） IOS および IOS-XE のみに適用	スピーカーまたはリスナーデバイスの最小保留時間（秒単位）。
最大保留時間（Hold Time Max） IOS および IOS-XE のみに適用	スピーカーまたはリスナーデバイスの最大保留時間（秒単位）。hold-time maximum-period 値は、peer speaker と local listener オプションを組み合わせて使用する場合のみ必要です。その他のインスタンスでは、hold-time minimum-period 値のみが必要です。

セキュリティ グループ オブジェクトの作成

作成したセキュリティ グループ オブジェクト グループは、Cisco TrustSec をサポートする機能で使用できます。そのグループを拡張 ACL に入れると、たとえばアクセス ルールで使用できるようになります。

Cisco TrustSec と統合されているときは、セキュリティデバイスは Cisco Identity Services Engine（ISE）からセキュリティグループの情報をダウンロードします。ISE はアイデンティティ リポジトリとしても動作し、Cisco TrustSec タグからユーザー アイデンティティへのマッピングと、Cisco TrustSec タグからサーバー リソースへのマッピングを行います。セキュリティ グループ アクセス リストのプロビジョニングおよび管理は、中央集中型で ISE 上で行います。

ただし、デバイスには、グローバルには定義されていない、ローカライズされたネットワーク リソースが存在することがあり、そのようなリソースにはローカル セキュリティ グループとローカライズされたセキュリティポリシーが必要です。ローカルセキュリティ グループには、ISEからダウンロードされた、ネストされたセキュリティ グループを含めることができます。セキュリティデバイスは、ローカルと中央のセキュリティグループを統合します。

デバイス上でローカル セキュリティ グループを作成するには、ローカル セキュリティ オブジェクト グループを作成します。1 つのローカル セキュリティ オブジェクト グループに、1 つ以上のネストされたセキュリティ オブジェクト グループまたはセキュリティ ID またはセキュリティ グループ名を入れることができます。ユーザーは、デバイス上に存在しない新しいセキュリティ ID またはセキュリティグループ名を作成することもできます。

作成したセキュリティ オブジェクト グループは、ネットワークリソースへのアクセスを制御するために使用できます。セキュリティ オブジェクト グループを、アクセス グループやサービス ポリシーの一部として使用できます。

ヒント

- これらのオブジェクトの使用は、ASA 9.0(1) 以降でのみサポートされます。
- これらのオブジェクトの使用を有効にするには、デバイスで TrustSec ポリシーを設定する必要があります。
- このオブジェクトタイプを使用するポリシー、またはオブジェクトを定義するときに、セキュリティ グループ オブジェクトを作成できます。詳細については、ポリシーでのセキュリティグループの選択 （865 ページ）を参照してください。

関連項目

- ポリシーでのセキュリティグループの選択 （865 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [セキュリティグループ（Security Group）] を選択します。

ステップ 3 作業領域を右クリックして [新規オブジェクト（New Object）] を選択し、[セキュリティグループの追加（Add Security Group）] ダイアログボックスを開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 [グループ内のメンバー（Members in Group）] リストにアイテムを追加したり、このリストからアイテムを削除したりして、オブジェクトに定義されているユーザーとユーザーグループを識別します。

リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なセキュリティグループ（Available Security Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。
- [名前/タグの検索（Search name/tag）] で、[ISE設定（ISE Settings）] の管理オプションで設定済みの ISE サーバーからセキュリティグループを選択します。名前またはタグを選択する前に、設定を行う必要があります（[ISE設定（ISE Settings）] ページ （718 ページ）を参照）。

セキュリティグループを検索するには、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。文字列がセキュリティグループ名のどこかにある場合、名前は一致したと見なされます。

セキュリティグループを追加するには、リストで選択し、リスト間にある [追加>>（Add >>）] ボタンをクリックします。

- [カンマ区切りで入力（名前またはタグ）（Type in comma separated (Name or Tag)）] で、最初に作成するエントリのタイプ（名前またはタグ）を選択します。有効なセキュリティグループ名またはタグ番号を入力し、リスト間の [追加>>（Add >>）] ボタンをクリックします。複数の名前やタグはカンマで

区切ります。名前やタグはメンバーリストに別々の行として追加されます。複数の名前やタグを追加する場合は、カンマの前後にスペースを追加しないでください。

有効なセキュリティタグ番号は、ASA 9.3 以降の場合は 0 ～ 65533、ASA のバージョンが 9.3 未満の場合は 1 ～ 65533 です。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。

ポリシーでのセキュリティグループの選択

セキュリティグループの指定を許可するポリシーまたはポリシーオブジェクトで、直接または TrustSec セキュリティ グループオブジェクトを選択して、[セキュリティグループ（Security Groups）] フィールドの横にある [選択（Select）] ボタンをクリックして情報を入力できます。

[セキュリティグループセレクタ（Security Group Selector）] ダイアログボックスで [グループ内のメンバー（Members in Group）] リストに入力することにより、[セキュリティグループ（Security Groups）] フィールドの内容を定義できます。リストに入力するには、次のいずれかの組み合わせを実行します。

- [利用可能なセキュリティグループ（Available Security Group）] で、既存のオブジェクトを選択し、リスト間の [追加>>（Add >>）] ボタンをクリックします。目的のオブジェクトが存在しない場合は、リストの下にある [追加（Add）]（+）ボタンをクリックして新しいオブジェクトを作成できます。オブジェクトを選択し [編集（Edit）]（鉛筆）ボタンをクリックして、オブジェクトを変更するか、内容を確認できます。
- [名前/タグの検索（Search name/tag）] で、[ISE設定（ISE Settings）] の管理オプションで設定済みの ISE サーバーからセキュリティグループを選択します。名前またはタグを選択する前に、設定を行う必要があります（[ISE設定（ISE Settings）] ページ （718 ページ）を参照）。

セキュリティグループを検索するには、検索文字列を入力します。次に、[検索（Search）] をクリックして一致する文字列を検索します。文字列がセキュリティグループ名のどこかにある場合、名前は一致したと見なされます。

セキュリティグループを追加するには、リストで選択し、リスト間にある [追加>>（Add>>）] ボタンをクリックします。

- [カンマ区切りで入力（名前またはタグ）（Type in comma separated (Name or Tag)）] で、最初に作成するエントリのタイプ（名前またはタグ）を選択します。有効なセキュリティグループ名またはタグ番号を入力し、リスト間の [追加>>（Add >>）] ボタンをクリックします。複数の名前やタグはカンマで区切ります。名前やタグはメンバーリストに別々の行として追加されます。複数の名前やタグを追加する場合は、カンマの前後にスペースを追加しないでください。

有効なセキュリティタグ番号は、ASA 9.3 以降の場合は 0 ～ 65533、ASA のバージョンが 9.3 未満の場合は 1 ～ 65533 です。

- オブジェクトから項目を削除するには、[メンバー（Members）] リストで項目を選択し、リスト間にある [<<削除（<< Remove）] ボタンをクリックします。

TrustSec ベースのファイアウォールルールの設定

セキュリティグループ認識は、ファイアウォールサービスを提供するために使用される ACL 内のアクセス コントロール エントリまたはルールと統合されます。この機能は ACL と統合されるため、セキュリティグループ認識をファイアウォール ポリシーに追加する方法は、すべてのタイプのファイアウォールポリシーで同じになります。この項では、セキュリティグループ認識を既存のポリシーに取り込む一般的な方法を説明し、セキュリティグループをサポートするポリシーごとの設定について、詳細な情報を提供します。

セキュリティグループをサポートするファイアウォール ポリシー

ASA 9.0.1 以降でのみ、次のポリシータイプのセキュリティグループを設定できます。

- AAA ルール：[ファイアウォール（Firewall）] > [AAA ルール（AAA Rules）] を選択します。ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）を参照してください。
- アクセスルール：**[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**を選択します。アクセス ルールの設定 （920 ページ）を参照してください。
- インスペクションルール：[ファイアウォール（Firewall）] > [インスペクションルール（Inspection Rules）] を選択します。インスペクション ルールの設定 （983 ページ）を参照してください。
- 拡張 ACL ポリシー オブジェクトを使用するポリシー：複数のファイアウォール ポリシーが拡張 ACL ポリシー オブジェクトを使用して、ルール テーブルを直接ポリシーに取り込む代わりにトラフィック照合基準を定義できます。セキュリティグループ指定を組み込むために拡張 ACL ポリシー オブジェクトを設定できます（拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）を参照）。これらの拡張 ACL オブジェクトは、次のポリシーで使用できます。

- ボットネット トラフィック フィルタ ルール：[ファイアウォール（Firewall）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）] を選択します。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170ページ）を参照してください。セキュリティグループは、イネーブルルールおよびドロップルールのトラフィック分類の一部として使用できます。
- IPS ルール、QoS ルール、および接続ルール（サービスポリシールール）：[プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）]を選択します。 [サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）を参照してください。

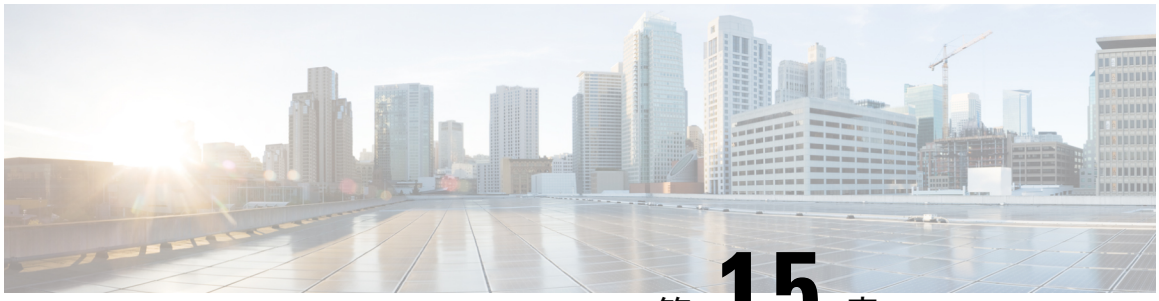
このポリシーのトラフィック照合基準は、トラフィック フロー ポリシー オブジェクトに組み込まれる拡張 ACL ポリシー オブジェクトに基づいて行われます。セキュリティグループのトラフィック分類を組み込むトラフィック フロー オブジェクトに、ACL を指定するオプションをいずれか選択する必要があります。詳細については、 トラフィック フロー オブジェクトの設定 （2965 ページ）を参照してください。

IOS 15.2(2)T 以降および IOS-XE 3.5.x(15.2(1)S) 以降を実行しているデバイスでは、ゾーンベースのファイアウォールルールにセキュリティグループを設定できます **([ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（ Zone Based Firewall Rules）])**。詳細については、ゾーンベースのファイアウォールルールの追加 （1210ページ）を参照してください。

TrustSec ファイアウォールポリシーのモニタリング

イベントビューアを使用して、他のタイプのポリシーやイベントと同じ方法で TrustSec ファイアウォールポリシーをモニタリングできます。次に、アイデンティティ ポリシーを効率的に監視するためのヒントをいくつか示します。Event Viewer 使用の一般情報については、イベントの表示 （3473 ページ）を参照してください。

- 特に Cisco TrustSec に関連する syslog メッセージには、766001 ～ 766020、766201 ～ 766205、766251 ～ 766254、および 766301 ～ 766313 の各グループがあります。これらのメッセージの説明については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html [英語] で、ご使用の ASA ソフトウェアバージョンの syslog メッセージを参照してください。
- イベントビューアには、TrustSec 情報を表示する次の列があります。[TrustSecセキュリティグループ名（TrustSec Security Group Name）]、[TrustSecセキュリティグループタグ（TrustSec Security Group Tag）]、[SXP接続ソースIP（SXP Connection Source IP）]、[SXP接続失敗理由（SXP Connection Failure Reason）]、[SXPピアIP（SXP Peer IP）]、[SXPピア接続失敗理由（SXP Peer Connection Failure Reason）]。
- [イベントタイプ（Event Type）] にフィルタを作成し、[すべてのファイアウォールイベント（All Firewall Events）] > [TrustSecイベント（TrustSec Events）] フォルダを選択することで、すべてのアイデンティティ関連の syslog メッセージをフィルタリングできます。



第 15 章

ファイアウォール AAA ルールの管理

認証、許可、アカウンティング（AAA）ルールを使用すると、IP アドレスではなくユーザ権限に基づいて、ネットワーク リソースへのアクセスを制御できます。認証ルールを設定すると、ユーザは保護されたデバイスの背後にあるネットワークにアクセスしようとするたびに、ユーザ名とパスワードを入力する必要があります。認証後、ネットワーク アクセスがユーザに認可されていることを確認するために、さらにユーザ アカウントのチェックを要求することもできます。最後に、アカウンティング ルールを使用して、請求、セキュリティ、またはリソース割り当ての目的でアクセスを追跡できます。

AAA ルールの設定は複雑であり、AAA ルール ポリシー以外の設定も必要となります。ここでは、AAA ルールについて詳しく説明し、AAA ルール ポリシーの設定だけでなく関連ポリシーで設定する必要があるものに関する手順を示します。

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）
- IOS デバイスの AAA ルールの設定 （877 ページ）
- [AAA Rules] ページ （880 ページ）
- AAA ファイアウォール設定ポリシー （894 ページ）

AAA ルールについて

認証、許可、アカウンティング（AAA）ルールを使用すると、IP アドレスではなくユーザ権限に基づいて、ネットワーク リソースへのアクセスを制御できます。AAA ルールは、従来のアクセス ルールとは異なるタイプの制御を実現します。アクセス ルールでは、許可する IP アドレスとサービスを制御できますが、AAA ルールでは、各ユーザの ACL を設定して、ユーザの接続元 IP アドレスに関係なくユーザごとに認可を定義できます（これらのユーザ単位の ACL は、デバイスに定義される AAA ルールではなく、AAA サーバで設定します）。

AAA ルール ポリシーは、デバイスに向けられたトラフィックではなく、デバイスを通過するトラフィックに AAA ルールが適用されることが、他のデバイス プラットフォームの AAA ポリシーとは異なります。AAA ルールを使用すると、ネットワークへの着信とネットワークからの発信を制御できます。このことは、セキュリティ レベルの高いネットワーク セグメントでアクセスを慎重に制御する必要がある場合に役立ちます。AAA ルールは、請求、セキュリ

ティ、またはリソース割り当ての目的でユーザ単位のアカウンティング レコードを維持する必要がある場合にも役立ちます。

AAA ルール ポリシーでは、実際には3つの異なるタイプのルールを設定します。これらのルールの設定は、IOS デバイスの場合と ASA、PIX、および FWSM デバイスの場合で大きく異なります。IOS デバイスの場合、これらのポリシーではいわゆる認証プロキシ アドミッション コントロールを定義します。共有 AAA ルールを作成する場合は、これらのデバイス タイプに別々のルールを作成します。AAA ルールで設定できるルール タイプは次のとおりです。

- 認証ルール：認証ルールでは、基本的なユーザアクセスを制御します。認証ルールを設定した場合、ユーザは、ルールが定義されているデバイスを接続要求が通過するときにログインする必要があります。HTTP、HTTPS、FTP、または Telnet 接続に対して、ユーザにログインを強制できます。ASA、PIX、および FWSM デバイスの場合、その他のタイプのサービスを制御できますが、ユーザは、まずサポートされているいずれかのプロトコルを使用して認証を受ける必要があり、その後、他のタイプのトラフィックが許可されます。

デバイスがこれらのトラフィック タイプを認識できるのは、デフォルト ポート（FTP（21）、Telnet（23）、HTTP（80）、HTTPS（443））上だけです。これらのタイプのトラフィックを他のポートにマッピングすると、ユーザにプロンプトが表示されず、アクセスは失敗します。

- 認可ルール：認証以外に、追加の制御レベルを定義できます。認証では、ユーザが自身を識別することだけが必要となります。認証に成功すると、認可ルールは、AAA サーバにユーザが試行した接続を完了するのに十分な権限を持っているかどうかを問い合わせることができます。認可に失敗した場合、接続はドロップされます。
  - ASA、PIX、および FWSM デバイスの場合は、AAA ルール ポリシーで直接認可ルールを定義します。認証を必要としないトラフィックの認可が必要な場合、認証されていないトラフィックは常にドロップされます。認証に RADIUS サーバを使用する場合、認可は自動的に実行されるため、認可ルールは必要ありません。認可ルールを設定する場合は、TACACS+ サーバを使用する必要があります。
  - IOS デバイスの場合、認可を設定するには、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA] ポリシーで認可サーバーグループを設定する必要があります。認可は、認証の対象となる、どのトラフィックに対しても実行されます。TACACS+ または RADIUS サーバを使用できます。
- アカウンティング：認証または認可を設定しない場合でも、アカウンティング ルールを定義できます。認証を設定すると、ユーザごとにアカウンティング レコードが作成されるため、接続を確立した特定のユーザを識別できます。ユーザ認証が実行されない場合、アカウンティング レコードは IP アドレスに基づきます。アカウンティングに TACACS+ または RADIUS サーバを使用できます。
  - ASA、PIX、および FWSM デバイスの場合は、AAA ルール ポリシーで直接アカウンティング ルールを定義します。TCP または UDP プロトコルに対してアカウンティングを実行できます。
  - IOS デバイスの場合、アカウンティングを設定するには、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA] ポリシーでアカウンティング サーバー グ

ループを設定する必要があります。アカウンティングは、認証の対象となる、どのトラフィックに対しても実行されます。

ユーザの認証方法について

AAA ルールを作成して、ユーザがデバイスから接続を確立しようとしたときに認証を要求する場合、ユーザはクレデンシャル（ユーザ名とパスワード）を入力するよう要求されます。これらのクレデンシャルは、AAA サーバまたはデバイスに設定されているローカル データベースで定義されている必要があります。

ユーザに要求されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです（認証を要求するようにこれらのプロトコルが設定されている場合）。また、ASA、PIX、およびFWSM デバイスの場合、他のプロトコルの認証を要求することもできます。ただし、その場合、ユーザにはプロンプトが表示されないため、認証を必要とする他のプロトコルの接続を完了するには、まずサポートされている 4 つのプロトコルのいずれかを試して認証に成功する必要があります。

ヒント　ASA、PIX、およびFWSMデバイスの場合、セキュリティアプライアンスからのHTTP、HTTPS、Telnet、またはFTPを許可せず、他のタイプのトラフィックを認証するには、対話型認証を使用するようにインターフェイスを設定して（**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシー）、ユーザーに HTTP または HTTPS を使用して直接セキュリティアプライアンスで認証を受けるように要求できます。この場合、ユーザーは、次のいずれかの URL を使用して他の接続を試行する前に、アプライアンスで認証されます。*interface_ip* はインターフェイスの IP アドレス、*port* はオプションのポート番号です（[対話型認証（Interactive Authentication）] テーブルのプロトコルにデフォルト以外のポートを指定する場合）：**http://***interface_ip* [**:***port*]**/netaccess/connstatus.html** または **https://***interface_ip* [**:***port*]**/netaccess/connstatus.html**。

デバイスから接続を試行すると、ユーザにはプロトコルに応じてプロンプトが表示されます。

- HTTP：ユーザにユーザ名とパスワードを入力するための Web ページが表示されます。このページは、認証に成功するまで繰り返し表示されます。ユーザが正しく認証されると、ユーザは元の宛先にリダイレクトされます。宛先サーバーにも独自の認証がある場合、ユーザーは別のユーザー名とパスワードを入力します。

ASA、PIX、および FWSM デバイスの場合、セキュリティ アプライアンスは、デフォルトでは基本HTTP認証を使用し、認証プロンプトを表示します。対話型認証を使用するようにインターフェイスを設定し、HTTP トラフィックのリダイレクトを指定すると、ユーザエクスペリエンスを向上できます。これにより、ユーザは認証のためにアプライアンス上でホスティングされている Web ページにリダイレクトされます。対話型認証を使用するようにインターフェイスを設定するには、**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシー（[AAA Firewall] 設定ページの [Advanced Setting] タブ（895 ページ）を参照）で [対話型認証（Interactive Authentication）] テーブルにインターフェイ

スを追加します。インターフェイスを追加するときに、HTTP およびリダイレクトのオプションを選択してください。

基本 HTTP 認証を継続して使用する例としては、セキュリティ アプライアンスでリスニング ポートを開きたくない場合、ルータで NAT を使用しているのでセキュリティ アプライアンスで処理する Web ページの変換ルールを作成したくない場合、および基本 HTTP 認証とネットワークとの相性がよい場合があります。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

ただし、基本 HTTP 認証を使用する場合、認証を必要とする HTTP サーバにユーザがアクセスしようとすると、アプライアンスでの認証に使用されたものと同じユーザ名とパスワードが HTTP サーバに送信されます。したがって、ASA と HTTP サーバで同じユーザ名とパスワードが使用される場合を除き、HTTP サーバへのログインは失敗します。この問題を回避するには、ASA に仮想 HTTP サーバーを設定する必要があります。**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシーを使用して、仮想 HTTP サーバーを設定できます([AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）を参照)。

ヒント HTTP 認証では、ユーザ名とパスワードがクリア テキストで送信されます。これを防ぐには、**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシーで [安全なHTTP認証の使用（Use Secure HTTP Authentication）] オプションを選択します。このオプションを選択すると、クレデンシャルが暗号化されます。

- HTTPS：HTTPS の場合、ユーザ エクスペリエンスは HTTP の場合と同じです。つまり、認証に成功するまでユーザにプロンプトが表示され、ユーザは認証されると元の宛先にリダイレクトされます。

ASA、PIX、および FWSM デバイスの場合、セキュリティ アプライアンスは、カスタム ログイン画面を使用します。HTTP と同様に、対話型認証を使用するようにインターフェイスを設定できます。その場合、HTTPS 接続は HTTP 接続と同じ認証ページを使用します。HTTPS リダイレクト用に個別にインターフェイスを設定する必要があります。設定には**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** ポリシーを使用します。

IOS デバイスの場合、HTTPS 接続が認証されるのは、デバイス上で SSL をイネーブルにし、AAA ルールで HTTP 認証プロキシが必要とされている場合だけです。この設定については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。

- FTP：デバイスは、一度だけ認証を要求します。認証に失敗すると、ユーザは接続を再試行する必要があります。

プロンプトが表示されたら、ユーザはデバイス認証に必要なユーザ名、そのあとに続けてアット マーク（@）、FTP ユーザ名を入力できます（name1@name2）。パスワードについては、

デバイス認証パスワード、そのあとに続けてアットマーク（@）、FTPパスワードを入力します（password1@password2）。たとえば、次のテキストを入力します。

name> asa1@partreqpassword> letmein@he110

IOSデバイスの場合は、この方法でデバイスとFTPの両方のクレデンシャルを入力する必要があります。ASA、PIX、およびFWSMデバイスの場合は、ファイアウォールが複数のログインを必要とするカスケード形式になっている場合に、この方法が役立ちます。複数の名前およびパスワードは、複数のアットマーク（@）で区切ることができます。

- Telnet：デバイスは、複数回認証を要求します。認証に数回失敗すると、ユーザは接続を再試行する必要があります。認証後、Telnet サーバはユーザ名とパスワードを要求します。**[ファイアウォール（Firewall）]>[設定（Settings）]>[AAAファイアウォール（AAA Firewall）]** ポリシーを使用して、仮想 Telnet サーバーを設定できます ([AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）を参照)。

ASA、PIX、および FWSM デバイスの AAA ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ASA、PIX、またはFWSMデバイスのAAAルールを設定する場合は、デバイスからのHTTP、HTTPS、FTP、および Telnet 接続（デバイスへの接続ではない）の確立をどのユーザに許可するかを定義するポリシーを設定します。ネットワーク アクセス認証を完全に設定するには、AAA ルール ポリシーだけでなく、いくつかのポリシーを設定する必要があります。

次の手順では、ネットワークアクセス認証に対応した完全な認証、許可、アカウンティングのサポートを提供するために設定する必要があるすべてのポリシーについて説明します。不要な機能のオプションを設定する必要はありません。

関連項目

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- 新しい共有ポリシーの作成 （278 ページ）
- ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）
- ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ステップ 1 次のいずれかを実行して、 [AAA Rules] ページ （880 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）]>[AAAルール（AAA Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）]>[AAAルール（AAA Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。 [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集 （767 ページ）を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、 [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）を参照してください。

- 認証（ユーザアイデンティティあり、またはなし）、許可、またはアカウンティングアクション：この規則に適用できるオプションを選択します。認証を選択した場合、ユーザはHTTP、HTTPS、FTP、または Telnet アクセスを試行するときにユーザ名とパスワードの入力を要求されます。認可は追加レベルであり、ユーザ認証後にAAAサーバをチェックして、ユーザにそのタイプのアクセスが認可されていることを確認します。アカウンティングは、AAAサーバに使用状況レコードを生成し、請求、セキュリティ、またはリソース割り当ての目的で使用できます。TCPまたはUDPトラフィックのアカウンティング情報を生成できます。

[認証（Authentication）] を選択すると、[ユーザアイデンティティ（User-Identity）] も選択できます（ASA 8.4(2+) のみ）。このオプションは、ASA がアイデンティティ ファイアウォール ドメイン マッピングで構成されている Active Directory サーバを使用して、ユーザを認証することを示します（Active Directory サーバおよびエージェントの識別 （818 ページ）を参照）。ユーザがドメイン名を入力すると、そのドメインに関連付けられた AD サーバーが照会されます。それ以外の場合は、デフォルトドメインに関連付けられた AD サーバーが照会されます。[User-Identity] を選択し、[Authorization] または [Accounting] を選択しなかった場合は、AAA サーバ グループを指定しないでください。

- 許可または拒否：識別されたトラフィックを AAA で制御するか（許可）、または AAA 制御から除外するか（拒否）どうか。拒否されたトラフィックは認証を要求されないので認証なしで通過できますが、アクセス ルールによってトラフィックがドロップされる場合があります。
- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスまたはその宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「All-Addresses」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホストオブジェクトを入力します。受け入れられるアドレス形式の詳細については、 ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

- 送信元および宛先のセキュリティグループ（ASA 9.0+ のみ）：送信元および宛先アドレスに加えて、トラフィックのフィルタリングに使用される TrustSec セキュリティグループを指定できます。セキュリティグループの詳細については、ポリシーでのセキュリティグループの選択 （865 ページ）、TrustSec ベースのファイアウォールルールの設定 （866 ページ）、およびセキュリティ グループ オブジェクトの作成 （863 ページ）を参照してください。
- 送信元ユーザー（ASA 8.4.2 以降のみ）：Active Directory（AD）ユーザー名（NetBIOS_DOMAIN\username 形式）、ユーザーグループ（NetBIOS_DOMAIN\\user_group）、または名前とグループを定義するアイデンティティ ユーザー グループ オブジェクトを指定して、トラフィックの送信元をさらに定義できます。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。詳細については、アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）およびアイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）を参照してください。
- サービス：認証ルールと認可ルールのあらゆるサービスタイプを指定できます。ただし、ユーザ認証が要求されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです。したがって、これらのサービス以外のサービスを指定した場合、ユーザは、まずこれらの接続のいずれかを試して認証（および認可アクションを含めた場合は認可）に成功する必要があります。その後、他のタイプの接続が許可されます。アカウンティングルールについては、すべてのトラフィック タイプのアカウンティングを実行する場合、TCP または UDP サービス（あるいは単純に TCP と UDP 自体）を指定できます。
- AAA サーバ グループ：認証、許可、またはアカウンティングに使用する AAA サーバ グループ ポリシー オブジェクト。ルールでこれらのアクションを複数適用する場合は、選択したすべてのアクションがサーバ グループでサポートされている必要があります。たとえば、TACACS+ サーバだけが認可規則のサービスを提供でき（ただし、認証規則に RADIUS を使用すると、自動的に RADIUS 認可が含まれます）、TACACS+ および RADIUS サーバだけがアカウンティング サービスを提供できます。アクションごとに異なるサーバ グループを使用する場合は、異なるグループを必要とするアクション タイプごとに別のルールを定義します。
- インターフェイス：ルールを設定するインターフェイスまたはインターフェイス ロール。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。

ステップ 5 （デバイスビューまたはポリシービューで）[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）] を選択して[AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）を開きます。AAA ファイアウォールを設定します。

- HTTP 認証のルールを設定した場合は、[安全なHTTP認証の使用（Use Secure HTTP Authentication）] を選択する必要があります。これにより、HTTP 認証で入力したユーザ名とパスワードが暗号化されます。このオプションを選択しない場合は、クレデンシャルがクリア テキストで送信されるため、安全性が損なわれます。

ヒント　このオプションを選択する場合は、[ユーザー認証のタイムアウト（user authentication timeout）] に 0 を設定（[プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）] ポリシーで **timeout uauth 0** を設定）しないでください。設定すると、ユーザーが繰り返し認証を要求され、ネットワーク機能が中断する可能性があります。

- インターフェイス上の HTTP または HTTPS トラフィックの認証を設定した場合は、インターフェイスを [Interactive Authentication] テーブルに追加することを検討してください。インターフェイスで対話型認証を使用できるようにすると、ユーザには改良された認可 Web ページ（HTTP と HTTPS の両方で同じページ）が表示されます。

[行の追加（Add Row）] をクリックして、インターフェイスをテーブルに追加します。インターフェイスで HTTP または HTTPS トラフィックを受信するか（両方のプロトコルを受信する場合はインターフェイスを 2 回追加します）、およびプロトコルのデフォルト ポート（それぞれ 80 と 443）を使用しない場合は受信するポートを選択します。[認証リクエストにネットワークユーザをリダイレクト（Redirect network users for authentication request）] を選択して、ネットワーク アクセス トラフィックに対して改良された認証プロンプトが表示されるようにします。このオプションを選択しない場合は、このデバイスにログインしようとするユーザにだけプロンプトが表示されます。

（注）　基本 HTTP 認証を継続して使用する例としては、セキュリティ アプライアンスでリスニング ポートを開きたくない場合、ルータで NAT を使用しているのでセキュリティ アプライアンスで処理する Web ページの変換ルールを作成したくない場合、および基本 HTTP 認証とネットワークとの相性がよい場合があります。たとえば、電子メールに URL が埋め込まれている場合などのように、ブラウザ以外のアプリケーションでは基本認証の方が適していることがあります。

- FWSM デバイスの場合は、認証を必要とするように設定したプロトコルの認証チャレンジをディセーブルにすることもできます。インターフェイスを [Clear Connections] テーブルに追加して、認証がタイムアウトしたユーザのアクティブな接続をクリアし、ハングしないようにすることもできます。

- Media Access Control（MAC：メディア アクセス コントロール）アドレスに基づいて AAA ルールから一部のデバイスを免除する場合は、[MAC免除リスト（MAC Exempt List）] タブをクリックして [AAA Firewall] ページの [MAC-Exempt List] タブ （902 ページ）を開きます。免除リストの名前を入力し、[行の追加（Add Row）] ボタンをクリックします。次に [Firewall AAA MAC Exempt Setting] ダイアログ ボックス （904 ページ）に入力し、許可ルールを使用して MAC アドレスをテーブルに追加します。この操作は、信頼できるセキュア デバイスに対して実行できます。

エントリの順序は処理に影響を及ぼします。このため、より広範なエントリにも当てはまるエントリは、テーブル内で、広範なエントリよりも前に配置してください。デバイスは、リストを順番に処理し、最初に一致したものがホストに適用されます。MAC 免除リスト内のエントリが処理される方法の詳細については、[AAA Firewall] ページの [MAC-Exempt List] タブ （902 ページ）を参照してください。

ステップ 6　RADIUS サーバを使用して認証ルールを設定し、ユーザ ポリシーにユーザ単位の ACL 設定を含める場合は、インターフェイスに対してユーザ単位のダウンロード可能 ACL をイネーブルにします（RADIUS 認証には、承認チェックが自動的に含まれます。）ユーザごとの ACL の設定については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_fwaaa.html にある『*Cisco ASA 5500 Series Configuration Guide Using the CLI*』の RADIUS 認証の設定に関する情報を参照してください。

a)　（デバイスビューまたはポリシービューで）[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）] を選択して [Access Control Settings] ページ （944 ページ）を開きます。

b) インターフェイス テーブルの下にある [Add Row] ボタンをクリックし、[Firewall ACL Setting] ダイアログボックス （947 ページ）で少なくとも次のオプションを入力または選択します。

- 認可を実行するインターフェイスまたはインターフェイス ロールを入力します。
- [ユーザ単位のダウンロード可能ACL（Per User Downloadable ACLs）] を選択します。

c) [OK] をクリックして変更を保存します。

IOS デバイスの AAA ルールの設定

IOS デバイスの AAA ルールを設定する場合は、認証プロキシ（AuthProxy）アドミッション コントロール ポリシーを設定します。これらのポリシーでは、デバイスからの HTTP、HTTPS、FTP、および Telnet 接続（デバイスへの接続ではない）の確立をどのユーザに許可するかを定義します。認証プロキシを完全に設定するには、AAA ルール ポリシーだけでなく、いくつかのポリシーを設定する必要があります。

次の手順では、認可プロキシ用の完全な認証、許可、アカウンティングのサポートを提供するために設定する必要がある、すべてのポリシーについて説明します。不要な機能のオプションを設定する必要はありません。

関連項目

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- 新しい共有ポリシーの作成 （278 ページ）
- ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ステップ 1 次のいずれかを実行して、[AAA Rules] ページ （880 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）] > [AAA ルール（AAA Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。 [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集 （767 ページ）を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、 [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）を参照してください。

- **認証アクション**：このオプションを選択します。認証ルールは、IOS デバイスの AAA ルール ポリシーで設定できる唯一のルール タイプです。
- 許可または拒否：識別されたトラフィックを AAA で制御するか（許可）、または AAA 制御から除外するか（拒否）どうか。拒否されたトラフィックは認証を要求されないので認証なしで通過できますが、アクセス ルールによってトラフィックがドロップされる場合があります。
- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスまたはトラフィックの宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「All-Addresses」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホスト オブジェクトを入力します。受け入れられるアドレス形式の詳細については、 ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。
- 送信元および宛先セキュリティグループ（ASA 9.0 以降のみ）：送信元および宛先アドレスに加えてトラフィックのフィルタ処理に使用される TrustSec セキュリティグループを指定できます。セキュリティグループの詳細については、ポリシーでのセキュリティグループの選択 （865 ページ）、TrustSec ベースのファイアウォールルールの設定 （866 ページ）、および セキュリティ グループ オブジェクトの作成 （863 ページ）を参照してください。
- 送信元ユーザー（ASA 8.4.2 以降のみ）：Active Directory（AD）ユーザー名（NetBIOS_DOMAIN\username 形式）、ユーザーグループ（NetBIOS_DOMAIN\\user_group）、または名前とグループを定義するアイデンティティ ユーザー グループ オブジェクトを指定して、トラフィックの送信元をさらに定義できます。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレスを制限します。詳細については、 アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）および アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）を参照してください。
- サービス：認証ルールと認可ルールのサービスタイプを指定できます。ただし、ユーザー認証が要求されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです。したがって、これらのサービス以外のサービスを指定した場合、ユーザは、まずこれらの接続のいずれかを試して認証（および認可アクションを含めた場合は認可）に成功する必要があります。その後、他のタイプの接続が許可されます。アカウンティング ルールについては、すべてのトラフィック タイプのアカウンティングを実行する場合、TCP または UDP サービス（あるいは単純に TCP と UDP 自体）を指定できます。
- インターフェイス：ルールを設定するインターフェイスまたはインターフェイス ロール。
- 認証プロキシをトリガーするサービス：ユーザ認証をトリガーするトラフィックのタイプ（HTTP、FTP、または Telnet）のチェックボックスをオンにします。自由に組み合わせて選択できます。HTTPS

サポート用のプロキシをトリガーする場合は、[HTTP] を選択し、あとの手順で説明する HTTPS 設定を実行します。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。

ステップ 5 （デバイスビューまたはポリシービューで）[ファイアウォール（Firewall）]>[設定（Settings）]>[AuthProxy] を選択して [AAA] ページ （905 ページ）を開きます。認証プロキシを設定します。

- **認可サーバーグループ**：すべての認証ルールでユーザー認可も実行する場合は、認可を制御する TACACS+ または RADIUS サーバーを識別する AAA サーバー グループ ポリシー オブジェクトのリストを指定します。[LOCAL] を指定して、デバイスに定義されているユーザ データベースを使用することもできます。サーバ グループを指定しない場合は、認可が実行されません。

ヒント AAA サーバでユーザごとに ACL を設定して、各ユーザに適用する権限を定義する必要があります。認可を設定する場合は、サービスとして [auth-proxy] を指定し（service = auth-proxy など）、権限レベルを 15 にします。AAA サーバーを設定する方法と一般的な認証プロキシを設定する方法の詳細については、次の URL にある『Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T』の「Configuring the Authentication Proxy」を参照してください。http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_prxy_ps6441_TSD_Products_Configuration_Guide_Chapter.html

- **アカウンティング サーバー グループ**：すべての認証ルールでアカウンティングを実行する場合は、アカウンティングを実行する TACACS+ または RADIUS サーバーを識別する AAA サーバー グループ ポリシー オブジェクトのリストを指定します。サーバ グループを指定しない場合、アカウンティングは実行されません。アカウンティングを実行する場合は、必要に応じて次のオプションも設定します。
  - 複数のサーバーグループを指定する場合は、[アカウンティングにブロードキャストを使用（Use Broadcast for Accounting）] の選択を検討してください。このオプションを選択すると、アカウンティング レコードが各サーバ グループ内のプライマリ サーバに送信されます。
  - [アカウンティング通知（Accounting Notice）] オプションでは、サーバーにいつ通知するかを定義します。デフォルトでは、接続の開始時と終了時にサーバに通知されますが、終了通知だけを送信するか、またはまったく通知を送信しないかを選択できます。

- 各サービスの認証バナーをカスタマイズすることもできます。[Timeout] タブで、デフォルト アイドルと絶対セッション タイムアウトをグローバルに変更したり、インターフェイスごとに変更したりできます。

ステップ 6 [プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA]（ポリシービューでは [ルータ プラットフォーム（Router Platform）] フォルダにあります）を選択して [AAA] ポリシー ページ （3119 ページ）を開きます。[Authentication] タブで次のオプションを設定します。

- [デバイス ログイン認証の有効化（Enable Device Login Authentication）] を選択します。
- 認証を制御するサーバ グループのリスト（プライオリティ順）を入力します。通常は、AuthProxy ポリシーで使用されているのと同じ LDAP、RADIUS、または TACACS+ サーバーグループの少なくとも

一部を使用します。ただし、このポリシーでは、デバイス ログイン制御も定義するため、他のサーバグループの一部を含めることが必要にある場合があります。詳細については、[AAA] ページ - [Authentication] タブ （3120 ページ）を参照してください。

ステップ 7 HTTP 接続で認証プロキシを使用し、HTTPS 接続でもそのプロキシを使用する場合は、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP]（ポリシービューでは [ルータプラットフォーム（Router Platform）] フォルダにあります）を選択して[HTTP] ポリシー ページ （3152 ページ）を開きます。次のオプションを設定します。

- [HTTP の有効化（Enable HTTP）] と [SSL の有効化（Enable SSL）] を選択します（まだ選択されていない場合）。
- [AAA] タブで、デバイスへのログインアクセスの設定が適切であることを確認します。AAA を使用してデバイスからのアクセスを制御する場合は、デバイスへのアクセスにその AAA を使用できます。

[AAA Rules] ページ

[AAA Rules] ページを使用して、デバイス インターフェイスの AAA ルールを設定します。AAA ルールでは、ネットワーク アクセス制御（IOS デバイスの認証プロキシと呼ばれる）を設定します。これにより、ユーザはデバイスを通過するネットワーク接続を試行するときに認証が必要になります。認証されたトラフィックに、認可を受けることを要求することもできます（ユーザーが有効なユーザー名とパスワードを入力したあとで、AAA サーバーをチェックして、ユーザーにネットワークアクセスが許可されていることを確認します）。認証されていないトラフィックにもアカウンティング ルールを設定して、請求、セキュリティ、およびリソース割り当ての目的で使用できる情報を提供することもできます。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 AAA ルールを設定するための個別のポリシーとオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスをどちらも使用できる一組の AAA ルールになりました（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 （14 ページ）を参照してください）。ポリシービューでは、IPv4 および統合バージョンの AAA ポリシータイプが提供されています。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが提供されています（IPv4 ルールから統合ルールへの変換 （792 ページ）を参照）。次の説明は、特に明記されている場合を除き、AAA ルールテーブルのすべてのバージョンに適用されます。IPv4 AAA ルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらのポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合 AAA ルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらの共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれなくなります。

AAAルールの設定は複雑であり、オペレーティングシステムによって大きく異なります。AAAルールを設定する場合には、次の項をよく読んでください。

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）
- IOS デバイスの AAA ルールの設定 （877 ページ）

ヒント　ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、 ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

ナビゲーション パス

[AAA Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで [ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [AAAルール（AAA Rules）] を選択します。

関連項目

- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）
- ルール テーブルの使用 （764 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *177 : [AAA Rules]* ページ

要素	説明
[すべての行を展開する（Expand all rows）]/[すべての行を折りたたむ（Collapse all rows）]	ルールテーブルのすべてのセクションを展開または折りたたむには、これらのボタンを使用します。 （注） ボタンは、アクセスルールテーブルの上にある [フィルタ（Filter）] 領域の右上隅にあります。
[競合インジケータ（Conflict Indicator）] アイコン	競合を識別し、競合のタイプをすばやく視覚的に表現します。競合の種類や、この列から実行できるアクションなどの詳細については、自動競合検出について （950 ページ）を参照してください。
番号	順序が付けられたルール番号。
許可（Permit）	定義済みのトラフィックをルールの対象とするか（[Permit]）、またはルールを免除するか（[Deny]）。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。
ソース	このルールのトラフィック ソース。つまり、ネットワーク、セキュリティ グループ（ASA 9.0 以降のみ）、およびユーザーになります。複数のエントリは、テーブル セル内の個別の行に表示されます。
宛先	このルールの宛先。つまり、ネットワークおよびセキュリティ グループになります（ASA 9.0 以降のみ）。複数のエントリは、テーブル セル内の個別の行に表示されます。
サービス	ルールが適用されるトラフィックのプロトコルおよびポートを指定するサービスまたはサービス オブジェクト。複数のエントリは、テーブル セル内の個別の行に表示されます。サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

要素	説明
アクション	このルールで定義される AAA 制御のタイプ： • [Authenticate]：デバイスから接続を確立するユーザは、ユーザ名とパスワードで認証される必要があります。認証を必要とするプロトコルは、[Service] フィールド（ASA/PIX/FWSM デバイスの場合）または [AuthProxy] 方式（IOS デバイスの場合）で定義します。 • [Authorize]：認証済みユーザは、接続の確立が許可されていることを確認するために AAA サーバでもチェックされます（ASA/PIX/FWSM だけ）。 • [Account]：識別されたトラフィックのアカウンティング レコードが AAA サーバに送信されます（ASA/PIX/FWSM だけ）。 既存の AAA ルールの [アクション（Action）] セルを右クリックし、[アクションの編集（Edit Action）] を選択して、選択を変更できます。詳細については、[Edit AAA Option] ダイアログボックス （893 ページ）を参照してください。
[AAA方式（AAA Method）]（IOS） （ASA 9.0 以降のデバイスには表示されません）	このルールの認証方法：Web 認証プロキシ（認証プロキシ）、HTTP 基本認証、または Windows NT LAN Manager（NTLM）
AuthProxy	認証プロキシ方式を使用した認証を必要とするプロトコル。このことは、IOS デバイスにだけ適用されます。 既存の AAA ルールの [認証プロキシ（AuthProxy）] セルを右クリックし、[認証プロキシの編集（Edit AuthProxy）] を選択して、選択を変更できます。詳細については、[AuthProxy] ダイアログボックス （893 ページ）を参照してください。
Server Group	ルールで定義された認証、許可、またはアカウンティングのサポートを提供する AAA サーバ グループ。このグループは、ASA/PIX/FWSM デバイスの場合だけ使用されます。これらのルールで使用する IOS デバイスの AAA サーバの設定については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。 既存の AAA ルールの [サーバーグループ（Server Group）] セルを右クリックし、[サーバーグループの編集（Edit Server Group）] を選択して、選択を変更できます。詳細については、[Edit Server Group] ダイアログボックス （894 ページ）を参照してください。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	ルールの説明（ある場合）。
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
ルールテーブルの下のページ要素	
クエリ	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。 ポリシー クエリー レポートの生成 （793 ページ）を参照してください
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。 ルール テーブルの項目の検索と置換 （777 ページ）を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。
[Add Row] ボタン	[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、 ルールの追加および削除 （766ページ）を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、 ルールの編集 （767 ページ）を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

右クリックメニュー

右クリックメニューも使用できます。このメニューから、上記の機能の多くにアクセスできます。表示されるオプションは、右クリックした場所によって異なります。

- テーブル内のルールを右クリックすると、右クリックした特定のテーブルセルに関連した編集機能がオプションに含められる場合があります。たとえば、[サーバーグループ（Server

Group）] セルを右クリックすると、コマンド「Edit Server Group」が含められます。詳細については、ルールの編集 （767 ページ）を参照してください。

- [ルールの結合（Combine Rules）] オプションも右クリックメニューに含まれています。詳細については、ルールの結合 （785 ページ）を参照してください。

[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス

[Add AAA Rules]/[Edit AAA Rules] ダイアログボックスを使用して、AAA ルールを追加および編集します。AAA ルールの設定は、このダイアログボックスに単に入力するよりも複雑であり、オペレーティング システムによって大きく異なります。AAA ルールを設定する場合には、次の項をよく読んでください。

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）
- IOS デバイスの AAA ルールの設定 （877 ページ）

ナビゲーション パス

[AAA Rules] ページ （880 ページ）から、[行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）

フィールド リファレンス

表 *178 : [Add AAA Rules]/[Edit AAA Rules]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

要素	説明
Action（[Permit]/[Deny]）	定義済みのトラフィックがルールの対象となるか（[Permit]）、またはルールが免除されるか（[Deny]）。 たとえば、HTTP サービスを使用した宛先への 10.100.10.0/24 ネットワークに認証拒否ルールを作成した場合、このネットワーク上のユーザは HTTP 要求時にデバイスでの認証を要求されません。

要素	説明
ソース	

要素	説明
	このルールのトラフィック ソースを提供します。ネットワーク、セキュリティ グループ、およびユーザーになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 • ネットワーク – さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイス オブジェクトを送信元として選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。 「All-Address」オブジェクトは、ルールを特定のホスト、ネットワーク、またはインターフェイスに制限しません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IPv4 または IPv6 アドレスです。 （注） 完全修飾ドメイン名（FQDN）は、FQDN ネットワーク/ホスト オブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを提供することによってのみ指定できます。FQDN を直接入力することはできません。 これらの定義の詳細については、ネットワーク/ホストオブジェクトについて （391 ページ）、ポリシー定義中の IP アドレスの指定 （401 ページ）、およびインターフェイス ロール オブジェクトについて （381 ページ）を参照してください。 • セキュリティ グループ（ASA 9.0 以降）– ルールについて、1 つ以上のソースセキュリティ グループの名前またはタグ番号を入力するか選択します（存在する場合）。セキュリティ グループの詳細については、ポリシーでのセキュリティ グループの選択 （865 ページ）、TrustSec ベースのファイアウォール ルールの設定 （866 ページ）、およびセキュリティ グループ オブジェクトの作成 （863 ページ）を参照してください。 • ユーザー：ルールについて、Active Directory（AD）ユーザー名、ユーザー グループ、またはアイデンティティ ユーザー グループ オブジェクトを入力するか選択します（存在する場合）。次のものを組み合わせて入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。

要素	説明
	詳細については、以下を参照してください。 • ポリシーでのアイデンティティ ユーザの選択 （835 ページ） • アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ） • アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ） （注） これらのフィールドのいずれかに、項目をカンマで区切って複数の値を入力します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックです。
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。送信元と同様に、ネットワークおよびセキュリティグループ（ASA 9.0 以降）タイプの 1 つ以上の宛先について、値またはオブジェクト名を入力するかオブジェクトを選択できます。

要素	説明
サービス	動作対象のトラフィックタイプを定義するサービス。サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。 項目をカンマで区切って複数の値を入力します。 サービスタイプは、デバイスタイプに基づいて慎重に選択することが重要です。 • IOS デバイスの場合、ダイアログボックスの下部で、認可プロキシのチェックボックスを使用して選択したプロトコルだけが AAA 制御に使用されるため、IP をプロトコルとして使用できます。 • ASA、PIX、およびFWSMデバイスの場合、どのタイプのトラフィックにも認証を強制できますが、セキュリティアプライアンスでプロンプトが表示されるのは、HTTP/HTTPS、FTP、および Telnet トラフィックの場合だけです。これらのサービス以外のサービスを指定した場合、ユーザは、これらのサービスのいずれかを試して認証に成功するまではアプライアンスから接続を確立できません。 アカウンティングのルールだけの場合は、レコードを作成する TCP または UDP プロトコルを指定できます。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポートリスト オブジェクトの理解と指定 （418 ページ）を参照してください。 （注） PIX 6.3 および FWSM デバイスには問題があるため、送信元ポートを使用してサービスを指定した場合、トラフィックは認証されません。そのため、これらのデバイス タイプのルールから CLI が生成される場合、送信元ポートは無視されます。
インターフェイス	ユーザの認証、許可、またはアカウンティングを実行するインターフェイスを識別するインターフェイスまたはインターフェイス ロール。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか新しいインターフェイス ロール オブジェクトを作成します。 ASA および PIX デバイス上の認証ルールの場合、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA ファイアウォール（AAA Firewall）] ポリシーを使用して、このインターフェイスによる HTTP/HTTPS トラフィックの認証方法を変更できます。インターフェイスを HTTP/HTTPS リスニング ポートとして設定すると、認証のユーザ エクスペリエンスを向上できます。詳細については、ユーザの認証方法について （871 ページ）および[AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。

要素	説明
[認証アクション（Authentication Action）]、[許可アクション（Authorization Action）]、および [アカウンティングアクション（Accounting Action）] チェックボックスでは、デバイスに生成されるルールのタイプを定義します。タイプごとに異なるコマンドセットが生成されますが、複数のオプションを選択すると、このダイアログボックスの他の選択肢は、選択したすべてのアクションでサポートされる選択肢に制限されます。 既存の AAA ルールの [アクション（Action）] セルを右クリックし、[アクションの編集（Edit Action）] を選択して、選択を変更できます。詳細については、[Edit AAA Option] ダイアログボックス （893 ページ）を参照してください。	
認証アクション（Authentication Action） ユーザーアイデンティティ（User-Identity）	• [認証（Authentication）]：ユーザーはデバイスから接続を確立するためにユーザー名とパスワードを入力する必要があります。ASA、PIX、および FWSM デバイスの場合、[Services] フィールドに入力した情報によって、認証を必要とするプロトコルが決まりますが、プロンプトが表示されるのは、HTTP、HTTPS、FTP、および Telnet 接続の場合だけです。IOS デバイスの場合、いずれのプロトコルが認証を必要とするかは、ダイアログボックスの下部で選択した認可プロキシのチェックボックスに基づきます。 • User-Identity（ASA 8.4(2+) のみ）：ASA デバイスでは、[Authentication Action] を選択した場合、[User-Identity] も選択できます。このオプションは、デバイスが、AAA ルールの AAA サーバーグループ設定の代わりに、アイデンティティ オプション ポリシーで定義されたアイデンティティ ファイアウォール ドメイン マッピングを使用してユーザーを認証する必要があることを示します。ユーザーがドメイン名を入力すると、そのドメインに関連付けられた AD サーバーが照会されます。それ以外の場合は、デフォルトドメインに関連付けられた AD サーバーが照会されます。Active Directory サーバおよびエージェントの識別 （818 ページ）を参照してください。
Authorization Action（PIX/ASA/FWSM）	[Authorization]：認証に成功すると、ユーザが要求した接続の確立を許可されているかどうかを確認するために AAA サーバもチェックされます。認証ルールに RADIUS サーバを指定した場合は、認可ルールを設定しなくても認可が実行されます。TACACS+ サーバを使用している場合は、認可ルールを別途作成する必要があります。

要素	説明
Accounting Action（PIX/ASA/FWSM）	[Accounting]：アカウンティング レコードが [Services] フィールドで指定された TCP および UDP プロトコルの TACACS+ または RADIUS サーバに送信されます。認証も設定する場合、これらのレコードはユーザ単位です。認証を設定しない場合は IP アドレスに基づきます。IOS デバイスの場合、アカウンティングは、AAA ルールではなく [ファイアウォール（Firewall）]>[設定（Settings）]>[ScanSafe Web セキュリティ（ScanSafe Web Security）] ポリシーで設定され、認証プロキシに選択したプロトコルにだけ適用されます。
AAA Server Group（PIX、ASA、FWSM）	ルールで定義されるトラフィックの認証、許可、またはアカウンティングを提供する AAA サーバを定義する AAA サーバ グループ ポリシー オブジェクト。ポリシーオブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストから名前を選択するか、新しいオブジェクトを作成します。 ルールに定義されているすべてのアクションを実行できるサーバのタイプを選択する必要があります。たとえば、（デバイスに定義されている）ローカル データベースでは、認可サービスを提供できません。認証に RADIUS サーバを使用する場合、認可サービスは自動的に提供されますが、RADIUS サーバを使用する認可ルールは定義できません。 同じ送信元/宛先ペアに対する異なるアクションに対して、複数のサーバ グループを混在させて使用できます。このことを行うには、認証、許可、アカウンティング アクションを用途に応じて組み合わせ、個別のルールを作成します。AAA サーバ グループ オブジェクトの詳細については、AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）を参照してください。 **ヒント** • [Authenticate] アクションと [User-Identity] を選択し、[Authorization] または [Accounting] アクションを選択しなかった場合、ここで指定したサーバは無視されます。検証時の警告を防止するため、サーバは選択しないでください。 • IOS デバイスの AAA サーバ グループは、他のポリシーで定義されます。設定の詳細については、IOS デバイスの AAA ルールの設定（877 ページ）を参照してください。 • 既存の AAA ルールの [サーバーグループ（Server Group）] セルを右クリックし、[サーバーグループの編集（Edit Server Group）] を選択して、選択を変更できます。詳細については、[Edit Server Group] ダイアログボックス （894 ページ）を参照してください。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用（304 ページ）を参照してください。
Method (IOS) （ASA 9.0 以降のデバイスでは表示されません）	認証プロキシ、HTTP Basic、または NTLM を選択します。 認証プロキシを選択する場合、次のオプションを使用できます。 • HTTP • FTP • Telnet 認証プロキシを使用して認証を強制するプロトコルを指定します。HTTP を選択した場合は、デバイスで SSL をイネーブルにして、HTTPS 認証プロキシを設定することもできます。詳細については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。 既存の AAA ルールの [認証プロキシ（AuthProxy）] セルを右クリックし、[認証プロキシの編集（Edit AuthProxy）] を選択して、選択を変更できます。詳細については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。

[Edit AAA Option] ダイアログボックス

[AAAオプションの編集（Edit AAA Option）] ダイアログボックスを使用して、ルールが認証（ユーザ ID あり、またはなし）、許可、またはアカウンティングのうち、いずれのアクションを実行するかを選択します。認可ルールとアカウンティング ルールは、ASA、PIX、および FWSM デバイスでだけ機能します。これらのオプションの詳細については、次の項の関連する説明を参照してください。

- [Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）
- AAA ルールについて （869 ページ）

ナビゲーション パス

（[AAA Rules] ページ （880 ページ）で）AAA ルール内の [アクション（Action）] セルを右クリックし、[AAAの編集（Edit AAA）] を選択します。

[AuthProxy] ダイアログボックス

[AuthProxy] ダイアログボックスを使用して、AAA ルール内の認可プロキシ設定を編集します。IOS デバイスの場合、認証プロキシを使用して認証を強制するプロトコル（HTTP、FTP、または Telnet）を選択します。HTTP を選択した場合は、デバイスで SSL をイネーブルにして、

HTTPS 認証プロキシを設定することもできます。詳細については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。

ナビゲーション パス

（[AAA Rules] ページ （880 ページ）で）AAA ルール内の [AuthProxy] セルを右クリックし、[AuthProxyの編集（Edit AuthProxy）] を選択します。

[Edit Server Group] ダイアログボックス

[Edit Server Group] ダイアログボックスを使用して、AAA ルールで使用する AAA サーバ グループを編集します。AAA サーバ グループは、ルールで定義されたトラフィックの認証、許可、またはアカウンティングを提供する AAA サーバを提供します。ポリシーオブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストから名前を選択するか、または新しいオブジェクトを作成します。AAA サーバ グループ オブジェクトの詳細については、AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）を参照してください。

ルールに定義されているすべてのアクションを実行できるサーバのタイプを選択する必要があります。たとえば、（デバイスに定義されている）ローカルデータベースでは、認可サービスを提供できません。認証に RADIUS サーバを使用する場合、認可サービスは自動的に提供されますが、RADIUS サーバを使用する認可ルールは定義できません。[Add AAA Rule]/[Edit AAA Rule] ダイアログボックス （885 ページ）とは異なり、このダイアログボックスでは選択内容は検証されません。

（注） この設定は、ASA、PIX、および FWSM デバイスにだけ適用されます。IOS デバイスの AAA サーバ グループは、他のポリシーで定義されます。設定の詳細については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。

ナビゲーション パス

（[AAA Rules] ページ （880 ページ）で）AAA ルール内の [サーバーグループ（Server Group）] セルを右クリックし、[サーバーグループの編集（Edit Server Group）] を選択します。

AAA ファイアウォール設定ポリシー

AAA ファイアウォール設定ポリシーの設定は、AAA ルールの動作に影響を及ぼします。

ここでは、次の内容について説明します。

- [AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）
- [AAA Firewall] ページの [MAC-Exempt List] タブ （902 ページ）
- [AAA] ページ （905 ページ）

[AAA Firewall] 設定ページの [Advanced Setting] タブ

AAA ファイアウォール設定ポリシーを使用して、AAA ルール ポリシーの動作を改良するためのオプション設定を指定します。ここでは、[Advanced Setting] タブで使用できる設定について説明します。[MAC Exempt List] タブの詳細については、[AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）を参照してください。

ナビゲーション パス

[AAA Firewall] 設定ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ASA、PIX、または FWSM デバイスを選択し、**[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** を選択します。必要に応じて [詳細設定（Advanced Setting）] タブを選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）]** の順に選択します。新しいポリシーを作成するか既存のポリシーを選択し、必要に応じて [詳細設定（Advanced Setting）] タブを選択します。
- （マップビュー）ASA、PIX、または FWSM デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAAファイアウォール（AAA Firewall）]** を選択し、必要に応じて [詳細設定（Advanced Setting）] タブを選択します。

関連項目

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）

フィールド リファレンス

表 *179 : [AAA Firewall]* 設定ページの *[Advanced Setting]* タブ

要素	説明
Use Secure HTTP Authentication	セキュリティ アプライアンスを通過する HTTP 要求を行うユーザが、まず SSL（HTTPS）を使用してセキュリティ アプライアンスで認証される必要があるかどうか。ユーザはユーザ名とパスワードの入力を要求されます。 セキュアな HTTP 認証を使用すると、HTTP ベースの Web 要求にセキュリティ アプライアンスの通過を許可する前に、セキュリティ アプライアンスに対するユーザ認証を安全な方法で実行できます。これは HTTP カットスルー プロキシ認証とも呼ばれます。 このオプションを選択する場合は、アクセス ルールによって HTTPS トラフィック（ポート 443）がブロックされないこと、および PAT 設定にもポート 443 が含まれていることを確認してください。また、許可される同時認証の最大数は 16 であり、ユーザー認証のタイムアウトに 0 を設定（**[プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）]** ポリシーで **timeout uauth 0** を設定）すると、ユーザーが繰り返し認証を要求され、ネットワーク機能が中断することに注意してください。 **ヒント** このオプションを選択しない場合、HTTP 認証では、ユーザ名とパスワードがクリア テキストで送信されます。
Enable Proxy Limit Maximum Concurrent Proxy Limit per User	プロキシ接続を許可するかどうか。プロキシをイネーブルにする場合は、ユーザごとに許可するプロキシ接続の数に制限を設定する必要があります（1 ～ 128）。デバイスのデフォルトは 16 ですが、数を指定する必要があります。

要素	説明
仮想HTTPの有効化（Enable Virtual HTTP）	仮想 HTTP サーバーを設定するかどうかを指定します。この機能を使用すると、AAA 認証を必要とするすべての HTTP 接続が、ASA 上の仮想 HTTP サーバーにリダイレクトされます。ASA により、AAA サーバーのユーザー名とパスワードの入力を求めるプロンプトが表示されます。AAA サーバーがユーザーを認証すると、ASA は HTTP 接続を元のサーバーにリダイレクトして戻しますが、AAA サーバーのユーザー名とパスワードは含めません。HTTP パケットにユーザー名とパスワードが含まれていないため、HTTP サーバーによりユーザーに HTTP サーバーのユーザー名とパスワードの入力を求めるプロンプトが別途表示されます。詳細については、ユーザの認証方法について （871 ページ）を参照してください。 着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセスルールに、宛先インターフェイスとして仮想 HTTP アドレスを追加する必要もあります。さらに、NAT が必要ない場合であっても、仮想 HTTP IP アドレスに対するスタティック NAT ルールを追加する必要があります。通常は、アイデンティティ NAT ルールが使用されます（アドレスをそれ自身に変換）。 発信ユーザについては、トラフィックに明示的な許可がありますが、内部インターフェイスにアクセス ルールを適用する場合は、必ず仮想 HTTP アドレスへのアクセスを許可する必要があります。スタティック NAT ルールは必要ありません。 仮想 HTTP サーバーを設定するには、次の手順を実行します。 **1.** [仮想HTTPの有効化（Enable Virtual HTTP）] チェックボックスをオンにします。 **2.** IP アドレスを入力するか、または仮想 HTTP サーバーを表すネットワーク/ホストオブジェクトを選択します。このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。たとえば、外部サーバにアクセスするときに内部アドレス用の NAT を実行し、仮想 HTTP サーバへの外部アクセスを可能にする場合は、仮想 HTTP サーバのアドレスとして、グローバル NAT アドレスをいずれか 1 つ使用できます。 **3.** （任意）リダイレクションが自動的に実行されないテキストベースのブラウザを使用している場合は、[警告（Warning）] チェックボックスをオンにします。これにより、HTTP 接続がリダイレクトされる際に、ユーザにそのことを通知するためのアラートがイネーブルになります。

要素	説明
仮想Telnetの有効化（Enable Virtual Telnet）	仮想 Telnet サーバーを設定するかどうかを指定します。 認証が済んでいないユーザーが仮想 Telnet IP アドレスに接続すると、ユーザーはユーザー名とパスワードを求められ、その後 AAA サーバーにより認証されます。ユーザーが認証されると、「Authentication Successful」というメッセージが表示されます。これで、ユーザは認証が必要な他のサービスにアクセスできます。 着信ユーザ（セキュリティの低い方から高い方へ向かう）については、送信元インターフェイスに適用されるアクセスルールに、宛先インターフェイスとして仮想 Telnet アドレスを追加する必要もあります。さらに、NAT が不要な場合でも、仮想 Telnet IP アドレスに対するスタティック NAT ルールを追加する必要があります。通常は、アイデンティティ NAT ルールが使用されます（アドレスをそれ自身に変換）。 発信ユーザについては、トラフィックに明示的な許可がありますが、内部インターフェイスにアクセス ルールを適用する場合は、必ず仮想 Telnet アドレスへのアクセスを許可する必要があります。スタティック NAT ルールは必要ありません。 仮想 Telnet サーバーを設定するには、次の手順を実行します。 **1.** [仮想Telnetの有効化（Enable Virtual Telnet）] チェックボックスをオンにします。 **2.** IP アドレスを入力するか、または仮想 Telnet サーバーを表すネットワーク/ホストオブジェクトを選択します。このアドレスは必ず、ASA にルーティングされる未使用のアドレスにしてください。たとえば、外部サーバーにアクセスするときに内部アドレス用の NAT を実行し、仮想 Telnet サーバーへの外部アクセスを可能にする場合は、仮想 Telnet サーバーのアドレスとして、グローバル NAT アドレスの 1 つを使用できます。

要素	説明
[Interactive Authentication] テーブル（ASA/PIX 7.2.2+）	このテーブルを使用して、認証対象のHTTPまたはHTTPSトラフィックを受信するインターフェイスを指定します。AAAルールがこのテーブルで指定されたインターフェイスにおけるこれらのプロトコルの認証を必要とする場合、ユーザには、アプライアンスで使用されるデフォルトの認証ページではなく、改良された認証Webページが表示されます。これらのページは、デバイスへの直接接続の認証にも使用されます。 • インターフェイスをテーブルに追加するには、[行の追加（Add Row）] ボタンをクリックし、[Interactive Authentication Configuration] ダイアログボックス （900 ページ）に入力します。 • 設定を編集するには、設定を選択して [行の編集（Edit Row）] ボタンをクリックします。 • 設定を削除するには、設定を選択して [行の削除（Delete Row）] ボタンをクリックします。
Disable FTP Authentication Challenge Disable HTTP Authentication Challenge Disable HTTPS Authentication Challenge Disable Telnet Authentication Challenge （すべて FWSM 3.x+ だけ）	示されているプロトコルの認証チャレンジをディセーブルにするかどうか。デフォルトでは、AAAルールが新しいセッションにおけるトラフィックの認証を強制し、トラフィックのプロトコルがFTP、Telnet、HTTP、またはHTTPSの場合に、FWSMはユーザにユーザ名とパスワードの入力を要求します。 これらのプロトコルの1つ以上に対して認証チャレンジをディセーブルにすることが必要になる場合もあります。特定のプロトコルの認証チャレンジをディセーブルにすると、そのプロトコルを使用しているトラフィックは、以前に認証されたセッションに属している場合にだけ、許可されます。この認証は、認証チャレンジがイネーブルのままになっているプロトコルを使用するトラフィックによって完了できます。たとえば、FTPの認証チャレンジをディセーブルにすると、トラフィックが認証 AAA ルールに含まれている場合に、FWSMではFTPを使用した新しいセッションを拒否します。認証チャレンジがイネーブルになっているプロトコル（HTTP など）を使用してユーザがセッションを確立した場合、FTP トラフィックは許可されます。

要素	説明
Clear Connections When Uauth Timer Expires table （FWSM 3.2+ だけ）	このテーブルを使用して、ユーザー認証がタイムアウトするか、または **clear uauth** コマンドで認証セッションをクリア後すぐにアクティブな接続を強制的に終了するインターフェイスと送信元アドレスを指定します。（ユーザー認証のタイムアウトは、**[プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）]** ポリシーで定義します）。このテーブルにインターフェイスと送信元アドレスのペアがない場合、ユーザー認証セッションが期限切れになっても、アクティブなセッションは終了しません。 • インターフェイスと送信元アドレスのペアを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Clear Connection Configuration] ダイアログボックス （901 ページ）に入力します。 • 設定を編集するには、設定を選択して [行の編集（Edit Row）] ボタンをクリックします。 • 設定を削除するには、設定を選択して [行の削除（Delete Row）] ボタンをクリックします。

[Interactive Authentication Configuration] ダイアログボックス

[Interactive Authentication Configuration] ダイアログボックスを使用して、HTTP または HTTPS トラフィックを受信してネットワーク ユーザを認証するようにインターフェイスを設定します。リスニング ポートで使用される認証 Web ページでは、これらのプロトコルに使用されるデフォルトの認証ページと比べてユーザエクスペリエンスが向上します。認証ページは、デバイスへの直接接続に使用されます。また、リダイレクション オプションを選択し、かつ、AAA ルール ポリシーで HTTP/HTTPS ネットワーク アクセス認証が必要とされている場合、認証ページはスルー トラフィックにも使用されます。詳細については、 ユーザの認証方法について （871 ページ）を参照してください。

ナビゲーション パス

[AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）に移動し、双方向認証テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- AAA ルールについて （869 ページ）
- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）

フィールド リファレンス

表 *180 : [Interactive Authentication Configuration]* ダイアログボックス

要素	説明
プロトコル	受信するプロトコル（[HTTP] または [HTTPS]）。インターフェイスで両方のプロトコルを受信する場合は、インターフェイスをテーブルに 2 回追加します。
インターフェイス	受信者をイネーブルにするインターフェイスまたはインターフェイスロール。インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。
[ポート（Port）]	デフォルト ポート（80（HTTP）および 443（HTTPS））を使用しない場合に、セキュリティ アプライアンスがこのプロトコルを受信するポート番号。
Redirect network users for authentication request	デバイスから要求しているユーザを、セキュリティ アプライアンスが提供する認証 Web ページにリダイレクトするかどうか。このオプションを選択しない場合、インターフェイスに向けられたトラフィックに対してだけ改良された認証 Web ページが表示されます。

[Clear Connection Configuration] ダイアログボックス

[接続設定のクリア（Clear Connection Configuration）] ダイアログボックスを使用して、ユーザー認証がタイムアウトするか、または **clear uauth** コマンドで認証セッションをクリア後すぐにアクティブな接続を閉じる送信元アドレスを指定します。これらのセッションをクリアするインターフェイスを指定する必要があります。これらの設定は、FWSM 3.2+デバイスだけに使用されます。

ユーザー認証のタイムアウトは、**[プラットフォーム（Platform）]>[セキュリティ（Security）]>[タイムアウト（Timeouts）]** ポリシーで定義します。

ナビゲーション パス

[AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）に移動し、[Uauthタイマーの終了時に接続をクリア（Clear Connections When Uauth Timer Expires）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の項目を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 181 : [Clear Connection Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	設定を行うインターフェイスまたはインターフェイス ロール。名前を入力します。または [選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択するか、または新しいロールを作成します。複数のエントリを指定する場合は、カンマで区切ります。
送信元 IP アドレス/ネットマスク	ユーザ認証のタイマーが切れるとすぐに接続をクリアするホストまたはネットワーク アドレス。リストには、ホスト IP アドレス、ネットワーク アドレス、アドレス範囲、またはネットワーク/ホスト オブジェクトを含めることができます。複数のアドレスを指定する場合は、カンマで区切ります。アドレスを入力する方法の詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

[AAA Firewall] ページの [MAC-Exempt List] タブ

ASA、PIX、および FWSM 3.x+ デバイスの場合、[AAA Firewall] 設定ポリシーの [MAC Exempt List] タブを使用して、認証と認可を免除するホストを指定します。たとえば、セキュリティ アプライアンスが特定のネットワーク上で発信される TCP トラフィックを認証し、特定のサーバからの認証されていない TCP 接続を許可する場合は、そのサーバの MAC アドレスからのトラフィックを許可するルールを作成します。

マスクを使用して、MACアドレスのグループのルールを作成できます。たとえば、MACアドレスが 0003.e3 で始まるすべての Cisco IP Phone を免除する場合は、マスク ffff.ff00.0000 を使用して 0003.e300.0000 の許可ルールを作成します（マスクの f はアドレス内の対応する数と一致し、0 はすべてと一致します）。

拒否ルールが必要になるのは、MACアドレスのグループを許可し、許可されたグループ内に、認証と認可を使用する必要があるいくつかのアドレスがある場合だけです。拒否ルールはトラフィックを禁止しません。ホストに通常の認証と認可を要求するだけです。たとえば、00a0.c95d で始まる MAC アドレスを持つすべてのホストを許可し、00a0.c95d.0282 に認証と認可の使用を強制する場合は、次のルールを順番に入力します。

1. Deny 00a0.c95d.0282 ffff.ffff.ffff
2. Permit 00a0.c95d.0000 ffff.ffff.0000

ポリシーをデバイスに展開すると、**mac-list** および **aaa mac-exempt** コマンドを使用してこれらのエントリが設定されます。

ヒント MAC 免除リストで最初に一致したものが処理されます。このため、エントリの順序が重要となります。MAC アドレスのグループを許可し、その一部を拒否する場合は、許可ルールの前に拒否ルールを配置する必要があります。ただし、Security Manager では、MAC 免除ルールを順序付けることはできません。ルールは示されている順に実装されます。テーブルをソートすると、ポリシーが変更されます。エントリが相互に依存していない場合、このことは重要ではありません。依存している場合は、行を正しい順序で入力してください。

ナビゲーション パス

[MAC Exempt List] タブにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ASA、PIX、または FWSM デバイスを選択し、[ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）] を選択します。[MAC-Exemptリスト（MAC-Exempt List）] タブを選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [AAAファイアウォール（AAA Firewall）] の順に選択します。新しいポリシーを作成するか既存のポリシーを選択し、[MAC-Exemptリスト（MAC-Exempt List）] タブを選択します。
- （マップビュー）ASA、PIX、または FWSM デバイスを右クリックし、[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAAファイアウォール（AAA Firewall）] を選択し、次に [MAC-Exemptリスト（MAC-Exempt List）] タブを選択します。

関連項目

- ASA、PIX、および FWSM デバイスの AAA ルールの設定 （873 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *182 : [AAA Firewall]* 設定ページの *[MAC-Exempt List]* タブ

要素	説明
MAC-Exempt List Name	MAC 免除リストの名前。

要素	説明
[MAC Exempt List] テーブル	実装する MAC 免除ルール。テーブルに MAC アドレスとマスク（16 進数）、およびそれらを許可するか（認証と認可を免除するか）または拒否するか（標準の認証と認可を強制するか）が表示されます。エントリはデバイスはによって順番に処理され、最適な一致ではなく、最初に一致するものが使用されます。 • 免除ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Firewall AAA MAC Exempt Setting] ダイアログボックス （904 ページ）に入力します。 • 免除ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • 免除ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Firewall AAA MAC Exempt Setting] ダイアログボックス

[Firewall AAA MAC Exempt Setting] ダイアログボックスを使用して、[MAC Exempt List] テーブルの免除エントリを追加および編集します。セキュリティアプライアンスは、許可された MAC アドレスに関連付けられているホストの認証と認可をスキップします。

ナビゲーション パス

[AAA Firewall] ページの [MAC-Exempt List] タブ （902 ページ）に移動し、[MAC免除リスト（MAC Exempt List ）] テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の項目を選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 183 : [Firewall AAA MAC Exempt Setting] ダイアログボックス

要素	説明
操作	指定した MAC アドレスを使用するホストに対して実行するアクション： • [Permit]：ホストの認証と認可を免除します。 • [Deny]：ホストに認証と認可を強制します。
MAC アドレス	標準的な 12 桁の 16 進形式のホストの MAC アドレス（00a0.cp5d.0282 など）。完全な MAC アドレスまたはアドレスの一部を入力できます。 アドレスの一部を入力する場合、照合しない桁には 0 を入力できます。

要素	説明
MAC Mask	MAC アドレスに適用するマスク。f は数と正確に一致し、0 はその位置の任意の数と一致します。 • アドレスの完全一致を指定するには、ffff.ffff.ffff を入力します。 • アドレス パターンを照合するには、任意の文字を照合する桁に 0 を入力します。たとえば、ffff.ffff.0000 は、最初の 8 桁が同じであるすべてのアドレスと一致します。

[AAA] ページ

AAA ファイアウォール設定プロキシを使用して、認証プロキシに使用するサーバーやバナーを指定したり、デフォルト以外のタイムアウト値を設定したりします。IOS デバイスの認証プロキシは、ユーザが IOS デバイスから HTTP、Telnet、または FTP 接続を確立しようとするときにユーザにログインと認証を強制するサービスです。ここでの設定は、AAA ルールと組み合わせて機能します。AuthProxy 設定は、AAA ルールでこれらのサービスのいずれかにユーザ認証が必要とされている場合にだけ適用されます。

このポリシーの設定が **[ファイアウォール（Firewall）] > [AAAルール（AAA Rules）]** ポリシーと矛盾していないことを確認してください。さらに、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]** ポリシーを使用して、ユーザーアクセスの認証に使用する AAA サーバーグループを定義する必要があります。このポリシーでは、許可およびアカウンティングのサーバーグループだけを定義します。HTTPS アクセスにも許可プロキシを使用する場合は、AAA ルールポリシーで HTTP 許可プロキシをイネーブルにするだけでなく、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP]** ポリシーで SSL をイネーブルにし、AAA を設定する必要があります。

ヒント AAA サーバでユーザごとに ACL を設定して、各ユーザに適用する権限を定義する必要があります。許可を設定する場合は、サービスとして [AAA] を指定し（service = AAA など）、権限レベルを 15 にします。AAA サーバーを設定する方法と一般的な認証プロキシを設定する方法の詳細については、次の URL にある『Cisco IOS Security Configuration Guide: Securing User Services, Release 12.4T』の「Configuring the Authentication Proxy」を参照してください。
http://www.cisco.com/en/US/docs/ios/sec_user_services/configuration/guide/sec_cfg_authen_proxy_ps6441_TSD_Products_Configuration_Guide_Chapter.html

ナビゲーション パス

[AAA] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [AAA]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAA]** を選択します。

関連項目

- AAA ルールについて （869 ページ）
- ユーザの認証方法について （871 ページ）
- IOS デバイスの AAA ルールの設定 （877 ページ）

フィールド リファレンス

表 *184 : AAA* ファイアウォール設定ポリシー

要素	説明
仮想 IP アドレス（Virtual IP Address）	仮想 IP アドレスは、IOS HTTP 認証とクライアント間の通信でのみ使用します。システムを正常に動作させるには、仮想 IP アドレスを設定する必要がありますが（0.0.0.0 は設定できません）、ネットワーク上の他のデバイスに同じアドレスを使用することはできません。1.1.1.1 など、割り当てられず、使用もされないゲートウェイ IP アドレスを使って設定する必要があります。
[General] タブ	
Authorization Server Groups	ユーザー単位の許可制御を提供する、LDAP、TACACS+ または RADIUS サーバーを識別する AAA サーバー グループ ポリシー オブジェクト。デバイスに定義されている LOCAL ユーザ データベースを使用することもできます。 サーバーグループオブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。グループをプライオリティ順に配置してください。認可は、最初のグループを使用して試行され、そのグループが使用できない場合は、その次のグループが使用されます。

要素	説明
Accounting Server Groups Use Broadcast for Accounting	アカウンティング サービスを提供する、LDAP、TACACS+、またはRADIUS サーバを識別する AAA サーバ グループ ポリシー オブジェクト。アカウンティングでは、請求、セキュリティ、またはリソース割り当ての目的でユーザ単位の使用情報を収集します。サーバーグループオブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 グループをプライオリティ順に配置してください。ブロードキャストオプションを選択しない場合、アカウンティングは、最初のグループを使用して試行され、そのグループが使用できない場合は、その次のグループが使用されます。 [アカウンティングにブロードキャストを使用（Use Broadcast for Accounting）]を選択した場合、アカウンティングレコードが各グループ内の最初のサーバーに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。
Accounting Notice	アカウンティング サーバ グループに送信されるアカウンティング通知のタイプ。 • [Start-stop]：ユーザ プロセスの開始時に開始アカウンティング通知を送信し、プロセスの終了時に終了アカウンティング通知を送信します。start アカウンティングレコードはバックグラウンドで送信されます。要求されたユーザ プロセスは、開始アカウンティング通知をアカウンティング サーバから受信したかどうかにかかわらず開始されます。 • [Stop-only]：要求されたユーザ プロセスの終了時に終了アカウンティング通知を送信します。 • [None]：アカウンティング レコードは送信されません。
HTTP Banner FTP Banner Telnet Banner	ユーザが指定サービスの認証を要求されたときに、認証プロキシページに表示されるバナー。 • [Disable Banner Text]：バナーは表示されません。 • [デフォルトのバナーテキストを使用（Use Default Banner Text）]：デフォルトのバナー「Cisco Systems, *router hostname* Authentication」が表示されます。 • [Use Custom Banner Text]：ユーザに表示されるテキストを入力します。
Use HTTP banner from File URL	HTTP 接続の認証に独自の Web ページを使用するかどうか。独自の HTTP バナーの URL を入力します。 HTTP バナー テキストと URL の両方を設定した場合は、URL バナーが優先されます。ただし、バナー テキストもデバイスに設定されます。

要素	説明
[Advanced] タブ	
Global Inactivity Time	セッションにユーザアクティビティがない場合に、ユーザの認証プロキシが保持される時間の長さ（分単位）。このタイマーが期限切れになると、動的なユーザ アクセス コントロール リスト（ACL）に従ってユーザ セッションがクリアされるので、ユーザは再度認証を受ける必要があります。有効な範囲は 1 ～ 2,147,483,647 です。デフォルトは 60 分です。 このタイムアウト値が**[ファイアウォール（Firewall）]>[設定（Settings）]>[インスペクション（Inspection）]**ポリシーで設定されたアイドルタイムアウト値以上であることを確認してください。アイドルタイムアウト値未満の場合は、タイムアウトしたユーザーセッションのモニタが続行され、最終的にハングする可能性があります。
Global Absolute Time	認証プロキシユーザセッションがアクティブなままでいることのできる時間の長さ（分単位）。このタイマーが期限切れになったあとは、新しいリクエストの場合と同様、ユーザセッションで接続確立のプロセス全体を実行する必要があります。有効な範囲は 0 ～ 35,791 です。デフォルトは 0 で、グローバルな絶対タイムアウトは設定されません。ユーザセッションはアクティブであるかぎり保持されます。
[Interface Timeout] テーブル	このテーブルには、グローバルタイムアウト値とは異なるタイムアウト値を設定するインターフェイスが含まれます。すべてのインターフェイスにグローバル値を使用する場合は、このテーブルに何も設定する必要はありません。 • カスタマイズされたタイムアウト値を持つインターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、 Firewall AAA IOS Timeout Value Setting （908 ページ）に入力します。 • 設定を編集するには、設定を選択して [行の編集（Edit Row）] ボタンをクリックします。 • 設定を削除するには、設定を選択して [行の削除（Delete Row）] ボタンをクリックします。

Firewall AAA IOS Timeout Value Setting

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

[Firewall AAA IOS Timeout Value Setting] ダイアログボックスを使用して、特定のインターフェイスのアイドル タイムアウト値と絶対タイムアウト値を設定します。これらの値は、[ファイアウォール（Firewall）] > [設定（Settings）] > [ScanSafe Webセキュリティ（ScanSafe Web

Security）] ポリシーの [サーバータイムアウト（Server Timeout）] タブで設定されたグローバルタイムアウト値を上書きします。

ナビゲーション パス

[AAA] ページ （905 ページ）の [詳細（Advanced）] タブで、インターフェイスのテーブルの下にある **[**行の追加（Add Row）] ボタンをクリックするか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

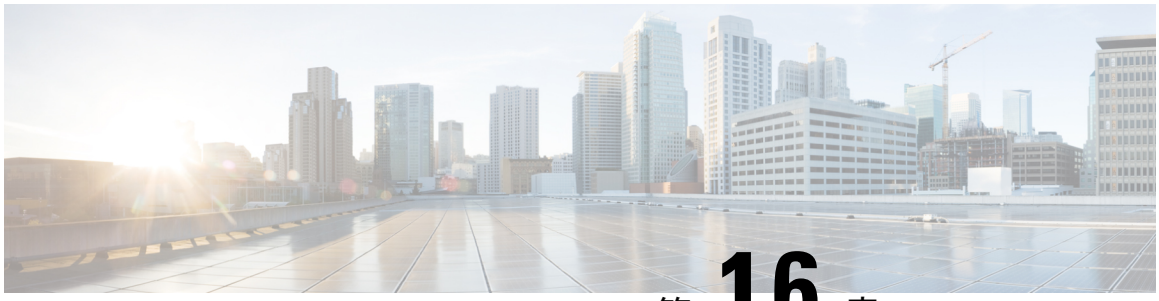
フィールド リファレンス

表 185 : [Firewall AAA IOS Timeout Value Setting] ダイアログボックス

要素	説明
インターフェイス	タイムアウト値を設定するインターフェイスまたはインターフェイスロール。インターフェイスまたはロールの名前を入力します。または、[選択（Select）] をクリックしてリストから名前を選択するか、新しいインターフェイスロールを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[Auth Proxy] タブ	
Inactivity/Cache Time	インターフェイス上のセッションにユーザ アクティビティがない場合に、ユーザの認証プロキシが保持される時間の長さ（分単位）。このタイマーが期限切れになると、動的なユーザ アクセス コントロール リスト（ACL）に従ってユーザセッションがクリアされるので、ユーザは再度認証を受ける必要があります。有効な範囲は 1 ～ 2,147,483,647 です。デフォルトは、グローバル非アクティブタイムアウト値（デフォルトは 60 分）です。
Absolute Time	認証プロキシユーザセッションをインターフェイスでアクティブなまま維持できる時間の長さ（分単位）。このタイマーが期限切れになったあとは、新しいリクエストの場合と同様、ユーザセッションで接続確立のプロセス全体を実行する必要があります。有効な範囲は 1 ～ 35,791 です。デフォルトは 0 で、絶対タイムアウトは設定されません。ユーザセッションはアクティブであるかぎり保持されます。
Authentication Proxy Method（IOS）	これらのタイムアウト値を適用するプロトコル。HTTP、FTP、または Telnet を自由に組み合わせて選択できます。
[HTTP/NTLM] タブ	[HTTP] 領域と [NTLM] 領域には、次の同じフィールドと選択項目があります。 HTTP/NTLM の [非アクティブ/キャッシュ時間（Inactivity/Cache Time）] および [絶対時間（Absolute Time）] を設定し、必要な場合には [パッシブ認証の有効化（Enable Passive Authentication）] を選択します。最後に、適用する [IDポリシー（Identity Policy）] を選択します。

要素	説明
[Method Order] タブ	使用する各方式のチェックボックスを選択し、上向きおよび下向き矢印を使用して方式を目的の順序に配置します。
[AAA Settings] タブ	[AAA設定（AAA Settings）] タブを選択して、下の説明に従い、認証、許可、アカウントの設定を指定します。
Authenticate Using	[Authenticate Using] セクションでは、認証に使用するサーバ グループを選択できます。選択肢は次のとおりです。 • なし（None）：認証を行いません。 • [デフォルト（Default）]：デフォルトの認証サーバーグループを使用します。 • [カスタム（Custom）]：ユーザーが指定した認証サーバーグループの選択を有効にします。 次に、[選択（Select）] をクリックして、サーバーグループを指定または追加します。
Authorize Exec Operation Using	[次を使用して実行操作を許可する（Authorize Exec Operation Using）] セクションでは、実行操作の許可に使用するサーバーグループを選択できます。選択肢は次のとおりです。 • [なし（None）]：許可はしません。 • [デフォルト（Default）]：デフォルトの許可サーバーグループを使用します。 • [カスタム（Custom）]：ユーザーが指定した許可サーバーグループの選択を有効にします。 次に、[選択（Select）] をクリックして、サーバーグループを指定または追加します。
Perform Exec Operation Using	[Authorize Exec Operation Using] セクションでは、実行操作の実行に使用するサーバ グループを選択できます。選択肢は次のとおりです。 • [なし（None）]：許可はしません。 • [デフォルト（Default）]：デフォルトのサーバーグループを使用します。 • [カスタム（Custom）]：ユーザーが指定したサーバーグループの選択を有効にします。次に、[選択（Select）] をクリックして、サーバーグループを指定または追加します。

要素	説明
Accounting Notice	[Accounting Notice] を使用して、アカウンティング操作を指定します。 • [なし（None）]：アカウンティング通知は行いません。 • [開始-停止（Start-stop）]：操作の最初と最後にアカウンティング通知を行います。 • [停止のみ（Stop-only）]：操作の最後にのみアカウンティング通知を行います。
Accounting Server Groups	使用するアカウンティング サーバー グループを指定します。アカウンティング サーバー グループを入力または選択します。 （注） アカウンティング サーバ グループを選択する場合、アカウンティング サーバ グループを追加することもできます。
Use Broadcast for Accounting	アカウンティング通知をブロードキャストするには、このチェックボックスを選択します。



第 16 章

ファイアウォール アクセス ルールの管理

アクセス ルールでは、トラフィックがインターフェイスを通過するために満たす必要のあるルールを定義します。着信トラフィックのルールを定義した場合、そのルールが他のどのポリシーよりも先にトラフィックに適用されます（ただし、一般的でない AAA ルールは例外です）。このため、アクセス ルールは防御の最前線となります。

デバイスの一部のタイプでは、IPv4 アクセス ルールに加えて IPv6 アクセス ルールを設定できます。サポートされているデバイスタイプについては、「Security Manager での IPv6 サポート」（8 ページ）を参照してください。

アクセス ルールの概要および使用方法については、次の項を参照してください。

- アクセス ルールについて （913 ページ）
- アクセス ルールの設定 （920 ページ）
- アクセス ルールの有効期限の設定 （942 ページ）
- アクセス コントロール ポリシー設定の指定 （943 ページ）
- 自動競合検出の使用 （950 ページ）
- ヒットカウントの詳細の表示 （960 ページ）
- ルールのインポート （966 ページ）
- 展開中のアクセス ルールの自動最適化 （973 ページ）
- [アクセスルールの追加（Add Access Rule）] ダイアログでのデフォルトのカスタマイズ （975 ページ）

アクセス ルールについて

アクセス ルール ポリシーでは、インターフェイスを通過するトラフィックを許可または拒否するルールを定義します。通常は、インターフェイスに入るトラフィックのアクセスルールを作成します。これは、特定タイプのパケットを拒否する場合、デバイスがパケットの処理に多くの時間を費やす前にパケットを拒否する方が有効なためです。

アクセス ルールは、デバイスに展開されると、インターフェイスに接続されているアクセス コントロール リスト（ACL）の 1 つ以上のエントリ（ACE）となります。通常、これらのアクセス ルールが、パケットに最初に適用されるセキュリティ ポリシーとなります。つまり、防御の最前線となります。アクセス ルールを使用して、サービス（プロトコルとポート番号）、

送信元アドレス、および宛先アドレスに基づいて、トラフィックを許可または拒否（ドロップ）することにより、望ましくないトラフィックをフィルタリングして除外します。インターフェイスに到着したパケットごとに、指定した基準に基づいてパケットを転送するかドロップするかが決定されます。Out 方向のアクセス ルールを定義した場合、パケットは、インターフェイスを出ていくときにも分析されます。

ヒント　ASA 8.3+ デバイスの場合は、グローバルなアクセス ルールを使用して、インターフェイス固有のアクセス ルールを増強できます。詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください。

アクセスルールでトラフィックを許可しても、後続のポリシーによってそのトラフィックが最終的にドロップされることがあります。たとえば、インスペクションルール、Web フィルタルール、およびゾーンベースのファイアウォールルールは、パケットがインターフェイスのアクセスルールに合格したあとに適用されます。この場合、これらの後続のルールによって、さらに深いトラフィック分析に基づいてトラフィックがドロップされることがあります。たとえば、パケット ヘッダーが検査要件を満たしていない場合や、Web 要求の URL が望ましくない Web サイトに対応している場合などです。

このため、アクセス ルールを定義する際は、作成する他のタイプのファイアウォール ルールについて慎重に検討する必要があります。検査する必要があるトラフィックに対しては、アクセスルールで全面的な拒否ルールを作成しないでください。一方、特定のホストやネットワークを起点または宛先とするサービスをどのような場合にも許可しないことがわかっている場合は、アクセス ルールを使用してトラフィックを拒否してください。

アクセスルールの順序に留意してください。つまり、デバイスは、ルールに基づいてパケットを比較するとき、上から下に検索を行い、一致した最初のルールに対するポリシーを適用します。それ以降のルールは、（最初のルールより一致率が高くても）すべて無視されます。したがって、特定のルールが無視されないようにするには、そのルールを汎用性の高いルールよりも上に配置する必要があります。IPv4 ルールがまったく一致しないケースを特定する場合、および冗長なルールを特定する場合は、自動競合検出ツールやポリシークエリツールを使用すると便利です。詳細については、自動競合検出の使用 （950 ページ）および ポリシー クエリー レポートの生成 （793 ページ）を参照してください。

次の方法でも、アクセス ルールを評価できます。

- ルールを結合する：IPv4 ルールを評価するためのツールを使用し、各ルールを結合することによって、より少ない数のルールで同じ機能を実行できます。これにより、ルールのリストが縮小され、管理が簡単になります。詳細については、ルールの結合 （785 ページ）を参照してください。
- ヒット カウントを生成する：IPv4 および IPv6 ACL のデバイスで管理されるヒット カウント統計を表示するためのツールを使用できます。これにより、ルールでトラフィックが許可または拒否された頻度がわかります。詳細については、ヒットカウントの詳細の表示 （960 ページ）を参照してください。
- CS-MARS により収集されたイベントを表示する：デバイスをモニタするように Cisco Security Monitoring, Analysis and Response System アプリケーションを設定した場合、およ

びsyslogメッセージを生成するようにルールを設定した場合は、このアプリケーションを使用して、IPv4ルールに関連するリアルタイムのイベントと過去のイベントを分析できます。詳細については、IPSシグニチャのCS-MARSイベントの表示 （3738ページ）を参照してください。

アクセス ルールの概念的な詳細については、次の項を参照してください。

- グローバル アクセス ルールについて （915ページ）
- デバイス固有のアクセス ルールの動作について （917ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918ページ）

関連項目

- アクセス ルールの設定 （920ページ）
- アクセス ルールの有効期限の設定 （942ページ）
- アクセス コントロール ポリシー設定の指定 （943ページ）
- 検出中のオブジェクト グループの展開 （806ページ）
- ルールのインポート （966ページ）
- ルールの追加および削除 （766ページ）
- ルールの編集 （767ページ）
- ルールのイネーブル化とディセーブル化 （782ページ）
- ルールの移動とルール順序の重要性 （781ページ）

グローバル アクセス ルールについて

アクセルルール（ACL）は、どのトラフィックがデバイスを通過できるかを制御するものであり、従来からデバイス インターフェイスに適用されています。ただし、ソフトウェア リリース8.3+が動作しているASAデバイスを使用している場合は、IPv4およびIPv6に対してグローバル アクセス ルールを作成することもできます。

グローバル アクセス ルールは、デバイス上のインターフェイスごとに、インターフェイスに入るトラフィックに対して処理される特殊なACLとして定義します。このため、ACLはデバイスで1回だけ設定されますが、In方向に対して定義されたインターフェイス固有のセカンダリ ACLのように機能します（グローバル ルールは常に、Out方向ではなくIn方向に適用されます）。

ASA 8.3+デバイス上のインターフェイスにトラフィックが入ると、デバイスは、ACLを適用する際に、まずインターフェイス固有のアクセス ルールをトラフィックに適用します。次に、グローバル ルールを適用します（全体的な処理については、ファイアウォール ルールの処理順序について （757ページ）を参照してください）。

着信インターフェイスに関係なくデバイスに入ってくるすべてのトラフィックに適用するルールには、グローバルルールを使用すると最適です。たとえば、常に拒否または常に許可する特定のホストまたはサブネットがあるとします。これらをグローバルルールとして作成すると、デバイス上で1回だけ設定すれば、各インターフェイスに対して繰り返し設定する必要がありません（機能的には、[All-Interfaces] ロールに対してインターフェイス固有のルールを設定した場合と同じですが、[All-Interfaces] ルールはデバイス上で 1 回だけ設定するのではなく、各インターフェイスに対して繰り返して設定します）。

ヒント　複数のデバイスに対して同じグローバル ルール セットを設定する場合は、共有ポリシーを作成して、デバイスごとにIPv4またはIPv6アクセス ルール ポリシー内に継承します。すべてのグローバル ルールを共有ポリシーの [Default] セクション内に配置する必要があります。いずれかのグローバル ルールを [Mandatory] セクションに配置した場合は、ローカルなインターフェイス固有のアクセス ルールが定義されているデバイス上でそのルールを継承できなくなります。共有ポリシーおよび継承ポリシーの詳細については、ローカルポリシーと共有ポリシー （211 ページ）およびルールの継承について （213 ページ）を参照してください。

Security Manager で ASA 8.3+ デバイスに対してアクセス ルールを設定する場合、インターフェイス固有のルールとグローバルルールは同じポリシー内に設定されます。ただし、デバイスでは常にインターフェイス固有のルールが最初に処理されるため、Security Manager ではこれらの異なるタイプのルールを混在させることはできません。そのため、1 つのデバイス上でインターフェイス固有のルールとグローバルルールの両方を設定する場合は、次の点に注意してください。

- アクセスルール ポリシー内では、常にグローバル ルールが最後に処理されます。インターフェイス固有のルールはいずれも、グローバル ルールよりも先に処理されます。
- 決められた順序に違反するようなルールの移動はできません。たとえば、インターフェイス固有のルールをグローバル ルールの下に移動したり、グローバル ルールをインターフェイス固有のルールの上に移動したりすることはできません。
- 決められた順序に違反する場所にルールを作成することはできません。たとえば、インターフェイス固有のルールを選択し、インターフェイス固有の別のルールをテーブル内でその次に配置した場合、グローバル ルールを作成することはできません。間違った種類のルールを作成しようとすると、ルールを保存するときに、Security Manager によって、ルールを最も近い有効な場所に作成できるかどうか尋ねられます。この提案を受け入れないと、ルールはテーブルに追加されません。提案された場所が不適切な場合は、ルールの作成後にいつでもルールを移動できます（ただし、ルールの順序に違反しない場合にかぎります）。
- 決められた順序に継承ポリシー内のルールが違反する場合、そのポリシーは継承できません。たとえば、デバイス ポリシー内にグローバル ルールを作成し、[Default] セクション内でインターフェイス固有のルールを含む共有ポリシーを継承しようとすると、Security Manager でそのポリシーが継承できなくなります。

- 共有ポリシーの割り当て後または継承後は、そのポリシーを使用するデバイス上のルール順序に違反するようなポリシーの編集はできません。
- グローバル ルールをサポートしていないデバイス上で、グローバル ルールを含むポリシーを割り当てまたは継承した場合、そのデバイスではすべてのグローバル ルールが無視され、設定はされません。たとえば、共有ポリシー内のグローバル ルールでホスト 10.100.10.10 からのすべてのトラフィックを許可し、そのポリシーを IOS デバイスに割り当てた場合、10.100.10.10 アクセスを許可するルールは IOS デバイス上では設定されません。そのホストからのトラフィックは、別のインターフェイス固有ポリシーか、またはデフォルトの deny all ポリシーによって処理されます。グローバル ルールをサポートしないデバイスには、グローバル ルールを含む共有ポリシーを割り当てないようにすることを推奨します。そうすれば、グローバル ルールで定義されているポリシーが、サポートされていないデバイスで設定されていると誤解することがありません。

また、特定のツールでグローバル ルールが処理される方法に関して、いくつかの変更点があります。

- Find/Replace：グローバル ルールは、Global というインターフェイス名を使用して検索できます。ただし、グローバル ルールとインターフェイス固有のルールを変換する方法はありません。グローバル ルールはグローバル インターフェイス名を使用して検索できますが、インターフェイス名を「Global」という名前で置換しようとすると、実際には Global という名前のポリシー オブジェクトを使用する、インターフェイス固有のアクセス ルールが作成されます。
- Rule Combiner：インターフェイス固有のルールとグローバル ルールが結合されることはありません。

関連項目

- グローバル アクセス ルールについて （915 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- アクセス ルールの設定 （920 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）

デバイス固有のアクセス ルールの動作について

次に、アクセス ルール ポリシーを作成しない場合のデフォルトの動作をデバイス タイプに基づいて示し、アクセス ルールを作成したときに行われる処理を示します。

- IOS デバイス：インターフェイスを通過するすべてのトラフィックを許可します。

送信元 A から宛先 B へのトラフィックを許可しているものの、インスペクション ルール テーブルに TCP/UDP インスペクションを設定していないか、ルールに [established] 拡張オプション

を設定していない場合、デバイスは A から B へのパケットをすべて許可します。ただし、B から A に戻るパケットについては、そのパケットを許可するためのアクセスルールがないかぎり、パケットは許可されません。トラフィックのインスペクション ルールテーブルに TCP/UDP インスペクションを設定した場合、B から A に戻るパケットはいずれも自動的にデバイスを通過するため、アクセス ルール内に B から A を許可するルールは必要ありません。

- ASA および PIX デバイス：高いセキュリティのインターフェイスから低いセキュリティのインターフェイスへのトラフィックを許可します。それ以外のトラフィックはすべて拒否されます。

アクセス ルールで単方向の TCP/UDP トラフィックが許可されている場合、アプライアンスによりリターン トラフィックが自動的に許可されます（リターン トラフィックのためのルールを設定する必要はありません）。ただし、ICMP トラフィックの場合は例外で、リターン ルールが必要となります（逆方向の送信元および宛先を許可します）。あるいは、ICMP のインスペクション ルールを作成する必要があります。

- FWSM デバイス：インターフェイスに入るすべてのトラフィックを拒否し、インターフェイスを出るすべてのトラフィックを許可します。

デバイスに入るすべてのトラフィックを許可するためのアクセスルールを設定する必要があります。

任意のタイプのデバイスに対してインターフェイスのルールを作成すると、デバイスによってポリシーの最後に暗黙的な [deny any] ルールが追加されます。このルールは、場所を忘れないように自分で追加することを推奨します。また、ルールを追加すると、ルールのヒット カウント情報を取得できます。詳細については、ヒットカウントの詳細の表示 （960 ページ）を参照してください。

ヒント アクセス ルール ポリシーを作成する場合、Security Manager サーバからデバイスへのアクセスを許可するルールを含める必要があります。そうしない場合、この製品を使用してデバイスを管理できなくなります。

関連項目

- アクセス ルールについて （913 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）

アクセス ルールのアドレス要件およびルールの展開方法について

コマンドライン インターフェイス（CLI）でオペレーティング システム コマンドを使用してアクセス制御リストを作成する場合の複雑な点の 1 つは、送信元アドレスと宛先アドレスの IP アドレス形式がオペレーティングシステムで異なっていることです。

たとえば、Cisco IOS Software では、サブネット マスクではなくワイルドカード マスクを使用してアドレスを入力する必要があります。10.100.10.0/24 ネットワーク（サブネット マスク

255.255.255.0）のルールを作成するには、アドレスを 10.100.10.0 0.0.0.255 として入力する必要があります。ワイルドカードマスクとサブネットマスクでは、0 と 1 の意味が逆になります。ただし、ASA、PIX、および FWSM ソフトウェアでは、サブネットマスクを使用するため、10.100.10.0 255.255.255.251 と入力します。

Security Manager では、アクセス ルールのアドレッシング要件が単純化されており、常にサブネット マスクを使用します。ワイルドカード マスクは入力できません。アクセス ルールをデバイスに展開すると、Security Manager によって、デバイスのオペレーティング システムが考慮され、必要に応じてサブネット マスクがワイルドカード マスクに自動変換されます。

このため、論理ポリシーに基づいて共有ルールを作成して、すべてのデバイスに適用することが可能になります。たとえば、すべてのデバイスで使用するアクセス ルール セットがある場合は、共有ポリシーを作成して、それをすべてのデバイスの継承ポリシーとして割り当てます。デバイスタイプごとに「適切な」構文を使用してルールを定義する必要はありません。他のポリシー タイプで使用する同じネットワーク/ホスト オブジェクトを使用して、対象のホストおよびネットワークを識別できます。

展開された設定内に生成される特定の CLI コマンドも、デバイス タイプに基づきます。IOS デバイスの場合、**ip access-list** コマンドを使用します。ASA、PIX、FWSM デバイスの場合、**access-list** または **ipv6 access-list** コマンドを使用し、**access-group** コマンドを使用してインターフェイスにバインドします。ASA、PIX、FWSM、および IOS 12.4(20)T 以降のデバイスでは、ネットワーク/ホストオブジェクトを使用してルールの送信元アドレスまたは宛先アドレスを識別する場合、それらのネットワーク/ホストオブジェクトに対してオブジェクトグループを作成するために、**object-group** コマンドを使用します。また、サービス オブジェクトに対してもオブジェクト グループが作成されます。

ヒント

- ネットワーク/ホスト オブジェクトを使用してルールの送信元アドレスや宛先アドレスを識別でき、またルールに対して展開の最適化を設定できるため、アクセス ルールと ACL の CLI 定義内の ACE が必ずしも 1 対 1 の関係になるとはかぎりません。
- ファイアウォール ルールから作成されるアクセス リストはすべて、（標準アクセス リストではなく）拡張アクセス リストです。[Access Control Settings] ページ （944 ページ）で ACL の名前を指定していない場合、Security Manager によってシステム生成名が ACL に適用されます。この名前は、名前が定義されているインターフェイスおよび方向に関連するすべてのルールが含まれる ACL に適用されます。
- オブジェクト グループの展開方法を制御する展開オプションがいくつかあります。この項では、デフォルトの動作について説明します。[Deployment] ページ （658 ページ）（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [展開（Deployment）]** を選択）で、ネットワーク/ホストオブジェクトからオブジェクトグループを作成するためのオプションの選択を解除できます。また、展開中にオブジェクト グループを最適化したり（ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化 （802 ページ）を参照）、複数のサービスまたは送信元アドレスや宛先アドレスを持つルールから新しいオブジェクト グループを作成したり、使用していないオブジェクト グループを削除したりできます。

- 展開オプションには、アクセス ルールから生成される ACL の名前および作成される ACL の数を制御する設定も含まれます。デフォルトでは、Security Manager により、インターフェイスごとに一意の ACL が作成されます。このため、複数の重複する ACL が作成されることがあります。

[ファイアウォールルールに対するACL共有の有効化（Enable ACL Sharing for Firewall Rules）] を選択した場合、Cisco Security Manager は単一の ACL を作成して複数のインターフェイスに適用できるため、重複する不要な ACL は作成されません。ただし、ACL の共有が行われるのは、ACL 命名要件が保たれている間に実行できる場合にかぎります。

- インターフェイスおよび方向に対して ACL 名を指定した場合は、その名前が常に使用されます。このため、重複する ACL が作成されることがあります。詳細については、アクセス コントロール ポリシー設定の指定 （943 ページ）を参照してください。
- [ファイアウォールアクセルリスト名（Firewall Access-List Names）] プロパティの [既存の名前を再利用（Reuse Existing Names）] を選択すると、既存の名前は保存されます（アクセス制御設定ポリシーで名前をオーバーライドした場合を除く）。つまり、重複する ACL がデバイスにすでに存在する場合は、異なる名前で ACL が重複して作成されます。

ヒント：ACL 共有を最大限に利用するには、[ファイアウォールアクセスリスト名（Firewall Access-List Names）] プロパティに [CS-Managerの生成名にリセット（Reset to CS-Manager Generated Names）] を選択し、[アクセスルールの展開の最適化対象（Optimize the Deployment of Access Rules For）] プロパティに [速度（Speed）] を選択する必要があります。アクセス制御設定ポリシー内に ACL 名は設定しないでください。

[ファイアウォールルールに対するACL共有の有効化（Enable ACL Sharing for Firewall Rules）] プロパティの詳細については、[Deployment] ページ （658 ページ）を参照してください。

- IPv4 および IPv6 ACL は同じ名前を持てません。

関連項目

- アクセス ルールについて （913 ページ）
- アクセス ルールの設定 （920 ページ）
- アクセス コントロール ポリシー設定の指定 （943 ページ）
- 検出中のオブジェクト グループの展開 （806 ページ）

アクセス ルールの設定

アクセス ルール ポリシーでは、トラフィックがインターフェイスを通過することを許可するためのルールを定義します。アクセス ルール ポリシーを設定しない場合、デバイス固有のアクセス ルールの動作について （917 ページ）に説明するように、デバイスの動作はデバイス タイプによって異なります。

（注） Security Manager 4.4 およびバージョン 9.0 以降の ASA のリリースより前は、IPv4 および IPv6 ファイアウォールルールとポリシーを設定するための個別のページ、ポリシー、およびポリシーオブジェクトが提供されていました。Cisco Security Manager 4.4 と ASA のバージョン9.0以降では、これらのポリシーとポリシーオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスを使用できる一組のアクセスルールになりました（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 （14 ページ）を参照してください）。ただし、以前の ASA バージョンでは、IPv6アクセスルールの別のページが引き続きデバイスビューで提供されますが、ポリシービューでは、IPv4 および統合バージョンのアクセスルールポリシータイプが提供されます。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが提供されています（IPv4 ルールから統合ルールへの変換 （792 ページ）を参照）。次の説明は、特に明記されている場合を除き、アクセスルールテーブルのすべてのバージョンに適用されます。IPv4アクセスルール共有ポリシーを9.0以降のデバイスに割り当てると、それらのポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合 アクセスルール共有ポリシーを 9.0 以降のデバイスに割り当てると、それらの共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれなくなります。

アクセス ルールを設定する前に、これから設定する他のタイプのファイアウォール ルールについて検討してください。アクセスルールは、他のタイプのルール（AAA ルールを除く）よりも先に処理されます。検討する必要のある事項の詳細については、次の項を参照してください。

- アクセス ルールについて （913 ページ）
- グローバル アクセス ルールについて （915 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）

はじめる前に

アクセス ルール セットをすべてのデバイスに適用するとします。このためには、共有ルールを作成して、そのルールを各デバイスのアクセスルールポリシーに継承します。詳細については、新しい共有ポリシーの作成 （278 ページ）およびルールの継承または継承の解除 （269 ページ）を参照してください。

関連項目

- セクションを使用したルール テーブルの編成 （783 ページ）
- デバイス間でのポリシーのコピー （251 ページ）
- デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

- インターフェイス ロール オブジェクトについて （381 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

ステップ 1 次のいずれかを実行して、 [Access Rules] ページ （924 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。 [Add Access Rule]/[Edit Access Rule] ダイアログボックス （930 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、 ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。1 つのポリシー内にインターフェイス固有のルールとグローバル ルールを混在させた場合は、特殊なルールが適用されます。詳細については、 グローバル アクセス ルールについて （915 ページ）を参照してください。

ステップ 3 ルールを設定します。次に、ルールの設定時に判断が必要となることが多い重要な点を示します。フィールドを設定する方法の詳細については、 [Add Access Rule]/[Edit Access Rule] ダイアログボックス （930 ページ）を参照してください。

- 許可または拒否：ルールに一致したトラフィックを許可するか、またはドロップするか。
- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスまたはトラフィックの宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「All-Addresses」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホスト オブジェクトを入力します。受け入れられるアドレス形式の詳細については、 ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。
- 送信元および宛先のセキュリティグループ（ASA 9.0+ のみ）：送信元および宛先アドレスに加えて、トラフィックのフィルタリングに使用される TrustSec セキュリティグループを指定できます。セキュリティグループの詳細については、 ポリシーでのセキュリティグループの選択 （865 ページ）、 TrustSec ベースのファイアウォールルールの設定 （866 ページ）、および セキュリティ グループ オブジェクトの作成 （863 ページ）を参照してください。
- 送信元ユーザー（ASA 8.4.2 以降のみ）：Active Directory（AD）ユーザー名（NetBIOS_DOMAIN\username 形式）、ユーザーグループ（NetBIOS_DOMAIN\\user_group）、または名前とグループを定義するアイデンティティ ユーザー グループ オブジェクトを指定して、トラフィックの送信元をさらに定義できます。ユーザ指定は送信元アドレスと結合され、送信元アドレス範囲の中で照合するユーザ アドレス

を制限します。詳細については、アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）およびアイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）を参照してください。

- サービス：IP サービスを使用して、すべてのトラフィックに適用します（たとえば、特定の送信元からのすべてのトラフィックを拒否する場合）。または、対象となるより具体的なサービス（プロトコルとポートの組み合わせ）を選択します。
- インターフェイスまたはグローバル：ルールを設定するインターフェイスまたはインターフェイス ロールを選択するか、ASA 8.3+ デバイスでグローバル アクセス ルールを作成する場合は [Global] を選択します（ グローバル アクセス ルールについて （915 ページ）を参照）。
- 詳細設定：[詳細設定（Advanced）] をクリックして、追加設定を行うための [詳細設定（Advanced）] ダイアログボックスを開きます。次のオプションを設定できます。詳細については、[Advanced]/[Edit Options] ダイアログボックス （936 ページ）を参照してください。
  - ロギング オプション。Security Manager または CS-MARS を使用してデバイスをモニタしている場合は、ロギングをイネーブルにする必要があります。
  - このルールを適用するトラフィックの方向（[in] または [out]）。デフォルトは [入力（in）] です。グローバルルールでは、この設定を変更できません。
  - ルールの時間範囲。これにより、特定の期間中（勤務時間中など）だけ有効になるルールを設定できます。詳細については、時間範囲オブジェクトの設定 （379 ページ）を参照してください。
  - フラグメンテーションを行い、確立されたアウトバウンド セッションのトラフィックのリターンを許可するための IOS デバイス オプション。
  - ルールの有効期限および通知の設定。詳細については、アクセス ルールの有効期限の設定 （942 ページ）を参照してください。

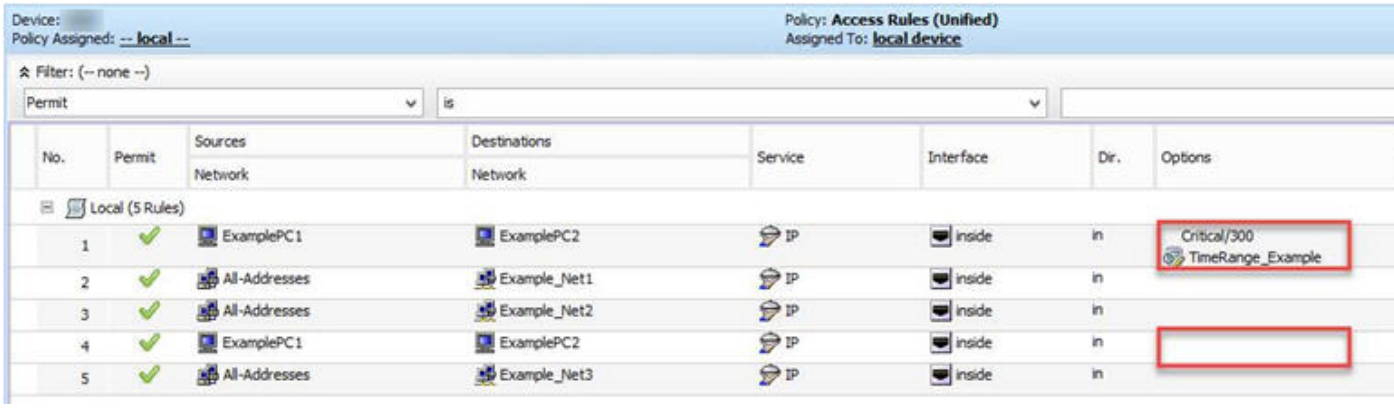
ステップ 4 ルールの定義が完了したら、[OK] をクリックします。

（注） 競合検出をイネーブルにして（競合検出の有効化 （955 ページ）を参照）、新しいルールが他のルールと競合または重複しているかどうかを確認できます。詳細については、自動競合検出の使用 （950 ページ）を参照してください。

ルールを追加または編集しているときに、時間範囲またはロギング値 （[Advanced]/[Edit Options] ダイアログボックス （936 ページ）で定義）の違いを除いて、任意の 2 つのルールが同一になる場合があります（例：図 23 : 同一のルール （924 ページ）の 1 と 2）。

- Cisco Security Manager では、一番下にあるルールのみが展開されます（図 23 : 同一のルール （924 ページ）の 2）。
- 設定のプレビューでの設定変更の識別には、ルール（2）のみが使用されます。（ 設定のプレビュー （535 ページ）を参照）。
- ルール（2）がデバイスに展開されている場合、設定のプレビューでは変更が検出されません。

図 *23 :* 同一のルール



ステップ 5 Cisco Security Manager による最上位のルール（図 23 : 同一のルール （924 ページ）の 1）の展開を阻止している最下位のルール（例：図 23 : 同一のルール （924 ページ）の（2））を特定する必要がある場合は、次の手順を実行します。

a) デバイスで、競合検出の有効化 （955 ページ） 。

b) 見つかった競合について、レポートの作成（Generate Report） （955 ページ）。

c) レポートの[ルール番号（Rule No）] の 列で最下位のルール （2）を見つけ、競合するルール番号を特定し（ルール（1））、必要に応じてルール（1）を削除します。

ステップ 6 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、 ルールの移動とルール順序の重要性 （781 ページ）を参照してください。インターフェイス固有のルールとグローバル ルールを混在させた場合には、ルールの移動に関する特別な制約はありません（ グローバル アクセス ルールについて （915 ページ）を参照）。

ステップ 7 すでに多数のルールが存在している場合は、新しいルールを展開する前に、ルールを分析して結合することを検討します。競合検出ツールを使用して、ルールを分析できます（ 自動競合検出の使用 （950 ページ）を参照）。分析により冗長なルールが多数あることが示された場合は、ルールテーブル内の任意の場所を右クリックして [ルールの結合（Combine Rules）] を選択し、ルールを結合します。ルール結合ツールを起動する前に、Security Manager で結合についてすべてのルールを評価するか、選択したルールだけを評価するかを選択できます。詳細については、 ルールの結合 （785 ページ）を参照してください。

[Access Rules] ページ

[アクセスルール（Access Rules）] ページを使用して、デバイスインターフェイスに対してアクセスコントロールルールを設定します。アクセス ルール ポリシーでは、インターフェイスを通過するトラフィックを許可または拒否するルールを定義します。通常は、インターフェイスに入るトラフィックのアクセス ルールを作成します。これは、特定タイプのパケットを拒否する場合、デバイスがパケットの処理に多くの時間を費やす前にパケットを拒否する方が有効なためです。アクセス ルールは、他のタイプのファイアウォール ルールよりも先に処理されます。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセスルールを設定するための個別のポリシーとオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスをどちらも使用できる一組のアクセスルールになりました。（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 （14 ページ）を参照してください。）ポリシービューでは、アクセスポリシータイプの IPv4 および統合バージョンが提供されます。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが提供されています（IPv4 ルールから統合ルールへの変換 （792 ページ）を参照）。以下の説明は、特に明記されている場合を除き、アクセスルールテーブルのすべてのバージョンに適用されます。

アクセス ルールを設定する前に、次の項を参照してください。

- アクセス ルールについて （913 ページ）
- グローバル アクセス ルールについて （915 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- アクセス ルールの設定 （920 ページ）

ヒント 無効なルールはグレー表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

ナビゲーション パス

[Access Rules] ページを開くには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、次にポリシーセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [アクセスルール（Access Rules）]**（または **[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [IPv6アクセスルール（IPv6 Access Rules）]**）を選択します。

関連項目

- アクセス ルールの有効期限の設定 （942 ページ）
- アクセス コントロール ポリシー設定の指定 （943 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）
- ルール テーブルの使用 （764 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

（注） 自動競合検出機能の一部として使用できるフィールドとユーザーインターフェイス要素の詳細については、 自動競合検出のユーザー インターフェイスについて （952 ページ）を参照してください。

表 *186 : [Access Rules]* ページ

要素	説明
[すべての行を展開する（Expand all rows）]/[すべての行を折りたたむ（Collapse all rows）]	ルールテーブルのすべてのセクションを展開または折りたたむには、これらのボタンを使用します。 （注） ボタンは、アクセスルールテーブルの上にある [フィルタ（Filter）] 領域の右上隅にあります。
[競合インジケータ（Conflict Indicator）] アイコン	競合を識別し、競合のタイプをすばやく視覚的に表現します。競合の種類や、この列から実行できるアクションなどの詳細については、 自動競合検出のユーザー インターフェイスについて （952 ページ） を参照してください。
番号	順序が付けられたルール番号。
許可（Permit）	設定された次の条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。

要素	説明
ソース	このルールのトラフィックソース。つまり、ネットワーク、セキュリティグループ（ASA 9.0 以降のみ）、およびユーザーになります。複数のエントリは、テーブルセル内の個別の行に表示されます。
宛先	このルールの宛先。つまり、ネットワークおよびセキュリティグループになります（ASA 9.0 以降のみ）。複数のエントリは、テーブルセル内の個別の行に表示されます。
サービス	ルールが適用されるトラフィックのプロトコルおよびポートを指定するサービスまたはサービス オブジェクト。複数のエントリは、テーブルセル内の個別の行に表示されます。 サービスとサービスオブジェクトおよびポートリストオブジェクトの理解と指定 （418ページ）を参照してください。
ヒット カウント（Hit Count）	このルールが「ヒット」された回数。つまり、トラフィックを許可または拒否した回数です。実際には、ルールによって作成されたすべてのアクセス制御エントリ（ACE）のヒットカウントの合計となります。この情報は、展開されたポリシーをデバッグする際に役立ちます。 ヒット情報を更新するには、このページの下部にある [ヒットカウントの更新（Refresh Hit Count）] ボタンを使用します。 [Hit Count Selection Summary] ダイアログボックス （939ページ）が開きます。 （注） 同じルール内または異なるルール内の重複した ACE のヒットカウントは、常に 0 に設定されます。 このセルを右クリックして [ヒットカウントの詳細を表示（Show Hit Count Details）] を選択すると、[Configuration Manager] ウィンドウの下部にある [ヒットカウントの詳細（Hit Count Details）] ペインを開くことができます。詳細については、 ヒットカウントの詳細の表示 （960 ページ）を参照してください。
前回のヒット時刻（Last Hit Time）	最新のヒットのタイムスタンプ。

要素	説明
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリは、テーブルセル内の個別の行に表示されます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。 ASA 8.3+ デバイスの場合、グローバルルールには **Global** という名前が付き、インターフェイスまたはインターフェイスロールの名前を使用するルールと区別するための特別なアイコンが示されます（アイコンの説明については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください）。
Dir.	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。
オプション	ルールに設定される追加のオプション。これには、ロギング、時間範囲、およびその他の IOS ルール オプションが含まれます。[Advanced]/[Edit Options] ダイアログボックス （936 ページ）を参照してください。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	ルールの説明（ある場合）。
期限日（Expiration Date）	ルールが期限切れになる日付。期限切れになったルールは、太字で [期限切れ（Expired）] と示されます。期限切れになったルールは自動的には削除されません。
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
ルールテーブルの下のページ要素	

要素	説明
競合検出の有効化（Enable conflict detection） レポートの作成（Generate Report） （[IPv6アクセス制御（IPv6 Access Control）] ページにはどちらのオプションも表示されません）	自動競合検出を有効または無効にします。この機能はデフォルトで有効になっており、設定はユーザーごとに管理されます。1 つのアクセスルールテーブルの競合検出を無効にすると、他のアクセスルールテーブルの機能も無効になります。 ルールテーブルの作成中または大規模な変更中は競合検出を無効にし、変更を検証する準備ができたら再度有効にすることができます。 自動競合検出の使用 （950 ページ）を参照してください。 （注） 自動競合検出機能の一部として使用できるフィールドとユーザーインターフェイス要素の詳細については、 自動競合検出のユーザーインターフェイスについて （952 ページ）を参照してください。 競合検出が有効になっている場合は、[レポートの生成（Generate Report）] ボタンをクリックして、検出されたルールの競合に関する HTML レポートを作成できます。このレポートは印刷または別のアプリケーションにエクスポートすることができます。
ヒットカウントの更新（Refresh Hit Count） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	テーブルに表示されるヒット情報を更新するには、このボタンをクリックします。 [Hit Count Selection Summary] ダイアログボックス （939 ページ）が開きます。
クエリ （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。 ポリシー クエリー レポートの生成 （793 ページ）を参照してください
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。 ルール テーブルの項目の検索と置換 （777 ページ）を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、 ルールの移動とルール順序の重要性 （781 ページ）を参照してください。

要素	説明
[Add Row] ボタン	[Add Access Rule]/[Edit Access Rule] ダイアログボックス （930 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、 ルールの追加および削除 （766 ページ）を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、 ルールの編集 （767 ページ）を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

右クリックメニュー

右クリックメニューも使用できます。このメニューから、上記の機能の多くにアクセスできます。表示されるオプションは、右クリックした場所によって異なります。

- テーブル内のルールを右クリックすると、右クリックした特定のテーブルセルに関連した編集機能がオプションに含められる場合があります。たとえば、[ヒットカウント（Hit Count）]セルを右クリックすると、[ヒットカウントの詳細を表示（Show Hit Count Details）]コマンドが含まれます。詳細については、ルールの編集 （767 ページ）を参照してください。
- イベントビューアまたは CS MARS のいずれかで、ルールからそのルールに関連付けられたイベントに移動することもできます。詳細については、アクセスルールのイベントの表示 （3543 ページ）および IPS シグニチャの CS-MARS イベントの表示 （3738 ページ）を参照してください。
- 右クリックメニューには、[ルールのインポート（Import Rules）] および [ルールの結合（Combine Rules）]オプションも含まれています。これらのオプションの詳細については、ルールのインポート （966 ページ）および ルールの結合 （785 ページ）を参照してください。

[Add Access Rule]/[Edit Access Rule] ダイアログボックス

security-device アクセスルールを追加または編集するには、[アクセスルールの追加（Add Access Rule）] および [アクセスルールの編集（Edit Access Rule）] ダイアログボックスを使用します。

（注） Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセスルールを設定するための個別のページが統合されました。ただし、それ以前の ASA バージョンでは、IPv6 アクセスルールの個別のページが引き続き提供されます。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

アクセス ルールを設定する前に、次の項を参照してください。

- アクセス ルールについて （913 ページ）
- グローバル アクセス ルールについて （915 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- アクセス ルールの設定 （920 ページ）

ナビゲーション パス

[Access Rules] ページ （924 ページ）で、[行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

（注） Cisco Security Manager 4.13 より前は、[アクセスルールの追加（Add Access Rule）] ダイアログにデフォルト値が入力されていました。4.13 以降、ユーザーは csm.properties ファイルを更新することにより、デフォルト値の状況をカスタマイズできます。詳細については、[アクセスルールの追加（Add Access Rule）] ダイアログでのデフォルトのカスタマイズ （975 ページ）を参照してください。

関連項目

- アクセス ルールの有効期限の設定 （942 ページ）
- ルールの編集 （767 ページ）
- ルールの追加および削除 （766 ページ）
- ルールのインポート （966 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

フィールド リファレンス

表 *187 : [Add Access Rule]/[Edit Access Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	このチェックボックスをオンにするとルールがイネーブルになります。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。選択を解除すると、ルールはディセーブルになりますが、ルール定義は保持されます。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。
操作	定義した条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。

要素	説明
ソース	

要素	説明

	このルールのトラフィック ソースを提供します。ネットワーク、セキュリティ グループ、およびユーザーになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。
	• ネットワーク – さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイスオブジェクトをソースとして選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。
	
	「All-Address」オブジェクトは、ルールを特定のホスト、ネットワーク、またはインターフェイスに制限しません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IPv4 または IPv6 アドレスです。
	（注） 完全修飾ドメイン名（FQDN）は、FQDN ネットワーク/ホストオブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを提供することによってのみ指定できます。FQDN を直接入力することはできません。
	これらの定義の詳細については、 ネットワーク/ホストオブジェクトについて （391 ページ）、 ポリシー定義中の IP アドレスの指定 （401 ページ）およびインターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
	• セキュリティグループ（ASA 9.0 以降）– ルールについて、1 つ以上のソースセキュリティグループの名前またはタグ番号を入力するか選択します（存在する場合）。セキュリティグループの詳細については、 ポリシーでのセキュリティグループの選択 （865 ページ）、 TrustSec ベースのファイアウォールルールの設定 （866 ページ）、およびセキュリティ グループ オブジェクトの作成 （863 ページ）を参照してください。
	• ユーザー - ルールの Active Directory（AD）ユーザー名、ユーザーグループ、またはアイデンティティユーザーグループ オブジェクト（使用する場合）。次のものを組み合わせて入力できます。
	  • 個別のユーザ名：NetBIOS_DOMAIN\username
	  • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group
	  • アイデンティティ ユーザ グループ オブジェクト名。
	
	詳細については、以下を参照してください。
	• ポリシーでのアイデンティティ ユーザの選択 （835 ページ）
	• アイデンティティ ベースのファイアウォール ルールの設定 （836 ページ）
	• アイデンティティ ユーザ グループ オブジェクトの作成 （833 ページ）

要素	説明
	（注） Enter more than one value in any of these fields by separating the items with commas.ロゴのソース イメージ ファイルに指定できるのは、GIF ファイル、JPG ファイル、または PNG ファイルです。ファイル名は最大 255 文字、サイズは最大 100 KB です。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックです。
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。送信元と同様に、ネットワークおよびセキュリティグループ（ASA 9.0 以降）タイプの 1 つ以上の宛先について、値またはオブジェクト名を入力するかオブジェクトを選択できます。
サービス	動作対象のトラフィックタイプを定義するサービス。サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。 項目をカンマで区切って複数の値を入力します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
インターフェイス Global（ASA 8.3+）	インターフェイス固有のルールまたはグローバル ルールのいずれを作成するかを指定します。グローバル ルールは ASA 8.3+ のデバイスだけで使用でき、特別なルールに従って処理されます（詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください）。 [インターフェイス（Interfaces）] を選択した場合は、ルールを割り当てるインターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックして、リストからインターフェイスまたはロールを選択します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 ルーテッド モードのブリッジ グループでは、ブリッジ仮想インターフェイス（BVI）と各ブリッジ グループ メンバーのインターフェイスの両方にアクセス ルールを作成できます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。グローバルルールは、特定のインターフェイスに関連付けられていない特殊なグローバル ACL として作成されますが、インターフェイス固有のルールの後で、着信方向ですべてのインターフェイスに対して処理されます。
説明	オプションで入力するルールの説明（最大 1024 文字）。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
[Advanced] ボタン	このボタンをクリックして、ルールのその他の設定（ロギング設定、トラフィック方向、時間範囲、およびルールの有効期限など）を行います。詳細については、「[Advanced]/[Edit Options] ダイアログボックス （936 ページ）」を参照してください。

[Advanced]/[Edit Options] ダイアログボックス

[詳細（Advanced）] ダイアログボックスを使用して、アクセスルールの追加の設定を行います。アクセスルールテーブルの3つの異なるセルに、方向、オプション、およびルールの有効期限の設定が表示されます。その後、該当するセルを右クリックして、設定を直接編集できます。

（注） Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセスルールを設定するための個別のページが統合されました。ただし、それ以前の ASA バージョンでは、IPv6 アクセスルールの個別のページが引き続き提供されます。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

ナビゲーション パス

[詳細（Advanced）] ダイアログボックスにアクセスするには：

- [Add Access Rule]/[Edit Access Rule] ダイアログボックス （930 ページ）で [詳細（Advanced）] ボタンをクリックします。

[オプションの編集（Edit options）] ダイアログボックスのいずれかにアクセスするには：

- （[Access Rules] ページ （924 ページ）の）アクセスルールの [オプション（Options）] または [有効期限（Expiration Date）] セルを右クリックし、関連する [編集（Edit）] コマンドを選択します。ルールの方向を変更するには、[方向（Dir.）] を右クリックして、反対の方向（インまたはアウト）を選択します。

複数の行を選択すると、選択したすべてのルールのオプションが、変更によって置き換えられます。

関連項目

- アクセス ルールの設定 （920 ページ）
- ルールの編集 （767 ページ）
- アクセス ルールについて （913 ページ）

- ファイアウォール アクセス ルールの管理 （913 ページ）
- 時間範囲オブジェクトの設定 （379 ページ）

フィールド リファレンス

表 *188 : [Advanced]* ダイアログボックス

要素	説明
Enable Logging（PIX、ASA、FWSM）	PIX、ASA、および FWSM デバイスの場合、ルールエントリ（アクセス制御エントリ、または ACE とも呼ばれる）についての syslog メッセージを生成するかどうかを指定します。選択すると、次の追加オプションが有効になります。 • [Default Logging]：デフォルトのロギング動作を使用します。パケットが拒否されると、メッセージ 106023 が生成されます。パケットが許可された場合、syslog メッセージは生成されません。デフォルトのロギング間隔は 300 秒です。 • [Per ACE Logging]：このエントリに固有のロギングを設定します。ACE のログイベントに対して使用するロギングレベルを選択し、ロギング間隔（1 ～ 600 秒の範囲）を指定します。ACE に対して syslog メッセージ 106100 が生成されます。 使用可能なロギングレベル： • [Emergency]：（0）システムが不安定 • [Alert]：（1）即時処理が必要 • [Critical]：（2）クリティカル条件 • [Error]：（3）エラー条件 • [Warning]：（4）警告条件 • [Notification]：（5）正常ではあるが重大な条件 • [Informational]：（6）情報メッセージだけ • [Debugging]：（7）デバッグ メッセージ （注） [オプション（Options）] セルを右クリックし、[オプションの編集（Edit Options）] を選択すると、[Access Rules] ページ （924 ページ）のテーブルに含まれる既存ルールのファイアウォールおよび IOS ロギングオプションを変更できます。

要素	説明
Enable Logging（IOS） Log Input （IPv4 のみ。[IPv6 アクセス制御（IPv6 Access Control）] ページにはどちらのオプションも表示されません）	IOS デバイスのコンソールに送信されるエントリに一致したパケットに関するロギング情報メッセージを生成するかどうかを指定します。メッセージは IOS デバイスのコンソールに送信されます。 入力インターフェイスおよび送信元 MAC アドレスまたは仮想回線をロギング出力に含める場合は、[Log Input] を選択します。
トラフィックの方向	インターフェイス固有のアクセス ルールの場合、このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。 （注） [方向（Dir.）] セルを右クリックして反対の方向を選択することで、[Access Rules] ページ （924 ページ）のテーブルに含まれる既存ルールの方向を変更できます。 グローバル ルールは常に In 方向で適用されるため、グローバル ルールの設定時にはこの設定を変更できません。
時間範囲	このルールが適用される時間を定義する時間範囲ポリシー オブジェクトの名前。時刻は、デバイスのシステム クロックに基づきます。この機能は、NTP を使用してシステム クロックを設定している場合に最適に機能します。 名前を入力するか、オブジェクトを選択します。必要なオブジェクトが表示されていない場合は、[Create] ボタンをクリックして作成します。 （注） 時間範囲は、FWSM 2.x デバイスまたは PIX 6.3 デバイスではサポートされていません。

要素	説明
Options（IOS） （IPv4 のみ。[IPv6 アクセス制御（IPv6 Access Control）] ページには表示されません）	IOS デバイス用の追加オプション： • [なし（none）]：適用されません。 • [Fragment]：フラグメンテーションを有効にします。これにより、パケット フラグメンテーションの追加管理が行われ、NFS との互換性が向上します。 デフォルトで、完全な IP パケットを再構築するために最大で 24 のフラグメントを受け入れます。ただし、ネットワーク セキュリティ ポリシーによっては、フラグメント化されたパケットがファイアウォールを通過しないようにデバイスを設定することが必要な場合もあります。 • [確立済み（Established）]：デバイスを介したアウトバウンド TCP 接続のリターン アクセスを有効にします。このオプションは、デバイスにより保護されたネットワークからのアウトバウンドの元の接続と、外部ホスト上の同じ 2 つのデバイス間のインバウンドのリターン接続という、2 つの接続に対して機能します。
Rule Expiration	ルールに有効期限を設定できます。カレンダー アイコンをクリックして、日付を選択します。詳細については、アクセス ルールの有効期限の設定 （942 ページ）を参照してください。 また、有効期限を設定している場合は、有効期限が近いことを示す通知を、ルールが失効する何日前に送信するか、およびその送信先となる電子メール アドレスを設定することもできます。最初、これらのフィールドには、[ルール有効期限の管理設定（Rule Expiration administrative settings）] ページ（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ルールの有効期限（Rule Expiration）] を選択）で設定した情報が設定されています。 [有効期限（Expiration Date）] セルを右クリックし、[ルールの有効期限の編集（Edit Rule Expiration）] を選択することにより、[Access Rules] ページ （924 ページ）のテーブルに含まれる既存ルールの該当するオプションを変更できます。 （注） 期限切れになったルールは自動的には削除されません。これらの情報を手動で削除し、デバイスに設定を再配布する必要があります。

[Hit Count Selection Summary] ダイアログボックス

[ヒットカウント選択サマリー（Hit Count Selection Summary）] ダイアログボックスを使用して、ヒットカウント情報を更新するルールを選択します。選択できるオプションは、[ヒットカウントの更新（Refresh Hit Count button）] ボタンをクリックする前に選択したルールによって制限されます。このダイアログボックスで [OK] をクリックすると、デバイスから更新され

たヒットカウント情報が取得されます。これには時間がかかることがあるため、途中で操作を中断できます。

（注） 同じルール内または異なるルール内の重複した ACE のヒットカウントは、常に 0 に設定されます。

ヒント [Access Rules] ページ （924 ページ）でそのルールの [ヒットカウント（Hit Count）] セルを右クリックすると、ルールの詳細なヒットカウント情報を表示できます。 ヒットカウントの詳細の表示 （960 ページ）で説明されているように、詳細なヒットカウント情報が [ヒットカウントの詳細（Hit Count Details）] ウィンドウに表示されます。

ナビゲーション パス

（デバイスビューのみ） [Access Rules] ページ （924 ページ）テーブルで、詳細なヒットカウント情報が必要なアクセスルールを 1 つ選択し、[ヒットカウント（Hit Count）] カラムを右クリックして、[ヒットカウント詳細の表示（Show Hit Count Details）] を選択します。

関連項目

- ヒットカウントの詳細の表示 （960 ページ）
- アクセス ルールについて （913 ページ）

フィールド リファレンス

表 *189 : [Hit Count Selection Summary]* ダイアログボックス

要素	説明
Policy Selected	選択されているポリシーを識別します。ポリシーを選択しなかった場合、これは通常、デバイスに特定のルールが定義されていることを示す [ローカル（Local）] です。ポリシーが、共有ポリシーまたは継承ポリシー内の範囲となることもあります。 このフィールドの表示内容によって、ヒットカウントレポートの範囲が実際に制限されることはありません。

要素	説明
Rules Selected	ヒットカウント詳細を取得するルール。以下を選択します。 • 選択したルールのみの情報を取得する場合は、[ルール（rules）] オプションを選択します。範囲の名前、セクション名、または複数の個別のルールに関連する行を選択したり、フィルタを作成してフィルタリングされたすべてのルールを選択したりできます。ヒットカウントレポートの開始時にいずれかの行が選択されていた場合は、これがデフォルトとなります。 • すべての継承ルール、共有ルール、およびローカルルールに対するヒットカウントを取得する場合は、[すべてのルール（All Rules）] を選択します。オプションは、[Policy Selected] フィールドで指定されている範囲に限定されません。 ヒットカウントレポートの開始前にルールを選択しなかった場合、このオプションだけが選択可能になります。
Fetch Data From	次のいずれかのオプションを選択し、[ヒットカウントの更新（Refresh Hit Count）] をクリックします。 • [デバイス（Device）]：Security Manager はデバイスからヒットカウント情報をフェッチし、[アクセスルールポリシー（Access Rules policy）] ページに同じ情報を表示します。バージョン 4.9 以降、Security Manager は ASA および ASASM デバイスのデータベースにヒットカウント情報を保存します。 • [履歴（History）]： Security Manager は、特定の ACE の最新のヒットカウント情報をデータベース（ヒットカウントの履歴）からフェッチし、[アクセスルールポリシー（Access Rules policy）] ページに同じ情報を表示します。 **注**： オープンなアクティビティがある場合、ヒットカウントデータは Security Manager データベースに保持されません。この機能は、ASASM/ASA バージョン 8.3 以降の IPv4 アクセスルールおよび ASASM/ASA バージョン 9.0 以降のユニファイドアクセスルールでサポートされています。 [デバイスからデータをフェッチ（Fetch Data From Device）] が [選択したルール（Rules Selected）] オプションに基づいている場合、ヒットカウント保持サポートは有効になりません。ヒットカウント保持サポートは、[デバイスからデータをフェッチ（Fetch Data From Device）] で [すべてのルール（All Rules）] オプションを選択した場合にのみ有効になります。 履歴からデータをフェッチした場合に、[ヒットカウント（Hit Count）] の値がゼロの場合、Security Manager は、ルールの [ヒットカウント履歴（Hit Count History）] に基づいてルールが以前にヒットしたかどうかを確認し、対応する値を表示します。Security Manager が履歴から以前のヒットの値を見つけられない場合、[ヒットカウント（Hit Count）] の値はゼロとして表示されます。

アクセス ルールの有効期限の設定

アクセスルールを頻繁に使用することは、ネットワークへの一時的なアクセスを提供することです。たとえば、特定のプロジェクトの期間中にパートナーアクセスを許可するようなアクセス ルールを設定するとします。この場合、プロジェクトの完了時にはアクセス ルールを削除することが理想的です。しかし、アクセス ルール リストが大きくなるにつれて、リストの管理が困難になり、どのルールを一時的なものとして設定したか覚えていられなくなります。

この問題に対処するために、アクセス規則に有効期限を設定できます。有効期限を設定することにより、ルールが必要でなくなる日時を計画できます。

有効期限は変更可能な日付で、期限切れになったルールが Security Manager によって削除されることはありません。代わりに、期限切れになった場合、Security Manager では、期限切れになったルールの [期限日（Expiration Date）] カラムに「Expired」という太字が表示されます。[期限日（expiration date）] フィールドに基づいて、[アクセスルール（access rules）] ページをフィルタリングできます。たとえば、「expiration date has passed」でフィルタリングすると、期限切れになったすべてのルールが表示されます。

ルールが必要でなくなった場合は、そのルールを削除する（右クリックして [行の削除（Delete Row）] を選択）か、またはディセーブルにし（右クリックして [無効化（Disable）] を選択）、そのあとで設定をデバイスに再展開できます。最初はルールをディセーブルにしておいて、そのルールがあとで必要だとわかったときのために、そのルールを（ハッシュマークが重なって表示された）テーブルに残しておけば、ルールを再作成する時間を節約できます。この場合は、ルールをイネーブルにし（右クリックして [有効化（Enable）] を選択）、設定を再展開するだけです。

有効期限を設定するときに、通知設定も行うことができます。有効期限が近づいたときに通知を受ける電子メールアドレスを指定します。ルールを評価する時間を与えるために、電子メールの通知メッセージの送信日から有効期限までの日数を指定できます。通知設定には、最初は管理設定で（[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [ルールの有効期限（Rule Expiration）] を選択して）設定された値が入力されています。特定のルールに対して別の設定を入力できます。

ルールの有効期限を設定するには、次の手順を実行します。

- 新しいルールを作成する場合、またはルール全部を編集する場合は、[Add Access Rule]/[Edit Access Rule] ダイアログボックス （930 ページ）の [詳細設定（Advanced）] ボタンをクリックして、ルールの有効期限の設定を表示します。
- 既存のルールの場合は、ルール全部を編集せずに、有効期限の設定を追加または編集できます。ルールの [期限日（Expiration Date）] セルを右クリックし、[ルールの期限日の編集（Edit Rule Expiration）] を選択します。複数の行を選択して、同じルール有効期限を設定できます。詳細については、[Advanced]/[Edit Options] ダイアログボックス （936 ページ）を参照してください。

関連項目

- [Rule Expiration] ページ （736 ページ）
- アクセス ルールの設定 （920 ページ）

アクセス コントロール ポリシー設定の指定

セキュリティデバイスアクセス制御リストに適用されるさまざまな設定を指定できます。これらの設定は、アクセスルールポリシーとともに機能します。インターフェイスとトラフィック方向の各組み合わせに対して、またはASA 8.3+デバイスではグローバルACLに対して、独自のACL名を設定できる点が重要です。PIX、ASA、およびFWSMデバイスの場合は、同時フローの最大数および関連するSyslog間隔も制御できます。

また、PIX、ASA、およびFWSMデバイスの場合は、ユーザ単位のダウンロード可能ACLが許可されるようにインターフェイスを設定することもできます。これにより、AAAサーバでユーザベースのACLを設定して、デバイスで定義されているACLを上書きできます。

（注） Security Manager 4.4のリリースとASAのバージョン9.0以降で、IPv4アクセス制御とIPv6アクセス制御を設定するための別個のページが統合されましたただし、それ以前のバージョンのASAでは、IPv6設定用の個別のページが引き続き提供されます。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

関連項目

- アクセス ルールの設定 （920 ページ）

ステップ 1 次のいずれかを実行して、 [Access Control Settings] ページ （944 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから[ファイアウォール（Firewall）]>[設定（Settings）]>[アクセス制御（Access Control）]（または[ファイアウォール（Firewall）]>[設定（Settings）]>[IPv6アクセス制御（IPv6 Access Control）]）を選択します。
- （ポリシービュー）ポリシータイプセレクタから[ファイアウォール（Firewall）]>[設定（Settings）]>[アクセス制御（Access Control）]（または[ファイアウォール（Firewall）]>[設定（Settings）]>[IPv6アクセス制御（IPv6 Access Control）]）を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ページの上部でグローバル設定を指定します。PIX、ASA、およびFWSMデバイスの場合は、現在の拒否フローの最大数および関連するsyslog間隔を定義できます。ASA 8.3以降デバイスの場合、オブジェクトグループ検索をイネーブルにして、Checkpointから変換する際のACLパフォーマンスを最適化できます。ただし、この設定が推奨されるのは、デバイスにメモリの制約がある場合だけです（[IPv6アクセス制御（IPv6 Access Control）]ページでは使用できません）。

これらの設定の具体的な情報、および ACL コンパイルをサポートするプラットフォームについては、[Access Control Settings] ページ （944 ページ）を参照してください。

ステップ 3 ACL 名を設定するインターフェイスごと、またはユーザー単位の ACL をイネーブルにするインターフェイスごとに、テーブルの下の [行の追加（Add Row）] ボタンをクリックし、[Firewall ACL Setting] ダイアログボックス （947 ページ）に値を入力して、インターフェイスをインターフェイステーブルに追加します。次の点を考慮してください。

- ACL 名を設定すると、その名前が特定のインターフェイスおよび方向に適用されます。名前を指定していないインターフェイスと方向の組み合わせに対しては、Security Manager によってシステム生成名が作成されます。
- また、ASA 8.3+ デバイスでは、グローバル ACL の名前も指定できます。

リスト内の既存のエントリを編集するには、そのエントリを選択して [行の編集（Edit Row）] をクリックします。また、リスト内のエントリを削除するには、[行の削除（Delete Row）] をクリックします。

[Access Control Settings] ページ

[Access Control Settings] ページを使用して、アクセス ルール ポリシーとともに使用する値を設定します。パフォーマンスおよびロギングの機能を制御し、各インターフェイスに対して ACL 名を設定できます。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 アクセス制御を設定するための個別のポリシーとオブジェクトが「統合」されました。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスをどちらも使用できる一組のルールになりましたただし、それ以前のバージョンの ASA では、IPv6 設定用の個別のページが引き続き提供されます。（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 （14 ページ）を参照してください）。以下の説明は、特に明記されている場合を除き、すべてのバージョンのページに適用されます。

従って、これらの設定の多くは、特定のデバイスタイプまたはソフトウェアバージョンにだけ適用されます。オプションを設定し、サポートされていないデバイスタイプにポリシーを適用した場合、それらのサポートされていないデバイスではそのオプションが無視されます。

ナビゲーション パス

アクセス制御ページを開くには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、次にポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセス制御（IPv6 Access Control）]**）を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [アクセス制御（Access Control）]**（または **[ファイアウォール（Firewall）] > [設定（Settings）] > [IPv6アクセス制御（IPv6 Access Control）]**）を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [アクセス制御（Access Control）]**（または **[ファイアウォール設定の編集（Edit Firewall Settings）] > [IPv6アクセス制御（IPv6 Access Control）]**）を選択します。

関連項目

- アクセス コントロール ポリシー設定の指定 （943 ページ）
- アクセス ルールについて （913 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 190 : [Access Control Settings] ページ

要素	説明
同時フローの最大数（Maximum number of concurrent flows）（PIX、ASA、FWSM） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	デバイスが作成できる並行拒否フローの最大数。デバイスがこの数に達すると、syslog メッセージ 106101 が生成されます。使用する必要のある範囲は、デバイスで使用可能なフラッシュ メモリの大きさによって異なります。 • 64 MB より大きい：値は 1 ～ 4096 です。デフォルトは 4096 です。 • 16 MB より大きい：値は 1 ～ 1024 です。デフォルトは 1024 です。 • 16 MB 以下：値は 1 ～ 256 です。デフォルトは 256 です。
Syslog 間隔（Syslog interval）（PIX、ASA、FWSM） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	セキュリティ アプライアンスが拒否フローの最大値に達したことを警告する syslog メッセージ 106101 を生成するための時間間隔。拒否フローの最大値に達した場合、最後の 106101 メッセージから指定の秒数が経過すると、新たに 106101 メッセージが生成されます。値は 1 ～ 3600 ミリ秒です。デフォルトは 300 です。

要素	説明
Enable Access List Compilation（グローバル） （IPv4 のみ。[IPv6アクセス制御（IPv6 Access Control）] ページにも表示されません）	アクセス リストをコンパイルするかどうか。コンパイルすると、サイズの大きなルールテーブルの処理が高速になります。コンパイルにより、すべての ACL に対するポリシー ルールおよびパフォーマンスが最適化されます。ただし、コンパイルがサポートされる旧式のプラットフォームの数は次のように限られています。 • ルータ（グローバル設定のみ）：7120、7140、7200、7304、および 7500 • PIX 6.3 ファイアウォール（グローバル モードまたはインターフェイス単位） ACL は、アクセス リスト要素の数が 19 以上である場合にだけコンパイルされます。推奨されるエントリの最大数は 16,000 です。 アクセス リストをコンパイルするには、デバイスに少なくとも 2.1 MB のメモリが必要となります。アクセス リストのコンパイルは、Turbo ACL とも呼ばれます。
Enable Object Group Search（ASA 8.3+） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	ASA 8.3+ デバイスでオブジェクト グループ検索をイネーブルにするかどうか。これにより、オブジェクト グループを展開せずに ACL パフォーマンスを最適化できます。オブジェクト グループ検索は主に、Checkpoint から ASA への移行時に使用されます。デバイスにメモリ制約がある場合（つまり、操作中にメモリが不足しているとわかった場合）は、これによってアクセス ルールの数が大幅に増加することがあります。 オブジェクト グループ検索をイネーブルにした場合、Hit Count ツールを使用してルールを分析することはできません。通常は、この機能をイネーブルにしないでください。代わりに、ルール結合ツールを使用してアクセスルールを簡素化し、すべてのインターフェイスで実施するルールに対してはグローバルルールを使用することを検討してください。
オブジェクトグループ検索のしきい値の有効化（Enable Threshold Object Group Search） （IPv4 のみ。[IPv6アクセス制御（IPv6 Access Control）] ページにも表示されません）	オブジェクトグループ検索のしきい値制限を有効にするには、このボックスをオンにします。デフォルトでは、しきい値は有効になっていません。

要素	説明
[アクセス制御の設定（Access Control settings）] テーブル	このテーブルには、特別な処理を設定するインターフェイスが示されます。[インターフェイス名（Interface Name）] は、特定のインターフェイスまたはインターフェイスロールを指します。また、ASA 8.3+ デバイスでのグローバル ACL 設定の場合は、[グローバル（Global）] です。 このテーブルを使用すると、Security Manager によるシステム生成名の自動設定を行わない場合に、ACL に名前を設定できます。この名前は、インターフェイスに対して生成された特定方向の ACL に適用されます。 ユーザー単位のダウンロード可能ACL、オブジェクトグループ検索およびACLコンパイルに対して、インターフェイスレベルの設定を行うこともできます。 • アクセス制御のインターフェイス設定を追加するには、[行の追加（Add Row）] ボタンをクリックし、[Firewall ACL Setting] ダイアログボックス （947 ページ）に入力します。 • アクセス制御のインターフェイス設定を編集するには、インターフェイス設定を選択し、[行の編集（Edit Row）] ボタンをクリックします。 • アクセス制御のインターフェイス設定を削除するには、インターフェイス設定を選択し、[行の削除（Delete Row）] ボタンをクリックします。

（注） CSMは、ASAデバイスの前方参照オプションをサポートしていません。CSMは、参照リンクが正しく確立されていないデバイスで設定されている CLI を検出しません。これらの CLI はサポート対象外として分類され、CSM 経由で管理されません。

[Firewall ACL Setting] ダイアログボックス

[ファイアウォールACL設定（Firewall ACL Setting）] ダイアログボックスを使用して、セキュリティデバイス アクセス ルール ポリシーとともに使用する、特定のインターフェイス、インターフェイスロール、またはグローバルルールの設定を行います。

ナビゲーション パス

[Access Control Settings] ページ （944 ページ）に移動し、インターフェイステーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- アクセス コントロール ポリシー設定の指定 （943 ページ）
- アクセス ルールについて （913 ページ）
- グローバル アクセス ルールについて （915 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *191 : [Firewall ACL Setting]* ダイアログボックス

要素	説明
インターフェイス（Interface） Global（ASA 8.3+）	設定の対象が特定のインターフェイス（またはインターフェイス ロール）か、あるいは ASA 8.3+ デバイスのグローバルルールかを指定します。 [インターフェイス（Interface）] を選択した場合は、設定するインターフェイスまたはインターフェイスロールの名前を指定します。名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 [Global] を選択した場合は、グローバル ACL の名前を指定するオプションしかありません。
トラフィックの方向	インターフェイスを通過するトラフィックの方向（[イン（in）] または [アウト（out）]）。方向が関係する場合、設定した値はこの方向にだけ適用されます。 ASA 8.3+ デバイスでは、グローバル ACL の方向は常に [in] です。

要素	説明
ユーザー定義の ACL 名（[IPv6アクセス制御（IPv6 Access Control）] ページにチェックボックスは表示されない） ACL Name	ACL に名前を指定するかどうか。このオプションを選択した場合、使用する名前を入力します。これは、インターフェイスと方向の組み合わせに対して生成された ACL に適用されます。名前は、デバイス上で一意である必要があります。 ASA 8.3+ デバイスでグローバル ACL に名前を設定する場合、オプションは自動的に選択されるため、目的の名前を入力するだけです。 （注） ファイアウォールルールの ACL 名が一意であり、Policy Object Manager で定義された ACL オブジェクトと同じ名前でないことを確認してください。詳細については、アクセス コントロール リスト オブジェクトの作成（356 ページ）を参照してください。 名前を設定しなかった場合は、Security Manager により自動的に名前が生成されます。
Enable Per User Downloadable ACLs（PIX、ASA、FWSM） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	ユーザ単位の ACL のダウンロードをイネーブルにしてインターフェイス上の ACL を上書きするかどうか。ユーザ ACL は、Security Manager で設定されるのではなく、AAA サーバで設定されます。ユーザ単位の ACL がない場合は、インターフェイスに設定されているアクセスルールがトラフィックに適用されます。 このオプションは、トラフィックの方向が[イン（in）]の場合にのみ、指定されたインターフェイスのデバイスで設定されます。
Enable Object Group Search（PIX 6.x） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	PIX 6.x インターフェイスでオブジェクトグループ検索をイネーブルにするかどうか。イネーブルにすると、サイズの大きいACLを保持するためのデバイスのメモリ要件が少なくなります。ただし、オブジェクト グループ検索によって、各パケットでの ACL 処理が低速になるため、パフォーマンスに影響します。 非常に大きなオブジェクトグループが存在する場合は、オブジェクトグループ検索を推奨します。 ヒント ASA 8.3+ デバイスでは、オブジェクト グループ検索の設定は、[Access Control Settings] ページ （944 ページ）で行います。

要素	説明
Enable Access List Compilation（PIX 6.x） （[IPv6アクセス制御（IPv6 Access Control）] ページには表示されません）	PIX 6.x デバイスで、このインターフェイス上のアクセス リストをコンパイルするかどうか。この設定は、[Access Control Settings] ページで設定した同等のグローバル設定を上書きします。 ACL をコンパイルすると、サイズの大きいルールテーブルの処理が高速になり、インターフェイスのポリシールールおよびパフォーマンスが最適化されます。ACL は、アクセス リスト要素の数が 19 以上である場合にだけコンパイルされます。推奨されるエントリの最大数は 16,000 です。 アクセス リストをコンパイルするには、デバイスに少なくとも 2.1 MB のメモリが必要となります。

自動競合検出の使用

Security Manager は、アクセスルール向けの自動競合検出機能を提供します。自動競合検出を使用すると、アクセスルールのロジックを評価できます。自動競合検出が有効になると、アクセスルールポリシー内の他のルールと重複または競合するルールが識別されます。この情報を使用して、削除、移動、または編集が必要なルールを特定します。

ここでは、次の内容について説明します。

- 自動競合検出について （950 ページ）
- 自動競合検出のユーザー インターフェイスについて （952 ページ）
- 競合の解決 （957 ページ）

自動競合検出について

Security Manager には、不要な冗長または重複したルールを特定するのに役立つ自動競合検出機能が用意されています。競合していても、導入後にデバイスに影響しないルールもありますが、ルールテーブルに不要なクラスタが作成されます。そのようなルールを検出することにより、ルールセットをクリーンアップして、より使いやすく、効率的なアクセスルールポリシーを作成することができます。

競合するルールによっては、ネットワークに望ましくない結果が生じる可能性があります。それらの競合するルールを検出することにより、セキュリティ面のニーズを意図したとおり満たすために削除、移動、または編集する必要のあるルールを特定できます。

（注） 競合検出機能は、2つのルール間での最初の競合を報告します。特定のルールと競合する付加的な複数のルールがテーブルにある場合、最初の競合が解決されるまで、それらのルールについては報告されません。

Security Manager によって検出された競合は、次のように分類されます。

- 冗長オブジェクト：ルールのフィールドに含まれる 1 つの要素が、ルールの同じフィールドに含まれる 1 つ以上の要素のサブセットになっています。次の例では、ソースセルに *net-group2* と *net-group1* の 2 つのネットワークオブジェクトがあります。*net-group2* は *net-group1* のサブセットなので、冗長なオブジェクトであり、安全に削除できます。

```
object-group network net-group1
network-object 10.2.0.0 255.255.0.0
object-group network net-group2
network-object 10.2.1.1 255.255.255.255
```

- 冗長なルール：基本ルールでも 2 つのルールによって同じタイプのトラフィックに同じ処理が適用される場合、基本ルールを削除しても最終的な結果は変わりません。たとえば、特定のネットワークの FTP トラフィックを許可するルールに、同じネットワークの IP トラフィックを許可するルールが続き、その間にアクセスを拒否するルールがない場合、最初のルールは冗長であり、削除できます。

次に、冗長なルールの単純な例を示します。

```
access-list acl permit ip 2.1.1.1 255.255.255.255 any
access-list acl permit ip 2.1.1.0 255.255.255.0 any
```

- 部分的に冗長なルール：複合ルールの一部が、1 つのルールまたはそれに続く複合ルールの一部に対して冗長になっています。

- シャドウイング状態のルール：これは、冗長なルールの逆です。この場合は、あるルールが別のルールと同じトラフィックに一致し、2 番目のルールはアクセスリスト内であとに配置されているためにいずれのトラフィックにも適用されません。両方のルールのアクションが同じ場合は、シャドウイング状態のルールを削除できます。2 つのルールがトラフィックに対して異なるアクションを指定している場合、必要なポリシーを導入するには、シャドウイング状態のルールを移動するか、いずれかのルールの編集が必要になる場合があります。たとえば、1 つの送信元または宛先に対して、基本ルールで IP トラフィックを拒否し、シャドウイング状態のルールで FTP トラフィックを許可する場合などです。

次に、シャドウイング状態のルールの単純な例を示します。

```
access-list acl permit ip 1.0.0.0 255.0.0.0 any
access-list acl permit ip 1.1.0.0 255.255.0.0 any
```

（注） 重複するルールは、自動競合検出機能によって、シャドウイング状態のルールとして報告されます。

- 部分的にシャドウイング状態のルール：複合ルールの一部が、その前のルールによってシャドウイングされます。両方のルールのアクションが同じ場合は、ルールのシャドウイングされている部分を削除できます。2つのルールがトラフィックに対して異なるアクションを指定している場合、必要なポリシーを導入するには、シャドウイング状態のルールを移動するか、いずれかのルールの編集が必要になる場合があります。

自動競合検出の範囲

競合を検出する際、Security Manager は、アクセスルールに含まれる次の情報を評価します。

- source
- destination
- サービス
- ユーザ
- interfaces

（注） 競合検出には、次の注意事項が適用されます。

- 競合検出は、デバイスまたは共有ポリシーのアクセスルールポリシーに含まれるアクセスルールに対してのみ使用できます。競合検出は、AAAルールや検査ルールなど、他のポリシーの一部であるアクセスルールに対しては使用できません。
- ルールに FQDN ネットワーク/ホストオブジェクトが含まれている場合、FQDN オブジェクトは無視されますが、そうではない場合は FQDN オブジェクトが分析に含まれます。
- 無効化されたルールは、競合検出時に評価されません。
- 競合検出では、アクセスルールの評価の際、時間範囲は考慮されません。競合検出時にフラグが立てられたルールを削除する前に、該当するルールが本当に競合していることを確認してください。

関連項目

- 自動競合検出のユーザー インターフェイスについて （952 ページ）
- 競合の解決 （957 ページ）
- アクセス ルールについて （913 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- アクセス ルールの設定 （920 ページ）

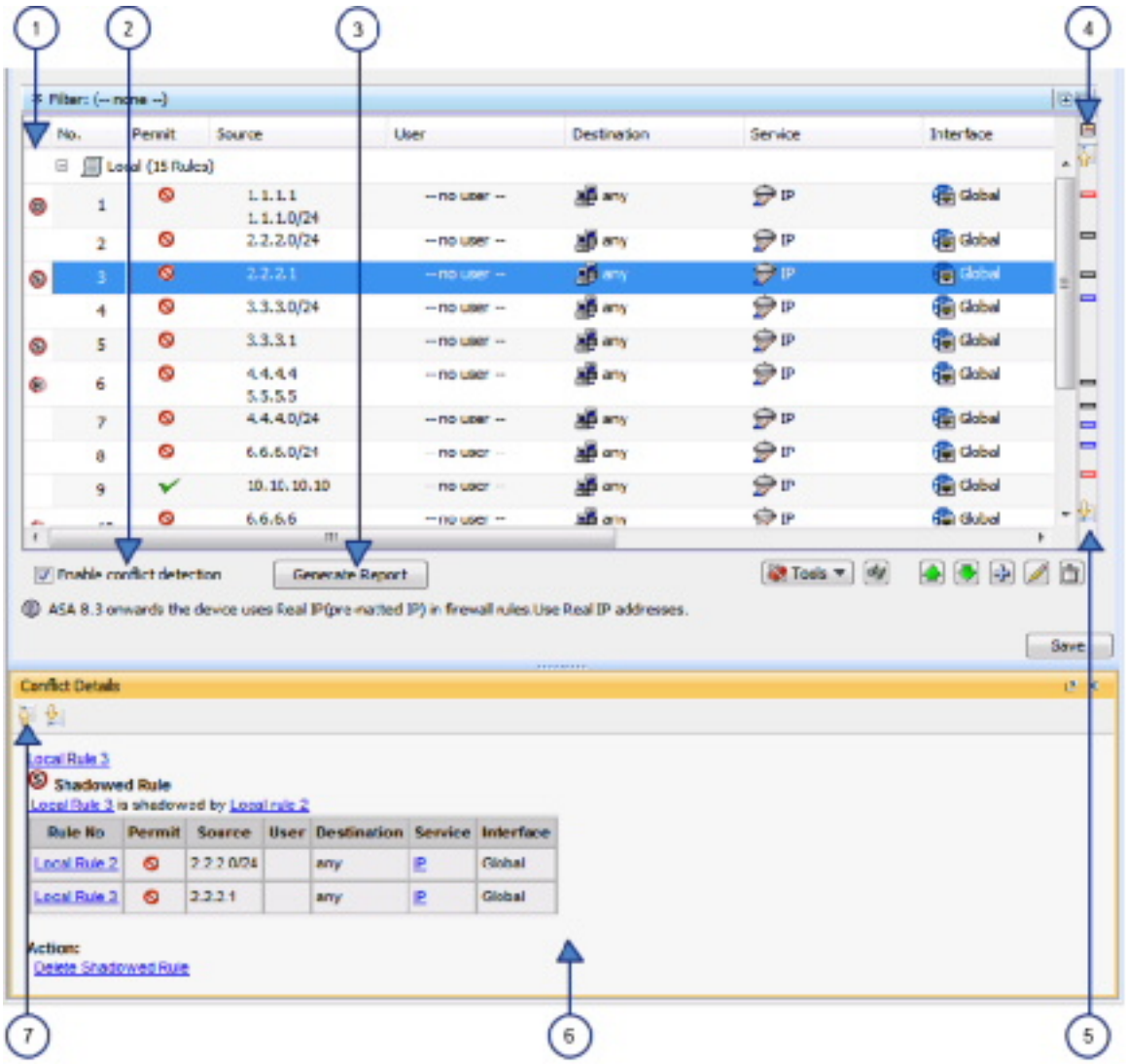
自動競合検出のユーザー インターフェイスについて

自動競合検出機能は、競合を識別し、それらの競合をより迅速かつ簡単に解決するために、アクセスルールテーブルと緊密に結合されています。競合検出が有効になっている場合、競合間

を移動したり、競合を解決したりするために、追加のユーザーインターフェイス要素を使用できます。

（注） アクセスルール ページの標準的な要素については、[Access Rules] ページ （924 ページ）を参照してください。

図 *24 :* 自動競合検出



1	競合インジケータアイコン	2	競合検出の有効化
3	[Generate Report] ボタン	4	注釈表示オプション
5	競合ナビゲーションバー	6	競合の詳細領域

1	競合インジケータアイコン	2	競合検出の有効化
7	競合ナビゲーションボタン		

競合インジケータアイコン

競合インジケータアイコンは、競合を識別し、競合の種類をすばやく視覚的に表現するために使用されます。次の表に、使用可能なアイコンの詳細を示します。

（注） 競合の種類の説明については、自動競合検出について （950 ページ）を参照してください。

	冗長オブジェクト
	冗長ルール
	部分的な冗長ルール
	シャドウルール
	部分的なシャドウルール
（注） アクセスルールに複数の競合がある場合、またはユーザーメモが添付されている場合、そのルールの競合インジケータアイコンに小さなプラス記号（+）が表示されます。	

[競合インジケータ（Conflict Indicator）]アイコンを使用すると、次のアクションを実行できます。

- [競合インジケータ（Conflict Indicator）]アイコンにマウスポインタを合わせると、競合に添付されたユーザーメモを含め、競合の説明が表示されます。
- [競合インジケータ（Conflict Indicator）]アイコンをクリックするか、アイコンを右クリックして[競合の詳細を表示（Show Conflict Detail）]を選択して、選択した競合の[競合の詳細（Conflict Details）]ペインを開きます。
- 冗長オブジェクトの[競合インジケータ（Conflict Indicator）]アイコンを右クリックし、[冗長オブジェクトの削除（Remove Redundant Object）]を選択して、ルールから冗長オブジェクトを削除します。
- [競合インジケータ（Conflict Indicator）]アイコンを右クリックし、[ユーザーメモの追加（Add User Note）]を選択して、選択した競合の[ユーザーメモの追加（Add User Note）]ダイアログボックスを開きます。[ユーザーメモの追加（Add User Note）]ダイアログボックスを使用して、競合に関するメモを入力できます。このメモは、後でルール分析詳細レポートに含めることができます。

（注） アクセスルールページを終了するとき、またはユーザーメモが入力されたルールを編集した後は、ユーザーメモは保存されません。

競合検出の有効化

[競合検出の有効化（Enable Conflict Detection）] オプションは、自動競合検出を有効にするかどうかを制御します。競合検出はデフォルトで有効になっていますが、このオプションの選択を解除すると無効にできます。この設定はユーザーごとに管理され、1つのアクセスルールテーブルの競合検出を有効または無効にすると、他のアクセスルールテーブルの機能も有効または無効になります。

レポートの作成（Generate Report）

競合検出が有効になっている場合は、[レポートの生成（Generate Report）] ボタンをクリックして、競合の HTML レポートを作成し、出力したり、別のツールにエクスポートしたりできます。ルール分析の詳細レポートには、ルールテーブル内のすべての競合の詳細が表示され、競合について入力されたユーザーのメモが含まれています。[注釈表示オプション（Annotation Display Options）] ダイアログボックスで選択した設定は使用されず、テーブルに定義されているフィルタ設定は考慮されません。

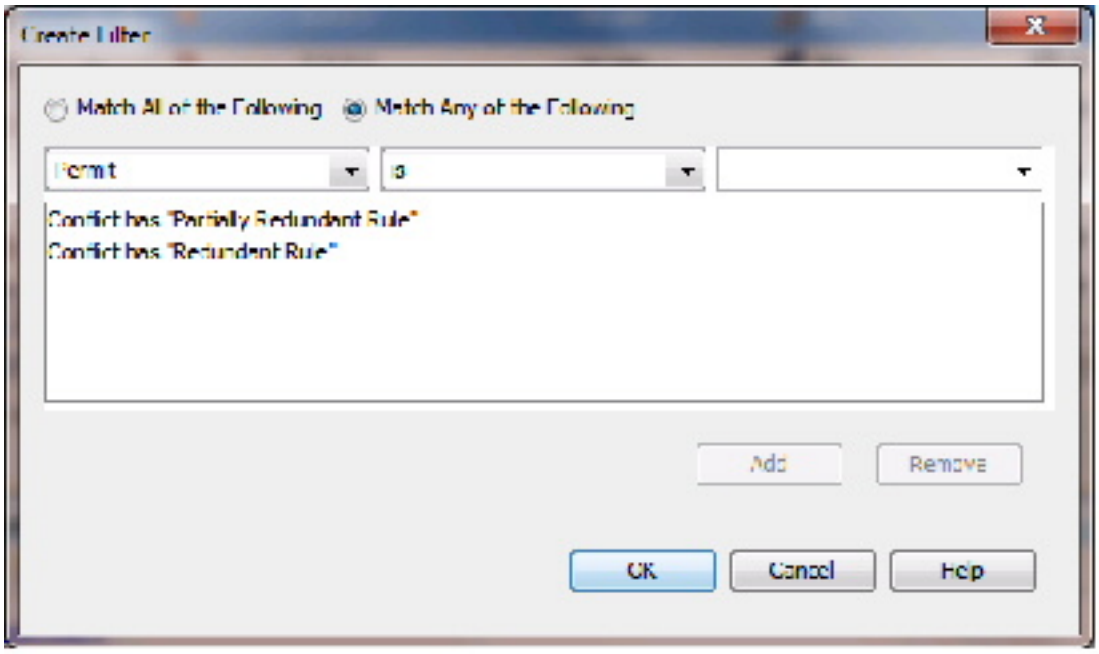
（注） アクセスルールページを終了するとき、またはユーザーメモが入力されたルールを編集した後は、ユーザーメモは保存されません。

最初に [アクセスルール（Access Rules）] ページを開くと、[レポートの生成（Generate Report）] ボタンが進行状況バーに置き換えられます。競合分析が完了すると、他の競合検出機能とともに [レポートの生成（Generate Report）] ボタンが使用できるようになります。

[注釈表示オプション（Annotation Display Options）] ボタン

[注釈表示オプション（Annotation Display Options）] ボタンをクリックすると、[注釈表示オプション（Annotation Display Options）] ダイアログボックスが開きます。このダイアログボックスは、報告する必要のある競合のタイプを選択するために使用します。競合の種類の説明については、自動競合検出について （950 ページ）を参照してください。

特定のタイプの競合を無効にしても、それらのルールはアクセスルールテーブルから削除されません。これらのタイプの競合に対する、ルールの競合通知がオフになるだけです。特定のタイプの競合ルールのみを非表示または表示するには、テーブルフィルタ機能を使用できます。たとえば、冗長および部分的に冗長なルールの競合のみを確認したい場合は、次の高度なフィルタを設定できます。



マウスポインタを [注釈表示オプション（Annotation Display Options）] ボタンの上に置くと、各タイプの競合の概要を表示でき、無効になっている競合タイプの確認もできます。

（注） 選択した [注釈表示オプション（Annotation Display Options）] は、オプションが変更されるまで有効です。競合の解決に取り組んでいるときは常に、これらの設定を確認してください。

競合ナビゲーションバー

競合ナビゲーションバーを使用して、競合に移動します。競合ナビゲーションバーの [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用して、競合間を移動できます。競合ナビゲーションバーの競合ロケータの 1 つをクリックして、特定の競合に直接移動することもできます。これは、大きなルールテーブルを操作する場合に特に役立ちます。

ヒント 競合ロケーターにカーソルを合わせると、競合の簡単な概要が表示されます。

競合ロケータは、次のように色分けされています。

- **赤色のロケータ**：冗長オブジェクト
- **青色のロケータ**：冗長ルールおよび部分的に冗長なルール
- 黒のロケーター：シャドウルールおよび部分的なシャドウルール

競合の詳細領域

[競合の詳細（Conflict Details）] ペインには、選択した競合の詳細が表示されます。必要に応じてペインをドッキングしたり、ドッキングを解除したりできます。[競合の詳細（Conflict Details）] ペインがドッキングされているときに [Policy Object Manager] ペインもドッキングされている場合、ウィンドウの下部にあるタブを使用して 2 つの機能間を移動できます。

直接比較しやすいように、競合するルールがテーブルにまとめて表示されます。競合のタイプはテーブルの上に表示されます。手動で解決する必要がある、部分的に冗長なルールと部分的にシャドウされたルールを除くすべての競合について、テーブルの下に推奨のアクションが表示されます。関連するルールへの直接移動するためのリンクがあります。競合するルールの一部であるポリシーオブジェクトをクリックして展開すると、オブジェクトの内容が表示されます。もう一度クリックすると、ポリシーオブジェクトが折りたたまれます。

提供されているリンクを使用して、競合するルールに移動できます。[アクション（Action）] の下のリンクをクリックして、Security Manager に提案されたアクションを自動的に実行させることもできます。

競合ナビゲーションボタン

[競合の詳細（Conflict Details）] ペインの上部にある [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用すると、[競合の詳細（Conflict Details）] ペインを離れることなく、解決する必要がある競合間を移動できます。

関連項目

- 自動競合検出について （950 ページ）
- 競合の解決 （957 ページ）
- アクセス ルールについて （913 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- アクセス ルールの設定 （920 ページ）

競合の解決

次の手順では、自動競合検出機能を使用してアクセスルールの競合を解決する方法について説明します。

ヒント Combine Rules ツールを使用して、ルールを評価するように Cisco Security Manager を設定し、より効率のよいルールに結合する方法を理解できます。詳細については、ルールの結合 （785 ページ）を参照してください。

関連項目

- 自動競合検出について （950 ページ）
- 自動競合検出のユーザー インターフェイスについて （952 ページ）
- アクセス ルールについて （913 ページ）
- デバイス固有のアクセス ルールの動作について （917 ページ）
- アクセス ルールのアドレス要件およびルールの展開方法について （918 ページ）
- アクセス ルールの設定 （920 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）]>[アクセスルール（Access Rules）]** の順に選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules]** を選択し、既存のポリシーを選択します。

[Access Rules] ページ （924 ページ）が開きます。競合検出が有効になっている場合、テーブルのロード後にアクセスルールの競合が分析されます。競合検出が無効になっている場合、[競合検出の有効化（Enable Conflict Detection）] を選択して競合分析を開始します。

分析の進行状況は、ルールテーブルの下に表示されます。競合検出機能以外の機能は、ルールの分析中にルールテーブルに対して実行できます。分析が完了すると、競合検出機能が有効になります。

ステップ 2 分析対象のルールがルールテーブルに表示されていることを確認してください。確認には、セクションの展開、およびフィルタを使用している場合は各フィルタが正しく設定されていることの確認が含まれます。フィルタ処理されているルール、または折りたたまれているセクションにあるルールは、競合検出分析に含まれません。

ヒント アクセスルールテーブルの上にある [フィルタ（Filter）] 領域の右上隅にある [すべての行を展開（Expand all rows）] または [すべての行を折りたたむ（Collapse all rows）] ボタンを使用して、ルールテーブルのすべてのセクションをすばやく展開または折りたたむことができます。

ステップ 3 垂直スクロールバーの右側にある競合ナビゲーションバーの上にある [注釈表示オプション（Annotation Display Options）] ボタンをクリックして、[注釈表示オプション（Annotation Display Options）] ダイアログボックスを開きます。検出する競合のタイプがすべて有効になっていることを確認し、[OK] をクリックします。

ヒント マウス ポインタを [注釈表示オプション（Annotation Display Options）] ボタンの上に置くと、各タイプの競合の概要を表示でき、無効になっている競合タイプの確認もできます。

（注） 選択した [注釈表示オプション（Annotation Display Options）] は、オプションが変更されるまで有効です。競合の解決に取り組んでいるときは常に、これらの設定を確認してください。

ステップ 4 ルールテーブルで見つかった競合のコピーを印刷または保存する場合は、[レポートの生成（Generate Report）] をクリックします。

ブラウザでルール分析詳細レポートが開きます。ルール分析詳細レポートには、ルールテーブル内のすべての競合の詳細が表示されます。[注釈表示オプション（Annotation Display Options）] ダイアログボックスで選択した設定は使用されず、テーブルに定義されているフィルタ設定は考慮されません。レポートは、保存したり、必要に応じて印刷したりできます。

ステップ 5 競合ナビゲーションバーを使用して、競合に移動します。競合ナビゲーションバーの [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用して、競合間を移動できます。競合ナビゲーションバーの競合ロケータの 1 つをクリックして、特定の競合に直接移動することもできます。これは、大きなルールテーブルを操作する場合に特に役立ちます。

ヒント 競合ロケータにカーソルを合わせると、競合の簡単な概要が表示されます。

競合ロケータは、次のように色分けされています。

- **赤色のロケータ**：冗長オブジェクト
- **青色のロケータ**：冗長ルールおよび部分的に冗長なルール
- **灰色のロケータ**：シャドウルールおよび部分的にシャドウされたルール

ステップ 6 選択した競合の [競合インジケータ（Conflict Indicator）] アイコンをクリックして、[競合の詳細（Conflict Details）] ペインを開きます。[競合インジケータ（Conflict Indicator）] アイコンの詳細については、自動競合検出のユーザー インターフェイスについて （952 ページ）を参照してください。

[競合の詳細（Conflict Details）] ペインには、選択した競合の詳細が表示されます。直接比較しやすいように、競合するルールがテーブルにまとめて表示されます。競合のタイプはテーブルの上に表示されます。手動で解決する必要がある、部分的に冗長なルールと部分的にシャドウされたルールを除くすべての競合について、テーブルの下に推奨のアクションが表示されます。関連するルールへの直接移動するためのリンクがあります。競合するルールの一部であるポリシーオブジェクトをクリックして展開すると、オブジェクトの内容が表示されます。もう一度クリックすると、ポリシーオブジェクトが折りたたまれます。

ステップ 7 提供されているリンクを使用してルールに移動し、必要に応じて競合を解決するか、[アクション（Action）] の下にあるリンクをクリックして、提案されたアクションを Cisco Security Manager に自動的に実行させます。

（注） この時点で競合を解決しない場合は、アクセスルールテーブルの競合の左側にある [競合インジケータ（Conflict Indicator）] アイコンを右クリックし、[ユーザー ノートの追加（Add User Note）] を選択して、競合に関するメモを入力できます。ユーザーメモはルール分析詳細レポートに含まれますが、[アクセスルール（Access Rules）] ページを終了するとき、またはユーザーメモを含むルールを編集した後は保存されません。

ステップ 8 競合ナビゲーションバー、または [競合の詳細（Conflict Details）] ペインの上部にある [前の競合（Previous Conflict）] ボタンと [次の競合（Next Conflict）] ボタンを使用して、解決する必要があるその他の競合にアクセスします。

ステップ 9 この時点で解決しない競合が残っている場合は、必要に応じて、[レポートの生成（Generate Report）] をクリックして、残りの競合のコピーを印刷または保存できます。

ヒットカウントの詳細の表示

[ヒットカウントの詳細（Hit Count Details）] ウィンドウを使用して、アクセスルールがトラフィックに適用された回数に関する情報を表示します。これらのルールは、デバイス上でインターフェイス ACL となるルールです。このヒット カウント結果には、他のタイプの ACL（クラス マップまたは AAA ルールで使用される ACL など）のカウントは示されません。

ASA 8.3(1) 以降のデバイスに関するアクセスルールの場合、詳細なヒットカウントレポートには、アクセスルールポリシーがトラフィックに最後に適用された時刻も表示されます。この情報は、他のポリシーの変更によって置き換えられた可能性があるルールを判断するのに役立ちます。

ヒット カウント情報を使用すると、アクセス ルールのデバッグに役立ちます。この情報は、ヒットしたことがない（つまり、不要であるか、または ACL における優先度の高いルールと重複している可能性がある）ルールや、頻繁にヒットする（つまり、改良が必要な）ルールを識別するのに役立ちます。

ヒント ルールの詳細を表示する前に、ページの下部にある [ヒットカウントの更新（Refresh Hit Count）]ボタンをクリックして、ヒットカウント情報を更新できます。詳細については、[Hit Count Selection Summary] ダイアログボックス （939 ページ）を参照してください。

ヒットカウントの詳細を分析する際には、次の点を考慮してください。

- ヒット カウントの表示前に、デバイスにポリシーを展開すると、最善の結果が得られます。デバイスを検出し、ヒット カウント レポートを生成したあとで展開した場合、結果が不完全になったり、解釈が困難になることがあります。たとえば、アクセス ルールにヒット カウント情報が含まれないことがあります。
- ヒット カウント統計は、インターフェイスではなく ACL に基づきます。[Cisco Security Manager管理の展開（Security Manager Administration Deployment）] ページ（[Deployment] ページ （658 ページ）を参照）で [ファイアウォールルールに対するACL共有の有効化（Enable ACL Sharing for Firewall Rules）] を選択した場合、共有 ACL により、その ACL を共有するすべてのインターフェイスの情報を統合した統計情報が提供されます。
- ファイアウォール ルールの展開時のネットワーク オブジェクト グループの最適化 （802 ページ）の説明に従ってネットワーク オブジェクト グループ最適化をイネーブルにした場合、正確なヒット カウント情報が得られない可能性があります。
- 展開中のアクセス ルールの自動最適化 （973 ページ）の説明に従ってACL最適化をイネーブルにした場合、ヒット カウント結果でのデバイスからアクセス ルールへの ACE のマッチングに問題がある可能性があります。このため、アクセスルールを選択したときに、そのルールに対するカウント結果が得られないことがあります。
- FQDN ネットワーク/ホストオブジェクトは無視されます。これらのオブジェクトのヒット カウント情報は取得できません。

- ヒットカウントと最終ヒット時間の情報は、デバイスの再起動時にクリアされます。
- 同じルール内または異なるルール内の複製された ACE のヒットカウントは、常に 0 に設定されます。

はじめる前に

ヒット カウント レポートには次の制限事項があります。

- ヒット カウント レポートは、デバイスに固有です。このレポートは、デバイスビューからのみ、一度に 1 つのデバイスに対して生成できます。レポートを生成する前に、デバイスにポリシーを展開する必要があります。
- ASA 8.3+ デバイスでオブジェクト グループ検索をイネーブルにした場合は、Hit Count ツールを使用できません。オブジェクト グループ検索は、[Access Control Settings] ページ（944 ページ）で設定します。
- FQDN ネットワーク/ホストオブジェクトを含むルールを選択できますが、それらのオブジェクトはヒットカウントの結果では無視されます。

ナビゲーション パス

（デバイスビューのみ）[Access Rules] ページ （924 ページ）で、テーブル内のルールの [ヒットカウント（Hit Count）] セルを右クリックし、[ヒットカウントの詳細を表示（Show Hit Count Details）] を選択します。

[ヒットカウントの詳細（Hit Count Details）] ウィンドウが、アクセスルールテーブルの下部にペインとして開きます。タイトルバーの右側にある [展開（expand）] ボタンをクリックして、ヒットカウントの詳細を別のウィンドウに表示します。

関連項目

- アクセス ルールについて （913 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）

フィールド リファレンス

表 *192 : [ACE*ヒットカウントの詳細（*ACE Hit Count Details***）*]*ウィンドウ**

要素	説明
移行方法	ヒットカウント情報の表示方法として、[展開されたテーブル（Expanded Table）] または [未展開のACE（Raw ACE）] を選択できます（それぞれの説明を参照）。

要素	説明
展開されたテーブル	このビューには、このウィンドウを開いたときに [アクセスルール（Access Rules）] テーブル（[Access Rules] ページ （924 ページ））で選択したルールのアクセス制御リストエントリ（ACE）のヒットカウント情報が表示されます。ポリシーをデバイスに展開したときにアクセス ルールによって複数の ACE が生成された場合、このリストには複数の ACE が含まれます。 このテーブルの列は、[アクセスルール（Access Rules）] テーブルの列と対応していますが、ルールに含まれているネットワーク/ホスト、サービス、またはインターフェイス ロール オブジェクトの代わりに、ACE で設定されている特定のデータが含まれている場合があります。ただし、IOS 12.4(20)T 以降のデバイスは例外で、オブジェクトレベルのデータだけが表示されます。また、ACE を含む ACL の名前も表示されます。 [差分（Delta）] 列に、最後の更新以降の ACE に関するヒットカウントの差分が表示されます。[Hit Count] カラムには、ルール全体ではなく特定の ACE に対するヒット数が表示されます。 このテーブルの例については、[サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ （963 ページ）を参照してください。 **ヒント** 複数の列を同時にソートするには、Ctrl キーを押しながら列見出しをクリックします。ソートできるカラムは、[Interface]、[Direction]、および [ACL Name] 以外のカラムです。
未展開のACE（Raw ACE）	このビューには、[ヒットカウント（Hit Count）] と [最後のヒット時刻（Last Hit Time）] とともに、アクセス制御エントリに対する実際の CLI が表示されます。デバイス コマンドを評価する方が慣れている場合は、この情報を使用してください。 このテーブルの例については、[サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ （963 ページ）を参照してください。
（注） バージョン 4.9 以降、Cisco Security Manager では、[展開されたテーブル（Expanded Table）] と [未展開のACE（Raw ACE）] オプションでヒットカウントの履歴を表示できます。[履歴を表示（Show History）] リンクをクリックして、新しいウィンドウにヒットカウントの履歴を表示します。この新しい [ヒットカウント履歴の詳細（Hit Count History Details）] ウィンドウには、[ヒットカウント（Hit Count）] と [最後のヒット時刻（Last Hit Time）] の情報が表示されます。	

[サンプルヒットカウントの詳細（Sample Hit Count Details）] ウィンドウ

ヒットカウントレポートを生成して、アクセスルールポリシー内の各ルールがトラフィックに一致する頻度を判断できます。たとえば、インターフェイス ロールを使用してルールを定義し、ロールが複数のインターフェイスに適用された場合、アクセス ルールが複数の Access Control Entries（ACE; アクセス コントロール エントリ）として展開されると、展開された ACE ごとに個別のヒット カウント情報が表示されます。このヒット カウント結果には、他のタイプの ACL（クラス マップまたは AAA ルールで使用される ACL など）のカウントは示されません。

ASA 8.3(1) 以降のデバイスに関するアクセスルールの場合、ヒットカウントレポートには、アクセスルールポリシーがトラフィックに最後に適用された時刻も表示されます。この情報は、他のポリシーの変更によって置き換えられた可能性のあるルールを判断するのに役立ちます。

ヒット カウント情報を使用すると、アクセス ルールのデバッグに役立ちます。この情報は、ヒットしたことがない（つまり、不要であるか、または ACL における優先度の高いルールと重複している可能性がある）ルールや、頻繁にヒットする（つまり、改良が必要な）ルールを識別するのに役立ちます。

次の各図に、ヒット カウント レポートの例と情報の使用方法を示します。

- 図 25 : 展開されたテーブル （964 ページ）は、デフォルトのビューを示しています。上半分のテーブルには、アクセス ルール ポリシー内に存在するルールが一覧表示されます。すべてのルールが表示されるか、またはレポートの生成前に選択したルールだけが表示されます。ルールを選択すると、そのルールに対してデバイス上で作成された ACE が、ウィンドウの下半分の展開されたテーブル内に一覧表示されます。最初にレポートを開くと、展開されたテーブルに、上半分のテーブル内に一覧表示されているすべてのポリシーに対する ACE が表示されます。

展開されたテーブル内のヒット カウントは、各 ACE に対応しています。一方、ルール テーブル内のカウントは、ルールにより作成されたすべての ACE に対するヒット カウントの合計です。ASA/PIX/FWSM デバイスおよび 12.4(20)T よりも前の IOS デバイスでは、展開されたテーブルに、ルールで使用されているポリシー オブジェクト内の各要素に対するヒット カウントが表示されます。一方、IOS 12.4(20)T+ デバイスでは、オブジェクト グループ レベルの情報だけが提供されます。

- 図 26 : 未展開の ACE テーブル （965 ページ）は同じ ACE を CLI 形式で示しています。これらは、デバイス設定に存在する ACE です。

  ヒット カウント レポートの判読および解釈方法の詳細については、 ヒットカウントの詳細の表示 （960 ページ）を参照してください。

図 *25* : 展開されたテーブル

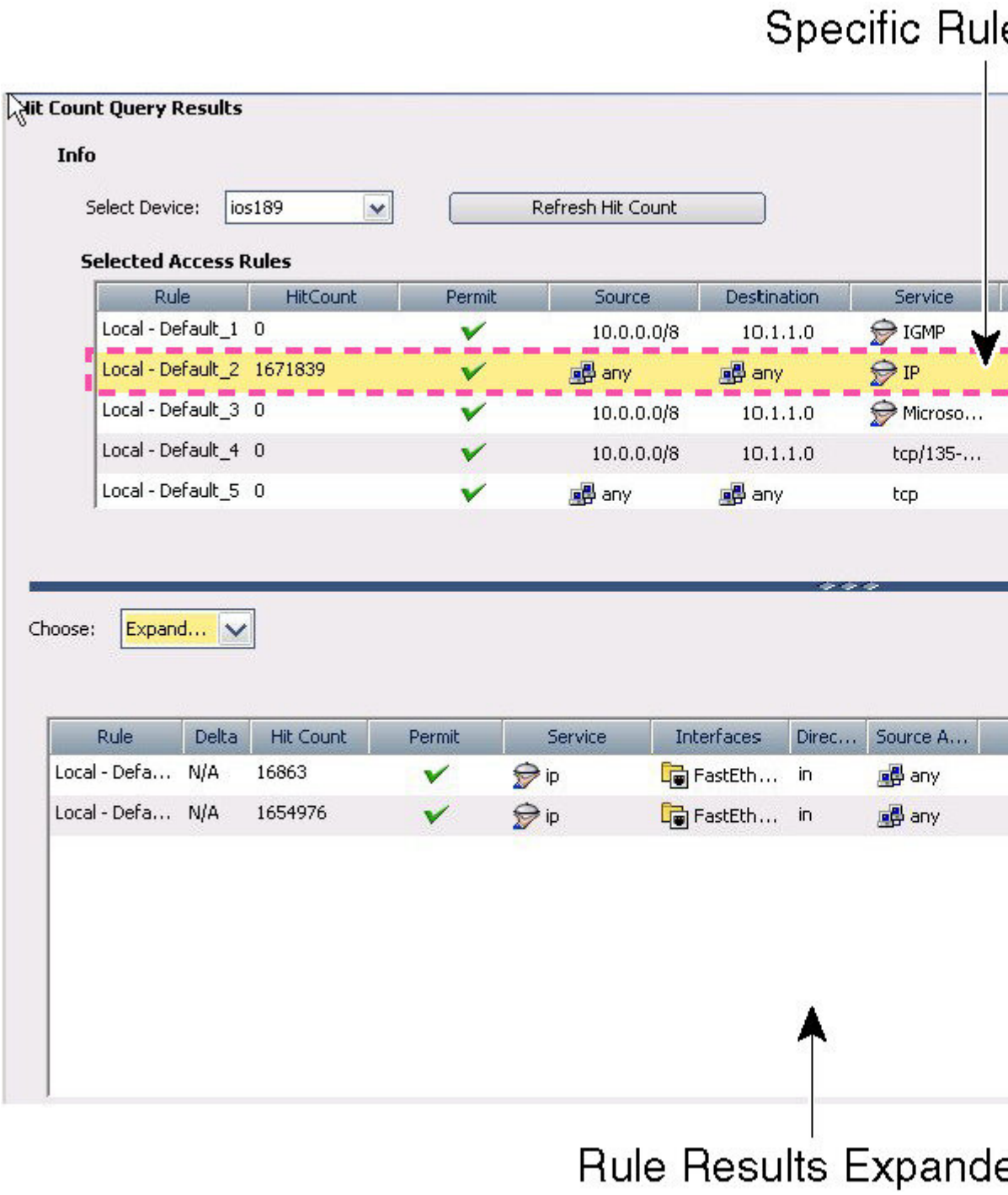
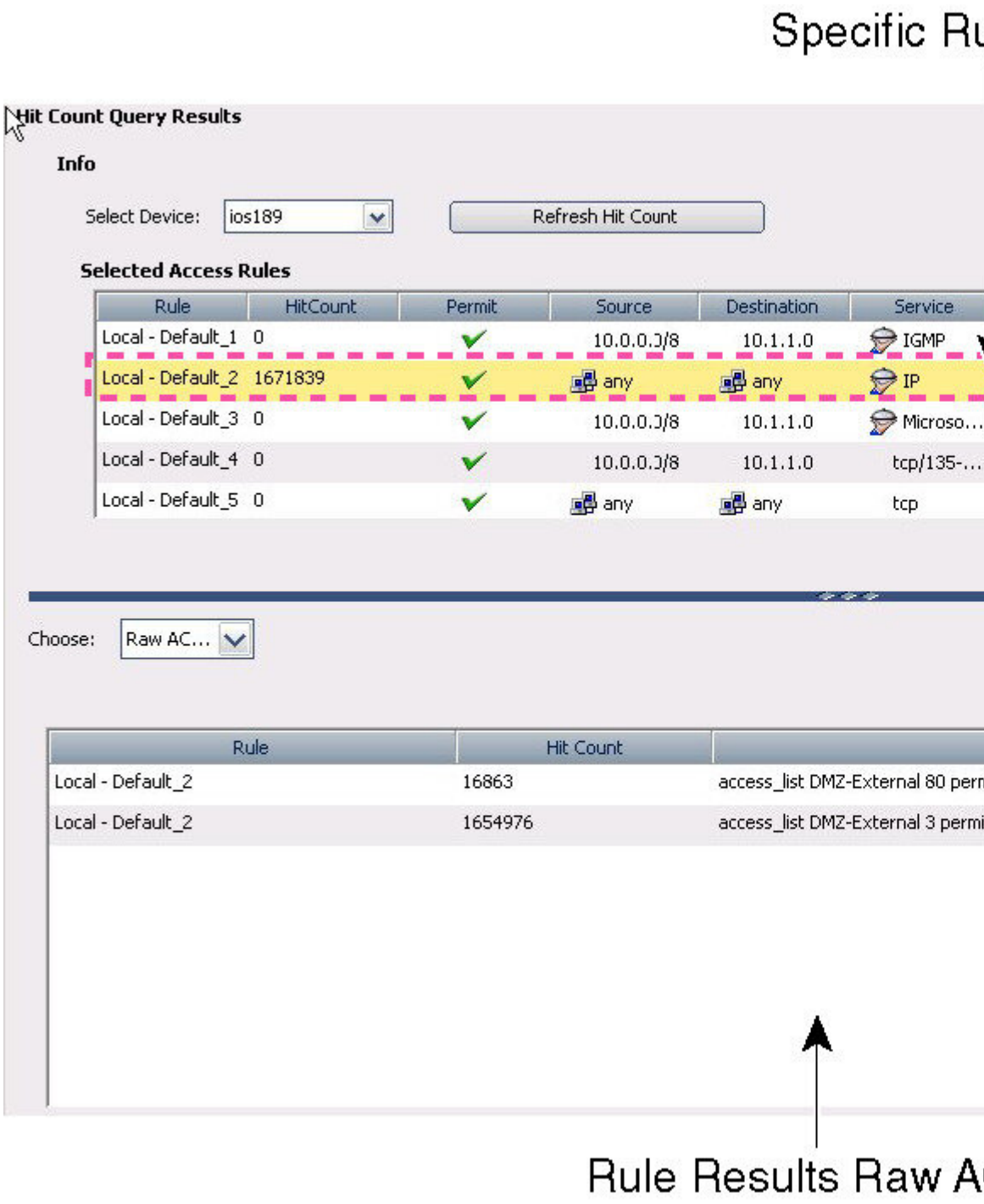


図 *26* : 未展開の *ACE* テーブル



関連項目

- アクセス ルールについて （913 ページ）

- アクセス ルールの設定 （920 ページ）

ルールのインポート

通常、デバイスを Security Manager に追加するときは、デバイスからポリシーを検出します。この処理により、デバイス上のすべてのアクティブなACLからのアクセス制御エントリ（ACE）が、アクセスルールポリシーに移入されます。

ポリシーに使用する ACE が含まれる ACL が他に存在している場合は、Security Manager で ACE を直接定義できます。

別の方法として、デバイス実行コンフィギュレーションからCLIエントリをコピーアンドペーストするか、目的のコマンドを入力することにより、ACE をインポートすることもできます。Import Rules ウィザードを使用すると、ACE および関連付けられたポリシーオブジェクトを、すでに機能している ACL からすばやく作成できます。また、ルールを定義するのに CLI コマンドを使用する方が慣れている場合は、この方法を使用すると便利です。

次の手順では、Import Rules ウィザードを使用して CLI ベースのルールを追加し、結果をプレビューする方法について説明します。

ステップ 1 （デバイスビューのみ）[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] を選択して、[Access Rules] ページ （924 ページ）を開きます。

ステップ 2 ルールの追加位置のすぐ上の行を選択します。ローカル範囲内の行を選択してください。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。

ステップ 3 ルールテーブル内の任意の場所を右クリックし、[ルールのインポート（Import Rules）] を選択してウィザードを開始します。

3 ページのウィザードの最初のページ（[パラメータの入力（Enter Parameters）]）が表示されます。

ステップ 4 Import Rules ウィザード - [Enter Parameters] ページ （967 ページ） で、次の手順を実行します。

- 選択したデバイスに適した実行コンフィギュレーション形式で、目的の CLI 情報を入力します。インポート可能な CLI ベースのルールの例については、インポートされたルールの例 （971 ページ）を参照してください。
- インターフェイス固有のルールの作成（その後にルールを適用するインターフェイスまたはインターフェイスロールを入力します）と、グローバルルールの作成（ASA 8.3+ デバイスの場合）のいずれかを選択します（ グローバル アクセス ルールについて （915 ページ）を参照）。
- インターフェイスに対するトラフィック方向を指定します（グローバルルールの場合、方向は常に[イン（In）] です）。

アクセス制御ルール以外に、次の項目がアクセス制御ルールによって参照される場合は、それらの項目も CLI 情報に含める必要があります。これらの項目を含めない場合、インポートを成功させるには、名前付きオブジェクトが Security Manager ですでに定義されている必要があります。

- 時間範囲オブジェクト（**time-range** コマンドとそのサブコマンド）。これにより、時間範囲ポリシー オブジェクトを作成できます。
- PIX、ASA、FWSM、および IOS 12.4(20)T+ デバイスの場合、オブジェクトグループ（**object-group** コマンドとそのサブコマンド）。これにより、ネットワーク/ホスト ポリシー オブジェクトを作成できます。

また、ASA 8.3 以降のデバイスの場合は、**object network** コマンドおよび **object service** コマンドを含めることができます。ただし、オブジェクト NAT 設定はインポートされません。

ステップ 5 [次へ（Next）] をクリックすると、ルールが処理され、Import Rules ウィザード - [Status] ページ （969 ページ）が開きます。

CLI の入力内容にエラーがある場合、[次へ（Next）] ボタンをクリックすると、プロンプトが表示されます。入力可能なコマンドに関するヒントについては、Import Rules ウィザード - [Enter Parameters] ページ（967 ページ）を参照してください。

CLI が評価され、インポート可能な場合は、CLI から作成されたオブジェクトのタイプが通知されます。

ステップ 6 [次へ（Next）] をクリックしてImport Rules ウィザード - [Preview] ページ （970 ページ）でルールおよびオブジェクトを確認するか、[完了（Finish）] をクリックしてルールをプレビューなしでインポートします。

[Preview] ページの情報は読み取り専用です。ルールに問題がなければ、[完了（Finish）] をクリックします。

変更する場合は、[戻る（Back）] ボタンをクリックしてウィザードの [パラメータの入力（Enter Parameters）] ページに戻るか、[完了（Finish）] をクリックして [アクセスルール（Access Rules）] ページでルールを編集します。

Import Rules ウィザード - [Enter Parameters] ページ

Import Rules ウィザードを使用して、ACL からデバイス実行コンフィギュレーション形式の一連のアクセス コントロール エントリをアクセス ルール ポリシーにインポートします。入力可能なコマンド構文は、ルールのインポート先のデバイスのタイプによって決まります。

アクセス制御ルール以外のルールによって参照される場合は、次の項目も CLI に含める必要があります。これらの項目を含めない場合、インポートを成功させるには、名前付きオブジェクトが Cisco Security Manager ですでに定義されている必要があります。

- 時間範囲オブジェクト（**time-range** コマンドとそのサブコマンド）。
- PIX、ASA、FWSM、および IOS 12.4(20)T デバイスの場合、オブジェクトグループ（**object-group** コマンドとそのサブコマンド）。

また、ASA 8.3 以降のデバイスの場合は、**object network** コマンドおよび **object service** コマンドを含めることができます。ただし、オブジェクト NAT 設定はインポートされません。

ナビゲーション パス

（デバイスビューのみ） [Access Rules] ページ （924 ページ）のルールテーブル内の任意の場所を右クリックし、[ルールのインポート（Import Rules）] を選択します。

関連項目

- ルールのインポート （966 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *193 : Import Rules - [Enter Parameters]* ダイアログボックス

要素	説明
CLI	インポートするルールおよび関連オブジェクトを定義する OS コマンド。これらのルールは実行コンフィギュレーション形式にする必要があるため、設定からコピーして貼り付ける（Ctrl+V を使用してフィールドに貼り付ける）方法が最適です。また、コマンドを手動で入力することもできます。コマンドを解釈できない場合は、プロンプトが表示されます。 一度にインポートできる ACL は、1 つだけです。 インポートできる CLI の例については、 インポートされたルールの例 （971 ページ）を参照してください。 **ヒント** • オブジェクトを参照するが CLI を含めない場合、ルールは作成可能ですが、そのオブジェクトは使用されません。 • PIX、FWSM、ASA、および IOS 12.4(20)T+ の場合、オブジェクト グループおよび名前のコマンドを含めることができます。 • 非アクティブな ACL をインポートすると、その ACL は Security Manager に無効な状態で表示されます。設定を展開すると、その ACL はデバイスから削除されます。 • 拡張 ACL は、すべてのデバイス タイプに対してインポートできます。IOS デバイスに対しては標準 ACL をインポートできます。ただし、標準 ACL は拡張 ACL に変換されます。

要素	説明
インターフェイス Global（ASA 8.3+）	インターフェイス固有のルールまたはグローバル ルールのいずれをインポートするかを選択します。グローバル ルールは ASA 8.3+ のデバイスだけで使用でき、特別なルールに従って処理されます（詳細については、グローバル アクセス ルールについて （915 ページ）を参照してください）。 [インターフェイス（Interfaces）] を選択した場合は、このルールを定義するインターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックして、リストからインターフェイスまたはロールを選択するか、または新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。インターフェイスまたはインターフェイス ロール名の任意の組み合わせを、カンマで区切って入力できます。
トラフィックの方向	インターフェイスに対するトラフィックの方向（[in] または [out]）。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

Import Rules ウィザード - [Status] ページ

Import Rules ウィザードの [Status] ページを使用して、インポート プロセスの結果に関する情報を参照します。

ナビゲーション パス

Import Rules ウィザードの開始方法の詳細については、Import Rules ウィザード - [Enter Parameters] ページ （967 ページ）を参照してください。

関連項目

- ルールのインポート （966 ページ）

フィールド リファレンス

表 194 : Import Rules ウィザード - [Status] ページ

要素	説明
進行状況バー	インポート プロセスのステータスが表示されます。
ステータス	インポートされた設定のステータス。
Rules Imported	インポートされるルールの数。

要素	説明
Policy Objects Created	作成されるポリシー オブジェクトの数。
メッセージ	重大度アイコンで示された、警告、エラー、および情報のメッセージ。通常の情報メッセージには、操作中に作成されたポリシー オブジェクトや、再利用された既存のポリシー オブジェクトの説明が表示されます。 項目を選択すると、右側の [Description] ボックスに詳細なメッセージが表示されます。右側の [Action] ボックスには、問題の修正方法が表示されます。
[Abort] ボタン	インポート操作を停止するには、このボタンをクリックします。

Import Rules ウィザード - [Preview] ページ

Import Rules ウィザードの [Preview] ページを使用して、[Finish] をクリックするとインポートされるルールおよびオブジェクトを確認します。

このプレビューは読み取り専用であるため、ルールまたはオブジェクトの編集はできません。ルールまたはオブジェクトの内容が希望どおりでない場合は、[Finish] をクリックしてルールおよびオブジェクトを追加し、アクセス ルール ページでそれを編集できます。たとえば、ルールの有効期限は Security Manager でだけ有効であるため、インポートできません。

このダイアログボックスのタブが表示されるのは、インポート対象のデータに、そのタブに表示される項目が含まれている場合だけです。

ヒント CLI が存在しないオブジェクト（時間範囲など）を参照している場合、そのオブジェクトはルールに含められません。前に戻ってそのオブジェクトの CLI を追加するか、または [Finish] をクリックし、手動でオブジェクトを作成して、ルールを編集することができます。

ナビゲーション パス

Import Rules ウィザードの開始方法の詳細については、Import Rules ウィザード - [Enter Parameters] ページ （967 ページ）を参照してください。

関連項目

- ルールのインポート （966 ページ）
- [Access Rules] ページ （924 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *195 : Import Rules* ウィザード - *[Preview]* ページ

要素	説明
[Rules] タブ	アクセス ルール ポリシーにインポートされる、CLI から作成されたルール。CLI が標準 ACL に対応している場合でも、すべてのルールは拡張形式に変換されます。 アイコンにより、許可および拒否のステータスが示されます。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。 送信元、宛先、サービス、およびインターフェイスのセルを右クリックして [コンテンツの表示（Show Contents）] を選択すると、そのセル内に詳細情報が表示されます。 右クリックして [コピー（Copy）] を選択すると、ルールを HTML 形式でクリップボードにコピーできます。このデータをテキストエディタに貼り付けることもできます。
[Objects] タブ	CLI から作成されたポリシー オブジェクト（ある場合）。CLI に応じて、Security Manager により時間範囲、ネットワーク/ホスト オブジェクト、サービス オブジェクト、またはポート リスト オブジェクトが作成されることがあります。 オブジェクトを右クリックして [オブジェクトの表示（View Object）] を選択すると、オブジェクト定義が読み取り専用形式で表示されます。

インポートされたルールの例

次に、インポート可能な CLI と、その CLI から作成されたルールおよびポリシー オブジェクトの例をいくつか示します。ルールのインポート方法の詳細については、ルールのインポート（966 ページ）を参照してください。

例 1：ネットワークから FTP サーバへのアクセスを制限する（ASA デバイス）

次のアクセス リストでは、オブジェクト グループを使用して、10.200.10.0/24 ネットワークから一部の FTP サーバへのアクセスを制限しています。他のトラフィックはすべて許可されます。

```
object-group network ftp_servers
```

```
network-object host 172.16.56.195
network-object 192.168.1.0 255.255.255.224
access-list ACL_IN extended deny tcp 10.200.10.0 255.255.255.0 object-group ftp_servers

access-list ACL_IN extended permit ip any any
```

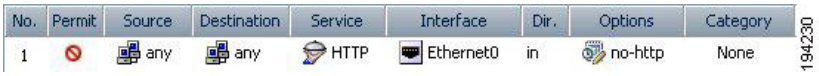
この例では、ftp_servers という名前の 1 つのネットワーク/ホスト オブジェクトと、2 つのアクセス ルールが作成されます。

例 2：勤務時間中の Web アクセスを制限する（ASA デバイス）

次の例では、午前 8 時～午後 6 時の間（通常の勤務時間）の HTTP 要求を拒否しています。

```
time-range no-http
 periodic weekdays 8:00 to 18:00
access-list 101 deny tcp any any eq www time-range no-http
```

この例では、no-http という名前の 1 つの時間範囲オブジェクトと、1 つのアクセス ルールが作成されます。

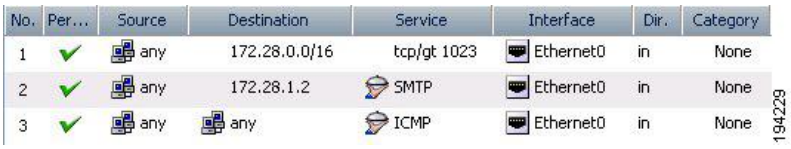


例 3：ポート番号を使用して TCP および ICMP をフィルタリングする（IOS デバイス）

次の例では、goodports という名前の拡張アクセス リストの最初の行で、1023 よりも大きい宛先ポートを持つ着信 TCP 接続を許可しています。2 行目で、ホスト 172.28.1.2 の Simple Mail Transfer Protocol（SMTP）ポートへの着信 TCP 接続を許可しています。最後の行では、エラーフィードバックのための着信 ICMP メッセージを許可しています。

```
ip access-list extended goodports
 permit tcp any 172.28.0.0 0.0.255.255 gt 1023
 permit tcp any host 172.28.1.2 eq 25
 permit icmp any 172.28.0.0 255.255.255.255
```

この例では、3 つのアクセス ルールが作成されます。IOS ACL 構文で使用されているワイルドカード マスクは通常のサブネット マスクに変換されることに注意してください。Security Manager は、標準のネットワーク/ホスト サブネット マスク指定と、IOS ACL で必要なワイルドカード マスクの間で自動変換を行います。ASA/PIX/FWSM では、ACL コマンド内にサブネットマスクを使用する必要があるため、すべてのデバイスに適用可能なルールを作成することが可能になります。Security Manager によって、ルールが正しい構文に変換されます。



例 4：ホストを制限する標準 ACL（IOS デバイス）

次の例では、Jones に属するワークステーションがイーサネット インターフェイス 0 へのアクセスを許可され、Smith に属するワークステーションはアクセスを許可されていません。

```
ip access-list standard workstations
 remark Permit only Jones workstation through
 permit 172.16.2.88
 remark Do not allow Smith workstation through
 deny 172.16.3.13
```

この例では、（任意の宛先に対して）標準ルールを拡張ルールに変換する 2 つのルールが作成されます。備考は、[description] フィールドに保存されます。

コマンド言語形式での ACL のその他の例については、次の URL を参照してください。

- IOS デバイス：http://www.cisco.com/en/US/docs/ios/sec_data_plane/configuration/guide/sec_create_IP_apply.html#wp1027258
- ASA デバイス：http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/acl_extended.html

展開中のアクセス ルールの自動最適化

特定のデバイスまたはすべてのデバイスに展開するときに、アクセス ルール ポリシーから作成されたアクセス コントロール リスト（ACL）が最適化されるようにシステムを設定できます。この最適化の影響を受けるのは、展開されたポリシーだけであり、アクセス ルール ポリシーは変更されません。

最適化によって、冗長性と競合がなくなり、複数のエントリ（ACE）を単一エントリに結合できます。エントリの順序は変更されても、ポリシーの意味は保持されます。つまり、最適化された ACL は、最適化されていないフォームのときと同じパケット セットを受け入れるか、または拒否します。次に、変更が行われる基本的なケースを示します。

- 非効率的な ACE：あるエントリが別のエントリのサブセットになっているか、または別のエントリと同一である場合、非効率的な ACE が削除されます。次の例を考えてみます。

```
access-list acl_mdc_inside_access deny ip host 10.2.1.1 any
access-list acl_mdc_inside_access deny ip 10.2.1.0 255.255.255.0 any
```

最初の ACE は実際には 2 番めの ACE のサブセットです。ACL の最適化では、2 番めのエントリだけが展開されます。

- スーパーセット ACE：あるエントリが別のエントリのスーパーセットであり、ルールの順序が重要ではない場合、冗長なルールが削除されます。次の例を考えてみます。

```
access-list acl_mdc_inside_access permit tcp any any range 110 120
access-list acl_mdc_inside_access deny tcp any any range 115
```

2 番めの ACE がヒットすることはありません。ACL の最適化により 2 番めの ACE が削除され、最初の ACE だけが展開されます。

- 隣接する ACE：2 つのエントリがよく似ているため、1 つのエントリで同じジョブを実行できる場合。各ルールにヒットするパケットが変更されるような介入ルールは存在できません。次の例を考えてみます。

```
access-list myacl permit ip 1.1.1.0 255.255.255.128 any
access-list myacl permit ip 1.1.1.128 255.255.255.128 any
```

2 つの ACE がマージされて 1 つの ACE になります（access-list myacl permit ip 1.1.1.0 255.255.255.0 any）。

ACL の展開最適化を設定することにより、作成される ACL が小さくなり、効率も高くなります。これにより、拡張不可能な制約付きのメモリ（FWSM など）を搭載するデバイスでのパフォーマンスを改善し、これを複数の仮想コンテキスト間で共有できます。

ただし、ACL の展開最適化の設定にはデメリットもあります。

- 最適化を行うと、アクセスルールに対して通常展開される内容が変更されるため、これらのルールを実際に展開されている ACE と相互に関連付けることが困難になります。この場合、ヒット カウント ツールの結果が使用できなくなることがあり、Cisco Security Monitoring, Analysis and Response System アプリケーションでイベントを相互に関連付けることが非常に困難になります。これらのツールを使用してアクセスルールをモニタすることが必要な場合は、最適化をイネーブルにしないでください。詳細については、ヒットカウントの詳細の表示 （960 ページ）および IPS シグニチャの CS-MARS イベントの表示（3738 ページ）を参照してください。
- 最適化を行っても、アクセス ルール ポリシー内の本質的な問題は解決されません。通常は、自動競合検出ツールを使用して冗長性と競合を事前に解決することを推奨します（自動競合検出の使用 （950 ページ）を参照）。また、展開の前に、ルール結合ツールを使用して、アクセス ルール ポリシー内のルールを最適化することもできます（ルールの結合（785 ページ）を参照）。

ACL の展開最適化を設定することにした場合は、メモリ制約のあるデバイスに対してだけイネーブルにすることを検討してください。

ステップ 1 Security Manager サーバ上の Windows にログインします。

ステップ 2 NotePad などのテキストエディタを使用して、**C:\Program Files\CSCOpx\MDC\athena\config\csm.properties** ファイルを開きます。最適化のセクションを見つけて、指示を確認します。

- すべてのデバイスに対して完全な最適化を有効にするには、次のように入力します。

OPTIMIZE.*=full

- 特定のデバイスに対して完全な最適化を有効にするには、アスタリスクを、そのデバイスに対する Security Manager の表示名で置き換えます。たとえば、表示名が west_coast.cisco.com の場合は、次のように入力します。

OPTIMIZE.west_coast.cisco.com=full

- 最適化を有効にするが、ACE で使用されているオブジェクトグループを保持する場合は、キーワード全部を preserve_og で置き換えます。次に例を示します。

OPTIMIZE.west_coast.cisco.com=preserve_og

- 隣接するエントリをマージしない場合は、次のように入力します。

AclOptimization.doMerge=false

ステップ 3 ファイルを保存します。設定は即時に有効になり、後続のすべての展開ジョブに適用されます。

展開ジョブの最適化レポートを生成するには、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration] > [デバッグオプション（Debug Options）]** から [検出/展開デバッグスナップショットのファイルへのキャプチャ（Capture Discovery/Deployment Debugging Snapshots to File）] を選択します。

展開結果には、情報メッセージとして要約された最適化結果が表示されます。これには、最適化前の最初の ACE の数と、最適化後の ACE の数が含まれます。結果は、サーバ上の C:\Program Files\CSCOpx\MDC\temp フォルダ内のファイルに保存されます。ファイル名の一部としてジョブ ID が使用されます。

[アクセスルールの追加（Add Access Rule）] ダイアログでのデフォルトのカスタマイズ

Cisco Security Manager 4.13 より前は、[アクセスルールの追加（Add Access Rule）] ダイアログにデフォルト値が入力されていました。4.13 以降、ユーザーは csm.properties ファイルを更新することにより、デフォルト値の状況をカスタマイズできます。

[アクセスルールの追加（Add Access Rule）] ダイアログでデフォルトをカスタマイズするには、次の手順を実行します。

ステップ 1 Cisco Security Manager インターフェイスを閉じて終了します。

ステップ 2 NotePad などのテキストエディタを使用して、**C:\Program Files\CSCOpx\MDC\athena\config\csm.properties** ファイルを開きます。

ステップ 3 csm.properties ファイルの下部にある CustDesk.Rule プロパティを見つけ、要件に基づいて値を true または false に設定します。

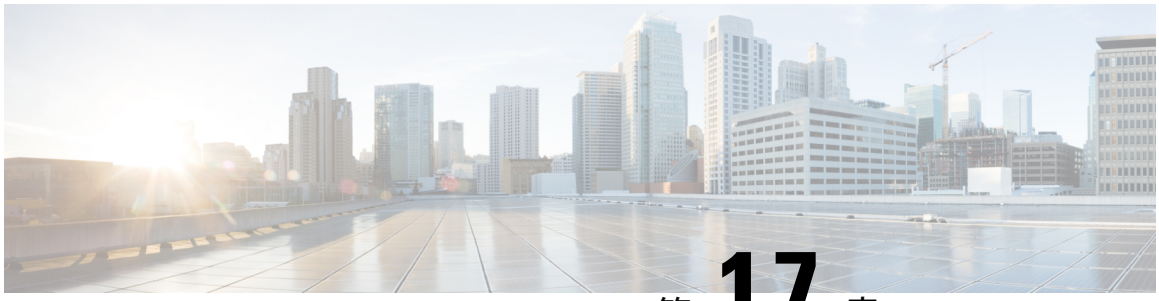
- CustDesk.Rule.Add.Op.Load.Intf.Default.Values：この値を true に設定すると、[アクセスルールの追加（Add Access Rule）] ダイアログでデフォルトのインターフェイス情報がロードされます。

- CustDesk.Rule.Add.Op.Load.Other.Default.Values：この値を true に設定すると、[アクセスルールの追加（Add Access Rule）] ダイアログで他のデフォルト値がロードされます。

ステップ 4 ファイルを保存します。

（注） この変更はすぐには有効になりません。カスタマイズしたデフォルト値を有効にするには、Cisco Security Manger サービスを再起動します。

ステップ 5 Cisco Security Manager インターフェイスを再度起動します。



第 17 章

ファイアウォール インスペクション ルールの管理

インスペクション ルールでは、デバイスに対するプロトコル インスペクションを設定します。インスペクションでは、アクセス ルールに一時的な穴を開けて、信頼ネットワーク内で開始された接続に対するリターン トラフィックを許可します。また、トラフィックが検査されるとき、デバイスでは、検査されるプロトコルに基づいて誤った形式のパケットを除外するための追加の制御も実装します。

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

インスペクション ルールに対して生成されるデバイス コマンドは、デバイス タイプに応じて異なります。ASA、PIX 7.0+、および FWSM 3.x+ を実行しているデバイスでは、access-list、policy-map、class-map の各コマンドが使用されます。古い FWSM および PIX 6.3 デバイスでは、fixup コマンドが使用されます。IOS デバイスでは、ip-inspect コマンドが使用されます。

インスペクション ルールの使用方法については、次の項を参照してください。

- インスペクション ルールについて （977 ページ）
- インスペクション ルールの設定 （983 ページ）
- [Inspection Rules] ページ （986 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- IOS デバイスのインスペクション ルールの設定 （1129 ページ）

インスペクション ルールについて

インスペクション ルールでは、Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）インスペクション コマンドを設定します。CBAC では、デバイスを通過するトラフィックを検査して、TCP および UDP セッションの状態情報を検出および管理します。デバイスでは、この状態情報を使用して、許容できるセッションのリターン トラフィックおよび追加のデータ接続を許可するための一時的な穴を作成します。

CBAC では、ファイアウォール インターフェイスでアクセス リストに一時的な穴を作成します。これらの穴は、検査されるトラフィックがファイアウォールを通過して内部ネットワークから出るときに作成されます。リターン トラフィック（通常はブロックされます）と追加のデータ チャネルは、この穴からファイアウォールを通って内部ネットワークに入ることができます。トラフィックは、そのトラフィックがファイアウォールを通って出るときにインスペクションをトリガーした、元のトラフィックと同じセッションの一部となっている場合にだけ、ファイアウォールを通って戻ることができます。

インスペクション ルールは、アクセス ルールのあとに適用されるため、アクセス ルールで拒否したトラフィックは検査されません。トラフィックが検査されるようにするには、入力インターフェイスと出力インターフェイスの両方で、アクセス ルールによってトラフィックが許可される必要があります。アクセス ルールではレイヤ 3（ネットワーク、IP）または 4（トランスポート、TCP または UDP プロトコル）で接続を制御できますが、インスペクション ルールを使用すると、アプリケーション レイヤ プロトコル セッション情報を使用してトラフィックを制御できます。

すべてのプロトコルについて、プロトコルを検査するときに、デバイスによって次の機能が提供されます。

- トラフィックのリターン パスを自動的に開く（送信元アドレスと宛先アドレスを反転する）ため、リターン トラフィックを許可するアクセス ルールを作成する必要がない。各接続はセッションと見なされ、デバイスはセッション状態情報を保持し、有効なセッションのリターン トラフィックだけを許可します。TCP を使用するプロトコルには明示的なセッション情報が含まれますが、UDP アプリケーションでは、送信元および宛先アドレスと一連の UDP パケットの時間的な近さに基づき、デバイスがセッションと同等のものをモデル化します。

これらの一時的なアクセス リストは動的に作成され、セッションが終了するとき、削除されます。

- すべての TCP パケットのシーケンス番号を追跡し、想定範囲内にないシーケンス番号を持つパケットをドロップする。
- タイムアウトとしきい値を使用してセッション状態情報を管理することによって、完全には確立されていないセッションをいつドロップするかの判断に役立てる。セッションがドロップまたはリセットされると、デバイスは、セッションの送信元と宛先の両方に接続をリセットするよう通知して、リソースを解放し、Denial of Service（DoS; サービス拒絶）攻撃の可能性を低減します。

ここでは、インスペクションについて詳しく説明します。

- インスペクション ルールのインターフェイスの選択 （979 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）

- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ルールの設定 （983 ページ）
- IOS デバイスのインスペクション ルールの設定 （1129 ページ）

インスペクション ルールのインターフェイスの選択

内部ネットワークを保護するインスペクションをデバイスに設定します。TCP、UDP、またはその他の特定のプロトコルとともに使用します。トラフィックセッションがデバイスの特定の側から（通常は、保護されている内部ネットワークから）開始された場合にだけ、アプリケーションのトラフィックがデバイスを通過できるようにするには、これらのアプリケーションを検査します。

ヒント IOSデバイスでは、インスペクションを明示的に設定する必要があり、検査するトラフィックの方向を指定できます。ASA、PIX、および FWSM の各デバイスでは、方向を指定できず、インスペクションを設定する必要があるのはインスペクションのデフォルトを使用しない場合だけです。以降の説明では、方向に関する文は IOS デバイスにだけ適用されます。ASA、PIX、および FWSM では、単純に指定されたインターフェイスにインスペクションを設定します。

多くの場合、単一のインターフェイスで一方向にだけインスペクションを設定します。これにより、トラフィックは許容される（有効、既存）セッションに属する場合にだけ内部ネットワークに戻ることができます。これは、インターネット上で発生したトラフィックから内部ネットワークを保護するための一般的な設定です。

1 つ以上のインターフェイスで、双方向のインスペクションを設定することもできます。エクストラネット設定やイントラネット設定などを使用して、ファイアウォールの両側のネットワークを保護する必要がある場合、および DoS 攻撃から保護する場合に、双方向のインスペクションを設定します。たとえば、デバイスが 2 つのパートナー企業のネットワークの間にある場合は、特定のアプリケーションに対してトラフィックを一方向に制限し、他のアプリケーションに対してトラフィックを反対方向に制限することが必要となることがあります。DMZ ゾーン内の Web サーバを保護している場合は、HTTP トラフィックに詳細なインスペクションを設定して、望ましくない特性を持つ接続を識別し、リセットすることが必要となることがあります。

インターネットまたは別の制御対象外ネットワークに接続するネットワークのアウトバウンドインターフェイスにインスペクションルールを設定する一方で、信頼ネットワーク内ではフィルタリングされない接続を許可することが必要となる場合があります。このため、デバイスでは、保護されていないことによって潜在的な危険性のあるネットワーク上を移動するセッションにだけ、インスペクションのリソースが使用されます。

関連項目

- 検査するプロトコルの選択 （980 ページ）

- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ルールの設定 （983 ページ）

検査するプロトコルの選択

TCP および UDP は汎用的に検査できます。これにより、これらのプロトコルを使用するすべてのアプリケーションがカバーされます。ただし、より特定的なプロトコルを検査することもできます。場合によっては、特定のプロトコルの検査によって、汎用的な TCP/UDP インスペクションよりも優れたサービスが提供されることがあります。TCP および UDP のインスペクションでは、アプリケーション固有のコマンドが認識されないため、あるアプリケーションのすべてのリターン パケットが許可されないことがあります。特に、リターン パケットのポート番号が前の既存パケットとは異なる場合は、その可能性が高くなります。

次に例を示します。

- 一部のプロトコルでは、詳細なインスペクションを設定できる。詳細なインスペクションでは、トラフィック ストリームに対して、より具体的なルールを設定できます。たとえば、要求および応答のコンテンツ タイプが一致しない HTTP 接続をドロップできます。詳細なインスペクションと設定オプションについては、インスペクションのプロトコルおよびマップの設定 （1004 ページ）を参照してください。
- FTP など、リターン チャネルをネゴシエーションするプロトコルは、明示的に検査する必要がある。FTP トラフィックの単純な汎用 TCP インスペクションを使用する場合は、ネゴシエーションされたチャネルは開かれず、接続が失敗します。FTP を許可する場合は、FTP 用の明示的なインスペクション ルールを作成してください。

また、マルチメディア プロトコルもリターン チャネルをネゴシエーションするため、明示的に検査する必要があります。これらのプロトコルには、H.323、Real Time Streaming Protocol（RTSP; リアルタイム ストリーミング プロトコル）、およびその他のアプリケーション固有のプロトコルが含まれます。一部のアプリケーションでは汎用 TCP チャネルも使用するため、汎用 TCP インスペクションも設定する必要があります。汎用的な TCP インスペクション ルールは、テーブル内でより明示的なインスペクション ルールよりも下にある必要があります（つまり、TCP または UDP を指定するルールは、すべて、インスペクション ルール テーブルの最後にある必要があります）。

関連項目

- インスペクション ルールのインターフェイスの選択 （979 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）

• インスペクション ルールの設定 （983 ページ）

インスペクション ルールのアクセス ルール要件について

アクセス ルールは、インスペクション ルールよりも前に適用されます。このため、検査するトラフィックがアクセス ルールで禁止されないようにする必要があります。次の注意事項に従ってください。

- 検査したトラフィックがファイアウォールを通過してネットワークから出ることを許可する。

検査されるトラフィックは、保護ネットワークから出るトラフィックを評価する、すべてのアクセス ルールで許可される必要があります。たとえば、Telnet が検査される場合、Telnet トラフィックは、ネットワークから出るトラフィックに適用されるすべてのアクセスルールで許可される必要があります。

- 検査されるリターン トラフィックがファイアウォールを通過してネットワークに入ることを拒否する。

アクセス リストに一時的な穴を作成する場合、アクセス リストでは、検査されるリターン トラフィックを拒否する必要があります。これは、インスペクションエンジンによって、このトラフィックのアクセスリストに一時的な穴が開けられるためです（通常、ネットワークに入るトラフィックはブロックされるようにします）。

- ネットワークでの必要性に応じて、検査できないトラフィック、または検査する必要のないトラフィックを許可または拒否する。

たとえば、ICMP トラフィックを検査しないで、一部の ICMP トラフィックを許可する場合は、両方向のトラフィックが許可されるようにアクセスルールを設定します。少なくとも、（ping コマンドに対する）echo reply、（トレース ルートに対する）time-exceeded、（パス MTU ディスカバリに対する）packet-too-big、（トレース ルートに対する）traceroute、および（ホストが見つからないことを通知する）unreachable の ICMP メッセージ タイプを許可することを検討します。

- 保護ネットワーク上のアドレスと一致する送信元アドレスからのすべてのネットワーク トラフィックを拒否するアクセス ルール エントリを追加する。

この方法は、保護されていないネットワークからのトラフィックが、保護ネットワーク上のデバイスの識別情報を偽って使用することを防ぐため、アンチ スプーフィング保護と呼ばれます。

- 送信元アドレスが 255.255.255.255 のブロードキャスト メッセージを拒否するエントリを追加する。

このエントリは、ブロードキャスト攻撃を防ぐのに役立ちます。

関連項目

- アクセス ルールについて （913 ページ）
- インスペクション ルールのインターフェイスの選択 （979 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールの設定 （983 ページ）

IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

アプリケーション層でパケットを検査すること、および TCP セッション情報と UDP セッション情報を保持することによって、デバイスは、SYN フラッディングなどの特定のタイプのネットワーク攻撃を検出および回避できます。SYN フラッド攻撃は、ネットワーク攻撃者がサーバに膨大な数の接続要求をフラッドし、接続を完了しないことによって発生します。これにより、ハーフオープン接続が大量に発生してサーバが処理しきれなくなり、有効な要求へのサービスが拒否されます。ネットワーク デバイスへのアクセスを拒否するネットワーク攻撃を、Denial-of-Service（DoS; サービス拒絶）攻撃と呼びます。

インスペクションは、他の方法で DoS 攻撃から保護するのに役立ちます。インスペクションは、TCP 接続のパケット シーケンス番号を参照し、それらが想定範囲内にあるかどうかを確認して、すべての疑わしいパケットをドロップします。また、ハーフオープン接続をドロップするインスペクション設定をすることもできます。このことを行うには、ファイアウォール処理とメモリ リソースの維持が必要です。これ以外に、インスペクションでは、新しい接続で頻繁に発生するエラーを検出してアラート メッセージを発行できます。

IOS デバイスでは、複数のインスペクション設定パラメータを設定して、SYN フラッディングとハーフオープン接続からの保護を微調整できます。**[ファイアウォール（Firewall）] > [設定（Settings）] > [検査（Inspection）]** ポリシーを設定します。各設定の詳細については、IOS デバイスのインスペクション ルールの設定 （1129 ページ）を参照してください。

インスペクションは、フラグメント化された IP パケットに関連する特定の DoS 攻撃からも保護できます。ファイアウォールは攻撃者が特定のホストに実際に接続することを防ぎますが、攻撃者はそのホストによって提供されるサービスを中断させることがあります。このことは、多くの非初期 IP フラグメントを送信するか、または、フラグメント化されたパケットの最初のフラグメントをフィルタする ACL を持つルータを経由して、完全にフラグメント化されたパケットを送信することによって行われます。ターゲット ホストでは不完全なパケットを再構成しようとし、これにより、これらのフラグメントによって、ターゲット ホスト上のリソースが占有されます。フラグメント インスペクションを微調整するには、**フラグメント**プロトコル

のインスペクションルールを設定し、許可するフラグメントの最大数とタイムアウト値を設定します。

関連項目

- インスペクション ルールについて （977 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ルールの設定 （983 ページ）

インスペクション ルールの設定

インスペクション ルール ポリシーは、インターフェイスを通じて検査されるトラフィックを識別します。インスペクションでは、許可されるセッションを追跡し、リターン トラフィックを許可するために、アクセス ルールに一時的な穴を開けます。

インスペクション ルールはアクセス ルールよりもあとに処理されるため、アクセス ルールでドロップされたトラフィックは検査されません。拒否ルールを使用して、特定のタイプのトラフィックを検査から選択的に除外することもできます。たとえば、他のすべての DNS トラフィックが検査されているときに、特定のクラスの DNS トラフィックが検査されないようにする検査拒否ルールを作成できます。基本的な手順は次のとおりです。

- 特定のプロトコルのデフォルトの検査ルールの前に、新しい拒否ルールを追加します。[トラフィックの照合基準（Match Traffic By）] オプションで、[送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）] を選択します。次に、送信元と宛先のネットワーク IP アドレスを指定し、目的のサービスタイプ（DNS-TCP など）を選択して、特定のタイプのトラフィックを定義します。最後に、検査ルールウィザードの 3 番目の画面で、適切なプロトコル（DNS など）を選択します。
- 次に、デフォルトの検査ルールを編集します（表の新しい拒否ルールの下）。[トラフィックの照合基準（Match Traffic By）] オプションで [送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）] を再度選択します。これが許可ルールであることを確認し、送信元アドレスと宛先アドレスとして all-addresses オプションを指定し、サービスタイプとして IP を入力します。3 番目の画面では、選択したプロトコルを保持します。必要に応じて、関連するマップを設定または削除します。

この手順とプロセスに関する詳細情報については、 [Inspection Rules] ページ （986 ページ）および Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）を参照してください。

インスペクションルールを作成するときに検討する必要のある事項の詳細については、次の各項を参照してください。

- インスペクション ルールについて （977 ページ）
- インスペクション ルールのインターフェイスの選択 （979 ページ）

- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- マップ オブジェクトについて （388 ページ）

はじめる前に

あるインスペクション ルールのセットをすべてのデバイスに適用するとします。このためには、共有ルールを作成して、そのルールを各デバイスのインスペクション ルール ポリシーに継承します。詳細については、 新しい共有ポリシーの作成 （278 ページ）および ルールの継承または継承の解除 （269 ページ）を参照してください。

ステップ 1 次のいずれかを実行して、 [Inspection Rules] ページ （986 ページ）を開きます。

- デバイス ビュー：ポリシー セレクタから **[ファイアウォール（Firewall）] > [インスペクション ルール（Inspection Rules）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[ファイアウォール（Firewall）] > [インスペクション ルール（Inspection Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。 Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、 ルールの編集 （767 ページ）を参照してください。

ステップ 3 ルールをデバイスのすべてのインターフェイスに適用するか、指定したインターフェイスにだけ適用するかを選択します。

インターフェイスを指定することを選択した場合は、インターフェイス名またはインターフェイス ロールを入力するか、[選択（Select）] をクリックしてリストから選択します。また、IOS デバイスの場合は、ルールを出力方向（インターフェイスから出るトラフィック）に適用するかどうかも選択できます。他のすべてのデバイス タイプには入力方向を使用します。

ステップ 4 トラフィックのマッチングに使用する基準を選択します。この基準により、このルールに基づいて検査される対象が決まります。

- [デフォルト プロトコル ポート（Default Protocol Ports）]：このオプションは、検査しているプロトコルでネットワークのデフォルト ポートが使用されている場合に選択します。

送信元アドレスまたは宛先アドレスに基づいてインスペクションを制約する場合は、[[送信元と宛先のIPアドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] も選択します（ASA、PIX 7.x+、および FWSM 3.x+ デバイスでだけ使用できます）。[次へ（Next）] をクリックすると、送信元アドレスと宛先アドレスの入力を求められます。他の値を設定することだけが目的である場合は、送信元またはアドレスに [任意（any）] を指定できます。

- [カスタム宛先ポート（Custom Destination Ports）]：このオプションは、追加のデフォルト以外の TCP または UDP ポートを特定のプロトコルに関連付ける場合（たとえば、宛先ポート 8080 上の TCP トラフィックを HTTP トラフィックとして扱う場合）に選択します。[次へ（Next）] をクリックすると、ポートまたはポート範囲の入力を求められます。
- [宛先アドレスとポート（Destination Address and Port）]（IOS デバイスのみ）：このオプションは、トラフィックが特定の宛先に向かっている場合にだけ、デフォルト以外の追加の TCP または UDP ポートを特定のプロトコルに関連付ける場合（たとえば、トラフィックが 192.168.1.10 に向かっている場合にだけ、宛先ポート 8080 上のトラフィックを HTTP として扱う場合）に選択します。[次へ（Next）] をクリックすると、宛先アドレスとポート情報の入力を求められます。
- [送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）]（PIX 7.x+、ASA、FWSM 3.x+）：このオプションは、IOS デバイスで [宛先アドレスとポート（Destination Address and Port）] を選択するのと同じ理由で選択しますが、トラフィックの送信元を識別する追加オプションがあります。[次へ（Next）] をクリックすると、送信元アドレス、宛先アドレス、およびサービスポート情報の入力を求められます。

（注） FWSM 2.x および PIX 6.3(x) の場合は、[Default Inspection Traffic] または [Custom Destination Ports] だけを選択できます。

ステップ 5 [次へ（Next）] をクリックします。[デフォルトプロトコルポート（Default Protocol Ports）] 以外のオプションを選択した場合は、上記で説明した必要なアドレッシングとポート情報を入力し、[次へ（Next）] をクリックします。[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）を参照してください。

ステップ 6 [検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）で、検査するプロトコルをリストから選択します。ルールを割り当てているデバイスでそのプロトコルのインスペクションがサポートされていることが [Device Type] フィールドに示されていることを確認します（サポートされていないデバイス タイプにルールを割り当てた場合、ルールは無視されますが、検証の警告が生成されます）。

選択したプロトコルで追加設定が許可されている場合は、[設定（Configure）] ボタンがアクティブになります。このボタンをクリックして、オプションを選択します。詳細については、インスペクションのプロトコルおよびマップの設定 （1004 ページ）を参照してください。

IOS デバイスのみ：

- トラフィックの一致基準として [カスタム宛先ポート（Custom Destination Ports）] または [宛先アドレスとポート（Destination Address and Port）] を選択した場合は、プロトコル名として [カスタムプロトコル（custom protocol）] を選択し、[設定（Configure）] をクリックして設定に名前を割り当てることができる。
- インスペクション設定ポリシーで設定された値を上書きする追加のアラート、監査、およびタイムアウトを設定できる。また、限られた数のプロトコルに対して、ルータによって設定されたトラフィッ

クを検査するかどうかも指定できます。インスペクション設定の詳細については、 IOS デバイスのインスペクション ルールの設定 （1129 ページ）を参照してください。

ステップ 7 [終了（Finish）] をクリックしてルールを保存します。

ステップ 8 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、 ルールの移動とルール順序の重要性 （781 ページ）を参照してください。

次のタスク

ASA 9.9.1 以降、Security Gateway 機能が有効になっているクラスタモードのデバイスでは、次の集中検査のリストが無効になっています。

- DCERPC
- NetBIOS
- PPTP
- RADIUS
- RSH
- SUNRPC
- TFTP
- XDMCP

プレビューの設定中に、サポートされていないデバイスに対して検査ルールが設定されている場合、検証エラーが表示されます。

（注） デバイスのロールバックがある場合、デフォルトの DNS ポリシーマップ設定がデバイスに自動的に追加されます。したがって、Cisco Security Manager がデバイスのロールバックを処理した後、デバイスが再検出されると、デフォルトの dns-policy-map 設定が Cisco Security Manager で検出されます。

[Inspection Rules] ページ

[Inspection Rules] ページを使用して、デバイス インターフェイスのインスペクション ルールを設定します。インスペクションでは、デバイスを通過するトラフィックを調べて、TCP および UDP セッションの状態情報を検出および管理します。デバイスでは、この状態情報を使用して、許容できるセッションのリターン トラフィックおよび追加のデータ接続を許可するための一時的な穴を作成します。

（注） Cisco Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降では、IPv4 および IPv6 インスペクションルールを設定するための個別のポリシーとオブジェクトが「統合」されています。つまり、IPv4 または IPv6 アドレス、あるいは両方のアドレスを合わせて使用できる一組のインスペクションルールになりました（詳細については、Cisco Security Manager 4.4 でのポリシーオブジェクトの変更 （14 ページ）を参照してください）。ポリシービューでは、IPv4 および統合バージョンのインスペクション ポリシー タイプが提供されています。さらに、既存の IPv4 ポリシーの変換に使用できるユーティリティが用意されています（IPv4 ルールから統合ルールへの変換 （792 ページ）を参照）。次の説明は、特に明記されている場合を除き、インスペクション ルール テーブルのすべてのバージョンに適用されます。IPv4 インスペクションルール共有ポリシーを 9.0 以降のデバイスに割り当てると、割り当てたポリシーの統合バージョンをそのデバイスに割り当てることはできなくなります。同様に、統合インスペクションルール共有ポリシーを 9.0 以降のデバイスに割り当てると、割り当てた共有ポリシーの IPv4 バージョンをそのデバイスに割り当てることはできなくなります。そのデバイスは、共有ポリシーの [割り当て（Assignments）] タブの使用可能なデバイスのリストには含まれません。

インスペクションルールは、アクセスルールのあとに処理されます。このため、アクセスルールで拒否されたトラフィックは検査されません。

インスペクション ルールを設定する前に、次の項を読んでください。

- インスペクション ルールについて （977 ページ）
- インスペクション ルールのインターフェイスの選択 （979 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- インスペクション ルールの設定 （983 ページ）

ヒント ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

ナビゲーション パス

[Inspection Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [インスペクションルール（Inspection Rules）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [インスペクションルール（Inspection Rules）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [インスペクションルール（Inspection Rules）] を選択します。

関連項目

- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）
- ルール テーブルの使用 （764 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *196 : [Inspection Rules]* ページ

要素	説明
すべての行を展開する/すべての行を折りたたむ（Expand all rows/Collapse all rows）	ルールテーブルのすべてのセクションを展開または折りたたむには、これらのボタンを使用します。 （注） 各ボタンは、インスペクション ルール テーブルの上にある [フィルタ（Filter）] 領域の右上隅にあります。
競合インジケータアイコン（Conflict Indicator icons）	競合を識別し、競合の種類をすばやく視覚的に表現します。競合の種類や、この列から実行できるアクションなどの詳細については、自動競合検出について （950 ページ）を参照してください。
番号	順序が付けられたルール番号。
許可（Permit）	設定された次の条件に基づいて、検査する必要のあるトラフィックがルールによって識別されるかどうか。 • [Permit]：検査するトラフィックを特定します。緑色のチェックマークとして表示されます。 • [Deny]：トラフィックを検査から免除します。トラフィックが許可されるかブロックされるかは、アクセス ルールによって決定されます。スラッシュの入った赤色の丸として表示されます。

要素	説明
ソース	このルールのトラフィックのソース。つまり、ネットワーク、セキュリティグループ（ASA 9.0 以降のみ）、およびユーザーになります。複数のエントリは、テーブルセル内の個別の行に表示されます。
宛先	このルールの宛先。つまり、ネットワークおよびセキュリティグループになります（ASA 9.0 以降のみ）。複数のエントリは、テーブルセル内の個別の行に表示されます。
Traffic Match	ルールで使用される一致のタイプ。 • [default-inspection]：ルールにより、デフォルトポートに基づいてトラフィックが検査されます。 • [TCP、UDP/ポート番号（TCP,UDP/port number）]：ルールにより、カスタムポート番号に基づいてトラフィックが検査されます。 • [Service]：ルールでは、サービスの仕様またはサービス オブジェクトに基づいてトラフィックが検査されます。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。 サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。[グローバル（Global）]は、ルールがすべてのインターフェイスに割り当てられていることを示します。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。 インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
Dir.	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。
Inspected Protocol	検査されるプロトコル。場合によってはプロトコルの設定の一部。このセルを右クリックし、[検査済みプロトコルの編集（Edit Inspected Protocol）] を選択してプロトコルを編集できます。詳細については、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）を参照してください。
時間範囲	ルールに割り当てられている時間範囲ポリシー オブジェクト。このオブジェクトでは、インスペクションが行われる時間枠を定義します。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	ルールの説明（ある場合）。
最後のチケット（Last Ticket(s)）	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
ルールテーブルの下のページ要素	
クエリ	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。ポリシー クエリー レポートの生成 （793 ページ）を参照してください
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。ルール テーブルの項目の検索と置換 （777 ページ）を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。
[Add Row] ボタン	Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除（766 ページ）を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集（767 ページ）を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード

Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザードを使用して、インスペクション ルールを追加および編集します。ウィザードでは、このページの [トラフィック一致基準（Match Traffic By）] グループでの選択に基づいてインスペクション ルールを設定するプロセスの手順が示されます。

インスペクション ルールを設定する前に、次の項を読んでください。

- インスペクション ルールについて （977 ページ）
- インスペクション ルールのインターフェイスの選択 （979 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- インスペクション ルールの設定 （983 ページ）

ナビゲーション パス

[Inspection Rules] ページ （986 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- [検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）
- [検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- ルールの編集 （767 ページ）

フィールド リファレンス

表 *197 : Add Inspect/Application FW Rule* ウィザードまたは *Edit Inspect/Application FW Rule* ウィザードの手順 *1*：トラフィック一致方式

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。
Apply the Rule to	ルールが適用されるインターフェイス。 • [All Interfaces]：ルールをすべてのインターフェイスに適用します。ルールは、ASA、PIX、およびFWSMデバイスでグローバルルールになります。IOSデバイスの場合は、各インターフェイスに対してルールが入力方向に設定されます。 • [Interface (PIX 7.x+, ASA, FWSM 3.x+, IOS)] - [Interfaces] フィールドで指定されたインターフェイスにだけルールを適用します。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 IOSデバイスの場合にのみ、このルールが適用されるトラフィックの方向（インターフェイスに入るトラフィック（[In]）またはインターフェイスから出るトラフィック（[Out]））を選択します。その他のデバイスの場合は、方向を [In] のままにします。
Match Traffic By 検査するトラフィックを識別する方法。デフォルトのプロトコルポート（単独）以外を選択した場合、[次へ（Next）] をクリックすると、他のポートまたはアドレス情報の入力を求められます。	

要素	説明
Default Protocol Ports Limit inspection between source and destination IP addresses（PIX 7.x+、ASA、FWSM 3.x+）	プロトコルに割り当てられているデフォルト ポートに基づいてトラフィックを検査します。次のページ（[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）]ページ （998 ページ）） でプロトコルを選択します。 また、[送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択して、指定した送信元と宛先間でのみ検査を実行するように設定できます。検査するトラフィックに制約を適用しないでプロトコルを検査する場合は、このオプションを選択しないでください。 このオプションも選択した場合、ウィザードの次のページの説明については、 [検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）を参照してください。
Custom Destination Ports	指定したデフォルト以外の TCP または UDP 宛先ポートに基づいてトラフィックを検査します。このオプションは、追加の TCP または UDP トラフィックを特定のプロトコルに関連付ける場合（たとえば、宛先ポート 8080 上の TCP トラフィックを HTTP トラフィックとして扱う場合）に選択します。 ウィザードの次のページでプロトコルとポートを指定します。[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）を参照してください。
宛先アドレスとポート（IOSデバイスのみ）（Destination Address and Port (IOS devices only)）	宛先 IP アドレスとポートに基づいて IOS デバイス上のトラフィックを検査します。このオプションは、トラフィックが特定の宛先に向かっている場合にだけ、デフォルト以外の追加の TCP または UDP ポートを特定のプロトコルに関連付ける場合（たとえば、トラフィックが 192.168.1.10 に向かっている場合にだけ、宛先ポート 8080 上のトラフィックを HTTP として扱う場合）に選択します。
Source and Destination Address and Port（PIX 7.x、ASA、FWSM 3.x）	送信元と宛先の IP アドレスとサービスに基づいて、PIX 7.x+、ASA、および FWSM 3.x+ デバイス上のトラフィックを検査します。このオプションは、IOS デバイスで [Destination Address and Port] を選択するのと同じ理由で選択しますが、トラフィックの送信元を識別する追加オプションがあります。 ウィザードの次のページで、アクション、送信元、宛先、およびサービスを指定します。[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）を参照してください。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。

[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2

[検査/アプリケーション FW ルール（Inspect/Application FW Rule）] ウィザードの 2 ページ目に表示されるオプションは、最初のページでの [トラフィック照合基準（Match Traffic By）] の選択によって異なります（Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）を参照）。表示されるオプションは、次のとおりです。

- 最初のページで [デフォルトプロトコルポート（Default Protocol Ports）] を選択し、[送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択しない場合、2 ページ目は [検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）で説明されているオプションで構成されます。
- 最初のページで [デフォルトプロトコルポート（Default Protocol Ports）] を選択し、[送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択する場合、このセクションにある 2 つ目の表で説明されているオプションで構成されます（3 ページ目は、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）で説明されているオプションで構成されます）。
- 最初のページで [カスタム宛先ポート（Custom Destination Ports）] を選択する場合、2 ページ目は、このセクションにある最初の表で説明されているオプションで構成されます（3 ページ目は、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）で説明されているオプションで構成されます）。
- 最初のページで [送信元と宛先のアドレスおよびポート（Source and Destination Address and Port）] を選択する場合、2 ページ目は、このセクションにある 2 つ目の表で説明されているオプションで構成されます（3 ページ目は、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）で説明されているオプションで構成されます）。

ナビゲーション パス

Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード（991 ページ）から、[トラフィック照合基準（Match Traffic By）] オプションを選択し、[次へ（Next）] をクリックします。

関連項目

- インスペクション ルールについて （977 ページ）
- インスペクション ルールのインターフェイスの選択 （979 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- インスペクション ルールの設定 （983 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- ルールの編集 （767 ページ）

フィールド リファレンス

次の表では、ウィザードの最初のページで [カスタム宛先ポート（Custom Destination Ports）] を選択した後に [検査/アプリケーション FW ルール（Inspect/Application FW Rule）] ウィザードの 2 ページ目に表示されるオプションについて説明します（ Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）を参照）。

表 *198 : [*検査/アプリケーション *FW* ルールの追加および編集（*Add or Edit Inspect/Application FW Rule*）*]* ウィザードのステップ *2* : *[*プロトコルおよびポート（*Protocol and Port*）*]* ページ

要素	説明
プロトコル	指定しているポートのプロトコル（TCP、UDP、または TCP/UDP）。 IOS デバイスに対して [Custom Destination Ports] を設定している場合は、TCP/UDP を選択する必要があります。

要素	説明
ポート	検査するトラフィックで使用されるポート。有効値の範囲は 1 ～ 65535 です。 • [Single]：ポート番号を 1 つだけ指定します。 • [Range]：10000-11000 など、ポートの範囲を指定します。 カスタム ポートを設定する場合、一部のプラットフォームまたは OS バージョンではポート範囲がサポートされないことに注意してください。すべての競合は、このルールを編集しているときではなく、ポリシーの検証中に識別されます。 **ヒント** 定義済みのポート マッピングと競合するポートまたはポート範囲を指定した場合は、デバイスでポートの再マッピングが許可されません。

次の表では、ウィザードの最初のページで [デフォルトプロトコルポート（Default Protocol Ports）] と [送信元と宛先の IP アドレス間で検査を制限する（Limit inspection between source and destination IP addresses）] を選択し、[送信元と宛先のアドレス（Source and Destination Address）] を選択した場合に、[検査/アプリケーション FW ルール（Inspect/Application FW Rule）] ウィザードの 2 ページ目に表示されるオプションについて説明します。ウィザードの最初のページについては、Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）で説明されています。

表 199 : [検査/アプリケーション FW ルールの追加および編集（Add and Edit Inspect/Application FW Rule）] ウィザードのステップ 2 : [アクション、送信元、宛先、およびサービス（Action, Sources, Destinations, and Services）] ページ

要素	説明
操作	設定された次の条件に基づいて、検査する必要のあるトラフィックを識別するかどうか。通常は、[許可（Permit）] ルールを作成します。 • [Permit]：検査するトラフィックを特定します。 • [Deny]：トラフィックを検査から免除します。トラフィックが許可されるかブロックされるかは、アクセス ルールによって決定されます。

要素	説明
ソース	このルールのトラフィックソースを提供します。ネットワーク、セキュリティグループ、およびユーザーになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 • ネットワーク – さまざまなネットワーク、ホスト、およびインターフェイスの定義を、個別に、またはオブジェクトとして指定できます。インターフェイスオブジェクトを送信元として選択した場合、ダイアログボックスにタブが表示され、ホスト/ネットワークとインターフェイスが区別されます。 「All-Address」オブジェクトは、ルールを特定のホスト、ネットワーク、またはインターフェイスに制限しません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IPv4 または IPv6 アドレスです。 （注） 完全修飾ドメイン名（FQDN）は、FQDN ネットワーク/ホストオブジェクトまたは FQDN オブジェクトを含むグループオブジェクトを提供することによってのみ指定できます。FQDN を直接入力することはできません。 • セキュリティグループ（ASA 9.0 以降）– ルールについて、1 つ以上のソースセキュリティグループの名前またはタグ番号を入力するか選択します（存在する場合）。 • ユーザー - ルールの Active Directory（AD）ユーザー名、ユーザーグループ、またはアイデンティティ ユーザー グループ オブジェクト（使用する場合）。次のものを組み合わせて入力できます。 • 個別のユーザ名：NetBIOS_DOMAIN\username • ユーザ グループ（\ を二重にします）：NetBIOS_DOMAIN\\user_group • アイデンティティ ユーザ グループ オブジェクト名。 （注） これらのフィールドのいずれかに、項目をカンマで区切って複数の値を入力します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックです。
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。送信元と同様に、ネットワークおよびセキュリティグループ（ASA 9.0 以降）タイプの 1 つ以上の宛先について、値またはオブジェクト名を入力するかオブジェクトを選択できます。

要素	説明
サービス	動作対象のトラフィックタイプを定義するサービス。サービスオブジェクトおよびサービスタイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力するか選択できます。 項目をカンマで区切って複数の値を入力します。
時間範囲	このルールが適用される時間を定義する時間範囲ポリシーオブジェクトの名前。時刻は、デバイスのシステム クロックに基づきます。この機能は、NTP を使用してシステム クロックを設定している場合に最適に機能します。 名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ

[検査/アプリケーションFWルール（Inspect/Application FW Rule）] ウィザードの [検査対象プロトコル（Inspected Protocol）] ページを使用して、このインスペクションルールによって監視されるプロトコルを設定します。

このセクションのオプションは、ファイアウォール インスペクション ルールを追加または編集したとき、および [Inspection Rules] ページ （986 ページ）のテーブルにある既存のルールの [検査対象のプロトコル（Inspected Protocol）] セルを右クリックしたときに表示されます。

（注） バージョン 4.9 以降、Security Manager では、ソフトウェアバージョン 9.4.0 以降を実行している ASA クラスタデバイスの SIP プロトコルをサポートします。

ナビゲーション パス

次のいずれかを実行します。

- Add Inspect/Application FW Rule ウィザードまたは Edit Inspect/Application FW Rule ウィザード （991 ページ）から、このページに達するまで [次へ（Next）] をクリックする。
- [検査対象プロトコルの編集（Edit Inspected Protocols）] ダイアログボックスを開くには、インスペクションルールの [検査対象プロトコル（Inspected Protocol）] セルを右クリックし、[検査対象プロトコルの編集（Edit Inspected Protocol）] を選択する。複数の行を選択すると、選択したすべてのルールに定義されている検査対象プロトコルが、変更によって置き換えられます。

関連項目

- [検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）
- インスペクション ルールについて （977 ページ）
- インスペクション ルールのインターフェイスの選択 （979 ページ）
- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールのアクセス ルール要件について （981 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- ルールの編集 （767 ページ）
- テーブルのフィルタリング （64 ページ）
- インスペクション ルールの設定 （983 ページ）

フィールド リファレンス

表 *200 : [*検査対象プロトコル（*Inspected Protocol***）*]* のオプション**

要素	説明
Protocols table	検査できるプロトコルのリストが表示されます。ルールごとに 1 つのプロトコルを選択できます。リストには、プロトコルのインスペクションを許可するデバイスのオペレーティングシステムに関する情報が含まれています。インスペクション ルール ポリシーを適用するデバイスタイプでサポートされていないプロトコルは選択しないでください。 **ヒント** IOS デバイスでは、ウィザードの最初のページで一致タイプに [カスタム宛先ポート（Custom Destination Ports）] または [宛先アドレスとポート（Destination Address and Port）] を選択した場合に、[カスタム プロトコル（custom protocol）] を選択し、[設定（Configure）] をクリックしてプロトコルに名前を付けることができます。その他のデバイス タイプでは、前に指定したポートに関連付けるプロトコルを選択します。 [オプション（Options）] 列には、選択したプロトコルに対して設定されているオプションが表示されます（存在する場合）。 [グループ（Group）] 列には、一部のプロトコルの使用に関する追加情報が表示されます。

要素	説明
Selected Protocol [Configure] ボタン	選択したプロトコルが表示されます。プロトコルで追加の設定が許可されている場合は、[Configure] ボタンがアクティブになります。このボタンをクリックするとオプションが表示され、開かれるダイアログボックスで [Help] ボタンをクリックすると、オプションに関する情報が表示されます。設定が許可されるプロトコルの詳細については、インスペクションのプロトコルおよびマップの設定 （1004 ページ）を参照してください。
Rule Settings (IOS)	ルールが Cisco IOS ソフトウェアを実行しているデバイスで使用されている場合は、そのルールの追加設定。[Use Default Inspection] 設定を選択した場合は、IOS のデフォルト、またはインスペクション設定ポリシーで定義されている設定（IOS デバイスのインスペクション ルールの設定 （1129 ページ）を参照）が使用されます。これらは、イネーブルまたはディセーブルにできる設定です。 • [Alert]：ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。 • [Audit]：監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。 • [Timeout]：アクティビティがない場合にセッションが管理される時間の長さ（秒単位）を設定するかどうか。[タイムアウトを指定（Specify Timeout）] を選択した場合は、5 ～ 43200 秒のタイムアウト値を入力します。 • [Inspect Router Generated Traffic]：デバイス自体によって生成されるトラフィックを検査するかどうか。このオプションは、限られた数のプロトコルに対して使用できます。

[Configure DNS] ダイアログボックス

[Configure DNS] ダイアログボックスを使用して、PIX 7.0+、ASA、FWSM、および IOS デバイスでの DNS インスペクションを設定します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルで [DNS] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 201 : [Configure DNS] ダイアログボックス

要素	説明
Maximum DNS Packet Length	最大 DNS パケット長。値は 512 ～ 65535 です。

要素	説明
DNS Map	トラフィックの一致条件とアクション、プロトコル準拠ポリシー、およびフィルタ設定を定義する DNS ポリシーマップ オブジェクト。オブジェクト名を入力するか、[選択（Select）] をクリックしてオブジェクトを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
動的フィルタスヌーピングの有効化（Enable Dynamic Filter Snooping）	DNS ルックアップ情報のデータベースを構築するために、セキュリティ アプライアンスに DNS パケットのスヌープを許可するかどうか。この情報は、DNS 名と IP アドレスをマッチングするためにボットネット トラフィック フィルタリングで使用されます。 ボットネット トラフィック フィルタリング ルール ポリシーを設定する場合は、このオプションを選択します。それ以外の場合は、このオプションを選択しないでください。詳細については、[Botnet Traffic Filter Rules] ページ （1174 ページ）を参照してください。

[Configure SMTP] ダイアログボックス

SMTP のダイアログボックスを使用して、Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）インスペクションの設定を編集します。SMTP は、インターネット上でのサーバとクライアント間の電子メールの転送に使用されます。

SMTP インスペクションでは、不正なコマンドがあるパケットがすべてドロップされます。パケットの最大データ長を設定できます。0 ～ 4294967295 の範囲の長さを入力します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルで [SMTP] を選択して、[設定（Configure）] をクリックします。

[Configure ESMTP] ダイアログボックス

[Configure ESMTP] ダイアログボックスを使用して、Extended Simple Mail Transport Protocol（ESMTP; 拡張シンプル メール転送プロトコル）インスペクションの設定を編集します。プラットフォームに基づいて、次の設定を行うことができます。

- [IOS devices]：パケットの最大データ長を設定できます。0 ～ 4294967295 の範囲の長さを入力します。
- [ASA/PIX 7.x+ devices]：ESMTP ポリシー マップ オブジェクトを指定して、詳細インスペクション パラメータを定義できます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルで [ESMTP] を選択して、[設定（Configure）] をクリックします。

[Configure Fragments] ダイアログボックス

[Configure Fragments] ダイアログボックスを使用して、IOS デバイスのフラグメント インスペクションの設定を編集します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルで [フラグメント（fragment）] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 *202 : [Configure Fragments]* ダイアログボックス

要素	説明
Maximum Fragments	Cisco IOS ソフトウェアによって状態情報（構造）が割り当てられる、アセンブルされていないパケットの最大数。アセンブルされていないパケットとは、セッションの初期パケットよりも前に、ルータ インターフェイスに到着したパケットのことです。値は 0 ～ 10000 の状態エントリです。デフォルトは 256 です。 （注） 状態構造にはメモリが割り当てられます。この値をより大きい数値に設定すると、メモリ リソースが枯渇することがあります。
[タイムアウト(秒)（Timeout (sec)）]	パケット状態構造がアクティブに保たれる秒数。タイムアウト値が経過すると、アセンブルされていないパケットがルータによってドロップされ、別のパケットで使用できるように構造が解放されます。値は 1 ～ 1000 です。デフォルトのタイムアウト値は 1 秒です。

[Configure IMAP]/[Configure POP3] ダイアログボックス

[Configure IMAP]/[Configure POP3] ダイアログボックスを使用して、IOS デバイスの Internet Message Access Protocol（IMAP）または Post Office Protocol 3（POP3）インスペクションの設定を編集します。

- IMAP は、共有できるメール サーバ上に保持される電子メールまたは掲示板メッセージにアクセスするためのメソッドです。クライアント電子メール プログラムが、リモート メッセージにローカルであるかのようにアクセスできます。

- メール サーバに格納されている電子メールを受信するには POP3 が使用されます。IMAP とは異なり、POP はリモート ホストだけからメールを取得します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、[IMAP] または [POP3] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 *203 : [Configure IMAP]/[Configure POP3]* ダイアログボックス

要素	説明
Reset Connection on Invalid IMAP/POP3 packet	無効なパケットが検出された場合に、クライアントとサーバ間の接続をリセットするか、またはドロップするか。クライアントは、サーバに再接続するために検証プロセスを繰り返す必要があります。
Enforce Secure Authentication	パスワードがクリアテキストで送信されないように、クライアントがサーバへのセキュア ログインを使用する必要があるかどうか。

[Configure RPC] ダイアログボックス

RPC のダイアログボックスを使用して、IOS デバイスの RPC インスペクションの設定を編集します。RPC インスペクションでは、指定した RPC プログラムを除くすべての RPC プログラムのトラフィックがブロックされます。複数の RPC プログラムを許可するには、許可するプログラム番号ごとにルールを作成します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルで [RPC] を選択して、[設定（Configure）] をクリックします。

フィールド リファレンス

表 *204 : [Configure RPC]* ダイアログボックス

要素	説明
プログラム番号	許可するプログラム番号。値は 1 ～ 4294967295 です。
待ち時間（Wait Time）	同じ送信元アドレスから同じ宛先アドレスおよびポートへの後続の接続を許可するために、ファイアウォールの穴を開けたまま維持する時間（分単位）。値は 0 ～ 35791 分です。デフォルトは 0 です。

[Custom Protocol] ダイアログボックス

[Custom Protocol] ダイアログボックスを使用して、[検査/アプリケーション FW ルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、ステップ 2 （994 ページ）で IOS デバイスに対して設定したプロトコルとポートの指定に名前を割り当てます。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルでカスタムプロトコルを選択して、[設定（Configure）] をクリックします。

[Configure] ダイアログボックス

[Configure] ダイアログボックスを使用して、HTTP または IM インスペクションのポリシーマップオブジェクトを選択します。これらのタイプのインスペクションに使用されるマップは、デバイスで使用されているオペレーティング システム バージョンによって異なります。目的のバージョンを選択し、[選択（Select）] をクリックして、目的のポリシーマップオブジェクトを選択するか、新規に作成します。

ナビゲーション パス

[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）に移動し、プロトコルテーブルで [HTTP] または [IM] を選択して、[設定（Configure）] をクリックします。

インスペクションのプロトコルおよびマップの設定

デバイスのインスペクションルールを設定する場合は、検査するプロトコルを選択します。これらのプロトコルの一部では、詳細インスペクション用の追加設定が可能です。詳細インスペクションでは、パケットがデバイスを通過するために満たす必要のある追加要件を指定できます。たとえば、要求および応答のコンテンツ タイプが一致しない HTTP 接続をドロップできます。（検査可能なプロトコルの完全なリストについては、[インスペクションルール（Inspection Rule）] ページで [行の追加（Add Row）] をクリックし、[次へ（Next）] をクリックしてプロトコルリストを表示します）。

設定できる内容は、プロトコルだけでなく、デバイスのオペレーティングシステムとバージョン番号によっても異なります。通常は、IOS デバイスに比べて ASA デバイスの方がインスペクションを細かく微調整できます（IOS デバイスを設定するとき、インスペクションをより詳細に制御するには、ゾーンベースのファイアウォールインスペクションの設定を検討します。詳細については、ゾーンベースのファイアウォール ルールについて （1197 ページ）を参照してください）。

一部の詳細インスペクション設定は、インスペクションルールで直接行います。ただし、一部のプロトコルでは、独立したポリシー オブジェクトとして作成するポリシー マップを含むようにインスペクションルールを設定できます（デフォルトのインスペクションオプション以外が必要な場合にのみ、ポリシーマップを設定する必要があります）。これらのマップは、ポリ

シーの設定時にポリシー オブジェクト セレクタ ダイアログボックスから設定するか、[Policy Object Manager] ウィンドウ（**[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択）で設定できます。

ポリシーマップを使用するプロトコルでは、ターゲットトラフィックの一致条件を定義する、目的のポリシー マップを選択できます。ASA、PIX、および FWSM の各デバイスでは、これらのポリシー マップは一致条件を定義するクラス マップを指す場合があります。これらのポリシーマップを Policy Object Manager で作成するには、**[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）]** フォルダの次のテーブルにリストされているマップの 1 つを選択し、記載されているリファレンスで詳細な使用方法情報を確認します。**[マップ（Maps）] > [クラスマップ（Class Maps）] > 検査（Inspect）]** フォルダにあるクラスマップの作成の詳細については、一致条件ダイアログボックスに関する参照情報と インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

表 *205 :* インスペクション ルールでの詳細インスペクションのプロトコルの設定

プロトコル	**Device Types**	ポリシー マップ	クラス マップ（**ASA、PIX、FWSM** のみ）	説明および一致基準の参照
DNS	ASA、PIX、FWSM、IOS	DNS	DNS	クラス マップおよびポリシー マップを使用して、広範な基準に基づいてトラフィックを検査します。これにより、DNS パケットの広範な制御が可能になります。また、インスペクション ルールで最大長を設定し、（ASA デバイスで）ボットネット ルールでの動的 DNS スヌーピングの使用をイネーブルにできます。次のトピックを参照してください。 • DNS マップの設定 （1017 ページ） • DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1023 ページ） • [Configure DNS] ダイアログボックス （1000 ページ）

プロトコル	**Device Types**	ポリシーマップ	クラスマップ（**ASA、PIX、FWSM** のみ）	説明および一致基準の参照
FTP Strict	ASA、PIX、FWSM、IOS	FTP	FTP	ファイル名、タイプ、サーバ、ユーザ、または FTP コマンドに基づいてトラフィックを検査します。FTP マップの設定 （1031 ページ）および FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1033 ページ）を参照してください。
GTP	ASA、PIX、FWSM、IOS	GTP	GTP	タイムアウト値、メッセージサイズ、トンネル数、およびセキュリティアプライアンスを通過する GTP バージョンに基づいてトラフィックを検査します。GTP マップの設定 （1036 ページ）および GTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1041 ページ）を参照してください。
H.323 H.225 H.323 RAS	ASA、PIX、FWSM	H.323（ASA、PIX、FWSM）	H.323（ASA、PIX、FWSM）	H.323 メッセージ タイプ、発信側、着信側などの広範な基準に基づいてトラフィックを検査します。H.323 マップの設定 （1044 ページ）および H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1049 ページ）を参照してください。

プロトコル	Device Types	ポリシーマップ	クラスマップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
HTTP	ASA、PIX、FWSM、IOS	HTTP（ASA 7.1.x、PIX 7.1.x、FWSM 3.x、IOS） HTTP（ASA 7.2 以降、PIX 7.2 以降）	HTTP（ASA、PIX、FWSM）	ヘッダーや本文の内容、ポートの誤用、トラフィックにJavaアプレットが含まれているかどうかなど、広範な基準に基づいてトラフィックを検査します。使用されるマップは、オペレーティングシステムとバージョンによって異なります。 **ASA/PIX 7.2 以降**の場合は、 ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定 （1062 ページ）および HTTP クラスマップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1064 ページ）を参照してください。 **ASA/PIX 7.1.x、FWSM 3.x 以降、および IOS** の場合は、 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ）を参照してください。
SIP	ASA、PIX、FWSM	SIP（ASA、PIX、FWSM）	SIP（ASA、PIX、FWSM）	広範な基準に基づいてトラフィックを検査します。 SIP マップの設定 （1089 ページ）および SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1091 ページ）を参照してください。
Skinny	ASA、PIX、FWSM、IOS	Skinny	（なし）	広範な基準に基づいてトラフィックを検査します。 Skinny マップの設定 （1095 ページ）および Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1098 ページ）を参照してください。
SMTP	ASA、PIX 7.x+、FWSM 3.x+、IOS	（なし）	（なし）	Simple Mail Transfer Protocol（SMTP; シンプルメール転送プロトコル）トラフィックを検査し、無効なコマンドを使用するパケットをすべてドロップします。パケットの最大データ長を設定できます。 [Configure SMTP] ダイアログボックス （1001 ページ）を参照してください。

プロトコル	Device Types	ポリシーマップ	クラスマップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
SNMP	ASA、PIX、FWSM 3.x+、IOS	SNMP	（なし）	SNMP バージョンに基づいて SNMP トラフィックを検査します。 SNMP マップの設定 （1099 ページ）を参照してください。
NetBIOS	ASA、PIX 7.x+、FWSM	NetBIOS	（なし）	NetBIOS トラフィックを検査し、セキュリティアプライアンスの NAT 設定に従って NetBIOS Name Service（NBNS）パケット内の IP アドレスを変換します。プロトコルに違反するパケットをドロップできます。 NetBIOS マップの設定（1086 ページ）を参照してください。
IPSec Pass Through	ASA、PIX 7.x+	IPsec Pass Through	（なし）	IPSec トラフィックを検査し、ESP または AH トラフィックが許可されるかどうかを制御します。 IPsec パススルー マップの設定 （1084 ページ）を参照してください。
DCE/RPC	ASA 7.2+、PIX 7.2+、FWSM 3.2+	DCE/RPC	（なし）	タイムアウトとマッパー サービスの実行に基づいてトラフィックを検査します。 DCE/RPC マップの設定 （1013 ページ）を参照してください。
IP オプション	ASA 8.2(2)+	IP オプション	（なし）	IP ヘッダーの Options セクションに特定のオプションが設定されている IP パケットを許可します。ルーテッドモードでは、router-alert オプションを含むパケットが許可されます。それ以外の場合は、いずれかのオプションが設定されていると、パケットがドロップされます。IP オプションはほとんどの通信で必要ではありませんが、NOP（no operation）オプションがパディングに使用される場合があるため、このオプションを許可することが必要となることがあります。 IP オプション マップの設定 （1075 ページ）を参照してください。

プロトコル	Device Types	ポリシーマップ	クラスマップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
IPv6	ASA 8.4(2)+	IPv6	（なし）	IPv6 パケット内の任意の場所で見つかった次のタイプの拡張ヘッダーに基づいて IPv6 トラフィックを検査します。ホップバイホップオプション、ルーティング（タイプ 0）、フラグメント、宛先オプション、認証、およびカプセル化セキュリティペイロード。IPv6 マップの設定（1079 ページ）および IPv6 ポリシーマップの [マッチ条件とアクションの追加または編集（Add/Edit Match Condition and Action] ダイアログボックス（1081 ページ）を参照してください。
ESMTP	ASA、PIX 7.x+、FWSM 3.x+、IOS	ESMTP	（なし）	ESMTP トラフィックを検査します。IOS では、最大データ長だけを設定できます。ASA、PIX、FWSM では、広範な基準に基づいてトラフィックを検査できます。[Configure ESMTP] ダイアログボックス（1001 ページ）を参照してください。
フラグメント	IOS	（なし）	（なし）	アセンブルされていないパケットフラグメントの最大許容数に基づいてトラフィックを検査します。[Configure Fragments] ダイアログボックス（1002 ページ）を参照してください。
Internet Message Access Protocol（IMAP） Post Office Protocol 3（POP3）	IOS	（なし）	（なし）	無効なコマンドまたはクリアテキストログインに基づいてトラフィックを検査します。[Configure IMAP]/[Configure POP3] ダイアログボックス（1002 ページ）を参照してください。

プロトコル	Device Types	ポリシーマップ	クラスマップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
Sun Remote Procedure Call（RPC; リモートプロシージャコール）	FWSM 2.x、IOS	（なし）	（なし）	RPC プロトコル番号に基づいてトラフィックを検査します。[Configure RPC] ダイアログボックス （1003 ページ）を参照してください。
IM	ASA、PIX 7.x+、IOS	IM（ASA 7.2+、PIX 7.2+） IM（IOS）	IM（ASA、PIX のみ）	広範な基準に基づいてトラフィックを検査します。許可されるマップは、オペレーティングシステムのバージョンによって異なります。 **ASA、PIX** の場合は、ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定 （1069 ページ）および IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1071 ページ）を参照してください。 **IOS** の場合は、IOS デバイスの IM マップの設定 （1073 ページ）を参照してください。
SCTP	ASA 9.5(2)+	SCTP	（なし）	ペイロード PID（PPID）に基づいてトラフィックを検査します。SCTP マップの設定 （1100 ページ）および SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （1102 ページ）を参照してください。
Diameter	ASA 9.5(2)+	Diameter	Diameter	アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックを検査します。Diameter マップの設定 （1103 ページ）および Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス （1106 ページ）を参照してください。

プロトコル	Device Types	ポリシー マップ	クラス マップ（ASA、PIX、FWSM のみ）	説明および一致基準の参照
LISP	ASA 9.5(2)+	LISP	なし（None）	エンドポイント識別子アクセスリストおよび検証キーで許可されたトラフィックを検査します。LISP マップの設定 （1116 ページ）を参照してください
M3UA	ASA 9.6(2)+	M3UA	なし（None）	M3UA プロトコル準拠を満たさないパケットをドロップしてログに記録します。M3UA マップの設定 （1118 ページ）を参照してください

関連項目

- 検査するプロトコルの選択 （980 ページ）
- インスペクション ルールについて （977 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）
- インスペクション ルールの設定 （983 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- マップ オブジェクトについて （388 ページ）
- 正規表現の追加/編集 （1126 ページ）
- 正規表現グループの設定 （1125 ページ）

インスペクション ポリシーのクラス マップの設定

[Add Class Map]/[Edit Class Map] ダイアログボックスを使用すると、同じタイプのポリシーマップで使用するクラスマップを定義できます。ダイアログボックスの名前は、作成するマップのタイプを示します。

クラス マップでは、アプリケーション固有の基準に基づいてトラフィックを定義します。次に、対応するポリシー マップ内のクラス マップを選択し、選択したトラフィックに適用するアクションを設定します。したがって、各クラスマップには、同じ方法（許可する、ドロップするなど）で処理するトラフィックを含める必要があります。

ASA/PIX 7.2 以降、または FWSM を実行しているデバイスのインスペクションルールを設定している場合は、DNS、FTP、H.323、HTTP、IM、SIP、および ScanSafe のトラフィックタイプのインスペクション用クラスマップを作成できます。

関連ポリシー マップにクラス基準を定義することもできます。ただし、クラス マップを作成すると、複数のポリシー マップでマップを再利用できます。

ここでは、使用可能な一致基準について説明します。

- DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1023 ページ）
- FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1033 ページ）
- H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1049 ページ）
- HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1064 ページ）
- IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1071 ページ）
- SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1091 ページ）
- Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス （1106 ページ）

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルの [マップ（Maps）] > [クラスマップ（Class Maps）] > [検査（Inspect）] フォルダで [DNS]、[FTP]、[H.323 (ASA/PIX/FWSM)]、[HTTP (ASA/PIX/FWSM)]、[IM]、[SIP (ASA/PIX/FWSM)]、または [Diameter] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ルールについて （977 ページ）

フィールド リファレンス

表 *206* : インスペクション ルールの *[Add Class Maps]/[Edit Class Maps]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。

要素	説明
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Match] テーブル 一致タイプ（Match Type）	[Match] テーブルには、クラス マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、および検査される基準と値が示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Criterion] ダイアログボックスに入力します。詳細については、上記で示している項を参照してください。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

DCE/RPC マップの設定

[Add DCE/RPC Map]/[Edit DCE/RPC Map] ダイアログボックスを使用して、DCE/RPC インスペクションのマップを定義します。DCE/RPC インスペクション ポリシー マップを使用すると、DCE/RPC インスペクションに使用されるデフォルトの設定値を変更できます。

DCE/RPC は、Microsoft 分散クライアントおよびサーバ アプリケーションで広く使用されているプロトコルであり、ソフトウェア クライアントがサーバ上のプログラムをリモートで実行できるようにします。

このような処理では、一般的に、必要なサービスに動的に割り当てられるネットワーク情報を取得するために、エンドポイント マッパーと呼ばれるサーバのウェルノウン ポート番号をリスニングすることによって、クライアントがクエリーを実行します。次に、クライアントは、サービスを提供しているサーバーのインスタンスへのセカンダリ接続をセットアップします。

セキュリティ アプライアンスは、適切なポート番号とネットワーク アドレスへのセカンダリ接続を許可し、必要に応じて NAT を適用します。

DCE/RPC インスペクション マップは、EPM とウェルノウン TCP ポート 135 上のクライアントとの間のネイティブ TCP 接続を検査します。クライアント用に EPM のマッピングとルックアップがサポートされています。クライアントとサーバーは、どのセキュリティ ゾーンにあってもかまいません。埋め込みサーバ IP アドレスとポート番号は、該当する EPM 応答メッセージから受信されます。クライアントは EPM によって返されたサーバ ポートに複数の接続を試行できるため、ユーザが設定可能なタイムアウトのあるピンホールを複数使用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [DCE/RPC] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *207 : [Add DCE/RPC]/[Edit DCE/RPC]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Pinhole Timeout	DCE/RPC ピンホールのタイムアウト。デフォルトは 2 分（00:02:00）です。有効な値は、00:00:01 ～ 1193:00:00 です。
Enforce Endpoint Mapper Service	バインディング時にエンドポイント マッパー サービスを実行するかどうか。このサービスを使用して、クライアントはエンドポイント マッパーと呼ばれるサーバに、必要なサービスについて動的に割り当てられたネットワーク情報をクエリーします。

要素	説明
Enable Endpoint Mapper Service Lookup Service Lookup Timeout	エンドポイントマッパーサービスの検索操作をイネーブルにするかどうか。このオプションを選択した場合は、検索操作のタイムアウトを入力できます。タイムアウトを指定しない場合は、ピンホール タイムアウトまたはデフォルトのピンホール タイムアウト値が使用されます。有効な値は、00:00:01 ～ 1193:00:00 です。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（DCE/RPC クラスとポリシーマップの [一致条件（とアクション）の追加（Add Match Condition (and Action)）]/[一致条件（とアクション）の編集（Edit Match Condition (and Action)）] ダイアログボックス （1015 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

DCE/RPC クラスとポリシーマップの [一致条件（とアクション）の追加（Add Match Condition (and Action)）]/[一致条件（とアクション）の編集（Edit Match Condition (and Action)）] ダイアログボックス

[DCE/RPC一致基準の追加（Add DCE/RPC Match Criterion）]/[DCE/RPC一致基準の編集（Edit DCE/RPC Match Criterion）] ダイアログボックス（DCE/RPC クラスマップの場合）または [一致条件とアクションの追加（Add Match Condition and Action）]/[一致条件とアクションの編集

（Edit Match Condition and Action）] ダイアログボックス（DCE/RPC ポリシーマップの場合）を使用して、次の処理を行います。

- DCE/RPC クラスマップの一致基準と値を定義します。
- DCE/RPC ポリシーマップを作成するときに、DCE/RPC クラスマップを選択します。
- DCE/RPC ポリシーマップで一致基準、値、およびアクションを直接定義します。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

DCE/RPC クラスマップを作成している場合は、[Policy Object Manager] で、DCE/RPC の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 インスペクション ポリシーのクラス マップの設定（1011 ページ）を参照してください。

DNS ポリシーマップを作成している場合は、[Policy Object Manager] で、[DNSマップの追加（Add DNS Map）]/[DNSマップの編集（Edit DNS Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 DCE/RPC マップの設定 （1013 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *208 : DCE/RPC* クラスとポリシーマップの *[*一致条件とアクションの追加（*Add Match Condition and Action*）*]/[*一致条件とアクションの編集（*Edit Match Condition and Action*）*]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の DCE/RPC クラスマップを使用するか、新規 DCE/RPC クラスマップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [クラスマップの値を使用（Use Values in Class Map）]：既存の DCE/RPC クラス マップ ポリシー オブジェクトを選択する場合。DNS クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合するトラフィック基準を指定します。 • ms-rpc-epm：Microsoft RPC EPM メッセージを照合します。 • ms-rpc-isystemactivator：ISystemMapper メッセージを照合します。 • ms-rpc-oxidresolver：OxidResolver メッセージを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。 • [リセット（Reset）]：パケットをドロップし、接続を閉じ、サーバーとクライアントの両方またはいずれかに TCP リセットを送信します。 • [ログ（Log）]：システムログメッセージを送信します。このオプションは単独で使用するか、または他のアクションのいずれかと一緒に使用できます。 • [リセットとログ（Reset and Log）]：リセットアクションとログアクションを実行します。

DNS マップの設定

[Add DNS Map]/[Edit DNS Map] ダイアログボックスを使用して、インスペクション用の DNS マップを定義します。DNS マップを使用すると、DNS アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

DNS アプリケーション インスペクションは、DNS スプーフィングとキャッシュ ポイズニングを防ぐための DNS メッセージ制御をサポートしています。特定の DNS タイプを許可、ドロップ、または記録し、その他の DNS タイプをブロックするルールを設定できます。たとえば、サーバ間でのゾーン転送を制限できます。

公開サーバが特定の内部ゾーンだけをサポートしている場合に、DNS ヘッダーにある Recursion Desired フラグと Recursion Available フラグをマスクして、サーバを攻撃から守ることができます。また、DNS ランダム化をイネーブルにすると、ランダム化をサポートしていないサーバや強度の低い疑似乱数ジェネレータを使用するサーバのスプーフィングやキャッシュ侵害を回避

できます。クエリーできるドメイン名を制限することによって、パブリック サーバがより確実に保護されます。

不一致の DNS 応答を過度に多数受信した（このことはキャッシュ侵害攻撃を示している可能性があります）場合に、DNS 不一致のアラートを設定して通知できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[DNS]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 *209 : [Add DNS Map]/[Edit DNS Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Protocol Conformance] タブ DNS セキュリティの設定とアクションを定義します。このタブのオプションの詳細については、 DNS マップの [Protocol Conformance] タブ （1020 ページ）を参照してください。	
[Filtering] タブ DNS のフィルタリング設定を定義します。このタブのオプションの詳細については、 DNS マップの [Filtering] タブ （1021 ページ）を参照してください。	

要素	説明
[Mismatch Rate] タブ [DNS IDの不一致レートが超過した場合にロギング（Log When DNS ID Mismatch Rate Exceeds）] オプションでは、DNS 識別子不一致が過度に発生した場合に、次の基準に基づいてレポートするかどうかを決定します。 • [Threshold]：システム メッセージ ログが送信される前に許容される不一致の最大発生数。値は 0 ～ 4294967295 です。 • [Time Interval]：モニタする期間（秒単位）。値は 1 ～ 31536000 です。	
[Cisco Umbrellaコネクタ（Cisco Umbrella Connector）] タブ DNS の DNS Umbrella コネクタ設定を定義します。このタブのオプションの詳細については、[DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ （1022 ページ）を参照してください。	
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1023 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

DNS マップの [Protocol Conformance] タブ

[Protocol Conformance] タブを使用して、DNS マップの DNS セキュリティ設定とアクションを定義します。

ナビゲーション パス

[Add DNS Map]/[Edit DNS Map] ダイアログボックスの [Protocol Conformance] タブをクリックします。 DNS マップの設定 （1017 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 210 : DNS マップの [Protocol Conformance] タブ

要素	説明
Enable DNS Guard Function	DNS ヘッダーの識別子フィールドを使用して DNS クエリーおよび応答の不一致チェックを実行するかどうか。クエリーごとに 1 つの応答がセキュリティ アプライアンスを通過できます。
Generate Syslog for ID Mismatch	DNS 識別子の不一致が過度に発生した場合に syslog エントリを作成するかどうか。
Randomize the DNS Identifier for DNS Query	DNS クエリー メッセージの DNS 識別子をランダム化するかどうか。

要素	説明
Enable NAT Rewrite Function	DNS 応答の A レコードで IP アドレス変換をイネーブルにするかどうか。
Enable Protocol Enforcement	ドメイン名、ラベル長、圧縮、ループ ポインタのチェックなど、DNS メッセージ形式チェックをイネーブルにするかどうか。
Enable DNS on TCP	DNS over TCP トラフィックのインスペクションを有効にするかどうかを指定します。DNS/TCP ポート 53 トラフィックが、DNS インスペクションを適用するクラスの一部であることを確認します。インスペクションのデフォルト クラスには、TCP/53 が含まれています。
Require Authentication Between DNS Server (RFC2845) 操作	RFC 2845 の規定に従って、DNS サーバ間で認証を要求するかどうか。このオプションを選択した場合は、認証がない場合に実行するアクションを選択します。

DNS マップの [Filtering] タブ

[Filtering] タブを使用して、DNS マップの DNS フィルタリング設定とアクションを定義します。

ナビゲーション パス

[Add DNS Map]/[Edit DNS Map] ダイアログボックスの [Filtering] タブをクリックします。 DNS マップの設定 （1017 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 211 : DNS マップの [Filtering] タブ

要素	説明
Drop Packets that Exceed Specified Length Maximum Packet Length	指定したバイト単位の最大長を超えたパケットをドロップするかどうか。これはグローバル設定です。
Drop Packets Sent to Server that Exceed Specified Maximum Length 最大長（Maximum Length）	指定したバイト単位の最大長を超えた、サーバに送信されたパケットをドロップするかどうか。

要素	説明
Drop Packets Sent to Server that Exceed Length Indicated by Resource Record	サーバに送信されたパケットのうち、リソース レコードで指定された長さを超えるものをドロップするかどうか。
Drop Packets Sent to Client that Exceed Specified Length 最大長（Maximum Length）	クライアントに送信されたパケットのうち、指定したバイト単位の最大長を超えたものをドロップするかどうか。
Drop Packets Sent to Client that Exceed Length Indicated by Resource Record	リソース レコードで指定された長さを超えた、クライアントに送信されたパケットをドロップするかどうか。

[DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ

[Umbrellaコネクタ（Umbrella Connector）] タブを使用して、DNS マップの DNS Umbrella コネクタ設定を定義します。Cisco Security Manager バージョン 4.18 以降、Umbrella グローバルポリシーは ASA 9.10.1 以降のデバイスでサポートされています。

ナビゲーション パス

[DNSマップの追加（Add DNS Map）]/[DNSマップの編集（Edit DNS Map）] ダイアログボックスの [Umbrellaコネクタ（Umbrella Connector）] タブをクリックします。 DNS マップの設定（1017 ページ） を参照してください。

関連項目

- Umbrella グローバルポリシーの設定 （2487 ページ）

フィールド リファレンス

表 212 : [DNS Umbrellaコネクタ（DNS Umbrella Connector）] タブ

要素	説明
Umbrellaポリシーの Umbrellaコネクタタグの有効化（Enable Umbrella Connector Tag for Umbrella Policy）	チェックボックスをオンにして、DNS ポリシーマップ Umbrella タグ名を入力します。tag 名には、最大 50 文字を指定できます。タグ名が 50 文字を超える場合、Cisco Security Manager からエラーメッセージがスローされます。 （注） Umbrella グローバルポリシーが設定されていない場合、Cisco Security Manager からアクティビティ検証エラーが表示されます。Umbrella グローバルポリシー設定の詳細については、Umbrella グローバルポリシーの設定 （2487 ページ） を参照してください。

要素	説明
フェールオープンの有効化（Enable Fail-Open）	Umbrella DNS サーバーが使用できない場合に DNS 解決を動作させるには、このチェックボックスをオンにします。 フェールオープンが選択されていて、Cisco Umbrella DNS サーバーが使用できない場合、このポリシーマップで Umbrella 自体が無効になり、システム上に設定された他の DNS サーバー（存在する場合）に DNS 要求を移動できます。Umbrella DNS サーバーが再度使用可能になると、ポリシーマップはそれらの使用を再開します。このオプションを選択しない場合、アクセスできない Umbrella リゾルバに DNS 要求が移動し続けるため応答を得られません。
デバイスID	デバイス ID は、デバイスが Umbrellaサーバーに正常に登録された後に生成されます。ID は、Cisco Security Manager でデバイスを再検出した後にのみ、このフィールドに表示されます。 （注） デバイス ID に変更がある場合は常に、Cisco Security Manager でデバイスを再検出して、変更内容と同期させる必要があります。
DNSCryptの有効化（Enable DNScrypt）	Umbrella データパスで DNS 暗号化を有効にするには、このチェックボックスをオンにします。1 時間ごとに、秘密鍵がキーエクスチェンジスレッドと Umbrella リゾルバの間で交換されます。 [Umbrellaコネクタの有効化（Enable Umbrella Connector）] チェックボックスがオンになっていることを確認します。チェックボックスがオフの場合、設定の不一致に関するエラーメッセージが表示されます。 （注） Umbrella グローバルポリシーが設定されていない場合、Cisco Security Manager からアクティビティ検証エラーが表示されます。Umbrella グローバルポリシー設定の詳細については、Umbrella グローバルポリシーの設定 （2487 ページ）を参照してください。

DNS クラス マップおよび DNS ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add DNS Match Criterion]/[Edit DNS Match Criterion] ダイアログボックス（DNS クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（DNS ポリシー マップの場合）を使用して、次の処理を行います。

- DNS クラス マップの一致基準と値を定義する。
- DNS ポリシー マップの作成時に DNS クラス マップを選択する。
- DNS ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

DNS クラスマップを作成している場合は、[Policy Object Manager] で、DNS の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

DNS ポリシーマップを作成している場合は、[Policy Object Manager] で、[DNSマップの追加（Add DNS Map）]/[DNSマップの編集（Edit DNS Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。DNS マップの設定 （1017 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *213 : DNS* クラス マップおよび *DNS* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の DNS クラス マップを使用するか、新規 DNS クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の DNS クラス マップ ポリシー オブジェクトを選択する場合。DNS クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合するトラフィック基準を指定します。 • [DNS Class]：DNS クエリーまたはリソース レコードのクラスを照合します。 • [DNS Type]：DNS クエリーまたはリソース レコードのタイプを照合します。 • [Domain Name]：DNS クエリーまたはリソース レコードのドメイン名を照合します。 • [Header Flag]：ヘッダー内の DNS フラグを照合します。 • [Question]：DNS の質問を照合します。 • [Resource Record]：DNS リソース レコードを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で[一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
値 （DNS クラス基準の場合）	検査する DNS クラス。 • [Internet]：インターネット DNS クラスと一致します。 • [DNS Class Field Value]：指定した数値と一致します。 • [DNS Class Field Range]：指定した数値範囲と一致します。

要素	説明
値 （DNS タイプ基準の場合）	検査する DNS タイプ。 • [DNS Type Field Name]：DNS タイプの名前と一致します。 • [A]：IPv4 アドレス。 • [AXFR]：完全（ゾーン）転送。 • [CNAME]：正規の名前。 • [IXFR]：増分（ゾーン）転送。 • [NS]：権限ネームサーバ。 • [SOA]：権限のゾーンの開始。 • [TSIG]：トランザクション シグニチャ。 • [DNS Type Field Value]：指定した数値と一致します。 • [DNS Type Field Range]：指定した数値範囲と一致します。
値 （ドメイン名基準の場合）	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。

要素	説明
オプション 値 （ヘッダーフラグ基準の場合）	検査するヘッダー フラグ。[Options] フィールドを使用して、完全一致（等しい）または部分一致（含む）のどちらを適用するかを指定します。 • [Header Flag Name]：選択したヘッダー フラグ名と一致します。 • AA（権威のある回答） • QR（クエリー） • RA（再帰可能） • RD（再帰拒否） • TC（切り捨て）フラグ ビット • [Header Flag Value]：指定した 16 ビットの 16 進数値と一致します。
Resource Record	照合するセクションをリストします。 • [Additional]：DNS 追加リソース レコード。 • [Answer]：DNS 回答リソース レコード。 • [Authority]：DNS 権限リソース レコード。

ESMTP マップの設定

[Add ESMTP Map]/[Edit ESMTP Map] ダイアログボックスを使用して、ESMTP 検査マップの一致基準と値を定義します。ESMTPポリシーマップを使用すると、ESMTPインスペクションに使用するデフォルト設定値を変更できます。

ESMTP インスペクションでは、スパム、フィッシング、不正形式メッセージ攻撃、バッファオーバーフロー/アンダーフロー攻撃などの攻撃を検出します。また、アプリケーションセキュリティとプロトコル準拠により、正常な ESMTP メッセージだけを通し、各種の攻撃の検出や送受信者およびメール中継のブロックも行います。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [ESMTP]** を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

• マップ オブジェクトについて （388 ページ）

- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *214 : [Add ESMTP Map]/[Edit ESMTP Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大200 文字を使用できます。
[パラメータ （Parameters）] タブ	
Mask Server Banner	クライアントがサーバ情報を検出することを防ぐためにサーバ バナーをマスクするかどうか。
Configure Mail Relay ドメイン名 操作	ESMTP インスペクションでメール中継を検出するかどうか。このオプションを選択する場合は、検査しているドメイン名を入力し、メール中継が検出された場合に実行するアクションを選択します。
Special Character （ASA7.2.3+/PIX7.2.3+） 操作	送信者または受信者の電子メールアドレス内の特殊文字を検出するかどうか。このオプションを選択した場合は、特殊文字が検出された場合に実行するアクションを選択します。
Allow TLS（ASA7.2.3+、8.0.3+/PIX7.2.3） Action Log	セキュリティ アプライアンスで TLS プロキシを許可するかどうか。このオプションを選択した場合は、[Action Log] も選択して、TLS の検出時にログ エントリを作成できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（ESMTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1029 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ESMTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックスを使用して、ESMTP ポリシー マップの一致基準、値、およびアクションを定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。次の基準を使用できます。

- [Body Length]：メッセージ本文の長さと一致します。
- [Body Line Length]：メッセージ本文の行の長さと一致します。
- [Commands]：ESMTP コマンドと一致します。
- [Command Recipient Count]：受信者の電子メール アドレスの数と一致します。
- [Command Line Length]：コマンドラインの文字数と一致します。
- [EHLO Reply Parameters]：ESMTP EHLO 応答パラメータと一致します。
- [Header Length]：ヘッダーの文字数と一致します。
- [Header Line Length]：メッセージ ヘッダー内の行の文字数と一致します。
- [To Recipients Count]：ヘッダーの To フィールドの受信者数と一致します。
- [Invalid Recipients Count]：ヘッダー内の無効な受信者数と一致します。
- [MIME File Type]：MIME ファイル タイプと一致します。
- [MIME Filename Length]：ファイル名の文字数と一致します。

- [MIME Encoding]：MIME 符号化スキームと一致します。
- [Sender Address]：送信元のアドレスと一致します。
- [送信元アドレスの長さ（Sender Address Length）]：送信元のアドレスの文字数と一致します。

ナビゲーション パス

[Policy Object Manager] で、[ESMTPマップの追加（Add ESMTP Map）]/[ESMTPマップの編集（Edit ESMTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ESMTP マップの設定 （1027 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *215 : ESMTP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	照合する ESMTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	

要素	説明
最大長	評価されるフィールドの長さ（バイト単位）。この基準は、長さが指定した数値よりも大きい場合に一致し、フィールドが指定した数値よりも小さい場合は一致しません。 ダイアログボックスでは、[Body Length] および [Header Length] を除き、1 ～ 4294967295 を指定できる有効な長さ範囲を指定します。
コマンド	検査する ESMTP コマンド バーブ。
Greater Than Count	評価される項目の数。この基準は、カウントが指定した数値よりも大きい場合に一致し、カウントが指定した数値よりも小さい場合は一致しません。
パラメータ	検査する ESMTP EHLO 応答パラメータ。
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
MIME Encoding	検査する MIME 符号化スキーム。

FTP マップの設定

[Add FTP Map]/[Edit FTP Map] ダイアログボックスを使用して、FTP 検査マップの一致基準と値を定義します。FTP マップを使用して、FTP PUT などの特定の FTP プロトコル方式がセキュリティ アプライアンスを通過して FTP サーバに到達するのをブロックできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [FTP]** を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 216 : [Add FTP Map]/[Edit FTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Mask Greeting Banner from Server	FTP サーバのグリーティング バナーをマスクして、クライアントがサーバ情報を検出するのを防ぐかどうか。
Mask Reply to SYST Command	**syst** コマンドへの応答をマスクして、クライアントがサーバー情報を検出するのを防ぐかどうか。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1033 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。
Validate For [Validate] ボタン	オブジェクトを検証するデバイス プラットフォーム。オブジェクトを使用するプラットフォームを選択し、[検証（Validate）] をクリックして、そのオブジェクトがポリシー展開を回避するように設定されているか判断します。

FTP クラス マップおよび FTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add FTP Match Criterion]/[Edit FTP Match Criterion] ダイアログボックス（FTP クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（FTP ポリシー マップの場合）を使用して、次の処理を行います。

- FTP クラス マップの一致基準と値を定義する。
- FTP ポリシー マップの作成時に FTP クラス マップを選択する。
- FTP ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

FTP クラスマップを作成している場合は、Policy Object Manager で、FTP の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

FTP ポリシーマップを作成している場合は、Policy Object Manager で、[FTPマップの追加（Add FTP Map）]/[FTPマップの編集（Edit FTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。FTP マップの設定（1031 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *217 : FTP* クラス マップおよび *FTP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の FTP クラス マップを使用するか、新規 FTP クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の FTP クラス マップ ポリシー オブジェクトを選択する場合。FTP クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。
基準	照合する FTP トラフィック基準を指定します。 • [Request Command]：FTP 要求コマンドを照合します。 • [Filename]：FTP 転送のファイル名を照合します。 • [File Type]：FTP 転送のファイル タイプを照合します。 • [Server]：FTP サーバ名を照合します。 • [Username]：FTP ユーザ名を照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。

要素	説明
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
Request Commands	検査する FTP コマンド。 • [Append (APPE)]：ファイルに追加します。 • [Delete (DELE)]：サーバ サイトでファイルを削除します。 • [Help (HELP)]：サーバからヘルプ情報を提供します。 • [Put (PUT)]：stor（ファイルの保存）コマンドの FTP クライアント コマンド。 • [Rename From (RNFR)]：名前変更する元のファイル名を指定します。 • [Server Specific Command (SITE)]：サーバに固有のコマンドを指定します。通常、リモート管理に使用します。 • [Change to Parent (CDUP)]：現在の作業ディレクトリの親ディレクトリに変更します。 • [Get (GET)]：retr（ファイルの取得）コマンドの FTP クライアント コマンド。 • [Create Directory (MKD)]：ディレクトリを作成します。 • [Remove Directory (RMD)]：ディレクトリを削除します。 • [Rename To (RNTO)]：名前変更する先の名前を指定します。 • [Store File with Unique Name (STOU)]：ファイルを一意のファイル名で保存します。
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。

GTP マップの設定

[Add GTP Map]/[Edit GTP Map] ダイアログボックスを使用して、GTP 検査マップの一致基準と値を定義します。

GPRS Tunnel Protocol（GTP; GPRS トンネル プロトコル）は、モバイル サブスクライバに対して、GSM ネットワークと企業ネットワークまたはインターネットの間の中断のない接続を提供します。GTP は、トンネリング メカニズムを使用して、ユーザー データ パケットを伝送するためのサービスを提供します。

GTP マップ オブジェクトを使用すると、GTP アプリケーション インスペクションに使用するデフォルト設定値を変更できます。GTP プロトコルは、インターネットなどの TCP/IP ネットワークへのワイヤレス接続にセキュリティを提供する設計になっています。GTP マップを使用して、タイムアウト値、メッセージ サイズ、トンネル数、およびセキュリティ アプライアンスを通過する GTP バージョンを制御できます。

バージョン 4.18 以降、Cisco Security Manager は ASA 9.10.1 のアンチリプレイ機能をサポートします。データパケットのリプレイを有効にすることで、ネットワークはリプレイアタックから保護されます。

ヒント　GTP インスペクションには、特別なライセンスが必要です。必要なライセンスがない場合は、GTP マップを展開しようとした場合にデバイス エラーが発生します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）]>[GTP]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *218 : [Add GTP Map]/[Edit GTP Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
[パラメータ（Parameters）] タブ	
Country and Network Codes Table	マップに含める 3 桁の Mobile Country Code（mcc; モバイル国コード）および Mobile Network Code（mnc; モバイル ネットワーク コード）。コードは 000 ～ 999 です。 • コードを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します。 • 行を編集するには、行を選択し、[Edit] ボタンをクリックします。 • 行を削除するには、行を選択し、[Delete] ボタンをクリックします。
Permit Response Table	応答の送信先とは異なる GSN からの GTP 応答を許可するネットワーク/ホストポリシーオブジェクト。 • オブジェクトを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します。詳細については、[Add Permit Response]/[Edit Permit Response] ダイアログボックス （1040 ページ）を参照してください。 • 行を編集するには、行を選択し、[Edit] ボタンをクリックします。 • 行を削除するには、行を選択し、[Delete] ボタンをクリックします。
Request Queue	キュー内で許可される最大要求数。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。値は 1 ～ 9999999 です。デフォルトは 200 です。
Tunnel Limit	許可されるトンネルの最大数。
Permit Errors	エラーがあるか GTP バージョンが異なるパケットを許可するかどうか。デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。

要素	説明
データパケットリプレイウィンドウの有効化（Enable Data Packet Replay Window）	チェックボックスをオンにしてアンチリプレイを設定し、4 つのウィンドウサイズ（128、256、512、または 1024）からいずれかを選択します。ウィンドウサイズ外のメッセージはドロップされます。 GTP マップポリシーの設定については、[検査/アプリケーションFWルールの追加または編集（Add or Edit Inspect/Application FW Rule）] ウィザード、[検査対象プロトコル（Inspected Protocol）] ページ （998 ページ）を参照してください。
ヘッダーチェックの有効化（Enable Header Check）	データパケットのヘッダーチェックを有効にするには、このチェックボックスをオンにします。
アンチユーザースプーフィング（Anti-User Spoofing）	このフィールドは、[ヘッダーチェックの有効化（Enable Header Check）] チェックボックスをオンにした場合にのみ有効になります。関連するオプションを選択します。 • [バイパス（Bypass）]：ヘッダーチェックに合格したパケットを転送します。 • [ドロップ（Drop）]：ヘッダーチェックに合格したパケットをドロップします。
[Edit Timeouts] ボタン	このボタンをクリックして、さまざまな操作のタイムアウト値を設定します。これらのオプションの詳細については、[GTP Map Timeouts] ダイアログボックス （1040 ページ）を参照してください。
ロケーションロギングの有効化（Enable Location Logging）	このチェックボックスをオンにすると、モバイル国コードとモバイルネットワークコードを含む syslog メッセージを介して位置情報が取得されます。この syslog メッセージは、GTPv0/v1 の Gn/Gp または GTPv2 の S5/S8 で PDP コンテキストをアクティブ化または更新するときに表示されます。

要素	説明
セルIDの有効化（Enable Cell ID）	（任意）このチェックボックスをオンにして、セル ID を syslog メッセージに追加します。 （注） このオプションは、[ロケーションロギングの有効化（Enable Location Logging）] チェックボックスをオンにした場合にのみ有効になります。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[追加（Add）]ボタンをクリックし、[一致条件とアクション（Match Condition and Action）] ダイアログボックスに入力します（GTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1041 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

要素	説明
Validate For [Validate] ボタン	オブジェクトを検証するデバイス プラットフォーム。オブジェクトを使用するプラットフォームを選択し、[検証（Validate）] をクリックして、そのオブジェクトがポリシー展開を回避するように設定されているか判断します。

[Add Country Network Codes]/[Edit Country Network Codes] ダイアログボックス

[Add Country Network Codes]/[Edit Country Network Codes] ダイアログボックスを使用して、Mobile Country Code（mcc; モバイル国コード）および Mobile Network Code（mnc; モバイル ネットワーク コード）値を GTP ポリシー マップに追加します。コードは 000 ～ 999 です。

ナビゲーション パス

[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスで、[国コードとネットワークコード（Country and Network codes）] テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。GTP マップの設定 （1036 ページ） を参照してください。

[Add Permit Response]/[Edit Permit Response] ダイアログボックス

[Add Permit Response]/[Edit Permit Response] ダイアログボックスを使用して、応答の送信先とは異なる GSN からの GTP 応答を許可します。

トラフィックの宛先（[宛先オブジェクトグループ（To Object Group）]）および送信元（[送信元オブジェクトグループ（From Object Group）]）を定義するネットワーク/ホストポリシーオブジェクトの名前を入力します。[選択（Select）] をクリックして、リストからオブジェクトを選択します。[オブジェクトセレクタ（Object Selector）] ダイアログボックスの [作成（Create）] ボタンをクリックして、新しいオブジェクトを作成することもできます。

「any」という名前のネットワーク/ホストオブジェクトは使用できません。

ナビゲーション パス

[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスで、[応答の許可（Permit Response）] テーブルの [追加（Add）] ボタンをクリックするか、行を選択して [編集（Edit）] ボタンをクリックします。GTP マップの設定 （1036 ページ） を参照してください。

[GTP Map Timeouts] ダイアログボックス

[GTP Map Timeouts] ダイアログボックスを使用して、GTP マップのタイムアウト値を設定します。

ナビゲーション パス

[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスで、[パラメータ（Parameters）] タブの [タイムアウトの編集（Edit Timeouts）] ボタンをクリックします。 GTP マップの設定 （1036 ページ）を参照してください。

フィールド リファレンス

表 *219 : [GTP Map Timeouts]* ダイアログボックス

要素	説明
GSN タイムアウト（GSN Timeout）（ASA 9.5(1) より前） エンドポイントタイムアウト（Endpoint Timeout）（ASA 9.5(1) 以降）	非活動状態のままこの時間（hh:mm:ss）が経過すると GSN が削除されます。デフォルトは 30 分です。すぐにティアダウンしない場合は、0 を入力します。
PDP Context Timeout	PDP コンテキストの受信を開始する前に許容される最大期間（hh:mm:ss）。デフォルトは 30 分です。制限なしを指定する場合は、0 を入力します。
Request Queue Timeout	GTP メッセージの受信を開始する前に許容される最大期間（hh:mm:ss）。デフォルトは 60 秒です。制限なしを指定する場合は、0 を入力します。
Signaling Connections Timeout	非活動状態のままこの時間（hh:mm:ss）が経過すると GTP シグナリングが削除されます。デフォルトは 30 分です。シグナルを削除しない場合は、0 を入力します。
Tunnel Timeout	非活動状態のままこの時間（hh:mm:ss）が経過すると GTP トンネルがティアダウンされます。デフォルトは 60 秒です（PDP コンテキストの削除要求を受信していない場合）。すぐにティアダウンしない場合は、0 を入力します。
T3 Response Timeout	接続を除去する前に応答を待機する最大時間。

GTP ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックスを使用して、GTP ポリシー マップの一致基準、値、およびアクションを定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。

ナビゲーション パス

[Policy Object Manager] で、[GTPマップの追加（Add GTP Map）]/[GTPマップの編集（Edit GTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。GTP マップの設定 （1036 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *220 : GTP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	照合する GTP トラフィック基準を指定します。 • [Access Point Name]：アクセス ポイント名を照合します。このため、GTP アプリケーションのインスペクションがイネーブルになっている場合にドロップするアクセス ポイントを定義できます。 • [Message ID]：ドロップするメッセージの数値 ID を照合します。デフォルトでは、すべての有効なメッセージ ID が許可されます。 • [Message Length]：UDP パケットの長さを照合します。この基準を使用して、UDP ペイロードに対して許可されるメッセージの最大長のデフォルトを変更します。 • [Version]：GTP バージョンを照合します。 • [MSISDN]：MSISDN を正規表現またはクラスと照合し、一致する MSISDN を持つすべての GTP パケットをドロップします。 • [選択モード（Selection Mode）]：0 ～ 3 の範囲。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。 • [Drop Packet]：デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。 • Drop Packet and Log • レート制限
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
アクセス ポイント名（Access Point Name）	GTP アプリケーションのインスペクションがイネーブルになっている場合に作用するアクセス ポイント。 • [Specified By]：ドロップするアクセス ポイント名。デフォルトでは、有効な APN を持つすべてのメッセージが検査され、すべての APN が許可されます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
ID タイプ	操作対象のメッセージの数値 ID。 • [Value]：単一のメッセージ ID。値は、1 ～ 255 です。 • [Range]：メッセージ ID の範囲。範囲は 1 ～ 255 です。
最小長（Minimum Length）	UDP ペイロード内の最小バイト数。
最大長（Maximum Length）	UDP ペイロード内の最大バイト数。

要素	説明
バージョン	バージョン 4.9 以降、Security Manager は、ASA デバイス 9.5(1) 以降の GTP マップ オブジェクトで GPRS トンネル プロトコル（GTP）v2 および拡張 v1 のサポートを提供します。GTPv1 と GTPv2 に個別のメッセージ ID 照合を設定できるようになりました。 ASA デバイス 9.5(1) 以降の場合、条件としてメッセージ ID を選択すると、v1 と v2 の 2 つのバージョンのオプションが表示されます。v1 または v2 を選択し、1 から 255 までの単一の値、または 1 から 255 までの値の範囲を入力します。
Version Type	ASA バージョン 9.5(1) より前のバージョン：バージョン 0 を指定するには 0 を使用し、バージョン 1 を指定するには 1 を使用します。バージョン 0 の GTP ではポート 2123 を使用し、バージョン 1 ではポート 3386 を使用します。デフォルトでは、すべての GTP バージョンが許可されます。
正規表現	バージョン 4.18 以降、Cisco Security Manager では、正規表現を使用して MSISDN を設定し、一致する MSISDN を持つすべての GTP パケットをドロップできます。このフィールドは、[条件（Criterion）] ドロップダウンで MSISDN を選択すると表示されます。
正規表現グループ（Regular Expression Group）	バージョン 4.18 以降、Cisco Security Manager では、正規表現クラスを使用して MSISDN を設定し、一致する MSISDN を持つすべての GTP パケットをドロップできます。このフィールドは、[条件（Criterion）] ドロップダウンで MSISDN を選択すると表示されます。
モード値（Mode Value）	[条件（Criterion）] ドロップダウンで [選択項目（Selection）] が選択されている場合、このフィールドが表示されます。モード値を 0 ～ 3 の範囲で入力します。これは必須フィールドです。

H.323 マップの設定

[Add H.323 Map]/[Edit H.323 Map] ダイアログボックスを使用して、H.323 検査マップの一致基準と値を定義します。H.323 ポリシー マップを使用すると、H.323 インスペクションに使用するデフォルト設定値を変更できます。

H.323 インスペクションでは、Cisco CallManager や VocalTec Gatekeeper などの H.323 準拠アプリケーションがサポートされます。H.323 は、国際電気通信連合によって定義されている、LAN を介したマルチメディア会議用のプロトコル群です。セキュリティ アプライアンスでは、バージョン 4 までの H.323 がサポートされます。これには、H.323 v3 機能である Multiple Calls on One Call Signaling Channel（1 つのコール シグナリング チャネルでの複数コール）が含まれます。

H.323 インスペクションがイネーブルになっている場合、セキュリティ アプライアンスでは、H.323 バージョン 3 で導入された機能である同じコール シグナリング チャネルでの複数コール

がサポートされます。この機能により、コール セットアップ時間が短縮され、セキュリティ アプライアンス上で使用されるポート数が削減されます。H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化フォーマットで符号化されているため、セキュリティ アプライアンスでは、ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]を選択し、オブジェクトタイプセレクタから**[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [H.323 (ASA/PIX/FWSM)]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 221 : [Add H.323 Map]/[Edit H.323 Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	

要素	説明
HSI Group table	マップに含める HSI グループ。グループ番号、HSI ホストの IP アドレス、およびセキュリティ アプライアンスに接続しているクライアントの IP アドレスとインターフェイス名がテーブルに表示されます。グループあたり最大 5 つの HSI ホスト、HSI グループあたり最大 10 個のエンド ポイントが許可されます。 • グループを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します（[Add HSI Group]/[Edit HSI Group] ダイアログボックス （1047 ページ）を参照）。 • グループを編集するには、グループを選択し、[Edit] ボタンをクリックします。 • グループを削除するには、グループを選択し、[Delete] ボタンをクリックします。
Call Duration Limit	秒単位でのコール期間制限。範囲は 0:0:0 ～ 1163:0:0 です。値 0 は、タイムアウトしないことを示します。
Enforce Presence of Calling and Called Party Numbers	コールの確立で使用されるコールと着番号を強制するかどうか。
H.460.18 の SETUP の前に FACILITY メッセージを許可する（Allow the facility message before SETUP for H.460.18）	着信メッセージ手順の一部として、SETUP メッセージの前に FACILITY メッセージを送信できるようにするかどうか。 （注） H.460.18 では、ネットワーク アドレス変換機能とファイアウォールを越えて H.323 シグナリングを伝送するための方法が定義されています。
Check State Transition on H.225 Messages	H.225 メッセージで状態チェック検証をイネーブルにするかどうか。
Check State Transition on RAS Messages	RAS メッセージで状態チェック検証をイネーブルにするかどうか。
Create Pinholes on Seeing RCF Packets	ネットワークの内部にゲートキーパーがある場合に、H.323 エンドポイント間でコールの確立をイネーブルにするかどうか。デバイスは、Registration Request/Registration Confirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開けます。これらの RRQ/RCF メッセージは Gatekeeper との間で送受信されるので、発信側エンドポイントの IP アドレスは不明で、デバイスは発信元 IP アドレス/ポート 0/0 を通じてピンホールを開きます。 このオプションは、ASA 8.0(5)+ デバイスで使用可能です。

要素	説明
Check for H.245 Tunneling 操作	H.245 トンネル ブロッキングを実施し、[Action] リストボックスで選択したアクションを実行するかどうか。
Check RTP Packets for Protocol Conformance	プロトコル準拠のために、RTP パケットのフローがピンホールを経由することを調べるかどうか。
Payload Type must be Audio or Video based on Signaling Exchange	シグナリング交換に基づいてペイロード タイプをオーディオまたはビデオに強制するかどうか。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1049 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add HSI Group]/[Edit HSI Group] ダイアログボックス

[Add HSI Group]/[Edit HSI Group] ダイアログボックスを使用して、H.323 ポリシー インスペクション マップに HSI グループを追加します。

ナビゲーション パス

[H.323マップの追加（Add H.323 Map）]/[H.323マップの編集（Edit H.323 Map）] ダイアログボックスの [パラメータ（Parameters）] タブで、[HSIグループ（HSI group）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。 H.323 マップの設定 （1044 ページ）を参照してください。

フィールド リファレンス

表 *222 : [Add HSI Group]/[Edit HSI Group]* ダイアログボックス

要素	説明
グループ ID（Group ID）	HSI グループの ID 番号（0 ～ 2147483647）。
IPアドレス	HSI ホストの IP アドレス。
Endpoint table	HSI グループに関連付けられているエンドポイント。グループあたり最大 10 個のエンド ポイントを追加できます。エンド ポイントごとに、IP アドレスとインターフェイス ポリシー グループを指定します。 • エンド ポイントを追加するには、[Add] ボタンをクリックし、ダイアログボックスに入力します（ [Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス （1048 ページ）を参照）。 • エンド ポイントを編集するには、エンド ポイントを選択し、[Edit] ボタンをクリックします。 • エンドポイントを削除するには、エンドポイントを選択し、[Delete] ボタンをクリックします。

[Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス

[Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックスを使用して、HSI グループにエンド ポイントを追加します。

ナビゲーション パス

[HSI グループの追加（Add HSI Group）]/[HSI グループの編集（Edit HSI Group）] ダイアログボックスで、エンドポイントテーブルの [行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。 H.323 マップの設定 （1044 ページ）を参照してください。

フィールド リファレンス

表 223 : [Add HSI Endpoint IP Address]/[Edit HSI Endpoint IP Address] ダイアログボックス

要素	説明
Network/Host	エンド ポイント ホストまたはネットワークの IP アドレス。
インターフェイス	セキュリティ アプライアンスに接続されているインターフェイスを識別するインターフェイス ポリシー グループ。ポリシーグループの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。ここで新しいポリシーグループを作成することもできます。

H.323 クラス マップおよび H.323 ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add H.323 Match Criterion]/[Edit H.323 Match Criterion] ダイアログボックス（H.323 クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（H.323 ポリシー マップの場合）を使用して、次の処理を行います。

- H.323 クラス マップの一致基準と値を定義する。
- H.323 ポリシー マップの作成時に H.323 クラス マップを選択する。
- H.323 ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

H.323 クラスマップを作成している場合は、Policy Object Manager で、H.323 の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

H.323 ポリシーマップを作成している場合は、Policy Object Manager で、[H.323マップの追加（Add H.323 Map）]/[H.323マップの編集（Edit H.323 Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。H.323 マップの設定 （1044 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *224 : H.323* クラス マップおよび *H.323* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の H.323 クラス マップを使用するか、新規 H.323 クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の H.323 クラス マップ ポリシー オブジェクトを選択する場合。H.323 クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラス マップオブジェクトを作成します。
基準	照合する H.323 トラフィック基準を指定します。 • [Called Party]：着信ユーザ アドレスを照合します。 • [Calling Party]：発信側アドレスを照合します。 • [Media Type]：メディア タイプを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	

要素	説明
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
メディア タイプ（Media Type）	検査するメディアのタイプ（オーディオ、ビデオ、またはデータ）。

ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

[Add HTTP Map]/[Edit HTTP Map] ダイアログボックスを使用して、ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップを定義します。

アプリケーション ファイアウォールとも呼ばれる拡張 HTTP インスペクション機能では、HTTP メッセージが RFC 2616 に準拠していること、RFC で規定された方式を使用していること、およびその他のさまざまな基準に準拠していることを確認します。このことは、HTTP メッセージを使用してネットワーク セキュリティ ポリシーを回避することによる攻撃を防止するのに役立ちます。

HTTP マップで HTTP インスペクションをイネーブルにした場合は、リセットおよびログ アクションを伴う厳格な HTTP インスペクションがデフォルトでイネーブルになります。インスペクションの失敗に対して実行するアクションは変更できますが、HTTP マップがイネーブルになっているかぎり、厳格なインスペクションはディセーブルにできません。Cisco Security Manager では、**http-map** コマンドを使用してデバイスにマップを設定します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [HTTP**

（**ASA 7.1.x/PIX 7.1.x/FWSM3.x/IOS**）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 225 : ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[一般（General）] タブ	準拠していない HTTP 要求が受信された場合に実行するアクションを定義し、コンテンツ タイプの検証をイネーブルにします。オプションの詳細については、HTTP マップの [General] タブ （1053 ページ）を参照してください。
[Entity Length] タブ	HTTP コンテンツの長さが設定したターゲットの範囲外の場合に実行するアクションを定義します。オプションの詳細については、HTTP マップの [Entity Length] タブ （1055 ページ）を参照してください。
[RFC Request Method] タブ	HTTP 要求で特定の RFC 要求メソッドが使用されている場合にセキュリティ アプライアンスが実行する必要のあるアクションを定義します。オプションの詳細については、HTTP マップの [RFC Request Method] タブ （1056 ページ）を参照してください。
[Extension Request Method] タブ	HTTP 要求で特定の拡張要求メソッドが使用されている場合に実行されるアクションを定義します。オプションの詳細については、HTTP マップの [Extension Request Method] タブ （1058 ページ）を参照してください。
[Port Misuse] タブ	特定の望ましくないアプリケーションが検出された場合に実行するアクションを定義します。オプションの詳細については、HTTP マップの [Port Misuse] タブ （1059 ページ）を参照してください。
[Transfer Encoding] タブ	HTTP 要求で特定の転送符号化タイプが使用されている場合に実行されるアクションを定義します。オプションの詳細については、HTTP マップの [Transfer Encoding] タブ （1060 ページ）を参照してください。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

HTTP マップの [General] タブ

[General] タブを使用して、準拠していない HTTP 要求が受信された場合に実行するアクションを定義し、コンテンツ タイプの検証をイネーブルにします。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [General] タブをクリックします。ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ） を参照してください。

関連項目

- 詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *226 : HTTP* マップの *[General]* タブ

要素	説明
Take action for non-RFC 2616 compliant traffic	RFC 2616 に準拠しないトラフィックに対して実行するアクションを設定するかどうか。指定できるアクションは、次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。 [Syslogの生成（Generate Syslog）] を選択して、非準拠トラフィックが検出された場合にメッセージを syslog に書き込むこともできます。
Verify Content-type field belongs to the supported internal content-type list.	サポートされる内部コンテンツ タイプ リストにコンテンツ タイプがないトラフィックに対して実行するアクションを設定するかどうか。指定できるアクションは、次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。 次のオプションも選択できます。 • [要求のACCEPTフィールドと応答のContent-typeフィールドの一致を検証する（Verify Content-type field for response matches the ACCEPT field of request）]：応答のコンテンツタイプが要求と一致することも確認します。 • [Syslogの生成（Generate Syslog）]：非準拠トラフィックが検出された場合にメッセージを syslog に書き込みます。
Override Global TCP Idle Timeout (IOS only)	TCP アイドル タイムアウトのデフォルト設定を変更するかどうか。この時間の経過後に通信アクティビティがない場合、IOS デバイスは接続を終了します。このオプションを選択した場合は、目的のタイムアウト値を秒単位で指定します。
Override Global Audit Trail Setting (IOS only) Enable Audit Trail	IOS デバイスの監査証跡設定を変更するかどうか。このオプションを選択した場合は、[監査証跡の有効化（Enable Audit Trail）] を選択して監査証跡メッセージを生成できます。

HTTP マップの [Entity Length] タブ

[Entity Length] タブを使用して、HTTP コンテンツの長さに基づくインスペクションをイネーブルにします。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Entity Length] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 227 : HTTP マップの [Entity Length] タブ

要素	説明

Inspect URI Length	URI の長さに基づくインスペクションをイネーブルにするかどうか。このオプションを選択した場合は、次の項目を設定します。
	• [Maximum]：バイト単位での URI の最大長（1 ～ 65535）。
	• [Excessive URI Length Action]：長さを超過した場合に実行するアクション。
	  • [Allow Packet]：メッセージを許可します。
	  • [Drop Packet]：接続を閉じます。
	  • [Reset Connection]：TCP リセット メッセージをクライアントとサーバに送信します。
	• [Generate Syslog]：違反が発生した場合に syslog メッセージを生成するかどうか。

要素	説明

Inspect Maximum Header Length	HTTP ヘッダーの長さに基づくインスペクションをイネーブルにするかどうか。このオプションを選択した場合は、次の項目を設定します。
	• [Request]：バイト単位での要求ヘッダーの最大長（1 ～ 65535）。
	• [Response]：バイト単位での応答ヘッダーの最大長（1 ～ 65535）。
	• [Excessive Header Length Action]：長さを超過した場合に実行するアクション。
	  • [Allow Packet]：メッセージを許可します。
	  • [Drop Packet]：接続を閉じます。
	  • [Reset Connection]：TCP リセット メッセージをクライアントとサーバに送信します。
	• [Generate Syslog]：違反が発生した場合に syslog メッセージを生成するかどうか。

Inspect Body Length	メッセージ本文の長さに基づくインスペクションをイネーブルにするかどうか。このオプションを選択した場合は、次の項目を設定します。
	• [Minimum Threshold]：バイト単位でのメッセージ本文の最小長（1 ～ 65535）。
	• [Maximum Threshold]：バイト単位でのメッセージ本文の最大長（1 ～ 65535）。
	• [Body Length Threshold Action]：メッセージ本文が設定した境界の範囲外の場合に実行するアクション。
	  • [Allow Packet]：メッセージを許可します。
	  • [Drop Packet]：接続を閉じます。
	  • [Reset Connection]：TCP リセット メッセージをクライアントとサーバに送信します。
	• [Generate Syslog]：違反が発生した場合に syslog メッセージを生成するかどうか。

HTTP マップの [RFC Request Method] タブ

[RFC Request Method] タブを使用して、HTTP 要求で特定の要求メソッドが使用されている場合に実行するアクションを定義します。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [RFC Request Method] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 228 : HTTP マップの [RFC Request Method]

要素	説明
Available and Selected Methods 操作 Syslog を生成する	[Available Methods] リストには、RFC 2616 で規定されている要求メソッドが表示されます。 メソッドのアクションを設定するには、メソッドを選択してから、アクションを選択します。選択したメソッドが含まれた HTTP 要求が発生したときに syslog にメッセージが追加されるようにする場合は、任意で [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、メソッドを [選択済みのメソッド（Selected Methods）] リストに追加します（メソッドを選択済みリストから削除するには、メソッドを選択し、[<<] ボタンをクリックします）。 **ヒント** アクションと syslog 要求がそれぞれ同じである場合は、Ctrl を押しながらクリックすることで、一度に複数のメソッドを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。
Specify the action to be applied for the remaining available methods above.	上記で特定のアクションを指定していないメソッドのデフォルトアクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルトアクションに使用する syslog 設定を選択します。

HTTP マップの [Extension Request Method] タブ

[Extension Request Method] タブを使用して、HTTP 要求で特定の拡張要求メソッドが使用されている場合に実行するアクションを定義します。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Extension Request Method] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 229 : HTTP マップの [Extension Request Method] タブ

要素	説明
Available and Selected Methods 操作 Syslog を生成する	[Available Methods] リストには、RFC 2616 で規定されている拡張要求メソッドが表示されます。 メソッドのアクションを設定するには、メソッドを選択してから、アクションを選択します。選択したメソッドが含まれた HTTP 要求が発生したときに syslog にメッセージが追加されるようにする場合は、任意で [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、メソッドを [選択済みのメソッド（Selected Methods）] リストに追加します（メソッドを選択済みリストから削除するには、メソッドを選択し、[<<] ボタンをクリックします）。 **ヒント** アクションと syslog 要求がそれぞれ同じである場合は、Ctrl を押しながらクリックすることで、一度に複数のメソッドを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。

要素	説明
Specify the action to be applied for the remaining available methods above.	上記で特定のアクションを指定していないメソッドのデフォルト アクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルト アクションに使用する syslog 設定を選択します。

HTTP マップの [Port Misuse] タブ

[Port Misuse] タブを使用して、ポートの誤用アプリケーション ファイアウォール インスペクションをイネーブルにします。設定できるアプリケーション カテゴリは次のとおりです。

- [IM]：インスタント メッセージング。チェックされるアプリケーションは、Yahoo! Messenger、AIM、および MSN IM です。
- [P2P]：ピアツーピア アプリケーション。Kazaa アプリケーションがチェックされます。
- [Tunneling]：トンネリング アプリケーション。チェックされるアプリケーションは、HTTPort/HTTHost、GNU Httptunnel、GotoMyPC、Firethru、および Http-tunnel.com Client です。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Port Misuse] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 230 : HTTP マップの [Port Misuse] タブ

要素	説明
Available and Selected Application Categories 操作 Syslog を生成する	[Available Application Categories] リストには、ファイアウォール インスペクション設定を定義できるカテゴリが表示されます。 カテゴリのアクションを設定するには、カテゴリを選択し、次にアクションを選択します。選択したアプリケーションが含まれるHTTP要求が発生したときにsyslogにメッセージが追加されるようにする場合は、任意で [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、カテゴリを [選択されたカテゴリ（Selected Categories）] リストに追加します（カテゴリを選択済みリストから削除するには、カテゴリを選択し、[<<] ボタンをクリックします）。 **ヒント** アクションとsyslog要求がそれぞれ同じである場合は、Ctrlを押しながらクリックすることで、一度に複数のカテゴリを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。
Specify the action to be applied for the remaining available categories above.	上記で特定のアクションを指定していないカテゴリのデフォルト アクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルト アクションに使用する syslog 設定を選択します。

HTTP マップの [Transfer Encoding] タブ

[Transfer Encoding] タブを使用して、転送符号化タイプに基づくインスペクションをイネーブルにします。設定できる符号化タイプは次のとおりです。

- [Chunked]：メッセージ本文が一連のチャンクとして転送される転送符号化タイプを識別します。
- [Compressed]：メッセージ本文が UNIX ファイル圧縮を使用して転送される転送符号化タイプを識別します。
- [Deflate]：メッセージ本文がzlib形式（RFC 1950）およびdeflate圧縮（RFC 1951）を使用して転送される転送符号化タイプを識別します。
- [GZIP]：メッセージ本文がGNU zip（RFC 1952）を使用して転送される転送符号化タイプを識別します。

- [Identity]：メッセージ本文で転送符号化が実行されない接続を識別します。

ナビゲーション パス

ASA 7.1.x/PIX 7.1.x/FWSM 3.x/IOS デバイスの [Add HTTP Map]/[Edit HTTP Map] ダイアログボックスの [Transfer Encoding] タブをクリックします。 ASA 7.1.x、PIX 7.1.x、FWSM 3.x、および IOS デバイスの HTTP マップの設定 （1051 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *231 : HTTP* マップの *[Transfer Encoding]* タブ

要素	説明
Available and Selected Encoding Types 操作 Syslog を生成する	[Available Encoding Types] リストには、ファイアウォール インスペクション設定を定義できる転送符号化のタイプが表示されます。 あるタイプのアクションを設定するには、タイプを選択し、アクションを選択します。選択したタイプを含むHTTPリクエストが発生したときにsyslogにメッセージが追加されるようにする場合は、必要に応じて [Syslogの生成（Generate Syslog）] を選択します。[>>] ボタンをクリックして、タイプを [選択済みのエンコードのタイプ（Selected Encoding Types）] リストに追加します（あるタイプを選択済みリストから削除するには、タイプを選択し、[<<]ボタンをクリックします）。 **ヒント** アクションと syslog 要求がそれぞれ同じである場合は、Ctrl を押しながらクリックすることで、一度に複数のタイプを選択できます。 指定できるアクションは次のとおりです。 • [Allow Packet]：メッセージを許可します。 • [Drop Packet]：接続を閉じます。 • [Reset Connection]（デフォルト）：TCP リセット メッセージをクライアントとサーバに送信します。
Specify the action to be applied for the remaining available encoding types above.	上記で特定のアクションを指定していないタイプのデフォルト アクションを定義するかどうか。このオプションを選択した場合は、アクション、およびデフォルト アクションに使用する syslog 設定を選択します。

ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

[HTTPマップの追加（Add HTTP Map）]/[HTTPマップの編集（Edit HTTP Map）] ダイアログボックスを使用して、ASA および PIX ソフトウェアリリース 7.2 以降の HTTP 検査マップの一致基準と値を定義します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [HTTP (ASA 7.2+/PIX 7.2+)] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 232 : [Add HTTP Map]/[Edit HTTP Map] ダイアログボックス（ASA 7.2+/PIX 7.2+）

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Body Match Maximum	本文一致で検索する必要のある HTTP メッセージの本文の最大文字数。 **ヒント** 値が大きいと、パフォーマンスに多大な影響を与えることがあります。
Check for protocol violations	プロトコル違反をチェックするかどうか。

要素	説明
操作	定義した設定に基づいて実行するアクション。接続をドロップ、リセット、または記録できます。
Spoof Server	サーバHTTPヘッダー値を指定した文字列で置換できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1064 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。
Overrides: None	デバイスにオーバーライドが存在しないことを示します。表示を変更するには、オーバーライドを手動で設定する必要があります。詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 （注） [Allow Value Override per Device] を選択してもオーバーライドは自動的には設定されません。

HTTPクラスマップおよびHTTPポリシーマップ（ASA7.2+/PIX7.2+）の[AddMatchCondition and Action]/[Edit Match Condition and Action] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[Add HTTP Match Criterion]/[Edit HTTP Match Criterion] ダイアログボックス（HTTP クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（HTTP ポリシー マップの場合）を使用して、次の処理を行います。

- HTTP クラス マップの一致基準と値を定義する。
- HTTP ポリシー マップの作成時に HTTP クラス マップを選択する。
- HTTP ポリシー マップに一致基準、値、およびアクションを直接定義する。

これらのタイプのマップは、ASA 7.2 以降または PIX 7.2 以降のオペレーティングシステムを実行しているデバイスにのみ使用されます。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。次の基準を使用できます。

- [Request/Response Content Type Mismatch]：応答のコンテンツ タイプが要求の accept フィールドの MIME タイプの 1 つと一致する必要があることを指定します。
- [Request Arguments]：要求の引数に正規表現照合を適用します。
- [Request Body]：要求の本文に正規表現照合を適用します。
- [Request Body Length]：要求の本文の長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Request Header Count]：要求のヘッダー数が指定した数よりも大きいまたは小さいものが一致することを指定します。
- [Request Header Length]：要求のヘッダーの長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Request Header Field]：要求のヘッダーに正規表現照合を適用します。
- [Request Header Field Count]：指定したヘッダー フィールド数に基づいて、要求のヘッダーに正規表現照合を適用します。
- [Request Header Field Length]：指定したフィールド長に基づいて、要求のヘッダーに正規表現照合を適用します。
- [Request Header Content Type]：要求の content-type ヘッダー フィールドで評価するコンテンツ タイプを指定します。

- [Request Header Transfer Encoding]：要求の transfer-encoding ヘッダー フィールドで評価する転送符号化を指定します。
- [Request Header Non-ASCII]：要求のヘッダーに非 ASCII 文字があるかどうかを指定します。
- [Request Method]：照合する要求メソッドを指定します。
- [Request URI]：要求の URI に正規表現照合を適用します。
- [Request URI Length]：要求の URI の長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Response Body ActiveX]：要求の本文に ActiveX コンテンツがあるかどうかを指定します。
- [Response Body Java Applet]：要求の本文に Java アプレットがあるかどうかを指定します。
- [Response Body]：応答の本文に正規表現照合を適用します。
- [Response Body Length]：応答の本文の長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Response Header Count]：応答のヘッダー数が指定した数よりも大きいまたは小さいものが一致することを指定します。
- [Response Header Length]：応答のヘッダーの長さが指定したバイト数よりも大きいまたは小さいものが一致することを指定します。
- [Response Header Field]：応答のヘッダーに正規表現照合を適用します。
- [Response Header Field Count]：指定したヘッダー フィールド数に基づいて、応答のヘッダーに正規表現照合を適用します。
- [Response Header Field Length]：指定したフィールド長に基づいて、応答のヘッダーに正規表現照合を適用します。
- [Response Header Content Type]：応答の content-type ヘッダー フィールドで評価するコンテンツ タイプを指定します。
- [Response Header Transfer Encoding]：応答の transfer-encoding ヘッダー フィールドで評価する転送符号化を指定します。
- [Response Header Non-ASCII]：応答のヘッダーに非 ASCII 文字があるかどうかを指定します。
- [Response Status Line]：応答の状況表示行に正規表現照合を適用します。

ナビゲーション パス

HTTP クラスマップを作成している場合は、Policy Object Manager で、HTTP の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編

集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

HTTP ポリシーマップを作成している場合は、Policy Object Manager で、ASA/PIX 7.2+ のデバイスの [HTTPマップの追加（Add HTTP Map）]/[HTTPマップの編集（Edit HTTP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ASA 7.2+ および PIX 7.2+ デバイスの HTTP マップの設定 （1062 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 233 : HTTP クラス マップおよび HTTP ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の HTTP クラス マップを使用するか、新規 HTTP クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の HTTP クラス マップ ポリシー オブジェクトを選択する場合。HTTP クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。
基準	照合する HTTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。一部の基準では、これは使用可能な唯一のオプションです。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。アクションのタイプは選択した基準によって決まります。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
フィールド名	評価するヘッダー フィールドの名前。次のいずれかを選択できます。 • [Predefined]：定義済みの HTTP ヘッダー フィールド。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。

要素	説明
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。 [Request Header Transfer Encoding] または [Response Header Transfer Encoding] 基準を評価する場合は、次のオプションも指定できます。 • [Specified By]：転送符号化の次の定義済みタイプの 1 つ。 • [Chunked]：メッセージ本文は、一連のチャンクとして転送されます。 • [Compressed]：メッセージ本文は、UNIX ファイル圧縮を使用して転送されます。 • [Deflate]：メッセージ本文は、zlib 形式（RFC 1950）および deflate 圧縮（RFC 1951）を使用して転送されます。 • [GZIP]：メッセージ本文は、GNU zip（RFC 1952）を使用して転送されます。 • [Identity]：転送の符号化は実行されません。 • [Empty]：要求ヘッダーの transfer-encoding フィールドは空です。
最大長	評価されるフィールドの長さ（バイト単位）。この基準は、長さが指定した数値よりも大きい場合に一致し、フィールドが指定した数値よりも小さい場合は一致しません。
Greater Than Count	評価される項目の数。この基準は、カウントが指定した数値よりも大きい場合に一致し、カウントが指定した数値よりも小さい場合は一致しません。

要素	説明
コンテンツ タイプ（Content Type）	コンテンツ タイプ ヘッダー フィールドで指定した、評価するコンテンツ タイプ。次のいずれかを選択できます。 • [Specified By]：定義済み MIME タイプ。 • [Unknown]：MIME タイプは不明です。既知のすべての MIME タイプに照らして項目を評価する場合は、[Unknown] を選択します。 • [Violation]：本文のマジック番号は、コンテンツ タイプ ヘッダー フィールドの MIME タイプに対応している必要があります。 • [Regular Expression]、[Regular Expression Group]：評価する正規表現または正規表現グループ。これらのオプションの詳細については、[Value] フィールドの説明を参照してください。
要求メソッド	照合する指定済み要求メソッド。次のいずれかを選択できます。 • [Specified By]：定義済みの要求メソッド。 • [Regular Expression]、[Regular Expression Group]：評価する正規表現または正規表現グループ。これらのオプションの詳細については、[Value] フィールドの説明を参照してください。

ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[IM Mapの追加（Add IM Map）]/[IM Mapの編集（Edit IM Map）] ダイアログボックスを使用して、ASA/PIX 7.2 以降を実行しているデバイスの Instant Messenger（IM）検査マップを定義するための設定を行います。IMマップを使用すると、IMアプリケーションインスペクションに使用するデフォルト設定値を変更できます。

インスタント メッセージングでは、業務の実行時にクリア テキストが使用されることから、潜在的なネットワーク攻撃やウイルスの拡散が懸念されます。このため、特定のタイプのインスタントメッセージの発生はブロックする一方で、他のタイプは許可することが必要となる場合があります。

ASA および PIX デバイスでは、IM アプリケーション インスペクションにより、ネットワークの使用を制御するための詳細なアクセス コントロールが提供されます。正規表現を使用して、機密データの漏れとネットワークの脅威の伝播を阻止できます。Yahoo! Messenger または MSN Messenger トラフィックを検査できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IM (ASA 7.2+/PIX 7.2+)] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *234 : [Add IM Map]/[Edit IM Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1071 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

[Add IM Match Criterion]/[Edit IM Match Criterion] ダイアログボックス（IM クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（IM ポリシー マップの場合）を使用して、次の処理を行います。

- IM クラス マップの一致基準と値を定義する。
- IM ポリシー マップの作成時に IM クラス マップを選択する。
- IM ポリシー マップに一致基準、値、およびアクションを直接定義する。

これらのタイプのマップは、ASA 7.2 以降または PIX 7.2 以降のオペレーティングシステムを実行しているデバイスにのみ使用されます。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

IM クラスマップを作成している場合は、Policy Object Manager で、IM の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

IM ポリシーマップを作成している場合は、Policy Object Manager で、ASA 7.2/PIX 7.2 の [IM マップの追加（Add IM Map）]/[IMマップの編集（Edit IM Map）] ダイアログボックスの [一致

条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ASA 7.2+、PIX 7.2+ デバイスの IM マップの設定 （1069 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 235 : IM クラス マップおよび IM ポリシー マップ（ASA 7.2+/PIX 7.2+）の [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシー マップのみ）	既存の IM クラス マップを使用するか、新規 IM クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の IM クラス マップ ポリシー オブジェクトを選択する場合。IM クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、または新しいクラスマップオブジェクトを作成します。
基準	照合する IM トラフィック基準を指定します。基準は次のとおりです。 • [Filename]：IM ファイル転送サービスのファイル名を照合します。 • [Client IP Address]：送信元クライアント IP アドレスを照合します。 • [Client Login Name]：IM サービスのクライアント ログイン名を照合します。 • [Peer IP Address]：ピアまたは宛先の IP アドレスを照合します。 • [Peer Login Name]：IM サービスのピアまたは宛先のログイン名を照合します。 • [Protocol]：IM プロトコルを照合します。 • [Service]：IM サービスを照合します。 • [File Transfer Service Version]：IM ファイル転送サービス バージョンを照合します。

要素	説明
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [一致（Matches）]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
IPアドレス	照合する IP アドレス。
プロトコル	IM プロトコル（MSN Messenger または Yahoo! Messenger）。
サービス	検査する IM サービス。表示されているサービスの 1 つ以上を選択します。

IOS デバイスの IM マップの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

[Add IM Map (IOS)]/[Edit IM Map (IOS)] ダイアログボックスを使用して、IOS デバイスの Instant Messaging（IM; インスタント メッセージング）インスペクション ポリシー マップ オブジェクトを設定します。IM マップを使用すると、IM アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

インスタント メッセージングでは、業務の実行時にクリア テキストが使用されることから、潜在的なネットワーク攻撃やウイルスの拡散が懸念されます。このため、特定のタイプのインスタント メッセージの発生はブロックする一方で、他のタイプは許可することが必要となる場合があります。

IM アプリケーション インスペクションにより、ネットワークの使用を制御するための詳細なアクセス コントロールが提供されます。機密データの漏れおよびネットワークの脅威の伝播を阻止するのにも役立ちます。許可または拒否されるサーバを指定することで、スコープを限定できます。Yahoo! Messenger、MSN Messenger、および AOL インスタント メッセージのインスペクションがサポートされます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクト タイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IM (IOS)]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 236 : [Add IM Map (IOS)]/[Edit IM Map (IOS)] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
サービス タブ さまざまな IM サービス プロバイダーを表すタブ。各タブで使用できる設定は同じです。サービス プロバイダーごとに個別に設定する必要があります。次のフィールドの説明は、Yahoo!、MSN、および AOL の各サービスに適用されます。	
Text Chat	許可、拒否、記録、またはそのいくつかの組み合わせなど、テキスト チャット サービスの処理方法。

要素	説明
その他のサービス	許可、拒否、記録、またはそのいくつかの組み合わせなど、テキスト チャット以外のサービスの処理方法。IOS ソフトウェアは、音声チャット、ビデオチャット、ファイルの共有と転送、ゲームなど、テキスト チャット以外のすべてのサービスを 1 つのグループとして認識します。
Permit Servers	ここで指定したサーバからのトラフィックを許可します。使用できる形式は、カンマで区切られた IP アドレス、IP 範囲、およびホスト名です。
Deny Servers	ここで指定したサーバからのトラフィックを拒否します。使用できる形式は、カンマで区切られた IP アドレス、IP 範囲、およびホスト名です。
アラート（Alert）	アラートをイネーブルにするかディセーブルにするか。デフォルトは、デフォルトのインスペクション設定の使用です。
Audit	監査証跡をイネーブルにするかディセーブルにするか。デフォルトは、デフォルトのインスペクション設定の使用です。
タイムアウト（Timeout）	サービスのタイムアウト。デフォルトのインスペクション設定を使用するか、タイムアウトを指定することを選択できます。[Specify Timeout] を選択した場合は、タイムアウト値を秒単位で入力します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

IP オプション マップの設定

[Add IP Options Map]/[Edit IP Options Map] ダイアログボックスを使用して、ASA 8.2(2)+ デバイスの IP パケット ヘッダー内のオプションのインスペクション用マップを定義します。options

フィールドで提供される制御機能は、一部の状況では必須ですが、ほとんどの一般的な状況では不要です。

IP オプション インスペクションを設定しない場合、ASA デバイスは、オプションが設定されているすべてのパケットをドロップしますが、例外が 1 つあります。ルーテッドモードでは、ルータ アラート オプションを含むパケットが許可されます（ルータ アラート パケットを禁止するには、ルータ アラートを選択解除した IP オプション マップを作成し、ポリシー マップを使用して IP オプションを検査するようにインスペクション ルールを設定します）。

ヒント　パケット ヘッダー サイズと位置合わせを適切に保つために No Operation（NOP）オプションがパディングとして使用される場合があるため、NOP を許可することが必要な場合があります。

各オプションについて、次の動作を選択できます。

- [許可（Allow）]：パケットを許可し、IP ヘッダーの options フィールドを変更しません。
- [クリア（Clear）]：パケットを許可し、IP ヘッダーの options フィールドのオプションをクリアします。

オプションを選択しない場合は、オプションが禁止され、オプションを含むパケットがドロップされます。ここにリストされていないオプションを選択しても、パケットがドロップされます。この動作は変更できません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IPオプション（IP Options）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 237 : [Add IP Options Map]/[Edit IP Options Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。

要素	説明
End of Options List	End of Options List（EOOL）、または IP オプション 0 は、単一の 0 バイトだけを含み、オプションのリストの終わりを示すためにすべてのオプションの最後に置かれます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
No operation	No Operation（NOP）、または IP オプション 1 はパディングに使用されます。IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合は、NOP オプションを使用してオプションが 32 ビット境界に合わせられます。
Router alert	Router Alert（RTRALT）、または IP オプション 20 は、パケットがそのルータ宛ではない場合でも、パケットの内容を検査するように通過ルータに通知します。この検査は、RSVP を導入している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。
[基本セキュリティ（Basic Security）]（*ASA* デバイス *9.5(1)* 以降）	RFC 1108 の IP オプション基本セキュリティ（番号 130）。デフォルトはドロップです。
[商用セキュリティ（Commercial Security）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション商用セキュリティ（番号 134）。デフォルトはドロップです。
[デフォルト（Default）]（*ASA* デバイス *9.5(1)* 以降）	IP オプションデフォルト設定。デフォルトはドロップです。
[実験的フロー制御（Experimental Flow Control）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション実験的フロー制御（番号 205）。デフォルトはドロップです。
[実験的測定（Experimental Measurement）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション実験的測定（番号 10）。デフォルトはドロップです。
[拡張セキュリティ（Extended-Security）]（*ASA* デバイス *9.5(1)* 以降）	RFC 1108 の IP オプション拡張セキュリティ（番号 133）。デフォルトはドロップです。

要素	説明
[IMIトラフィック記述子（IMI Traffic Descriptor）]（*ASA* デバイス *9.5(1)* 以降）	IP オプション IMI トラフィック記述子（番号 144）。デフォルトはドロップです。
[クイックスタート（Quick Start）]（*ASA* デバイス *9.5(1)* 以降）	RFC 4782 の IP オプションルータアラート（番号 25）。デフォルトはドロップです。
[レコードルート（Record Route）]（*ASA* デバイス *9.5(1)* 以降）	RFC 791 の IP オプションレコードルート（番号 7）。デフォルトはドロップです。
[タイムスタンプ（Time Stamp）]（*ASA* デバイス *9.5(1)* 以降）	RFC 791 の IP オプションルータアラート（番号 68）。デフォルトはドロップです。
（注） バージョン 4.9 以降、Security Manager は、ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスに対して 10 の新しい IP オプションをサポートします。標準的または試行的なオプションを許可、クリア、またはドロップするように検査を調整できます。定義されているものとは別に、特定の IP オプションを設定することもできます。たとえば、0 ～ 255 の範囲の値を使用して、IP オプションを直接設定できます。Security Manager は CLI「[no] 0-255 allow | clear」をサポートします。また、IP オプションインスペクションマップで明示的に定義されていないオプションのデフォルトの動作を設定できます。許可およびオプションでクリアするオプションを選択するようになりました。IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml [英語]）を参照してください。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）]フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

IPv6 マップの設定

[IPv6マップの追加（Add IPv6 Map）]/[IPv6マップの編集（Edit IPv6 Map）] ダイアログボックスを使用して、IPv6 インスペクションマップの一致基準と値を定義します。IPv6 マップを使用して、IPv6パケットにある拡張ヘッダーの次に示すタイプに基づいて、選択的にIPv6パケットをドロップすることができます。

- ホップバイホップ オプション
- ルーティング（タイプ 0）
- フラグメント
- 宛先オプション
- 認証
- カプセル化セキュリティ ペイロード

これらのプロトコルに対応するサービスオブジェクトは、Policy Object Manager （290 ページ）のサービステーブルで利用できます。

（注） Security Manager 4.4 のリリースと ASA のバージョン 9.0 以降で、IPv4 インスペクションルールと IPv6 インスペクションルールを設定するための別個のポリシーが統合されました。ただし、IPv6 マップは、以前のバージョンをサポートするために引き続き提供されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [FTP] を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *238 : [IPv6マップの追加（Add IPv6 Map）]/[IPv6マップの編集（Edit IPv6 Map）]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。

要素	説明
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
[既存の拡張ヘッダーのみを許可（Permit only known Extension Headers）]	ASA が IPv6 拡張ヘッダーを検証するかどうかを指定します。これが選択された場合、不明な IPv6 拡張ヘッダーが検出されると、ASA はパケットをドロップし、アクションをログに記録します。 このオプションは、デフォルトで選択されます。
[拡張ヘッダーの順序を適用（Enforce Extension Header Order）]	RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用するかどうかを指定します。これが選択された場合、エラーが検出されると、ASA はパケットをドロップし、アクションをログに記録します。 このオプションは、デフォルトで選択されます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 これらの基準エントリは、 IPv6 ポリシーマップの [マッチ条件とアクションの追加または編集（Add/Edit Match Condition and Action] ダイアログボックス （1081 ページ）で作成および編集されます。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、 [Policy Object Overrides] ウィンドウ （314 ページ）でオーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

IPv6ポリシーマップの[マッチ条件とアクションの追加または編集（Add/EditMatchCondition and Action] ダイアログボックス

[一致条件とアクションの追加（Add Match Condition and Action）]/[一致条件とアクションの編集（Edit Match Condition and Action）] ダイアログボックスを使用して、IPv6 ポリシーマップの拡張ヘッダー一致基準およびアクションを定義します。拡張ヘッダーの内容は処理されません。アクションは、指定された EH タイプの存在のみに基づいて適用されます。

これらのダイアログボックスのフィールドは、選択した基準によって変わります。

（注） 複数の一致定義を 1 つの IPv6 ポリシーマップに適用できます。

ナビゲーション パス

[Policy Object Manager] で、[IPv6 マップの追加（Add IPv6 Map）]/[IPv6 マップの編集（Edit IPv6 Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。IPv6 マップの設定 （1079 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *239 : IPv6* ポリシーマップの *[*マッチ条件とアクションの追加または編集（*Add/Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	

要素	説明
	一致させる IPv6 拡張ヘッダーのタイプを選択します。 • [認証ヘッダー（AH）（Authentication Header (AH)）]：IP パケットの整合性とデータ発信元の認証を提供します。 • [宛先オプションヘッダー（Destination Options Header）]：IPv6 モビリティに使用され、特定のアプリケーションのサポートにも使用されます。 • [カプセル化セキュリティペイロード（ESP）ヘッダー（Encapsulating Security Payload (ESP) Header）]：ESP ヘッダーに続くすべての情報は暗号化され、中間ネットワーク デバイスからアクセスできません。 • [フラグメントヘッダー（Fragment Header）]：トラフィック送信元のフラグメント化パケット通信をサポートします。 • [ホップバイホップオプションヘッダー（Hop-by-Hop Options Header）]：パケットの配信パス内のすべてのノードによって検査される必要があるオプションの情報。 • [ヘッダー数（Header Count）]：パケット内のヘッダーの数。このオプションを選択すると、次のフィールドが表示されます。ここで、ヘッダー数の上限を指定します。 • [次より多い数（Greater Than Count）]：0 ～ 255 の値を入力します。 ヘッダー数が指定した数値よりも大きい場合に、パケットは一致とみなされます。ヘッダー数が指定した数値以下の場合は一致しません。 • [ルーティングヘッダータイプ（Routing Header Type）]：このオプションを使用して、ヘッダーコードに基づいて 1 つのヘッダータイプ、または複数の EH タイプを一致させます。このタイプを選択すると次の値オプションが表示されます。いずれかの値を指定します。 • [ルーティングタイプ（Routing Type）]：1 つの拡張ヘッダーコードを入力します（例：認証ヘッダーの場合は 51）。 • [ルーティングタイプフィールド範囲（Routing Type Field Range）]：開始値と終了値を入力して、EH コードの範囲を定義します。 • [ルーティングヘッダーアドレスカウント（Routing Header Address Count）]：パケットに埋め込まれている IP アドレスの数。このオプションを選択すると、次のフィールドが表示されます。アドレス数の上限を指定します。 • [次より多い数（Greater Than Count）]：0 ～ 255 の値を入力します。 アドレス数が指定した数値よりも大きい場合に、パケットは一致とみなされます。アドレス数が指定した数値以下の場合は一致しません。

要素	説明
タイプ（Type）	定義された基準に一致するトラフィックにのみマップが適用されることを指定します。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクションを選択します。 • [パケットをドロップ（Drop Packet）]：一致するパケットは通知なしでドロップされます。 • [パケットをドロップしてログに記録（Drop Packet and Log）]：一致するパケットはログに記録されてからドロップされます。 • [ログに記録（Log）]-一致するパケットがログに記録され、処理が続行されます。

IPsec パススルー マップの設定

[Add IPsec Pass Through Map]/[Edit IPsec Pass Through Map] ダイアログボックスを使用して、IPsec パススルー マップ ポリシー オブジェクトを設定します。IPsec パススルー マップ ポリシー マップを使用すると、IPsec パススルー インスペクションに使用するデフォルトの設定値を変更できます。

IPSecパススルーインスペクションエンジンを使用すると、セキュリティアプライアンスで、特定の ESP または AH アクセス リストを必要とすることなく、IKE（UDP ポート 500）ネゴシエーションが正常に行われたことによって 2 つのホスト間に生成される、ESP（IP プロトコル 50）および AH（IP プロトコル 51）トラフィックを渡すことができます。

ESP または AH トラフィックは、既存の制御フローが MPF フレームワークで定義された接続制限内である場合に、インスペクションエンジンによって許可されます。このとき、設定されたアイドル タイムアウトが適用されます。制御フローがない場合は、UDP アイドル タイムアウトが設定された IKE UDP ポート 500 トラフィックに対して新しい制御フローが作成されます。または、既存のフローが使用されます。

インスペクションエンジンにパケットが確実に到着するように、このようなすべてのトラフィック（ESP および AH）のために穴を開けます。この検査は制御フローに付加されます。制御フローは、少なくとも 1 つのデータ フロー（ESP または AH）が確立されているかぎり存在しますが、トラフィックのフローは常に同じ接続を経由します。この IKE 接続は、データ フローがあるかぎり開いた状態で保たれるため、キーの再生成は常に成功します。フローは、NAT が使用されているかどうかに関係なく作成されます。ただし、PAT はサポートされません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [IPSecパススルー（IPsec Pass Through）] を選択します。作業領域内を右クリックしてから [新

規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *240 : [Add IPsec Pass Through Map]/[Edit IPsec Pass Through Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Allow ESP Maximum ESP Tunnels per Client ESP Idle Timeout	ESP トラフィックを許可するかどうか。このオプションを選択した場合は、各クライアントで使用できる ESP トンネルの最大数と、ESP トンネルが閉じられる前にアイドル状態のままでいられる時間（時間:分:秒の形式）を設定できます。デフォルトのタイムアウトは 10 分（00:10:00）です。
Allow AH Maximum AH Tunnels per Client AH Idle Timeout	AH トラフィックを許可するかどうか。このオプションを選択した場合は、各クライアントで使用できる AH トンネルの最大数と、AH トンネルが閉じられる前にアイドル状態のままでいられる時間（時間:分:秒の形式）を設定できます。デフォルトのタイムアウトは 10 分（00:10:00）です。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

NetBIOS マップの設定

[Add NetBIOS Map]/[Edit NetBIOS Map] ダイアログボックスを使用して、NetBIOS インスペクションのマップを定義します。NetBIOS ポリシー マップを使用すると、NetBIOS インスペクションに使用するデフォルト設定値を変更できます。

NetBIOS インスペクション エンジンは、セキュリティ アプライアンスの NAT 設定に従って NetBIOS Name Service（NBNS）パケット内の IP アドレスを変換します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [NetBIOS]** を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *241 : [Add NetBIOS Map]/[Edit NetBIOS Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Check for Protocol Violation 操作	NetBIOS プロトコル違反をチェックするかどうか。このオプションを選択した場合は、違反の発生時に実行するアクションを選択します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ScanSafe マップの設定

[NetBIOSマップの追加（Add NetBIOS Map）]/[NetBIOSマップの編集（Edit NetBIOS Map）] ダイアログボックスを使用して、NetBIOS インスペクションのマップを定義します。ScanSafe ポリシーマップを使用すると、ScanSafe インスペクションに使用するデフォルト設定値を変更できます。

このダイアログボックスのフィールドは、クラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [ScanSafe]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 242 : ScanSafe の [一致条件およびアクションの追加（Add Match Condition and Action）] ダイアログボックス

要素	説明
パラメータ	

要素	説明
トランスポート プロトコル（Transport Protocol）	HTTPS または HTTP のいずれかを選択できます。 HTTPS の場合、許容される値の範囲は 1 ～ 65535 です。 HTTP の場合、許容される値の範囲は 1 ～ 65535 です。デフォルト値は 8080 です。
デフォルトのユーザー名（Default User Name）	ScanSafe サーバーのデフォルトのユーザー名
デフォルトのグループ名（Default Group Name）	ScanSafe サーバーのデフォルトのグループ名
カテゴリ	Cat-A ～ Cat-G を選択できます。 これは、オブジェクトに割り当てられたカテゴリです。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。
[一致条件とアクション（Match Condition and Action）] タブのみ	
クラス	クラスマップの名前
操作	ポリシー違反が発生したときに実行するアクションを選択できます
+（「追加」ボタン）	[一致条件およびアクションの追加（Add Match Condition and Action）] ダイアログボックスを開きます。このダイアログボックスには、次のフィールドがあります。 • 一致タイプ（Match Type） • クラスマップ • 操作

SIP マップの設定

[Add SIP Map]/[Edit SIP Map] ダイアログボックスを使用して、SIP アプリケーション インスペクションに使用する値を設定します。SIP インスペクション マップを使用すると、SIP アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーションセキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [SIP (ASA/PIX/FWSM)] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 243 : [Add SIP Map]/[Edit SIP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
Enable SIP Instant Messaging Extensions	インスタントメッセージング拡張をイネーブルにするかどうか。

要素	説明
Permit Non-SIP Traffic on SIP Port	SIP ポートで SIP 以外のトラフィックを許可するかどうか。
[サーバーとエンドポイントのIPアドレスの非表示（Hide Server's and Endpoint's IP Address）]	IP アドレスを非表示にして、IP アドレスのプライバシーをイネーブルにするかどうか。
Check RTP Packets for Protocol Conformance Limit Payload to Audio or Video based on the Signaling Exchange	プロトコル準拠のために、RTP/RTCP パケットのフローがピンホールを経由することを調べるかどうか。このオプションを選択した場合は、シグナリング交換に基づいてペイロードタイプをオーディオ/ビデオに強制することも選択できます。
If Number of Hops to Destination is Greater Than 0	Max-Forwards ヘッダーの値が 0 かどうかをチェックするかどうか。0 よりも大きい場合は、[Action] フィールドで選択するアクションが実装されます。デフォルトは、パケットのドロップです。
If State Transition is Detected	SIP 状態遷移をチェックするかどうか。遷移が検出された場合は、[Action] フィールドで選択するアクションが実装されます。デフォルトは、パケットのドロップです。
If Header Fields Fail Strict Validation	SIP ヘッダー フィールドが無効な場合に [Action] フィールドで指定したアクションを実行するかどうか。デフォルトは、パケットのドロップです。
[サーバーおよびエンドポイントのソフトウェアバージョンの検査（Inspect Server's and Endpoint's Software Version）]	User-Agent および Server ヘッダーで SIP エンドポイント ソフトウェア バージョンを検査するかどうか。デフォルトは、情報のマスクです。
If Non-SIP URI is Detected	SIP 以外の URI が Alert-Info および Call-Info ヘッダーに検出された場合に、[Action] フィールドで指定したアクションを実行するかどうか。デフォルトは、情報のマスクです。

要素	説明
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（SIP クラスマップおよびポリシーマップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1091 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

SIP クラス マップおよびポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add SIP Match Criterion]/[Edit SIP Match Criterion] ダイアログボックス（SIP クラス マップの場合）または [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス（SIP ポリシー マップの場合）を使用して、次の処理を行います。

- SIP クラス マップの一致基準と値を定義する。
- SIP ポリシー マップの作成時に SIP クラス マップを選択する。
- SIP ポリシー マップに一致基準、値、およびアクションを直接定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

SIP クラスマップを作成している場合は、Policy Object Manager で、SIP の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。インスペクション ポリシーのクラス マップの設定 （1011 ページ）を参照してください。

DNS ポリシーマップを作成している場合は、Policy Object Manager で、[SIPマップの追加（Add SIP Map）]/[SIPマップの編集（Edit SIP Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。SIP マップの設定（1089 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *244 : SIP* クラス マップおよび *SIP* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type） クラス名 （ポリシーマップのみ）	既存の SIP クラス マップを使用するか、新規 SIP クラス マップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の SIP クラス マップ ポリシー オブジェクトを選択する場合。IM クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明
基準	照合する SIP トラフィック基準を指定します。 • [Called Party]：To ヘッダーで指定された着信側を照合します。 • [Calling Party]：From ヘッダーで指定された発信側を照合します。 • [Content Length]：Content Length ヘッダーを照合します。 • [Content Type]：Content Type ヘッダーを照合します。 • [IM Subscriber]：SIP インスタント メッセンジャの加入者を照合します。 • [Message Path]：SIP Via ヘッダーを照合します。 • [Third Party Registration]：サードパーティ登録の要求者を照合します。 • [URI Length]：SIP ヘッダーの URI を照合します。 • [Request Method]：SIP 要求メソッドを照合します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で [一致しない（Doesn’t Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
操作 （ポリシーマップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	

要素	説明
値	評価する正規表現。次のいずれかを選択できます。 • [Regular Expression]：パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。 • [Regular Expression Group]：パターン マッチングに使用する正規表現を定義する、正規表現グループ オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現グループオブジェクトを作成できます。
URI Type	照合する URI のタイプ（SIP または TEL）。
最大長	評価されるフィールドの長さ（バイト単位）。この基準は、長さが指定した数値よりも大きい場合に一致し、フィールドが指定した数値よりも小さい場合は一致しません。
コンテンツ タイプ（Content Type）	コンテンツ タイプ ヘッダー フィールドで指定した、評価するコンテンツ タイプ。次のいずれかを選択できます。 • [SDP]：SDP SIP コンテンツ ヘッダー タイプを照合します。 • [Regular Expression]、[Regular Expression Group]：評価する正規表現または正規表現グループ。これらのオプションの詳細については、[Value] フィールドの説明を参照してください。

要素	説明
Resource Method	検査する要求メソッドを次に示します。 • [ack]：クライアントが INVITE 要求に対する最終的な応答を受信したことを確認します。 • [bye]：コールを終了し、発信側または着信側から送信できます。 • [cancel]：保留中のすべての検索を取り消しますが、すでに受け入れられているコールは終了しません。 • [info]：コールのシグナリング パスを経由する中間セッション シグナリング情報を伝えます。 • [invite]：ユーザまたはサービスがコール セッションへの参加を招待されることを示します。 • [message]：各メッセージが他のメッセージに依存しないインスタント メッセージを送信します。 • [notify]：以前の SUBSCRIBE メソッドによって要求されたイベントが発生したことを SIP ノードに通知します。 • [options]：サーバの機能をクエリーします。 • [prack]：暫定応答確認。 • [refer]：受信者が要求で提供されているリソースを参照することを要求します。 • [register]：To ヘッダー フィールドにリストされているアドレスを SIP サーバに登録します。 • [subscribe]：1 つのイベントまたは一連のイベントに関する通知をあとで受け取ることを要求します。 • [unknown]：ネットワークのセキュリティに未知の影響を与える可能性がある非標準拡張を使用します。 • [update]：セッションのパラメータを更新することをクライアントに許可しますが、ダイアログの状態に影響はありません。

Skinny マップの設定

[Add Skinny Map]/[Edit Skinny Map] ダイアログボックスを使用して、Skinny インスペクションの Skinny マップを定義します。Skinny ポリシー マップを使用すると、Skinny インスペクションに使用するデフォルト設定値を変更できます。

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager とともに使用する場合、

SCCP クライアントは H.323 準拠端末と相互運用できます。セキュリティ アプライアンスのアプリケーション層機能は、SCCP バージョン 3.3 を認識します。SCCP プロトコルには、2.4、3.0.4、3.1.1、3.2、3.3.2 の 5 つのバージョンがあります。

セキュリティ アプライアンスでは、3.3.2 までのすべてのバージョンがサポートされます。セキュリティ アプライアンスでは、SCCP に対して PAT と NAT がサポートされます。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。SCCP シグナリング パケットの NAT および PAT をサポートすることで、Skinny アプリケーションは、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できることを保証します。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。セキュリティ アプライアンスでは、DHCP オプション 150 および 66 もサポートされます。これは、TFTP サーバの場所を Cisco IP Phone およびその他の DHCP クライアントに送信することで実現されます。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [Skinny] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 245 : [Add Skinny Map]/[Edit Skinny Map] ダイアログボックス

要素	説明
名前	Skinny マップの名前。最大 40 文字を使用できます。
説明	最大 200 文字の Skinny マップの説明。
[パラメータ（Parameters）] タブ	
Enforce Endpoint Registration	コールを行う前に登録を強制するかどうか。
Maximum SCCP Station Message ID 0x	許可される SCCP スタティック メッセージ ID の最大数（16 進数）。

要素	説明
Check RTP Packets for Protocol Conformance Enforce Payload Type to be Audio or Video based on Signaling Exchange	プロトコル準拠のために、RTP パケットのフローがピンホールを経由することを調べるかどうか。このオプションを選択した場合は、ペイロード タイプを強制するかどうかも選択できます。
Minimum SCCP Prefix Length	許可される最小の SCCP 長。
Maximum SCCP Prefix Length	許可される最大の SCCP 長。
Media Timeout	メディア接続のタイムアウト値。
Signaling Timeout	シグナリング接続のタイムアウト値。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1098 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

Skinny ポリシー マップの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

[Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックスを使用して、Skinny ポリシー マップの一致基準、値、およびアクションを定義します。

ナビゲーション パス

[Policy Object Manager] で、[スキニーマップの追加（Add Skinny Map）]/[スキニーマップの編集（Edit Skinny Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 Skinny マップの設定 （1095 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *246 : Skinny* ポリシー マップの *[Add Match Condition and Action]/[Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	照合する Skinny トラフィック基準を指定します。
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、0xFFFF で [一致しない（Doesn't Match）] が選択されている場合は、メッセージ ID が 0xFFFF であるすべてのトラフィックがマップから除外されます。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。
ID Type	検査するメッセージ ID の 16 進値。 • [Value]：単一の 16 進数値を照合します。 • [Range]：値の範囲を照合します。
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。

SNMP マップの設定

[Add SNMP Map]/[Edit SNMP Map] ダイアログボックスを使用して、SNMP インスペクションのマップを定義します。SNMP ポリシー マップを使用すると、SNMP アプリケーション インスペクションに使用するデフォルト設定値を変更できます。

SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。セキュリティ アプライアンスでは、SNMP バージョン 1、2、2c、または 3 を拒否できます。許可するバージョンは、SNMP マップを作成して制御します。さらに、SNMP インスペクションをイネーブルにする場合に SNMP マップを適用します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [SNMP] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *247 : [SNMP*マップの追加（*Add SNMP Map*）*]/[SNMP*マップの編集（*Edit SNMP Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Disallowed SNMP Versions	禁止する SNMP のバージョン。 • SNMP Version 1 • SNMP Version 2c（コミュニティ ベース） • SNMP Version 2（パーティ ベース） • SNMP バージョン 3
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

SCTP マップの設定

SCTP は、TCP や UDP と同様、プロトコル スタックの IP の最上部で動作するトランスポート層プロトコルです。SCTP は、複数の送信元 IP アドレスまたは宛先 IP アドレス上の 2 つのエンドノード間でアソシエーションと呼ばれる論理的な通信チャネルを作成します。アソシエーションでは、各ノード（送信元と宛先）での IP アドレスのセットと、各ノードでのポートが定義されます。任意の IP アドレスを、アソシエーションのデータパケットの送信元または宛先 IP アドレスとして使用できます。メッセージは、ストリームとして定義された IP アドレスのペア間で送信できます。

ASA を通過する SCTP トラフィックがある場合、SCTP ポートに基づいてアクセスを制御するために Cisco Security Manager を設定し、アプリケーション層のインスペクションを導入して、接続を有効にし、必要に応じてペイロードプロトコル ID でフィルタ処理を実行し、アプリケーションを選択的にドロップ、ログに記録、またはレート制限できます。

SCTP 検査マップを追加し、SCTP アプリケーションでフィルタリングすることにより、アクセスルールを改善できます。ペイロードプロトコル識別子（PPID）に基づいて、SCTP トラフィッククラスを選択的にドロップ、ログに記録、またはレート制限できます。

PPID でフィルタ処理する場合は、次の点に注意してください。

- PPID はデータ チャンクに含まれており、1 つのパケットが複数のデータ チャンクを持つ場合があります。パケットに異なる PPID を持つデータ チャンクが含まれている場合、パケットはフィルタ処理されず、割り当てられたアクションがパケットに適用されません。
- PPID フィルタリングを使用してパケットをドロップまたはレート制限する場合は、トランスミッタによりドロップされたパケットが再送されることに注意してください。レート制限が適用された PPID のパケットは再試行で通過する可能性がありますが、ドロップされた PPID のパケットは再びドロップされます。ネットワーク上のこのような反復的ドロップの最終成果を評価することができます。

[SCTPマップの追加（Add SCTP Map）]/[SCTPマップの編集（Edit SCTP Map）] ダイアログボックスを使用して、SCTP 検査マップの一致基準と値を定義します。SCTP マップを使用して、ペイロード PID 基準に基づいてパケットを検査できます。PPID 一致基準に基づいて、パケットに対して次のアクションを実行できます。

- アクションなし
- パケットのドロップ
- パケットのログ記録
- レート制限

SCTP プロトコルに対応するサービスオブジェクトは、マップ オブジェクトについて （388 ページ） のサービステーブルで利用できます。

（注） SCTP 検査マップは、Cisco Security Manager 4.10 および ASA バージョン 9.5.2 以降でサポートされています。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [SCTP]** を選択します。テーブル内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- Policy Object Manager （290 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *248 : [SCTP*マップの追加（*Add SCTP Map*）*]/[SCTP*マップの編集（*Edit SCTP Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 これらの基準エントリは、SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （1102 ページ） で作成および編集されます。	

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、[Policy Object Overrides] ウィンドウ （314 ページ）でオーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス

[一致条件とアクションの追加（Add Match Condition and Action）]/[一致条件とアクションの編集（Edit Match Condition and Action）] ダイアログボックスを使用して、SCTP ポリシーマップのペイロード PID の一致基準およびアクションを定義します。選択的に処理するすべての PPID を識別するまで、プロセスを繰り返します。

ナビゲーション パス

[Policy Object Manager] で、[IPv6マップの追加または編集（Add or Edit IPv6 Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行を追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。IPv6 マップの設定 （1079 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *249 : IPv6* ポリシーマップの *[*一致条件とアクションの追加または編集（*Add or Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	ペイロード PID（PPID）基準を選択します。
タイプ（Type）	定義された基準に一致するトラフィック、または一致しないトラフィックにのみマップが適用されることを指定します。
SCTP PPID の現在のリストは http://www.iana.org/assignments/sctp-parameters/sctp-parameters.xhtml#sctp-parameters-25 で確認できます。	
最小ペイロード PID	PPID 番号を入力します。Cisco Security Manager が受け入れ、内部で処理される、名前に関連付けられた特定の PPID があります。テキストボックスに PPID 番号を入力し、[OK] をクリックします。デフォルト名と一致する場合、対応する名前が一致アクションテーブルに表示されます。
最大ペイロード PID	（オプション）2番目に高いPPIDを入力して、PPIDの範囲を指定します。
操作	SCTP データチャンクの PPID に基づいてアクションを選択します。 • [パケットをドロップ（Drop Packet）]：一致するすべてのパケットをドロップし、ログに記録します。 • [ログ（Log）]：システムログメッセージを送信します。 • [レート制限（Rate Limit）]：メッセージのレートを制限します。1秒間のパケット数で表したレートです。

Diameter マップの設定

Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。

Diameter はトランスポート層として TCP および SCTP を使用し、TCP/TLS および SCTP/DTLS によって通信を保護します。また、オプションで、データ オブジェクトの暗号化も提供できます。Diameter の詳細については、RFC 6733 を参照してください。

Diameterアプリケーションは、課金のユーザーアクセス、サービス認証、QoS、およびレートの決定といったサービス管理タスクを実行します。Diameter アプリケーションは LTE アーキテクチャのさまざまなコントロール プレーン インターフェイスで使用されますが、ASA は、次のインターフェイスについてのみ、Diameter コマンドコードおよび属性値ペア（AVP）を検査します。

- S6a：モビリティ マネージメント エンティティ（MME）- ホーム サブスクリプション サービス（HSS）
- S9：PDN ゲートウェイ（PDG）- 3GPP AAA プロキシ/サーバー
- Rx：ポリシー/課金ルール機能（PCRF） - コール セッション制御機能（CSCF）

Diameterインスペクションでは、Diameterエンドポイント用にピンホールを開いて通信を可能にします。このインスペクションは、3GPP バージョン 12 をサポートし、RFC 6733 に準拠しています。

パケットや接続のドロップまたはロギングなどの特別なアクションを適用するために、[Diameter マップの追加（Add Diameter Map）] および [Diameterマップの編集（Edit Diameter Map）] ダイアログボックスを使用し、アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックをフィルタリングできます。新規に登録されたDiameterアプリケーション用のカスタム AVP を作成できます。フィルタリングにより、ネットワークで許可するトラフィックを微調整できます。詳細については、カスタム AVP の作成と追加 （1109 ページ）を参照してください。

（注） 他のインターフェイス上で動作するアプリケーションに対する Diameter メッセージはデフォルトで許可され、渡されます。ただし、アプリケーション ID によって該当するアプリケーションを破棄するための Diameter インスペクション ポリシー マップを設定できます。これらのサポートされていないアプリケーションに対してコマンドコードまたはAVP に基づいてアクションを指定することもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [調査（Inspect）] > [Diameter] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

- インスペクション ポリシーのクラス マップの設定 （1011 ページ）
- カスタム AVP の作成と追加 （1109 ページ）

フィールド リファレンス

表 *250 : [Diameter*マップの追加および編集（*Add and Edit Diameter Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
[サポートされていないアプリケーションIDアクションログ（Unsupported application-id action log）]	マップ内のサポートされていない Diameter アプリケーション識別子（Diameter アプリケーション名）を記録します。 アプリケーション ID は、マップ内の 0 ～ 4294967295 の番号です。これらのアプリケーションは IANA に登録されます。次のコア アプリケーションがサポートされますが、他のアプリケーションもフィルタ処理できます。 3gpp-rx-ts29214（16777236） 3gpp-s6a（16777251） 3gpp-s9（16777267） common-message（0）：これは基本 Diameter プロトコルです。
[サポートされていないコマンドコードアクションログ（Unsupported command code action log）]	サポートされていない Diameter コマンドコードを記録します。コードは Diameter コマンドコードの名前または番号（0 ～ 4294967295）です。
[サポートされていないAVPアクションログ（Unsupported avp action log）]	サポートされていない属性と値のペアのパラメータをログに記録します。
[厳格なパラメータ（Strict Parameters）]	
[セッション検証の有効化（Enable Session Validation）]	セッション ID AVP 関連メッセージを検証します。
[ステート検証の有効化（Enable State Validation）]	ステートマシンの検証を有効にします。

要素	説明
[Match Condition and Action] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス（1106 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス

[Diameter一致基準の追加（Add Diameter Match Criterion）]/[Diameter一致基準の編集（Edit Diameter Match Criterion）] ダイアログボックス（Diameter クラスマップの場合）または [一致条件とアクション（Match Condition and Action）] ダイアログボックス（Diameter ポリシーマップの場合）を使用して、次の処理を行います。

- Diameter クラスマップの一致基準と値を定義する。
- Diameter ポリシーマップを作成するときに、Diameter クラスマップを選択する。
- Diameter ポリシーマップに直接、一致基準、値、およびアクションを定義する。

このダイアログボックスのフィールドは、選択した基準、およびクラスマップとポリシーマップのどちらを作成しているかによって変わります。

ナビゲーション パス

Diameter クラスマップを作成している場合は、Policy Object Manager で、Diameter の [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 インスペクション ポリシーのクラス マップの設定（1011 ページ）を参照してください。

Diameter ポリシーマップを作成している場合は、[Policy Object Manager] で、Diameterマップの追加（Add Diameter Map）]/[Diameterマップの編集（Edit Diameter Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 Diameter マップの設定 （1103 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *251 : Diameter* クラスとポリシーマップの *[*一致条件とアクションの追加および編集（*Add and Edit Match Condition and Action*）*]* ダイアログボックス

要素	説明
一致タイプ（Match Type） （ポリシーマップのみ）	既存の Diameter クラスマップを使用するか、新しい Diameter クラスマップを定義できます。 • [Use Specified Values]：このダイアログボックスでクラス マップを定義する場合。 • [Use Values in Class Map]：既存の Diameter クラス マップ ポリシー オブジェクトを選択する場合。Diameter クラスマップの名前を [クラス名（Class Name）] フィールドに入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。

要素	説明

基準	照合する Diameter トラフィックの基準を指定します。
	• [Application ID]：アプリケーション ID を照合します。アプリケーション ID は、[開始値（Begin Value）] フィールドの Diameter アプリケーションの名前または番号（0 ～ 4294967295）です。照合したい連続する番号が付いたアプリケーションの範囲がある場合は、[開始値（Begin Value）] フィールドの 2 番目の ID を含めることができます。アプリケーションの名前または番号別に範囲を定義でき、開始値と終了値間のすべての番号に適用されます。
	• [Command Code]：コマンドコードを照合します。コードは、[開始値（Begin Value）] フィールドの Diameter コマンドコードの名前または番号（0 ～ 4294967295）です。照合したい連続する番号が付されたコマンドコードの範囲がある場合は、[開始値（Begin Value）] フィールドの 2 番目のコードを含めることができます。コマンドコードの名前または番号別に範囲を定義でき、開始値と終了値間のすべての番号に適用されます。
	• [AVP]：属性値ペアを照合します。
	  • AVB ベースの属性値のみ照合するには、属性値ペアの名前または番号（1 ～ 4294967295）を指定します。最初のコードについては、カスタム AVP、RFC または 3GPP 技術仕様に登録されている AVP、およびソフトウェアで直接サポートされている AVP の名前を [開始値（Begin Value）] フィールドで指定できます。AVP の範囲を照合する場合は、[開始値（Begin Value）] フィールドの 2 番目のコードを番号で指定します。値によって AVP を照合する場合は、2 番目のコードを指定できません。[ベンダーID（Vendor ID）] フィールドに、一致するベンダーの ID 番号（0 ～ 4294967295）を指定します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
	  • 属性の値に基づいて AVP を照合するには、[AVPデータタイプ（AVP Data Type）] フィールドで追加の属性値を指定します。
	
	（注） カスタム AVP を作成して、新規 Diameter アプリケーションに追加できます。詳細については、以下を参照してください。 カスタム AVP の作成と追加 （1109 ページ）

タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で[一致しない（Doesn't Match）] を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
AVP データタイプ（AVP DataType）	これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。次に、サポートされているデータタイプの値オプションの特定の構文を示します。 • [Address]：照合する IPv4 または IPv6 アドレスを指定します。例：10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。 • [Diameter Identity]、[Diameter URI]、[Octet String]、[UTF8tString]：これらのデータタイプの照合には正規表現または正規表現クラスオブジェクトを使用します。 • [Enumerated]：[開始範囲（Begin Range）] および [終了範囲]（End Range）] フィールドで数値の範囲を指定します。範囲は 0 ～ 4294967295 です。 • Float32：8 桁の小数点表現 • Float64：16 桁精度の小数点表記 • Integer32：-2147483647 ～ 2147483647 • Integer64：-9223372036854775807 ～ 9223372036854775807 • Unsigned32：0 ～ 4294967295 • Unsigned64：0 ～ 18446744073709551615 • [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。 （注） カスタム AVP を作成して、新規 Diameter アプリケーションに追加できます。
操作 （ポリシー マップのみ）	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。

カスタム AVP の作成と追加

[AVPの追加（Add AVP）] ダイアログボックスを使用して、カスタム AVP を作成および追加します。カスタム AVP は IETF に登録して、新しい Diameter アプリケーションに追加できます。

（注） Cisco Security Manager では、一度作成したカスタム AVP オブジェクトは編集できません。ただし、[デバイスオーバーライド（Device Override）] オプションを使用すると、特定のデバイスのカスタム AVP を編集できます。カスタム AVP オブジェクトのパラメータを変更する場合は、Diameter 構成要素からカスタム AVP 参照を削除し（参照されている場合）、デバイスに展開します（デバイスに存在する場合）。次に、必要な値を設定してオブジェクトを再作成し、Diameter 構成要素で参照し直して、再度展開します。

ナビゲーション パス

Policy Object Manager でカスタム AVP を作成する場合、Diameter の [一致基準の追加（Add Match Criterion）] ダイアログボックスから [基準のAVP（AVP in the Criterion）] を選択し、[開始値（Begin Value）] を選択して、[AVPマップセレクタ（AVP Maps Selector）] ダイアログボックスで右クリックして AVP を追加します。

フィールド リファレンス

表 *252 : [AVP*の追加（*Add AVP*）*]* ダイアログボックス

要素	説明
名前	カスタム AVP の名前。最大 32 文字で指定できます。 （注） 名前の少なくとも 1 文字はアルファベットにする必要があります。
説明	AVP の説明。最大 80 文字で指定できます。
AVP コード	特定のベンダーコードアドレス空間に属する AVP コード（256 ～ 4294967295）の値を設定します。

要素	説明
データタイプ（DataType）	これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。次に、サポートされているデータタイプの値オプションに固有の構文を示します。 • [Address]：照合する IPv4 または IPv6 アドレスを指定します。例：10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。 • [Diameter Identity]、[Diameter URI]、[Octet String]、[UTF8tString]：これらのデータタイプの照合には正規表現または正規表現クラスオブジェクトを使用します。 • [Enumerated）]：[開始範囲（Begin Range）] および [終了範囲（End Range）] フィールドで数値の範囲を指定します。範囲は 0 ～ 4294967295 です。 • Float32：8 桁の小数点表現 • Float64：16 桁精度の小数点表記 • Integer32：-2147483647 ～ 2147483647 • Integer64：-9223372036854775807 ～ 9223372036854775807 • Unsigned32：0 ～ 4294967295 • Unsigned64：0 ～ 18446744073709551615 • [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。
ベンダー ID	[ベンダーID（Vendor ID）] フィールドに、ベンダーの ID 番号（0 ～ 4294967295）を指定します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて（310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

TLS プロキシオブジェクトの作成と追加

Diameter アプリケーションが TCP 上で暗号化されたデータを使用する場合、インスペクションはメッセージのフィルタリングルールを実装するためにパケット内を確認することはできません。したがって、フィルタリング ルールを作成し、それらを暗号化された TCP トラフィックにも適用する場合は、TLSプロキシを設定する必要があります。暗号化されたトラフィックで厳密なプロトコルを適用するには、プロキシも必要です。この設定はSCTP/DTLS トラフィックには適用されません。

TLSプロキシは中間者として機能します。このプロキシは、トラフィックを復号化し、検査してから再度暗号化し、目的の宛先に送信します。したがって、接続の両側（Diameterサーバーと Diameter クライアント）は ASA を信頼する必要があり、すべての当事者が必要な証明書を保有している必要があります。TLSプロキシを実装するには、デジタル証明書を十分に理解しておく必要があります。

（注） TLS プロキシ機能は、バージョン ASA 9.7.1 以降のマルチコンテキストデバイスでサポートされています。

Diameter インスペクション用の TLS プロキシを設定するには、次のオプションがあります。

- フル TLS プロキシ：ASA および Diameter クライアントと ASA および Diameter サーバー間のトラフィックを暗号化します。サーバーとの信頼関係を確立するには、次のオプションがあります。
  - スタティック プロキシ クライアント トラストポイントを使用します。ASA は、Diameterサーバーとの通信時に、すべてのDiameterクライアントに同じ証明書を示します。Diameterサーバーにとって全クライアントが同じように見えるので、クライアントごとに差別化サービスを提供することはできません。一方、このオプションは LDC 方式よりも高速です。
  - ローカルダイナミック証明書（LDC）を使用します。このオプションを使用すると、ASA は Diameter サーバーとの通信時に、Diameter クライアントごとに一意の証明書を示します。この方法では、Diameterサーバーでクライアントトラフィックの可視性が向上し、クライアントの特性に基づいて差別化サービスを提供できるようになります。
- TLS オフロード：ASA と Diameter クライアント間のトラフィックを暗号化しますが、ASA と Diameterサーバー間でクリアテキスト接続を使用します。このオプションは、デバイス間のトラフィックが保護された場所から離れることがないと確信している場合に、Diameter サーバーが ASA と同じデータセンターにあれば実行可能です。TLS オフロードを使用すると、必要な暗号化処理量が減るので、パフォーマンスを向上させることができます。これは、オプションの中で最速です。Diameter サーバーは、クライアントの IP アドレスのみに基づいて差別化サービスを適用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [TLS プロキシ（TLS Proxy）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *253 : [TLS* プロキシの追加（*Add TLS Proxy*）*]* ダイアログボックス

要素	説明
名前	TLS プロキシオブジェクトの名前。最大 63 文字で指定できます。 （注） 名前の少なくとも 1 文字はアルファベットにする必要があります。
説明	TLS プロキシオブジェクトの説明。
サーバーの設定	
[サーバープロキシ証明書（Server Proxy Certificate）]	[選択（Select）] をクリックして、Diameter クライアントの証明書への署名に使用されている CA 証明書を ASA トラストポイントにインポートします。この手順では、TLS ハンドシェイク中に提示するプロキシトラストポイント証明書を指定します。トラストポイントは、自己署名の場合またはサードパーティによって発行される場合があります。 これにより、ASA が Diameter クライアントを信頼できます。
[TLS プロキシハンドシェイク時のクライアント認証を有効化（Enable client authentication during TLS proxy handshake）]	TLS ハンドシェイク時に、ASA に証明書の提示と TLS クライアントの認証を要求する場合にオンにします。

要素	説明
暗号化（オプション）	4.14 以降、Cisco Security Manager では、TLS プロキシがサーバとして使用されている場合に暗号スイートを設定できます。 このフィールドでは、TLSハンドシェイク時に通知/照合される暗号スイートを定義します。 データの暗号化に必要なハッシュアルゴリズムを [使用可能なメンバー（Available Members）] リストから選択して [選択済みのメンバー（Selected Members）] リストに追加します。 （注） 4.19 以降、Cisco Security Manager では、ASA 9.12(1) デバイスの SSL 暗号において TLS プロキシを NULL SHA1 で設定すると、アクティビティ検証エラーメッセージが表示されます。
クライアント設定	
[リモート TCP サーバーとの通信にクリアテキスト使用するようにプロキシクライアントを設定（Configure the proxy client to use clear text to communicate with the remote TCP server）]	暗号化が必要ない場合は、クリアテキストを使用するプロキシクライアントを選択します。
[TLS クライアント用のプロキシ証明書を指定します。このクライアントプロキシ証明書は、自己署名の場合、CA に登録済みの場合、またはサードパーティによって発行される場合があります。（Specify the proxy certificate for the TLS client. The client proxy certificate could either be self-signed, enrolled with a CA or issued by a third party.）]	クライアントプロキシ証明書を指定する場合は、オンにします。 または、[選択（Select）] をクリックして TLS クライアント用の CA 証明書をインポートします。

要素	説明
[電話のローカルダイナミック証明書に署名する内部認証局を指定します。このローカル CA は、proxy-ldc-issuer が有効になっている自己署名証明書にするか、組み込みのローカル CA サーバーを使用して LDC を電話に発行することができます。（Specify the internal Certificate Authority to sign the local dynamic certificates for phones. This local CA can be self-signed certificate with proxy-ldc-issuer enabled or you may use embedded Local CA Server to issue LDC to phones.）]	ローカルダイナミック証明書の発行元を指定する場合は、オンにします。 または、[選択（Select）] をクリックして CA 証明書をインポートします。これは、ローカルダイナミック証明書（LDC）の発行者として機能します。
[ローカルダイナミック証明書のキーペア（Local Dynamic Certificate Key Pair）]	
[キーペア名（Key Pair Name）]	クライアントまたはサーバーのダイナミック証明書で使用する RSA キーペアを指定します。このキーペアは、「crypto key generate」コマンドで生成されている必要があります。 キーペアは、展開前にデバイスに存在している必要があります。
暗号化（オプション）	TLS ハンドシェイク時に通知/照合される暗号スイートを定義します。クライアントプロキシ（このプロキシはサーバーに対する TLS クライアントとして機能します）の場合、2 つの TLS レッグ間の非対称暗号化方式のために、ユーザー定義の暗号スイートで Hello メッセージの元の暗号スイートが置き換えられます。 データの暗号化に必要なハッシュアルゴリズムを [使用可能なメンバー（Available Members）] リストから選択して [選択済みのメンバー（Selected Members）] リストに追加します。 （注） ASA バージョン 9.7.1 以降、Cisco Security Manager は TLS1.2 の新しい暗号スイート（aes256-sha384 および aes128-sha256）をサポートしています。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

TLS プロキシオブジェクトの編集

Cisco Security Manager では、一度作成された TLS プロキシオブジェクトを編集することはできません。ただし、[デバイスの上書き（Device Override）] オプションを使用すると、特定のデバイスの TLS プロキシオブジェクトを編集できます。

TLS プロキシオブジェクトのパラメータを変更する場合は、Diameter 構成要素（これを参照している場合）から TLS プロキシ参照を削除し、デバイスに展開します（デバイスに存在する場合）。次に、新しい名前と必要な値でオブジェクトを再作成し、それを Diameter 構成要素内で参照し直し、再度展開します。

クラスマップで TLS プロキシを編集するには、次の展開手順を実行します。

1. [プラットフォーム（Platform）] > [サービスポリシー（Service Policy] > [ルール（Rules）] に移動して、デバイスから既存の TLS プロキシサーバーを含む関連するクラスマップを削除します。
2. [プラットフォーム（Platform）] > [サービスポリシー（Service Policy）] > [ルール（Rules）] に移動して、新しい TLS プロキシサーバーを含む関連するクラスマップをデバイスに展開します。

LISP マップの設定

Locator/ID Separation Protocol（LISP）は、ネットワーク アーキテクチャ兼プロトコルです。LISP は、単一の IP アドレスを 2 つのナンバリング スペースで置き換えます。ナンバリング スペースの一方は、ネットワーク接続ポイントにトポロジ的に割り当てられ、そのネットワーク経由のパケットのルーティングおよび転送に使用されるルーティング ロケータ（RLOC）です。もう一方は、ネットワーク トポロジとは関係なく割り当てられ、ナンバリング デバイスに使用されて管理境界で集約されるエンドポイント ID です。

LISP が定義しているのは、これら 2 つのナンバリング スペースをマッピングし、ルーティング不可能な EID を使用してデバイスから発信されたトラフィックを、ルーティングと転送に RLOC を使用するネットワーク インフラストラクチャで転送できるようにカプセル化するため

の機能です。LISP では、デバイスがルーティング不可能な EID をルーティング可能な RLOC にマップする際に使用する情報を交換するための一連の機能を提供しています。

LISP での ACL の展開を検討する場合、次の側面が重要です。

- LISP カプセル化では、すべてのパケットの LISP ヘッダーの直前にある UDP ヘッダーを使用して、2 つの異なるパケットグループを区別します。UDP 宛先ポート（4342）を使用する LISP コントロール プレーン パケットと、UDP 宛先ポート（4341）を使用する LISP データプレーンパケットです。ACL では、これら 2 つのパケットグループ間の区別を考慮する必要がある場合があります。
- LISP はカプセル化プロトコルであり、ACL ではレイヤ 3 およびレイヤ 4 ヘッダー情報に基づいてのみフィルタ処理されるため、サイトのセキュリティポリシーを実装するためには、パケット転送および LISP カプセル化プロセス内の特定のポイントまたは複数の異なるポイントで ACL を適用する必要がある場合があります。ACL のアプリケーションポイントと方向によって、ACL 自体の中で EID 名前空間と RLOC 名前空間のどちらが使用されるかが決まります。パケットは、LISP カプセル化の直前または LISP カプセル化解除の直後に、EID 名前空間を使用してフィルタ処理できます。パケットは、LISP カプセル化の直後または LISP カプセル化解除の直前に、RLOC 名前空間を使用してフィルタ処理できます。

[LISPマップの追加（Add LISP Map）] および [LISPマップの編集（Edit LISP Map）] ダイアログボックスを使用して、EID アクセスリストと検証キーに基づいてトラフィックをフィルタ処理できます。フィルタリングにより、ネットワークで許可するトラフィックを微調整できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [LISP]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 *254 : [LISP*マップの追加および編集（*Add and Edit LISP Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。

要素	説明
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[パラメータ（Parameters）] タブ	
許可されたEIDアクセスリスト（Allowed Eid access-list）	統合アクセスリストの構成要素を選択できます。
検証キー（Validation key）	暗号化されていないクリアテキストパスワードを指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可（311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

M3UA マップの設定

MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベース アプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバー プロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザー パート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。

M3UA は SCTP をトランスポート層として使用します。SCTP ポート 2905 が想定されるポートですが、異なるポートを使用するようにシグナリング ゲートウェイを設定することもできます。

MTP3 レイヤは、ルーティングおよびノードアドレッシングなどのネットワーク機能を提供しますが、ノードの識別にポイント コードを使用します。M3UA 層は、発信ポイント コード（OPC）および宛先ポイント コード（DPC）を交換します。これは、IP が IP アドレスを使用してノードを識別する仕組みと似ています。

M3UAインスペクションは、限定されたプロトコル準拠を提供します。オプションで、ポイント コードまたはサービス インジケータ（SI）に基づいてアクセス ポリシーを適用できます。また、メッセージのクラスおよびタイプに基づいてレート制限を適用できます。

M3UA プロトコル準拠

M3UAインスペクションでは、次の限定されたプロトコルを強制できます。インスペクションは、要件を満たさないパケットをドロップしてログに記録します。

- 共通のメッセージヘッダー。インスペクションでは、共通ヘッダー内のすべてのフィールドを確認します。
  - バージョン 1 のみ。
  - メッセージの長さが正しく設定されている必要があります。
  - 予約済みの値を使用したメッセージ タイプのクラスは許可されません。
  - メッセージ クラス内での無効なメッセージ ID は許可されません。
- ペイロード データ メッセージ。
  - 特定のタイプの 1 つのパラメータのみが許可されます。
  - SCTP ストリーム 0 でのデータ メッセージは許可されません。

M3UA インスペクションの制限事項

M3UA インスペクションには次の制限事項があります。

- NAT は、M3UA データに埋め込まれている IP アドレスではサポートされません。
- セグメント化されたM3UA メッセージは検査されず、ドロップされる可能性が高いです。
- SCTP はマルチホーミングまたはマルチストリーミングをサポートしていません。マルチホームフローをサポートする必要がある場合は、それらを許可するアクセスリストを作成する必要があります。
- ステートフルフェールオーバーは、コールフローおよびメッセージではサポートされません。コールフロー中に障害が発生すると、パケットがドロップされ、コールが切断される可能性があります。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）] > [M3UA] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- インスペクション ポリシーのクラス マップの設定 （1011 ページ）

フィールド リファレンス

表 *255 : [M3UA* マップの追加および編集（*Add and Edit M3UA Map*）*]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシーオブジェクトの説明。最大200文字を使用できます。
[パラメータ（Parameters）] タブ	
[SS7 バリアント（SS7 Variant）]	ネットワークで M3UA インスペクションに使用する SS7 バリアントを選択します。このオプションによって、ポイントコードの有効な形式が決定します。 オプションを設定して、M3UAポリシーを導入した後は、最初にポリシーを削除しないかぎり、ポリシーを変更することはできません。 デフォルトの SS7 バリアントは ITU です。
[M3UA アプリケーション サーバープロセス（ASP）状態検証を有効にする（Enable M3UA Application Server Process (ASP) State Validation）]	アプリケーションサーバープロセス（ASP）状態検証を実行する場合はオンにします。システムはM3UAセッションのASPの状態を維持し、検証結果に基づいてASPメッセージをドロップします。 ASPの厳密な状態検証を無効にすると、すべてのASPメッセージが検査されずに転送されます。
[タイムアウトの適用（Enforce Timeout）]	
エンドポイント（Endpoint）	M3UAエンドポイントの統計情報を削除するアイドルタイムアウトを入力します（hh:mm:ss形式）。タイムアウトを付けない場合は、0 を指定してください。デフォルトは 30 分（0:30:00）です。
セッション	ASPの厳密な状態検証を有効にしている場合にM3UAセッションを削除するためのアイドルタイムアウトを入力します（hh:mm:ss 形式）。 タイムアウトを付けない場合は、0 を指定してください。デフォルト値は 30 分（0:30:00）です。このタイムアウトが無効になっている場合、システムは古いセッションを削除できません。

要素	説明
[M3UA メッセージタグの検証（M3UA Message Tag Validation）] 指定したメッセージタイプの特定フィールドの内容を確認および検証するかどうかを指定します。検証で合格しなかったメッセージはドロップされます。検証はメッセージ タイプによって異なります。検証するメッセージを選択します。	
[利用できない宛先ユーザー部（DUPU）（Destination User Part Unavailable (DUPU)）]	ユーザー/理由フィールドが存在し、有効な理由およびユーザー コードのみが含まれている必要があります。
エラー（Error）	すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。
通知	ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。
[一致条件およびアクション（Match Condition and Action）] タブ [Match All] テーブルに、ポリシー マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、検査される基準と値、および条件を満たすトラフィックに対して実行されるアクションが示されます。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（M3UA ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （1122 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

M3UA ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス

[一致条件とアクション（Match Condition and Action）] ダイアログボックスを使用して、M3UA ポリシーマップで一致基準、値、およびアクションを直接定義します。

このダイアログボックスのフィールドは、ポリシーマップの作成中に選択した基準によって変わります。

ナビゲーション パス

M3UA ポリシーマップを作成している場合は、[Policy Object Manager] で、[M3UAマップの追加（Add M3UA Map）]/[M3UAマップの編集（Edit M3UA Map）] ダイアログボックスの [一致条件とアクション（Match Condition and Action）] タブのテーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。M3UA マップの設定 （1118 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）

フィールド リファレンス

表 *256 : M3UA* ポリシーマップの *[*一致条件とアクションの追加および編集（*Add and Edit Match Condition and Action]* ダイアログボックス

要素	説明
基準	一致する SCTP トラフィックの基準（メッセージ、DPC、OPC、またはサービスインジケータ）を指定します。

要素	説明
メッセージ基準	M3UA メッセージのクラスとタイプを照合します。ここでは、メッセージクラス ID の可能な値とそれに対応するメッセージ ID について詳しく説明します。これらのメッセージの詳細については、M3UA の RFC およびドキュメンテーションを参照してください。 • クラス ID 0（管理メッセージ）：メッセージ ID 0-1 • クラス ID 1（メッセージの転送）：メッセージ ID 1 • クラス ID2（SS7 シグナリングネットワーク管理メッセージ）：メッセージ ID 1-6 • クラス ID 3（ASP 状態保守メッセージ）：メッセージ ID 1-6 • クラス ID 4（ASP トラフィック メンテナンス メッセージ）：メッセージ ID 1-4 • クラス ID 9（ルーティングキー管理メッセージ）：メッセージ ID 1-4
DPC 基準	データメッセージ内の宛先ポイントコードを照合します。ポイントコードは zone-region-sp 形式で、各要素に使用できる値は SS7 バリアントによって異なります。
OPC 基準	データメッセージ内の発信ポイントコード、つまりトラフィックの送信元を照合します。ポイント コードは zone-region-sp 形式で、各要素に使用可能な値は SS7 バリアントによって異なります。 • ITU：ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。 • ANSI：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。 • Japan：ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。 • China：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

要素	説明
サービスインジケータ基準	サービスインジケータ番号を照合します（0～15）。使用可能なサービスインジケータは、変数セクションにリストされています。これらのサービスインジケータの詳細については、M3UA の RFC およびドキュメンテーションを参照してください。 • 0：シグナリング ネットワーク管理メッセージ • 1：シグナリング ネットワーク テストおよびメンテナンス メッセージ • 2：シグナリング ネットワーク テストおよびメンテナンス特別メッセージ • 3：SCCP • 4：電話ユーザー部 • 5：ISDN ユーザー部 • 6：データ ユーザー部（コールおよび回線関連のメッセージ） • 7：データ ユーザー部（設備の登録およびキャンセル メッセージ） • 8：MTP テスト ユーザー部に予約済み • 9：ブロードバンド ISDN ユーザー部 • 10：サテライト ISDN ユーザー部 • 11：予約済み • 12：AAL タイプ 2 シグナリング • 13：ベアラー非依存コール制御 • 14：ゲートウェイ制御プロトコル • 15：予約済み
タイプ（Type）	基準に一致する、または一致しないトラフィックをマップに含めるかどうかを指定します。たとえば、文字列「example.com」で[一致しない（Doesn’t Match）]を選択した場合、「example.com」を含むトラフィックはすべてマップの対象外になります。 • [Matches]：基準に一致する。 • [一致しない（Doesn't Match）]：基準に一致しない。

要素	説明
操作	定義された基準に一致するトラフィックに対してデバイスが適用するアクション。 • [Drop Packet]：デフォルトでは、解析時に失敗したすべての無効パケットがドロップされます。 • [ドロップパケットとログ（Drop Packet and Log）]：ドロップパケットと同じですが、加えてシステムログメッセージを送信します。 • [レート制限（Rate Limit）]：メッセージのレートを制限します。このオプションは、メッセージ基準が選択されている場合に使用できます。

正規表現グループの設定

[Add Regular Expression Groups]/[Edit Regular Expression Groups] ダイアログボックスを使用して、複数の正規表現を含む正規表現グループを定義します。グループにより、モジュール形式の正規表現を作成し、さまざまな用途のためにそれらの正規表現を複数の方法でグループ化できるようになります。オブジェクトは、一部のインスペクション クラス マップとインスペクション ポリシー マップで使用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから **[マップ（Maps）] > [正規表現グループ（Regular Expressions Groups）]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

フィールド リファレンス

表 257 : [Add Regular Expression Class Map]/[Edit Regular Expression Class Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
正規表現	グループに含める正規表現を含む正規表現ポリシー オブジェクト。オブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

正規表現の追加/編集

[Add Regular Expression]/[Edit Regular Expression] ダイアログボックスを使用して、クラスおよびポリシー インスペクション マップ、または正規表現グループ ポリシー オブジェクトで使用する正規表現を定義します。正規表現は、リモートアクセス SSL VPN クライアントの設定でも使用されます。

正規表現は、厳密な文字列として、またはテキスト文字列の複数のバリアントと一致するようにメタ文字を使用して、テキスト文字列を照合します。正規表現をさまざまなタイプのクラスおよびポリシー インスペクション マップで使用して、さまざまなターゲット アイテムを照合できます。たとえば、HTTP パケット内の本文テキストなど、特定のアプリケーション トラフィックのコンテンツを照合できます。

ナビゲーション パス

- **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択し、次にオブジェクトタイプセレクタから **[マップ（Maps）] > [正規表現（Regular Expressions）]** を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。
- ASA デバイスの [SSL VPNのその他の設定（SSL VPN Other Settings）] ポリシーの [クライアント設定（Client Settings）] タブから、[AnyConnectクライアントイメージ（AnyConnect Client Image）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、イメージを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）を参照してください。[AnyConnect クライアントイメージの追加（Add AnyConnect Client Image）] ダイ

アログボックスで、[選択（Select）]をクリックして[正規表現セレクタ（Regular Expressions Selector）]ダイアログボックスを開きます。新しい正規表現を追加するには、[正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスの [追加]（+）（Add (+)）] ボタンをクリックします。

関連項目

- マップ オブジェクトについて （388 ページ）
- インスペクションのプロトコルおよびマップの設定 （1004 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

フィールド リファレンス

表 *258 : [Add Regular Expression]/[Edit Regular Expression]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
値	100 文字までの長さの正規表現。正規表現の作成に使用できるメタ文字の詳細については、正規表現の作成に使用されるメタ文字 （1127 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）]フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

正規表現の作成に使用されるメタ文字

次の表で、[Add Regular Expression]/[Edit Regular Expression] ダイアログボックス（ 正規表現の追加/編集 （1126 ページ）を参照）で正規表現の構築に使用できるメタ文字について説明します。

正規表現を作成するときは、次のことに注意してください。

- テキスト文字列に、文字どおりに使用するメタ文字を入力する場合は、それらの文字の前にバックスラッシュ（\）エスケープ文字を追加します。例：「example\.com」。
- 大文字、小文字ともに一致させる場合は、大文字と小文字の両方でテキストを入力します。たとえば、「cats」は「[cC][aA][tT][sS]」と入力します。

表 *259* : 正規表現の作成に使用されるメタ文字

文字	説明	注記
.	ドット	任意の単一文字と一致します。たとえば、d.g は dog、dag、dtg、doggonnit など、これらの文字が含まれているすべての単語と一致します。
(exp)	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、d(o|a)g は dog および dag と一致しますが、do や ag とは一致しません。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、ab(xy){3}z は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、dog|cat は dog または cat と一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、lo?se は lse または lose と一致します。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、lo*se は lse、lose、loose などと一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、lo+se は lose および loose と一致しますが、lse とは一致しません。
{x}	繰り返し限定作用素	厳密に x 回繰り返します。たとえば、ab(xy){3}z は、abxyxyxyz に一致します。
	最小繰り返し限定作用素	少なくとも x 回繰り返します。たとえば、ab(xy){2,}z は abxyxyz、abxyxyxyz などと一致します。
[abc]	文字クラス	カッコ内の任意の文字と一致します。たとえば、[abc] は a、b、または c と一致します。
[^abc]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、[^abc] は、a、b、c 以外の任意の文字に一致します。[^A-Z] は、大文字以外の任意の 1 文字に一致します。

文字	説明	注記
[a-c]	文字範囲クラス	範囲内の任意の文字と一致します。[a-z] は、任意の小文字と一致します。文字と範囲を混合できます。[abcq-z] は、a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、[a-cq-z] も同じです。 ダッシュ（-）文字は、角カッコ内の最後または最初の文字である場合にだけリテラルになります（[abc-] または [-abc]）。
“”	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、「test」 は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、\[は左の角カッコと一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\xNN	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

IOS デバイスのインスペクション ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX、FWSM、および IPS の機能をサポートしていますが、拡張機能はサポートしていません。

インスペクション ルールを設定する場合は、インスペクション設定も設定して、IOS デバイスの一部のグローバル インスペクション パラメータのデフォルト設定を変更できます。ほとんどのインスペクション設定は、Denial of Service（DoS; サービス拒絶）攻撃の防止または軽減に関連します。これらのほとんどのオプションのデフォルト設定は、ほとんどのネットワークに適しているため、1 つ以上の設定を調整する必要がある場合にだけこのポリシーを設定しま

す。設定を変更しない場合は、デバイスに設定されません（デフォルトが設定されたままになります）。

[Inspection settings] ページを開くには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [設定（Settings）] > [インスペクション（Inspection）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [インスペクション（Inspection）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [インスペクション（Inspection）]** を選択します。

次の表で、使用可能なインスペクション設定について説明します。

表 *260 : [Inspection]* ページ

要素	説明
Global Timeout Values	
TCP Establish Timeout (seconds)	セッションをドロップする前に、TCP セッションが設定された状態に到達するのを待機する時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 30 です。
FIN Wait Time (seconds)	ファイアウォールが FIN 交換を検出したあと、TCP セッション状態情報を保持する時間の長さ。1 ～ 2147483 の秒単位です。TCP セッションを閉じる準備が整うと、FIN 交換が発生します。デフォルトは 5 です。
TCP Idle Time (seconds)	セッションでアクティビティがない間、TCP セッションを維持する時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 3600（1 時間）です。

要素	説明
UDP Idle Time (seconds)	セッションでアクティビティがない間、UDP セッションを維持する時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 30 です。 ソフトウェアは、有効な UDP パケットを検出すると、新しい UDP セッションの状態情報を確立します。UDP はコネクションレス型サービスであるため、実際のセッションは存在しません。したがって、ソフトウェアは、パケット内の情報を調べることでセッションを見積もり、そのパケットが他の UDP パケットと似ているかどうか（類似の送信元アドレスまたは宛先アドレスを持っているなど）、および別の類似 UDP パケットの直後にそのパケットが検出されたかどうかを判断します。 ソフトウェアが、UDP アイドル タイムアウトで定義されている期間中に UDP セッションの UDP パケットを検出しなかった場合、ソフトウェアは、そのセッションの状態情報の管理を継続しません。
DNS Timeout (seconds)	アクティビティがない間、DNS lookup セッションが管理される時間の長さ。1 ～ 2147483 の秒単位です。デフォルトは 5 です。
SYN Flooding DoS Attack Thresholds	
Maximum 1 Minute Connection Rate - low Maximum 1 Minute Connection Rate - high	新しい未確立セッションの数。これにより、システムは、ハーフオープン状態のセッションの削除を開始および停止します。[Low] フィールドには、[High] フィールドに入力した数値よりも小さい数値を必ず入力してください。使用できる値は 1 分あたり 1 ～ 2147483647 です。low のデフォルトは 400 で、high のデフォルトは 500 です。
Maximum Incomplete Sessions Stop Threshold Maximum Incomplete Sessions Start Threshold	既存のハーフオープン セッションの数。これにより、ソフトウェアは、ハーフオープン状態のセッションの削除を開始および停止します。[stop] フィールドには、[start] フィールドに入力した数値よりも小さい数値を必ず入力してください。使用できる値は 1 ～ 2147483647 です。low のデフォルトは 400 で、high のデフォルトは 500 です。
Thresholds per Host	
Max Sessions Per Host	ソフトウェアがホストへのハーフオープン セッションの削除を開始する前に同時に存在できる、同じホスト宛先アドレスを持つハーフオープン TCP セッションの数。使用できる値は 1 ～ 4294967295 です。デフォルトは 50 です。 ハーフオープン セッションの数が多い場合は、ホストに対する DoS 攻撃があることを示している可能性があります。

要素	説明
Max Sessions Blocking Interval (min)	ホストごとの最大セッション数のしきい値に達した場合に、TCP ホスト固有の Denial-of-Service（DoS; サービス拒絶）攻撃の可能性を軽減するために適用するブロック時間。使用できる値は 0 ～ 35791 分です。デフォルトは 0 です。 • ブロック時間値が 0 の場合、ソフトウェアは、最大セッション制限を超えるホストへの新規接続要求のたびに、ホストの最も古い既存のハーフオープン セッションを削除する。これにより、ホストに対するハーフオープン セッション数がしきい値を超えないことが保証されます。 • ブロック時間値が 0 よりも大きい場合、ソフトウェアはホストのすべての既存のハーフオープン セッションを削除し、ホストに対するすべての新規接続要求をブロックする。ソフトウェアは、ブロック時間が経過するまですべての新規接続要求のブロックを継続します。
その他	
Session Hash Table Size (buckets)	バケットの観点で見たハッシュ テーブルのサイズ。ハッシュ テーブルに使用できる値は、1024、2048、4096、および 8192 です。デフォルトは 1024 です。 デバイスを介して実行されているセッションの合計数が現在のハッシュ サイズのほぼ 2 倍の場合は、ハッシュ テーブル サイズを大きくする必要があります。セッションの合計数が現在のハッシュ サイズの約半分に減った場合は、ハッシュ テーブル サイズを小さくします。基本的には、セッション数とハッシュ テーブルのサイズ間の比率を 1:1 に維持するようにしてください。
Enable Alert Messages	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail Messages	監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。
Permit DHCP Passthrough (Transparent Firewall)	DHCP パケットをブリッジ経由でインスペクションなしで転送することをトランスペアレント ファイアウォールに許可するかどうか。 DHCP パススルーを許可すると、DHCP パケットの ACL がオーバーライドされるため、ACL がすべての IP パケットを拒否するように設定されている場合でも、DHCP パケットが転送されます。このため、ブリッジの一方の側のクライアントは、ブリッジの反対側の DHCP サーバから IP アドレスを取得できます。

要素	説明
Block Non-SYN Packets	確立されたセッションに属さない TCP パケットをドロップするかどうか。これらは、セッションを開始しない TCP パケットです。つまり、これらのパケットでは SYN ビットが設定されていません。
Log Dropped Packets	ドロップしたパケットのログ メッセージを作成して、ドロップの理由を指定するかどうか。

関連項目

- インスペクション ルールについて （977 ページ）
- インスペクション ルールの設定 （983 ページ）
- IOS デバイスでの Denial of Service（DoS; サービス拒絶）攻撃を防ぐためのインスペクションの使用 （982 ページ）

第 18 章

ファイアウォール Web フィルタ ルールの管理

Web フィルタ ルール ポリシーでは、要求された URL またはトラフィックのアプレット コンテンツに基づいて Web トラフィックを許可または阻止するポリシーを定義します。ASA、PIX、および FWSM デバイスの場合は、FTP および HTTPS トラフィックもフィルタリングできます。

Web フィルタ ルールを設定する方法は、Cisco IOS ソフトウェアではなく、デバイスが ASA、PIX、または FWSM ソフトウェアを使用するかどうかによって異なります。

Web フィルタ ルールの使用方法については、次の項を参照してください。

- Web フィルタ ルールについて （1135 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （1136 ページ）
- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）
- Web フィルタ サーバの設定 （1155 ページ）

Web フィルタ ルールについて

Web フィルタ ルール ポリシーでは、要求された URL またはトラフィックのアプレット コンテンツに基づいて Web トラフィックを許可または阻止するポリシーを定義します。ASA、PIX、および FWSM デバイスの場合は、FTP および HTTPS トラフィックもフィルタリングできます。

Web または URL フィルタリングを使用すると、ユーザがアクセスできる Web サイトおよび Web コンテンツを制御できます。たとえば、ある種のコンテンツは、組織のメンバーの作業環境に悪影響を及ぼすと考えられます（ポルノを提供する Web サイトなど）。安全ではないと見なされる Web サイトや、アプリケーションがウイルスの感染源となるおそれのある Web サイトもあります。Web フィルタ ルールを使用すると、これらの好ましくないサイトまたは安全ではないサイトへのアクセスをブロックできます。

Web 要求をフィルタリングするには、Websense または SmartFilter（N2H2）のいずれかの外部 Web フィルタリング サーバをインストールする必要があります。ASA、PIX、および FWSM デバイスの場合は、URL、FTP、または HTTPS のフィルタリングにこれらの外部サーバが必

要です。IOS デバイスの場合は、これらのサーバーを使用することもできますが、さらに許可リスト（常に許可）URL またはブロックリスト（常に拒否）URL のリストをローカルに作成できます。フィルタリング サーバは、Web フィルタ設定ポリシーで設定します。Web フィルタ サーバの設定 （1155 ページ）を参照してください。

ヒント IOS デバイスの場合は、Web フィルタ ルールの代わりに、ゾーンベースのファイアウォール ルールを使用して Web フィルタリングを設定できます。このルールを使用すると、さらに Trend Micro Web フィルタリング サーバの使用を選択できます。詳細については、ゾーンベースのファイアウォール ルールの管理 （1195 ページ）を参照してください。

URL に基づいて要求をフィルタリングする以外に、アプレットのフィルタリングを実行して ActiveX または Java アプレットを除去できます。サイトを信頼していればダウンロードを許可しますが、十分に信頼していない場合はこのフィルタリングを実行し、アプレット ダウンロードを阻止できます。特定のサイトからのアプレットはブロックし、信頼できるサイトのアプレットは許可するようにルールを設定できます。

Web フィルタ ルールを設定するポリシーおよび手順は、デバイス タイプによって異なります。詳細については、次のトピックを参照してください。

- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （1136 ページ）
- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）

ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ASA、PIX、および FWSM デバイスの Web フィルタ ルール ポリシーでは、HTTP、FTP、および HTTPS のトラフィックを処理する方法を定義します。ActiveX および Java アプレットをフィルタリングすることもできます。Web フィルタ ルールは、Web 要求に含まれる Universal Resource Locator（URL）アドレスに基づいてトラフィックを許可または拒否します。アクセス ルールで HTTP トラフィックを許可した場合、トラフィックが好ましくない Web サイトまたは FTP サイトに向けられた場合に、あとからそのトラフィックを拒否（またはドロップ）したり、信頼できない送信元からの ActiveX または Java アプレットを除去できます。

ASA、PIX、および FWSM デバイスに Web フィルタリング ルールを設定するには、次の手順を実行します。

1. フィルタリングを適用するトラフィック、およびフィルタリング ルールを免除するトラフィックを識別するルールを設定します（手順については次を参照してください）。

2. URL フィルタリング サーバを識別する Web フィルタ設定およびその他の設定を行います。詳細については、 Web フィルタ サーバの設定 （1155 ページ）を参照してください。

関連項目

- Web フィルタ ルールについて （1135 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）

ステップ 1 次のいずれかを実行して、[Webフィルタルール（Web Filter Rules）]ページ（ASA/PIX/FWSM） （1138 ページ）を開きます。

- デバイスビュー：ポリシーセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。
- ポリシービュー：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（PIX/FWSM/ASA）（Web Filter Rules (PIX/FWSM/ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。 [Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス （1141 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集 （767 ページ）を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、 [Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス （1141 ページ）を参照してください。

- [Filtering] および [Type]：フィルタリングするトラフィックを識別するルール（[Filter]）を作成するか、既存のフィルタ ルールを免除するトラフィックを識別するルール（[Filter Except]）を作成するかどうか、および実行されるフィルタリングのタイプ。
  - URL：Web アドレスに基づいてトラフィックをフィルタ処理します。

- [HTTPS]：セキュアなサイトへの Web トラフィックをフィルタリングします。SSL VPN トラフィックは含まれません。
- [FTP]：FTP トラフィックをフィルタリングします。
- [ActiveX] または [Java]：ActiveX または Java アプレットを削除します。これらのオプションにより、アプレット タグまたはオブジェクト タグ内のすべてのエンティティが削除されます。したがって、削除できるのが ActiveX または Java アプレットだけに留まらない場合があります。

- 送信元アドレスおよび宛先アドレス：トラフィックを生成したアドレスやトラフィックの宛先にかかわらず、ルールを適用する場合は、送信元または宛先に「any」を使用します。ルールがホストまたはネットワークに固有の場合は、アドレスまたはネットワーク/ホスト オブジェクトを入力します。受け入れられるアドレス形式の詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。
- [Service]：モニタが必要なポートを主に定義します。いくつかのタイプの TCP サービスを指定する必要があります。通常は、事前定義されたサービスの HTTP、HTTPS、または FTP を使用しますが、これは実行するフィルタリングのタイプに合わせる必要があります。ただし、フィルタリング対象のトラフィックが含まれる可能性のある、ネットワークの任意の TCP ポートを指定できます。
- [Options]：追加するオプション（ある場合）。該当する主なオプションは、フィルタリング サーバが利用不能な場合にトラフィックを許可するかどうか、および長い URL またはパラメータが含まれる URL を切り捨てるかどうかです。URL をドロップする場合、一般には 1 つのパラメータ値が原因ではないため、通常はパラメータが含まれる URL は切り捨てることを推奨します。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。ただし、フィルタ例外ルールがフィルタ ルールの前後のいずれにあっても、常に関連するフィルタ ルールの例外が作成されるため、Web フィルタリング ルールの順序は重要ではありません。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。

[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

Web または URL フィルタリング ルールを設定するには、ASA、PIX、および FWSM デバイスの [Web Filter Rules] ページを使用します。Web フィルタリングは、HTTP インスペクションの一種です。アクセス ルールで HTTP トラフィックを許可している場合は、ルールを設定してサーバベースの Web フィルタリングを適用すると、望ましくない Web サーバへのユーザ アクセスを防止できます。

Web フィルタルールを設定する場合は、[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）] ポリシーで Web フィルタ設定も設定します。これらの設定は、Web フィルタリング サーバを識別し、ポリシーの機能全体を制御するその他の設定を含みます。Web フィルタリング サーバを設定して、展開する URL、FTP、または HTTPS のフィルタルールを指定する必要があります。詳細については、Web Filter 設定ページ （1156 ページ）を参照してください。

ヒント　重複するルールは作成できません。たとえば、送信元、宛先、およびサービスが同じか、重複する 2 つのルールを作成しても、それらのルールは展開できません。また、すべての filter-except ルールは、免除を作成するフィルタ ルールの下に配置する必要があります。

ナビゲーション パス

ASA、PIX、および FWSM デバイスの [Web Filter Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ASA、PIX、または FWSM デバイスを選択し、ポリシーセレクタから [ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）] を選択します。
- （ポリシービュー）：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（PIX/FWSM/ASA）（Web Filter Rules (PIX/FWSM/ASA)）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （

  マップビュー）ASA、PIX、または FWSM デバイスを右クリックし、**[ファイアウォール ポリシーの編集（Edit Firewall Policies）] > [Webフィルタルール（Web Filter Rules）]** を選択します。

関連項目

- Web フィルタ ルールについて （1135 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （1136 ページ）
- Web フィルタ サーバの設定 （1155 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）
- セクションを使用したルール テーブルの編成 （783 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *261 : [Web Filter Rules]* ページ（*ASA*、*PIX*、*FWSM*）

要素	説明
番号	順序が付けられたルール番号。
送信元 接続先	ルールの送信元アドレスおよび宛先アドレス。「any」アドレスを指定すると、ルールは特定のホスト、ネットワーク、またはインターフェイスに制限されません。これらのアドレスは、ホストまたはネットワーク、ネットワーク/ホスト オブジェクト、インターフェイス、またはインターフェイス ロールの IP アドレスです。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。ネットワーク/ホストオブジェクトについて （391 ページ）を参照してください。
サービス	ルールが適用されるトラフィックのプロトコルおよびポートを指定するサービスまたはサービス オブジェクト。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。 サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
タイプ（Type）	ルールに対するフィルタリング処置のタイプであり、識別されたトラフィックをフィルタリングするか、または識別されたトラフィックをフィルタリングから除外（Filter Except）するかのいずれか。詳細な説明については、 [Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス （1145 ページ）を参照してください。
オプション	選択したプロトコルの追加設定オプション（ある場合）。詳細については、 [Edit Web Filter Options] ダイアログボックス （1147 ページ）を参照してください。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用（304 ページ）を参照してください。
説明	ルールの説明（ある場合）。
最後のチケット	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。

要素	説明
クエリ	ポリシークエリを実行するには、このボタンをクリックします。実行すると、ルールを評価して、効果のないルールを特定できます。ポリシークエリー レポートの生成 （793 ページ）を参照してください
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内のさまざまなタイプの項目を検索し、必要に応じてその項目を置換するには、このボタンをクリックします。 ルール テーブルの項目の検索と置換 （777 ページ）を参照してください。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。
[Add Row] ボタン	[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス （1141 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除 （766 ページ）を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集 （767 ページ）を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

これらのタイプのデバイスに Web フィルタリング ルールを設定するには、[Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule] ダイアログボックスを使用します。

ナビゲーション パス

[Webフィルタルール（Web Filter Rules）]ページ（ASA/PIX/FWSM） （1138 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （1136 ページ）

- Web フィルタ ルールについて （1135 ページ）
- Web フィルタ サーバの設定 （1155 ページ）

フィールド リファレンス

表 *262 : [Add PIX/ASA/FWSM Web Filter Rule]/[Edit PIX/ASA/FWSM Web Filter Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。
フィルタリング	定義するルールのタイプを次に示します。 • [Filter]：このルールは、送信元と宛先間の識別されたトラフィックのタイプをフィルタリングします。 • [Filter Except]：このルールによって、フィルタ ルールの免除を作成します。送信元と宛先間の識別されたトラフィックはフィルタリングされません。

要素	説明
タイプ（Type）	このルールでフィルタリングする（またはフィルタリングを免除する）トラフィックのタイプ。外部サーバを使用するフィルタリングの場合は、ご使用のサーバ バージョンのマニュアルを参照して、このタイプのフィルタリングがサポートされているかどうかを確認してください。 Web Filter 設定ページ （1156 ページ）でフィルタリング サーバを設定します。 • [URL]：HTTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [HTTPS]：HTTPS トラフィック。SSL VPN に関連付けられているトラフィックは含まれていません。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [Java]：Java アプレットがアプレット タグで識別された場合に、HTTP トラフィックから Java アプレットを削除します。このルールでは、Java アプレットを SSL VPN トラフィックから削除しません。アプレット タグが複数のパケットに及ぶ場合、またはタグ内のコードが MTU よりも大きい場合、Java アプレットは削除されません。 • [ActiveX]：ActiveX または Java アプレットを HTTP トラフィックから削除します。このルールによって、オブジェクトまたはアプレット タグ内のすべての項目が削除され、これにより、イメージおよびマルチメディア オブジェクトも削除される場合があります。このルールでは、SSL VPN トラフィックからアプレットを削除しません。オブジェクト タグが複数のパケットに及ぶ場合、またはタグ内のコードが MTU よりも大きい場合、オブジェクトは削除されません。 • [FTP]：FTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。

要素	説明
ソース 宛先	トラフィックの送信元または宛先。項目をカンマで区切って複数の値を入力できます。 次のアドレス タイプを自由に組み合わせて入力し、トラフィックの送信元または宛先を定義できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 • ネットワーク/ホスト オブジェクト。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。 • ホスト IP アドレス（10.10.10.100 など）。 • ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。 • IP アドレスの範囲（10.10.10.100-10.10.10.200 など）。 • 10.10.0.10/255.255.0.255 形式の IP アドレスのパターン。この場合のマスクは不連続なビット マスクです（連続および不連続ネットワーク マスク（IPv4 アドレスに対応） （393 ページ）を参照）。
サービス	動作対象のトラフィックのポート番号を定義するサービス。項目をカンマで区切って複数の値を入力できます。 サービスは TCP を使用する必要があります。仕様で、フィルタリングするポートを定義します（サービス名に意味はありません）。たとえば、ポート 80 をフィルタリングする場合は、HTTP サービス オブジェクトを使用します。ネットワーク上の HTTP トラフィックが別のポートを使用する場合は、TCP/ポート番号（たとえば、TCP/8080）を指定します。TCP を単独で入力して、すべてのポートをフィルタリングできます。 サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）を入力できます。サービスを入力する場合は、有効な値の入力を求められます。リストから値を選択して、Enter または Tab を押します。 サービスを指定する方法の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
Allow traffic if URL Filter Server unavailable （URL、FTP、HTTPS のみ）	すべての URL フィルタリング サーバが使用できない場合に、アウトバウンド接続でのフィルタリングされていないトラフィックを許可するかどうか。このオプションを選択しなかった場合は、影響を受けるすべての発信トラフィック（HTTP、FTP、または HTTPS）は、少なくとも 1 台のフィルタリング サーバが使用できるようになるまで、ブロックされます。

要素	説明
Block connection to HTTP Proxy Server （URL のみ）	ユーザによる HTTP プロキシ サーバへの接続を阻止するかどうか。
Truncate CGI request by removing CGI parameters （URL のみ）	URL に疑問符（?）で始まるパラメータ リスト（CGI スクリプトなど）が含まれている場合に、フィルタリング サーバに送信される URL に対して、その URL に含まれる疑問符と疑問符のあとのすべての文字を削除する切り捨てを行うかどうか。
Block outbound requests if absolute FTP path is not provided （FTP のみ）	ユーザがディレクトリを変更しようとしたときに、ディレクトリ全体のパスを提供しない対話型 FTP セッションを阻止するかどうか。
Long URL （URL のみ）	フィルタリング サーバで許可されている最大数（Websense の場合は 4 KB、Smartfilter [N2H2] の場合は 3 KB）よりも大きい URL を処理する方法。多くの場合、長い URL はパラメータリストが原因であり、[CGIパラメータを削除することでCGI要求を切り捨てる（Truncate CGI request by removing CGI parameters）] オプションを使用して、それらの URL を処理できます。これ以外の長い URL の場合は、次のオプションから選択します。 • [Drop]：長い URL 要求をドロップします。 • [Truncate]：URL 要求を、URL のホスト名または IP アドレス部分だけに切り捨てます。 • [Deny]：URL 要求を拒否します。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。

[Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス

ASA、PIX、および FWSM デバイスの Web フィルタ ルールによって実行されるフィルタリングのタイプを編集するには、[Edit Web Filter Type] ダイアログボックスを使用します。

ナビゲーション パス

（[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （1138 ページ） 上で）ASA/PIX/FWSM の Web フィルタルールの [タイプ（Type）] セルを右クリックし、[Webフィル

タタイプの編集（Edit Web Filter Type）] を選択します。一度に 1 つの行のタイプを編集できます。

フィールド リファレンス

表 *263 : [Webフィルタタイプの編集（Edit Web Filter Type）] ダイアログボックス*

要素	説明
フィルタリング	定義するルールのタイプを次に示します。 • [フィルタ（Filter）]：このルールは、送信元と宛先間の識別されたトラフィックのタイプをフィルタ処理します。 • [Filter Except]：このルールによって、フィルタ ルールの免除を作成します。送信元と宛先間の識別されたトラフィックはフィルタリングされません。
タイプ（Type）	このルールでフィルタリングする（またはフィルタリングを免除する）トラフィックのタイプ。外部サーバを使用するフィルタリングの場合は、ご使用のサーバ バージョンのマニュアルを参照して、このタイプのフィルタリングがサポートされているかどうかを確認してください。Web Filter 設定ページ （1156 ページ） でフィルタリング サーバを設定します。 • [URL]：HTTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [HTTPS]：HTTPS トラフィック。SSL VPN に関連付けられているトラフィックは含まれていません。フィルタリングは、外部フィルタリング サーバを使用して行われます。 • [Java]：Java アプレットがアプレット タグで識別された場合に、HTTP トラフィックから Java アプレットを削除します。このルールでは、Java アプレットを SSL VPN トラフィックから削除しません。アプレット タグが複数のパケットに及ぶ場合、またはタグ内のコードが MTU よりも大きい場合、Java アプレットは削除されません。 • [ActiveX]：ActiveX または Java アプレットを HTTP トラフィックから削除します。このルールによって、オブジェクトまたはアプレット タグ内のすべての項目が削除され、これにより、イメージおよびマルチメディア オブジェクトも削除される場合があります。このルールでは、SSL VPN トラフィックからアプレットを削除しません。オブジェクト タグが複数のパケットに及ぶ場合、またはタグ内のコードが MTU よりも大きい場合、オブジェクトは削除されません。 • [FTP]：FTP トラフィック。フィルタリングは、外部フィルタリング サーバを使用して行われます。

[Edit Web Filter Options] ダイアログボックス

ASA、PIX、および FWSM デバイスの Web フィルタ ルールに定義されたフィルタリング オプションを編集するには、[Edit Web Filter Options] ダイアログボックスを使用します。

このダイアログボックスに表示されるオプションは、ルールに設定されたフィルタリングのタイプによって異なります。一部のタイプにはオプションがなく、ダイアログボックスは空になります。以下の参照テーブルには、選択可能なすべてのオプションが含まれています。

ナビゲーション パス

（[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （1138 ページ）上で）ASA/PIX/FWSM の Web フィルタルールの [オプション（Options）] セルを右クリックし、[Web フィルタタイプの編集（Edit Web Filter Type）] を選択します。一度に 1 つの行のタイプを編集できます。

フィールド リファレンス

表 264 : [Edit Web Filter Options] ダイアログボックス

要素	説明
Allow traffic if URL Filter Server unavailable （URL、FTP、HTTPS のみ）	すべての URL フィルタリング サーバが使用できない場合に、アウトバウンド接続でのフィルタリングされていないトラフィックを許可するかどうか。このオプションを選択しなかった場合は、影響を受けるすべての発信トラフィック（HTTP、FTP、または HTTPS）は、少なくとも 1 台のフィルタリング サーバが使用できるようになるまで、ブロックされます。
HTTPプロキシサーバーへの接続をブロックする（Block connection to HTTP Proxy Server） （URL のみ）	ユーザによる HTTP プロキシ サーバへの接続を阻止するかどうか。
Truncate CGI request by removing CGI parameters （URL のみ）	URL に疑問符（?）で始まるパラメータ リスト（CGI スクリプトなど）が含まれている場合に、フィルタリング サーバに送信される URL に対して、その URL に含まれる疑問符と疑問符のあとのすべての文字を削除する切り捨てを行うかどうか。
絶対FTPパスが指定されていない場合にアウトバウンドリクエストをブロックする（Block outbound requests if absolute FTP path is not provided） （FTP のみ）	ユーザがディレクトリを変更しようとしたときに、ディレクトリ全体のパスを提供しない対話型 FTP セッションを阻止するかどうか。

要素	説明
長いURL（Long URL） （URL のみ）	フィルタリング サーバで許可されている最大数（Websense の場合は 4 KB、Smartfilter [N2H2] の場合は 3 KB）よりも大きいURL を処理する方法。多くの場合、URL が長い原因はパラメータリストにあり、[CGIパラメータを削除することでCGI要求を切り詰める（Truncate CGI request by removing CGI parameters）] オプションを使用して、長い URL を処理できます。これ以外の長い URL の場合は、次のオプションから選択します。 • [Drop]：長い URL 要求をドロップします。 • [Truncate]：URL 要求を、URL のホスト名または IP アドレス部分だけに切り捨てます。 • [Deny]：URL 要求を拒否します。

IOS デバイス用の Web フィルタルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS デバイスの Web フィルタ ルール ポリシーでは、HTTP トラフィックを処理する方法を定義します。Web フィルタ ルールは、Web 要求に含まれる Universal Resource Locator（URL）アドレスに基づいてトラフィックを許可または拒否するインスペクション ルールのタイプです。アクセス ルールでインターフェイスの HTTP トラフィックを許可した場合、トラフィックが好ましくない Web サイトに向けられた場合に、あとからそのトラフィックを拒否（またはドロップ）できます。

IOS デバイスに Web フィルタリング ルールを設定するには、次の手順を実行します。

1. Web トラフィックをフィルタリングするインターフェイスを設定します（手順については次を参照してください）。
2. ローカル Web フィルタリング リストを設定して、常に許可または拒否する必要がある Web サイトを指定します（手順については、以下を参照してください）。
3. URL フィルタリング サーバを識別する Web フィルタ設定およびその他の設定を行います。詳細については、Web フィルタ サーバの設定 （1155 ページ）を参照してください。

ヒント　ゾーン ベースのファイアウォール ルールとして Web フィルタリングを設定することもできます。詳細については、ゾーンベースのファイアウォールルールの追加 （1210ページ）を参照してください。

関連項目

- Web フィルタ ルールについて （1135 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

ステップ 1　次のいずれかを実行して、[Web Filter Rules] ページ（IOS） （1150 ページ）を開きます。

- デバイスビュー：ポリシーセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。
- ポリシービュー：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（IOS）（Web Filter Rules (IOS)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2　HTTP トラフィックをフィルタリングするインターフェイスを設定します。フィルタリングをイネーブルにするインターフェイスごとに、次のようにルールを作成します。

a) [Webフィルタルール（Web Filter Rules）] タブがまだ選択されていない場合は選択し、次のいずれかを実行して [IOS Web Filter Rule and Applet Scanner] ダイアログボックス （1152 ページ）を開きます。

- 新しいルールを作成するには、作業領域内を右クリックし、[行の追加（Add Row）] を選択します。
- 既存のルールを編集するには、ルールを右クリックし、[行の編集（Edit Row）] を選択します。

b) このルールを適用するインターフェイスを指定します。インターフェイスの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェースロールをリストから選択します。次の設定も行います。

- インターフェイスに関するトラフィックの方向：通常、デバイスがパケットの処理により多くの時間を費やす前に、望ましくないトラフィックがドロップされるように、[イン（In）] を選択します。
- J

  ava アプレットスキャン：インターフェイスで Web フィルタリングを有効にすると、パフォーマンスに影響する可能性のある Java アプレットが検査されます。通常は、Java アプレット スキャンをイネーブルにし、許可された送信元と拒否された送信元を識別して、拒否されたアプレットをスキャンしないようにできます。インターフェイスで許可されるソースと拒否されるソースの両方を設定する場合は、インターフェイスに 2 つのルールを設定する必要があります。

c) [OK] をクリックして Web フィルタリングルールテーブルにルールを追加します。

ステップ 3 （オプション）ローカルフィルタリングリストを定義する排他的ドメインのリストを設定します。このリストは、Web 要求が外部の Web フィルタリング サーバに送信される前に適用されます（ Web Filter 設定ページ （1156 ページ）で定義）。常に許可（自社の Web サイトなど）または拒否する Web サイトがある場合は、ローカルリストにこれらのサイトを設定します。必要な数だけルールを設定し、すべてのリストを定義します。

a) [排他的ドメイン（Exclusive Domains）] タブをクリックし、次のいずれかを実行して [IOS Web Filter Exclusive Domain Name] ダイアログボックス （1154 ページ）を開きます。

- 新しいルールを作成するには、作業領域内を右クリックし、[行の追加（Add Row）] を選択します。
- 既存のルールを編集するには、ルールを右クリックし、[行の編集（Edit Row）] を選択します。

b) 指定したドメインを許可するか拒否するかどうかを選択して、ドメイン名またはホスト IP アドレスを入力します。完全ドメイン名（特定 Web サイトの名前）または部分的な名前（同様に扱うすべてのドメイン）のいずれかを入力できます。

c) [OK] をクリックして、排他的ドメインルールをポリシーに追加します。

[Web Filter Rules] ページ（IOS）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

Web または URL フィルタリング ルールを設定するには、IOS デバイスの [Web Filter Rules] ページを使用します。Web フィルタリングは、HTTP インスペクションの一種です。アクセス規則でインターフェイス上の HTTP トラフィックを許可している場合は、規則を設定してローカルおよびサーバーベースの Web フィルタリングを適用すると、望ましくない Web サーバーへのユーザアクセスを防止できます。

Web フィルタルールを設定する場合は、[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）] ポリシーで Web フィルタ設定も設定します。これらの設定は、Web フィルタリング サーバを識別し、ポリシーの機能全体を制御するその他の設定を含みます。たとえば、設定ポリシーを使用して、フィルタリングサーバーが使用できなくなった場合にすべての Web トラフィックを許可できます。詳細については、 Web Filter 設定ページ （1156 ページ）を参照してください。

ヒント ゾーン ベースのファイアウォール ルールとして Web フィルタリングを設定することもできます。詳細については、 [Zone-based Firewall Rules] ページ （1272 ページ）を参照してください。

ナビゲーション パス

IOS デバイスの [Webフィルタルール（Web Filter Rules）] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）IOS デバイスを選択して、ポリシーセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。
- （ポリシービュー）：ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [Webフィルタルール（Web Filter Rules）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）IOS デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [Webフィルタルール（Web Filter Rules）]** を選択します。

関連項目

- Web フィルタ ルールについて （1135 ページ）
- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）
- ファイアウォール Web フィルタ ルールの管理 （1135 ページ）

フィールド リファレンス

表 *265 : [Web Filter Rules]* ページ（*IOS*）

要素	説明
[Web Filter Rules] タブ	ポリシーに定義された URL フィルタリング ルール。各ルールには、そのルールを定義したインターフェイス、ルールが着信または発信トラフィックに適用されるかどうか、および Java アプレット スキャンがイネーブルの場合に許可または拒否される Java アプレットの送信元が表示されます。Java アプレット スキャンに許可と拒否の両方を設定した場合、インターフェイスに 2 つ以上のルールが存在する場合があります。 • ルールを追加するには、[Add Row] ボタンをクリックし、[IOS Web Filter Rule and Applet Scanner] ダイアログボックス （1152 ページ）に入力します。 • ルールを編集するには、ルールを選択し、[Edit Row] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[Delete Row] ボタンをクリックします。

要素	説明
[Exclusive Domains] タブ	ローカル Web フィルタ リスト。このリストは、Web 要求がフィルタリングサーバーに送信される前にチェックされ、Web フィルタリングを構成するすべてのインターフェイスに適用されます。 常に許可する特定のドメイン（組織の独自のドメイン名など）または禁止するドメインがあることがわかっている場合は、ここにリストすることができます。ローカルフィルタリストを構成すると、デバイスがフィルタリングサーバーからの応答を待つ必要がないため、パフォーマンスを向上させることができます。 • ドメインを追加するには、[Add Row] ボタンをクリックし、[IOS Web Filter Exclusive Domain Name] ダイアログボックス （1154 ページ）に入力します。 • ドメインを編集するには、ドメインを選択し、[Edit Row] ボタンをクリックします。 • ドメインを削除するには、そのドメインを選択して [Delete Row] ボタンをクリックします。

[IOS Web Filter Rule and Applet Scanner] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS デバイスに Web フィルタリング ルールを作成するには、[IOS Web Filter Rule and Applet Scanner] ダイアログボックスを使用します。

ナビゲーション パス

このダイアログボックスを開くには、の [Webフィルタルール（ Web Filter Rules）] タブを選択します。新しい [Web Filter Rules] ページ（IOS） （1150 ページ）ルールを作成するには [行の追加（Add Row）] をクリックし、既存のルールを編集するには行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）
- Web フィルタ ルールについて （1135 ページ）

フィールド リファレンス

表 *266 : [IOS Web Filter Rule and Applet Scanner]* ダイアログボックス

要素	説明
Enable Web Filtering	Web フィルタリング ルールをイネーブルにするかどうか。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイスロール。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
トラフィックの方向	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。
Java Applet Scanning Enable Java Applet Scanner	[Java アプレットスキャンを有効にする（Enable Java Applet Scanning）] を選択すると、デバイスは、Web サーバーから内部ホストへの HTTP トラフィックに Java アプレットが存在するかどうかをチェックします。Java アプレットが存在した場合、許可される送信元リストに Web サーバ（アプレット送信元）が含まれていれば、HTTP トラフィック内の Java アプレットは変更されません。存在しない場合、Java アプレットは HTTP ページから削除されます。 **ヒント** Web フィルタリングを有効にすると、パフォーマンスに影響する可能性のある Java アプレットが検査されます。Java アプレット スキャナをイネーブルにすると、許可または拒否される送信元のリストを識別し、これらのアプレットを検査しないようにできます。送信元を拒否しない場合でも、スキャンをイネーブルにして**すべての**送信元を許可します。

要素	説明
Permit Traffic Applet Sources	Java アプレットを許可または拒否される送信元アドレスのリスト。許可または拒否された送信元のリストを設定するには、以下の手順に従います。 • [指定した送信元から許可する（Permit from Specified Sources）] または [指定した送信元から拒否する（Deny from Specified Sources）] を選択します。許可リストと拒否リストの両方を作成する場合は、2 つの別個の Web フィルタルールを作成します。許可リストを設定しなかった場合は、すべての送信元が拒否されます。 • [アプレットの送信元（Applet Sources）] フィールドに、許可されるアドレスまたは拒否されるアドレスのリストを入力します。このリストには、ホスト IP アドレス、ネットワーク アドレス、アドレス範囲、またはネットワーク/ホストオブジェクトを含めることができますが、ドメイン名を含めることはできません。カンマで複数のアドレスを区切ります。アドレスを入力する方法の詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

[IOS Web Filter Exclusive Domain Name] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS デバイスにローカル Web フィルタリング ルールを作成するには、[IOS Web Filter Exclusive Domain Name] ダイアログボックスを使用します。許可または拒否されるドメイン名または IP アドレスのリストを作成できます。デバイスは、Web フィルタリング サーバに Web 要求を転送する前に、このリストをチェックします。

ローカル フィルタリングを使用すると、常に許可または常に拒否するとわかっている Web サイトをユーザが要求した場合に、サーバから応答を受け取るまでの待機時間を節約できます。

ナビゲーション パス

このダイアログボックスを開くには、[Web Filter Rules] ページ（IOS） （1150 ページ）の [排他的ドメイン（Exclusive Domains）] タブを選択します。新しいルールを作成するには [行の追加（Add Row）] をクリックし、既存のルールを編集するには行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）>
- Web フィルタ ルールについて （1135 ページ）

フィールド リファレンス

表 *267 : [IOS Web Filter Exclusive Domain Name]* ダイアログボックス

要素	説明
トラフィック	一覧表示された Web サイトへのアクセスを許可するか、または拒否するかどうか。
ドメイン名	許可または拒否する Web サイトのドメイン名またはホスト IP アドレス。複数のエントリを指定する場合は、カンマで区切ります。 ドメイン名の場合、完全な名前または部分的な名前を入力できます。たとえば、cisco.com には cisco.com ドメインのすべての Web サーバが含まれますが、www.cisco.com はワールドワイド ウェブ用の Web サーバだけを示します。

Web フィルタ サーバの設定

Web フィルタ ルール ポリシーとともに使用する Web フィルタ サーバの設定およびその他の設定を行うには、Web フィルタ設定ポリシーを使用します。Websense または Smartfilter（N2H2）のフィルタリング サーバを使用でき、（IOS デバイスの場合は）外部サーバを使用しないことも可能です。

ポリシーを設定および配置する前に、サーバのマニュアルで指示されているように Web フィルタ サーバをインストールおよび設定する必要があります。Security Manager は、サーバが存在すること、またはサーバが適切に設定されていることを確認できません。

ヒント これらの設定は、Web フィルタ ルール ポリシーでだけ機能します。ここで設定した Web サーバは、Web コンテンツ フィルタリングを設定するゾーンベースのファイアウォール ルール ポリシーでは使用されません。

関連項目

- Web フィルタ ルールについて （1135 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （1136 ページ）
- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）

ステップ 1 次のいずれかを実行して、 Web Filter 設定ページ （1156 ページ）を開きます。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [Web フィルタ（Web Filter）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから**[ファイアウォール（Firewall）]>[設定（Settings）]>[Webフィルタ（Web Filter）]**を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 使用する Web フィルタリングサーバーのタイプを [Web フィルタサーバーのタイプ（Web Filter Server Type）] フィールドで選択し、サーバーを Web フィルタリングサーバーのテーブルに追加します。複数のサーバーがある場合は、優先度順に追加します。リストの先頭のサーバーがプライマリサーバーです。

- サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Web Filter Server Configuration] ダイアログボックス （1160 ページ）に入力します。
- サーバを編集するには、サーバを選択し、[Edit Row] ボタンをクリックします。
- サーバを削除するには、サーバを選択し、[Delete Row] ボタンをクリックします。

ステップ 3 設定ポリシーの下半分には、設定可能なデバイス固有のオプションが含まれています。各設定の詳細については、Web Filter 設定ページ （1156 ページ）を参照してください。設定の概要は次のとおりです。

- IOS デバイス：最も重要な設定は [サーバーに到達できないときにトラフィックを許可する（Allow Traffic when Servers Unreachable）] です。この設定では、フィルタリングサーバーが利用不能な場合に Web 接続を許可するかどうかを指定します。このオプションを選択しないと、何らかの理由でサーバがオフラインになった場合にすべての Web トラフィックが削除されます。

残りの設定では、ロギングおよびキャッシュ サイズのオプションを設定します。

- ASA、PIX、FWSM デバイス：これらのオプションでは、フィルタリング サーバで使用されるキャッシュ サイズおよびバッファ制限を設定します。また、フィルタリングサーバーの設定に応じて、キャッシュされた応答に送信元と宛先の両方を含めるか（ユーザごとに異なるフィルタリングポリシーがある場合）、宛先のみを含めるか（すべてのユーザに対して 1 つのポリシー）を制御することもできます。

Web Filter 設定ページ

[Webフィルタ設定（Web Filter Settings）] ページを使用して、Web フィルタルールポリシーとともに使用する Web フィルタサーバーの設定およびその他の設定を行います。

ポリシーを設定および配置する前に、サーバのマニュアルで指示されているように Web フィルタ サーバをインストールおよび設定する必要があります。Security Manager は、サーバが存在すること、またはサーバが適切に設定されていることを確認できません。

ヒント これらの設定は、Web フィルタ ルール ポリシーでだけ機能します。ここで設定した Web サーバは、Web コンテンツ フィルタリングを設定するゾーンベースのファイアウォール ルール ポリシーでは使用されません。

ナビゲーション パス

[Web Filter settings] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [Webフィルタ（Web Filter）] を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [Webフィルタ（Web Filter）]** を選択します。

関連項目

- Web フィルタ ルールについて （1135 ページ）
- Web フィルタ サーバの設定 （1155 ページ）
- ASA、PIX、および FWSM デバイスの Web フィルタ ルールの設定 （1136 ページ）
- IOS デバイス用の Web フィルタルールの設定 （1148 ページ）

フィールド リファレンス

表 268 : [Web Filter] ページ

要素	説明
Web Filter Server Type	使用する Web フィルタ サーバのタイプ。 • [None]：Web フィルタ サーバを使用しません。 • [Websense]：Websense サーバを使用します。 • [Secure Computing SmartFilter/N2H2]：Smartfilter サーバを使用します。このオプションを選択した場合は、通信に使用するサーバーポートを [ポート（Port）] フィールドで指定できます。 **ヒント** この設定を変更した場合は、既存のサーバリストをテーブルから削除するように要求されます。[はい（Yes）] をクリックしても、テーブルはクリアされません。このプロンプトは、リストに間違ったタイプのサーバーが含まれている可能性があることを通知するために表示されます。

要素	説明
Webフィルタサーバーテーブル（Web Filter Servers table）	デバイスが Web フィルタリングに使用するサーバ。サーバはプライオリティ順に入力します。デバイスは、リストの先頭にあるサーバを使用し、そのサーバが応答しなくなると、応答を受け取るようになるまでリストの次のサーバに移行します。 フィルタタイプで [なし（None）] を選択すると、このリストは無視されます。 • サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Web Filter Server Configuration] ダイアログボックス（1160 ページ）に入力します。 • サーバーを編集するには、サーバーを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • サーバーを削除するには、サーバーを選択し、[行の削除（Delete Row）] ボタンをクリックします。
IOS 固有の設定	
サーバーに到達できないときにトラフィックを許可する（Allow Traffic when Servers Unreachable）	Web フィルタ サーバから応答がない場合に、デバイスが Web トラフィックを許可するかどうか。このオプションを選択しない場合は、サーバがオンラインに戻るまで、すべての Web アクセスが抑制されます。 サーバがダウンしているときの Web トラフィックを許可した場合、Web 要求はフィルタリングされず、すべての Web サーバへのアクセスが許可されます。
アラートの有効化（Enable Alerts）	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail	監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。
Enable Web Filter Server Logging	システム メッセージを URL フィルタリング サーバに送信してロギングするかどうか。デバイスは、URL ルックアップ要求の直後にログ要求を送信します。ログ要求には、URL、ホスト名、送信元 IP アドレス、および宛先 IP アドレスが含まれます。サーバーはログ要求を独自のログサーバーに記録するため、必要に応じてこの情報を表示できます。
キャッシュ サイズ（Cache Size）	デバイスでキャッシュ可能な宛先 IP アドレス（およびその認可ステータス）の最大数。デフォルト値は 5000 です。 キャッシュが 80 % まで一杯になると、デバイスは非アクティブなエントリを古い方から順に削除します。

要素	説明
Maximum Requests	ある特定の時点で存在する未処理要求の最大数。指定した数を超えた場合、新しい要求はドロップされます。デフォルトは 1000 です。
パケットバッファ	Web フィルタサーバーが要求を許可または拒否するのを待機している間に、デバイスのパケットバッファに格納できる HTTP 応答の最大数。最大値に達した場合、デバイスは応答をドロップします。デフォルト（最大値）は 200 です。 ユーザが Web 要求を行うと、同時にデバイスが要求を Web サイトおよび Web フィルタリング サーバに送信します。サーバーが許可または拒否の応答を提供する前に Web サイトからの応答を受信した場合、デバイスはサーバーから応答を受け取るまで、要求をパケットバッファに保持します。 サーバーが応答した場合、またはサーバーを利用できないとデバイスが判断し、[サーバーに到達できないときにトラフィックを許可する（Allow Traffic when Servers Unreachable）] も選択している場合、応答はバッファから削除されます。
PIX/ASA/FWSM 固有の設定	
Cache Match Criteria	Web 要求をキャッシュする方法。 • [Source] と [Destination]：キャッシュ エントリは、要求を開始するアドレスと宛先 Web アドレスの両方に基づいています。ユーザがフィルタリング サーバ上の同じフィルタリング ポリシーを共有しない場合は、このモードを選択します。 • [Destination]：キャッシュ エントリは、宛先 Web アドレスが基になります。すべてのユーザがフィルタリング サーバ上の同じフィルタリング ポリシーを共有する場合は、このモードを選択します。
URL Buffer Memory （ASA 7.2+、PIX 7.2+ のみ）	URL バッファ メモリ プールのサイズ（KB 単位）。値は 2 ～ 10240 です。
Maximum Allowed URL Size （ASA 7.2+、PIX 7.2+ のみ）	バッファ対象の URL ごとに許容される URL の最大サイズ（KB 単位）。使用できる値はサーバ タイプによって異なります。 • [Websense]：2 ～ 4 • [Smartfilter (N2H2)]：2 または 3

要素	説明
キャッシュ サイズ（Cache Size）	フィルタリングサーバーからの応答を格納するためのキャッシュのサイズ（KB 単位）。値は 1 ～ 128 です。 キャッシングにより、URL アクセス権限がセキュリティアプライアンス上のメモリに保存されます。ホストが接続を要求すると、セキュリティ アプライアンスは Websense サーバに要求を転送する代わりに、まず URL キャッシュを検索して一致するアクセス権限の有無を調べます。
URLブロックバッファの制限（URL Block Buffer Limit）	フィルタリング サーバのフィルタリング判定を待機している間、Web サーバ応答を格納しておくバッファのサイズ。値は 1 ～ 128 です。この値は、1550 バイトのブロックの数を示しています。

[Web Filter Server Configuration] ダイアログボックス

Web フィルタ ルール ポリシーとともに使用する外部 Web フィルタ サーバを設定するには、[Web Filter Server Configuration] ダイアログボックスを使用します。Websense サーバまたは Smartfilter（N2H2）サーバを設定できます。

ナビゲーション パス

Web Filter 設定ページ （1156 ページ）から、[Web フィルタサーバー（Web Filter Servers）] テーブルの下にある [行の追加（Add Row）] をクリックするか、行を選択して [行の編集（Edit Row）] をクリックします。

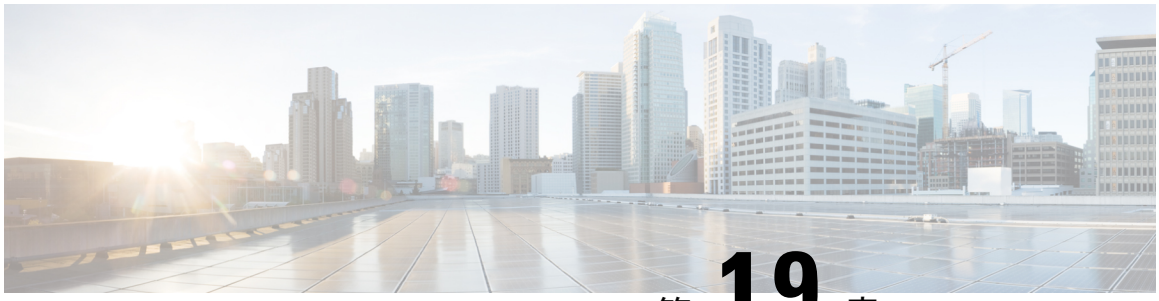
関連項目

- Web フィルタ サーバの設定 （1155 ページ）
- Web フィルタ ルールについて （1135 ページ）

表 269 : [Web Filter Server Configuration] ダイアログボックス

要素	説明
コモン接点	
IPアドレス	Web フィルタ サーバの IP アドレス。
タイムアウト（Timeout）	デバイスが Web フィルタ サーバからの応答を待機する時間の長さ（秒単位）。デフォルトは 5 秒です。 複数のサーバーを設定している場合、要求がタイムアウトすると、デバイスは次のサーバーを試行します。
PIX/ASA/FWSM 固有の設定	

要素	説明
インターフェイス	認証サーバが配置されているネットワーク インターフェイス（FastEthernet0 など）。インターフェイスを指定しない場合、デフォルトは内部インターフェイスとなります。 インターフェイスの名前またはインターフェイスを識別するインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択します。あるいは、新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。
プロトコル	Web フィルタリング サーバと通信する場合に使用するプロトコル。サーバに設定されている次のオプションを選択します。 • TCP（バージョン 1） • TCP バージョン 4 • UDP バージョン 4
Connection Number	（任意）デバイスとサーバの間で許容される TCP 接続の最大数。
IOS 固有の設定	
Retransmit	サーバが応答しない場合に、デバイスが要求を再送信する回数。デフォルト値は 2 回です。
[ポート（Port）]	サーバが受信に使用するポート番号。デフォルトのポートは 15868 です。



第 19 章

ファイアウォールの Botnet Traffic Filter ルールの管理

マルウェアとは、知らないうちにホストにインストールされている悪意のあるソフトウェアです。個人情報（パスワード、クレジット カード番号、キー ストローク、または独自データ）の送信などのネットワーク アクティビティを試みるマルウェアは、マルウェアが既知の不正な IP アドレスへの接続を開始したときにボットネット トラフィック フィルタによって検出できます。Botnet Traffic Filter は、悪意のある既知のドメイン名および IP アドレスを含む動的データベースと、着信接続および発信接続とを照合して、疑わしいアクティビティをすべてログに記録します。

また、ブロックアドレスを選択してスタティックブロックリストに追加することで、シスコのダイナミックデータベースを補完できます。ブロックリストに記載すべきでないと考えられるアドレスがシスコのダイナミックデータベースに含まれている場合は、それらのアドレスをスタティック許可リストに手動で入力できます。許可リストのアドレスに関する syslog メッセージは依然として生成されます。ただし、ターゲットになるのはブロック syslog メッセージだけであるため、これは単なる情報提供に過ぎません。内部要件のためにシスコのダイナミックデータベースを使用しない場合は、スタティックブロックリストだけを使用することもできます（ターゲットにするマルウェアサイトをすべて特定できる場合）。

この章は、次のセクションで構成されています。

- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）

Botnet Traffic Filter について

Botnet Traffic Filter のアドレス カテゴリ

ボットネット トラフィック フィルタのモニター対象のアドレスは次のとおりです。

- **既知のマルウェア アドレス**：これらのアドレスは、動的データベースおよび静的ブロックリストによって識別されるブロックリストに含まれています。

- **既知の許可アドレス**：これらのアドレスは、許可リストに含まれています。許可されるには、アドレスが、動的データベースによってブロックされ、かつ静的許可リストによって識別される必要があります。
- **あいまいなアドレス**：ブロックリストに記載されていないドメイン名を1つ以上含む複数のドメイン名に関連付けられているアドレス。これらのアドレスは、グレーリストに含まれています。
- **リストに記載されていないアドレス**：どのリストにも記載されていない不明アドレス。

既知アドレスに対する Botnet Traffic Filter のアクション

ボットネット トラフィック フィルタを設定して、疑わしいアクティビティをログに記録できます。必要に応じてボットネット トラフィック フィルタを設定して、疑わしいトラフィックを自動的にブロックすることもできます。

リストに記載されていないアドレスについては、syslog メッセージは生成されません。ただし、ブロックリスト、許可リスト、およびグレイリストに記載されているアドレスについては、タイプ別の syslog メッセージが生成されます。

Botnet Traffic Filter データベース

ボットネット トラフィック フィルタでは、既知のアドレスについて 2 つのデータベースが使用されます。両方のデータベースを使用するか、ダイナミック データベースをディセーブルにしてスタティック データベースだけを使用することができます。このセクションは、次のトピックで構成されています。

- 動的データベースに関する情報
- 静的データベースに関する情報

動的データベースに関する情報

ボットネット トラフィック フィルタでは、Cisco アップデート サーバーからダイナミック データベースの定期アップデートを受け取ることができます。このデータベースには、数千もの既知の不正なドメイン名と IP アドレスが含まれています。

セキュリティ アプライアンスでは動的データベースを次のように使用します。

1. DNS 応答内のドメイン名が動的データベース内の名前と一致した場合、Botnet Traffic Filter はその名前および IP アドレスを DNS 逆ルックアップ キャッシュに追加します。
2. 感染したホストがマルウェア サイトの IP アドレスへの接続を開始すると、セキュリティ アプライアンスは、疑わしいアクティビティについて通知する syslog メッセージを送信します。
3. 場合によっては、IP アドレス自体がダイナミック データベースに入力され、ボットネット トラフィック フィルタは DNS 要求を検査せずに、その IP アドレスへのすべてのトラフィックをログに記録します。

（注） データベースを使用するには、セキュリティ アプライアンスが URL にアクセスできるように、必ずセキュリティ アプライアンス用にドメイン ネーム サーバを設定してください。動的データベースでドメイン名を使用するには、Botnet Traffic Filter のスヌーピングとともに DNS パケット インスペクションをイネーブルにする必要があります。セキュリティ アプライアンスは DNS パケット内を調べて、ドメイン名と関連する IP アドレスを見つけます。

静的データベースに関する情報

不正な名前と見なすドメイン名または IP アドレス（ホストまたはサブネット）をブロックリストに手動で入力できます。許可リストに名前または IP アドレスを入力して、許可リストと動的ブロックリストの両方に表示される名前またはアドレスが syslog メッセージおよびレポートでは許可リストアドレスとしてのみ識別されるようにすることもできます。

これ以外に、Botnet Traffic Filter のスヌーピングとともに DNS パケット インスペクションをイネーブルにする方法もあります。DNS スヌーピングを使用すると、感染したホストが静的データベース上の名前に対して DNS 要求を送信した場合に、セキュリティ アプライアンスは DNS パケット内を調べてドメイン名および関連する IP アドレスを見つけ、その名前および IP アドレスを DNS 逆ルックアップ キャッシュに追加します。

関連項目

- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）

ボットネット トラフィック フィルタの設定のタスク フロー

Botnet Traffic Filter を設定するには、次の手順を実行します。

ステップ 1 DNS サーバの使用をイネーブルにします。

この手順により、セキュリティ アプライアンスで DNS サーバを使用できるようになります。マルチ コンテキスト モードで、コンテキストごとに DNS をイネーブルにします。

詳細については、[DNS] ページ （2616 ページ）を参照してください。

ステップ 2 ダイナミック データベースの使用をイネーブルにする。

この手順により、シスコの更新サーバからデータベースを更新できるようになり、また、セキュリティ アプライアンスでダウンロード済み動的データベースを使用できるようになります。ダウンロードされたデー

タベースのディセーブル化は、マルチ コンテキスト モードでデータベースの使用をコンテキストごとに設定できるようにする場合に有用です。

詳細については、ダイナミック データベースの設定 （1167 ページ）を参照してください。

ステップ 3 （任意）スタティック エントリをデータベースに追加する。

この手順では、ブロックまたは許可するドメイン名またはIPアドレスを使用してダイナミックデータベースを補完します。ダイナミック データベースをインターネット経由でダウンロードしない場合は、ダイナミック データベースの代わりにスタティック データベースを使用できます。

詳細については、スタティック データベースへのエントリの追加 （1168 ページ）を参照してください。

ステップ 4 DNS スヌーピングをイネーブルにする。

この手順により、DNSパケットのインスペクションがイネーブルになり、（セキュリティアプライアンス用のDNSサーバを使用できない場合は）ドメイン名と動的データベースまたは静的データベース内のドメイン名が比較され、名前および IP アドレスが DNS 逆ルックアップ キャッシュに追加されます。その後、疑わしいアドレスに対して接続が確立されたとき、Botnet Traffic Filter ロギング機能によってこのキャッシュが使用されます。

詳細については、DNS スヌーピングのイネーブル化 （1169 ページ）を参照してください。

ステップ 5 ボットネット トラフィック フィルタのトラフィック分類およびアクションをイネーブルにします。

この手順により、Botnet Traffic Filterで、各初期接続パケット内の送信元および宛先IPアドレスを動的データベース、静的データベース、DNS 逆ルックアップ キャッシュ、およびDNS ホスト キャッシュと比較して、一致トラフィックに関する syslog メッセージを送信するか、そのトラフィックをドロップできるようになります。

詳細については、ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（1170 ページ）を参照してください。

ステップ 6 ボットネット アクティビティをモニタおよび軽減します。

デバイスに Botnet Traffic Filter を設定すると、デバイスはボットネット アクティビティを通知する syslog メッセージの生成を開始します。メッセージが適切にログに記録され、必要に応じて通知が送信されるように、デバイス上のsyslog設定を確認する必要があります。悪意のあるトラフィックが識別された場合は、必要なアクションを実行してこのようなトラフィックを停止し、悪意のあるトラフィックを生成している感染コンピュータを浄化する必要があります。

詳細については、次の情報を参照してください。

1. ファイアウォール デバイスでのロギング ポリシーの設定 （2635 ページ）
2. ボットネット アクティビティのモニタリングと軽減 （3550 ページ）
3. ファイアウォール サマリー ボットネット レポートについて （3579 ページ）

ダイナミック データベースの設定

この手順により、データベースを更新できるようになり、また、セキュリティアプライアンスでダウンロード済み動的データベースを使用できるようになります。

マルチコンテキストモードの場合、すべてのセキュリティコンテキストで使用できるように、システムコンテキストで動的データベースのダウンロードをイネーブルにします。そのあと、コンテキストごとに、動的データベースの使用をイネーブルにするかディセーブルにするかを決定できます。

デフォルトでは、ダイナミックデータベースのダウンロードおよび使用はディセーブルになっています。

関連項目

- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- スタティック データベースへのエントリの追加 （1168 ページ）
- DNS スヌーピングのイネーブル化 （1169 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）

はじめる前に

セキュリティアプライアンスでDNSサーバの使用をイネーブルにします（[DNS] ページ （2616 ページ）を参照）。マルチ コンテキスト モードで、コンテキストごとにDNSをイネーブルにします。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） マルチ コンテキスト モードのデバイスの場合、システム コンテキストで動的データベースのダウンロードをイネーブルにし、必要に応じて各セキュリティ コンテキストで動的データベースの使用をイネーブルにします。

[Botnet Traffic Filter Rules] ページ （1174 ページ）が開きます。

ステップ 2 [ダイナミックブロックリスト設定（Dynamic Blocklist Configuration）] タブで [サーバーからのダイナミックブロックリストの有効化（Enable Dynamic Blocklist From Server）] を選択して、動的データベースのダウンロードをイネーブルにします。

（注） マルチコンテキストモードの場合、システムコンテキストで動的データベースのダウンロードをイネーブルにします。

この設定により、シスコの更新サーバから動的データベースをダウンロードできるようになります。データベースをセキュリティ アプライアンスにまだインストールしていない場合は、約 2 分後にデータベースがダウンロードされます。セキュリティ アプライアンスが今後の更新を検出するためにサーバをポーリングする頻度（通常は 1 時間おき）が、更新サーバによって決定されます。

ステップ 3 （マルチコンテキストモードだけ）[保存（Save）] をクリックして、システムコンテキストに変更を保存します。次に、Botnet Traffic Filter を設定するコンテキストに移動し、そのコンテキストの [ファイアウォール（Firewall）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）] を選択してステップ 4 （1168 ページ）に進みます。

ステップ 4 [ダイナミックブロックリスト設定（Dynamic Blocklist Configuration）] タブで [ダイナミックブロックリストの使用（Use Dynamic Blocklist）] を選択して、動的データベースの使用を有効にします。

（注） マルチコンテキストモードの場合、これらの設定はシステム コンテキストでディセーブルになっています。

スタティック データベースへのエントリの追加

スタティックデータベースを使用すると、ブロックまたは許可するドメイン名、IP アドレス、またはネットワークアドレスを使用してダイナミックデータベースを増強できます。詳細については、 Botnet Traffic Filter について （1163 ページ）を参照してください。

関連項目

- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- ダイナミック データベースの設定 （1167 ページ）
- DNS スヌーピングのイネーブル化 （1169 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（1170 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）

はじめる前に

- セキュリティ アプライアンスで DNS サーバの使用をイネーブルにします（[DNS] ページ（2616 ページ）を参照）。マルチ コンテキスト モードで、コンテキストごとに DNS をイネーブルにします。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） マルチ コンテキスト モードのデバイスの場合、セキュリティ コンテキストで静的データベースを設定します。

これにより、[Botnet Traffic Filter Rules] ページ （1174 ページ）が開きます。

ステップ 2 [許可リスト/ブロックリスト（Permitlist / Blocklist）] タブで、追加するエントリのタイプ（[許可リスト（Permitlist）] または [ブロックリスト（Blocklist）]）に対応した [行の追加（Add Rows）] ボタンをクリックします

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）が開きます。

ステップ 3 [Domain or IP Address] フィールドに、1 つ以上のドメイン名、IP アドレス、および IP アドレス/ネットマスクを入力します。複数のエントリは、カンマで区切るかまたは別々の行に入力します。タイプごとに最大 1000 のエントリを入力できます。

ステップ 4 [OK] をクリックします。

DNS スヌーピングのイネーブル化

この手順では、DNS パケットのインスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。DNS パケットのインスペクションとボットネット トラフィック フィルタ スヌーピングでは、ドメイン名がダイナミック データベースまたはスタティック データベースのドメイン名と比較され、ドメイン名と IP アドレスがボットネット トラフィック フィルタの DNS 逆ルックアップ キャッシュに追加されます。その後、疑わしいアドレスに対して接続が確立されたとき、Botnet Traffic Filter ロギング機能によってこのキャッシュが使用されます。

DNS インスペクションのデフォルト設定では、すべてのインターフェイス上のすべての UDP DNS トラフィックが検査され、Botnet Traffic Filter のスヌーピングはディセーブルになります。外部 DNS 要求を送信するインターフェイスでだけ Botnet Traffic Filter のスヌーピングをイネーブルにすることを推奨します。内部 DNS サーバへの送信を含むすべての UDP DNS トラフィックで Botnet Traffic Filter のスヌーピングをイネーブルにすると、セキュリティ アプライアンスに不要な負荷がかかります。

（注） TCP DNS トラフィックはサポートされません。

関連項目

- [Configure DNS] ダイアログボックス （1000 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- ダイナミック データベースの設定 （1167 ページ）
- スタティック データベースへのエントリの追加 （1168 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）

ステップ 1 最初に、Botnet Traffic Filter を使用してスヌーピングするトラフィックの DNS インスペクションを設定する必要があります。ファイアウォール インスペクション ルールの管理 （977 ページ）を参照してください。

ステップ 2 新しいインスペクション ルールの定義または既存のインスペクション ルールの編集時に、検査するプロトコルとして [DNS] を選択します。

[Selected Protocol] フィールドの右側にある [Configure] ボタンがアクティブになります。

ステップ 3 [構成] をクリックします。

[Configure DNS] ダイアログボックス （1000 ページ）が開きます。

ステップ 4 DNS スヌーピングをイネーブルにするには、[動的フィルタスヌーピングを有効化（Enable Dynamic Filter Snooping）] を選択します。

ステップ 5 [OK] をクリックします。

ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化

この手順により、Botnet Traffic Filter で、各初期接続パケット内の送信元および宛先 IP アドレスを動的データベース、静的データベース、DNS 逆ルックアップ キャッシュ、および DNS ホスト キャッシュと比較して、一致トラフィックに関する syslog メッセージを送信できるようになります。また、Botnet Traffic Filter では、一致トラフィックの発生時に接続をドロップすることもできます。特定のインターフェイスに関して、ボットネット トラフィック フィルタリングが適用されるトラフィックを識別するイネーブル化ルールを 1 つだけ指定できます。た

だし、Botnet Traffic Filter によってドロップされるトラフィックを識別する場合は、複数の廃棄ルールを指定できます。

DNS スヌーピングは個別にイネーブルにします（DNS スヌーピングのイネーブル化 （1169 ページ）を参照）。一般的に、Botnet Traffic Filter を最大限に利用するには、DNS スヌーピングをイネーブルにする必要がありますが、必要に応じて、Botnet Traffic Filter のロギングだけを単独で使用できます。ダイナミック データベースに DNS スヌーピングが設定されていない場合、ボットネット トラフィック フィルタでは、スタティック データベースのエントリとダイナミック データベースの IP アドレスだけが使用されます。ダイナミック データベースのドメイン名は使用されません。

[ボットネットトラフィック分類ACLに関する注意事項（ What You Need To Know About Botnet Traffic Classification ACLs）]

イネーブル化ルールおよび廃棄ルールを設定する場合、拡張 ACL ポリシー オブジェクトを指定して、ボットネット トラフィック フィルタリングが適用されるトラフィックを制限することもできます。ACL オブジェクトを指定しなかった場合、すべてのトラフィックに対してフィルタリングが実行されます。このことは、単一の permit IP any any ルールを持つ ACL を指定することと同等です。

フィルタリングが一部のトラフィックで実行されるように ACL を指定する場合は、次の点を考慮してください。

- 許可ルールは、ボットネット トラフィック フィルタリングが適用されるトラフィックを識別します。廃棄ルールの場合、許可エントリは ASA でドロップできるトラフィックを識別します。
- 拒否ルールは、フィルタリングが適用されないトラフィックを識別します。Botnet Traffic Filter は、拒否エントリと一致するトラフィックを無視します。
- 廃棄ルールに選択した ACL は、インターフェイスのイネーブル化ルールに使用されている ACL のサブネットである必要があります。ドロップされるトラフィックについては、ドロップルールの ACL 内に許可ルールがあるだけでなく、トラフィックがイネーブル化ルールの ACL 内にある許可ルールに分類されている必要もあります。これは、イネーブル化ルールで許可されているトラフィックが先にブロック対象として識別されるまで、ドロップルールは考慮されないためです。

インターネットに直接接続されているインターフェイスのすべてのトラフィックに対してボットネット トラフィック フィルタをイネーブルにし、Moderate 以上の重大度のトラフィックのドロップをイネーブルにすることをお勧めします。

関連項目

- [Traffic Classification] タブ （1176 ページ）
- BTF イネーブル化ルール エディタ （1178 ページ）
- BTF 廃棄ルール エディタ （1179 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）

- ダイナミック データベースの設定 （1167 ページ）
- スタティック データベースへのエントリの追加 （1168 ページ）
- DNS スヌーピングのイネーブル化 （1169 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）]>[ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）]>[ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） マルチ コンテキスト モードのデバイスの場合、セキュリティ コンテキストでトラフィック分類を設定します。

[Botnet Traffic Filter Rules] ページ （1174 ページ）が開きます。

ステップ 2 指定したトラフィックで Botnet Traffic Filter をイネーブルにするには、次の手順を実行します。

a) [トラフィック分類（Traffic Classification）] タブで、[イネーブル化ルール（Enable Rules）] テーブルの下にある [行の追加（Add Row）] をクリックします。

BTF イネーブル化ルール エディタ （1178 ページ）が開きます。

b) [Interfaces] フィールドで、Botnet Traffic Filter をイネーブルにするインターフェイスを指定します。通常は、インターネットに接しているインターフェイスだけをイネーブルにします。インターフェイス セレクタを使用してインターフェイスまたはインターフェイス ロール オブジェクトを選択するには、[選択（Select）] をクリックします（インターフェイス ロール オブジェクトについて （381 ページ）を参照）。

All インターフェイス ロール オブジェクトを選択することで（デフォルトで選択されています）、すべてのインターフェイスに適用されるグローバルな分類を設定できます。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によってグローバル設定が上書きされます。

c) 次のいずれかを実行して、モニタするトラフィックを特定します。

- すべてのトラフィックをモニタするには、ACL フィールドを空白のままにしておきます。
- モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。

（注） イネーブル化ルールはインターフェイスごとに 1 つだけ指定できます。

d) [OK] をクリック

BTF イネーブル化ルール エディタが閉じ、ルールが [Enable Rules] テーブルに追加されます。

ステップ 3 マルウェア トラフィックを自動的にドロップするには、次の手順を実行します。

（注） 自動的にドロップするトラフィックの廃棄ルールを作成する前に、そのトラフィックの Botnet Traffic Filter をイネーブルにする必要があります。

a) [トラフィック分類（Traffic Classification）] タブで、[ドロップルール（Drop Rules）] テーブルの下にある [行の追加（Add Row）] をクリックします。

BTF 廃棄ルール エディタ （1179 ページ）が開きます。

b) [Interfaces] フィールドで、トラフィックをドロップするインターフェイスを指定します。そのインターフェイス用のイネーブル化ルールが存在している必要があります。インターフェイスセレクタを使用してインターフェイスまたはインターフェイス ロール オブジェクトを選択するには、[選択（Select）] をクリックします（インターフェイス ロール オブジェクトについて （381 ページ）を参照）。

All インターフェイス ロール オブジェクトを選択することで（デフォルトで選択されています）、すべてのインターフェイスに適用されるグローバルな分類を設定できます。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によってグローバル設定が上書きされます。

c) 次のいずれかを実行して、ドロップするトラフィックを特定します。

- すべてのトラフィックをモニタするには、ACL フィールドを空白のままにしておきます。
- モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。

d) [Threat Level] 領域で、次のいずれかのオプションを選択して、特定の脅威レベルを持つトラフィックをドロップします。デフォルト レベルは、Moderate から Very High までの範囲となります。

（注） デフォルト設定を変更する確固たる理由がない限り、デフォルト設定を使用することを強くお勧めします。

- [Value]：ドロップする脅威レベルを指定します。
- [Range]：脅威レベルの範囲を指定します。

（注） 静的ブロックリストエントリは、常に Very High 脅威レベルに指定されます。

e) [OK] をクリック

BTF 廃棄ルール エディタが閉じ、ルールが [Drop Rules] テーブルに追加されます。

ステップ 4 さらにルールを追加するには、必要に応じて、手順 2 および 3 を繰り返します。ルールの追加が完了したら、[保存（Save）] をクリックして変更を保存します。

ステップ 5 アクション目的でグレーリストのトラフィックをブラックリストのトラフィックとして処理するには、[ダイナミックブラックリスト設定（Dynamic Blacklist Configuration）] タブで [不明なトラフィックをブラック

リストのトラフィックとして処理（Treat Ambiguous traffic as Blacklist）] チェックボックスをオンにします。

このオプションをイネーブルにしないと、グレーリストのトラフィックに廃棄ルールを設定している場合にも、そのトラフィックはドロップされません。

[Botnet Traffic Filter Rules] ページ

[Botnet Traffic Filter Rules] ページを使用すると、ASA セキュリティ デバイスを通過する悪意のあるトラフィックを識別するためのルールを定義できます。

[Botnet Traffic Filter Rules] ページは、次の 3 つのセクションに分かれています。

- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [Traffic Classification] タブ （1176 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）

ナビゲーション パス

[Botnet Traffic Filter Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択してから、ポリシーセレクタで **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）]>[ボットネットトラフィックフィルタルール（Botnet Traffic Filter Rules）] を選択します。

関連項目

- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [Traffic Classification] タブ （1176 ページ）
- BTF イネーブル化ルール エディタ （1178 ページ）
- BTF 廃棄ルール エディタ （1179 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）

- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- [Configure DNS] ダイアログボックス （1000 ページ）

[動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ

[動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブを使用すると、シスコの更新サーバーからデータベースを更新できるようになり、セキュリティアプライアンスでダウンロード済み動的データベースを使用できるようになります。

ナビゲーション パス

[Botnet Traffic Filter Rules] ページ （1174 ページ）から [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブをクリックします。

関連項目

- ダイナミック データベースの設定 （1167 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）
- [Traffic Classification] タブ （1176 ページ）
- BTF イネーブル化ルール エディタ （1178 ページ）
- BTF 廃棄ルール エディタ （1179 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- [Configure DNS] ダイアログボックス （1000 ページ）

フィールド リファレンス

表 *270 : [*動的ブラックリスト設定（*Dynamic Blacklist Configuration*）*]* タブ

要素	説明
サーバーからのダイナミックブロックリストの有効化（Enable Dynamic Blacklist From Server）	Cisco アップデート サーバからのダイナミック データベースのダウンロードをイネーブルにします。データベースをセキュリティ アプライアンスにまだインストールしていない場合は、約 2 分後にデータベースがダウンロードされます。セキュリティ アプライアンスが今後の更新を検出するためにサーバをポーリングする頻度（通常は 1 時間おき）が、更新サーバによって決定されます。 （注） デバイスがマルチ コンテキスト モードの場合は、そのデバイスのシステム コンテキストでこのオプションを設定します。
ダイナミックブロックリストを使用（Use Dynamic Blocklist）	Botnet Traffic Filter に対して動的データベースの使用をイネーブルにします。 （注） マルチ コンテキスト モードでは、コンテキストごとにデータベースの使用を設定します。
不明なトラフィックをブラックリストのトラフィックとして処理（Treat Ambiguous traffic as Blacklist）	選択すると、グレーリストのトラフィックは、アクション目的でブロックリストのトラフィックとして処理されます。 このオプションをイネーブルにしないと、グレーリストのトラフィックに廃棄ルールを設定している場合にも、そのトラフィックはドロップされません。

[Traffic Classification] タブ

[Traffic Classification] タブを使用して、デバイスまたは共有ポリシーのトラフィック分類定義を表示または設定し、自動的にドロップされる悪意のあるトラフィックを指定します。トラフィック分類定義（イネーブル化ルール）はACLを伴うインターフェイスまたはインターフェイス ロールで構成され、この ACL によって Botnet Traffic Filter でモニタするトラフィックが識別されます。特定のインターフェイスまたはインターフェイス ロールの設定値を設定できます。All インターフェイス ロール オブジェクトを使用して、ボットネット フィルタリングをグローバルにイネーブルにできます（デフォルトで選択されています）。インターフェイス固有の分類を設定した場合は、そのインターフェイス設定によって、インターフェイス ロールに定義されているすべての設定が上書きされます。

特定のインターフェイスに関して、ボットネット トラフィック フィルタリングが適用されるトラフィックを識別するイネーブル化ルールを 1 つだけ指定できます。ただし、Botnet Traffic Filter によってドロップされるトラフィックを識別する場合は、複数の廃棄ルールを指定できます。

（注） Botnet Traffic Filter を適切に機能させるために、動的フィルタのスヌーピングを設定することを強く推奨します。デバイス ビューでは、Cisco Security Manager によって [Traffic Classification] タブの下部にリンクが表示され、このリンクを使用すると、直接 [Inspection Rules] ページに移動して動的フィルタのスヌーピングをイネーブルにできます。詳細については、 DNS スヌーピングのイネーブル化 （1169 ページ）を参照してください。

テーブル内のカラムはエントリ設定の概要を示しており、これについては BTF イネーブル化ルール エディタ （1178ページ）およびBTF 廃棄ルール エディタ （1179ページ）で説明します。

トラフィック分類およびアクションを設定するには、次の手順を実行します。

- [行の追加（Add Row）] ボタンをクリックして、インターフェイスまたはインターフェイス ロールをテーブルに追加し、BTF イネーブル化ルール エディタ （1178 ページ）またはBTF 廃棄ルール エディタ （1179 ページ）に入力します。
- エントリを選択し、[行の編集（Edit Row）] ボタンをクリックして、既存のエントリを編集します。
- エントリを選択し、[行の削除（Delete Row）] ボタンをクリックして削除します。

ナビゲーション パス

[Botnet Traffic Filter Rules] ページ （1174 ページ）で、[トラフィック分類（Traffic Classification）] タブをクリックします。

関連項目

- BTF イネーブル化ルール エディタ （1178 ページ）
- BTF 廃棄ルール エディタ （1179 ページ）
- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- [Configure DNS] ダイアログボックス （1000 ページ）

BTF イネーブル化ルール エディタ

BTF イネーブル化ルール エディタを使用して、Botnet Traffic Filter をイネーブルにするインターフェイスを指定し、モニタするトラフィックを特定します。イネーブル化ルールはインターフェイスごとに 1 つだけ指定できます。

ナビゲーション パス

BTF イネーブル化ルールエディタにアクセスするには、[トラフィック分類（Traffic Classification）] タブの [イネーブル化ルール（Enable Rules）] テーブルで、作業領域内を右クリックしてから [行の追加（Add Row）] を選択するか、または既存エントリを右クリックして [行の編集（Edit Row）] を選択します。

関連項目

- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（1170 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [Traffic Classification] タブ （1176 ページ）
- BTF 廃棄ルール エディタ （1179 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- [Configure DNS] ダイアログボックス （1000 ページ）

フィールド リファレンス

表 *271 : BTF* イネーブル化ルール エディタ

要素	説明
インターフェイス	Botnet Traffic Filter をイネーブルにするインターフェイスまたはインターフェイス ロール。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 All インターフェイス ロール オブジェクトを使用して、ボットネット フィルタリングをグローバルにイネーブルにできます（デフォルトで選択されています）。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によって、グローバル設定が上書きされます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
ACL	モニタするトラフィックの識別に使用するアクセス リストを指定します。アクセス リストを指定しないと、デフォルトですべてのトラフィックがモニタされます。 モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。

BTF 廃棄ルール エディタ

BTF 廃棄ルール エディタを使用して、自動的にドロップされるマルウェア トラフィックを識別します。インターフェイスごとに複数の廃棄ルールを指定できます。

ナビゲーション パス

BTF ドロップルールエディタにアクセスするには、[トラフィック分類（Traffic Classification）] タブの [ドロップルール（Drop Rules）] テーブルで、作業領域内を右クリックしてから [行の追加（Add Row）] を選択するか、または既存エントリを右クリックして [行の編集（Edit Row）] を選択します。

関連項目

- ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化（1170 ページ）

- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [Traffic Classification] タブ （1176 ページ）
- BTF イネーブル化ルール エディタ （1178 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- [Configure DNS] ダイアログボックス （1000 ページ）

フィールド リファレンス

表 *272 : BTF* 廃棄ルール エディタ

要素	説明
インターフェイス	Botnet Traffic Filter をイネーブルにするインターフェイスまたはインターフェイス ロール。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 All インターフェイス ロール オブジェクトを使用して、ボットネット フィルタリングをグローバルにイネーブルにできます（デフォルトで選択されています）。インターフェイス固有の分類を設定する場合は、そのインターフェイス設定によって、グローバル設定が上書きされます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
ACL	モニタするトラフィックの識別に使用するアクセス リストを指定します。アクセス リストを指定しないと、デフォルトですべてのトラフィックがモニタされます。 モニターするトラフィックを指定するには、ACL フィールドの右側にある [選択（Select）] をクリックして、モニターするトラフィックを識別するアクセス制御リストオブジェクトを選択します。たとえば、外部インターフェイス上のポート 80 トラフィックをすべてモニタします。アクセス コントロール リスト オブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。

要素	説明
脅威レベル	[Threat Level] フィールドは、ドロップされる悪意のあるトラフィックの脅威レベルを特定します。デフォルト レベルは、Moderate から Very High までの範囲となります。 （注） デフォルト設定を変更する確固たる理由がない限り、デフォルト設定を使用することを強くお勧めします。 • [Value]：ドロップする脅威レベルを指定します。 • Very-low • 低い • 中程度 • 高 • Very-high • [Range]：脅威レベルの範囲を指定します。 （注） 静的ブロックリストエントリは、常に Very High 脅威レベルに指定されます。

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブを使用して、デバイスまたは共有ポリシー用の静的データベースのエントリを表示または設定します。[デバイスブロックリスト（Device Blocklist）] には、悪意のあるサイトまたは望ましくないサイトのドメイン名または IP アドレスが含まれます。静的ブロックリストを使用してシスコの動的データベースを補強できます。また、対象とするすべてのマルウェアサイトを特定できる場合は静的ブロックリストだけを使用できます。

[デバイス許可リスト（Device Permitlist）] には、許容可能と認められるサイトのドメイン名または IP アドレスが含まれます。ブロックする必要はないと考えられるアドレスがブロックアドレスとして動的データベースに含まれている場合は、これらのアドレスを手動で静的な許可リストに加えることができます。静的な許可リストのエントリは、静的なブロックリストおよびシスコの動的データベース内のエントリに優先します。許可リストのアドレスに関する syslog メッセージは依然として生成されます。ただし、ターゲットになるのはブロック syslog メッセージだけであるため、これは単なる情報提供に過ぎません。

静的データベースを設定するには、次の手順を実行します。

- [行の追加（Add Row）] ボタンをクリックし、[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）を使用して静的データベースのエントリを定義します。

- エントリを選択し、[行の編集（Edit Row）] ボタンをクリックして、既存のエントリを編集します。

ワンポイント アドバイス

エントリを選択して **F2** キーを押すか、または [デバイス許可リスト（Device Permitlist）] か [デバイスブロックリスト（Device Blocklist）] でエントリをダブルクリックして、その場でエントリを編集します。

- エントリを選択し、[行の削除（Delete Row）] ボタンをクリックして削除します。

ナビゲーション パス

[Botnet Traffic Filter Rules] ページ （1174 ページ）から、[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブをクリックします。

関連項目

- スタティック データベースへのエントリの追加 （1168 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス （1182 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [Traffic Classification] タブ （1176 ページ）

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックス

[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] ダイアログボックスを使用して、許可リスト（安全）またはブロックリスト（悪意）に追加するドメイン名または IP アドレスを手動で定義します。静的ブロックリストを使用してシスコの動的データベースを補強できます。また、対象とするすべてのマルウェアサイトを特定できる場合は静的ブロックリストだけを使用できます。許可リストと動的ブロックリストの両方に表示される名前またはアドレスは、syslog メッセージとレポートでは許可リストアドレスとしてのみ識別されます。

ドメイン名は完全な形式（www.cisco.com など、ホスト名を含む）にしたり、部分的な形式（cisco.com など）にしたりできます。部分的な名前の場合、そのドメイン上のすべての Web サイトホストが、許可リストまたはブロックリストに追加されます。また、ホストの IP アドレスを入力することもできます。カンマまたは改行を使用して、複数のエントリを区切ります。

ナビゲーション パス

[許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）で、[デバイス許可リスト（Device Permitlist）] または [デバイスブロックリスト（Device Blocklist）] テーブルの下にある [行の追加（Add Rows）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- スタティック データベースへのエントリの追加 （1168 ページ）
- Botnet Traffic Filter について （1163 ページ）
- ボットネット トラフィック フィルタの設定のタスク フロー （1165 ページ）
- [Botnet Traffic Filter Rules] ページ （1174 ページ）
- [動的ブラックリスト設定（Dynamic Blacklist Configuration）] タブ （1175 ページ）
- [Traffic Classification] タブ （1176 ページ）
- BTF イネーブル化ルール エディタ （1178 ページ）
- BTF 廃棄ルール エディタ （1179 ページ）
- [許可リスト/ブロックリスト（Permitlist/Blocklist）] タブ （1181 ページ）
- [Configure DNS] ダイアログボックス （1000 ページ）

第 20 章

ScanSafe Web Security の使用

Security Manager により、ScanSafe Web Security との統合が可能になります。ScanSafe Web Security は、クラウド ベースの SaaS（Security as a Service）機能であり、Web セキュリティ データセンターを世界中のさまざまな場所で利用できるようになります。ScanSafe Web Security とルータを統合すると、他の方法によるコンテンツ スキャンおよびマルウェアの検出のために、選択した HTTP トラフィックと HTTPS トラフィックが ScanSafe Cloud にリダイレクトされます。また、ScanSafe Web Security を使用して特定のユーザ、ユーザ グループ、および IP にディファレンシエーテッド サービスも提供できます。

Security Manager から ScanSafe Web Security を起動すると、次の領域のポリシーおよび設定を定義できます。

- コンテンツ スキャン設定
- コンテンツ スキャン ポリシー
- AAA サーバ設定
- AAA ポリシー

Security Manager で ScanSafe Web Security を統合することにより、ほぼすべてのポリシーおよびフレームワーク ベースのポリシー機能をコピーおよび共有できます。次の表で、スキャンおよび AAA ポリシー タイプのサポート範囲について詳しく説明します。

サポートされるタイプ	例
コンテンツスキャン設定	プライマリ サーバ IP、セカンダリ サーバ IP、サーバ タイムアウト
コンテンツ スキャン ポリシー	グローバル許可リストポリシー ユーザ グループの追加または除外、デフォルト ユーザ設定、デフォルト ユーザ グループの設定 コンテンツ スキャンをイネーブルする必要があるインターフェイス

サポートされるタイプ	例
AAA サーバー設定	HTTP Basic および NTLM ポリシーで使用されるアイデンティティ ポリシー オブジェクト HTTP Basic および NTLM に関連するタイムアウト プロキシ、HTTP Basic、および NTLM の発生順序 IOS の LDAP サーバーおよび LDAP 属性マップ設定 （注） また、RADIUS サーバおよび TACAS サーバもサポートされています。 インターフェイスごとの AAA リスト
AAA ポリシー	HTTP Basic および NTLM アドミッションルールのサポート（認証方式）が、以前から使用可能な認証プロキシ方式に追加されました。

Security Manager は、次の機能をサポートしていません。

- http/https の検査ルールまたは ZBF ルールが存在しない場合の PAM 設定
- 古い IOS バージョンで LDAP を使用する認証プロキシ（ScanSafe Web Security をサポートする IOS バージョンでのみ可能）
- AAA 方式としての AuthProxy によるアイデンティティ ポリシー。（NTLM および HTTP Basic のみをサポートしています）
- アイデンティティ ポリシーを作成するための Virtual Template 番号の検証
- LDAP サーバ用の Secure Trust Point の検証
- コンテンツスキャンルールの継承
- ユーザーグループおよびユーザーの AD ブラウジング
- 新しいポリシー（ポリシー クエリーなど）に対するツール サポート
- 制御タグポリシー

ScanSafe Web セキュリティ製品の詳細については、http://www.cisco.com/en/US/partner/products/ps11720/index.html を参照してください。

この章は、次のセクションで構成されています。

- ScanSafe Web セキュリティの設定 （1187 ページ）
- ScanSafe Web Security ページ （1189 ページ）
- [ScanSafe Web Security Settings] ページ （1192 ページ）

ScanSafe Web セキュリティの設定

[ScanSafe Web Security設定（ScanSafe Web Security Settings）] ページを使用して、デフォルトのユーザグループの設定を定義します。他の設定ポリシーと同様に、デフォルトのユーザグループ ポリシー設定を共有できます。

関連項目

- ScanSafe Web Security ページ （1189 ページ）
- [ScanSafe Web Security Settings] ページ （1192 ページ）
- [Add Default User Group]/[Edit Default User Group] ダイアログボックス （1191 ページ）
- [AAA Rules] ページ （880 ページ）

（注） すべての手順は、ポリシービューから実行されたものとして表示されます。

ScanSafe Web セキュリティを設定するには、次の手順を実行します。

ステップ 1 ポリシータイプセレクタから、[ファイアウォール（Firewall）]、[ScanSafe Webセキュリティ（ScanSafe Web Security）] の順に選択します。 >

[ScanSafe Web Security] ページが表示され、[Interfaces] タブが選択されています。

ステップ 2 Web リクエストを ScanSafe Web セキュリティサーバーに転送するために使用するインターフェイスを、[利用可能なインターフェイス（Available Interfaces）] 列のリストから選択して、[選択したインターフェイス（Selected Interfaces）] 列に移動することにより、有効にします。

ステップ 3 [正規表現の許可リスト（Permitlisting Regular Expressions）] タブを選択します。

ステップ 4 通知を許可リストに関する ScanSafe Web セキュリティサーバーに送信するには、[通知タワー（Notify Tower）] チェックボックスをオンにします。これは、IP ベースのものを除くすべての許可リストに適用できます。

（許可リストに正規表現が指定されていない場合、ScanSafe Web セキュリティは警告を受け取ります。）

ステップ 5 HTTP ホストエリアで、[利用可能な正規表現（Available Regular Expressions）] カラムのリストから正規表現を選択し、[選択した正規表現（Selected Regular Expressions）] カラムに移動することにより、（正規表現マッチングを使用して）許可される正規表現を指定します。

ステップ 6 HTTP ユーザーエージェントエリアで、[利用可能な正規表現（Available Regular Expressions）] カラムのリストから正規表現を選択し、[選択した正規表現（Selected Regular Expressions）] カラムに移動することにより、許可される正規表現を指定します。

ステップ 7 [許可リストACL（Permitlisting ACLs）] タブを選択します。

ステップ 8 タイプリストから [拡張（Extended）] または [標準（Standard）] を選択して、操作する ACL のタイプを指定します。

ステップ 9 許可リストに追加する ACL を指定するには、左側の列のリストから ACL を選択し、それらを [選択したアイテム（Selected items）] カラムに移動します。

ステップ 10 [ユーザーグループ（User Groups）] タブを選択します。

ヒント [ユーザーグループ（User Groups）] ページを使用して、ユーザーグループを定義し、デフォルトユーザとデフォルトユーザーグループの両方を指定し、ユーザーグループを含めたり除外したりできます。これら 3 つのリストすべてのエントリを編集または削除することもできます。

ステップ 11 [デフォルトユーザ（Default User）] フィールドにユーザ名を入力して、デフォルトユーザを指定します（任意）。

ステップ 12 [デフォルトユーザーグループ（Default User Group）] フィールドにユーザーグループ名を入力して、デフォルトユーザーグループを指定します。

ステップ 13 インターフェイスを選択し、ユーザーグループを [含める（Include）] リストに追加して、ユーザーグループを含めます。

ステップ 14 インターフェイスを選択し、ユーザーグループを [除外（Exclude）] リストに追加して、ユーザーグループを除外します。

ステップ 15 ポリシーセレクタから [ポリシー（Policy）] > [ファイアウォール（Firewall）] > [設定（Settings）] > [ScanSafe Webセキュリティ（ScanSafe Web Security）] を選択します。

ステップ 16 [詳細（Details）] タブを選択し、次の値を入力してプライマリ ScanSafe サーバーを指定します。

- IP アドレス/名前（IP Address/Name）
- HTTP ポート（デフォルトは 8080）
- HTTPS ポート（デフォルトは 8080）

ステップ 17 [詳細（Details）] タブを選択し、次の値を入力してセカンダリ ScanSafe サーバーを指定します。

- IP アドレス/名前（有効な IP アドレスまたは FQDN のみ）。
- HTTP ポート（デフォルトは 8080）
- HTTPS ポート（デフォルトは 8080）

ステップ 18 [サーバーのタイムアウト（Server Timeout）] 期間を秒で指定します（デフォルトは 300）。

ステップ 19 [セッションアイドルタイムアウト（Session Idle Timeout）] 期間を秒で指定します（デフォルトは 300）。

ステップ 20 次のいずれか *1* つを実行して、送信元アドレスを指定します。

- [IPアドレス（IP Address）] ボタンをクリックし、IP アドレスを入力します。
- [インターフェイス（Interface）] ボタンをクリックし、[選択（Select）] ボタンをクリックして、インターフェイスセレクタを参照してインターフェイスを選択します。

（注） 有効なソース IP またはインターフィエスは、ScanSafe Web セキュリティが有効になっているインターフェイスの 1 つである必要があります（[ファイアウォール（Firewall）] > [ScanSafe Web セキュリティ（ ScanSafe Web Security）] ページ > [インターフェイス（Interface）] タブで）。

ステップ 21 **ライセンス**を入力し、暗号化されている場合はチェックボックスをオンにします。

ヒント　[暗号化（Encrypted ）] が選択されていない場合、入力する値は 32 文字の 16 進数にする必要があります。

ステップ 22　必要に応じて、[ログの有効化（Enable Logging）] チェックボックスをオンにします。

ScanSafe Web Security ページ

Security Manager により、ScanSafe Web Security との統合が可能になります。ScanSafe Web Security は、クラウド ベースの SaaS（Security as a Service）機能であり、Web セキュリティ データセンターを世界中のさまざまな場所で利用できるようになります。ScanSafe Web Security とルータを統合すると、他の方法によるコンテンツ スキャンおよびマルウェアの検出のために、選択した HTTP トラフィックと HTTPS トラフィックが ScanSafe Cloud にリダイレクトされます。また、ScanSafe Web Security を使用して特定のユーザ、ユーザ グループ、および IP にディファレンシエーテッド サービスも提供できます。

Security Manager で ScanSafe Web セキュリティを使用すると、次の領域の設定およびポリシーを定義できます。

- コンテンツ スキャン設定
- コンテンツ スキャン ポリシー
- AAA サーバ設定
- AAA ポリシー

Security Manager で ScanSafe Web Security を統合することにより、ほぼすべてのポリシーおよびフレームワーク ベースのポリシー機能をコピーおよび共有できます。

ナビゲーション パス

（ポリシー ビュー）ポリシー タイプ セレクタから [Firewall] を選択し、[Settings] を開きます。次に [ScanSafe Web Security] をクリックし、[ScanSafe Web Security Settings] ページを開きます。

（注）　ScanSafe Web セキュリティのポリシーと設定は、マップ ビューを使用して設定することもできます。

関連項目

- ScanSafe Web セキュリティの設定 （1187 ページ）
- [ScanSafe Web Security Settings] ページ （1192 ページ）
- [Add Default User Group]/[Edit Default User Group] ダイアログボックス （1191 ページ）
- [AAA Rules] ページ （880 ページ）

フィールド リファレンス

要素	説明
[インターフェイス（Interfaces）] タブ	
：フィルタ（Filter）	Security Manager でのフィルタの使用方法の詳細については、テーブルのフィルタリング （64 ページ）を参照してください。
インターフェイス	このタブでは、コンテンツスキャンのために Web 要求が ScanSafe Web セキュリティサーバーに転送されるインターフェイスおよび Security Manager 定義のインターフェイスロールを選択できます。
— Available Interfaces	ScanSafe Web Security 用に選択可能なインターフェイス。
— 選択されたインターフェイス（Selected Interfaces）	選択されたインターフェイスは、Web サービスに対するホストの要求が ScanSafe Web セキュリティサーバーに転送される WAN に面している必要があります。
-	-
[正規表現の許可リスト（Permitlisting Regular Expressions）] タブ	
— Notify Tower	このチェックボックスをオンにすると、許可リストに関して ScanSafe Web セキュリティタワーに通知する必要があることを指定します。これは、IP ベースの許可リストを除く、すべての ACL ベースの許可リストのバリエーションに適用されます。デフォルトの動作では、通知は送信されません。
— Available Regular Expressions (HTTP Host)	ScanSafe Web Security サーバへの配信で使用可能であり、検討対象となる正規表現をリストします。
—フィルター（Filter）（HTTP ホスト）	管理者は、ユーザーグループリストの包含および除外を指定することにより、ScanSafe Web セキュリティサーバーに送信される許可された正規表現をフィルタリングできます。このフィルタは、[Match All] または [Match Any] のいずれかで操作します。
— Selected Regular Expressions (HTTP Host)	選択した正規表現に一致するホストは許可リストに追加され、ScanSafe Web セキュリティサーバーにリダイレクトされません。
— Available Regular Expressions (HTTP User Agent)	使用可能な正規表現に一致するエージェントは許可リストに追加され、ScanSafe Web セキュリティサーバーにリダイレクトされません。

要素	説明
— 選択された正規表現（Selected Regular Expressions）（HTTP ホスト）	設定すると、[選択された正規表現（Selected Regular Expressions）] リストにある正規表現のみが ScanSafe クラウドに送信されます。
[許可リストACL（Permitlisting ACLs）] タブ	
— ACL タイプ（ACL Type）	ACL許可リストのタイプ（標準または拡張のいずれか）を指定します。 （注） 許可リストに使用される標準 ACL は、拡張 ACL として検出されます。ACL名に「CSM_EXT_」のプレフィックスが付加されます。拡張 ACL は完全であり推奨されるため、標準 ACL は拡張 ACL に変換されます
— 選択された ACLS（Selected ACLS）	設定すると、[選択された正規表現（Selected Regular Expressions）] リストにある正規表現のみが ScanSafe クラウドに送信されます。
[User Groups] タブ	
— デフォルトユーザー（Default User）	コンテンツ スキャン セッションに固有のユーザ名がない場合、ScanSafe Web Security サーバに送信されるグローバル名。たとえば、支社内のすべてのユーザに対して、同じコンテンツ スキャン ポリシーを適用する場合に使用します。
— Default User Group	コンテンツ スキャン セッションに固有のユーザ名がない場合、ScanSafe Web Security サーバに送信されるグローバル名。たとえば、支社内のすべてのユーザ グループに対して、同じコンテンツ スキャン ポリシーを適用する場合に使用します。
— インターフェイス固有のデフォルト ユーザー グループ（Interface Specific Default User Groups）	各インターフェイスのデフォルトのユーザーグループを一覧表示します。
— 包含（Include）/除外（Exclude）	包含リストまたは除外リストを使用して、包含または除外する特定のユーザーグループを指定できます。

[Add Default User Group]/[Edit Default User Group] ダイアログボックス

特定のインターフェイスのデフォルト ユーザ グループを指定するには、[Default User Groups] ダイアログボックスを使用します。

これらの ScanSafe Web Security サーバーの設定の詳細については、[ScanSafe Web Security Settings] ページ （1192 ページ）を参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

関連項目

- ScanSafe Web Security ページ （1189 ページ）
- [ScanSafe Web Security Settings] ページ （1192 ページ）
- ScanSafe Web セキュリティの設定 （1187 ページ）
- [AAA Rules] ページ （880 ページ）

ナビゲーション パス

（ポリシー ビュー）[Firewall] を選択し、[ScanSafe Web Security] ページを開きます。次に [User Groups] タブをクリックします。

[ScanSafe Web Security Settings] ページ

関連項目

- ScanSafe Web Security ページ （1189 ページ）
- ScanSafe Web セキュリティの設定 （1187 ページ）
- [Add Default User Group]/[Edit Default User Group] ダイアログボックス （1191 ページ）
- [AAA Rules] ページ （880 ページ）

ナビゲーション パス

（ポリシー ビュー）ポリシー タイプ セレクタから [Firewall] を選択し、[Settings] を開きます。次に [ScanSafe Web Security] をクリックし、[ScanSafe Web Security Settings] ページを開きます。

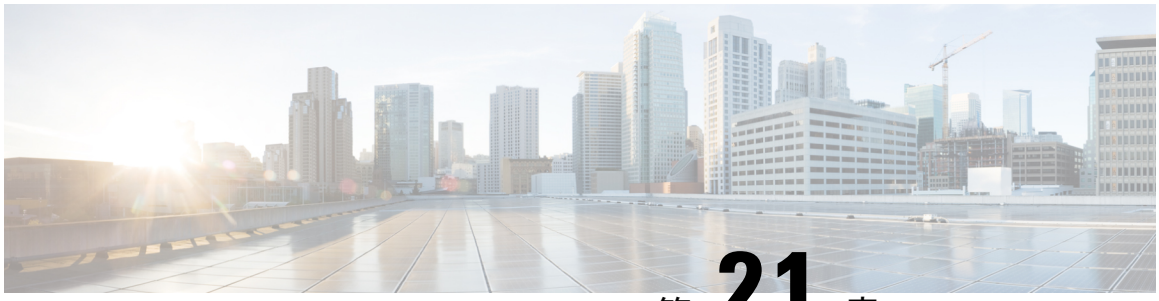
（デバイス ビュー）ポリシー タイプ セレクタから [Firewall] を選択し、[Settings] を開きます。次に [ScanSafe Web Security] をクリックし、[ScanSafe Web Security Settings] ページを開きます。

フィールド リファレンス

表 *273 : ScanSafe Web Security* の設定

要素	説明（Description）	使用方法
IP Address|Name (Primary ScanSafe Server)	ScanSafe Web Security を操作するために設定されたサーバのプライマリ FQDN または IP アドレス。	両方
HTTP Port (Primary ScanSafe Server)	プロキシ HTTP トラフィック用のデフォルト プライマリ ポート（デフォルトは 8080）。	両方
[HTTPS ポート（プライマリ ScanSafe サーバー）（HTTPS Port (Primary ScanSafe Server)）]	プロキシ HTTPS トラフィック用のデフォルトプライマリポート（デフォルトは 8080）。	両方
[IP アドレス/名前（バックアップ ScanSafe サーバー）（IP Address/Name (Backup ScanSafe Server)）]	ScanSafe Web Security を操作するために設定されたサーバーのセカンダリ FQDN または IP アドレス。	両方
[HTTP ポート（バックアップ ScanSafe サーバー）（HTTP Port (Backup ScanSafe Server)）]	プロキシ HTTP トラフィック用のデフォルト セカンダリ ポート（デフォルトは 8080）。	両方
[HTTPS ポート（セカンダリ ScanSafe サーバー）（HTTPS Port (Secondary ScanSafe Server)）]	プロキシ HTTPS トラフィック用のデフォルトセカンダリポート（デフォルトは 8080）。	両方
サーバー タイムアウト（Server timeout）	ScanSafe Web セキュリティサーバーの可用性をチェックするときのポーリングタイムアウト。	IOS のみ
セッション アイドル タイムアウト（Session Idle Timeout）	ScanSafe Web セキュリティサーバーの非アクティブタイムアウト（デフォルトは 300 秒）。セッションが非アクティブであることが検出された場合にセッションを削除するために使用されます。	IOS のみ
On Failure	プライマリとセカンダリの両方の ScanSafe Web Security サーバが非アクティブであることを検出した場合に、実行する処置（すべてのトラフィックをドロップする、またはすべてのトラフィックを通過させる）を決定します。	IOS のみ
IP Address (Source Address)	ScanSafe Web Security サーバへのパケットがルータから送信される際の、送信元の IP アドレス。	IOS のみ

要素	説明（Description）	使用方法
Interface (Source Address)	ScanSafe Web Security サーバへのパケットがルータから送信される際の、送信元のインターフェイス アドレス。	IOS のみ
ライセンス	ScanSafe Web Security サーバに送信されたライセンス（32 文字の 16 進数）	Both
Encrypted	選択すると、暗号化がイネーブルになります。ASA は、暗号化されたライセンステキストの設定を受け入れません。	IOS のみ
Enable Logging Checkbox	IOS syslogs をイネーブルにします（デフォルトでは、イネーブルされません）。	IOS のみ
[公開キーファイル（Public Key File）]	公開キーファイルの名前。	ASA のみ
[接続再試行回数（Connection Retry Count）]	システムが接続を再試行する回数。	ASA のみ



第 21 章

ゾーンベースのファイアウォール ルールの管理

ゾーンベースのファイアウォール機能（ゾーンベース ポリシーファイアウォールとも呼ばれる）を使用すると、「ゾーン」と呼ばれるインターフェイスのグループ間でIOSファイアウォールポリシーを一方向に適用できます。つまり、インターフェースはゾーンに割り当てられ、ファイアウォールルールはゾーン間を一方向に移動する特定のタイプのトラフィックに適用されます。Cisco Security Manager 4.16 以降では、サブインターフェイスをゾーンに割り当てることができます。ゾーンベースのファイアウォールは、デフォルトでセキュア ゾーン間ポリシーを強制します。これにより、トラフィックを許可する明示的なポリシーが定義されるまで、トラフィックはセキュリティ ゾーンを通過できません。

「ゾーン」自体は抽象的なものであり、同じまたは類似するセキュリティ要件を持つ、論理的にグループ化できる複数のインターフェイスを指しています。たとえば、ルータインターフェイス Ethernet 0/0 および Ethernet 0/1 が、ローカル LAN に接続されている場合があります。ファイアウォールの観点では、これら 2 つのインターフェイスは内部ネットワークを表す点と、ファイアウォール設定の目的で単一のゾーンにグループ化できる点で同じです。次に、そのゾーンと他のゾーン間にファイアウォール ポリシーを指定できます。ゾーン間ポリシーでは十分な柔軟性と精度が提供されるので、同一のルータ インターフェイスに接続された複数のホスト グループにさまざまな検査ポリシーを適用できます。

（注） ゾーンベースのファイアウォール機能は、12.4(6)T以降を実行するIOSデバイス、および 12.2(33) 以降を実行する ASR デバイスでサポートされています。

単純な例

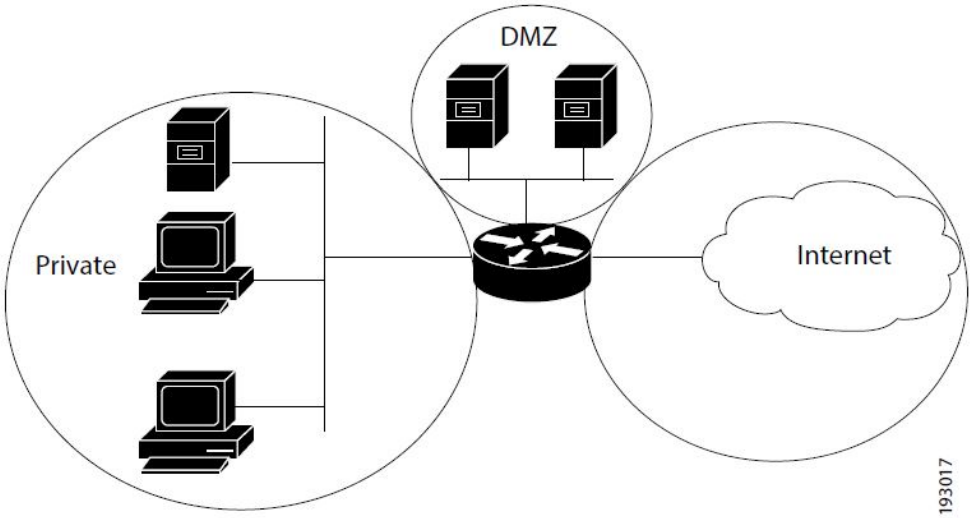
ネットワーク内のセキュリティが類似する領域ごとにセキュリティ ゾーンを設定して、同じゾーンに割り当てられているすべてのインターフェイスが類似するセキュリティ レベルで保護されるようにする必要があります。たとえば、次のように3つのインターフェイスを持つアクセス ルータを考えます。

- 1 つのインターフェイスはパブリック インターネットに接続されています。

- 1 つのインターフェイスは、パブリック インターネットからアクセスできてはいけないプライベート LAN に接続されています。
- 1 つのインターフェイスは、インターネットサービスの「緩衝地帯」（DMZ）に接続されています。ここでは、Web サーバー、

ドメインネームシステム（DNS）サーバーと電子メールサーバーが、公共のインターネットにアクセスできる必要があります。次の図に示すように、このネットワークの各インターフェイスは、独自のゾーンに割り当てられます。

図 *27*：基本セキュリティ ゾーン トポロジ



この設定例では、通常、以下を定義する 3 つのメインポリシー（ルールセット）があります。

- インターネットへのプライベート ゾーン接続
- DMZ ホストへのプライベート ゾーン接続
- DMZ ホストへのインターネット ゾーン接続

ゾーンベースのファイアウォールは、禁止されたデフォルトのセキュリティ ポスチャの制約を課します。たとえば、DMZ ホストが他のネットワークへのアクセスを特別に許可されていない場合、これらのネットワークは DMZ ホストからの不要な接続から保護されます。同様に、インターネット ホストからプライベート ゾーンへの直接アクセス権が明示的に付与されていないかぎり、プライベート ゾーンのホストはインターネット ホストによる望ましくないアクセスから保護されます。

この単純な例では、各ゾーンにメンバインターフェイスが1つだけあります。たとえば、追加のインターフェイスがプライベートゾーンに追加された場合、その新しいインターフェイスに接続しているホストは、ゾーン内の既存のインターフェイスに接続しているすべてのホストにトラフィックを即時に渡すことができます。また、他のゾーン内のホストへのトラフィックは、既存のプライベート ゾーン ポリシーによって即時に制御されます。

より現実的な例として、DMZ 内の特定のホストへのパブリック インターネットからのさまざまなアクセスを許可する場合、および保護された LAN 内のホストに対するさまざまなアプリケーション使用ポリシーを許可する場合があります。

この章は次のトピックで構成されています。

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （1203 ページ）
- ゾーンベースのファイアウォール ルールの Services と Protocols の関係について （1207 ページ）
- ゾーンベースのファイアウォール ルールに対する一般的な推奨事項 （1208 ページ）
- ゾーンベースのファイアウォールルールの開発と適用 （1209 ページ）
- ゾーンベースのファイアウォールルールの追加 （1210 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- デフォルトのドロップ動作の変更 （1260 ページ）
- ゾーンベースのファイアウォール ルールの設定 （1261 ページ）
- ゾーンベースのルールと設定のトラブルシューティング （1267 ページ）
- [Zone-based Firewall Rules] ページ （1272 ページ）

ゾーンベースのファイアウォール ルールについて

ゾーンは、ネットワークのセキュリティ境界を設定します。ゾーンは、トラフィックがネットワークの別の領域に移動するときにインスペクションまたはフィルタリングの対象となる境界を定義します。ゾーン間のデフォルトのゾーンベースのファイアウォールポリシーは、「deny all」です。このため、ゾーンベースのファイアウォールルールが明示的に設定されていない場合、すべてのゾーン間のトラフィックの移動がブロックされます。

ゾーンベースのファイアウォール ルールは、ゾーンのペア間にあるさまざまなタイプの単方向トラフィックに、特定のアクション（Drop、Pass、Inspect、および Content Filter）を適用します。トラフィックの方向は、送信元ゾーンと宛先ゾーンを各ルールの一部として指定することで設定します。

ログ

ゾーンベースのファイアウォール ルールには、syslog、alert、audit-trail のロギング オプションがあります。ほとんどのメッセージは、syslog サーバが設定されていないかぎりルータ コン

ソールに記録されます。syslog ロギングの設定の詳細については、Cisco IOS ルータにおけるロギング （3269 ページ）を参照してください。

重要なポイント

ゾーンとゾーンベースのファイアウォール ルールについて、次の点に注意してください。

- ゾーンベースのファイアウォール機能は、12.4(6)T 以降を実行する IOS デバイス、および 12.2(33) 以降を実行する ASR デバイスでのみサポートされています。
- ゾーンベースのファイアウォール ルールと IOS インスペクション ルールが同じインターフェイスを使用する場合は、エラーが発生します。

ゾーンベースのファイアウォールモデルと以前のインターフェイスベースのインスペクションルールモデルは、ルータ上で互いに排他的ではありませんが、指定されたインターフェイス上で結合することはできません。つまり、インターフェイスは、インスペクションルールで設定されている場合に、セキュリティゾーンのメンバとして設定できません。さらに、両方のモデルを同時に使用するようにルーターを設定することはお勧めしません。

- インターフェイスは1つのセキュリティゾーンにのみ割り当てることができますが、ゾーンには複数のインターフェイスを含めることができます。インターフェイスが複数のゾーンに割り当てられている場合は、エラーが発生します。
- 特定のインターフェイスとの間のすべてのトラフィックは、インターフェイスがゾーンに割り当てられている場合に暗黙的にブロックされます（同じゾーンの他のインターフェイスとの間で送受信されるトラフィック、およびルータ上の任意のインターフェイスに送信されるトラフィックを除く）。このため、ゾーンメンバ インターフェイスとの間のトラフィックを許可するには、そのゾーンと他の任意のゾーンとの間にトラフィックを許可または検査するルールを 1 つ以上設定する必要があります。
- トラフィックは、同じゾーンのメンバであるインターフェイス間を流れることを暗黙に許可されます。ただし、同じゾーンのメンバ間のトラフィックのインスペクションを要求するルールを定義できます。
- 「Self」ゾーンは、ルータ自体を独立したセキュリティゾーンとして定義するデフォルトのゾーンであり、送信元ゾーンまたは宛先ゾーンとして指定できます。Self ゾーンは、デフォルトの「deny all」ポリシーの唯一の例外です。任意のルータ インターフェイスへのすべてのトラフィックは、明示的に拒否されるまで許可されます。

Self ゾーンを含むゾーンベースのファイアウォール ルールは、ローカル トラフィック（ルータに向けられたトラフィック、またはルータによって生成されたトラフィック）に適用されます。ルータを通過するトラフィックには適用されません。詳細については、Self ゾーン （1200 ページ）を参照してください。

- Self ゾーンに適用されるルールでは、検査アクションは許可されません。
- Pass アクションは、一方向でだけトラフィックを許可します。リターン トラフィックのルールは明示的に定義する必要があります。ただし、Inspect アクションでは、リターン トラフィックは確立済みの接続に対して自動的に許可されます。

- トラフィックは、ゾーンメンバインターフェイスと、ゾーン メンバでない任意のインターフェイスとの間を流れることができません。
- ゾーンに割り当てられていないインターフェイスは、依然として従来のルータ ポートとして機能でき、他のタイプのファイアウォール ルールが設定されている場合があります。

ただし、インターフェイスがゾーンベースのファイアウォールポリシーに含まれない場合でも、そのインターフェイスをゾーンに追加し、そのゾーンとゾーン間トラフィックフローが必要な他のゾーンとの間に「pass all」ポリシー（「ダミーポリシー」の一種）を設定する必要がある場合があります。

- ゾーンのメンバーであるインターフェイスに適用されるアクセス制御リスト（ACL）は、ゾーンルールが適用される前に処理されます。したがって、両方のルールタイプの使用を継続するには、インターフェイス ACL を緩和して、特定のトラフィック フローがゾーンベースのルールによって処理されるようにすることが必要な場合があります。
- ゾーン内のすべてのインターフェイスは、同じ Virtual Routing and Forwarding（VRF; 仮想ルーティングおよび転送）インスタンスに属している必要があります。ゾーンベースのルールは、メンバ インターフェイスが別々の VRF にあるゾーン間に設定できます。ただし、トラフィックがこれらの VRF 間を流れることができない場合、これらのルールは実行されません。詳細については、ゾーンと VRF 対応ファイアウォール （1202 ページ）を参照してください。
- ゾーンは、インターフェイス ロール オブジェクトを使用して定義されます。ゾーンに使用されているインターフェイスロールの定義を変更した場合は、ゾーンを変更することになり、既存のトラフィック フローに影響することがあります。さらに、インターフェイスロールでワイルドカードを使用してインターフェイス名のパターンを指定すると、ルータで新しいインターフェイスを作成するときに、インターフェイスがゾーンに自動的に追加される可能性があることに注意してください。
- ゾーンベースのファイアウォールルールに、競合するゾーン情報が含まれている場合、テーブルで最初に定義されたルールが優先されます。有効なゾーンを参照しないルールは展開されず、アクティビティ検証警告が表示されます。
- 空のゾーンがあると、特定のデバイスでアクティビティ検証エラーが発生します。次の制約事項リストを参照してください。
- 特定のデバイスでは、送信元ゾーンと宛先ゾーンを同じにできません。次の制約事項リストを参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

関連項目

- Self ゾーン （1200 ページ）
- ゾーンベースのファイアウォールポリシーでの VPN の使用 （1201 ページ）
- ゾーンと VRF 対応ファイアウォール （1202 ページ）
- ゾーンベースのファイアウォール ルールの設定 （1261 ページ）
- ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （1203 ページ）
- ゾーンベースのファイアウォール ルールの Services と Protocols の関係について （1207 ページ）
- ゾーンベースのファイアウォール ルールに対する一般的な推奨事項 （1208 ページ）
- ゾーンベースのファイアウォールルールの開発と適用 （1209 ページ）

Self ゾーン

ルータ自体は「**Self**」という固有の名前を持つ独立したセキュリティ ゾーンとして定義されており、IOS ファイアウォールがルータで終端または発信するトラフィック（「ローカル」トラフィックと呼ばれる）の検査をサポート（TCP、UDP および H.323 のみ）しているため、着信および発信ルータトラフィックは、ルーテッドゾーン間トラフィックと同じ方法でルールの対象となります。

インターフェイスがゾーンに割り当てられると、そのインターフェイスに接続されているホストがそのゾーンに含まれます。デフォルトでは、トラフィックは同じゾーンのメンバーであるインターフェイス間のフローを許可されており、デフォルトの「deny-all」ポリシーがゾーン間を移動するトラフィックに適用されます。

ただし、その他のゾーンおよびルータの IP インターフェイス（Self ゾーン）間を直接流れるトラフィックは暗黙的に許可されています。これにより、ゾーンファイアウォール設定がルータに適用される場合に、ルータの管理インターフェイスへの接続が維持されることが保証されます。

つまり、ルータのインターフェイスの IP アドレスへのトラフィックフローおよび IP アドレスからのトラフィックフローは、当初はゾーンポリシーによって制御されていません。ルータインターフェイスと他のゾーンの間を移動するトラフィックを制御する場合は、このローカルトラフィックをブロックまたは許可するルールを適用する必要があります。

Self ゾーンのルールを設定する場合は、次の点を考慮します。

- ルータに設定されているすべての IP アドレスは、インターフェイス ゾーンのメンバーシップに関係なく Self ゾーンに属します。
- 逆に明示的なルールを設定するまで、Self ゾーンとの間のトラフィックは制限されません。

つまり、Self ゾーンを含むゾーンベースのファイアウォールルールを構成すると、Self ゾーンと他のゾーンの間のトラフィックはすぐに両方向で制限されます。たとえば、「プライベート」ゾーンから Self ゾーンへのトラフィックに影響するルールを定義した場合、Self からプライベートへのルールを 1 つ以上定義するまで、ルータはプライベート ゾーンにトラフィックを発信できません。

ルータ自体と、Self ゾーン ルールに含まれない他のゾーンとの間のトラフィックは影響を受けません。

- Self ゾーンに適用されるルールでは、検査アクションは許可されません。

インバウンド Self ゾーン トラフィックに制限を設定する場合は、必要なアウトバウンド トラフィック（ルーティング プロトコルおよびネットワーク管理プロトコルを含む）を検討します。たとえば、あるゾーンからルータ自体へのインバウンド トラフィックを制限した場合、ルーティング プロトコルはそのゾーンに属するすべてのインターフェイスで動作を停止することがあります。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）

ゾーンベースのファイアウォールポリシーでの VPN の使用

IP Security（IPsec）VPN 実装が最近拡張されて、VPN 接続のファイアウォール ポリシー設定が単純化されました。IPSec Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）と GRE+IPSec により、特定のセキュリティ ゾーンにトンネル インターフェイスを配置することで、VPN サイト間接続およびクライアント接続をそのセキュリティ ゾーンに限定できます。接続が特定のポリシーによって制限される必要がある場合は、接続を VPN DMZ 内で隔離できます。または、VPN 接続が暗黙的に信頼されている場合は、VPN 接続をネットワーク内で信頼されているのと同じセキュリティ ゾーンに配置できます。

（トンネル/ループバック/仮想インターフェイスを動的に作成する）動的VPN でゾーンベースのファイアウォール ルールを使用するようにルータを設定するには、次の操作を行います。

- VPN インターフェイス専用のゾーンを定義します。
- [Zone Based Firewall] ページ （1262 ページ）の [VPN] タブの [VPNゾーン（VPN Zone）] フィールドに、このゾーンを入力します。
- ゾーンベースのファイアウォール ルールを作成して、VPN トラフィックを適宜許可します。

VTI 以外の IPsec が採用されている場合は、VPN にゾーンベースのファイアウォール ポリシーを設定するときに注意する必要があります。ゾーン ポリシーでは、保護されたホストが暗号化された VPN トラフィックの入力インターフェイスとは異なるゾーンにある場合に、リモート VPN ホストまたはクライアントによるそれらのホストへのアクセスを明示的に許可する必要があります。このアクセス ポリシーは、VPN クライアントの送信元 IP アドレスを列挙するアクセス コントロール リスト（ACL）、および VPN クライアントが到達することを許可されてい

るすべての保護ホストの宛先 IP アドレスを含めることで設定する必要があります。アクセスポリシーが適切に設定されていない場合、ポリシーによって、脆弱なホストが敵対的なトラフィックにさらされる可能性があります。

これらのトピックの詳細については、cisco.com のホワイトペーパー『Using VPN with Zone-Based Policy Firewall』を参照してください。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）

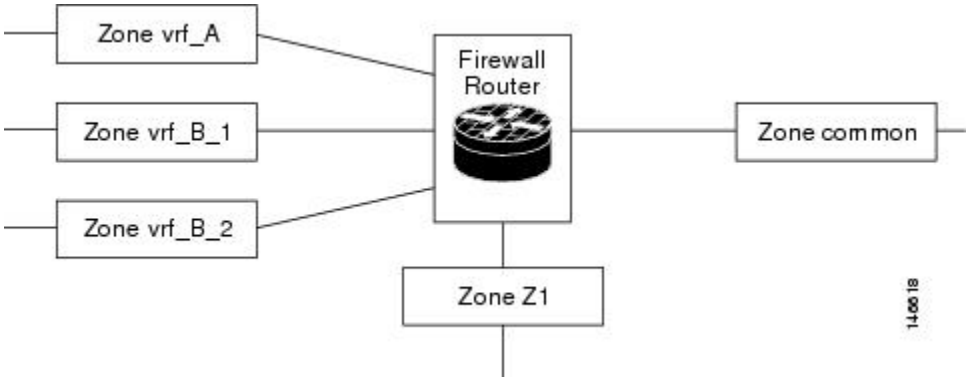
ゾーンと VRF 対応ファイアウォール

Cisco IOS ファイアウォールは Virtual Routing and Forwarding（VRF）に対応しており、異なる VRF 間で重複する IP アドレス、VRF に対する個別のしきい値とタイムアウトなどを管理できます。ゾーンベースのファイアウォール ルールを適用するには、ゾーン内のすべてのインターフェイスが同じ VRF に属している必要があります。

ルータで複数の VRF が設定されていて、あるインターフェイスですべての VRF に共通のサービス（インターネットサービスなど）が提供されている場合は、そのインターフェイスを別のゾーンに配置します。その後、共通ゾーンと他のゾーンとの間のポリシーを定義できます（VRF あたり 1 つ以上のゾーンを設定できます）。

次の図に示すように、異なる VRF を含む 2 つのゾーン間でルールを設定できます。

図 *28 : ゾーンと VRF*



この図の場合：

- 共通サービスを提供するインターフェイスはゾーン「common」のメンバです。
- すべての VRF A は、単一のゾーン「vrf_A」にあります。
- VRF B には複数のインターフェイスが含まれており、「vrf_B_1」と「vrf_B_2」の 2 つのゾーンに分割されています。
- ゾーン Z1 には VRF インターフェイスがありません。

この設定に基づいて、次の処理を行うことができます。

- これらの各ゾーンとcommonゾーンの間にポリシーを指定できます。さらに、VRFルートエクスポートが設定されていて、トラフィックパターンが適切である場合は、ゾーンvrf_A、vrf_B_n、およびZ1のそれぞれの間でポリシーを指定できます。
- ゾーン vrf_A と vrf_B_1 の間にポリシーを設定できますが、トラフィックがこれらのゾーン間を流れることができることを確認します。
- VRF ごとにグローバルなしきい値とタイマーを指定する必要はありません。その代わりに、パラメータマップによって inspect アクションにパラメータが提供されます。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）

ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について

ゾーンベースのファイアウォールルールを作成する場合、実行に関連する2つの設定を行う必要があります。許可/拒否とアクション（ドロップ、パス、検査、またはコンテンツフィルタ）です。目的の結果を得るには、この2つのパラメータ間の関係を明確に理解する必要があります。

- **許可/拒否**：許可/拒否設定は、アクセス制御リスト（ACL）エントリの許可/拒否に対応しているように見えます。ただし、ゾーンベースのファイアウォール ルールでは、標準のアクセス ルールとは異なり、これらのキーワードでトラフィックは許可または拒否されません。代わりに、[Source]、[Destination]、および[Services]フィールドで定義されたトラフィック フローにアクションを適用するかどうかと、それらが関連クラス マップの処理に影響するかどうかを指定します。
  - **許可**：指定したアクションを、[送信元（Source）]、[宛先（Destination）]、および[サービス（Services）]フィールドと一致するトラフィックに適用します（プロトコルが [Protocols] テーブルにリストされている場合、アクションはそれらのプロトコルに限定されます）。

ヒント：ゾーンベースのすべてのルールは基本的に「許可」 ルールである必要があります。これは最も理解しやすい設定です。選択したアクションを適用するトラフィックを識別しているということです。

- - **拒否**：[送信元（Source）]、[宛先（Destination）]、および[サービス（Services）]フィールドで定義されたトラフィックを除外します。（プロトコルが [プロトコル（Protocols）] テーブルにリストされている場合、除外はそれらのプロトコルに限定されます）。つまり、ルールに一致しないトラフィックとして処理します。代わりに、ゾーン ペアの後続のクラス マップ（ゾーン ルールと同じではない）を評価し、トラフィックと一致する後続マップを探します。後続マップがトラフィックと一致し

ない場合は、デフォルトのルールをトラフィックに適用します（デフォルトのドロップ動作の変更 （1260 ページ）を参照）。

ゾーン ルールとクラスマップ間には1対1関係がないことに注意してください。したがって、ルール テーブルで参照するだけでは、ルールがクラス マップに変換される方法を判断できません。Deny 規則に一致するトラフィックに適用できる後続規則を確認するには、設定をプレビューする必要があります（設定をプレビューするには、変更を保存し、[ツール（Tools）] > [設定のプレビュー（ Preview Configuration）] を選択します。詳細については、設定のプレビュー （535 ページ）を参照してください）。

一般的に、拒否ルールを使用して、サブネットに適用する許可ルールからサブネット内の特定の IP アドレスを除外できます。たとえば、10.100.10.0/24 に適用されるルールから 10.100.10.1 を除外します。ただし、特定の IP アドレスの Permit ルールを作成し、目的のアクションを適用して、このルールがゾーンベースのルールテーブルの一般ルールよりも上にリストされるようにする方がはるかに簡単です。

Denyルールを使用する場合は、ゾーンベースのルールと設定のトラブルシューティング （1267 ページ）も参照してください。

- **アクション**：アクションパラメータは、許可ルールに一致するトラフィックに起きることを定義します。どのクラス マップにルールが追加されるかを判断する場合を除き、Deny ルールではこれらのパラメータが無視されます。

Permit ルールを作成する場合、[Source]、[Destination]、[Services]、および [Protocol] フィールドと一致するトラフィックは、選択したアクション（トラフィックをドロップ（さらにオプションでログに記録）、トラフィックを渡す（さらにオプションでログに記録）、トラフィックを検査、またはコンテンツ フィルタリングを適用（Web トラフィックの場合のみ））に従って処理されます。

一部のプロトコルでトラフィックを検査する場合、またはコンテンツ フィルタリングを実行する場合は、詳細インスペクションに使用するポリシー マップを指定するオプションもあります。詳細インスペクション ポリシー マップでは、トラフィックのより詳細な特性に基づくアクションも指定します。この追加のインスペクションは、割り当てたポリシーマップが参照するクラスマップの要件を満たすパケットに適用されます。詳細インスペクションのクラスマップに一致しないパケットは許可されます。このため、詳細インスペクションは、ポリシーマップでそのアクションが指定されている場合に TCP 接続をリセットすることがあります。

次の表に、ゾーンベースのファイアウォール ルールで選択した Permit/Deny とアクションの関係を示します。この表では、TCP サービスを例として使用しますが、全般的な説明は IP サービスにも適用されます。結果は、ルールで指定した [From Zone] と [To Zone] にだけ適用されます。

表 *274 :* ゾーンベースのルールの *Permit/Deny* とアクションとの関係

許可/拒否	サービス	ルール アクション	プロトコル	結果
許可（Permit）	[TCP]	成功（Pass）	（なし）	すべての TCP トラフィックを通過させます。
拒否（Deny）	[TCP]	成功（Pass）	（なし）	ルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルトルールが適用されます。 Pass アクションは無視されます。
許可（Permit）	[TCP]	削除（Drop）	（なし）	すべての TCP トラフィックをドロップします。
拒否（Deny）	[TCP]	削除（Drop）	（なし）	ルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルトルールが適用されます。 Drop アクションは無視されます。
許可（Permit）	[TCP]	成功（Pass）	DNS	DNS トラフィックのみ通過させます。その他の TCP トラフィックは、以降のルールによって処理されます。
許可（Permit）	[TCP]	削除（Drop）	DNS	DNS トラフィックはドロップされます。その他の TCP トラフィックは、以降のルールによって処理されます。
拒否（Deny）	[TCP]	成功（Pass）	DNS	DNS トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 Pass アクションは無視されます。
拒否（Deny）	[TCP]	削除（Drop）	DNS	DNS トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 Drop アクションは無視されます。

許可/拒否	サービス	ルール アクション	プロトコル	結果
許可（Permit）	[TCP]	検査（Inspect）	HTTP	HTTP トラフィックを許可して検査します。より詳細な検査用のポリシーマップを指定すると、ポリシーマップのアクションは、より詳細な検査パラメータに一致するすべてのパケットに適用されます（プロトコル違反の接続のリセットなど）。
拒否（Deny）	[TCP]	検査（Inspect）	HTTP	HTTP トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 検査アクションは無視されます。 **ヒント** 後続のルールまたはクラス デフォルトが検査なしでトラフィックを通過させる場合、HTTP 接続のリターン トラフィックを許可するために、もう一方の方向に Permit/Pass ルール（またはアクセス ルール）を作成する必要があります。HTTP接続を禁止する場合は、拒否/検査ルールの代わりに許可/ドロップルールを作成します。
許可（Permit）	[TCP]	コンテンツ フィルタ	HTTP	HTTP トラフィックを許可して検査し、URL フィルタリング マップを適用して、要求された Web サイトに基づいて Web 接続を選択的に許可または拒否します。 より詳細な検査用のポリシー マップを指定すると、ポリシーマップのアクションは、より詳細な検査パラメータに一致するすべてのパケットに適用されます（プロトコル違反の接続のリセットなど）。 このため、Webサイトがブラックリストに追加されたか、HTTP パケットが詳細インスペクション ルールに違反したため、トラフィックがドロップされることがあります。

許可/拒否	サービス	ルール アクション	プロトコル	結果
拒否（Deny）	[TCP]	コンテンツ フィルタ	HTTP	HTTP トラフィックのルールをスキップし、次のクラスマップを評価します。Permit ルールを含む次のクラスマップが適用されるか、またはクラスのデフォルト ルールが適用されます。 コンテンツ フィルタ アクションは無視されます。 **ヒント** このタイプのルールでは、トラフィックをドロップまたはコンテンツ フィルタリングを適用する後続のクラス マップがない場合に、指定した送信元/宛先をコンテンツ フィルタリングから免除できます。ただし、このトラフィックに対して HTTP 接続を許可する場合は、トラフィックの Permit/Inspect ルールを作成する必要があります。

ゾーンベースのファイアウォール ルールの Services と Protocols の関係について

ゾーンベースのファイアウォールを作成する場合、ターゲット トラフィックの特性の識別に役立つ、一見すると同じような 2 つのパラメータ（Services と Protocols）があります。これらのフィールドのエントリは非常によく似た情報を提供する場合がありますが、デバイス設定でゾーンベースのファイアウォール ポリシーを構築するときに異なる方法で使用されます。ここでは、これらのフィールドの推奨される使用方法について説明します。

- [サービス（Services）] : [サービス（Services）] フィールドは、アクセス制御リスト（ACL）エントリのトラフィック プロトコルの定義に使用されます。この ACL エントリは、指定された送信元と宛先とともに、ポリシーを適用するトラフィックを定義するためにクラスマップによって使用されます。ただし、標準のアクセス ルールとは異なり、このサービス情報はトラフィック プロトコルを識別する主要な手段ではありません。ACL ではエントリごとにサービスを指定する必要があるため、サービス情報が必要となります。

一般に、[プロトコル（Protocol）] テーブルを使用して Drop、Pass、または Inspect の対象とする特定のプロトコルを識別するため、すべてのゾーンベースのファイアウォール ルールの [サービス（Services）] フィールドはデフォルト エントリ（IP）のままにできます。

[Service] に IP 以外を指定する場合は、[Protocol] テーブルにリストされているプロトコルと競合しないように選択してください。たとえば、[サービス（Services）] フィールドで UDP を指定せずに、テーブルに TCP ベースのプロトコルをリストします。一般に、特定のルールに対して、[Services] フィールドに特定のサービスを指定する場合は、[Protocol] テーブルにプロトコルを入力しないでください。

- [プロトコル（Protocol）]：[ゾーンベースのルールの追加（Add Zone Based Rule）] ダイアログボックスと [ゾーンベースのルールの編集（Edit Zone Based Rule）] ダイアログボックスの [アクション（Action）] 領域にある [プロトコル（Protocol）] テーブルは、1 つ以上のプロトコルの選択、カスタム ポート アプリケーション マッピングの追加（デフォルト以外のポートを指定した場合）、およびディープ インスペクション ポリシー マップの適用に使用されます。DNS などの非常に特定的なプロトコル、TCP や UDP などの一般プロトコル、さらに特殊なアプリケーションに使用するポートを識別するカスタムプロトコルを指定できます。

原則として、[Services] は [IP] に設定したままにし、[Protocol] テーブルを使用して、Drop、Pass、Inspect アクションのすべてのゾーンベース ルールに対するプロトコル（これもサービスです）を指定します（コンテンツ フィルタ アクションは、HTTP プロトコルを自動的に使用します。これを設定することはできますが、変更はできません。）このアプローチに従うと、可能な限り「クリーン」で、解釈（およびトラブルシューティング）が容易な設定が作成されます。

デバイス コンフィギュレーションを生成するときにこれらのフィールドがどのように使用されるかの詳細については、ゾーンベースのルールと設定のトラブルシューティング （1267 ページ）を参照してください。

ゾーンベースのファイアウォール ルールに対する一般的な推奨事項

ゾーンベースのファイアウォール ルールでは、さまざまな設定が可能です。標準のアクセス ルール、インスペクション ルール、および Web フィルタ ルールの代わりにゾーンベースのルールを使用できるため、非常に複雑で分析が難しい一連のルールをすばやく生成できます。

ゾーンベースのルールを定義する際は、それらをできるだけ単純明快なものにするように努めてください。ゾーンベースのファイアウォール ポリシーの簡略性を維持するために、次の推奨事項を考慮してください。

- **許可**ルールのみを使用します。選択したアクションによって、一致したトラフィックに対する処理が決定されます。**拒否**ルールは解析が困難です。詳細については、ゾーンベースのファイアウォール ルールの Permit/Deny とアクションとの関係について （1203 ページ）を参照してください。
- **ドロップ**ルールと**パス**ルールは、標準のインターフェイス アクセス ルールと同等ですが、指定されたゾーン ペアに適用されます。[サービス（Services）] フィールドまたは [プロトコル（Protocol）] テーブルのいずれかを使用してトラフィックのタイプを識別できますが、[プロトコル（Protocol）] テーブルのみを使用することをお勧めします。トラフィックをドロップするには、アクション [ドロップ（Drop）] とともに [許可（Permit）] を指定します。
- 最初のトラフィックを検査する前に、それを通過させる必要はありません。たとえば、ゾーン間の HTTP トラフィックを許可する場合、必要な許可/インスペクション ルールは 1 つだけです。最初に許可/パス ルールを作成する必要はありません。Pass ルールを使用す

る場合で、リターン トラフィックを許可する場合には、リターン方向の Pass ルールも作成する必要があることに注意してください。実際には、通常、インスペクションルールのみを使用して、パスルールの作成を避けることができます。

- 許可/パスルールと許可/ドロップルールを使用して、標準のアクセスルールと同じ機能を実行できます。このため、アクセス ルール ポリシーを排除し、ゾーンベースのファイアウォール ルールだけを使用できます。

ただし、インターフェイス アクセス ルールの解析に使用できるツールは複数あり、Security Manager ではゾーンベース ルールとアクセス ルールに同じインターフェイス ロールを使用できるため、ゾーン ルール テーブルではなくアクセス ルール テーブルに Pass/Drop ポリシー（標準アクセス ルールの Permit/Deny）を作成する方が便利な場合があります。ゾーン ルール テーブルは、主にゾーンベースの Inspection および Content Filter ルールに使用します。

- セクションを使用して、各ゾーンペアのルールを編成します。セクションを使用すると、ペアのすべてのルールを簡単に参照できます。これは、ルールに順序の依存関係がある場合に重要になることがあります。セクションでの作業の詳細については、セクションを使用したルール テーブルの編成 （783 ページ）を参照してください。

ゾーンベースのファイアウォールルールの開発と適用

次に、ゾーンベースのファイアウォールルールを作成してネットワークに適用する方法の概要を示します。

- セキュリティ ゾーンに関してネットワークとそのサブネットワークを検討します。さまざまなゾーンのセキュリティ要件について考えます。一般的なガイドラインとして、セキュリティの観点から見たときに類似するルータ インターフェイスをグループ化します。
- あるゾーンから別のゾーンに移動するときに検査されるトラフィックのタイプを決定し、それぞれのタイプをどのように検査し、処理するかを決定します。
- これらの決定を実行するゾーンベースのファイアウォールルールを定義します。このプロセスには、ルール自体を定義する前に実行できる、またはルールの定義中に必要に応じて実行できる次の手順の一部またはすべてが含まれる場合があります。
  - 名前付きインターフェイス ロール オブジェクトを作成し、適切なインターフェイスとインターフェイス パターンをそれらのオブジェクトに割り当てることで、ゾーンを定義します。
  - 特定のレイヤ 4 プロトコルとポート、およびオプションで特定のネットワークとホストの Port Application Mapping（PAM; ポート アプリケーション マッピング）設定を定義/編集します。
  - レイヤ 7 プロトコル（HTTP、IMAP、インスタントメッセージング（IM）、ピアツーピア（P2P））のディープ パケット インスペクション（DPI）ポリシーを設定します。
  - プロトコル情報パラメータ マップを設定します。これらのパラメータ マップは IM アプリケーションと対話する DNS サーバを定義します。

- 検査アクションの接続、タイムアウト、およびその他の設定を定義する検査パラメータマップを設定します。
- URL ベース コンテンツ フィルタリングの WebFilter パラメータまたは WebFilter ポリシー マップを定義します。

ここでは、これらの手順に関する追加情報を提供します。

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）

ゾーンベースのファイアウォールルールの追加

この手順では、Security Manager でゾーンベースのファイアウォール ルールを設定する方法について説明します。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォール ルールの設定 （1261 ページ）
- マップ オブジェクトについて （388 ページ）
- ルールのイネーブル化とディセーブル化 （782 ページ）
- ルールの追加および削除 （766 ページ）
- ルールの移動とルール順序の重要性 （781 ページ）

ステップ 1 [Zone-based Firewall Rules] ページ （1272 ページ）へのアクセス方法を次に示します。

- （デバイスビュー）IOS ルータを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、テーブル内の任意の場所を右クリックして [行の追加（Add Row）] を選択し、[ゾーンベースのファイアウォールルールの追加（Add Zone Based Firewall Rule）] ダイアログボックスを開きます。

このダイアログボックスの詳細な説明については、ゾーンベースのファイアウォール ルールの追加と編集（1276 ページ）を参照してください。

ステップ 3 このルールの基本トラフィック フローを定義します。

（注） [Permit/Deny]、[Sources]、[Destinations]、および [Services] オプションは、詳細なアクション関連ポリシーを適用することで拡張でき、特定のゾーンのペア間の特定の方向に制限される単純なアクセス ルールの定義と考えることができます。

a) [Permit] または [Deny] で、このルールに一致するトラフィックをさらに処理するかどうかを選択します。詳細については、ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （1203 ページ）を参照してください。

b) 必要に応じて、送信元と宛先のホスト/ネットワークまたはセキュリティグループ（IOS 15.2(2)T+ および IOS-XE 3.5.x(15.2(1)S)+ のみ）を指定します。

デフォルトでは、トラフィック定義には、「any」（任意）の送信元から「any」（任意）の宛先へのパケットが含まれます。これらのフィールドを使用して、1 つ以上の送信元および宛先ホスト/ネットワークを指定することにより、この基本トラフィック定義を改良できます（詳細については、ネットワーク/ホストオブジェクトについて （391 ページ）およびネットワーク/ホストオブジェクトについて（391 ページ）を参照してください）。

c) IP や TCP など、トラフィックのタイプを示す 1 つ以上のサービス（プロトコル）を指定します。

複数のサービスを指定できますが、IP は通常、単独で使用されます（サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ） を参照。）

d) [From Zone] を指定します。このゾーンから発信したトラフィックだけが一致します。

e) [To Zone] を指定します。このゾーンに流れるトラフィックだけが一致します。

ゾーン/インターフェイス オブジェクトの詳細については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

（注） [開始ゾーン（From Zone）] と [終了ゾーン（To Zone）] は、「ゾーンペア」と呼ばれるものを構成します。

f) [Advanced] ボタンをクリックして時間範囲を追加するか、このゾーンベースのファイアウォール ルールに packet-fragment または established-connection 制限を適用します。

これらのオプションの詳細については、ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス （1281 ページ）を参照してください。

ステップ 4 ベースアクションを選択し、必要に応じて追加のパラメータを指定することにより、この定義に一致するトラフィックに適用されるアクションを指定します。

a) ベースアクションを選択します。

- [ドロップ（Drop）]：一致するトラフィックはサイレントにドロップされます。ドロップの通知は発信元ホストに送信されません。
- [ドロップして記録（Drop and Log）]：一致するトラフィックはドロップされ、syslog メッセージが生成されます。ドロップの通知は発信元ホストに送信されません。

- [通過（Pass）]：トラフィックは転送されます。 このアクションは単方向です。[Pass] では、指定した方向のトラフィックだけが許可されます。
- [通過させて記録（Pass and Log）]：トラフィックは転送され、syslog メッセージが生成されます。

（注） [通過（Pass）] アクションは、トラフィック内の接続またはセッションの状態を追跡しません。[通過（Pass）] は、一方向のトラフィックのみを許可します。リターン トラフィックを許可するには、対応するルールを定義する必要があります。Pass アクションは、IPSec ESP、IPSec AH、ISAKMP、およびその他の動作が予測可能なセキュアなプロトコルに役立ちます。ただし、ほとんどのアプリケーション トラフィックは、Inspect アクションを指定したゾーンベースのファイアウォール ルールでより適切に処理されます。

- [検査（Inspect）]：このオプションは、状態に基づくトラフィック制御を提供します。デバイスは TCP および UDP トラフィックに関する接続またはセッション情報を維持するため、接続要求に対するリターントラフィックが許可されます。

選択したレイヤ 4（TCP、UDP）プロトコルおよびレイヤ 7（HTTP、IMAP、インスタント メッセージング、およびピアツーピア）プロトコルに基づいたパケット インスペクションを適用する場合、このオプションを選択します。選択したプロトコルのポート アプリケーション マッピング（PAM）も編集でき、ディープ パケット インスペクション（DPI）を設定して、レイヤ 7 プロトコルの追加のプロトコル関連情報を指定できます。

- [コンテンツフィルタ（Content Filter）]：WebFilter パラメータマップまたは WebFilter ポリシーマップに基づいて HTTP コンテンツインスペクション（URL フィルタリング）を設定します。このアクションは一般に Web フィルタ ルールと同等ですが、ゾーンベースのファイアウォール ルールでは、HTTP ディープ パケット インスペクション（DPI）などの追加の詳細オプションがサポートされます。

ルータが HTTP 要求を代行受信し、プロトコル関連の検査を実行します。また、任意で、要求を許可するかブロックするかを決定するためにサードパーティ製サーバに接続します。WebFilter パラメータ マップを提供できます。このマップにより、ローカル URL リスト、および外部 SmartFilter（以前の N2H2）や Websense サーバからの情報に基づくフィルタリングを定義します。または、ローカル、N2H2、Websense、または Trend Micro フィルタリング データにアクセスする WebFilter ポリシー マップを提供できます。

b) コンテンツフィルタ以外のアクションについては、考慮される特定のトラフィックプロトコルを選択および編集できます。

[プロトコル（Protocol）] テーブルの横にある [選択（Select）] をクリックして [Protocol Selector] ダイアログボックス （1283 ページ）を開きます。1 つ以上のプロトコルを選択し、[>>] をクリックしてそれらを [選択済みのプロトコル（Selected Protocols）] リストに追加します。選択したプロトコルの [Port Application Mapping (PAM)] 設定を編集できます。詳細については、[Configure Protocol] ダイアログボックス （1284 ページ）を参照してください。

インスタント メッセージングおよび Stun-ice プロトコルでは、プロトコル情報パラメータ マップを選択できます。また、アクションとして [Inspect] が選択されている場合、一部のプロトコルでは詳細インスペクション ポリシー マップを選択できます。

詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）および プロトコル情報パラメータ マップの設定 （1237 ページ）を参照してください。

（注） [ドロップ（Drop）]、[ドロップして記録（Drop and Log）]、[通過（Pass）]、[通過させて記録（Pass and Log）] アクションのプロトコルを指定する必要はありません。[Protocol] テーブルを空のままにして、[送信元（Sources）]、[宛先（Destinations）]、および[サービス（Services）] パラメータに基づいてトラフィックを渡すかドロップできます。

c) 選択したアクションが [Content Filter] の場合は、URL フィルタリングを設定します。

1. [Protocol] フィールドの横の [Configure] をクリックして HTTP PAM 設定をカスタマイズし、HTTP 詳細インスペクション ポリシー マップを適用します。詳細については、[Configure Protocol] ダイアログボックス （1284 ページ）を参照してください。
2. [WebFilter Parameter Map] または [WebFilter Policy Map] を選択し、適切な WebFilter マップの名前を入力または選択します。詳細については、ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）を参照してください。

d) 選択したアクションが [Inspect] または [Content Filter] の場合は、カスタマイズした接続、タイムアウト、およびその他の設定のセットに適用するインスペクション パラメータ マップの名前を入力または選択します。詳細については、インスペクション パラメータ マップの設定 （1234 ページ）を参照してください。

ステップ 5 （任意）ルールの識別に役立つ説明を入力します。

ステップ 6 （任意）[Category] の下で、ルール テーブルでこのルールを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 7 [OK] をクリックして [ゾーンベースのファイアウォールルールの追加（Add Zone Based Firewall Rule）] ダイアログボックスを終了し、[ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] テーブルに戻ります。

新しいルールがテーブルにリストされます。

ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定

ルータのゾーンベースのファイアウォール ポリシーを設定する場合は、ルールのアクションとして [Inspect] を選択することで、トラフィックを検査するルールを定義できます。続いて、検査する特定のプロトコルを選択できます。

一部のプロトコルでは、ポリシーマップを選択して、基準に一致するパケットに対して詳細インスペクションを実行できます。これらのマップは、ルールの定義時に [ポリシーオブジェクトセレクタ（Policy Object Selector）] ダイアログボックスから設定するか、[Policy Object Manager] ウィンドウでいつでも設定できます（[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択）。ポリシー マップに加えて、インスペクションに対して設定できるパラメータ マップがいくつかあります。

- 詳細インスペクションを許可するプロトコルでは、関連ポリシーマップを選択できます。ポリシー マップには、ターゲットのトラフィックの一致条件を定義するクラス マップが含まれます。これらのポリシーマップを [Policy Object Manager] で作成するには、[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[検査（Inspect）] フォルダから、次の表に一覧表示されている使用可能なマップタイプの 1 つを選択し、ゾーンベースのファイアウォール ポリシーのポリシー マップの設定 （1239 ページ）に記載の詳細な使用方法情報を確認します。

詳細インスペクション ポリシー マップで使用するクラス マップの作成については、次の表の一致基準ダイアログボックスと、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ）を参照してください。これらのクラスマップは、[Policy Object Manager] の [マップ（Maps）]>[クラスマップ（Class Maps）]>[検査（Inspect）] フォルダにあります。

- アクションとして [Inspect]（または [Content Filter]）が選択されている場合は、ゾーンベースのファイアウォール ルールの追加と編集 （1276 ページ）のインスペクション パラメータ マップも適用できます。ゾーンベースのファイアウォール インスペクションには、いくつかの一般設定が含まれ、そのすべてに、ほとんどのネットワークに適切なデフォルト値があります。これらの設定のいずれかを調整する場合は、検査パラメータマップを作成する必要があります。[Policy Object Manager] で、[マップ（Maps）]>[パラメータマップ（Parameter Maps）]>[検査（Inspect）]>[検査パラメータ（Inspect Parameters）] を選択し、インスペクション パラメータ マップの設定 （1234 ページ）の詳細な使用状況情報を確認します。

表 *275 :* ゾーンベースのファイアウォール インスペクション ルールのポリシー オブジェクト

プロトコル	IOS ソフトウェアの最小バージョン	ポリシーマップ	クラスマップ	パラメータマップ	説明および一致基準の参照
インスタントメッセージング：AOL、ICQ、MSN Messenger、Windows Messenger、Yahoo Messenger	12.4(9)T	IM（ゾーンベースの IOS）	AOL ICQ MSN Messenger Windows Messenger Yahoo Messenger	Protocol Info	サービスのタイプ（テキストチャットまたはその他）に基づいてトラフィックを検査します。ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （1220ページ）を参照してください。 プロトコル情報パラメータ マップを選択して、検査しているトラフィックで使用されている DNS サーバも定義する必要があります。 プロトコル情報パラメータ マップの設定 （1237ページ）を参照してください。

プロトコル	IOS ソフトウェアの最小バージョン	ポリシーマップ	クラスマップ	パラメータマップ	説明および一致基準の参照
Peer-to-peer（P2P; ピアツーピア）：eDonkey、FastTrack、Gnutella、Kazaa2	12.4(9)T	P2P	eDonkey FastTrack Gnutella Kazaa2	なし（None）	ファイル名に基づいてトラフィックを検査します。 ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （1221ページ）を参照してください。
H.323	12.4(6)T	H.323（IOS）	H.323（IOS）	なし（None）	H.323 メッセージタイプに基づいてトラフィックを検査します。 H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1222ページ）を参照してください。
HTTP	12.4(6)T	HTTP（Zone ベースの IOS）	HTTP（IOS）	なし（None）	ヘッダーや本文の内容、ポートの誤用、トラフィックに Java アプレットが含まれているかどうかなど、広範な基準に基づいてトラフィックを検査します。 HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1222ページ）を参照してください。
Internet Message Access Protocol（IMAP） Post Office Protocol 3（POP3）	12.4(6)T	IMAP POP3	IMAP POP3	なし（None）	無効なコマンドまたはクリアテキストログインに基づいてトラフィックを検査します。 IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1226ページ）を参照してください。
SIP（Session Initiation Protocol）	12.4(6)T	SIP（IOS）	SIP（IOS）	なし（None）	広範な基準に基づいてトラフィックを検査します。 SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1226ページ）を参照してください。

プロトコル	IOS ソフトウェアの最小バージョン	ポリシーマップ	クラスマップ	パラメータマップ	説明および一致基準の参照
SMTP（Simple Mail Transfer Protocol）	12.4(6)T	SMTP	SMTP	なし（None）	データ長に基づいてトラフィックを検査します。 SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1228 ページ）を参照してください。
Stun-ice	12.4(9)T	なし	なし	Protocol Info	プロトコル情報パラメータマップを選択して、検査しているトラフィックで使用されている DNS サーバーを定義する必要があります。 プロトコル情報パラメータマップの設定 （1237ページ）を参照してください。
Sun Remote Procedure Call（RPC; リモート プロシージャ コール）	12.4(6)T	Sun RPC	Sun RPC	なし（None）	RPC プロトコル番号に基づいてトラフィックを検査します。 Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1232ページ）を参照してください。
SCTP（Stream Control Transmission Protocol）	12.4(6)T	SCTP	なし	なし	PPID 一致基準に基づいてトラフィックを検査します。 SCTP ポリシーマップの [一致条件とアクションの追加または編集（Add or Edit Match Condition and Action] ダイアログボックス （1102 ページ）を参照してください。
Diameter プロトコル	12.4(6)T	Diameter	Diameter	なし（None）	アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックを検査します。 Diameter クラスとポリシーマップの [一致条件（とアクション）の追加または編集（Add or Edit Match Condition (and Action)] ダイアログボックス （1106 ページ）を参照してください。
LISP（Locator and ID Separation Protocol）	12.4(6)T	LISP	なし	なし	アプリケーション ID、コマンドコード、および AVP に基づいてトラフィックを検査します。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- [Zone-based Firewall Rules] ページ （1272 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- マップ オブジェクトについて （388 ページ）

ゾーンベースのファイアウォール ポリシーのクラス マップの設定

[Add Class Map]/[Edit Class Map] ダイアログボックスを使用すると、同じタイプのポリシー マップで使用するクラスマップを定義できます。ダイアログボックスの名前は、作成するマップのタイプを示します。

クラス マップでは、アプリケーション固有の基準に基づいてトラフィックを定義します。次に、対応するポリシー マップ内のクラス マップを選択し、選択したトラフィックに適用するアクションを設定します。したがって、各クラスマップには、同じ方法（許可する、ドロップするなど）で処理するトラフィックを含める必要があります。

Cisco IOS ソフトウェアを実行しているデバイスのゾーンベースのファイアウォール ルールを設定する場合は、次の目的でクラス マップを作成できます。

- 12.4(6)T 以降では、H.323、HTTP、IMAP、POP3、SIP、SMTP、および Sun RPC タイプのトラフィックのインスペクション用のクラスを作成できます。Local、N2H2（SmartFilter）、WebSense のクラス タイプを使用して、Web フィルタリングのクラスを作成できます。一致基準の詳細については、次の項を参照してください。
  - H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1222 ページ）
  - HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1222 ページ）
  - IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1226 ページ）
  - SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1226 ページ）
  - SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1228 ページ）
  - Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1232 ページ）
  - ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1232 ページ）
  - N2H2 および Websense クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1233 ページ）

- 12.4(9)T 以降では、AOL、eDonkey、FastTrack、Gnutella、ICQ、Kazaa2、MSN Messenger、Windows Messenger、および Yahoo Messenger タイプのトラフィックのインスペクション用のクラスを作成できます。一致基準の詳細については、次の項を参照してください。
  - ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （1220 ページ）
  - ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス （1221 ページ）
- 12.4(20)T 以降では、トレンドポリシーオブジェクトを使用して Web フィルタリングのクラスを作成できます。Trend コンテンツ フィルタ クラス マップの一致基準については、次の表で説明します。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルの **[マップ（Maps）]>[クラスマップ（Class Maps）]** フォルダ内のフォルダにある任意のゾーンベースのクラスマップオブジェクトを選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *276 :* ゾーンベースのファイアウォール ポリシーの *[Add Class Maps]/[Edit Class Maps]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

要素	説明
[Match] テーブル 一致タイプ（Match Type） （Trend コンテンツ フィルタ クラス マップを除く）	[Match] テーブルには、クラス マップに含まれている基準が表示されます。各行には、各基準に一致する、または一致しないトラフィックを検査で検索するかどうか、および検査される基準と値が示されます。 テーブルの名前は、クラスに一致するためにトラフィックがすべての基準を満たす必要があるか（[Match All]）、またはリストされているいずれかの基準との一致で十分か（[Match Any]）を示します。HTTP（IOS）および SMTP クラスの場合は、すべて一致といずれか一致のどちらかを選択できます。[Match All] テーブルを使用しているときに、複数の基準を追加する場合は、いずれのトラフィックとも一致しない特性のセットを定義しないようにしてください。 **ヒント** [完全一致（Match All）] は、Cisco IOS Software バージョン 12.4(20)T 以降を実行しているデバイスでだけ動作します。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Criterion] ダイアログボックスに入力します。詳細については、上記で示している項を参照してください。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。
Trend コンテンツ フィルター一致基準	Trend コンテンツ フィルタ クラス マップの一致基準は、他のどのクラス マップとも異なります。テーブルに項目を追加する代わりに、リストから目的の項目を選択します。次のタブにある Trend-Micro 分類のいずれかの [Enable] チェックボックスをオンにします。トラフィックは、いずれかの選択項目と一致する場合にクラスと一致します。 • [Productivity Categories]：トラフィックを URL が属するカテゴリと照合します。たとえば、ギャンブルやポルノに関連するトラフィックをターゲットにできます。 • [Security Ratings]：トラフィックを、Trend-Micro によって割り当てられたセキュリティ レーティングと照合します。たとえば、広告に関連するトラフィックであるアドウェアをターゲットにできます。 これらのカテゴリまたはセキュリティ分類の詳細については、Trend-Micro のマニュアルを参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ゾーンベースのファイアウォールの IM アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用するさまざまな Instant Messenger（IM; インスタント メッセンジャ）アプリケーション クラス用の [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

次のタイプのトラフィックに対して一致を定義できます。

- [Any]：テキスト チャット トラフィックを除く、アプリケーションからの任意のタイプのトラフィック。
- [Text-chat]：テキスト チャット トラフィック。

ナビゲーション パス

AOL、ICQ、MSN Messenger、Windows Messenger、または Yahoo Messenger クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。 ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

ゾーンベースのファイアウォールの P2P アプリケーション クラス マップ：[Add Match Condition]/[Edit Match Condition] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用するさまざまな Peer-to-Peer（P2P; ピアツーピア）アプリケーション クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

ナビゲーション パス

eDonkey、FastTrack、Gnutella、または Kazaa2 クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *277*：ゾーンベースのファイアウォールの *P2P* アプリケーション クラス マップの *[Add Match Condition]/[Edit Match Condition]* ダイアログボックス

要素	説明
基準	照合の基準を選択します。 • [File Transfer]：ファイル転送トラフィックを照合します。 • [Search Filename]：ユーザが検索しているファイルの名前を照合します。この基準を使用して、ユーザが eDonkey を使用して特定のファイルを検索できないようにできます。 • [Text Chat]：eDonkey テキスト チャット トラフィックを照合します。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
ファイル名	トラフィックに関連付けられているファイルの名前。正規表現を使用して、名前のパターンを指定できます。正規表現の作成に使用できるメタ文字の詳細については、正規表現の作成に使用されるメタ文字 （1127 ページ） を参照してください。 **ヒント**　eDonkey にはファイル名は不要です。

H.323（IOS）クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

ゾーンベースのファイアウォール ポリシーで使用する H.323（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。H.323 プロトコル メッセージ タイプに基づいてトラフィックを照合できます。照合するメッセージを選択します。

ナビゲーション パス

H.323（IOS）クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

ゾーンベースのファイアウォール ポリシーで使用する HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。次の基準を使用できます。

- [Request/Response Body Length]、[Request Body Length]、[Response Body Length]：要求、応答、またはその両方の本文の長さが指定した数よりも小さいまたは大きいことを指定します。これにより、最小または最大のメッセージ長を設定できます。

- [Request/Response Body]、[Request Body]、[Response Body]：要求、応答、またはその両方の本文の照合に正規表現を適用します。
- [Request/Response Header]、[Request Header]、[Response Header]：ヘッダーと正規表現の照合、繰り返しフィールドのテスト、コンテンツ タイプのチェック、またはヘッダー内のレコードの合計の長さまたはレコード数のチェックを行うことができます。
- [Request/Response Protocol Violation]：非準拠 HTTP トラフィックを照合します。
- [Request Argument]、[Request URI]：要求メッセージ内の引数（パラメータ）または Uniform Resource Identifier（URI）の長さやコンテンツ（正規表現）を照合します。
- [Request Port Misuse]：特定のタイプのアプリケーションによるポートの誤使用を照合します。
- [Response Body Java Applet]：HTTP 接続の Java アプレットを照合します。
- [Response Header Status Line]：ヘッダー内のステータス行のコンテンツの照合に正規表現を適用します。

ナビゲーション パス

HTTP（IOS）クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *278 : HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス*

要素	説明
基準	照合する HTTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。

要素	説明
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
最小長	評価されるフィールドの最小長（バイト単位）。指定した数値よりも長さが小さい場合は、条件が一致します。
最大長	評価されるフィールドの最大長（バイト単位）。指定した数値よりも長さが大きい場合は、条件が一致します。
ヘッダーオプション	ヘッダー レコードのタイプ。レコード タイプを選択しない場合は、ヘッダー内のすべてのレコードにカウントまたは表現が適用されます。レコード タイプを選択した場合、それらの選択は選択したタイプのレコードにだけ適用されます。コンテンツ タイプまたは転送の符号化を選択した場合は、それらのタイプに関連する追加の選択を行うことができます。
要求メソッド	照合する要求メソッド。
値（コンテンツタイプ）	[Header Option] フィールドでコンテンツ タイプを選択した場合、次のタイプを選択できます。 • [Mismatch]：要求メッセージの受け入れフィールド値に照らして応答メッセージのコンテンツ タイプを検証します。 • [Unknown]：コンテンツ タイプは不明です。既知のすべての MIME タイプに照らして項目を評価する場合は、[Unknown] を選択します。 • [Violation]：コンテンツ タイプ定義と実際の本文のコンテンツ タイプが一致しません。

要素	説明
エンコード タイプ	[Header Option] フィールドで転送の符号化を選択した場合、次のタイプを選択できます。 • [All]：すべての転送符号化タイプ。 • [Chunked]：メッセージ本文は一連のチャンクとして転送され、各チャンクに固有のサイズ インジケータが含まれます。 • [圧縮（Compress）]：メッセージ本文は、UNIX ファイル圧縮を使用して転送されます。 • [Deflate]：メッセージ本文は、zlib 形式（RFC 1950）および deflate 圧縮（RFC 1951）を使用して転送されます。 • [GZIP]：メッセージ本文は、GNU zip（RFC 1952）を使用して転送されます。 • [Identity]：転送の符号化は実行されません。
Greater Than Count	ヘッダーで使用できるレコードの最大数。特定のヘッダー オプションを選択した場合、カウントはそれらのタイプのレコードに適用されます。特定のヘッダー オプションを選択しない場合、カウントはタイプにかかわらずヘッダー内のレコードの総数に適用されます。
正規表現	パターンマッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。
ポート誤使用	照合する要求ポート誤使用のタイプ。選択できるオプションは、次のとおりです。 • [Any]：リストされている誤使用タイプのいずれか。 • [IM]：インスペクションの対象となるインスタント メッセージング プロトコル アプリケーション。 • [P2P]：インスペクションの対象となるピアツーピア プロトコル アプリケーション。 • [Tunneling]：インスペクションの対象となるトンネリング アプリケーション（HTTPPort/HTTPHost）。

IMAP および POP3 クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用する Internet Message Access Protocol（IMAP）および Post Office Protocol 3（POP3）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

照合するトラフィックを識別するために次の基準を選択できます。

- [Invalid Command]：POP3 サーバまたは IMAP 接続で有効でないコマンドを照合します。
- [Login Clear Text]：パスワードがクリア テキストで提供されるセキュアでないログインを照合します。

ナビゲーション パス

IMAP または POP3 クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラスマップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

ゾーンベースのファイアウォール ポリシーで使用する SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

このダイアログボックスのフィールドは、選択した基準によって変わります。

ナビゲーション パス

SIP（IOS）クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *279 : SIP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス*

要素	説明
基準	照合するトラフィック基準を指定します。次の中から選択できます。 • [Protocol Violation]：プロトコルに違反するトラフィックを照合します。 • [Request/Response Header Options]：選択した要求または応答ヘッダー フィールドと正規表現を照合します。 • [Request Options]：選択した要求ヘッダー フィールドと要求メソッドを照合するか、正規表現を照合します。 • [Response Options]：選択した応答ヘッダー フィールドまたはステータス メッセージと正規表現を照合します。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
ヘッダー	要求または応答メッセージのヘッダーのタイプ。正規表現は、選択したタイプのヘッダーの内容と照合されます。

要素	説明
方法	検査する要求メソッドを次に示します。 • [ack]：前のメッセージが有効で受け入れられることを確認応答します。 • [bye]：コールを終了することを示します。 • [cancel]：保留中の要求を終了します。 • [info]：コールのシグナリング パスを経由する中間セッション シグナリング情報を伝えます。 • [invite]：コールをセットアップします。 • [message]：インスタント メッセージを送信します。 • [notify]：状態変更を加入者に通知します。 • [options]：別のユーザ エージェントまたはプロキシ サーバの容量を問い合わせます。 • [prack]：暫定応答メッセージの信頼性の高い転送を提供します。 • [refer]：受信者が要求で提供されている連絡先情報を使用してサードパーティに連絡する必要があることを示します。 • [register]：レコードのアドレスの SIP 要求の転送先とする連絡先アドレスを含みます。 • [subscribe]：1 つのイベントまたは一連のイベントに関する通知をあとで受け取ることを要求します。 • [update]：セッションのパラメータを更新することをクライアントに許可しますが、ダイアログの状態に影響はありません。
ステータス	正規表現が応答内のステータス行と照合されます。
正規表現	パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）]をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。

SMTP クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ゾーンベースのファイアウォール ポリシーで使用する SMTP クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

ヒント　12.4(20)T よりも前の Cisco IOS ソフトウェアを実行しているルータでは、[Data Length] 基準だけを使用できます。

このダイアログボックスのフィールドは、選択した基準によって変わります。次の基準を使用できます。

- [Data Length]：トラフィックのデータ長が指定した数値よりも大きいことを指定します。トラフィックのデータ長を照合して、SMTP 接続で転送されるデータが指定したバイト数を超えているかどうかを判断できます。デフォルトでは、インスペクションはデータ長を 20 未満に維持します。
- [Body Regular Expression]：正規表現を適用して、電子メール メッセージの本文のテキストおよび HTML のコンテンツ タイプおよびコンテンツ符号化タイプを照合します。7 ビットまたは 8 ビット符号化を使用するテキストまたは HTML だけがチェックされます。正規表現は、別の符号化タイプ（base64 や Zip ファイルなど）を使用するメッセージではスキャンできません。
- [Command Line Length]：指定した数値以下の ESMTP コマンドラインの長さを指定します。この基準を使用して、Denial of Service（DoS; サービス拒絶）攻撃を阻止します。
- [コマンドVerb（Command Verb）]：選択した SMTP または ESMTP コマンドに検査を制限します。SMTP の検査を設定すると、制限しない限り、すべてのコマンドが検査されます。
- [Header Length]：SMTP ヘッダーの長さが指定した数値よりも大きいことを指定します。この基準を使用して、ヘッダーの使用可能サイズを制限することで DoS 攻撃を阻止します。
- [Header Regular Expression]：正規表現を適用して、電子メール メッセージのヘッダーのコンテンツを照合します。たとえば、この基準を使用して件名、差出人、または宛先フィールドの特定のパターンをテストできます。
- [MIMEコンテンツタイプの正規表現（Mime Content-Type Regular Expression）]：正規表現を適用して、電子メール添付ファイルの Multipurpose Internet Message Exchange（MIME）コンテンツタイプと照合します。この基準を使用して、望ましくないタイプの添付ファイルの送信を防ぎます。
- [Mime Encoding]：検査する電子メール添付ファイルの MIME 符号化タイプを指定します。この基準を使用して、送信を制限する不明または非標準の符号化を識別します。
- [Recipient Address]：正規表現を適用して、SMTP RCPT コマンドの電子メール メッセージの受信者を照合します。この基準を使用して、存在しない受信者を検索します。これは、スパムの送信元の識別に役立つ場合があります。
- [Recipient Count]：電子メール メッセージの受信者数が指定した数を超えられないことを指定します。この基準を使用して、スパムの発信者が多数のユーザに電子メールを送信することを防ぎます。

- [無効な受信者数（Recipient Invalid Count）]：電子メールメッセージの無効な受信者の数が指定した数を超えられないことを指定します。これを使用して、スパマーが多数の一般的な名前に電子メールを送信し、実際のアドレスを狙っているのを防ぎます。SMTP は通常、アドレスが無効な場合に「no such address」メッセージを返信します。無効なアドレスの数を制限することで、これらのスパム発信者への応答を防ぐことができます。
- [Reply EHLO]：EHLO サーバ応答のサービス拡張パラメータを指定します。この基準を使用して、クライアントが特定のサービス拡張を使用することを防ぎます。
- [Sender Address]：正規表現を適用して、電子メール メッセージの送信者を照合します。この基準を使用して、既知のスパム発信者などの特定の送信者がデバイスを介して電子メール メッセージを送信することをブロックします。

ナビゲーション パス

SMTP クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *280 : SMTP* クラスの *[Add Match Criterion]/[Edit Match Criterion]* ダイアログボックス

要素	説明
基準	照合する SMTP トラフィック基準を指定します。基準については、上記で説明しています。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
可変フィールド 次のフィールドは、[Criterion] フィールドでの選択内容によって変わります。このリストは、表示されると想定されるフィールドのスーパーセットです。	
最大長	評価されるフィールドの最大長（バイト単位）。指定した数値よりも長さが大きい場合は、条件が一致します。

要素	説明
Greater Than Count	電子メール メッセージで許可される受信者または無効な受信者の最大数。指定した数値よりも数が大きい場合は、条件が一致します。
Verb Option User Defined Format （[Command Verb] 基準のみ）	検査する SMTP または ESMTP コマンド。[User Defined] を選択した場合は、電子メール メッセージの本文の単語に対応するテキスト文字列を入力する必要があります。単語には、スペースまたは特殊文字は使用できません。使用できるのは英数字だけです。
Service Extension Parameter User Defined Format （[EHLO応答（Reply EHLO）] 基準の場合）	検査する EHLO サーバ応答のサービス拡張パラメータ。よく知られたパラメータの 1 つを選択するか、[User Defined] を選択して [User Defined Format] フィールドでプライベート拡張を指定します。
Encoding Format User Defined Format	テストする MIME 符号化フォーマット。エンコーディングタイプは次のとおりです。 • [7-bit]：ASCII 符号化。 • [8-bit]：7 ビット ASCII の範囲外のオクテットを含む電子メール メッセージの交換に使用されます。 • [base64]：数値として扱い、base 64 表現に変換することでバイナリ データを符号化します。 • [quoted-printable]：印刷可能文字を使用して 8 ビット データを 7 ビット データ パス上に送信する符号化。 • [binary]：0 と 1 だけを使用した符号化。 • [unknown]：符号化タイプは不明です。 • [x-uuencode]：非標準の符号化。 • [user defined]：定義する符号化タイプ。[User Defined] を選択した場合は、探している符号化タイプを定義するテキスト文字列を入力する必要があります。
正規表現	パターン マッチングに使用する正規表現を定義する、正規表現オブジェクト。オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しい正規表現オブジェクトを作成できます。

Sun RPC クラス マップの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ゾーンベースのファイアウォールポリシーで使用するSunリモートプロシージャコール（RPC）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラスマップの一致基準と値を定義します。照合する RPC プロトコル番号を入力できます。プロトコル番号の詳細については、Sun RPC のマニュアルを参照してください。

ナビゲーション パス

Sun RPC クラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。

ナビゲーション パス

ローカル Web フィルタクラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラスマップの設定 （1217ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *281 :* ローカル *Web* フィルタ クラスの *[Add Match Criterion]/[Edit Match Criterion]* ダイアログボックス

要素	説明
基準	照合するトラフィック基準を指定します。次の中から選択できます。 • [Server Domain]：サーバの名前に基づいてトラフィックを照合します。選択する URLF Glob パラメータ マップでは、*.cisco.com や www.cisco.com などのサーバ ドメイン名を指定する必要があります。 • [URL Keyword]：URL 内のキーワードに基づいてトラフィックを照合します。キーワードは、URL 内の / 文字の間に出現する完結した文字列です。たとえば、URL セグメント www.cisco.com/en/US では、en と US がキーワードの例です。
タイプ（Type）	基準に一致するトラフィックをマップに含めることを指定します。
URLF Globパラメータマップ（URLF Glob Parameter Map）	照合する URL パターンを定義する URLF Glob パラメータ マップ オブジェクト。選択したオブジェクトに、選択した照合タイプに適したコンテンツがあることを確認します。 オブジェクトの名前を入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。

N2H2 および Websense クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス

N2H2（SmartFilter）および Websense Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックスを使用して、クラス マップの一致基準と値を定義します。使用可能な一致基準は、SmartFilter または Websense サーバからの応答の照合だけです。

ナビゲーション パス

N2H2 または Websense Web フィルタクラスの [クラスマップの追加（Add Class Maps）]/[クラスマップの編集（Edit Class Maps）] ダイアログボックスで、テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ） を参照してください。

関連項目

• マップ オブジェクトについて （388 ページ）
• ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）

- ゾーンベースのファイアウォール ルールについて （1197 ページ）

インスペクション パラメータ マップの設定

[Add Inspect Parameter Map]/[Edit Inspect Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーのインスペクション用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシールールのアクションを [Inspect] または [Content Filter] に設定する場合は、インスペクション パラメータ マップを選択して、インスペクション アクションの接続、タイムアウト、およびその他の設定を定義できます。ゾーンベースのファイアウォールルールのインスペクション パラメータ マップを選択しない場合は、これらの設定にデフォルト値が使用されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルから [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [検査（Inspect）] > [パラメータの検査（Inspect Parameters）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *282 : [Add Inspect Parameter Map]/[Edit Inspect Parameter Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
DNS Timeout	アクティビティがないときに DNS ルックアップ セッションが管理される時間の長さ（秒単位）。
ICMP Timeout	非アクティブな Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）セッションが維持される時間の長さ（秒単位）。

要素	説明
Max Incomplete Low Max Incomplete High	既存のハーフオープンセッションの数。これにより、ソフトウェアは、ハーフオープン状態のセッションの削除を開始（上限しきい値に達したとき）および停止（下限しきい値に達したとき）します。 [低（Low）]フィールドには、必ず[高（High）]フィールドに入力した数値よりも小さい数値を入力してください（たとえば、400 と 500 など）。デフォルトでは、ハーフオープン セッションは無制限です。
One Minute Low One Minute High	新しい未確立セッションの数。これにより、システムは、ハーフオープン状態のセッションの削除を開始および停止します。[Low] フィールドには、[High] フィールドに入力した数値よりも小さい数値を必ず入力してください。デフォルトは無制限です。
最大セッション数（Max Sessions）	ゾーン ペア上のインスペクション セッションの最大数（200 など）。デフォルトは無制限です。
TCP FINWAIT Timeout	ファイアウォールが FIN 交換を検出したあと、TCP セッション状態情報を保持する時間の長さ（秒単位）。TCP セッションを閉じる準備が整うと、FIN 交換が発生します。
TCP SYNWAIT Timeout	セッションをドロップする前に、TCP セッションが設定された状態に到達するのを待機する時間の長さ（秒単位）。
TCP Idle Timeout	セッションでアクティビティがない間、TCP セッションを維持する時間の長さ（秒単位）。

要素	説明
TCP Max Incomplete Hosts TCP Max Incomplete Block Time	TCP ホスト固有の Denial of Service（DoS; サービス拒絶攻撃）の検出と防止のしきい値とブロッキング時間（分単位）。 最大不完全ホストは、ソフトウェアがホストへのハーフオープン セッションの削除を開始する前に同時に存在できる、同じホスト宛先アドレスを持つハーフオープン TCP セッションの数です。同じ宛先ホスト アドレスを持つハーフオープン セッションの数が異常に多い場合は、ホストに対して DoS 攻撃が起動されていることを示している可能性があります。 しきい値を超えた場合、ハーフオープン セッションは、最大不完全ブロック時間に基づいてドロップされます。 • ブロック時間が 0 の場合、ソフトウェアは、ホストへの新規接続要求のたびに、ホストの最も古い既存のハーフオープン セッションを削除します。これにより、ホストに対するハーフオープン セッション数がしきい値を超えないことが保証されます。 • ブロック時間が 0 よりも大きい場合、ソフトウェアはホストのすべての既存のハーフオープン セッションを削除し、ホストに対するすべての新規接続要求をブロックします。ソフトウェアは、ブロック時間が経過するまですべての新規接続要求のブロックを継続します。 ソフトウェアは、指定されたしきい値を超えるたびに、またホストへの接続開始のブロッキングが開始または終了したときに、syslog メッセージを送信します。
UDP Idle Timeout	セッションでアクティビティがない間、UDP セッションを維持する時間の長さ（秒単位）。 ソフトウェアは、有効な UDP パケットを検出すると、新しい UDP セッションの状態情報を確立します。UDP はコネクションレス型サービスであるため、実際のセッションは存在しません。したがって、ソフトウェアは、パケット内の情報を調べることでセッションを見積もり、そのパケットが他の UDP パケットと似ているかどうか（類似の送信元アドレスまたは宛先アドレスを持っているなど）、および別の類似 UDP パケットの直後にそのパケットが検出されたかどうかを判断します。 ソフトウェアが、UDP アイドル タイムアウトで定義されている期間中に UDP セッションの UDP パケットを検出しなかった場合、ソフトウェアは、そのセッションの状態情報の管理を継続しません。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail	監査証跡メッセージを syslog サーバまたはルータに記録するかどうか。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

プロトコル情報パラメータ マップの設定

[Add Protocol Info Parameter Map]/[Edit Protocol Info Parameter Map] ダイアログボックスを使用して、ルータ上のゾーンベースのファイアウォール ポリシーの Instant Messaging（IM; インスタント メッセージング）アプリケーションまたは Stun-ice プロトコルのインスペクション用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシー ルールのアクションを [Inspect] に設定した場合は、AOL、ICQ、MSN Messenger、Windows Messenger、Yahoo Messenger、Stun-ice のいずれかのアプリケーションを設定するときにプロトコル情報パラメータ マップを選択する必要があります。プロトコル情報パラメータ マップでは、これらのアプリケーションと対話する DNS サーバを定義します。これにより、インスタント メッセンジャ アプリケーション エンジンは、インスタント メッセンジャ トラフィックを認識し、そのインスタント メッセンジャ アプリケーションに対して設定済みポリシーを適用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、目次から **[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [検査（Inspect）] > [プロトコル情報パラメータ（Protocol Info Parameters）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 283 : [Add Protocol Info Parameter Map]/[Edit Protocol Info Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
DNS Server Table	トラフィックが許可（および検査）または拒否される DNS サーバ。 • サーバを追加するには、[Add] ボタンをクリックし、[Add Server] ダイアログボックスに入力します（プロトコル情報パラメータの [Add DNS Server]/[Edit DNS Server] ダイアログボックス （1238 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

プロトコル情報パラメータの [Add DNS Server]/[Edit DNS Server] ダイアログボックス

[Add DNS Server]/[Edit DNS Server] ダイアログボックスを使用して、トラフィックが許可（および検査）または拒否される DNS サーバを識別します。これらのサーバは、ゾーンベースのファイアウォール ポリシーでこれらのサーバを必要とするプロトコルのインスペクションに使用するプロトコル情報パラメータ マップで定義されます。

次のいずれかのタイプを使用して、サーバを識別できます。

- [Server Name]：DNS サーバの名前。アスタリスク（*）をワイルドカードとして使用して、1 文字以上を照合できます。たとえば、cisco.com ドメイン上のすべての DNS サーバを識別する場合は、*.cisco.com を指定できます。

- [IP Address]：単一の DNS サーバの IP アドレス。
- [IP アドレス範囲（IP Address Range）]：開始アドレスと終了アドレスの間にある DNS サーバーを識別する IP アドレスの範囲。

ナビゲーション パス

[プロトコル情報パラメータマップの追加（Add Protocol Info Parameter Map）]/[プロトコル情報パラメータマップの編集（Edit Protocol Info Parameter Map）] ダイアログボックスで、サーバーテーブルの下にある [追加（Add）] ボタンをクリックするか、サーバーを選択して [編集（Edit）] ボタンをクリックします。プロトコル情報パラメータ マップの設定 （1237ページ） を参照してください。

ゾーンベースのファイアウォール ポリシーのポリシー マップの設定

ゾーンベースのファイアウォール ポリシーの [Add Policy Map]/[Edit Policy Map] ダイアログボックスを使用して、Cisco IOS ルータのゾーンベースのファイアウォール ポリシーで使用するインスペクション マップの一致基準と値を定義します。H.323（IOS）、HTTP（ゾーン ベース IOS）、IM（ゾーン ベース IOS）、IMAP、P2P、POP3、SIP（IOS）、SMTP、および Sun RPC インスペクションのポリシー インスペクション マップを作成できます。ダイアログボックスの名前は、作成しているマップのタイプを示します。

インスペクション マップを定義するときに、同じタイプのクラス マップを選択し、一致するトラフィックに対して実行するアクションを定義します。ポリシーマップを作成する前、またはポリシー マップの作成時に、必要なクラス マップを設定できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、コンテンツテーブルの **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect）]** フォルダで、[H.323 (IOS)]、[HTTP (Zone based IOS)]、[IM (Zone based IOS)]、[IMAP]、[P2P]、[POP3]、[SIP (IOS)]、[SMTP]、[Sun RPC] のいずれかの項目を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）

フィールド リファレンス

表 *284* : ゾーンベースのファイアウォール ポリシーの *[Add Policy Maps]/[Edit Policy Maps]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Match All] テーブル	[Match All] テーブルには、ポリシー マップに含まれているクラス マップ、およびこのクラスに一致するトラフィックに適用するアクションが表示されます。トラフィックがこのクラスと照合される場合、選択したクラスマップで定義されているすべての基準を満たす必要があります。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1240 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて（310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス

ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]、[Edit Match Condition and Action] ダイアログボックスを使用して、インスペクションのクラスマップを選択し、クラスに一致するトラフィックに対して実行するアクションを定義します。このダイアログボックスは、H.323（IOS）、HTTP（ゾーンベース IOS）、IM（ゾー

ン ベース IOS）、IMAP、P2P、POP3、SIP（IOS）、SMTP、Sun RPC、Web フィルタのタイプのポリシー マップに使用されます。

このダイアログボックスのフィールドは、定義しているポリシーマップのタイプによって若干異なります。

ナビゲーション パス

ゾーンベースのファイアウォールポリシーの [ポリシーマップの追加（Add Policy Maps）]/[ポリシーマップの編集（Edit Policy Maps）] ダイアログボックスで、一致テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。ゾーンベースのファイアウォール ポリシーのポリシー マップの設定 （1239 ページ） を参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *285* : ゾーンベースのファイアウォール ポリシーの *[Add Match Condition and Action]*、*[Edit Match Condition and Action]* ダイアログボックス

要素	説明
一致タイプ（Match Type）	クラスマップを選択していることを指定します。ゾーンベースのファイアウォール ポリシーのポリシー マップを作成する場合は、クラスマップを定義する必要があります。
クラスマップ P2P、IM、および Web フィルタ クラスマップ タイプ	作成しているポリシーマップ タイプのクラスマップの名前です。[選択（Select）] をクリックしてリストからマップを選択するか、新しいクラスマップオブジェクトを作成します。 P2P、IM、および Web フィルタ ポリシー マップの場合は、作成しているポリシーマップのタイプも選択する必要があります。たとえば、P2P マップでは、[eDonkey]、[FastTrack]、[Gnutella]、[Kazaa2] から選択する必要があります。IM（ゾーン ベース IOS）マップでは、[AOL]、[MSN Messenger]、[Yahoo Messenger]、[Windows Messenger]、[ICQ] から選択する必要があります。Web フィルタ マップでは、[Local]、[N2H2]、[WebSense]、[Trend] から選択する必要があります。

要素	説明
操作	選択したクラスに一致するトラフィックに対してデバイスが適用するアクション。

ゾーンベースのファイアウォールポリシーのコンテンツフィルタリング マップの設定

ルータのゾーンベースのファイアウォールポリシーを設定する場合は、ルールのアクションとして [Content Filter] を選択することで、Web コンテンツをフィルタリングするルールを定義できます。

Web コンテンツをフィルタリングするには、特定のマップオブジェクトを設定する必要があります。マップオブジェクトは、ルールを定義しているときに [ポリシーオブジェクトセレクタ（policy object selector）] ダイアログボックスから設定するか、[Policy Object Manager] ウィンドウ（[管理（Manage）]> [ポリシーオブジェクト（Policy Objects）] を選択） でいつでも設定できます。

必要なマップのタイプは、コンテンツのフィルタリングに使用している手法と、使用している Cisco IOS ソフトウェア バージョンによって異なります。デバイスにローカルに定義されている URL リストに基づいてコンテンツをフィルタリングするか、SmartFilter（N2H2）、Websense、Trend Micro などの外部フィルタリング サーバを使用できます。

ヒント　外部サーバを使用する場合は、選択したサーバ タイプ用のマニュアルに基づいて、サーバを適切に設定する必要があります。Trend Micro サーバを使用する場合は、[Zone Based Firewall] ページ（[Firewall] > [Settings] > [Zone Based Firewall] を選択）の [Content Filtering] タブで、サーバの詳細を指定し、製品を登録して証明書をダウンロードする必要があります。[Zone-based Firewall Rules] ページ （1272 ページ）を参照してください。

次に、ゾーンベースのコンテンツ フィルタリングに使用されるマップ オブジェクトの要件を示します。

- 12.4(20)T よりも前のリリースを実行しているデバイスでは、URL フィルタ パラメータ マップを作成する必要があります。[Policy Object Manager] で、[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [ウェブフィルタ（Web Filter）] > [URLフィルタ（URL Filter）] を選択し、URL フィルタ パラメータ マップの設定 （1251 ページ）の詳細な使用状況情報を確認します。
  - 許可されるホストのリスト（許可リストの一部）および拒否されるホストのリスト（ブロックリストの一部）を使用して、ルータでローカルフィルタリングを実行するには、[ローカルフィルタリング（Local Filtering）] タブでリストを作成します。最初に Web アクセス要求がこれらのリストと比較されてから、要求が外部フィルタリング サーバに送信されます（外部フィルタリング サーバを設定している場合）。これらのリストには、完全なドメイン名（www.cisco.com など）、または部分的な名前

（cisco.com など）が含まれますが、パスやページ名は含まれず、ワイルドカードは使用できません。

- SmartFilter（N2H2）または Websense サーバを使用するには、使用しているサーバのタイプとそのアドレス情報を [External Filter] タブで設定します。サーバとの通信を制御するその他の設定も設定できます。URL フィルタ パラメータ マップを使用して Trend Micro サーバを設定することはできません。

- リリース 12.4(20)T 以降を実行しているデバイスでは、Web フィルタポリシーマップを使用するアプローチが推奨されます。Web フィルタ ポリシー マップはより複雑ですが、柔軟性が向上し、Trend Micro フィルタリング サーバにアクセスできます。[Policy Object Manager] で、[マップ（Maps）]>[ポリシーマップ（Policy Maps）]>[ウェブフィルタ（Web Filter）]>[ウェブフィルタ（Web Filter）] を選択し、Web フィルタ マップの設定 （1258 ページ）の詳細な使用状況情報を確認します。

Web フィルタ ポリシー マップには、他のタイプのマップが組み込まれます。ポリシー マップを作成するには、次のマップ タイプの 1 つ以上が必要です。

- - パラメータ マップ：デフォルト設定を使用しない場合は、[Add Web Filter Map]/[Edit Web Filter Map] ダイアログボックスの [Parameters] タブで、さまざまなタイプの Web フィルタリングのパラメータ マップを選択できます。SmartFilter（N2H2）または Websense を使用している場合は、パラメータ マップがこれらのサーバを識別するため、マップを選択する必要があります。ローカル フィルタリングおよび Trend Micro フィルタリングでは、パラメータマップでいくつかの一般設定を設定します。その中で最も重要な設定は、URL がブロックされるときにメッセージまたは Web ページを表示するかどうかです。[Policy Object Manager] の [マップ（Maps）]>[パラメータマップ（Parameter Maps）]>[ウェブフィルタ（Web Filter）] フォルダで、ローカル、N2H2、Trend、および Websense のパラメータマップを検索できます。詳細な使用方法については、ローカル Web フィルタ パラメータ マップの設定 （1245 ページ）、N2H2 または WebSense パラメータ マップの設定 （1246 ページ）、またはTrend パラメータ マップの設定 （1250 ページ）を参照してください。

（注） Trend Micro サーバ情報は、[Zone Based Firewall] ページ（[Firewall]>[Settings]>[Zone Based Firewall] を選択）の [Content Filtering] タブで設定します。[Zone-based Firewall Rules] ページ （1272 ページ）を参照してください。

- - 一致条件のクラスマップ：これらのクラスマップでは、ターゲットとするトラフィックのタイプを定義し、実行するアクションを指定します。フィルタリングのタイプ（[Local]、[SmartFilter/N2H2]、[Websense]、または [Trend Micro]）を選択し、ターゲットのトラフィックを識別するクラスマップを指定し、そのトラフィックに対して実行するアクション（[Allow]、[Reset] など）を選択します。[Policy Object Manager] の [マップ（Maps）]>[クラスマップ（Class Maps）]>[ウェブフィルタ（Web Filter）] フォルダで、ローカル、N2H2、Trend、および Websense のクラスマップを検索できます。

これらのクラスマップ設定は、フィルタリングのタイプによって異なります。

[Local Filtering]：Local WebFilter クラスマップは、ターゲットにするドメイン名または URL キーワードを指定する 1 つ以上の URLF Glob パラメータのリストです。URL キーワードは、URL 内のスラッシュ（/）文字で囲まれた任意のテキスト文字列です。これらのクラスマップは、Web フィルタポリシーで許可する URL リスト（許可リストの一部）と拒否する URL リスト（ブロックリストの一部）を定義するのに役立ちます。リストごとに別々のマップを作成します。詳細な使用方法については、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ）、ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1232 ページ）、および URLF Glob パラメータ マップの設定 （1255 ページ）を参照してください。

[SmartFilter (N2H2)] または [Websense Filtering]：N2H2 および Websense のクラスマップでは、任意のサーバー応答を一致基準として定義します。詳細な使用方法については、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ）を参照してください。

[Trend Micro Filtering]：Trend クラスマップでは、Trend Micro によって定義されている、ターゲットにするさまざまなプロダクティビティカテゴリおよびセキュリティレーティングを選択できます。詳細な使用方法については、ゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ）を参照してください。

コンテンツ フィルタリングの定義に使用されるマップ以外に、コンテンツ フィルタ ルールの次のマップも設定できます。

- インスペクション パラメータ マップ：ゾーンベースのファイアウォール インスペクションには、いくつかの一般設定が含まれ、そのすべてに、ほとんどのネットワークに適切なデフォルト値があります。これらの設定のいずれかを調整する場合は、インスペクション パラメータ マップを作成できます。[Policy Object Manager] で、[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [検査（Inspect）] > [検査パラメータ（Inspect Parameters）] を選択し、インスペクション パラメータ マップの設定 （1234 ページ）の詳細な使用状況情報を確認します。

- HTTP ポリシーマップ：Web フィルタリングに加えて個々の HTTP パケットに詳細インスペクションを使用する場合は、ゾーンベースのファイアウォール ルールの追加と編集 （1276 ページ）の [アクション（Action）] セクションの [プロトコル（Protocol）] フィールドの横にある [設定（Configure）] をクリックして、HTTP ポリシーマップを設定できます。HTTP ポリシーマップには、照合するトラフィックのタイプを定義し、実行するアクションを定義する HTTP クラスマップが組み込まれます。たとえば、Java アプレットを含むトラフィックをターゲットにできます。[Policy Object Manager] で、[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [検査（Inspect））] > [HTTP（ゾーンベースのIOS）（HTTP (Zone Based IOS)）] を選択し、ゾーンベースのファイアウォール ポリシーのポリシーマップの設定 （1239 ページ）、HTTP（IOS）クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1222 ページ）、およびゾーンベースのファイアウォール ポリシーのクラス マップの設定 （1217 ページ）の詳細な使用状況情報を確認します。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）

- [Zone-based Firewall Rules] ページ （1272 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- マップ オブジェクトについて （388 ページ）

ローカル Web フィルタ パラメータ マップの設定

[Add Local Parameter Map]/[Edit Local Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーのローカル Web フィルタリング用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシー ルールのアクションを [Content Filter] に設定する場合は、（[Parameter] タブでパラメータ タイプに [Local] を選択するときに）ローカル Web フィルタ パラメータ マップを組み込む Web フィルタ ポリシー マップを選択できます。Web フィルタ ポリシー マップの詳細については、Web フィルタ マップの設定 （1258 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルから **[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] > [ローカル（Local）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 286 : [Add Local Web Filter Parameter Map]/[Edit Local Web Filter Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。

要素	説明
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべてのURL要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。
Block Page	ブロックしているページにユーザがアクセスしようとした場合に、ユーザに表示する Web ページ。次の中から選択できます。 • [None]：ユーザには何の情報も示されません。 • [Message]：編集ボックスに入力したテキスト メッセージがユーザに表示されます。 • [リダイレクトURL（Redirect URL）]：編集ボックスに入力した URL にユーザーがリダイレクトされます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）]ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

N2H2 または WebSense パラメータ マップの設定

[Add N2H2 Parameter Map]/[Edit N2H2 Parameter Map] または [Add Websense Parameter Map]/[Edit Websense Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーの Smartfilter（N2H2）または Websense Web フィルタリング用のパラメータ マップを定義します。ゾーンベースのファイアウォール ポリシー ルールのアクションを [Content Filter] に設定する場合は、（[Parameter] タブでパラメータ タイプに [N2H2] または [Websense] を選択するときに）N2H2 または Websense Web フィルタ パラメータ マップを組み込む Web フィルタ ポリシー マップを選択できます。Web フィルタ ポリシー マップの詳細については、Web フィルタ マップの設定 （1258 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルの [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）]

フォルダから [N2H2] または [WebSense] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 287 : [Add N2H2 Parameter Map]/[Edit N2H2 Parameter Map] または [Add Websense Parameter Map]/[Edit Websense Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
URL Filtering Server Table	URL フィルタリング サーバのリストとそれらの属性。 • サーバを追加するには、[Add] ボタンをクリックし、[Add External Filter] ダイアログボックスに入力します（[Add External Filter]/[Edit External Filter] ダイアログボックス （1249 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。

要素	説明
Block Page	ブロックしているページにユーザがアクセスしようとした場合に、ユーザに表示する Web ページ。次の中から選択できます。 • [None]：ユーザには何の情報も示されません。 • [Message]：編集ボックスに入力したテキスト メッセージがユーザに表示されます。 • [リダイレクトURL（Redirect URL）]：編集ボックスに入力した URL にユーザーがリダイレクトされます。
送信元インターフェイス（Source Interface）	TCP 接続がシステムと URL フィルタリング サーバ間で確立された場合に、送信元 IP アドレスとして使用される IP アドレスのインターフェイス。
Maximum Cache Entries	分類キャッシュに格納されるエントリの最大数。デフォルトは 5000 です。
Cache Life Time	エントリがキャッシュ テーブルに残る時間の長さ（時間数）。デフォルトは 24 です。
Maximum Requests	保留中の要求の最大数。範囲は、1 ～ 2147483647 です。デフォルトは 1000 です。
Maximum Responses	バッファできる HTTP 要求の最大数。範囲は、0 ～ 20000 です。デフォルトは 200 です。
Truncate Hostname Truncate Script Parameters	URL を切り捨てるかどうかを次のように指定します。： • オプションを選択しない場合、URL は切り捨てられません。 • ホスト名を選択した場合、URL はドメイン名の末尾で切り捨てられます。 • スクリプト パラメータを選択した場合、URL は、URL 内の左端の疑問符で切り捨てられます。 **ヒント** 両方のオプションを選択できますが、そのような指定方法は論理的ではありません。
Enable Server Log	HTTP 要求に関する情報を URL フィルタリングサーバーのログサーバーに送信するかどうか。この情報には、URL、ホスト名、送信元 IP アドレス、および宛先 IP アドレスが含まれます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）F を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add External Filter]/[Edit External Filter] ダイアログボックス

[Add External Filter]/[Edit External Filter] ダイアログボックスを使用して、URL フィルタリング サーバを N2H2、Websense、または URL フィルタ パラメータ マップ ポリシー オブジェクトに追加します。

ナビゲーション パス

次のいずれかのダイアログボックスで、サーバーテーブルの下の [追加（Add）] ボタンをクリックするか、サーバーを選択して [編集（Edit）] ボタンをクリックします。

- [Add N2H2 Parameter Map]/[Edit N2H2 Parameter Map] または [Add Websense Parameter Map]/[Edit Websense Parameter Map] ダイアログボックス N2H2 または WebSense パラメータ マップの設定 （1246 ページ）を参照してください。
- [Add URL Filter Parameter Map]/[Edit URL Filter Parameter Map] ダイアログボックス URL フィルタ パラメータ マップの設定 （1251 ページ）を参照してください。

フィールド リファレンス

表 288 : [Add External Filter]/[Edit External Filter] ダイアログボックス

要素	説明
サーバ	URL フィルタリング サーバの完全修飾ドメイン名または IP アドレス。
[ポート（Port）]	要求をリスニングするポート。
Retransmission Count	サーバからの応答がないときに、ルータがルックアップ要求を再送信する回数。値の範囲は 1 ～ 10 です。
タイムアウト（Timeout）	サーバからの応答をルータが待機する秒数。範囲は、1 ～ 300 です。
外部	サーバがネットワークの外部にあるかどうか。

Trend パラメータ マップの設定

[Add Trend Parameter Map]/[Edit Trend Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーの Trend Micro Web フィルタリング用のパラメータ マップを定義します。ゾーン ベースのファイアウォール ポリシールールのアクションを [Content Filter] に設定する場合は、（[Parameter] タブでパラメータ タイプに [Trend] を選択するときに）Trend Web フィルタ パラメータ マップを組み込む Web フィルタ ポリシー マップを選択できます。Web フィルタ ポリシー マップの詳細については、Web フィルタ マップの設定（1258 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルから **[マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] > [傾向（Trend）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 289 : [Add Trend Parameter Map]/[Edit Trend Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。

要素	説明
Block Page	ブロックしているページにユーザがアクセスしようとした場合に、ユーザに表示する Web ページ。次の中から選択できます。 • [None]：ユーザには何の情報も示されません。 • [Message]：編集ボックスに入力したテキスト メッセージがユーザに表示されます。 • [リダイレクトURL（Redirect URL）]：編集ボックスに入力した URL にユーザーがリダイレクトされます。
Maximum Requests	保留中の要求の最大数。範囲は、1 ～ 2147483647 です。デフォルトは 1000 です。
Maximum Responses	バッファできる HTTP 要求の最大数。範囲は、0 ～ 20000 です。デフォルトは 200 です。
Truncate Hostname	ドメイン名の末尾で URL を切り捨てるかどうか。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

URL フィルタ パラメータ マップの設定

[Add URL Filter Parameter Map]/[Edit URL Filter Parameter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーで使用するインスペクション マップのパラメータ、および一致基準と値を定義します。

ゾーンベースのファイアウォール ポリシールールのアクションを [Content Filter] に設定する場合は、URL フィルタ パラメータ マップを選択して、Web フィルタリング パラメータと一致基準を定義できます。ただし、ルータが Cisco IOS Software Release 12.4(20)T 以降を実行している場合、適切なサーバータイプ（ローカル、N2H2、Trend、または Websense）のパラメータおよびクラスマップとともに Web フィルタポリシーマップを設定することを推奨します。詳細については、Web フィルタ マップの設定 （1258 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に目次から [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Web フィルタ（Web Filter）] > [URL フィルタ（URL Filter）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 290 : [Add URL Filter Parameter Map]/[Edit URL Filter Parameter Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。
[Local Filtering] タブ このタブのフィールドでは、ローカル URL フィルタリングのプロパティを定義します。	

要素	説明
[許可リスト登録ドメイン（Permitlisted Domains）] テーブルと [ブロックリスト登録ドメイン（Blocklisted Domains）] テーブル	これらのテーブルでは、ソフトウェアが外部 URL フィルタリング サーバにアクセスしないドメイン名を定義します。許可リストにあるドメイン名は常に許可されます。ブロックリストにあるドメイン名は常にブロックされます。これらのリストを使用して、制限なしで許可する（自社の Web サイトなど）または完全にブロックする（ポルノサイトなど）ドメイン全体を識別します。 ドメイン名は完全な形式（www.cisco.com など、ホスト名を含む）にしたり、部分的な形式（cisco.com など）にしたりできます。部分的な名前の場合、そのドメイン上のすべての Web サイト ホストが、許可されるか、または拒否されます。また、ホストの IP アドレスを入力することもできます。 • ドメイン名を追加するには、[Add] ボタンをクリックし、[Add Server] ダイアログボックスに入力します（URL フィルタ パラメータの [Add URL Domain Name]/[Edit URL Domain Name] ダイアログボックス （1255 ページ）を参照）。 • ドメイン名を編集するには、ドメインを選択し、[Edit] ボタンをクリックします。 • ドメイン名を削除するには、ドメインを選択し、[Delete] ボタンをクリックします。
Enable Alert	ステートフル パケット インスペクションのアラート メッセージをコンソールで生成するかどうか。
Enable Audit Trail	URL 情報を syslog サーバまたはルータのログに記録するかどうか。
Enable Allow Mode	URL フィルタリング プロセスが URL フィルタリング データベースに接続していない場合に、URL 要求を許可するかまたはブロックするか。許可モードがオンの場合、一致しないすべての URL 要求が許可され、オフの場合は、一致しないすべての URL 要求がブロックされます。
[External Filtering] タブ このタブのフィールドでは、外部 URL フィルタリング サーバのプロパティを定義します。	

要素	説明
サーバー タイプ Server Table	設定している外部URL フィルタリング サーバのタイプ（[SmartFilter (N2H2)] または [Websense]）。 • サーバを追加するには、[Add] ボタンをクリックし、[Add External Filter] ダイアログボックスに入力します（[Add External Filter]/[Edit External Filter] ダイアログボックス （1249 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit]ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
送信元インターフェイス（Source Interface）	TCP 接続がシステムと URL フィルタリング サーバ間で確立された場合に、送信元 IP アドレスとして使用される IP アドレスのインターフェイス。
Maximum Cache Entries	分類キャッシュに格納されるエントリの最大数。デフォルトは5000です。
Maximum Requests	保留中の要求の最大数。範囲は、1 ～ 2147483647 です。デフォルトは 1000 です。
Maximum Responses	バッファできる HTTP 要求の最大数。範囲は、0 ～ 20000 です。デフォルトは 200 です。
Truncate Hostname Truncate Script Parameters	URL を切り捨てるかどうかを次のように指定します。: • オプションを選択しない場合、URL は切り捨てられません。 • ホスト名を選択した場合、URL はドメイン名の末尾で切り捨てられます。 • スクリプト パラメータを選択した場合、URL は、URL 内の左端の疑問符で切り捨てられます。 12.4(15)T よりも前のソフトウェア リリースを実行しているデバイスには切り捨てオプションを選択しないでください。選択すると検証エラーが発生します。 ヒント　両方のオプションを選択できますが、そのような指定方法は論理的ではありません。
Enable Server Log	HTTP 要求に関する情報を URL フィルタリングサーバーのログサーバーに送信するかどうか。この情報には、URL、ホスト名、送信元 IP アドレス、および宛先 IP アドレスが含まれます。

要素	説明
その他のフィールド	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

URL フィルタ パラメータの [Add URL Domain Name]/[Edit URL Domain Name] ダイアログボックス

[URLドメイン名の追加（Add URL Domain Name）] ダイアログボックスを使用して、許可リスト（許可）またはブロックリスト（拒否）に Web サイトのドメイン名を追加します。

ドメイン名は完全な形式（www.cisco.com など、ホスト名を含む）にしたり、部分的な形式（cisco.com など）にしたりできます。部分的な名前の場合、そのドメイン上のすべての Web サイト ホストが、許可されるか、または拒否されます。また、ホストの IP アドレスを入力することもできます。

ナビゲーション パス

[URLフィルタパラメータマップの追加（Add URL Filter Parameter Map）]/[URLフィルタパラメータマップの編集（Edit URL Filter Parameter Map）] ダイアログボックスで、許可リストまたはブロックリストテーブルの下にある [追加（Add）] ボタンをクリックするか、名前を選択して [編集（Edit）] ボタンをクリックします。URL フィルタ パラメータ マップの設定 （1251 ページ） を参照してください。

URLF Glob パラメータ マップの設定

[Add URLF Glob Parameter Map]/[Edit URLF Glob Parameter Map] ダイアログボックスを使用して、ローカル Web フィルタ クラス マップの URL のインスペクション用のパラメータ マップを定義します。

1 つの URLF Glob に、ブロックまたは許可する URL のセグメントだけが含まれている必要があります。許可またはブロックリスト URL のクラスマップを作成することが目的です。続い

て、ローカル Web フィルタ ポリシー マップを定義して、識別された URL を許可またはブロックできます。

1 つの URLF Glob は、次のタイプの URL セグメントの 1 つに制限する必要もあります。

- URL のサーバ名に出現する文字列。これには、サーバ名とネットワークのドメイン名が含まれます。たとえば、www.cisco.com などです。
- URL キーワードに出現する文字列。これは、URL 内の / 文字の間に出現する文字列、またはファイル名です。たとえば、URL セグメント www.cisco.com/en/US/ では、en と US の両方がキーワードです。index.html など、URL 内のファイル名もキーワードと見なされます。

URLF Glob では、/、{、}、? の文字を使用できません。

サーバ名または URL キーワードが一致するためには、ワイルドカード メタ文字を使用して可変文字列パターンを指定しないかぎり、URL 内の文字列が URLF Glob に含まれる文字列と完全に一致する必要があります。サーバ名または URL キーワードのパターン マッチングには、次のメタ文字を使用できます。

- *（アスタリスク）。0 個以上の任意の文字のシーケンスと一致します。たとえば、*.edu は教育機関ドメインにあるすべてのサーバと一致し、hack* を使用すると www.example.com/hacksite/123.html をブロックできます。
- [abc]（文字クラス）。カッコ内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。たとえば、[abc] は a、b、または c と一致しますが、A、B、または C とは一致しません。このため、www.[ey]xample.com を使用して、www.example.com と www.yxample.com をブロックできます。
- [a-c]（文字範囲クラス）。範囲内の任意の文字と一致します。文字のマッチングでは大文字と小文字が区別されます。[a-z] は、任意の小文字と一致します。文字と範囲を混合できます。たとえば、[abcq-z] は、a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、[a-cq-z] も同じです。ダッシュ（-）文字は、角カッコ内の最後または最初の文字である場合にだけリテラルになります（[abc-] または [-abc]）。
- [0-9]（数字範囲クラス）。カッコ内のすべての数字とマッチします。たとえば、[0-9] は 0、1、2、3、4、5、6、7、8、または 9 と一致します。このため、www.example[0-9][0-9].com を使用して、www.example01.com、www.example33.com、および www.example99.com などをブロックできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にコンテンツテーブルから [マップ（Maps）] > [パラメータマップ（Parameter Maps）] > [Webフィルタ（Web Filter）] > [URLFグロブパラメータ（URLF Glob Parameters）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ローカル Web フィルタ クラスの [Add Match Criterion]/[Edit Match Criterion] ダイアログボックス （1232 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *291 : [Add URLF Glob Parameter Map]/[Edit URLF Glob Parameter Map]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 200 文字を使用できます。

値	ターゲットとしている URL のサーバ ドメインまたはキーワード。1 種類の Glob だけを入力できます（すべてのサーバ ドメイン、またはすべての URL キーワードは指定できますが、両方の混合はできません）。
	複数のエントリを含める場合は、エントリを改行で区切ります。たとえば、次のエントリは、すべての政府または教育機関の Web サーバを識別します。
	`*.gov`
	`*.edu`

カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）]ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

Web フィルタ マップの設定

[Add Web Filter Map]/[Edit Web Filter Map] ダイアログボックスを使用して、ルータのゾーンベースのファイアウォール ポリシーで使用するインスペクション マップのパラメータ、および一致基準と値を定義します。

ゾーンベースのファイアウォール ポリシールールのアクションを [Content Filter] に設定する場合は、Web フィルタ ポリシー マップを選択して、Web フィルタリング パラメータと一致基準を定義できます。Web フィルタポリシーマップは、Cisco IOS ソフトウェアリリース 12.4(20)T 以降を実行しているルータでだけ選択できます。Cisco IOS Software Release 12.4(6)T から 12.4(20)T までを実行しているルータにゾーンベースのファイアウォールを設定する場合は、Web フィルタ ポリシー マップの代わりに URL フィルタ パラメータ マップを設定する必要があります。詳細については、URL フィルタ パラメータ マップの設定 （1251 ページ）を参照してください。

ローカル Web フィルタリングとサーバベースの Web フィルタリングの組み合わせを設定できます。これを設定するには、使用しているサーバのタイプおよび一致基準に適したパラメータ マップと、ローカルおよびサーバ クラス マップの適切な組み合わせを選択する必要があります。異なるタイプのサーバのクラスマップとパラメータ マップは組み合わせないでください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから **[マップ（Maps）] > [ポリシーマップ（Policy Maps）] > [Webフィルタ（Web Filter）] > [Webフィルタ（Web Filter）]** を選択します。テーブル内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- マップ オブジェクトについて （388 ページ）
- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 292 : [Add FTP Map]/[Edit FTP Map] ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 40 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大200 文字を使用できます。

要素	説明
[パラメータ（Parameters）] タブ	
パラメータ タイプ パラメータマップ	Web フィルタ ポリシー マップに含めるパラメータ マップのタイプ。パラメータ マップを選択しない場合は [None] を選択します。 特定のパラメータタイプを選択する場合は、[パラメータ マップ（Parameter Map）] フィールドにパラメータマップの名前を入力します。[選択（Select）] をクリックしてリストからマップを選択するか、新しいパラメータマップオブジェクトを作成します。
[Match Condition and Action] タブ [Match All] テーブルには、ポリシー マップに含まれているクラス マップ、およびこのクラスに一致するトラフィックに適用するアクションが表示されます。トラフィックがこのクラスと照合される場合、選択したクラス マップで定義されているすべての基準を満たす必要があります。 • 基準を追加するには、[Add] ボタンをクリックし、[Match Condition and Action] ダイアログボックスに入力します（ゾーンベースのファイアウォール ポリシーおよび Web フィルタ ポリシーの [Add Match Condition and Action]/[Edit Match Condition and Action] ダイアログボックス （1240 ページ）を参照）。 • 基準を編集するには、基準を選択し、[Edit] ボタンをクリックします。 • 基準を削除するには、基準を選択し、[Delete] ボタンをクリックします。	
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

デフォルトのドロップ動作の変更

デフォルトでは、ゾーン間のすべてのトラフィックは明示的に許可されていないかぎりドロップされます。ただし、この項の説明に従って、このデフォルト動作を変更できます。

Security Managerは、ゾーンベースのファイアウォールルールに対して指定されているパラメータ（クラス、パラメータ、およびポリシー マップを含みます）を、ルータが認識する一連のIOS コマンドに変換します。これらはいわゆる「CLI」（コマンドライン インターフェイス）コンフィギュレーション コマンドであり、[ツール（Tools）] > [設定のプレビュー（Preview Configuration）] を選択することで別のウィンドウでプレビューできます。詳細については、設定のプレビュー （535ページ）を参照してください。また、ゾーンベースのルールと設定のトラブルシューティング （1267ページ）では、ゾーンベースのファイアウォールのCLIコマンドの例について説明しています。

この説明の目的では、これらのコマンドのうち最も重要なコマンドは **policy-map** です。このコマンドは、ゾーンの各ペアにゾーンポリシーを適用するために使用します。つまり、任意のゾーンペアに対して、トラフィック（クラス）とアクションを定義するすべてのルールが1つの policy-map で適用されます。さらに、Security Manager は、現在の **class-default** クラスを policy-map のクラスリストの末尾に追加して、ゾーンルールで処理されないすべてのパケットをキャプチャします。

デフォルトの class-default はドロップです。このクラスを各 policy-map に追加すると、ゾーン間のトラフィックの暗黙的なドロップが実現されます。ただし、前に述べたように、このデフォルト動作は任意のゾーンペアに対して変更できます。たとえば、すべての不一致トラフィックを渡すことを選択したり、デフォルトを [Drop and Log] に変更して、既存のルールで一致しないトラフィックを判断したりできます。

（注） デフォルト動作のオプションは、[Drop]、[Drop and Log]、[Pass]、および [Pass and Log] だけです。

デフォルト ポリシーでパケットを引き続きドロップする場合は、Security Manager で何も行う必要がありません。このルールは自動的に生成されます。ゾーンペアのデフォルト動作を変更しない場合は、**Permit any any IP** ルール（つまり、ゾーンベースのファイアウォール ルールの追加と編集 （1276ページ）の [一致（Match）] : 許可（Permit）、[送信元（Sources）] : any、[宛先（Destinations）] : any、[サービス（Services）] : IP）を指定し、[アクション（Action）] として [ドロップして記録（Drop and Log）]、[通過（Pass）]、または [通過させて記録（Pass and Log）] を選択する必要があります。このルールがゾーンペアのルールのリストの最後にあることも確認する必要があります。Security Manager は、これを目的の class-default ルールとして解釈します。

ゾーンベースのルール テーブルに大量のルールが含まれる場合は、このルールがゾーン ペアの他のすべてのルールよりもあとにあることを確認するのが難しい場合があります。この確認作業を軽減するのに使用できる手法をいくつか示します。

- セクションを使用して、ゾーンペアごとに1つのセクションでテーブルを編成します。これにより、ゾーンペアのルールを並べること、また class-default ルールが最後にくるようにすることができます。セクションでの作業の詳細については、セクションを使用したルール テーブルの編成 （783 ページ）を参照してください。
- [デフォルト（Default）] スコープに class-default ルールを含む共有ゾーンベースルールポリシーを作成し、デバイスのローカル ゾーンベース ルール ポリシーでこのルールを継承します。共有ポリシーの継承と作成の詳細については、ルールの継承または継承の解除（269 ページ）および新しい共有ポリシーの作成 （278 ページ）を参照してください。

ゾーンベースのファイアウォール ルールの設定

[ゾーンベースのファイアウォール（Zone Based Firewall）]設定ページを使用して、参照されないゾーンの識別、VPN インターフェイス用のゾーンの指定、WAAS サポートの有効化または無効化、Trend Micro のサーバーと証明書情報のメンテナンス、およびグローバルログ設定の指定をします。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

関連項目

- [Zone Based Firewall] ページ （1262 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

ステップ 1 [Zone Based Firewall] ページ （1262 ページ）へのアクセス方法を次に示します。

- （デバイスビュー）IOS デバイスを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 （任意）[Zones] タブで、参照されないゾーンを追加、編集、および削除します。

[Zones] タブには、デバイスに定義されているすべての参照されないゾーン、つまり関連付けられているインターフェイス、ルール、またはポリシーのないゾーンがリストされます。参照されないゾーンは、通常、デバイス検出時に検索および表示されますが、名前を付けた「空の」ゾーンをこの手順で作成することもできます。

ステップ 3 （任意）[VPN] タブで、VPN トラフィックに対して設定されたゾーンの名前を指定します。

このゾーンは、このルータのゾーンベースのファイアウォール ルールで動的 VPN トラフィックを処理できるようにします。詳細については、ゾーンベースのファイアウォールポリシーでの VPN の使用 （1201 ページ）を参照してください。

ステップ 4 （任意）[WAAS] タブで、[WAASの有効化（Enable WAAS）] を選択して Wide Area Application Services 相互運用性を有効にします。

このオプションがイネーブルになっていない場合、WAASデバイスによって最適化されたパケットは、TCP ハンドシェイク時に WAAS によって TCP パケット シーケンス番号が増加したため、ドロップされる可能性があります。この動作は、IOS デバイスによって潜在的攻撃と見なされる可能性があります。

ステップ 5 （任意）[コンテンツフィルタの設定（Content Filter Settings）] タブで、Trend Micro ベースのコンテンツ フィルタリング用のサーバー 0 設定を指定します。

Trend Micro ベースのコンテンツ フィルタリングを使用するには、[Zone Based Firewall] ページのこのタブで、Trend Micro サーバの接続情報を設定する必要があります。このタブでは、Trend Micro の登録および証明書のダウンロードへのリンクも提供されます。この形式のコンテンツ フィルタリングを利用するには、Trend Micro とのアクティブなサブスクリプションを取得し、有効なサブスクリプション証明書をダウンロードして IOS デバイスにインストールする必要があります。

詳細については、[Zone Based Firewall] ページ - [Content Filter] タブ （1265 ページ）を参照してください。

ステップ 6 （任意）[Global Parameters (ASR)] タブで、ASR デバイスに固有のグローバルなログ関連設定を設定できます。

- [Log Dropped Packets]：このオプションを選択して、デバイスによってドロップされたすべてのパケットを記録し、syslog ロギングをイネーブルにして情報を表示する必要があります。
- [Log Flow export timeout rate]：フローが期限切れになるか、またはタイムアウトしたあとに NetFlow ログが作成されます。フローが期限切れになるまでアクティブでいられる期間に関して時間制限を設定することが重要です。この値は、フローが期限切れになるまでアクティブなままでいることのできる最大分数です。この値は、1 ～ 3600 の任意の整数で、デフォルトは 30 です。
- [Log Flow export destination IP]：フロー データの送信先となる、NetFlow Collector の IP アドレスまたはホスト名。
- [Log Flow export destination port]：NetFlow Collector によってモニタされる、フロー データの UDP ポート。

[Zone Based Firewall] ページ

[Zone Based Firewall] ページを使用して、参照されないゾーンの設定と識別、VPN ゾーンの指定、WAAS サポートのイネーブル化またはディセーブル化、Trend Micro のサーバと証明書情報のメンテナンス、およびサポートされる ASR デバイスでのグローバル ログ設定の指定を行います。

次のタブについては、このページの表で説明されています。

- **ゾーン**
- **VPN**
- **WAAS**
- **Global Parameters (ASR)**

[コンテンツフィルタリング（Content Filtering）] タブの詳細については、[Zone Based Firewall] ページ - [Content Filter] タブ （1265 ページ）を参照してください。

ナビゲーション パス

[Zone Based Firewall] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。

関連項目

- ゾーンベースのファイアウォール ルールの設定 （1261 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォールルールの追加 （1210 ページ）

フィールド リファレンス

表 293 : [Zone Based Firewall] ページ

要素	説明
[Zones] タブ	このタブには、参照されないゾーン、つまり関連付けられているインターフェイス、ルール、またはポリシーのないゾーンをリストする [Zones] テーブルが表示されます。参照されないゾーンは、通常、デバイス検出時に検索および表示されますが、名前を付けた「空の」ゾーンをこの手順で作成することもできます。 [Zones] テーブルには、参照されないゾーンごとに次の情報がリストされます。 • [Zone]：ゾーン/インターフェイス ロールの名前。 • [Content]：ゾーンに割り当てられているインターフェイス。 • [Description]：ゾーンに関してユーザが指定するコメント。 このテーブルにゾーンを追加するには、[Add Row] ボタンをクリックし、[Zone] ダイアログボックスでゾーン名を指定します。
[VPN] タブ	このタブには、[VPN Zone] フィールドが表示されます。このフィールドのゾーン エントリによって、動的 VPN トラフィックをこのルータ上のゾーンベースのファイアウォール ルールで処理できます。このゾーンの詳細については、ゾーンベースのファイアウォールポリシーでの VPN の使用 （1201 ページ）を参照してください。 VPN トラフィックが通過するゾーンを入力または選択します。
[WAAS] タブ	このタブには、[Enable WAAS] チェックボックスが表示されます。このオプションをオンにすると、Wide Area Application Services 相互運用性がイネーブルになります。 このオプションがイネーブルになっていない場合、WAAS デバイスによって最適化されたパケットは、TCP ハンドシェイク時に WAAS によって TCP パケット シーケンス番号が増加したため、ドロップされる可能性があります。この動作は、IOS デバイスによって潜在的攻撃と見なされる可能性があります。
[Content Filtering] タブ	このタブには、Trend Micro ベースのコンテンツ フィルタリングのサーバ設定と証明書リンクが表示されます。詳細については、[Zone Based Firewall] ページ - [Content Filter] タブ （1265 ページ）を参照してください。

要素	説明
[Global Parameters (ASR)] タブ	このタブには、ASR デバイスに固有のグローバルなロギング関連設定が表示されます。これらの設定は、次のように設定します。 • [Log Dropped Packets]：このオプションを選択して、デバイスによってドロップされたすべてのパケットを記録し、syslog ロギングをイネーブルにして情報を表示する必要があります。 • [Log Flow export timeout rate]：フローが期限切れになるか、またはタイムアウトしたあとに NetFlow ログが作成されます。フローが期限切れになるまでアクティブでいられる期間に関して時間制限を設定することが重要です。この値は、フローが期限切れになるまでアクティブなままでいることのできる最大分数です。この値は、1 ～ 3600 の任意の整数で、デフォルトは 30 です。 • [Log Flow export destination IP]：フロー データの送信先となる、NetFlow Collector の IP アドレスまたはホスト名。 • [Log Flow export destination port]：NetFlow Collector によってモニタされる、フロー データの UDP ポート。

[Zone Based Firewall] ページ - [Content Filter] タブ

Trend Micro ベースのコンテンツ フィルタリングを使用するには、[Zone Based Firewall] ページのこのタブで、Trend Micro サーバの接続情報を設定する必要があります。このタブでは、Trend Micro の登録および証明書のダウンロードへのリンクも提供されます。この形式のコンテンツ フィルタリングを利用するには、Trend Micro とのアクティブなサブスクリプションを取得し、有効なサブスクリプション証明書をダウンロードして IOS デバイスにインストールする必要があります。

ナビゲーション パス

[Zone Based Firewall] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、デバイスセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォール設定の編集（Edit Firewall Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。

関連項目

- [Zone-based Firewall Rules] ページ （1272 ページ）

- ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定（1242 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォールルールの追加 （1210 ページ）

フィールド リファレンス

表 294 : [Zone Based Firewall] ページ - [Content Filter] タブ

要素	説明
Trend Micro Server Settings	
Cache-entry-lifetime (hrs)	Trend Micro サーバーへのルックアップ要求がルータのローカル URL キャッシュ テーブルに残る時間数。許可される範囲は 0 ～ 120 です。デフォルト値は 24 です。
Cache-size (KBytes)	ルータのローカル URL キャッシュで使用する最大メモリ量。許可される範囲は 0 ～ 120,000 KB です。デフォルト値は 250 です。
サーバー（Server）	Trend Micro URL フィルタリング サーバの完全修飾ドメイン名または IP アドレス。
HTTP ポート（HTTP Port）	Trend Micro サーバが HTTP 要求をリスニングするポート。デフォルトは 80 です。
HTTPS ポート（HTTPS Port）	Trend Micro サーバが HTTPS 要求をリスニングするポート。デフォルトは 443 です。
Retransmission Count	サーバからの応答がないときに、ルータがルックアップ要求を再送信する回数。指定できる範囲は 1 ～ 10 です。
Retransmission Timeout	サーバからの応答をルータが待機する秒数。範囲は 1 ～ 300 です。
アラート（Alert）	ステートフル パケット インスペクション メッセージが syslog にコピーされるかどうか。
Trend Micro Server Certificate Download Links	
Link to download certificates	Cisco IOS ルータに Trend URL フィルタリング サポートの信頼できる CA の証明書をインストールするページを開きます。
Link for product registration	製品ライセンス登録のページを開きます。製品認証キーを入力し、ルータを登録する必要があります。

[Add Zone]/[Edit Zone] ダイアログボックス

[Add Zone]/[Edit Zone] ダイアログボックスを使用して、参照されないゾーン（関連付けられているインターフェイス、ルール、またはポリシーのないゾーン）を追加および編集します。

ナビゲーション パス

[Add Zone]/[Edit Zone] ダイアログボックスにアクセスするには、次のいずれかを行います。

- （デバイスビュー）デバイスを選択し、デバイスセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。[ゾーン（Zones）] テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行項目を右クリックして [行の編集（Edit Row）] を選択します。
- （ポリシービュー）ポリシーセレクタから **[ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]** を選択します。テーブル内を右クリックして [行の追加（Add Row）] を選択するか、行項目を右クリックして [行の編集（Edit Row）] を選択します。
- （マップビュー）デバイスを右クリックし、**[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]** を選択します。

[ゾーン（Zone）] フィールドにゾーン名を入力するか、[選択（Select）] をクリックして [インターフェイスセレクタ（Interfaces Selector）] ダイアログボックスからゾーンを選択します。

関連項目

- [Zone Based Firewall] ページ （1262 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォール ルールの設定 （1261 ページ）

ゾーンベースのルールと設定のトラブルシューティング

ゾーンベースのファイアウォール ルールは強力ですが、複雑でもあります。ゾーン ルールを使用して、アクセル ルール、インスペクション ルール、および Web フィルタ ルールを 1 種類のファイアウォール ルールで置換できます。ゾーンベースのファイアウォール ルールでは非常に多くのアクションを実行できるため、アクセス コントロール リスト（ACL）、クラスマップ、およびポリシーマップの構造といった、これらのアクションから生成された設定では、多くの異なるタイプのコンフィギュレーション コマンドが使用されます。（たとえばアクセス ルールとは異なり）ゾーンベースのファイアウォール ルールと設定の行との間には、1 対 1 対応はありません。

この複雑さを示すために、ここではゾーンベースのファイアウォール ルールと、そのルールから生成された設定の関係を説明します。ゾーンベースのファイアウォール ルールを作成および展開するために、このトピックの情報を理解する必要はありません。ただし、CLI（コマンド

ラインインターフェイス）に精通している場合、またはルールによって望ましくない結果が生成される場合は、ゾーンベースのファイアウォールルールを理解およびトラブルシューティングするのにこの情報が役立つ場合があります。

次の図に示すルールのセットについて考えます。これらのルールは単一のゾーン ペアのポリシーを構成し、内部ゾーンから外部ゾーンに移動するトラフィックに影響します。これは、インターネットに向かう内部ネットワークからのトラフィックです。ルールでは、次のアクションを定義します。

- 10.100.10.0/24 および 10.100.11.0/24 ネットワークからのすべてのトラフィックをドロップする。
- 10.100.12.0/24 ネットワークからのすべての FTP および FTPS トラフィックをドロップする。
- 任意のネットワークからのすべてのピアツーピア トラフィックをドロップする。
- すべての FTP/FTPS トラフィック（すでにドロップされている 10.100.12.0/24 からのトラフィックを除く）を検査（および許可）する。
- 追加の詳細インスペクション ポリシー マップを使用して、すべての HTTP トラフィックを検査する。
- 最後に、残りのすべての TCP/UDP トラフィックの汎用インスペクションを実行する。

図 *29 :* ゾーン ペアのゾーンベース ルールの例

これらのルールを展開すると、Security Manager は次の設定を生成します。太字は、設定に続く説明の参照用に追加されています。

A.

```
class-map type inspect http match-any HTTPcmap
 match req-resp protocol-violation
 match request port-misuse any
!
```

B.

```
policy-map type inspect http HTTPpmap
 class type inspect http HTTPcmap
  reset
  log
!
```

C.

```
class-map type inspect CSM_ZBF_CLASS_MAP_1
 match access-group name CSM_ZBF_CMAP_ACL_1
!
```

D.

```
class-map type inspect match-any CSM_ZBF_CMAP_PLMAP_1
 match protocol ftp
 match protocol ftps
!
```

E.

```
class-map type inspect CSM_ZBF_CLASS_MAP_2
 match access-group name CSM_ZBF_CMAP_ACL_2
 match class-map CSM_ZBF_CMAP_PLMAP_1
!
```

F.

```
class-map type inspect match-any CSM_ZBF_CLASS_MAP_3
 match protocol bittorrent
 match protocol edonkey
 match protocol fasttrack
 match protocol icq
 match protocol kazaa2
!
```

G.

```
class-map type inspect CSM_ZBF_CLASS_MAP_4
 match protocol http
!
```

H.

```
class-map type inspect match-any CSM_ZBF_CLASS_MAP_5
 match protocol tcp
 match protocol udp
!
```

I.

```
policy-map type inspect CSM_ZBF_POLICY_MAP_1
 class type inspect CSM_ZBF_CLASS_MAP_1
  drop
 class type inspect CSM_ZBF_CLASS_MAP_2
  drop
 class type inspect CSM_ZBF_CLASS_MAP_3
  drop
class type inspect CSM_ZBF_CMAP_PLMAP_1
  inspect
 class type inspect CSM_ZBF_CLASS_MAP_4
  inspect
  service-policy http HTTPpmap
 class type inspect CSM_ZBF_CLASS_MAP_5
  inspect
 class class-default
  drop
!
```

J.

```
zone security Inside
zone security Outside
zone-pair security CSM_Inside-Outside_1 source Inside destination Outside
 service-policy type inspect CSM_ZBF_POLICY_MAP_1
!
interface GigabitEthernet0/1
 ip address dhcp
 zone-member security Inside
!
interface GigabitEthernet0/2
 ip address dhcp
 zone-member security Outside
!
```

K.

```
ip access-list extended CSM_ZBF_CMAP_ACL_1
 permit ip 10.100.10.0 0.0.0.255 any
 permit ip 10.100.11.0 0.0.0.255 any
!
```

L.

```
ip access-list extended CSM_ZBF_CMAP_ACL_2
 permit ip 10.100.12.0 0.0.0.255 any
!
```

次のリストでは、Security Manager のルールが device-configuration コマンドにどのように変換されるかを説明し、このルールとコマンドの関係を理解できるようにします。リストの番号は、Security Manager のルール テーブルのルール番号に対応します（前の図を参照）。

1. このルールでは、10.100.10.0/24 ネットワークからのすべてのトラフィックがドロップされます。[Permit]、[Source]、[Destination]、[Service] の各フィールドは、（K）で定義されている CSM_ZBF_CMAP_ACL_1 という名前の ACL の最初のアクセス コントロール エントリ（ACE）の作成に使用されます。この ACL は、（I）で定義されているポリシー マップ

CSM_ZBF_POLICY_MAP_1 の最初の廃棄ルールを定義する、（C）で定義されているクラス マップ CSM_ZBF_CLASS_MAP_1 から参照されます。

ポリシー マップ（I）は、（J）のゾーン サービス ポリシーの定義に使用されます。このポリシー マップはすべてのルールがゾーン ペアに割り当てられる方法であるため、（J）は再び言及されていません。

1. このルールでは、10.100.11.0/24 ネットワークからのすべてのトラフィックがドロップされます。このルールは、（K）で定義されている ACL に ACE を追加することで、ルール 1 に結合されています。残りの設定は、ルール 1 と同じです。このため、ルール 1 と 2 は、基本的にデバイス設定の単一のルールになります。

2. このルールでは、10.100.10.12/24 ネットワークからのすべての FTP/FTPS トラフィックがドロップされます。[Permit]、[Source]、[Destination]、[Service] の各フィールドは、（L）で定義されている CSM_ZBF_CMAP_ACL_2 という名前の ACL の作成に使用されます。[Protocol] テーブルでは、FTP および FTPS プロトコルを指定する、（D）で定義されているクラス マップ CSM_ZBF_CMAP_PLMAP_1 が生成されます。ACL および FTP/FTPS クラス マップは、（E）で定義されている新しいクラス マップ CSM_ZBF_CLASS_MAP_2 で使用されます。これにより、送信元とプロトコルの組み合わせに基づいてトラフィックの特徴付けが完了します。最後に、（E）は、ポリシー マップ（I）で第 2 のルールとして参照されています。

3. このルールは、Bittorrent、eDonkey、FastTrack、ICQ、または Kazaa2 のいずれかのプロトコルを使用する送信元からのピアツーピア トラフィックをドロップします。このルールにより、内部サーバがこれらのサービスのファイル共有ソースとして使用されることを防ぎます。ルールはデフォルト IP サービスのすべての送信元と宛先に適用されるため、ACL は不要です。代わりに、設定は（F）で定義されているクラス マップ CSM_ZBF_CLASS_MAP_3 から開始します。このクラス マップは、ポリシー マップ（I）の第 3 の廃棄ルールで参照されています。

4. このルールは、任意の送信元から任意の宛先への FTP/FTPS トラフィックを検査します。これは、これらのサービスが許可されることを意味します。ルール 3 は、ルール 5 よりも上にあるため 10.100.12.0/24 ネットワークからの FTP/FTPS トラフィックをすでにドロップしています。このため、これらのルールの組み合わせは、FTP/FTPS トラフィックが 10.100.12.0/24 以外のすべての送信元に対して検査されることを意味します。[Protocol] テーブルでは、ルール 3 に対するのと同じプロトコルを指定するため、新しいクラス マップは不要です。代わりに、ポリシー マップ（I）は、クラス マップ（D）を単純に第 4 のクラス タイプとして参照しますが、今回は Inspect アクションを伴います。

5. このルールは、HTTP トラフィックを検査し、HTTPpmap という名前の詳細インスペクション ポリシー マップを適用します。HTTPpmap ポリシー マップ（B）は、トラフィックがクラス マップ HTTPcmap（A）で定義されている基準と一致する場合に実行するアクションを定義します。これらのマップでは、HTTP プロトコルに違反する HTTP 接続、またはポートを誤用する HTTP 接続をリセット（ドロップ）し、syslog エントリを生成する必要があることを指定します（プロトコル違反とポートの誤用は、サービス妨害（DoS）攻撃の特徴を示している可能性があります）。（A）と（B）の組み合わせにより、このポリシーの詳細検査ルールが定義されます。

追加のクラス マップ CSM_ZBF_CLASS_MAP_4 は、HTTP プロトコル（G）を指定するために必要です。次に、ポリシー マップ（I）の第 5 のクラス タイプ ルールは、インスペクションのクラス マップ（G）を参照し、service-policy コマンドは詳細インスペクションのポリシー マップ（B）を参照します。

1. このルールは、TCP/UDP トラフィックに対する汎用インスペクションを提供し、内部ネットワークからインターネットおよびその戻り方向の他の TCP/UDP トラフィックを許可および検査します。（H）で定義されているクラス マップ CSM_ZBF_CLASS_MAP_5 は、[Protocols] テーブルから生成されています。このクラス マップは、ポリシー マップ（I）の最後から 2 つめのルールになります。
2. 最後に、ポリシー マップ（I）の最後の class-default ルールとして出現する自動ルールがあります。このルールは、ポリシー マップ（I）で参照されているクラス マップの 1 つと一致しないトラフィックをドロップします。たとえば、内部ネットワークからインターネットへの ICMP トラフィックは許可されません。さまざまな class-default ルールの設定方法については、デフォルトのドロップ動作の変更 （1260 ページ）を参照してください。

[Zone-based Firewall Rules] ページ

ゾーンベースのファイアウォールルールは、「ゾーン」と呼ばれるインターフェイスのグループ間でファイアウォールポリシーを一方向に適用します。つまり、インターフェイスはゾーンに割り当てられ、特定のインスペクションポリシーがゾーン間を一方向に移動するトラフィックに適用されます。

ゾーンは、トラフィックがネットワークの別の領域に移動するときに特定の制限の対象となる境界を定義します。ゾーン間のデフォルトのゾーンベース ファイアウォール ポリシーは、[すべて拒否（deny all）] です。このため、ポリシーが明示的に設定されていない場合は、ゾーン間のすべてのトラフィックがブロックされます。

（注） バージョン 4.21 以降、Cisco Security Manager では、すべてのアグリゲーション サービス ルータ、統合サービスルータ、埋め込み型サービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体が終了します。

[Zone Based Firewall Rules] ページには、現在設定されているゾーンベースのファイアウォール ルールのリストが表示され、ルールを追加、編集、および削除できます。

ヒント ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

ナビゲーション パス

[Zone Based Firewall Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）デバイスを選択し、ポリシーセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。
- （マップビュー）デバイスを右クリックし、[ファイアウォールポリシーの編集（Edit Firewall Policies）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）] を選択します。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォールルールの追加 （1210 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 295 : [Zone Based Firewall Rules] ページ

要素	説明
番号	この番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。
許可（Permit）	ルールでトラフィックが許可されるか拒否されるかを示します。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。

要素	説明
ソース	ルールのトラフィックの送信元。ネットワークまたはセキュリティグループにすることができます。複数のエントリは、テーブルセル内の個別の行に表示されます。 • [ネットワーク（Network）]：このルールの送信元として定義されているネットワーク、ホスト、または IP アドレスオブジェクトおよび定義。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについて （391 ページ）およびポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーションサービスルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックなどに制限します。
宛先	ルールのトラフィックの宛先。ネットワークまたはセキュリティグループにすることができます。複数のエントリは、テーブルセル内に個別の行に表示されます。 • [ネットワーク（Network）]：このルールの宛先として定義されているネットワーク、ホスト、またはIPアドレスオブジェクトおよび定義。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについて （391 ページ）およびポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーションサービスルータ、統合サービスルータ、組み込みサービスルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザートラフィックなどに制限します。

要素	説明
サービス	このルールで照合されるトラフィックのタイプを定義するサービス。サービスは、プロトコルおよびポート情報を指定するオブジェクトで定義されます。詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
From Zone	このルールは、このゾーンから発信されるトラフィックにだけ適用されます。
To Zone	このルールは、このゾーンを宛先とするトラフィックにだけ適用されます。
Inspected Protocol	ルールが選択されたアクションを実行するプロトコル。
操作	一致したプロトコルの処理方法を識別します。 • [Drop]：一致したトラフィックはサイレントにドロップされます。すべてのトラフィックに適用されるデフォルト アクション。 • [Drop and Log]：一致したトラフィックは、記録され、ドロップされます。 • [Pass]：ルータは、一致したトラフィックを送信元ゾーンから宛先ゾーンに転送します。 • [Pass and Log]：トラフィックが記録され、転送されます。 • [Inspect]：状態ベースのトラフィック コントロール。[Inspect] は、Port to Application Mapping（PAM）に基づいて、特定のプロトコルのアプリケーション インスペクションとコントロールを提供できます。 • [Content Filter]：WebFilter パラメータ マップまたは WebFilter ポリシー マップに基づく HTTP コンテンツ インスペクション。 （注） ログ オプションによって、システム ログ メッセージが生成されます。これらのメッセージをキャプチャするように syslog ロギングが設定されていることを確認する必要があります。
オプション	このルールに割り当てられているインスペクション パラメータ マップ。[Inspect] アクションと [Content Filter] アクションでだけ使用できます。
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	このルールの説明（提供されている場合）。最大 1024 文字を使用できます。

要素	説明
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
[クエリ（Query）] ボタン	ポリシークエリを実行します。実行すると、ルールを評価して、効果が得られない削除可能なルールを特定できます。 ポリシー クエリー レポートの生成 （793 ページ）を参照してください。
[Find and Replace] ボタン（双眼鏡アイコン）	テーブル内でのルールの検索と変更を容易にするために、IP アドレスやポリシー オブジェクト名などのルール テーブルの値を検索します。 ルール テーブルの項目の検索と置換 （777 ページ）を参照してください。
[Up] ボタン	選択したルールをテーブル内で 1 行上に移動します。
[Down] ボタン	選択したルールをテーブル内で 1 行下に移動します。
[追加（Add）] ボタン	新しいルールを作成できる [Add Zone-based Firewall Rule] ダイアログボックスを開きます。
[編集（Edit）] ボタン	テーブル内の選択したルールの編集に使用します。[Edit Zone-based Firewall Rule] ダイアログボックスを開きます。
[削除（Delete）] ボタン	選択したルールをテーブルから削除します。

ゾーンベースのファイアウォール ルールの追加と編集

[Add Zone based Firewall Rule]/[Edit Zone based Firewall Rule] ダイアログボックスを使用して、Cisco IOS および ASR デバイスに対するゾーンベースのファイアウォール ルールを追加および編集します。

ナビゲーション パス

[Zone-based Firewall Rules] ページ （1272 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォール ルールの設定 （1261 ページ）
- ゾーンベースのファイアウォールルールの追加 （1210 ページ）

フィールド リファレンス

表 *296 : [Add Zone based Firewall Rule]* および *[Edit Zone based Firewall Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	選択されている場合は、設定が生成および展開されたあとでルールがデバイスでイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
トラフィック	このルールが適用されるトラフィック フローを定義します。
一致（Match）	一致したトラフィックを許可するか拒否するかどうかを選択します。このオプションの詳細については、ゾーンベースのファイアウォールルールの Permit/Deny とアクションとの関係について （1203 ページ）を参照してください。
ソース	このルールのトラフィック ソースを提供します。ネットワークまたはセキュリティ グループになります。次の 1 つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 （注） これらのフィールドのいずれかに、 項目をカンマで区切って、1 つ以上の値を入れます。 • ネットワーク – さまざまなネットワーク、ホスト、および IP アドレスの定義を、個別に、またはオブジェクトとして指定できます。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、ネットワーク/ホストオブジェクトについて （391 ページ）およびポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービス ルータ、組み込みサービス ルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザ トラフィックです。

要素	説明
宛先	このルールのトラフィックの宛先を指定します。ネットワークまたはセキュリティグループにすることができます。次の1つ以上のタイプのソースに対して、値またはオブジェクト名を入力するか、オブジェクトを選択できます。 （注） これらのフィールドのいずれかに、 項目をカンマで区切って、1 つ以上の値を入れます。 • ネットワーク – さまざまなネットワーク、ホスト、および IP アドレスの定義を、個別に、またはオブジェクトとして指定できます。「All-Address」オブジェクトは、ルールを特定のホストまたはネットワークに制限しません。 これらの定義の詳細については、 ネットワーク/ホストオブジェクトについて （391 ページ）および ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。 （注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービス ルータ、組み込みサービス ルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。 各仕様を他の仕様と組み合わせて、トラフィックの一致をすべての定義を含むフローのみに制限します。たとえば、指定された送信元アドレス範囲内から発信された指定されたユーザ トラフィックです。
サービス	このルールで照合されるトラフィックのタイプを定義するサービスを指定します。サービス オブジェクトおよびサービス タイプの任意の組み合わせ（通常はプロトコルとポートの組み合わせ）をカンマで区切って入力できます。このオプションの詳細については、 ゾーンベースのファイアウォール ルールの Services と Protocols の関係について （1207 ページ）を参照してください。 サービスを入力する場合は、有効な値の入力を求められます。[Select] をクリックして、リストからサービスを選択することもできます。サービスを指定する方法の詳細については、 サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。
From Zone To Zone	基本的なゾーンベースのファイアウォール ルールは単方向です。つまり、2 つのゾーン間で一方向にだけ移動するトラフィック フローを定義します。 このルールのトラフィック フローが発信されるゾーンを入力または選択し、トラフィックが流れる先のゾーンを入力または選択します。
[Advanced] ボタン	時間範囲オプションを選択できる [Advanced Options] ダイアログボックスを開きます。 ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス （1281 ページ）を参照してください。
アクション	このルールと一致するトラフィックに適用されるアクション。目的のアクションを選択します。

要素	説明
[Action]：[Drop]、[Drop and Log]、[Pass]、[Pass and Log]	• [ドロップ（Drop）]：指定したサービスに対するすべてのパケットをサイレントにドロップします。すべてのトラフィックに適用されるデフォルト アクション。 • [ドロップアンドログ（Drop and Log）]：一致したトラフィックは、記録され、ドロップされます。 • [パス（Pass）]：ルータは、一致したパケットを [送信元ゾーン（From Zone）] から [宛先ゾーン（To Zone）] に転送します。リターン トラフィックは認識されないため、リターン トラフィック用に追加のルールを指定する必要があります。このオプションは、IPsec で符号化されたトラフィックなどのプロトコルにだけ役立ちます。 • [パスアンドログ]：トラフィックが記録され、転送されます。 これらのアクションについては、[プロトコル（Protocol）] テーブルの横の [選択（Select）] ボタンをクリックして [Protocol Selector] ダイアログボックス （1283 ページ）を開くことにより、照合する 1 つ以上のプロトコルを選択できます。ただし、これは必須ではありません。[Protocol] テーブルを空のままにして、[Sources]、[Destinations]、および [Services] パラメータに基づいてトラフィックを渡すかドロップできます。実際には、これらは標準アクセス ルールです。 [Protocol Selector] ダイアログボックスでは、選択したプロトコルの Port Application Mapping（PAM; ポートアプリケーションマッピング）パラメータを編集できる [Configure Protocol] ダイアログボックス （1284 ページ）にもアクセスできます。 （注） ログオプションによって、システム ログ メッセージが生成されます。これらのメッセージをキャプチャするように syslog ロギングが設定されていることを確認する必要があります。

要素	説明
[Action]：[Inspect]	[検査（Inspect）]は状態に基づくトラフィック制御を提供します。デバイスは、TCP および UDP トラフィックに関する接続またはセッション情報を維持するため、接続要求に対するリターントラフィックが許可されます。 選択したレイヤ 4（TCP、UDP）プロトコルおよびレイヤ 7（HTTP、IMAP、インスタントメッセージング、およびピアツーピア）プロトコルに基づいたパケット インスペクションを適用する場合、このオプションを選択します。選択したプロトコルの PAM も編集でき、ディープ パケット インスペクション（DPI）を設定して、レイヤ 7 プロトコルの追加のプロトコル関連情報を提供できます。詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）を参照してください。 **1.** [プロコトル（Protocol）]テーブルの横の [選択（Select）]ボタンをクリックして [Protocol Selector] ダイアログボックス （1283 ページ）を開くことにより、インスペクションに対して 1 つ以上のプロトコルを選択できます。 **2.** [Protocol Selector] ダイアログボックスでは、カスタム プロトコルを作成し、選択したプロトコルの PAM および DPI パラメータを編集できる [Configure Protocol] ダイアログボックス （1284 ページ）にもアクセスできます。 **3.** [検査パラメータ（Inspect Parameters）]：このフィールドにインスペクション パラメータ マップの名前を入力するか、または [選択（Select）] を選択してリストから選択することで、カスタマイズされた一連の接続、タイムアウト、およびその他の設定を適用できます。選択リスト ダイアログボックスから新しいインスペクション パラメータ マップを作成することもできます。詳細については、インスペクション パラメータ マップの設定 （1234 ページ）を参照してください。 インスペクション パラメータ マップを指定しない場合、デフォルト設定が使用されます。

要素	説明
[Action]：[Content Filter]	[コンテンツフィルタ（Content Filter）] では、指定されたパラメータまたはポリシーマップに基づく URL フィルタリングが提供されます。ルータが HTTP 要求を代行受信し、プロトコル関連の検査を実行します。また、任意で、要求を許可するかブロックするかを決定するためにサードパーティ製サーバに接続します。WebFilter パラメータ マップを提供できます。このマップにより、ローカル URL リスト、および外部 SmartFilter（以前の N2H2）や Websense サーバからの情報に基づくフィルタリングを定義します。または、ローカル、N2H2、Websense、または Trend Micro フィルタリング データにアクセスする WebFilter ポリシー マップを提供できます。 **1.** アクションとして [コンテンツフィルタ（Content Filter）] が選択されている場合は、HTTP がプロトコルとして指定されます。[Configure] をクリックして、HTTP PAM 設定を編集し、HTTP DPI マップを適用できる [Configure Protocol] ダイアログボックス （1284 ページ）を開くことができます。 **2.** [ウェブフィルタパラメータマップ（WebFilter Parameter Map）] または [ウェブフィルタポリシーマップ（WebFilter Policy Map）] を選択し、適切なマップの名前を指定します。適切な [Select] ボタンをクリックしてリストからマップを選択できます。選択リスト ダイアログボックスから新しいマップを作成することもできます。これらのマップの設定の詳細については、ゾーンベースのファイアウォール ポリシーのコンテンツ フィルタリング マップの設定 （1242 ページ）を参照してください。 **3.** [検査パラメータ（Inspect Parameters）]：このフィールドにインスペクション パラメータ マップの名前を入力するか、または [選択（Select）] を選択してリストから選択することで、カスタマイズされた一連の接続、タイムアウト、およびその他の設定を適用できます。選択リスト ダイアログボックスから新しいインスペクション パラメータ マップを作成することもできます。詳細については、インスペクション パラメータ マップの設定 （1234 ページ）を参照してください。 インスペクション パラメータ マップを指定しない場合、デフォルト設定が使用されます。
説明	（任意）ルール テーブルを表示するときにルールを識別するのに役立つ最大 1024 文字の説明を入力できます。
カテゴリ	（任意）ルールにカテゴリを割り当てて、ルールとオブジェクトの整理および識別に役立てることができます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ゾーンベースのファイアウォール ルール：[Advanced Options] ダイアログボックス

ゾーンベースのファイアウォール ルールの [Advanced Options] ダイアログボックスを使用して、特定の時間範囲情報をゾーンベースのファイアウォール ルールに適用します。

ナビゲーション パス

[ゾーンベースのファイアウォールルールの追加（Add Zone based Firewall Rule）]/[ゾーンベースのファイアウォールルールの編集（Edit Zone based Firewall Rule）] ダイアログボックスの [トラフィック（Traffic）] セクションで、[詳細設定（Advanced）] ボタンをクリックします。

関連項目

- ゾーンベースのファイアウォール ルールの追加と編集 （1276 ページ）
- ゾーンベースのファイアウォール ルールについて （1197 ページ）

フィールド リファレンス

表 *297 : [Advanced Options]* ダイアログボックス

要素	説明
時間範囲（Time Range）	この機能では、このゾーンベースのファイアウォール ルールがアクティブになる期間を定義できます。時間範囲を指定しない場合は、ルールが即時に、そして常にアクティブになります。 時間範囲オブジェクトの名前を入力するか、[選択（Select）] をクリックして [時間範囲セレクタ（Time Ranges Selector）] ダイアログボックスのリストから選択します。このダイアログボックスで、時間範囲オブジェクトを作成および編集できます。詳細については、時間範囲オブジェクトの設定 （379 ページ）を参照してください。
オプション	この機能では、このゾーンベースのファイアウォール ルールに initial-packet-fragment または established-connection 制限を適用できます。次のいずれかのオプションを選択します。 • [なし（None）]：packet-fragment または established-connection 制限は適用されません。 • [フラグメント（Fragment）]：選択されている場合は、ルールが初期以外のパケットフラグメントに適用されます。フラグメントはルールに従って許可または拒否されます。ホワイトペーパー『Access Control Lists and IP Fragments』に、ゾーンベースのファイアウォールルールにも関連する追加情報が記載されています。 • [確立済み（Established）]：TCP プロトコルの場合にだけ、確立済みの接続を要求します。TCP データグラムに ACK または RST 制御ビットが設定されている場合に一致します。一致しないケースは、接続を形成する初期 TCP データグラムです。

[Protocol Selector] ダイアログボックス

[Protocol Selector] ダイアログボックスを使用して、ゾーンベースのファイアウォール ルールのトラフィック定義の一部として、1 つ以上の通信プロトコルを指定します。

[Protocol Selector] ダイアログボックスでは、カスタム プロトコルの作成および既存のプロトコルの Port Application Mapping（PAM; ポート アプリケーション マッピング）パラメータの編集に使用できる [Configure Protocol] ダイアログボックスにもアクセスできます。[Configure Protocol] ダイアログボックスでは、特定のプロトコルの詳細インスペクション ポリシー マップ、およびプロトコル情報パラメータ マップも選択します。詳細については、[Configure Protocol] ダイアログボックス （1284 ページ）を参照してください。

ナビゲーション パス

[Protocol Selector] ダイアログボックスには、[Add Zone based Firewall Rule]/[Edit Zone based Firewall Rule] ダイアログボックス（ゾーンベースのファイアウォール ルールの追加と編集（1276ページ）で説明しています）からアクセスできます。いずれかのダイアログボックスで、[Content Filter] 以外のアクションを選択し、[Protocol] テーブルの横の [Select] ボタンをクリックします。

[Zone Based Firewall Rules] テーブルの任意のエントリの [Inspected Protocol] カラムを右クリックしてから [Edit Protocols] を選択することでも、[Protocol Selector] ダイアログボックスを開くことができます。

関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォール ルールの追加と編集 （1276 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- [Configure Protocol] ダイアログボックス （1284 ページ）

表 *298 : [Protocol Selector]* ダイアログボックス

要素	説明
Available Protocols	ゾーンベースのファイアウォール ルールに対して選択できるプロトコルのリスト。 **ヒント** [Selected Protocols] カラムの下の [Create] ボタンをクリックして [Configure Protocol] ダイアログボックス （1284 ページ）を開くことにより、カスタム プロトコルを作成できます。

要素	説明
Selected Protocols	このゾーンベースのファイアウォール ルールに対して選択したプロトコルのリスト。 ヒント [Selected Protocols] カラムで強調表示されているプロトコルの Port Application Mapping（PAM; ポート アプリケーション マッピング）設定を編集できます。[Selected Protocols] カラムの下の [Edit] ボタンをクリックして [Configure Protocol] ダイアログボックス（1284 ページ）を開きます。
[>>] ボタン	強調表示されているプロトコルを [Available Protocols] カラムから [Selected Protocols] カラムに移動します。Shift を押しながらのクリックおよび Ctrl を押しながらのクリックという標準機能を使用して、複数のプロトコルを選択できます。
[<<] ボタン	強調表示されているプロトコルを [Selected Protocols] カラムから [Available Protocols] カラムに戻します。Shift を押しながらのクリックおよび Ctrl を押しながらのクリックという標準機能を使用して、複数のプロトコルを選択できます。

[Configure Protocol] ダイアログボックス

特定のプロトコル オブジェクトの選択によって、Port Application Mapping（PAM; ポート アプリケーションマッピング）パラメータ（レイヤ4プロトコルとポート、およびオプションで特定のネットワークとホスト）を定義するパケットインスペクションをゾーンベースのファイアウォール ルールに設定できます。レイヤ7（HTTP、IMAP、Instant Messaging、およびピアツーピア）プロトコルには、そのプロトコルに固有の詳細パケット インスペクション ポリシーも含めることができます。ゾーンベースのファイアウォール ルールの定義中のプロトコルの選択については、ゾーンベースのファイアウォール ルールの追加と編集 （1276 ページ）を参照してください。

[Configure Protocol] ダイアログボックスは、ゾーンベースのファイアウォール ルールで使用する既存のプロトコル定義の編集、およびカスタム定義の作成に使用されます。たとえば、プロトコルで一部またはすべてのネットワークにデフォルト ポートを使用しない場合は、異なるポート マッピングを設定できます。

ナビゲーション パス

[Configure Protocol] ダイアログボックスには、[Protocol Selector] ダイアログボックス （1283 ページ）から次のようにアクセスします。

- [Selected Protocols] リストの下にある [Create]（+）ボタンをクリックして、新規プロトコルを作成する。
- [Selected Protocols] リストでプロトコルを選択し、[Edit]（鉛筆）ボタンをクリックしてそのプロトコルを編集する。

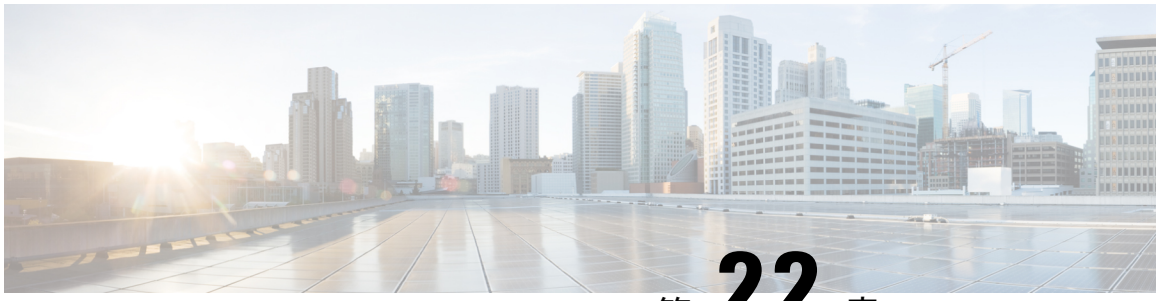
関連項目

- ゾーンベースのファイアウォール ルールについて （1197 ページ）
- ゾーンベースのファイアウォールルールの追加 （1210 ページ）
- [Protocol Selector] ダイアログボックス （1283 ページ）

表 *299 : [Configure Protocol]* ダイアログボックス

要素	説明
Protocol Name	選択したプロトコルの名前。カスタム プロトコルを作成している場合は、最大 19 文字の名前を入力できます。カスタム プロトコル名は **user-** から始まる必要があります。
Enable Signature	このオプションは、ピアツーピア（eDonkey、FastTrack、Gnutella、Kazaa2）プロトコルを編集する場合にだけ使用できます。 このオプションをイネーブルにすると、Network-Based Application Recognition（NBAR; ネットワークベース アプリケーション認識）ヒューリスティックがトラフィックに適用され、特定の P2P アプリケーション アクティビティを示す「telltale」が検出されます。これらの telltale には、ポートホッピング、およびトラフィック検出を回避するためのアプリケーション動作のその他の変更が含まれます。 （注） このレベルのトラフィック インスペクションは、CPU 使用率の増加およびネットワーク スループットの低減を伴います。
Deep Inspection	このオプションは、H.323、HTTP、IM（AOL、ICQ、MSN Messenger、Windows Messenger、および Yahoo Messenger）、IMAP、P2P（eDonkey、FastTrack、Gnutella、Kazaa2）、POP3、SIP、SMTP、Sun RPC プロトコルを編集する場合、およびゾーンベースのファイアウォールルールに対して [検査（Inspect）] アクションが選択されている場合にだけ使用可能です。 選択したプロトコルで使用するインスペクション ポリシー マップの名前を入力または選択します。これらのポリシー マップの詳細については、ゾーンベースのファイアウォール ポリシーのインスペクション マップの設定 （1213 ページ）を参照してください。

要素	説明
Protocol Info	このオプションは、インスタント メッセージング（AOL、ICQ、MSN Messenger、Windows Messenger、および Yahoo Messenger）と Stun-ice プロトコルを編集する場合だけ使用可能です。 選択したプロトコルで使用するプロトコル情報パラメータ マップの名前を入力または選択します。これらのパラメータ マップでは、これらのアプリケーションと対話する DNS サーバを定義します。このパラメータ マップにより、Instant Messaging（IM; インスタント メッセージング）アプリケーション エンジンが IM トラフィックを認識し、その IM アプリケーションの設定済みポリシーを適用できます。 これらのパラメータ マップの詳細については、プロトコル情報パラメータ マップの設定 （1237 ページ）を参照してください。
Port Application Mapping	これらのオプションでは、選択したプロトコルの Port Application Mapping（PAM; ポート アプリケーション マッピング）パラメータをカスタマイズできます。
プロトコル	このマッピングのトランスポート プロトコルを選択します。 • TCP/UDP • [TCP] • UDP
ポート	単一のポート番号、複数のポート番号、またはポートの範囲（60000-60005 など）を任意に組み合わせて入力します。複数のエントリを指定する場合は、カンマで区切ります。すでにマッピングされているポートと重複する範囲は指定しないでください。
ネットワーク	このプロトコル/ポート マッピングが特定のネットワークまたはホストだけに対するものである場合は、ネットワークまたはホストの名前または IP アドレス、あるいはネットワーク/ホスト オブジェクトの名前を入力します。[Select] をクリックして、ネットワーク/ホスト セレクタを開くことができます。複数のエントリを指定する場合は、カンマで区切ります。



第 22 章

トラフィック ゾーンの管理

1 つのトラフィック ゾーンに複数のインターフェイスを割り当てることができます。これにより、ゾーン内のインターフェイスで、既存のフローのトラフィックが ASA に出入りできるようになります。この機能により、ASA 上での等コスト マルチパス（ECMP）のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロード バランシングが可能になります。

ゾーン分割されていない動作

アダプティブ セキュリティ アルゴリズムは、トラフィックの許可または拒否を決定する際に、パケットの状態を考慮します。フローに適用されたパラメータの 1 つは、トラフィックが同じインターフェイスに出入りすることです。異なるインターフェイスに入る既存のフローのトラフィックは、ASA によってドロップされます。

トラフィック ゾーンにより、複数のインターフェイスを 1 つにまとめることができるため、ゾーン内の任意のインターフェイスに出入りするトラフィックがアダプティブ セキュリティ アルゴリズムのセキュリティ チェックを満たすことができるようになります。

- ゾーンを使用する理由 （1287 ページ）
- ECMP ルーティング （1289 ページ）
- トラフィックゾーンについて （1290 ページ）
- トラフィック ゾーンの前提条件 （1292 ページ）
- トラフィック ゾーンのガイドライン （1293 ページ）
- トラフィックゾーンの設定 （1295 ページ）

ゾーンを使用する理由

非対称ルーティング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。宛先ネットワークの非対称ルーティングが原因で、Outside2 インターフェイスの ISP 2 からリターン トラフィックが到達しています。

ゾーン分割されていない場合の問題：ASA は、インターフェイスごとに接続テーブルを保持します。リターン トラフィックが Outside2 に到達すると、そのトラフィックは、接続テーブルに一致しないため、ドロップされます。

ゾーン分割されたソリューション：ASAは、ゾーンごとに接続テーブルを保持します。Outside1 と Outside2 を 1 つのゾーンにグループ化した場合、リターン トラフィックが Outside2 に到達すると、ゾーンごとの接続テーブルに一致するため、接続が許可されます。

紛失したルート

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。Outside1 と ISP 1 間でルートが紛失または移動したため、トラフィックは ISP 2 を経由する別のルートを通る必要があります。

ゾーン分割されていない場合の問題：内部ホストと外部ホスト間の接続が削除されるため、新しい次善のルートを使用して新しい接続を確立する必要があります。UDP の場合、1 つのパケットがドロップダウンすると新しいルートが使用され、UDP がない場合は、新しい接続を再確立する必要があります。

ゾーン分割されたソリューション：ASA は、紛失したルートを検出し、フローを ISP 2 経由の新しいパスに切り替えます。トラフィックは、パケットがドロップすることなくシームレスに転送されます。

ロード バランシング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。2 番目の接続が Outside2 の ISP 2 を経由する等コスト ルートを介して確立されています。

ゾーン分割されていない場合の問題：インターフェイス間でロードバランシングを行うことができません。可能なのは、1 つのインターフェイスの等コスト ルートによるロードバランスだけです。

ゾーン分割されたソリューション：ASA は、ゾーン内のすべてのインターフェイスで最大 8 つの等コスト ルート間の接続をロードバランスすることができます。

関連項目

- ゾーンを使用する理由　（1287 ページ）
- ECMP ルーティング　（1289 ページ）
- トラフィックゾーンについて　（1290 ページ）
- トラフィック ゾーンの前提条件　（1292 ページ）
- トラフィック ゾーンのガイドライン　（1293 ページ）
- トラフィックゾーンの設定　（1295 ページ）

ECMP ルーティング

ASA では、等コスト マルチパス（ECMP）ルーティングをサポートしています。

ゾーン分割されていない ECMP サポート

ゾーンがない場合は、インターフェイスごとに最大 3 つの等コストのスタティックルートタまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで 3 つのデフォルト ルートを設定できます。

route outside 0 0 10.1.1.2

route outside 0 0 10.1.1.3

route outside 0 0 10.1.1.4

この場合、トラフィックは、10.1.1.2、10.1.1.3 と 10.1.1.4 間の外部インターフェイスでロードバランスされます。トラフィックは、送信元 IP アドレスおよび宛先 IP アドレスをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMP は複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

route outside2 0 0 10.2.1.1

ゾーン分割された ECMP サポート

ゾーンがある場合は、ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に 3 つのデフォルト ルートを設定できます。

route outside1 0 0 10.1.1.2

route outside2 0 0 10.2.1.2

route outside3 0 0 10.3.1.2

同様に、ダイナミック ルーティング プロトコルは、自動的に等コスト ルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス全体でトラフィックをロードバランスします。

ルートが紛失した場合、ASA はフローをシームレスに別のルートに移動させます。

接続のロード バランス方法

ASA では、パケットの 6 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル、入力インターフェイス）から生成されたハッシュを使用して、等コスト ルート間の接続をロードバランスします。ルートが紛失しない限り、接続は接続期間中、インターフェイスで継続されます。

接続内のパケットは、ルート間でロードバランスされません。接続では、そのルートが紛失しない限り、単一ルートを使用します。

ASA では、ロード バランシング時にインターフェイス帯域幅やその他のパラメータを考慮しません。同じゾーン内のすべてのインターフェイスが MTU、帯域幅などの同じ特性を持つことを確認します。

ロード バランシング アルゴリズムは、ユーザー設定可能ではありません。

別のゾーンのルートへのフォール バック

ルートがインターフェイスで紛失したときにゾーン内で使用可能な他のルートがない場合、ASA では、異なるインターフェイス/ゾーンからのルートを使用します。このバックアップ ルートを使用した場合、ゾーン分割されていないルーティングのサポートと同様にパケットのドロップが発生することがあります。

関連項目

- ECMP ルーティング （1289 ページ）
- トラフィック ゾーンについて （1290 ページ）
- トラフィック ゾーンの前提条件 （1292 ページ）>
- トラフィック ゾーンのガイドライン （1293 ページ）
- トラフィック ゾーンの設定 （1295 ページ）

トラフィック ゾーンについて

インターフェイスベースのセキュリティ ポリシーの設定

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。必須のパラレル インターフェイス設定の詳細については、 トラフィック ゾーンの前提条件 （1292 ページ）を参照してください。

トラフィック ゾーンでサポートされるサービス

次のサービスがゾーンでサポートされています。

- アクセル ルール
- NAT
- QoS トラフィック ポリシングを除くサービス ルール。
- Routing

完全にゾーン分割されたサポートは利用できませんが、to-the-box サービスや from-the-box サービス（以下を参照）も設定できます。

トラフィック ゾーンのインターフェイスに他のサービス（VPN、ボットネット トラフィック フィルタなど）を設定しないでください。これらのサービスは、想定どおりに機能または拡張しないことがあります。

（注） セキュリティ ポリシーの設定方法の詳細については、トラフィック ゾーンの前提条件（1292 ページ）を参照してください。

セキュリティ レベル

ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1 つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

フローのプライマリおよび現在のインターフェイス

各接続フローは、最初の入出力インターフェイスに基づいて構築されます。これらのインターフェイスは、プライマリ インターフェイスです。

ルート変更または非対称ルーティングにより、新しい出力インターフェイスが使用されている場合は、新しいインターフェイスが現在のインターフェイスになります。

ゾーンの追加または削除

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

To-the-Box および From-the-Box トラフィック

- management-only インターフェイスまたは management-access インターフェイスをゾーンに追加することはできません。
- ゾーンの通常のインターフェイスでの管理トラフィックでは、既存のフローの非対称ルーティングのみがサポートされます。ECMP サポートはありません。
- 1 つのゾーン インターフェイスにのみ管理サービスを設定できますが、非対称ルーティング サポートを利用するには、すべてのインターフェイスでそれを設定する必要があります。構成がすべてのインターフェイスでパラレルである場合でも、ECMP はサポートされません。
- ASA は、ゾーンで次の To-the-Box および From-the-Box サービスをサポートします。

- [Telnet]
- SSH
- HTTPS
- SNMP
- Syslog
- BGP

ゾーン内の IP アドレスのオーバーラップ

ゾーン分割されていないインターフェイスの場合、ASA では、NAT が正しく設定されていれば、インターフェイスでの IP アドレス ネットワークのオーバーラップをサポートします。ただし、同じゾーンのインターフェイスでは、ネットワークのオーバーラップはサポートされていません。

関連項目

- ゾーンを使用する理由 （1287 ページ）
- トラフィックゾーンについて （1290 ページ）
- トラフィック ゾーンの前提条件 （1292 ページ）
- トラフィック ゾーンのガイドライン （1293 ページ）
- トラフィックゾーンの設定 （1295 ページ）

トラフィック ゾーンの前提条件

- 名前、IP アドレス、およびセキュリティ レベルを含むすべてのインターフェイス パラメータを設定します。ゾーンのすべてのインターフェイスでセキュリティ レベルが一致する必要があることに注意してください。帯域幅および他のレイヤ 2 のプロパティについては、インターフェイスのようにグループ化する計画を立てる必要があります。
- 次のサービスをゾーンのすべてのインターフェイスで一致するように設定します。
  - アクセス ルール：同じアクセス ルールをゾーンのすべてのメンバー インターフェイスに適用するか、グローバル アクセス ルールを使用します。
  - NAT：ゾーンのすべてのメンバーインターフェイスで同じ NAT ポリシーを設定するか、グローバル NAT ルールを使用します。

インターフェイス PAT はサポートされていません。

（注） インターフェイス固有の NAT および PAT プールを使用すると、ASA は、元のインターフェイスに障害が発生した場合に接続を切り替えることができません。インターフェイス固有の PAT プールを使用すると、同じホストからの複数の接続が異なるインターフェイスにロードバランシングされ、異なるマッピングされた IP アドレスを使用する場合があります。この場合、複数の同時接続を使用するインターネット サービスが正しく機能しないことがあります。

- サービス ルール：グローバル サービス ポリシーを使用するか、ゾーンの各インターフェイスに同じポリシーを割り当てます。

QoS トラフィック ポリシングはサポートされていません。

（注） VoIP インスペクションでは、ゾーンのロード バランシングにより、順序が正しくないパケットが増加する可能性があります。この状況は、異なるパスを通る先行パケットの前に後行パケットが ASA に到達する可能性があるために発生することがあります。順序が不正なパケットには次のような兆候が見られます。キューイングを使用した場合に、中間ノード（ファイアウォールと IDS）および受信エンドノードでメモリ使用率が高い。これらの影響を低減するために、VoIP トラフィックの負荷分散専用の IP アドレスを使用することをお勧めします。

- ECMP ゾーン機能を考慮してルーティングを設定します。

関連項目

- ゾーンを使用する理由 （1287 ページ）
- ECMP ルーティング （1289 ページ）
- トラフィックゾーンについて （1290 ページ）
- トラフィック ゾーンのガイドライン （1293 ページ）
- トラフィックゾーンの設定 （1295 ページ）

トラフィック ゾーンのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フェールオーバー

- フェールオーバー リンクまたはステート リンクをゾーンに追加することはできません。
- アクティブ/アクティブ フェールオーバー モードでは、各コンテキストのインターフェイスを非対称ルーティング（ASR）グループに割り当てることができます。このサービスにより、ピア装置の同様のインターフェイスに戻るトラフィックを元の装置に復元することができます。コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。
- 各接続のプライマリ インターフェイスのみがスタンバイ装置に 複製されます。現在のインターフェイスは複製されません。スタンバイ装置がアクティブになると、その装置によって必要に応じて現在の新しいインターフェイスが割り当てられます。

クラスタ

クラスタ制御リンクをゾーンに追加することはできません。

その他のガイドライン

- 最大 256 ゾーンを作成できます。
- ゾーンに追加できるのは、物理インターフェイスのみです。
- 1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。
- ゾーンごとに最大 8 つのインターフェイスを含めることができます。
- ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。
- ECMP の場合、ゾーンのすべてのインターフェイス間で、ゾーンごとに最大 8 つの等コスト ルートを追加できます。また、8 ルート制限の一部として 1 つのインターフェイスに複数のルートを設定することもできます。

関連項目

- ゾーンを使用する理由 （1287 ページ）
- ECMP ルーティング （1289 ページ）
- トラフィックゾーンについて （1290 ページ）
- トラフィック ゾーンの前提条件 （1292 ページ）
- トラフィックゾーンの設定 （1295 ページ）

トラフィックゾーンの設定

1つのトラフィック ゾーンに複数のインターフェイスを割り当てることができます。これにより、ゾーン内のインターフェイスで、既存のフローのトラフィックが ASA に出入りできるようになります。この機能により、ASA 上での等コスト マルチパス（ECMP）のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロード バランシングが可能になります。

関連項目

- インターフェイス ロール オブジェクトについて （381 ページ）
- ゾーンを使用する理由 （1287 ページ）
- ECMP ルーティング （1289 ページ）
- トラフィックゾーンについて （1290 ページ）
- トラフィック ゾーンの前提条件 （1292 ページ）
- トラフィック ゾーンのガイドライン （1293 ページ）

ステップ 1 次のいずれかを実行します。

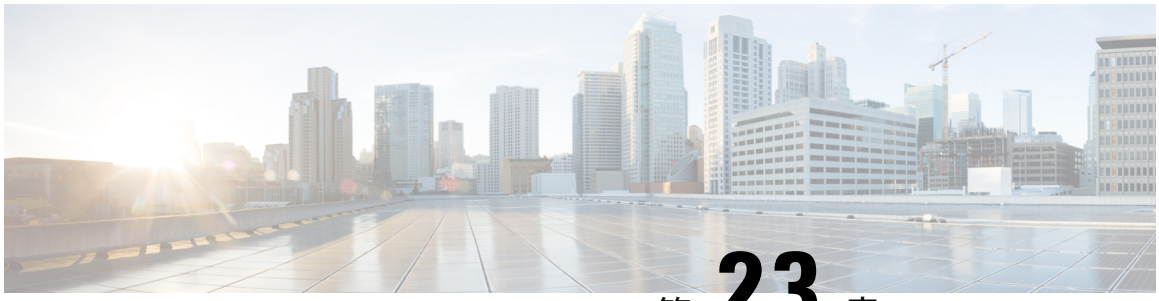
- （デバイスビュー）ポリシーセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーン（Zone）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [設定（Settings）] > [ゾーン（Zone）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [ゾーン（Zone）] テーブルの下にある [追加（Add）] ボタンをクリックして、[ゾーン（Zone）] ダイアログボックスを表示します。

ステップ 3 設定しているトラフィックゾーンに属するインターフェイスを識別するインターフェイス ロールの名前を入力し、[OK] をクリックします。インターフェイス ロール オブジェクトの詳細については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

ヒント [選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイス ロールを選択するか、新しいインターフェイス ロール オブジェクトを定義します。

ステップ 4 [保存（Save）] をクリックして、変更内容を保存します。



第 23 章

トランスペアレントファイアウォールルールの管理

トランスペアレント ファイアウォール ルールは、非 IP レイヤ 2 トラフィックのアクセス コントロール ルールです。これらのルールを使用して、レイヤ 2 パケット内の Ethertype 値に基づいてトラフィックを許可またはドロップできます。

この章は次のトピックで構成されています。

- トランスペアレント ファイアウォール ルールの設定 （1297 ページ）
- [Transparent Rules] ページ （1300 ページ）

トランスペアレント ファイアウォール ルールの設定

トランスペアレント ファイアウォール ルールは、非 IP レイヤ 2 トラフィックのアクセス コントロール ルールです。これらのルールを使用して、レイヤ 2 パケット内の Ethertype 値に基づいてトラフィックを許可またはドロップできます。これらのルールによって、デバイス上に Ethertype アクセス コントロール リストが作成されます。トランスペアレント ルールを使用すると、デバイスでの非 IP トラフィック フローを制御できます（IP トラフィックを制御するには、アクセス ルールを使用します。アクセス ルールについて （913 ページ）を参照してください）。

トランスペアレント ファイアウォールは、ブリッジ経由のトラフィック フローを制御するために単一のサブネット内に配置するデバイスです。トランスペアレント ファイアウォールを使用すると、ネットワークに番号を付け直すことなく、サブネット上にファイアウォールを配置できます。

トランスペアレント ルールは、次のタイプのインターフェイス上でだけ設定できます。

- **IOS 12.3(7)T 以降のデバイスの場合**：ブリッジグループの一部であるレイヤ 3 インターフェイス上：
  - [インターフェイス（Interfaces）] > [インターフェイスポリシー（Interfaces policy）] で、ブリッジするインターフェイスをレイヤ 3 として設定します。

- [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）] ポリシーで、2 つ以上のレイヤ 3 インターフェイスが含まれるブリッジ グループを設定します（Cisco IOS ルータにおけるブリッジング （3135 ページ）および ブリッジ グループの定義 （3137 ページ）を参照）。
- このブリッジ グループと同じ番号を使用して、Bridge-group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）を作成します（ブリッジ グループ仮想インターフェイス （3136 ページ）を参照）。たとえば、ブリッジ グループ 12 を作成する場合は、BVI12 を作成します。

- **ASA、PIX 7.0 以降、FWSM デバイスの場合**：デバイスがトランスペアレント モードで実行されている場合の任意のインターフェイス上。複数のコンテキストを使用する場合は、個々のセキュリティ コンテキストでルールを設定します。

[プラットフォーム（Platform）] > [ブリッジング（Bridging）] ポリシーグループで設定できるその他のブリッジングポリシーには、ARP テーブルと ARP インスペクション、MAC テーブルと MAC 学習ディセーブル化機能、およびデバイスのリモート管理を可能にするための管理 IP アドレスの設定機能があります。トランスペアレント ファイアウォールの詳細については、ファイアウォール デバイスでのブリッジング ポリシーの設定 （2449 ページ）および ルーテッド モードおよびトランスペアレント モードのインターフェイス （2336 ページ）を参照してください。

ヒント トランスペアレント モードの ASA、PIX、および FWSM では、すべての IP トラフィックがデバイスを通過できるようにアクセス ルールを設定する必要があります。トランスペアレント ルールでは、レイヤ 2 の非 IP トラフィックだけが制御されます。

また、セキュリティ デバイスでネットワーク アドレス変換を使用する方法については、 トランスペアレント モードの NAT （1326 ページ）を参照してください。

これらのインターフェイス上に、他のタイプのファイアウォール ルールを設定することもできます。その他のタイプのルールは、レイヤ 3 以上のトラフィックに適用されます。

ヒント トランスペアレント ルールを設定すると、暗黙的な **deny all** ルールが、各インターフェイスのルールリストの最後に追加されます。必要なトラフィックをすべて許可していることを確認してください。特定のタイプのトラフィックだけを許可するのではなく、単に特定のタイプのトラフィックを拒否する場合は、**permit any**（ASA/PIX/FWSM デバイスの場合）または **permit 0x0000 0xFFFF**（IOS デバイスの場合）ルールをテーブル内の最後のルールとして含めることができます。

関連項目

- ルールの追加および削除 （766 ページ）
- ルールの編集 （767 ページ）

• ルールのイネーブル化とディセーブル化 （782 ページ）

ステップ 1 次のいずれかを実行して、[Transparent Rules] ページ （1300 ページ）を開きます。

- （デバイスビュー）サポートされているデバイスタイプのポリシーセレクタから [ファイアウォール（Firewall）] > [トランスペアレントルール（Transparent Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ファイアウォール（Firewall）] > [トランスペアレントルール（Transparent Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （1302 ページ）が開きます。

ヒント 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。既存の行を選択して、行全体または特定のセルを編集することもできます。詳細については、ルールの編集 （767 ページ）を参照してください。

ステップ 3 ルールを設定します。次に、一般的に判断が必要となる重要な点を示します。フィールドを設定する方法の詳細については、[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （1302 ページ）を参照してください。

- 許可または拒否：ルールに一致したトラフィックを許可するか、またはドロップするか。
- インターフェイス：ルールを設定するインターフェイスまたはインターフェイス ロール。
- このルールを適用するトラフィックの方向（[in] または [out]）。デフォルトは [in] です。
- EtherType：トラフィックを識別する 16 進コードまたはキーワード（ASA/PIX/FWSM の場合だけ）。コードのリストについては、https://www.ietf.org/rfc/rfc1700.txtで RFC 1700 を参照し、「EtherType」を検索してください。ASA/PIX/FWSM の場合、キーワードを選択して一部の EtherType を識別できます。ASA/PIX/FWSM の場合、このコードは少なくとも 0x0600 である必要があります。
- マスク：IOS デバイスに適用するルールの場合は、EtherType に適用するマスクも指定する必要があります。EtherType が文字どおり解釈されるようにするには、0xFFFF を使用します。

EtherType のグループに適用する単一のルールを作成する場合は、EtherType を 2 進数に変換し、適切なマスクを計算します。この場合、1 は、EtherType を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します。次に、マスクを 16 進数に変換する必要があります。

ルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。

ステップ 5 （IOS デバイスだけ）IOS デバイスでトランスペアレント ルールを設定する場合、DHCP トラフィックを検査せずにブリッジ経由で転送できます。これを設定するには、[ファイアウォール（Firewall）] > [設定（Settings）] > [検査（Inspection）] ポリシーを選択し、[DHCPパススルーを許可（トランスペアレントファ

イアウォール）（Permit DHCP Passthrough (Transparent Firewall)）] オプションを選択します。この設定は、一部の IOS バージョンではサポートされていないため、検証結果をよく調べて、使用しているデバイスで設定できるかどうかを確認してください。

[Transparent Rules] ページ

[Transparent Rules] ページを使用して、非 IP レイヤ 2 トラフィックのアクセスを制御します（IP トラフィック アクセスを制御するには、アクセス ルールを使用します。アクセス ルールについて （913 ページ）を参照してください）。

トランスペアレント ルールの対象は、トランスペアレント ファイアウォール（トランスペアレント モードで動作する ASA、PIX 7.0+、および FWSM の各デバイス）またはレイヤ 3 インターフェイス（IOS 12.3(7)T+ デバイス上のブリッジ グループに属している）に限定されます。展開されたトランスペアレント ルールは、Ethertype アクセス コントロール リストになります。

トラフィックをデバイス経由で両方向に渡せるようにするには、すべてのブリッジ インターフェイスに同じルールを設定します。

トランスペアレント ファイアウォールの設定の詳細について、およびこれらのルールを展開するためのデバイス要件については、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください。

ヒント　ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなルールはデバイスから削除されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。

ナビゲーション パス

トランスペアレント ルールにアクセスするには、次のいずれかを実行します。

- （デバイス ビュー）サポートされているデバイス タイプのポリシー セレクタから [ファイアウォール（Firewall）] > [トランスペアレント ルール（Transparent Rules）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [ファイアウォール（Firewall）] > [トランスペアレント ルール（Transparent Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- （マップ ビュー）デバイスを右クリックし、[ファイアウォール ポリシーの編集（Edit Firewall Policies）] > [トランスペアレント ルール（Transparent Rules）] を選択します。

関連項目

- ルーテッド モードおよびトランスペアレント モードのインターフェイス （2336 ページ）

- ファイアウォール デバイスでのブリッジング ポリシーの設定 （2449 ページ）
- Cisco IOS ルータにおけるブリッジング （3135 ページ）
- ブリッジ グループの定義 （3137 ページ）
- ブリッジ グループ仮想インターフェイス （3136 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *300 : [Transparent Rules]* ページ

要素	説明
番号	順序が付けられたルール番号。
許可（Permit）	設定された次の条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。 • [Permit]：緑色のチェック マークとして表示されます。 • [Deny]：スラッシュの入った赤色の丸として表示されます。
EtherType	Ethernet パケット タイプ。パケット内の EtherType 値です。16 進コードまたはキーワードとなります。
Mask	EtherType の 16 ビットの 16 進マスク（IOS デバイスだけ）。0xFFFF のマスクは、EtherType がリテラルであることを示します。それ以外のマスクはすべて、EtherType 内の対応するビットを無視することを示します。マスクを完全に解釈するには、16 進数を 2 進数に変換する必要があります（2 進数 1 は、対応する EtherType 値を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します）。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。複数のエントリがある場合は、テーブル セル内に個別のサブフィールドとして表示されます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
Dir.	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用（304 ページ）を参照してください。
説明	ルールの説明（ある場合）。
[最後のチケット（Last Ticket(s)）]	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内またはセクション内で上下に移動するには、これらのボタンをクリックします。詳細については、ルールの移動とルール順序の重要性 （781 ページ）を参照してください。
[Add Row] ボタン	[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （1302 ページ）を使用して選択したテーブルの行のあとにルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。ルールを追加する方法の詳細については、ルールの追加および削除 （766 ページ）を参照してください。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。個々のセルを編集することもできます。詳細については、ルールの編集 （767 ページ）を参照してください。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。

[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス

[Add Transparent Firewall Rule] および [Edit Transparent Firewall Rule] の各ダイアログボックスを使用して、デバイス上で EtherType アクセス コントロール リストとして設定されているトランスペアレント ファイアウォール ルールを追加および編集します。トランスペアレント ルールを設定する前に、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を読んでください。

ナビゲーション パス

[Transparent Rules] ページ （1300 ページ）から、[列の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ルーテッド モードおよびトランスペアレント モードのインターフェイス （2336 ページ）
- ファイアウォール デバイスでのブリッジング ポリシーの設定 （2449 ページ）
- Cisco IOS ルータにおけるブリッジング （3135 ページ）
- ブリッジ グループの定義 （3137 ページ）
- ブリッジ グループ仮想インターフェイス （3136 ページ）
- ルールの編集 （767 ページ）
- ルールの追加および削除 （766 ページ）

フィールド リファレンス

表 301 : [Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	ルールをイネーブルにするかどうか。イネーブルにすると、デバイスに設定を展開したときにルールがアクティブになります。ディセーブルなルールには、ルール テーブルにハッシュ マークが重なって表示されます。詳細については、ルールのイネーブル化とディセーブル化 （782 ページ）を参照してください。
操作	定義した条件に基づいて、ルールがトラフィックを許可または拒否するかどうか。
インターフェイス	ルールが割り当てられるインターフェイスまたはインターフェイス ロール。ブリッジングされたトランスペアレント インターフェイスだけを選択する必要があります（詳細については、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください）。 インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストからインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。インターフェイスをリストに表示するには、あらかじめ定義しておく必要があります。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイス名で置き換えられます。 インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
トラフィックの方向	このルールが適用されるトラフィックの方向。 • [In]：インターフェイスで受信するパケット。 • [Out]：インターフェイスから送信するパケット。

要素	説明
EtherType	パケット内の EtherType 値に基づいたトラフィックを識別する 16 進のコードまたはキーワード（ASA/PIX/FWSM 専用）。次の内容を入力または選択します。 • 16 進の EtherType 値。コードのリストについては、http://www.ietf.org/rfc/rfc1700.txt「Ether Type」の RFC 1700 を参照してください。 • IOS デバイス：0x0000 ～ 0xFFFF の任意の値を入力できます。 • ASA/PIX/FWSM デバイス：値は 0x0600 以降である必要があります。 • ASA/PIX/FWSM デバイスの場合、次のキーワードも選択できます。 • bpdu：スパニング ツリー ブリッジ プロトコル データ ユニット • ipx：インターネット パケット交換 • mpls-unicast：マルチプロトコル ラベル スイッチング、ユニキャスト。 • mpls-multicast：MPLS マルチキャスト。 • isis：IS-IS パススルー • any：EtherType に関係なく、すべてのパケット。 • eii-ipx • raw-ipx **ヒント** 上記のリストのキーワード「isis」は、Security Manager 4.4 の新機能である IS-IS パススルーサポートを指します。「IS-IS パススルーサポート」とは、IS-IS トラフィックが透過モードで ASA を通過できることを意味します。 （注） 4.16 以降、ethertype dsap CLI を使用して、インストールされた ACE を、ether タイプ bpdu、ipx、または isis で作成されたかどうかに関係なく、ether タイプ dsap フォーマットで解釈します。この機能は、ASA 9.9(1) 以降のデバイスでサポートされています。
Wildcard Mask (IOS)	マスクは、EtherType コードの解釈方法を決定する 16 ビットの 16 進数です。 0xFFFF のマスクは、EtherType がリテラルであることを示します。それ以外のマスクはすべて、EtherType 内の対応するビットを無視することを示します。マスクを完全に解釈するには、16 進数を 2 進数に変換する必要があります（2 進数 1 は、対応する EtherType 値を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します）。

要素	説明
カテゴリ	ルールに割り当てられるカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	オプションで入力するルールの説明（最大 1024 文字）。

[Edit Transparent EtherType] ダイアログボックス

[Edit Transparent EtherType] ダイアログボックスを使用して、トランスペアレント ファイアウォール ルールの EtherType を編集します。トラフィックを識別する 16 進コードを入力します。ASA/PIX/FWSM デバイスの場合、一部のタイプのトラフィックには、キーワードを選択することもできます。コードのリストについては、http://www.ietf.org/rfc/rfc1700.txtで RFC 1700 を参照し、「EtherType」を検索してください。EtherType の詳細については、[Add Transparent Firewall Rule]/[Edit Transparent Firewall Rule] ダイアログボックス （1302 ページ）を参照してください。

詳細については、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください。

ナビゲーション パス

トランスペアレントルール（[Transparent Rules] ページ （1300 ページ））の [EtherType] セルを右クリックし、[EtherTypeの編集（Edit EtherType）] を選択します。一度に 1 つの行の EtherType を編集できます。

[トランスペアレントマスクの編集（Edit Transparent Mask）] ダイアログボックス

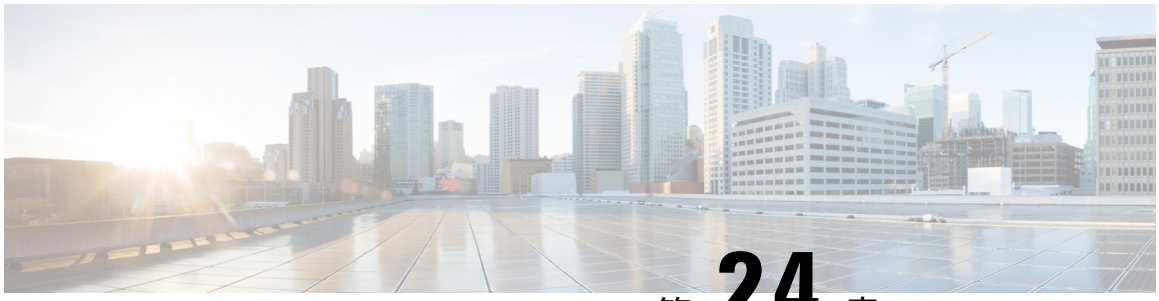
[Edit Transparent Mask] ダイアログボックスを使用して、IOS デバイス用のトランスペアレント ファイアウォール ルールのマスクを編集します。マスクは、EtherType コードの解釈方法を決定する 16 ビットの 16 進数です。

0xFFFF のマスクは、EtherType がリテラルであることを示します。それ以外のマスクはすべて、EtherType 内の対応するビットを無視することを示します。マスクを完全に解釈するには、16 進数を 2 進数に変換する必要があります（2 進数 1 は、対応する EtherType 値を文字どおり解釈することを示し、0 は、その位置にあるすべての値を許可することを示します）。

詳細については、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください。

ナビゲーション パス

トランスペアレントルール（[Transparent Rules] ページ （1300 ページ））の [マスク（Mask）] セルを右クリックし、[マスクの編集（Edit Mask）] を選択します。一度に 1 つの行のマスクを編集できます。



第 24 章

ネットワーク アドレス変換の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、および IPS をサポートしますが、拡張機能はサポートしていません。

ここでは、ネットワーク アドレス変換（NAT）に関する一般的な概念と、変換タイプおよびさまざまな実装について説明します。

- ネットワーク アドレス変換について （1307 ページ）
- Cisco IOS ルータにおける NAT ポリシー （1313 ページ）
- セキュリティ デバイスの NAT ポリシー （1326 ページ）

ネットワーク アドレス変換について

アドレス変換は、パケット内の実際のアドレスを、宛先ネットワーク上でルーティング可能な、マッピングされたアドレスで置き換えます。また、プロセスの一環として、デバイスにより変換データベースにその置換が記録されます。これらのレコードは、「xlate」エントリと呼ばれます。適切な xlate エントリが存在して、戻りパケットでのアドレス変換（マッピングされたアドレスの元の実アドレスの置換）を許可する必要があります。この手順は、「非変換」と呼ばれることもあります。したがって、ネットワークアドレス変換（NAT）は、実際には次の 2 つのステップから成ります。実アドレスからマッピングされたアドレスへの変換、およびリターントラフィックの逆変換。

NAT の主な機能の 1 つは、プライベート IP ネットワークがインターネットに接続できるようにすることです。ネットワーク アドレス変換により、プライベート IP アドレスはパブリック IP アドレスに置き換えられます。つまり、内部ネットワーク内のプライベート アドレスが、パブリックなインターネットで使用できる合法的なルーティング可能アドレスに変換されます。このようにして、NAT はパブリック アドレスを保護します。たとえば、ネットワーク全体で 1 つのパブリック アドレスだけを外部との通信に使用するように NAT ルールを設定できます。

NAT の他の機能には、次のおりです。

- セキュリティ：内部 IP アドレスを隠蔽することで、直接攻撃を阻止します。

- IP ルーティング ソリューション：重複する IP アドレスの問題がなくなります。
- 柔軟性：外部で使用可能なパブリック アドレスに影響を与えずに、内部 IP アドレッシング方式を変更できます。たとえば、インターネットにアクセス可能なサーバでは、インターネット用に固定の IP アドレスを保持できますが、内部的には、サーバ アドレスを変更できます。

シスコ デバイスでは、NAT（アウトバウンドの各ホスト セッションに、グローバルに一意のアドレスを提供する）とポートアドレス変換（PAT）（一意のポート番号を組み合わせた単一の同じアドレスを提供する）の両方を、最大で 64,000 個のアウトバウンドまたはインバウンドの同時ホスト セッションに対してサポートしています。NAT で使用するグローバル アドレスは、アドレス変換用に特別に指定したアドレス プールから取得されます。PAT で使用する一意のグローバル アドレスには、1 つのグローバル アドレスまたは指定されたインターフェイスの IP アドレスのいずれかを指定できます。

デバイスは、既存の NAT ルールが特定のトラフィックと一致した場合にアドレスを変換します。NAT ルールが一致しなかった場合、パケットの処理が続行されます。ただし、NAT 制御をイネーブルにしている場合は例外です。NAT 制御では、よりセキュリティの高いインターフェイス（内部）からよりセキュリティの低いインターフェイス（外部）へのパケット通過は NAT ルールに一致している必要があります。一致していない場合、パケットの処理は停止します。

シスコ デバイスは、インバウンドとアウトバウンドの両方の接続で、NAT または PAT を実行できます。インバウンドアドレスを変換するこの機能は、外部の、つまりセキュリティの高くないインターフェイス上のアドレスが、使用可能な内部 IP アドレスに変換されるため、「外部 NAT」と呼ばれます。アウトバウンド トラフィックを変換する場合と同様に、ダイナミック NAT、スタティック NAT、ダイナミック PAT、またはスタティック PAT を選択できます。必要に応じて、内部 NAT とともに外部 NAT を使用して、パケットの送信元 IP アドレスおよび宛先 IP アドレスの両方を変換できます。

（注） このマニュアルでは、すべての変換タイプを一般的に NAT と呼びます。それぞれのタイプの詳細については、アドレス変換のタイプ （1309 ページ）を参照してください。NAT を説明する場合、内部および外部という用語は 2 つのインターフェイス間のセキュリティ関係を表します。セキュリティ レベルの高い方が内部で、セキュリティ レベルの低い方が外部になります。

以前の ASA バージョンおよび他のデバイスと比較すると、ASA バージョン 8.3 のリリースでは、ネットワーク アドレス変換を設定する、インターフェイスに依存しない簡単なアプローチが提供されています。詳細については、ASA 8.3 以降のデバイスでの「簡易」NAT について （1311 ページ）を参照してください。

Cisco IOS ルータ

- Cisco IOS ルータにおける NAT ポリシー （1313 ページ）
  - [NAT] ページ - [Interface Specification] （1313 ページ）

- [NAT] ページ - [Static Rules] （1314 ページ）
- [NAT] ページ - [Dynamic Rules] （1319 ページ）
- [NAT] ページ - [Timeouts] （1323 ページ）

PIX、FWSM、および ASA セキュリティ デバイス

- セキュリティ デバイスの NAT ポリシー （1326 ページ）
- トランスペアレント モードの NAT （1326 ページ）
- [Translation Options] ページ （1329 ページ）
- **PIX、FWSM、および 8.3 よりも前の ASA デバイス**
  - PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
  - アドレス プール （1331 ページ）
  - [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
- **ASA 8.3+ デバイス**
  - ASA 8.3+ デバイスでの NAT の設定 （1352 ページ）
  - [Translation Rules]：ASA 8.3+ （1352 ページ）
  - [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （1355 ページ）
  - [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）
  - Per-Session NAT ルール: ASA 9.0（1）+ （1371 ページ）
  - [セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （1374 ページ）

関連項目

- アドレス変換のタイプ （1309 ページ）
- ASA 8.3 以降のデバイスでの「簡易」NAT について （1311 ページ）

アドレス変換のタイプ

次の表に、アドレス変換のさまざまなタイプについての簡単な説明を示します。

表 *302 :* アドレス変換のタイプ

スタティック NAT	実際の送信元アドレスから特定のマッピングされたアドレスへの固定変換。個々の送信元アドレスは、IP プロトコルおよびポート番号に関係なく、常にマッピングされた同じアドレスに変換されます。
スタティック PAT	特定の TCP または UDP ポート番号を含む実際の送信元アドレスから特定のマッピングされたアドレスおよびポートへの固定変換。つまり、個々の送信元アドレス/ポートは、常にマッピングされた同じアドレス/ポートに変換されます。
ポリシー スタティック NAT	実際の送信元アドレスから特定のマッピングされたアドレスへの固定変換。宛先ネットワーク/ホストも指定しますが、サービスは常に IP です。
ポリシー スタティック PAT	特定の TCP または UDP ポート番号を含む実際の送信元アドレスから特定のマッピングされたアドレスおよびポートへの固定変換。宛先ネットワーク/ホストおよびサービスも指定します。
ダイナミック NAT	実際の送信元アドレスから、共有アドレス プールから取得されるマッピングされたアドレスへのダイナミック変換。個々の送信元アドレスを、プール内の使用可能な任意のアドレスにマッピングできます。
ダイナミック PAT	実際の送信元アドレスから単一のマッピングされたアドレスへの変換。関連するポート番号のダイナミック変換によって、単一性が実現されます。つまり、個々の実際のアドレス/ポートの組み合わせは、マッピングされた同じアドレスに変換されますが、一意のポートに割り当てられます。これは、「オーバーロード」と呼ばれることがあります。
ポリシー ダイナミック NAT	共有アドレス プールを使用する、指定したインターフェイス上の特定の送信元アドレス/宛先アドレス/サービスの組み合わせのダイナミック変換。変換の方向（アウトバウンドまたはインバウンド）も指定します。
アイデンティティ NAT	指定したアドレスがそれ自身に変換されます。つまり、事実上、変換されません。アウトバウンド接続だけに適用されます。アイデンティティ NAT は、スタティック NAT の特別なタイプです。
NAT Exempt	指定した送信元/宛先アドレスの組み合わせに対して変換がバイパスされます。接続は、アウトバウンド方向とインバウンド方向の両方で開始できます。

（注） これらのタイプの一部は ASA 8.3 以降のデバイスに適用されませんが、ASA 8.3+ デバイスではダイナミック NAT と PAT のオプションが提供されます。これは、ダイナミック PAT のバックアップ機能を伴うダイナミック NAT です。

ASA 8.3 以降のデバイスでの「簡易」NAT について

以前の ASA バージョンおよび他のデバイスと比較すると、ASA バージョン 8.3 のリリースでは、ネットワーク アドレス変換（NAT）を設定する簡単なアプローチが提供されています。NAT の設定は、以前のフローベース方式を、「元のパケット」から「変換後のパケット」へのアプローチで置き換えることによって簡素化されています。

デバイス上のすべての NAT ルール（スタティック NAT、ダイナミック PAT、およびダイナミック NAT）が単一のテーブルに示され、基本的にすべての NAT ルールの設定に同じダイアログボックスが使用されます。NAT ルールはインターフェイスに依存せず（つまり、インターフェイスは任意）、このことは、セキュリティ レベルにも依存しないということを意味します。

NAT ルールは、セキュリティ レベルに依存しなくなりました。すべてのインターフェイスで構成されるグローバルアドレス空間が利用可能であり、キーワード「any」を使用して指定されます。すべてのインターフェイスフィールドはデフォルトで**any**に設定されるため、特定のインターフェイスが指定されない限り、ルールはすべてのインターフェイスに適用されます。

ネットワーク オブジェクト NAT

対応する NAT ルールが指定したセキュリティ デバイスに自動的に適用されるように、ホスト、アドレス範囲、およびネットワーク オブジェクトに NAT プロパティを定義することもできます。これらのオブジェクトを使用するということは、必要な IP アドレス、サービス、ポート、および任意のインターフェイスを 1 度だけ入力すればよいということを意味します。自動的に生成されるこれらのオブジェクトベースのルールは、「ネットワーク オブジェクト NAT」ルールと呼ばれます。これらのルールはルールテーブルからは編集または削除できません。Policy Object Manager で適切なオブジェクトを編集する必要があります。ただし、ネットワークオブジェクトに定義した後でルールテーブルから編集できます。詳細については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）を参照してください。

（注） ネットワークオブジェクト NAT ルールはデバイス固有であるため、ポリシービューの [変換ルール（Translation Rules）] テーブルには表示されません。

NAT テーブル

前述のとおり、デバイス上の NAT ルールはすべて単一のテーブルに表示されます。このテーブルは、「手動」セクション、ネットワークオブジェクト NAT ルールセクション、およびもう 1 つの手動ルールセクションの 3 つのセクションに分かれています。両方の手動セクションでルールを追加、編集、および順序付けできます。ネットワーク オブジェクト NAT ルールは自動的に追加および順序付けされます。前述のとおり、これらのルールを編集するには、関連するオブジェクトを編集する必要があります。

テーブル内の NAT ルールはトップダウン方式で最初に一致したルールから順に適用されます。つまり、パケットは、NAT ルールに一致した場合にだけ変換され、一致するとすぐに、その位置またはセクションに関係なく、NAT ルールの処理が停止します。

このテーブルを使用して、手動ルールの整理および管理を行うことができます。つまり、任意の順序でルールを挿入したり、ルールを再順序付けしたりできます。手動ルールの2つのセクションにより、自動オブジェクト ルールの前と後の両方に手動ルールを配置できます。

ネットワーク オブジェクト NAT ルールは、スタティック ルールがダイナミック ルールの前にくるように、自動的に配置されます。これらの2つのタイプは、それぞれさらに次のように順序付けされます。

- IP アドレスの数が最も少ないルール：1 つの IP アドレスを持つオブジェクトのルールのあとに、2 つのアドレスを持つオブジェクトのルールが表示され、そのあとに 3 つのアドレスを持つオブジェクトのルールが表示されるというように続きます。
- IP アドレス番号：同じ数の IP アドレスを持つオブジェクトについては、IP アドレス自体が番号順（昇順）になるように整列されます。たとえば、10.1.1.1 のルールのあとに 11.1.1.1 のルールが表示されます。
- オブジェクト名：IPアドレスが等しい場合は、オブジェクト名のアルファベット順にルールが順序付けされます。

また、変換は最初に一致したルールに基づくことに注意してください。

Destination Translation

手動のスタティック ルールでは、送信元アドレス変換に加えて、宛先アドレス変換も設定できます。送信元変換と宛先変換は、同じダイアログボックスで同時に定義できます。さらに、送信元変換にはスタティックまたはダイナミックを指定できますが、宛先変換は常にスタティックであり、手動ルールでだけ使用できます。

双方向または Twice NAT

手動のスタティックルールを作成するときに、[双方向（Bi-directional）] オプションを選択できます。このオプションでは、実際には 2 つのスタティック NAT ルール（両方向の変換を含む）を示す 1 つのエントリがルールテーブル内に作成されます。つまり、指定した送信元/変換後のアドレスのペアに対してスタティック ルールが作成されるとともに、変換後のアドレス/送信元のペアに対して、逆のルールが作成されます。

たとえば、[Source] フィールドが [Host1] で [Translated] フィールドが [Host2] のスタティック ルールを作成するときに [Bi-directional] を選択した場合、ルール テーブルに 2 つの行が追加されます。1 つは Host1 を Host2 に変換する行、もう 1 つは Host2 を Host1 に変換する行です。

この変換は、実際には2つのルールを取得および処理するために必要なルックアップが 1 つで済むため、「Twice NAT」と呼ばれることもあります。

多対 1 のアドレッシング

一般に、スタティック NAT ルールは、1 対 1 のアドレス マッピングを使用して設定されますが、多数の IP アドレスを少数または 1 つの IP アドレスにマッピングするスタティック NAT ルールを定義できるようになりました。機能的には、多対少数のマッピングは多対1のマッピングと同じですが、設定がより複雑になるため、必要に応じてアドレスごとに多対1のルールを作成することを推奨します。

多対1のアドレッシングは、たとえば、要求を内部ネットワークにリダイレクトするロードバランサにアクセスするためにパブリック IP アドレスの範囲を使用する場合などに役立つことがあります。

関連項目

- [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （1355 ページ）
- [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）

Cisco IOS ルータにおける NAT ポリシー

[NAT] ポリシー ページの次のタブから Cisco IOS ルータ上の NAT ポリシーを設定できます。

- [NAT] ページ - [Interface Specification] （1313 ページ）
- [Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス （1316 ページ）
- [NAT] ページ - [Dynamic Rules] （1319 ページ）
- [NAT] ページ - [Timeouts] （1323 ページ）

ネットワーク アドレス変換（NAT）はプライベートな内部 LAN アドレスをグローバルにルーティング可能な IP アドレスに変換します。NAT を使用すると、少ない数のパブリック IP アドレスで多数のホストにグローバル接続を提供できます。

詳細については、ネットワーク アドレス変換について （1307 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[NAT] ページ - [Interface Specification]

NAT ルールを作成する前に、内部および外部インターフェイスを指定して、変換されるトラフィックの「方向」を定義する必要があります。内部インターフェイスは、通常、ルータが提供する LAN に接続されます。外部インターフェイスは、通常、組織の WAN またはインターネットに接続されます。少なくとも内部インターフェイスおよび外部インターフェイスを1つずつ指定して、ルータがネットワーク アドレス変換を実行できるようにする必要があります。

内部および外部の指定は、変換ルールを解釈するときに使用されます。つまり、内部インターフェイスに接続されたアドレスが、外部インターフェイス上のアドレスに変換されます。これらのインターフェイスの定義が完了したあと、これらをすべてのスタティックおよびダイナミック NAT 変換ルールに使用します。

[NAT] ポリシー ページの [Interface Specification] タブを使用して、内部および外部インターフェイスを指定します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択し、次に [インターフェイスの仕様（Interface Specification）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[インターフェイスの仕様（Interface Specification）] タブをクリックします。

内部インターフェイスと外部インターフェイスの定義

[NAT内部インターフェイス（NAT Inside Interfaces）] および [NAT外部インターフェイス（NAT Outside Interfaces）] フィールドに、内部および外部インターフェイスのインターフェイス名またはインターフェイスロールをそれぞれ入力するか、または選択します。複数の名前またはロールは、カンマで区切ります（Ethernet1/1, Ethernet1/2 など）。両方のフィールドに同じ名前は入力できないことに注意してください。

関連項目

- Cisco IOS ルータにおける NAT ポリシー （1313 ページ）
- [NAT] ページ - [Static Rules] （1314 ページ）
- [NAT] ページ - [Dynamic Rules] （1319 ページ）
- [NAT] ページ - [Timeouts] （1323 ページ）

[NAT] ページ - [Static Rules]

変換が必要なローカル アドレスと、そのローカル アドレスが変換されるグローバル アドレスを指定して、スタティック NAT ルールを定義します。これは、スタティックまたは固定のマッピングであり、ローカル アドレスは常に同じグローバル アドレスに変換されます。

単一ホストのアドレスを変換するスタティック NAT ルールと、サブネット内の複数のアドレスを変換するスタティック ルールを定義できます。複数のローカル アドレスで同じグローバル アドレスを使用する必要がある場合は、必要なポート リダイレクト情報を定義する必要があります。リダイレクト情報では、グローバル アドレスを使用して各ローカル アドレスにそれぞれ異なるポートを定義します。

（注） VPN を介して送信されるトラフィックに対しては NAT を実行しないことを強く推奨します。このトラフィックでアドレスを変換すると、暗号化された状態ではなく暗号化されていない状態で VPN を介して送信されます。

スタティック ルールの作成手順は、変換されるアドレスがポート、単一ホスト、またはサブネット全体のいずれを示しているかで決まります。

- 単一ホスト用のスタティック NAT ルールを定義するには、変換する元のアドレスと、そのアドレスが変換されるグローバルアドレスを入力します。グローバルアドレスは、デバイス上のインターフェイスから取得できます。
- サブネット用のスタティック NAT ルールを定義するには、元のアドレスとしてサブネット内（サブネットマスクを含む）のアドレスの 1 つを入力し、変換されたアドレスとして使用するグローバルアドレスの 1 つを入力します。ルータは、入力したサブネットマスクに基づいて残りのアドレスを設定します。
- ポート用のスタティック NAT ルールを定義するには、元の IP アドレスと、そのアドレスが変換されるグローバルアドレスを入力します。グローバルアドレスは、デバイス上のインターフェイスから取得できます。さらに、ポートが使用するプロトコルと、ローカル ポート番号およびグローバル ポート番号も選択する必要があります。

これらのルールを追加および編集するには、[Add Static NAT Rule] および [Edit Static NAT Rule] ダイアログボックスを使用します。このページのテーブルに表示されるフィールドについては、[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス （1316 ページ）を参照してください。

はじめる前に

- NAT に使用する内部インターフェイスと外部インターフェイスを定義します。[NAT] ページ - [Interface Specification] （1313 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択し、次に [スタティックルール（Static Rules）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[スタティックルール（Static Rules）] タブをクリックします。

関連項目

- Cisco IOS ルータにおける NAT ポリシー （1313 ページ）
- [NAT] ページ - [Dynamic Rules] （1319 ページ）
- [NAT] ページ - [Timeouts] （1323 ページ）
- Security Manager の標準のルール テーブルに関する項：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）

• テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス

[Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックスを使用して、スタティック アドレス変換ルールを追加または編集します。タイトルを除き、2 つのダイアログボックスは同じです。

ナビゲーション パス

[NAT] ページ - [Static Rules] （1314 ページ）タブに移動します。テーブルの下にある [追加（Add）] ボタンをクリックして新しいルールを追加するか、テーブルでルールを選択し、[編集（Edit）] をクリックしてそのルールを更新します。

関連項目

• インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 303 : [Add NAT Static Rule]/[Edit NAT Static Rule] ダイアログボックス

要素	説明
Static Rule Type	このスタティック ルールで変換されるローカル アドレスのタイプ。 • [Static Host]：単一ホストでスタティック アドレス変換が必要な場合。 • [Static Network]：サブネットでスタティック アドレス変換が必要な場合。 • [Static Port]：単一ポートでスタティック アドレス変換が必要な場合。このオプションを選択した場合は、[Port Redirection] パラメータを定義する必要があります。
元のアドレス	IP アドレス、または変換されるアドレスを示すネットワーク/ホスト オブジェクトの名前。オブジェクト名を入力するか、または選択できます。 ネットワーク/ホストオブジェクトは、ネットワーク、ホスト、またはこれらの両方を表す IP アドレスの論理集合です。詳細については、ネットワーク/ホストオブジェクトについて （391 ページ）を参照してください。 （注） Security Manager の管理トラフィックを変換してしまう可能性があるため、このルータに属するローカル アドレスは入力しないでください。このトラフィックを変換すると、ルータと Security Manager 間の通信が失われます。

要素	説明
Translated Address	ダイアログボックスのこのセクションのオプションを使用して、元のアドレスが変換されるアドレスを指定します。 • [IPの指定（Specify IP）]：IP アドレス、または変換後のアドレスを提供するネットワーク/ホストオブジェクトの名前を指定するには、このオプションを選択します。IPアドレス、またはネットワーク/ホストオブジェクトの名前を [変換後のIP/ネットワーク（Translated IP/Network）] フィールドに追加します。オブジェクト名を入力するか、または選択できます。 • [インターフェイスIPの使用（Use Interface IP）]：特定のインターフェイスに割り当てられているIPアドレスを変換後のアドレスとして使用するように指定するには、このオプションを選択します。対象の [インターフェイス（Interface）] の名前を入力するか、選択します。（これは、通常、変換されたパケットがルータから発信される際の発信元のインターフェイスです）。 （注） このオプションは、ルールのタイプとして [Static Network] を選択している場合には使用できません。1 つのインターフェイスに 1 つのスタティック ルールしか定義できません。
Port Redirection	これらのパラメータは、アドレス変換のポート情報を指定します。ポートアドレス変換を使用すると、デバイスごとに異なるポートを指定しているかぎり、複数のデバイスに同じパブリック IP アドレスを使用できます。 （注） これらのポートは、ルールのタイプとして [Static Port] を選択している場合にだけ使用できます。 [リダイレクトポート（Redirect Port）]：ルールのタイプとして [スタティックポート（Static Port）] を選択した場合、このチェックボックスは自動的にオンになります。変更はできません。次のフィールドに、適切な情報を入力します。 • [プロトコル（Protocol）]：これらのポートで使用する通信プロトコル：TCP または UDP。 • [ローカルポート（Local Port）]：送信元ネットワーク上のポート番号。有効値の範囲は 1 ～ 65535 です。 • [グローバルポート（Global Port）]：ルータによってこの変換に使用される宛先ネットワーク上のポート番号。有効値の範囲は 1 ～ 65535 です。

要素	説明
詳細設定（Advanced）	このセクションには、任意の高度な変換オプションが含まれています。 （注） [Advanced] オプションは、変換されたアドレスの定義方法として [Specify IP] オプションを選択している場合にだけ使用できます。 • [No Alias]：選択すると、グローバル IP アドレス変換の自動エイリアス設定がディセーブルになります。 内部グローバル プールとして使用する NAT プールが、接続されているサブネット上のアドレスで構成されている場合、ルータでこれらのアドレスのアドレス解決プロトコル（ARP）要求に応答できるように、そのアドレスに対してエイリアスが生成されます。 選択を解除すると、グローバル アドレスのエイリアスが許可されます。 • [No Payload]：選択すると、ペイロード内の埋め込みアドレスまたはポートの変換が禁止されます。 ペイロード オプションは、同じ IP アドレスを共有している重複ネットワーク上のデバイス間で NAT を実行します。外部デバイスが DNS クエリーを送信して内部デバイスにアクセスした場合、DNS 応答のペイロード内のローカル アドレスは、関連する NAT ルールに応じて、グローバル アドレスに変換されます。 この機能は、[No Payload] オプションを選択することでディセーブルにできます。ディセーブルにしなかった場合、ペイロード内の埋め込みアドレスおよびポートが変換されることがあります。詳細については、重複するネットワークのペイロード オプションのディセーブル化 （1318 ページ）を参照してください。 • [Create Extended Translation Entry]：オンにすると、変換テーブル内に拡張変換エントリ（アドレスおよびポート）が作成されます。これにより、複数のグローバル アドレスを単一のローカル アドレスに関連付けることができます。これがデフォルトです。 このオプションをオフにすると、簡単な変換エントリが作成され、単一のグローバル アドレスをローカル アドレスに関連付けできるようになります。 （注） このオプションは、ルールのタイプとして [Static Port] を選択している場合には使用できません。

重複するネットワークのペイロード オプションのディセーブル化

すでに合法的に所有されインターネットまたは外部ネットワーク上のデバイスに割り当てられている IP アドレスを、独自のネットワーク上の別のデバイスに割り当てると、ネットワークの重複が発生します。また、ネットワークの重複は、それぞれのネットワーク内で RFC 1918 IP アドレスを使用している 2 つの会社をマージした場合にも発生する可能性があります。これらの 2 つのネットワークは、可能であれば、すべてのデバイスのアドレスを再指定することなく、通信できる必要があります。

この通信は、次のように実現されます。内部デバイスの IP アドレスは外部デバイスに割り当てられているアドレスと同じであるため、外部デバイスは内部デバイスの IP アドレスを使用できません。代わりに、外部デバイスは内部デバイスのドメイン名を問い合わせるドメインネームシステム（DNS）クエリを送信します。このクエリーの送信元は外部デバイスの IP アドレスであり、この IP アドレスは指定したアドレス プールのアドレスに変換されます。内部ネットワーク上に配置されている DNS サーバーは、パケットのデータ部分に格納されている内部デバイスのドメイン名に関連付けられた IP アドレスを使用して応答します。応答パケットの宛先アドレスは外部デバイスのアドレスに変換され、応答パケットのデータ部分に格納されているアドレスは別のアドレスプールのアドレスに変換されます。このような方法で、外部デバイスは、内部デバイスの IP アドレスが 2 番めのアドレス プールのアドレスの 1 つであることを学習して、内部デバイスとの通信時にこのアドレスを使用します。NAT を実行しているルータは、この時点で変換を処理します。

ペイロード内のアドレスの変換をディセーブルにするには、グローバル IP 変換に基づいたスタティック NAT ルールを作成するときに、[ペイロードなし（No Payload）] オプションをオンにします。

[NAT] ページ - [Dynamic Rules]

ルータの [NAT] ページの [NATダイナミックルール（NAT Dynamic Rules）] タブを使用して、ダイナミックアドレス変換ルールを管理します。ダイナミック アドレス変換ルールは、特定のインターフェイスの IP アドレス（ダイナミック ポート変換を使用）、または宛先ネットワーク内でグローバルに一意であるアドレス プール内のアドレスを使用して、ホストをアドレスに動的にマッピングします。

ダイナミック NAT ルールの定義

ダイナミック NAT ルールを定義するには、最初に、変換が必要なトラフィックをルールで指定しているアクセス コントロール リスト（ACL）を選択します。

次に、変換後の IP アドレスを持つインターフェイスを選択するか、または使用されるアドレス プールを定義する必要があります。プールを定義するには、アドレスの範囲を指定して、その範囲に一意の名前を指定します。複数の範囲を指定できます。ルータは、インターネットまたは別の外部ネットワークとの接続に、プール内の使用可能なアドレス（スタティック変換にも、独自の WAN IP アドレスにも使用されていないアドレス）を使用します。アドレスは、不用になると、あとで別のデバイスに動的に割り当てられるようにアドレス プールに戻されます。

ネットワークのアドレッシング要求がダイナミック NAT プール内の使用可能なアドレスの数を超えた場合は、ポートアドレス変換（PAT）機能（オーバーロードとも呼ばれる）を使用して、多数のプライベート アドレスを 1 つまたは少数のパブリック IP アドレス グループに関連付け、ポート アドレッシングを使用して各変換を一意にすることができます。PAT をイネーブルにすると、ルータは各アウトバウンド変換スロットの IP アドレスに対して一意のポート番号を選択します。この機能は、アウトバウンド接続に割り当て可能な十分な数の一意の IP アドレスがない場合に役立ちます。ポート アドレス変換は、アドレス プールが枯渇するまでは行われません。

（注） デフォルトでは、Security Manager は VPN を介して送信されるトラフィックに対して NAT を実行しません。それ以外の場合、暗号化の前には常に NAT が実行されるため、インターフェイスに定義されている NAT ACL とクリプト ACL の両方に含まれるすべてのトラフィックが暗号化されずに送信されます。ただし、このデフォルト設定は変更できます。

ヒント [Global VPN Settings] ページから直接、VPN トポロジのスポーク上のスプリット トンネル トラフィックに対して PAT を実行できます。スポークごとにダイナミック NAT ルールを作成する必要はありません。個々のデバイスに定義した NAT ルールによって、VPN 設定は上書きされます。詳細については、VPN グローバル NAT 設定 （1532 ページ）を参照してください。

これらのルールを追加および編集するには、[Add Dynamic NAT Rule] および [Edit Static NAT Rule] ダイアログボックスを使用します。このページのテーブルに表示されるフィールドについては、[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。

はじめる前に

- NAT に使用する内部インターフェイスと外部インターフェイスを定義します。[NAT] ページ - [Interface Specification] （1313 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシー セレクタから [NAT] を選択し、次に [ダイナミックルール（Dynamic Rules）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[ダイナミックルール（Dynamic Rules）] タブをクリックします。

関連項目

- Cisco IOS ルータにおける NAT ポリシー （1313 ページ）
- [NAT] ページ - [Static Rules] （1314 ページ）
- [NAT] ページ - [Timeouts] （1323 ページ）
- Security Manager の標準のルール テーブルに関する項：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）

• テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス

[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックスを使用して、ダイナミック アドレス変換ルールを追加または編集します。タイトルを除き、2つのダイアログボックスは同じです。

ナビゲーション パス

[NAT] ページ - [Dynamic Rules] （1319 ページ）タブに移動します。テーブルの下にある [追加（Add）] ボタンをクリックして新しいルールを追加するか、テーブルでルールを選択し、[編集（Edit）] をクリックしてそのルールを更新します。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *304 : [Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule]* ダイアログボックス

要素	説明
トラフィック フロー	[アクセスリスト（Access List）] フィールドで、ダイナミック変換が必要なアドレスをエントリで定義しているアクセス制御リスト（ACL）オブジェクトの名前を入力するか選択します。 （注） 指定した ACL で、このルータ上のデバイス アドレスを経由する Security Manager 管理トラフィックの変換が許可されていないことを確認してください。このトラフィックを変換すると、ルータと Security Manager 間の通信が失われます。

要素	説明
Translated Address	ダイアログボックスのこのセクションのオプションを使用して、ダイナミック変換に使用する方式およびアドレスを指定します。 • [ユーザーインターフェイスIP（Use Interface IP]：特定のインターフェイスに割り当てられているグローバルに登録された IP アドレスを変換後のアドレスとして使用するように指定するには、このオプションを選択します。ポートアドレッシングによって、各変換が一意であることが保証されます（[Enable Port Translation (Overload)] オプションは、[Use Interface IP] を選択すると自動的にオンになります）。 対象の [インターフェイス（Interface）] の名前を入力するか、選択します。これは、通常、変換されたパケットがルータから発信される際の発信元のインターフェイスです。つまり、インターフェイスまたはインターフェイス ロールは、ルータ上の外部インターフェイスを示している必要があります（ [NAT] ページ - [Interface Specification] （1313 ページ）を参照）。 • [アドレスプール（Address Pool）]：[ネットワーク範囲（Network Ranges）] プールで指定したアドレスに基づいてアドレス変換を実行させるには、このオプションを選択します。 プレフィックスを含めた 1 つまたは複数のアドレス範囲を入力します。書式は min1-max1/prefix（CIDR 表記）を使用します（「prefix」は有効なネットマスクを示します）。たとえば、172.16.0.0-172.31.0.223/12 のように入力します。 必要な数のアドレス範囲をアドレス プールに追加できますが、すべての範囲で同じプレフィックスを共有している必要があります。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
設定	このセクションには 2 つのオプションが含まれています。 • [ポート変換（オーバーロード）の有効化（Enable Port Translation (Overload)）]：選択すると、アドレスプール内のグローバルアドレスの供給が枯渇した場合に、ルータはポートアドレッシング（PAT）を使用します。選択を解除すると、PAT は使用されません。 （注） [Translated Address] セクションで [Use Interface IP] を選択した場合、このチェックボックスは自動的にオンになります。変更はできません。 • [VPNトラフィックを変換しない（サイト間VPNのみ）（Do Not Translate VPN Traffic (Site-to-Site VPN only)）]：このオプションの選択を解除すると、サイト間 VPN 向けのトラフィックに対してアドレス変換が許可されます。 選択すると、VPN トラフィックに対してアドレス変換は実行されません。選択を解除した場合、ルータは、NAT ACL とクリプト ACL 間でアドレスが重複している場合に、VPN トラフィックに対してアドレス変換を実行します。 （注） このオプションの選択は解除しないことを強く推奨します。解除した場合、NAT ACL とクリプト ACL の両方に定義されているすべてのトラフィックが暗号化されずに送信されます。IPsec に対して NAT を実行する場合も、このオプションは選択したままにしておくことを推奨します。このオプションを選択しても、重複するネットワークから到着したアドレスの変換は実行されます。 この設定は、NAT ACL がサイト間 VPN で使用されるクリプト ACL と重複している状況でだけ適用されます。インターフェイスは最初に NAT を実行するため、この重複内のアドレスから到着したトラフィックはすべて変換され、その結果、トラフィックは暗号化されずに送信されます。このチェックボックスをオンのままにすると、このような問題は発生しなくなります。 （注） このオプションは、リモート アクセス VPN には適用されません。

[NAT] ページ - [Timeouts]

ルータの [NAT] ページの [NATタイムアウト（NAT Timeouts）] タブを使用して、ポートアドレス（オーバーロード）変換のタイムアウト値を管理します。これらのタイムアウトにより、指定した非アクティブ期間が経過したあと、ダイナミック変換は期限切れになります。また、このページのオプションを使用すると、ダイナミック NAT テーブルに格納できるエントリの数を制限したり、PAT 処理を含まないすべてのダイナミック変換に対してデフォルトのタイムアウトを変更したりできます。

ダイナミック NAT のタイムアウトについて

ダイナミック NAT 変換には不使用に対するタイムアウト時間があり、この時間が経過すると、ダイナミック NAT 変換は期限切れとなり、変換テーブルから削除されます。各変換エントリ

には、そのエントリを使用するトラフィックの状況に応じた追加情報が含まれているため、オーバーロード機能をイネーブルにして PAT を実行する場合は、これらのタイムアウトを詳細に制御できるさまざまな値を指定できます。

たとえば、非 DNS 変換は、デフォルトでは 5 分後にタイムアウトしますが、DNS 変換は 1 分後にタイムアウトします。さらに、TCP 変換は、RST または FIN がストリーム上で検出されないかぎり 24 時間後にタイムアウトし、検出された場合は、1 分後にタイムアウトします。これらのタイムアウト値はいずれも変更できます。

（注） すべてのダイナミック ルールに対してポート変換（オーバーロード）機能をディセーブルにしている場合は、PAT 関連のタイムアウト値を入力する必要はありません。ただし、PAT 以外のダイナミック変換のデフォルト タイムアウト値は変更できます（デフォルトでは、すべてのダイナミック変換は 24 時間後に期限切れになります）。オーバーロード機能の詳細については、[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [NAT] を選択し、次に [タイムアウト（Timeouts）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [NAT（ルータ）（NAT (Router)）] > [変換ルール（Translation Rules）] を選択します。既存のポリシーを選択するか新しいポリシーを作成してから、[タイムアウト（Timeouts）] タブをクリックします。

関連項目

- [NAT] ページ - [Interface Specification] （1313 ページ）
- [NAT] ページ - [Static Rules] （1314 ページ）
- [NAT] ページ - [Dynamic Rules] （1319 ページ）

フィールド リファレンス

表 305 : [NAT Timeouts] タブ

要素	説明
エントリの最大数（Max Entries）	ダイナミック NAT テーブルに格納できるエントリの最大数。1 ～ 2147483647 の値を入力できます。またはこのフィールドを空白（デフォルト）のままにできます。空白にすると、テーブル内のエントリの数は無制限になります。
Timeout (sec.)	ダイナミック変換が期限切れになるまでの秒数。PAT（オーバーロード）変換には適用されません。デフォルトは 86400 秒（24 時間）です。

要素	説明
UDP Timeout (sec.)	ユーザー データグラム プロトコル（UDP）ポートに適用されるタイムアウト値。デフォルトは 300 秒（5 分）です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。
DNS Timeout (sec.)	Domain Naming System（DNS; ドメイン ネーミング システム）サーバー接続に適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。
TCP Timeout (sec.)	伝送制御プロトコル（TCP）ポートに適用されるタイムアウト値。デフォルトは 86400 秒（24 時間）です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。
FINRST Timeout (sec.)	終了（FIN）パケットまたはリセット（RST）パケット（どちらも接続を終了させる）が TCP ストリーム内で検出された場合に適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。
ICMP Timeout (sec.)	インターネット制御メッセージ プロトコル（ICMP）フローに適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。

要素	説明
PPTP Timeout (sec.)	NAT Point-to-Point Tunneling Protocol（PPTP; ポイントツーポイント トンネリング プロトコル）フローに適用されるタイムアウト値。デフォルトは 86400 秒（24 時間）です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。
SYN Timeout (sec.)	同期伝送（SYN）メッセージ（正確なクロッキングに使用）が検出されたあと、TCP フローに適用されるタイムアウト値。デフォルトは 60 秒です。 （注） この値が適用されるのは、ダイナミック NAT ルールでポート変換（オーバーロード）がイネーブルになっている場合だけです。[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照してください。

セキュリティ デバイスの NAT ポリシー

ここでは、管理対象のセキュリティ アプライアンス（PIX ファイアウォール、Catalyst スイッチの Firewall Service Modules（FWSM; ファイアウォール サービス モジュール）、8.3 よりも前のバージョンの Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）、および ASA 8.3+ デバイス）でネットワーク アドレス変換（NAT）オプションを設定する方法について説明します。説明の順序は次のとおりです。

- トランスペアレント モードの NAT （1326 ページ）
- [Translation Options] ページ （1329 ページ）
- **PIX、FWSM、および 8.3 よりも前の ASA**
  - PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
  - アドレス プール （1331 ページ）
- **ASA 8.3+**
  - ASA 8.3+ デバイスでの NAT の設定 （1352 ページ）
  - [Translation Rules]：ASA 8.3+ （1352 ページ）

トランスペアレント モードの NAT

トランスペアレント モードで動作しているセキュリティ アプライアンスで NAT を使用すると、上流または下流のルータでそれらのネットワークに対して NAT を実行する必要性がなくなります。トランスペアレント モードの NAT には、次の要件および制限があります。

- マッピングされたアドレスがトランスペアレントファイアウォールと同じネットワークにない場合、マッピングされたアドレス用に、（セキュリティアプライアンス経由で）下流のルータを指し示すスタティック ルートを上流のルータに追加する必要があります。
- 実際の宛先アドレスが直接セキュリティアプライアンスに接続されていない場合は、実際の宛先アドレス用に、下流のルータを指し示すスタティック ルートをセキュリティ アプライアンスに追加する必要もあります。NAT を使用しない場合、上流のルータから下流のルータへのトラフィックは MAC アドレス テーブルを使用するため、セキュリティ アプライアンス上のルートを必要としません。ただし、NAT を使用すると、セキュリティ アプライアンスは MAC アドレス ルックアップの代わりにルート ルックアップを使用するため、下流のルータへのスタティック ルートが必要になります。
- トランスペアレント ファイアウォールにはインターフェイス IP アドレスがないため、インターフェイス PAT を使用できません。
- ARP インスペクションはサポートされていません。さらに、何らかの理由でセキュリティアプライアンスの片側にあるホストからもう片側にあるホストに ARP 要求が送信され、送信側ホストの実アドレスが同じサブネット上の別のアドレスにマップされている場合、その実アドレスは ARP 要求で表示されたままになります。

[CGNATマップ（CGNAT Map）] ページ

バージョン 4.20 以降、Cisco Security Manager は、シングル、マルチコンテキスト、およびルーテッドモードで動作する ASA 9.13(1) デバイスのアドレスおよびポート（CGNAT マップ）ドメインのキャリアグレード NAT マッピングをサポートしています。この機能は、デフォルトまたは基本的なマッピングルールを使用して MAP ドメインを構成するのに役立ちます。

（注） トランスペアレントモードでは CGNAT マップはサポートされていません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [CGNATマップ（CGNAT MAP）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[NAT（PIX/ASA/FWSM）] > [CGNAT マップ（CGNAT MAP）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [CGNATマップ（CGNAT MAP）] を右クリックして新しい CGNAT マップポリシーを作成します。

関連項目

- セキュリティ デバイスの NAT ポリシー （1326 ページ）

フィールド リファレンス

表 *306 :*

要素	説明
マップドメインの追加（Add Map Domain）	選択すると、基本またはデフォルトのマッピングルールを使用してマップドメインを追加できます。
マップドメイン名（Map Domain Name）	マッピングルールを適用する必要があるマップドメインの名前を入力します。
Basic Mapping Rule	[基本マッピングルール（Basic Mapping Rule）] チェックボックスをオンにして、IPv4 および IPv6プレフィックス、共有率、および開始ポート番号を指定します。
Default Mapping Rule	IPv6 プレフィックスを入力して、デフォルトのマッピングルールを適用します。

[グローバルオプション（Global Options）] ページ

Cisco Security Manager バージョン 4.9 は、ASA デバイス 9.5(1) 以降のポートブロック割り当てのブロックサイズとホストあたりの最大ブロック数を設定するキャリアグレードNATをサポートしています。グローバルオプションを設定するには、[グローバルオプション（Global Options）] ページを使用します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [グローバルオプション（Global Options）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[NAT（PIX/ASA/FWSM）] > [グローバルオプション（Global Options）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [グローバルオプション（Global Options）] を右クリックして新しいポリシーを作成します。

関連項目

- セキュリティ デバイスの NAT ポリシー （1326 ページ）
- [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （1355 ページ）

フィールド リファレンス

表 *307 : [*グローバルオプション（***Global Options***）*]* ページ

要素	説明
xlate block-allocation size	32 ～ 4096 の値を入力します。デフォルト値は 512 です。
xlate block-allocation maximum-per-host	1 ～ 8 の値を入力します。デフォルト値は 4 です。
xlate block-allocation interim logging	タイマー間隔を設定して、その時点で ASA 9.12(1) 以降のデバイスに割り当てられているすべてのアクティブポートブロックの syslog を生成します。43200 ～ 604800 の値を入力します。

[Translation Options] ページ

[Translation Options] ページを使用して、選択したセキュリティ アプライアンスのネットワーク アドレス変換に影響するオプションを設定します。これらの設定は、デバイス上のすべてのインターフェイスに適用されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [変換オプション（Translation Options）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[NAT (PIX/ASA/FWSM)] > [変換オプション（Translation Options）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [変換オプション（Translation Options）] を右クリックして新しいポリシーを作成します。

関連項目

- セキュリティ デバイスの NAT ポリシー （1326 ページ）

フィールド リファレンス

表 *308 : [Translation Options]* ページ

要素	説明
アドレス変換なしでファイアウォール経由のトラフィックを有効にする（Enable traffic through the firewall without address translation）	選択すると、トラフィックはアドレス変換なしでセキュリティアプライアンスを通過できるようになります。このオプションを選択しなかった場合、変換ルールと一致しないトラフィックはすべてドロップされます。 （注） このオプションは、PIX 7.x、FWSM 3.x、および ASA デバイスのみで使用可能です。
Enable xlate bypass	選択すると、変換されないトラフィックに対する NAT セッションの確立がディセーブルになります（この機能は「xlate バイパス」と呼ばれます）。 （注） このオプションは、FWSM 3.2 以降のみで使用可能です。 デフォルトでは、FWSM は、NAT が使用されていなくても、すべての接続に対して NAT セッションを作成します。たとえば、NAT 制御がイネーブルになっていない場合、NAT 免除またはアイデンティティ NAT が使用されている場合、または同じセキュリティのインターフェイスを使用しており NAT を設定していない場合にも、セッションは変換対象でない接続ごとに作成されます。NAT セッションの数には最大限度があるため（266、同時には 144）、このような種類の NAT セッションで制限に達してしまう可能性があります。制限に達しないようにするには、xlate バイパスをイネーブルにします。 NAT 制御をディセーブルにして変換対象でないトラフィックを存在させるか NAT 免除を使用する場合、または NAT 制御をイネーブルにして NAT 免除を使用する場合には、xlate バイパスを使用すると、FWSM はこれらのタイプの変換対象でないトラフィックに対してセッションを作成しません。ただし、次の場合には、NAT セッションが作成されます。 • （NAT 制御の有無に関係なく）アイデンティティ NAT を設定する場合。アイデンティティ NAT は 1 つの変換と見なされます。 • NAT 制御で同じセキュリティのインターフェイスを使用する場合。同じセキュリティのインターフェイス間のトラフィックは、そのトラフィックに NAT を設定していなくても、NAT セッションを作成します。このような場合に NAT セッションを回避するには、NAT 制御をディセーブルにするか、または NAT 免除と xlate バイパスを使用します。
Do not translate VPN traffic	選択すると、VPN トラフィックはアドレス変換なしでセキュリティ アプライアンスを通過します。

要素	説明
Clear translates for existing connections	選択すると、ダイナミック変換に割り当てられた変換スロットおよび関連付けられた接続が、各セッションのあとにクリアされます。 セキュリティアプライアンスを介して接続し、なんらかの形式の NAT または PAT を受ける各セッションには、「xlate」と呼ばれる変換スロットが割り当てられます。これらの変換スロットは、セッションが完了した後も持続する可能性があり、変換スロットの枯渇、予期しないトラフィック動作、またはその両方につながる可能性があります。

PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、PIX デバイスと FWSM デバイス、および 8.3 よりも前のバージョンの ASA でネットワーク アドレス変換を設定する方法について説明します（ASA 8.3+ デバイスでの NAT の設定については、ASA 8.3+ デバイスでの NAT の設定 （1352 ページ）を参照してください）。

- アドレス プール （1331 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
  - [Translation Exemptions (NAT 0 ACL)] （1334 ページ）
  - [Dynamic Rules] タブ （1337 ページ）
  - [Policy Dynamic Rules] タブ （1340 ページ）
  - [Static Rules] タブ （1342 ページ）
  - [General] タブ （1349 ページ）

アドレス プール

[Address Pools] ページを使用して、ダイナミック NAT ルールで使用されるグローバル アドレス プールを表示および管理します。

これらのアドレス プールを追加および編集するには、[Address Pool] ダイアログボックスを使用します。このページの [Global Address Pools] テーブルに表示されるフィールドについては、[Address Pool] ダイアログボックス （1332 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[NAT] > [アドレスプール（Address Pools）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[NAT（PIX/ASA/FWSM）] > [アドレスプール（Address Pools）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [アドレスプール（Address Pools）] を右クリックして新しいポリシーを作成します。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）

[Address Pool] ダイアログボックス

[Address Pool] ダイアログボックスを使用して、ダイナミック NAT ルールで使用するグローバル アドレス プールを追加または編集します。

ナビゲーション パス

[Address Pool] ダイアログボックスを開くには、アドレス プール （1331 ページ）で [Add Row] または [Edit Row] ボタンをクリックします。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）

フィールド リファレンス

表 309 : [Address Pools] ダイアログボックス

要素	説明
Interface Name	マッピングされた IP アドレスが使用されるデバイス インターフェイスの名前を入力するか、または選択します。
Pool ID	このアドレス プールの一意の識別番号を 1 ～ 2147483647 の整数で入力します。ダイナミック NAT ルールを設定する場合は、[Pool ID] を選択して、変換に使用されるアドレス プールを指定します。

要素	説明
IP アドレス範囲	このアドレス プールに割り当てられるアドレスを入力するか、または選択します。これらのアドレスは次のように指定できます。 • ダイナミック NAT のアドレス範囲（192.168.1.1-192.168.1.15 など） • サブネットワーク（192.168.1.0/24 など） • カンマ区切りのアドレスのリスト（192.168.1.1, 192.168.1.2, 192.168.1.3 など） • PAT に使用する単一のアドレス（192.168.1.1 など） • 上記の組み合わせ（192.168.1.1-192.168.1.15, 192.168.1.25 など） • 接続されるネットワーク上のホストの名前。これらは IP アドレスに解決されます。
説明	アドレス プールの説明を入力します。
Enable Interface PAT	オンにすると、指定したインターフェイスでポートアドレス変換がイネーブルになります。

[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしていますが、拡張機能はサポートしていません。

[Translation Rules] ページを使用して、選択したデバイスのネットワーク アドレス変換（NAT）規則を定義します。[Translation Rules] ページは、次のタブで構成されています。

- [Translation Exemptions (NAT 0 ACL)] （1334 ページ）：このタブを使用して、アドレス変換が免除されるトラフィックを指定するルールを設定します。

（注） 変換免除は、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

- [Dynamic Rules] タブ （1337 ページ）：このタブを使用して、ダイナミック NAT ルールとダイナミック PAT ルールを設定します。

（注） ダイナミック変換ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

- [Policy Dynamic Rules] タブ （1340 ページ）：このタブを使用して、送信元アドレスと宛先アドレスおよびサービスに基づいたダイナミック変換ルールを設定します。

（注） ポリシーのダイナミック ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

- [Static Rules] タブ （1342 ページ）：このタブを使用して、セキュリティ アプライアンスまたは共有ポリシーのスタティック変換ルールを設定します。
- [General] タブ （1349 ページ）：このタブを使用して、デバイス上で検証される順序で、現在あるすべての変換ルールを一覧表示します。

（注） [General] タブは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけで表示されます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされ、概要情報を表示する必要はありません。

ナビゲーション パス

[Translation Rules] ページにアクセスするには、次のいずれかを実行します。

- （デバイス ビュー）デバイス ポリシー セレクタから [NAT] > [変換ルール（Translation Rules）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [NAT (PIX/ASA/FWSM)] > [変換ルール（Translation Rules）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または [変換ルール（Translation Rules）] を右クリックして新しいポリシーを作成します。

[Translation Exemptions (NAT 0 ACL)]

[Translation Rules] ページの [Translation Exemptions (NAT 0 ACL)] タブを使用して、トラフィックにアドレス変換を免除するルールを表示および指定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックス （1335 ページ）を参照してください。

（注） 変換免除は、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

ナビゲーション パス

[Translation Exemptions (NAT 0 ACL)] タブには、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）ページからアクセスできます。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）
- [General] タブ （1349 ページ）
- Security Manager の標準のルール テーブルに関する項：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックス

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックスを使用して、ルータ モードの PIX、FWSM、および 8.3 よりも前の ASA デバイスと、トランスペアレント モードの FWSM 3.2 デバイスでの変換免除ルールを定義および編集します。

ナビゲーション パス

[Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックスには、[Translation Exemptions (NAT 0 ACL)] タブからアクセスできます。詳細については、[Translation Exemptions (NAT 0 ACL)] （1334 ページ）を参照してください。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）

フィールド リファレンス

表 *310 : [Add/Edit Translation Exemption (NAT-0 ACL) Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
操作	このルールのアクションを選択します。 • [exempt]：NAT が免除されるトラフィックをルールで指定します。 • [do not exempt]：NAT が免除されないトラフィックをルールで指定します。
Original: Interface	ルールを適用するデバイスインターフェイスの名前を入力するか、または選択します。
Original: Sources	ルールを適用する発信元ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。 このパラメータは、[変換免除（NAT 0 ACL）（Translation Exemptions (NAT 0 ACL)）] テーブルの列見出し [元のアドレス（Original Address）] の下に表示されることに注意してください。
Translated: Direction	このオプションによる指定に従って、ルールをインバウンド トラフィックまたはアウトバウンド トラフィックに適用できます。
Traffic flow: Destinations	ルールを適用する宛先ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリは、ラベルやカラーコーディングを使用したルールとオブジェクトの識別に役立ちます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。 （注） カテゴリ属性のコマンドは生成されません。
説明	ルールの説明を入力します。
[詳細設定（Advanced）] ボタン（FWSM のみ）	クリックすると、[Advanced NAT Options] ダイアログボックス （1346 ページ）が開き、このルールの高度な設定を行うことができます。

[Dynamic Rules] タブ

[Translation Rules] ページの [Dynamic Rules] タブを使用して、ダイナミック NAT ルールとダイナミック PAT ルールを表示および設定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

ダイナミック NAT では、内部 IP アドレスは、グローバル アドレス プールの IP アドレスを使用して動的に変換されます。ダイナミック PAT では、内部 IP アドレスは、動的に割り当てられるポート番号とマッピングされたアドレスを併用して、単一のマッピングされたアドレスに変換されます。ダイナミック変換は、多くの場合、ローカルの RFC 1918 IP アドレスをインターネットでルーティング可能なアドレスにマッピングするために使用されます。

[Add/Edit Dynamic Translation Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Dynamic Translation Rule] ダイアログボックス （1338 ページ）を参照してください。

（注） ダイナミック変換ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

ナビゲーション パス

[Dynamic Rules] タブには、[Translation Rules] ページからアクセスできます。[Translation Rules] ページの詳細については、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）を参照してください。

（注） デフォルトでは、[Dynamic Rule] の標準要素だけがこのテーブルに表示されます。カラムの見出しを右クリックすると、[Advanced NAT Options] ダイアログボックスで定義されている要素の他のカラムを表示できます（[General] タブ （1349 ページ）には、デフォルトですべてのカラムが表示されます）。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）
- [Select Address Pool] ダイアログボックス （1339 ページ）
- [General] タブ （1349 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）

- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add/Edit Dynamic Translation Rule] ダイアログボックス

[Add/Edit Dynamic Translation Rule] ダイアログボックスを使用して、ダイナミック NAT ルールとダイナミック PAT ルールを定義および編集します。

ナビゲーション パス

[Add/Edit Dynamic Translation Rule] ダイアログボックスには、[Dynamic Rules] タブからアクセスできます。詳細については、 [Dynamic Rules] タブ （1337 ページ）を参照してください。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）
- [Select Address Pool] ダイアログボックス （1339 ページ）

フィールド リファレンス

表 311 : [Add/Edit Dynamic Translation Rule] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
Original: Interface	ルールを適用するデバイスインターフェイスの名前を入力するか、または選択します。
Original: Address	ルールを適用する発信元ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
Translated: Pool	変換に使用するアドレスのプールの ID 番号を入力するか、または選択します。[Select] をクリックすると [Select Address Pool] ダイアログボックス （1339 ページ）が開きます。 これをアイデンティティ NAT ルールとして指定するには、値 0 を入力します。
Translated: Direction	このオプションによる指定に従って、ルールをインバウンド トラフィックまたはアウトバウンド トラフィックに適用できます。

要素	説明
[Advanced] ボタン	クリックすると、[Advanced NAT Options] ダイアログボックス （1346 ページ）が開き、このルールの高度な設定を行うことができます。

[Select Address Pool] ダイアログボックス

[Select Address Pool] ダイアログボックスには、グローバル アドレス プールのリストが表示されます。これらのプールは、アドレス プール （1331 ページ）を使用して定義および管理されます。このダイアログボックスを使用して、ダイナミック変換ルールまたはポリシー ダイナミック変換ルールで使用するアドレス プールを選択します。

ナビゲーション パス

ダイナミック変換ルールを追加または編集する場合は [Add/Edit Dynamic Translation Rule] ダイアログボックス （1338ページ）から、ポリシー ダイナミック変換ルールを追加または編集する場合は [Add/Edit Policy Dynamic Rules] ダイアログボックス （1341 ページ）から [Select Address Pool] ダイアログボックスにアクセスできます。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
- アドレス プール （1331 ページ）

フィールド リファレンス

表 *312 : [Select Address Pool]* ダイアログボックス

要素	説明
Pool ID	アドレス プールの識別番号。
インターフェイス	アドレス プールが適用されるデバイス インターフェイスの名前。
IP アドレス範囲（IP Address Ranges）	プールに割り当てられる IP アドレス。このリストの「インターフェイス」は、指定したインターフェイスで PAT が有効になっていることを示します。
説明	アドレス プールの説明。
Selected Row	このフィールドは、リスト内で現在選択されているプールを示します。[OK] をクリックするとダイアログボックスが閉じ、このプールが変換ルールに割り当てられます。

[Policy Dynamic Rules] タブ

[Translation Rules] ページの [Policy Dynamic Rules] タブを使用して、送信元アドレスと宛先アドレスおよびサービスに基づいたダイナミック変換ルールを表示および設定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

[Add Policy Dynamic Rule]/[Edit Policy Dynamic Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Policy Dynamic Rules] ダイアログボックス （1341 ページ）を参照してください。

（注） ポリシーのダイナミック ルールは、ルータ モードの PIX、ASA、および FWSM とトランスペアレント モードの FWSM 3.2 デバイスだけでサポートされます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされます。

ナビゲーション パス

[Policy Dynamic Rules] タブには、[Translation Rules] ページからアクセスできます。詳細については、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）を参照してください。

（注） デフォルトでは、[Policy Dynamic Rule] の標準要素だけがこのテーブルに表示されます。カラムの見出しを右クリックすると、[Advanced NAT Options] ダイアログボックスで定義されている要素の他のカラムを表示できます（[General] タブ （1349 ページ）には、デフォルトですべてのカラムが表示されます）。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- < [Add/Edit Policy Dynamic Rules] ダイアログボックス （1341 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）
- [Select Address Pool] ダイアログボックス （1339 ページ）
- [General] タブ （1349 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add/Edit Policy Dynamic Rules] ダイアログボックス

[Add/Edit Policy Dynamic Rules] ダイアログボックスを使用して、送信元アドレスと宛先アドレスおよびサービスに基づいたダイナミック変換ルールを定義および編集します。

ナビゲーション パス

[Add/Edit Policy Dynamic Rules] ダイアログボックスには、[Policy Dynamic Rules] タブからアクセスできます。詳細については、[Policy Dynamic Rules] タブ （1340 ページ）を参照してください。

関連項目

- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Policy Dynamic Rules] タブ （1340 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）
- [Select Address Pool] ダイアログボックス （1339 ページ）

フィールド リファレンス

表 313 : [Add/Edit Policy Dynamic Rules] ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
Original: Interface	ルールを適用するデバイスインターフェイスの名前を入力するか、または選択します。
Original: Sources	ルールを適用する発信元ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。 このパラメータは、[ポリシーダイナミックルール（Policy Dynamic Rules）] テーブルのカラム見出し [元のアドレス（Original Address）] の下に表示されることに注意してください。
Translated: Pool	変換に使用するアドレスのプールの ID 番号を入力するか、または選択します。[Select] をクリックすると [Select Address Pool] ダイアログボックス （1339 ページ）が開きます。 これをアイデンティティ NAT ルールとして指定するには、値 0 を入力します。

要素	説明
Translated: Direction	このオプションによる指定に従って、ルールをインバウンドトラフィックまたはアウトバウンド トラフィックに適用できます。
Traffic flow: Destinations	ルールを適用する宛先ホストおよびネットワーク オブジェクトの IP アドレスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
Traffic flow: Services	ルールを適用するサービスを入力するか、または選択します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリは、ラベルやカラーコーディングを使用したルールとオブジェクトの識別に役立ちます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。 （注） カテゴリ属性のコマンドは生成されません。
説明	ルールの説明を入力します。
[Advanced] ボタン	クリックすると、[Advanced NAT Options] ダイアログボックス （1346 ページ）が開き、このルールの高度な設定を行うことができます。

[Static Rules] タブ

[Translation Rules] ページの [Static Rules] タブを使用して、セキュリティ アプライアンスまたは共有ポリシーのスタティック変換ルールを表示および設定します。ルールは、リスト内の順序に従って評価されます。行番号は、リスト内の順序におけるルールの位置を示します。[Up Row] ボタンおよび [Down Row] ボタンを使用して、選択したルールの位置を変更できます。

スタティック変換では、内部 IP アドレスは常にグローバル IP アドレスにマッピングされます。これらのルールは、セキュリティレベルの低いインターフェイス上のホストアドレスをセキュリティレベルの高いインターフェイス上のグローバルアドレスにマッピングします。たとえば、スタティックルールは、境界ネットワーク上の Web サーバーのローカルアドレスを、外部インターフェイス上のホストが Web サーバーへのアクセスに使用するグローバルアドレスにマッピングするために使用されます。

注意 セキュリティデバイス上のスタティック NAT ルールの順序は重要であり、Security Manager は展開時にこの順序を保持します。ただし、セキュリティ アプライアンスでは、スタティック NAT ルールのインライン編集はサポートしていません。つまり、リストの末尾よりも上の任意の場所でルールを移動、編集、または挿入すると、Security Manager は、新規または変更したルールの後に続くすべてのスタティック NAT ルールをデバイスから削除し、その時点から更新されたリストを再送信します。リストの長さによっては、この処理にかなりのオーバーヘッドがかかる可能性があり、結果としてトラフィックが中断されることがあります。可能なかぎり、新しいスタティック NAT ルールはリストの末尾に追加してください。

[Add/Edit Static Rule] ダイアログボックスを使用して、これらのルールを追加および編集します。このページのテーブルに表示されるフィールドについては、[Add/Edit Static Rule] ダイアログボックス （1344 ページ）を参照してください。

[スタティックルール（Static Rules）] テーブルの「Nailed」カラム

[Add/Edit Static Rule] ダイアログボックス （1344 ページ）で指定されたパラメータを表す列に加えて、[スタティックルール（Static Rules）] テーブルには、「Nailed」というラベルの付いた列が表示されます。この値はデバイス検出の製品です。Security Manager では変更できません。

「Nailed」カラムのエントリは、その接続に対して TCP ステートトラッキングおよびシーケンスチェックがスキップされるかどうかを「true」または「false」で示します。

ナビゲーション パス

[Static Rules] タブには、[Translation Rules] ページからアクセスできます。詳細については、[Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）を参照してください。

（注） デフォルトでは、[Static Rules] の標準要素だけがこのテーブルに表示されます。カラムの見出しを右クリックすると、[Advanced NAT Options] ダイアログボックスで定義されている要素の他のカラムを表示できます（[General] タブ （1349 ページ）には、デフォルトですべてのカラムが表示されます）。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Add/Edit Static Rule] ダイアログボックス （1344 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）
- [General] タブ （1349 ページ）
- 標準のルール テーブルに関する内容：

- ルール テーブルの使用 （764 ページ）
- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add/Edit Static Rule] ダイアログボックス

[Add/Edit Static Rule] ダイアログボックスを使用して、ファイアウォール デバイスまたは共有ポリシーのスタティック変換ルールを追加または編集します。

ナビゲーション パス

[Add/Edit Static Rule] ダイアログボックスには、[Static Rules] タブ （1342 ページ）からアクセスできます。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）
- [Advanced NAT Options] ダイアログボックス （1346 ページ）

フィールド リファレンス

表 *314 : [Add/Edit Static Rule]* ダイアログボックス

要素	説明
ルールの有効化（Enable Rule）	オンにすると、ルールがイネーブルになります。ルールを削除せずにディセーブルにするには、このオプションの選択を解除します。
Translation Type	このルールの変換のタイプ（[NAT] または [PAT]）を選択します。
Original Interface	変換される元のアドレスを持つホストまたはネットワークに接続されているデバイス インターフェイスを入力するか、または選択します。
元のアドレス	変換される送信元アドレスを入力するか、または選択します。
Translated Interface	変換後のアドレスが使用されるインターフェイスを入力するか、または選択します。 このルールをアイデンティティ NAT ルールとして指定するには、このフィールドと [Original Interface] フィールドの両方に同じインターフェイスを入力します。

要素	説明
Use Interface IP/Use Selected Address	変換後のインターフェイスで使用するアドレスを指定します。[Use Interface IP]（アドレス）を選択するか、または [Use Selected Address] を選択してアドレスを入力するかネットワーク/ホスト オブジェクトを選択します。
Enable Policy NAT	この変換ルールに対してポリシー NAT をイネーブルにするには、このオプションを選択します。
宛先アドレス（Dest Address）	ポリシー NAT をイネーブルにした場合は、ルールが適用されるホストまたはネットワークの宛先アドレスを指定します。
サービス	ポリシー NAT をイネーブルにした場合は、ルールが適用されるサービスを入力するか、または選択します。 （注） スタティック ポリシー NAT の場合、指定できるサービスは IP だけです。 サービスおよびサービス オブジェクトを指定する構文は、次のとおりです。 {**tcp** | **udp** | **tcp&udp**}/{*source_port_number* | *port_list_object* }/{*destination_port_number* | *port_list_object* } 1 つのポートパラメータしか入力しなかった場合、このパラメータは宛先ポートとして解釈されることに注意してください（送信元ポートは「any」になります）。たとえば、**tcp/4443** は tcp、送信元ポート any、宛先ポート 4443 を意味し、**tcp/4443/Default Range** は tcp、送信元ポート 4443、宛先ポート Default Range（通常、1 ～ 65535）を意味します。 すべてのテキスト入力フィールドと同様に、Security Manager によってオートコンプリート オプションが表示されることがあります。たとえば、このフィールドに **tcp/** と入力すると、Security Manager に定義されているすべてのポートリストオブジェクトのオートコンプリートリストが表示されます。このリストには、DEFAULT RANGE、HTTPS、および WEBPORTS などのシステム生成オブジェクトが含まれています。 ポートリストの詳細についてはポート リスト オブジェクトの設定 （420 ページ）を、サービス定義の詳細についてはサービス オブジェクトの設定 （422 ページ）を参照してください。
プロトコル	[Translation Type] で [PAT] を選択した場合は、ルールが適用されるプロトコル（TCP または UDP）を選択します。
元のポート	[Translation Type] で [PAT] を選択した場合は、変換されるポート番号を入力します。 このパラメータは、[スタティックルール（Static Rules）] テーブルのカラム見出し [ローカルポート（Local Port）] の下に表示されることに注意してください。

要素	説明
[変換されたポート（Translated Port）]	[Translation Type] で [PAT] を選択した場合は、元のポート番号が変換されるポート番号を入力します。 このパラメータは、[スタティックルール（Static Rules）] テーブルのカラム見出し [グローバルポート（Global Port）] の下に表示されることに注意してください。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリは、ラベルやカラーコーディングを使用したルールとオブジェクトの識別に役立ちます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。 （注） カテゴリ属性のコマンドは生成されません。
説明	ルールの説明を入力します。
[Advanced] ボタン	クリックすると、[Advanced NAT Options] ダイアログボックス （1346 ページ）が開き、このルールの高度な設定を行うことができます。

[Edit Translated Address] ダイアログボックス

スタティック変換ルールに割り当てられている変換後のアドレスだけを変更するには、[Edit Translated Address] ダイアログボックスを使用します。変換後のアドレスとは、元のアドレスが変更されるアドレスです。インターフェイスの IP アドレスを使用するか、特定の IP アドレスを入力できます。スタティック ルールおよび変換後のアドレスの詳細については、[Static Rules] タブ （1342 ページ）を参照してください。

ファイアウォール ルールのセルの編集に関する詳細については、ルールの編集 （767 ページ）を参照してください。

ナビゲーション パス

（[NAT]>[変換ルール（Translation Rules）]ページにある）[スタティックルール（Static Rules）] テーブルの [変換済みアドレス（Translated Address）]セルを右クリックして、[変換済みアドレスの編集（Edit Translated Address）] を選択します。

[Advanced NAT Options] ダイアログボックス

[Advanced NAT Options] ダイアログボックスを使用して、NAT およびポリシー NAT の高度な接続設定（DNS 書き換え、最大 TCP および最大 UDP 接続数、初期接続制限、タイムアウト（PIX 6.x）、およびシーケンス番号のランダム化）を指定します。これらのオプションは、FWSM の変換免除（NAT 0 ACL）ルールでも設定できます。

ナビゲーション パス

変換ルールの追加または編集時に [詳細設定（Advanced）] ボタンをクリックすると、[NAT詳細オプション（Advanced NAT Options）] ダイアログボックスにアクセスできます。詳細については、次のトピックを参照してください。

- [Add/Edit Translation Exemption (NAT-0 ACL) Rule] ダイアログボックス （1335 ページ）
- [Add/Edit Dynamic Translation Rule] ダイアログボックス （1338 ページ）
- [Add/Edit Policy Dynamic Rules] ダイアログボックス （1341 ページ）
- [Add/Edit Static Rule] ダイアログボックス （1344 ページ）

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Translation Rules]：PIX、FWSM、および 8.3 よりも前の ASA （1333 ページ）

フィールド リファレンス

表 *315 : [Advanced NAT Options]* ダイアログボックス

要素	説明
Translate the DNS replies that match the translation rule	オンにすると、外部クライアントが内部 DNS サーバを使用して内部ホストの名前を解決できるように、またその逆ができるように、セキュリティ アプライアンスは DNS 応答を書き換えます。たとえば、NAT ルールに、DNS サーバ内にエントリを持つホストの実際のアドレスが含まれていて、DNS サーバがクライアントとは別のインターフェイス上にある場合、クライアントおよび DNS サーバにはそれぞれ異なるホスト用アドレスが必要です。つまり、片方にはマッピングされたアドレス、もう片方には実際のアドレスが必要です。このオプションは、クライアントに送信される DNS 応答内のアドレスを書き換えます。 例として、内部 Web サーバ www.example.com に IP アドレス 192.168.1.1 があり、このアドレスがアプライアンスの外部インターフェイス上の 10.1.1.1 に変換されるとします。外部クライアントは内部 DNS サーバに DNS 要求を送信し、これにより www.example.com は 192.168.1.1 に解決されます。DNS 書き換えをイネーブルにしたセキュリティ アプライアンスに応答が到着すると、外部クライアントが正しい IP アドレスを取得できるように、セキュリティ アプライアンスはペイロード内の IP アドレスを 10.1.1.1 に変換します。 マッピングされたホストがクライアントまたは DNS サーバと同じインターフェイス上に存在している必要があることに注意してください。通常、他のインターフェイスからのアクセスを許可する必要があるホストはスタティック変換を使用するため、このオプションはスタティック ルールで使用される可能性があります。

要素	説明
ルールあたりの最大TCP接続数（Max TCP Connections per Rule）	許容される TCP 接続の最大数を入力します。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
Max UDP Connections per Rule	許容される UDP 接続の最大数を入力します。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。
Max Embryonic Connections	初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限は、初期接続のフラッドによる攻撃を防ぐために設定します。有効な値は 0 ～ 65,535 です。この値を 0 に設定すると、接続数は無制限になります。 任意の正の値を入力すると、TCP 代行受信機能がイネーブルになります。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中に SYN クッキーが使用され、ドロップされる有効なトラフィックの数が最小限に抑えられます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。
タイムアウト（Timeout）	PIX 6.x デバイスの場合は、この変換ルールのタイムアウト値を hh:mm:ss の書式で入力します。この値は、00:00:00 を指定しないかぎり、[Platform] > [Security] > [Timeouts] で指定したデフォルトの変換タイムアウトを上書きします。00:00:00 を指定した場合、このルールに一致する変換では、（[Platform] > [Security] > [Timeouts] で指定した）デフォルトの変換タイムアウトが使用されます。

要素	説明
Randomize Sequence Number	オンにすると、セキュリティ アプライアンスによって TCP パケットのシーケンス番号がランダム化されます。個々の TCP 接続には 2 つの Initial Sequence Number（ISN; 初期シーケンス番号）があり、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、インバウンド方向とアウトバウンド方向の両方で、TCP SYN の ISN をランダム化します。保護対象のホストの ISN をランダム化することにより、攻撃者が新しい接続に使用される次の ISN を予測して新しいセッションをハイジャックするのを阻止します。 この機能は、次の場合にかぎりディセーブルにします。 • 別のインライン セキュリティ アプライアンスでも初期シーケンス番号をランダム化しており、データがスクランブル化されている場合。 • セキュリティアプライアンスを介して eBGP マルチホップを使用しており、eBGP ピアが MD5 を使用している場合。ランダム化により、MD5 チェックサムは分解されます。 • セキュリティ アプライアンスによって接続のシーケンス番号がランダム化されないことを必要とする WAAS デバイスを使用している場合。 このオプションをディセーブルにすると、セキュリティ アプライアンスにセキュリティ ホールが開きます。

[General] タブ

[Translation Rules] ページの [General] タブを使用して、現在のデバイスまたは共有ポリシーに定義されているすべての変換ルールの概要を表示します。変換ルールは、デバイス上で検証される順序で一覧表示されます。

（注） [General] タブは、ルータ モードの PIX、ASA、および FWSM デバイスとトランスペアレント モードの FWSM 3.2 デバイスだけで表示されます。トランスペアレント モードのその他のデバイスでは、スタティック変換ルールだけがサポートされ、概要情報を表示する必要はありません。

ナビゲーション パス

[General] タブには、[Translation Rules] ページからアクセスできます。詳細については、を参照してください。

関連項目

- PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）
- [Translation Exemptions (NAT 0 ACL)] （1334 ページ）

- [Dynamic Rules] タブ （1337 ページ）
- [Policy Dynamic Rules] タブ （1340 ページ）
- [Static Rules] タブ （1342 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

フィールド リファレンス

表 *316 : [*全般（*General*）*]* タブ：変換ルール概要テーブル

要素	説明
（注） テーブル内のエントリに斜線の網掛けが適用されている場合は、ルールが現在ディセーブルになっていることを示します（これらのルールのイネーブル化およびディセーブル化の詳細については、 [Add/Edit Dynamic Translation Rule] ダイアログボックス （1338 ページ）の [Enable Rule] を参照してください）。	
番号	ルールは、リスト内の順序に従って評価されます。この番号は、リストの順序におけるルールの位置を示します。
タイプ（Type）	トランスレーション ルールのタイプ。[Static]、[Dynamic]、[Exemption] など。
操作	ルールが NAT から免除される場合は、「exempt」と表示されます。
Original Interface	ルールが適用されるデバイス インターフェイスの ID。
元のアドレス	ルールが適用される送信元ホストおよびネットワークのオブジェクト名または IP アドレス。
ローカル ポート（Local Port）	ホストまたはネットワークによって提供されるポート番号（スタティック PAT 用）。
Translated Pool	変換に使用されるアドレス プールの ID 番号。
Translated Interface	変換後のアドレスが使用されるインターフェイス。
Translated Address	変換後のアドレス。
Global Port	元のポート番号が変換されるポート番号（スタティック PAT 用）。

要素	説明
[接続先（Destination）]	ルールが適用される宛先ホストまたはネットワークのオブジェクト名および IP アドレス。
プロトコル	ルールが適用されるプロトコル。
サービス	ルールが適用されるサービス。
方向	ルールが適用されるトラフィックの方向（[Inbound] または [Outbound]）。
DNS Rewrite	DNS 書き換えオプションがイネーブルかどうか（このオプションは [Advanced NAT Options] ダイアログボックス （1346 ページ）で設定される）。
Maximum TCP Connections	静的に変換された IP アドレスに接続できる TCP 接続の最大数。0 の場合、接続数は無制限です。このオプションは、[Advanced NAT Options] ダイアログボックス （1346 ページ）で設定します。
Embryonic Limit	セキュリティアプライアンスが初期接続を拒否し始めるまでに確立が許可される初期接続の数。0 の場合、接続数は無制限です。正の数を入力すると、TCP 代行受信機能がイネーブルになります。 このオプションは、[Advanced NAT Options] ダイアログボックス （1346 ページ）で設定します。
Maximum UDP Connections	静的に変換された IP アドレスに接続できる UDP 接続の最大数。0 の場合、接続数は無制限です。このオプションは、[Advanced NAT Options] ダイアログボックス （1346 ページ）で設定します。
タイムアウト（Timeout）	PIX 6.x デバイスの場合、これはスタティック変換ルールのタイムアウト値です。この値は、[Platform] > [Security] > [Timeouts] で指定したデフォルトの変換タイムアウトを上書きします。ここで 00:00:00 のタイムアウト値を指定すると、このルールと一致する変換では、[Platform] > [Security] > [Timeouts] で指定したデフォルトの変換タイムアウトが使用されます。
Randomize Sequence Number	セキュリティアプライアンスが TCP パケットのシーケンス番号をランダム化するかどうか：「Yes」または「No」。このオプションは [Advanced NAT Options] ダイアログボックス （1346 ページ）で設定され、デフォルトはイネーブル）。
カテゴリ	ルールが割り当てられるカテゴリ。カテゴリはラベルやカラーコーディングを使用して、ルールおよびオブジェクトを識別しやすくします。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。 （注） カテゴリ属性のコマンドは生成されません。

要素	説明
説明	ルールの説明（指定してある場合）。
最後のチケット	ルールの最終変更に関連付けられたチケットを表示します。[最後のチケット（Last Ticket(s)）] 列のチケット ID をクリックして、チケットの詳細を表示し、そのチケットに移動できます。外部チケット管理システムへのリンクが設定されている場合は、チケットの詳細からそのシステムに移動することもできます（[チケット管理（Ticket Management）] ページ （740 ページ）を参照）。

ASA 8.3+ デバイスでの NAT の設定

ここでは、バージョン 8.3 以降の ASA デバイスでネットワーク アドレス変換を設定する方法について説明します。

- [Translation Rules]：ASA 8.3+ （1352 ページ）
  - [Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （1355 ページ）
  - [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）
- Per-Session NAT ルール: ASA 9.0（1）+ （1371 ページ）

他のセキュリティ アプライアンスでの NAT の設定については、 PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）を参照してください。NAT ルールの一般的な情報、および ASA 8.3 で実装された NAT 設定の変更点については、 ASA 8.3 以降のデバイスでの「簡易」NAT について （1311 ページ）を参照してください。

（注） ロールにマップされた変更権限を持っている場合にのみ、NAT オブジェクトを作成できます。Cisco Security Manager は認証のエラーメッセージを表示します。

[Translation Rules]：ASA 8.3+

[Translation Rules] ページを使用して、選択した ASA 8.3+ デバイスのネットワーク アドレス変換（NAT）規則を管理します。他のセキュリティデバイスでの変換ルールの設定については、セキュリティ デバイスの NAT ポリシー （1326 ページ）を参照してください。

このテーブルには 2 つのタイプの NAT ルールが表示されます。該当ユーザや別のユーザが追加した「手動」ルールと、NAT プロパティを持つオブジェクトがデバイスに割り当てられている場合に Security Manager によって生成および適用される「自動」ルールです。これらはそれぞれ「NAT ルール」および「ネットワークオブジェクト NAT ルール」と呼ばれます。

[Translation Rules] テーブルの一部の機能

この [Translation Rules] テーブルは、ルール テーブルの使用 （764 ページ）で示すような標準的な Security Manager のルール テーブルです。たとえば、カラムを移動、表示、または非表示にしたり、手動ルールを再順序付けしたり、特定のテーブル セルを右クリックしてそのパラメータを編集したりできます。また、次の機能はこの [Translation Rules] テーブルに固有です。

- すべてのルールが、テーブル内にある事前定義済みの 3 つのセクションのいずれかに割り当てられます。
  - [NAT Rules Before]：これらは、該当ユーザまたは別のユーザがそのデバイスに「手動で」定義したルールです。ルールを追加する前にセクション見出しをクリックすることで、このセクションにルールが追加されることを指定できますが、セクションを指定しなかった場合にも、新しいルールはデフォルトでこのセクションに追加されます。
  - [Network Object NAT Rules]：これらは、NAT プロパティを含むネットワークオブジェクトがデバイスに割り当てられている場合に、Security Manager によって自動的に生成され、順序付けされるルールです。NAT プロパティをオブジェクトに割り当てる方法については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）を参照してください。これらのルールを順序付けする方法については、ASA 8.3 以降のデバイスでの「簡易」NAT について （1311 ページ）のセクション「NAT テーブル」を参照してください。

（注） これらのルールはデバイス固有であるため、このセクションはポリシー ビューの [Translation Rules] テーブルには表示されません。

  - [NAT Rules After]：これらもまた、該当ユーザまたは別のユーザがそのデバイスに手動で定義したルールです。ルールを追加する前にセクション見出しをクリックすることで、このセクションにルールが追加されることを指定できます。

このテーブルに一覧表示されている NAT ルールは最初に一致したものから順に処理されます。そのため、順序は重要です。ルールはそのセクション内でしか再順序付けできないため、自動ルールの前と後の両方で手動セクションを指定することによって、すべてのルールが適切な順序になるように設定できます。各セクションのルールは、そのあとのセクションのルールに優先します。たとえば、一番上の「前」セクションのルールは、ネットワークオブジェクト NAT セクションのルールに優先するというように続きます。

- 各ルールのタイプ（スタティック、ダイナミック PAT、またはダイナミック NAT と PAT）は、[変換済み（Translated）] カラムの [送信元（Source）] パラメータの次に青色で **(S)**、**(DP)**、または**(DNP)** を表示することによって、テーブル内で視覚的に示されます。
- 双方向ルールは、実際にはペアになった 2 つのルール（指定した送信元の値と宛先の値の間で実行される発信変換と着信変換のそれぞれに 1 つずつ）で構成されるスタティック ルールです。ルール テーブルには、各双方向ルール エントリが 2 行で表示されます。

たとえば、[Source] フィールドが [Host1] で [Translated] フィールドが [Host2] のスタティック ルールを作成するときに [Bi-directional] を選択した場合、ルール テーブルに 2 つの行が追加されます。1 つは Host1 を Host2 に変換する行、もう 1 つは Host2 を Host1 に変換する行です。

関連項目

- セキュリティ デバイスの NAT ポリシー （1326 ページ）
- ASA 8.3 以降のデバイスでの「簡易」NAT について （1311 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから [NAT] > [変換ルール（Translation Rules）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [NAT (PIX/ASA/FWSM)] > [変換ルール（Translation Rules）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または [変換ルール（Translation Rules）] を右クリックして新しいポリシーを作成します。

[Translation Rules] ページが表示されます。ネットワーク オブジェクト NAT ルールはデバイス固有であるため、ポリシー ビューでは [Network Object NAT Rules] セクションが表示されないことに注意してください。

ルールの追加、編集、および削除

NAT ルールを**追加**するには、次の手順を実行します。

1. ルールを追加するセクションの見出しを選択します。見出しを選択しなかった場合、ルールはデフォルトで [NAT Rules Before] に追加されます。
2. [Add NAT Rule] ダイアログボックスを開きます。テーブルの下部にある [Add Row] ボタンをクリックするか、またはテーブル内の任意の場所（既存のルール エントリの上以外）を右クリックしてポップアップ メニューから [Add Row] を選択します。
3. ルールを定義してから [OK] をクリックしてダイアログボックスを閉じると、ルールがテーブルに追加されます。

NAT ルールを**編集**するには、次の手順を実行します。

1. 目的のルールの [Edit NAT Rule] ダイアログボックスを開きます。NAT ルール テーブルでルールを選択してテーブルの下部にある [Edit Row] ボタンをクリックするか、または単に

目的のルール エントリを右クリックしてポップアップ メニューから [Edit Row] を選択します。

2. ルールを編集してから [OK] をクリックしてダイアログボックスを閉じます。

[Add NAT Rule] ダイアログボックスの詳細な説明については、[Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （1355 ページ）を参照してください。

NAT ルールを**削除**するには、テーブルでルールを選択してテーブルの下部にある [行の削除（Delete Row）] ボタンをクリックするか、または単に目的のルールエントリを右クリックしてポップアップメニューから [行の削除（Delete Row）] を選択します。

（注） このテーブルからネットワーク オブジェクト NAT ルールを削除するには、関連する [Edit Network Host] ダイアログボックスで [Add Automatic Address Translation NAT Rule] オプションをオフにするか、またはルールの割り当て先のデバイスを変更します。詳細については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）を参照してください。

ルールの有効化と無効化

次のように、1 つ以上の連続するルールをテーブルから削除せずにディセーブルにできます。

1. ディセーブルにするルールを選択します。連続したルールのブロックを選択する場合は、ブロックの最初のルールをクリックしてから、ブロックの最後のルールを Shift を押した状態でクリックします。
2. 選択したルールを右クリックして、ポップアップメニューから [無効化（Disable）] を選択します。

無効になっているルールは、テーブルでグレー表示されます。

無効になっている 1 つ以上の連続するルールを再度有効にするには、このプロセスを繰り返して、ポップアップメニューから [有効化（Enable）] を選択します。

[Add NAT Rule]/[Edit NAT Rule] ダイアログボックス

[Add NAT Rule] ダイアログボックスを使用して、選択した ASA 8.3+ デバイスに NAT ルールを追加します。このダイアログボックスは、以前のバージョンの ASA でも、PIX または FWSM デバイスでも使用できません。これらのデバイスで NAT ルールを追加および編集する方法については、PIX、FWSM、および 8.3 よりも前の ASA デバイスでの NAT の設定 （1331 ページ）を参照してください。

（注） タイトルを除いて、[Add NAT Rule] ダイアログボックスと [Edit NAT Rule] ダイアログボックスは同一であり、次の説明は両方に適用されます。

ナビゲーション パス

ルールを追加するには、ルールを追加するセクション（[NATルールを前に（NAT Rules Before）] または [NATルールを後に（NAT Rules After）]）を選択してから、ルールテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の任意の場所を右クリックし、[行の追加（Add Row）] を選択して [NATルールの追加（Add NAT Rule）] ダイアログボックスを開きます。セクションを選択しなかった場合、新しいルールは [NAT Rules Before] セクションに追加されることに注意してください。

ルールを編集するには、ルールを選択して [Edit Row] ボタンをクリックするか、単にルールを右クリックし [Edit Row] コマンドを選択して、そのルールの [Edit NAT Rule] ダイアログボックスを開きます。

関連項目

- ネットワーク アドレス変換の設定 （1307 ページ）
- [Translation Rules]：ASA 8.3+ （1352 ページ）
- [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）

フィールド リファレンス

表 *317 : [Add NAT Rule]/[Edit NAT Rule]* ダイアログボックス

要素	説明
送信元インターフェイス（Source Interface）	パケットが発信されるインターフェイスの名前。これは「実際の」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。目的のインターフェイスを入力するか、または選択します。 （注） トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。
Destination Interface	[宛先インターフェイス（Destination Interface）]：パケットが到着するインターフェイスの名前。これは「マッピングされた」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。目的のインターフェイスを入力するか、または選択します。 （注） トランスペアレント ファイアウォール モードでは、特定のインターフェイスを設定する必要があります。

要素	説明
[送信元NATタイプ（Source NAT Type）]	作成する変換ルールのタイプ。 • [Static]：実際のアドレスからマッピングされたアドレスへのスタティックな割り当てを提供します。 • [ダイナミックPAT（非表示）（Dynamic Dynamic PAT (Hide)）]：複数のローカルアドレスから単一のグローバル IP アドレスおよび一意のポート番号へのダイナミックな割り当てを提供し、実質的に、ローカルアドレスを 1 つのグローバルアドレスの背後に「隠します」。 • [ダイナミックNATおよびPAT（Dynamic NAT and PAT）]：実際のアドレスからマッピングされたアドレス、および実際のポートからマッピングされたポートへのダイナミックな割り当てを提供します。 このオプションを選択すると、[PATプールアドレス変換（PAT Pool Address Translation）]オプションがダイアログボックスに追加されます。ルーテッドモードで稼働しているデバイスでは、このオプションによって次で説明するフォールスルーオプションも提供されます。 （注） このセクションは指定した送信元の変換にだけ適用されます。宛先の変換は常にスタティックになります。
[送信元の変換（Source Translation）]	
Original Source	NAT ルールで変換される送信元アドレス。アドレス範囲またはネットワークの場合は、範囲またはネットワーク内のすべてのアドレスが変換されます。

要素	説明
Translated Source アドレス（Address） インターフェイス	変換がデバイス上のアドレスまたはインターフェイスのどちらに基づくかを示します。次のいずれかを選択します。 • [アドレス（Address）] : [変換済み送信元（Translated Source）] フィールドで指定したネットワーク/ホストオブジェクトを使用して、元のアドレスを変換します。このエントリは変換アドレスのプールを示します。目的のネットワーク/ホストを入力するか、選択します。デフォルトは元の送信元アドレスです（アイデンティティ NAT ルールが作成されます）。 • [インターフェイス（Interface）] : [変換済み送信元（Translated Source）] フィールドで指定したインターフェイスに基づいて、元のアドレスを変換します。 このインターフェイスに基づくポート アドレス変換については、必ず（このダイアログボックスの [Advanced] パネルにある）[Service Translation] セクションでオプションを設定してください。 [宛先インターフェイス（Destination Interface）] フィールドを定義しなかった場合、[アドレス（Address）] と [インターフェイス（Interface）] の選択は [アドレス（Address）] に戻り、元の送信元アドレスが [アドレス（Address）] フィールドに挿入されます。これにより、アイデンティティ NAT ルールが作成されます。つまり、指定したアドレスはそれ自身に変換されます（事実上、変換されません）。アイデンティティ NAT はアウトバウンド接続だけに適用されます。 （注） これらのオプションは、選択されたタイプがダイナミック NAT および PAT である場合には使用できません。また、トランスペアレントモードで動作しているデバイスでは使用できません。

要素	説明
PAT Pool Address Translation	

要素	説明
	このオプションは、タイプとして [Dynamic NAT and PAT] を選択している場合に使用できます。関連パラメータを使用すると、PATマッピングに使用されるアルゴリズムを変更できるだけでなく、特にポートアドレス変換に使用する IP アドレスの「プール」を指定することができます。これらの機能の詳細については、PAT プールおよびラウンド ロビン割り当て （1364 ページ）を参照してください。 [PAT Pool Address Translation] チェックボックスをオンにして、次のオプションをイネーブルにします。 • [アドレス（Address）] または [インターフェイス（Interface）]：[PATプールアドレス（PAT Pool Address）] フィールドに含まれているのが、PAT プールとして使用するネットワーク/ホスト（またはネットワーク/ホストオブジェクト）であることを示すには、[アドレス（Address）] を選択します。インターフェイスを選択して、フォールスルー インターフェイスを指定します。 • [アドレス（Address）]：上記のアドレスまたはインターフェイスの選択に従って、目的のネットワーク/ホストまたはインターフェイスを入力するか、選択します。 • [ラウンドロビン割り当てを使用（Use Round Robin Allocation）]：「ラウンドロビン」アプローチを使用してアドレス/ポートをマッピングするには、このボックスをオンにします。このオプションの詳細については、PAT プールおよびラウンド ロビン割り当て （1364 ページ）を参照してください。 • [拡張PATテーブル（Extended PAT Table）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：拡張 PAT を有効にするには、このボックスをオンにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IPアドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、ASA 8.4(3) 以降（8.5(1) または 8.6(1) を除く）で使用できます。 • [フラットなポート範囲（Flat Port Range）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：ポートの割り当て時に 1024 ～ 65535 のポート範囲全体の使用を有効にするには、このボックスをオンにします。変換のマッピング ポート番号を選択するときに、ASAによって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッ

要素	説明
	ピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含める（Include Reserved Ports）] もオンにします。 • [予約済みポートを含める（Include Reserved Ports）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：PAT 範囲に予約ポート 1 ～ 1023 を含めるには、このボックスをオンにします。 • [ブロック割り当て（Block Allocation）]（ASA 9.5(1) 以降で使用可能）：ホストごとにポートのブロックを割り当てるには、このボックスをオンにします。この機能は、ASA デバイス 9.5(1) 以降の Security Manager バージョン 4.9 以降でサポートされています。
Destination Translation 宛先アドレスの任意のスタティック変換を設定するには、このセクションのオプションを使用します。 （注） 定義すると、ルールのタイプに関係なく、宛先変換は常にスタティックになります。 （注） これらのオプションは、トランスペアレントモードで動作しているデバイスでは使用できません。	
[元の宛先（Original Destination）] アドレス（Address） インターフェイス	変換がデバイス上のアドレスまたはインターフェイスのどちらに基づくかを示します。次のいずれかを選択します。 • [アドレス（Address）]：[変換済み宛先（Translated Destination）] フィールドで指定したネットワーク/ホストオブジェクトを使用して、元の宛先を変換します。 [アドレス（Address）] を選択した場合、[元の宛先（Original Destination）] エントリフィールドで、元の宛先アドレスを変換するネットワーク/ホストオブジェクトを指定します。 • [インターフェイス（Interface）]：[変換済み宛先（Translated Destination）] フィールドで指定したネットワーク/ホストオブジェクトを使用して、元の宛先を変換します。 [インターフェイス（Interface）] を選択した場合は、[宛先インターフェイス（Destination Interface）] フィールドで目的のインターフェイスを入力または選択します。インターフェイス セレクタ リストには、デバイスに現在定義されているすべてのインターフェイスが含まれています。

要素	説明
[変換済みの宛先（Translated Destination）]	このエントリは、変換に使用する宛先アドレスのプールを示します。目的のネットワーク/ホストオブジェクトを入力するか、選択します。 （注） FPR-2000、FPR-4000、および FPR-9000 シリーズ プラットフォームの ASA 9.17(1) 以降のデバイスで使用する FQDN シングルトンオブジェクトを入力または選択できるようになりました。
Service Translation ポートアドレス変換を設定するには、このセクションのオプションを使用します。 これらのサービス オブジェクトは、サービス プロトコル（TCP または UDP）と 1 つ以上のポートを示します。元のポートから変換後のポートへのマッピングは循環されます。つまり、最初の元の値が最初の変換後の値にマッピングされ、2 番めの元の値が 2 番めの変換後の値にマッピングされるというように、元の値がすべて変換されるまで続きます。その時点までに変換後のポートのプールが枯渇してしまった場合、マッピングは、最初の変換後の値を再使用して続行されます。サービス オブジェクトの設定の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。 （注） [サービス変換（Service Translation）] と次の [このルールに一致するDNS応答を変換（Translate DNS replies that match this rule）] オプションは、同時には使用できません。	
[元のサービス（Original Service）]	変換対象のサービスが定義されているサービスオブジェクトを入力するか、選択します。任意のサービスから、指定した変換後のサービスへの変換を設定するには、[Original Service] フィールドを空白のままにします。 （注） 両方のサービス オブジェクトに指定されているプロトコルが同じである必要があります。
[変換対象サービス（Translated Service）]	変換に使用されるサービスを示すサービスオブジェクトを入力するか、選択します。
[オプション（Options）]	
このルールに一致する DNS 回答の変換	オンにすると、このルールに一致する DNS 応答に埋め込まれたアドレスが書き換えられます。 マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address（または「A」）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、A レコードは実際の値からマッピングされた値に書き換えられます。この機能をサポートするには、DNS インスペクションをイネーブルにする必要があります。

要素	説明
[インターフェイスPATへのフォールスルー(宛先インターフェイス)（Fallthrough to Interface PAT (Destination Interface)）]	オンにすると、ダイナミック PAT のバックアップが有効になります。ダイナミック NAT アドレスのプールが枯渇すると、[Use Address] フィールドで指定されたアドレス プールを使用して、ポート アドレス変換が実行されます。このオプションは、ルーテッド モードで稼働しているデバイスで、タイプとして [Dynamic NAT and PAT] を選択している場合にだけ使用できます。
IPv6	選択すると、インターフェイスの IPv6 アドレスが使用されます。
[IPv4からIPv6へのネット間マッピング（Net to net mapping of IPv4 to IPv6）]	オンにすると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に変換されます（以降も同様）。このオプションを指定しない場合、32 ビットの IPv4 アドレスが IPv6 プレフィックスの後に埋め込まれる IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを選択する必要があります。
[宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]	指定した宛先インターフェイスでプロキシ ARP を無効にするには、このボックスをオンにします。このオプションは、ルールのタイプとして [スタティック（Static）] を選択している場合には使用できません。 （注） このオプションは、方向として [Bidirectional] を選択している場合に、ASA 8.4.2+ デバイスだけで使用できます。 デフォルトでは、すべての NAT ルールは、出力インターフェイスでプロキシ ARP が含まれます。NAT 免除ルールは出力インターフェイスを検出するときにルートの概要に依存する入力トラフィックと出力トラフィックの両方に対して NAT をバイパスするために使用されます。したがって、プロキシ ARP は、NAT 免除ルールを無効にする必要があります。（NAT 免除ルールが常に優先し、[Translation Rules] テーブルの他のすべての NAT ルールの上に表示されます。） （注） [No Proxy ARP] の設定 （2703 ページ）の説明に従って、個々のインターフェイスでプロキシ ARP を無効にすることもできます。
[宛先インターフェイスのルートルックアップの実行（Perform route lookup for Destination Interface）]	このオプションを選択すると、出力インターフェイスは、指定した宛先インターフェイスを使用する代わりにルートルックアップを使用して決定されます。NAT 免除ルールでは、このチェックボックスをオンにしてください。このオプションは、スタティック アイデンティティ NAT でだけサポートされています。 （注） このオプションは、方向として [Bidirectional] を選択している場合に、ASA 8.4.2+ デバイスだけで使用できます。このオプションは、トランスペアレント モードで動作しているデバイスでは使用できません。

要素	説明
単一方向（Unidirectional）	この機能を使用すると、単一方向のみのスタティック NAT ルールか、両方向（順方向と逆方向）に 1 つずつの 2 つのルールを設定できます。 選択すると、このダイアログボックスに含まれる他のオプションの指定に従って、単一のスタティック NAT が作成されます。ダイナミック ルールは、デフォルトでは単一方向です。 選択を解除すると、このダイアログボックスに含まれる他のオプションの指定に従って、両方向の変換を含む 2 つのリンクされたスタティック NAT ルールが作成されます。ルール テーブルでは、各双方向ルール エントリが 2 行で構成されることに注意してください。
説明	（任意）ルールの説明を入力します。
カテゴリ	（任意）ルールに割り当てるカテゴリを選択します。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。 （注） このオプションは、ルールのタイプとして [Dynamic NAT and PAT] を選択している場合には使用できません。

PAT プールおよびラウンド ロビン割り当て

適応型セキュリティ アプライアンス バージョン 8.4.2 以降には、ポートアドレス変換（PAT）が行われる方法を変更できる 2 つの機能が含まれています。特に PAT の IP アドレスプールを明示的に定義でき、PAT 時のポート割り当てに「ラウンド ロビン」アルゴリズムを選択できます。

これらの機能によって、大量の PAT アドレスの設定を単純化でき、DoS 攻撃の一部として利用されることがある、単一の PAT アドレスからの大量の接続を防ぐことができます。

明示的な PAT プールの定義

バージョン 8.4.2 以前では、ダイナミック NAT および PAT ルールを定義するときに、変換に使用する IP アドレスのプールを指定します（ [NATルールの追加/編集（Add/Edit NAT rule）] ダイアログボックスの [変換済みソース（Translated Source）] フィールド）。このプールは、個別のIPアドレス、アドレスの範囲、ネットワーク/ホストオブジェクトまたはネットワーク/ホスト グループ オブジェクト、およびこれらの組み合わせで構成できました。

複数の IP アドレスを含む範囲とオブジェクトが「NAT プール」にあると見なされましたが、個々の IP アドレス、および 1 つ以上の個々の IP アドレスで構成されるグループ オブジェクトが「PAT プール」の一部と見なされました。

デバイスでのアドレス変換は、使用可能なすべてのアドレスを使い果たすまで NAT プールを通じて進行します。その後、PAT プールを使用してポート アドレス変換が起動します。PAT プールの最初の IP アドレスにポートを割り当て、すべてのポート（約 64,000 個）を割り当て

終えると、プールの次のアドレスにポートを割り当てます。その後も同様に動作します。プール内のすべての IP アドレスですべてのポートが完全に登録されると、これ以上の変換は行われません。

バージョン 8.4.2 以降の ASA デバイスでは、ダイナミックな NAT の個別の PAT プールと PAT ルールを明示的に定義できます。このように定義する場合、アドレスの最初の集合（[変換済みソース（Translated Source）] フィールドで定義される）は NAT プールと見なされますが、PAT プールアドレスは、[PATプールアドレス変換（PAT Pool Address Translation）] フィールドで指定されます。

（注） 明示的に PAT プールを指定しない場合、アドレス変換は 8.4.2 以前のデバイスの説明に従って実行されます。

トランスレーション ルールの定義の詳細については、[Add NAT Rule]/[Edit NAT Rule] ダイアログボックス （1355 ページ） を参照してください。

ラウンド ロビン ポート割り当て

バージョン 8.4.2 以降の ASA デバイスでは、PAT 処理でのポート割り当てに別の方法を指定することもできます。すでに説明したように、PAT ポート番号は、最後のポート番号が割り当てられるまで単一の IP アドレスに連続して割り当てられ、その後、プールで次に使用できる IP アドレスを使用して、プロセスが再開します。

ただし、8.4.2 以降のデバイスの新しいパラメータである [PATプールにラウンドロビン割り当てを使用（Use Round Robin Allocation for PAT Pool）] を使用すると、使用可能な IP アドレスとポート番号を使用した「ラウンド ロビン」サイクルを指定できます。 この方法では、プールでそれぞれ連続するアドレスを使用して、アドレス/ポートの組み合わせを割り当てます。その後、最初のアドレスを異なるポートで再度使用し、次に 2 番目のアドレスを使用し、以後、同様に動作します。

さらに、ラウンドロビン アルゴリズムは、PAT 処理でアドレスとポートの組み合わせを割り当てるときに準拠を試行する 2 つの追加の原則を組み込みます。

- 送信元から宛先への特定のマッピングがすでに存在する場合は、アルゴリズムは新しい接続に対して既存の変換を使用しようとします。これが不可能な場合（たとえば、その IP アドレスのすべてのポートが使い果たされたとき）、アルゴリズムは標準のラウンドロビン サイクルを続行します。
- 可能な場合、元の送信元ポート番号がマッピング ポート番号として使用されます。つまり、たとえば、変換するアドレスとポートの組み合わせのポート番号が 4904 で、4904 が PAT プールの次の IP アドレスで使用可能な場合、変換後のアドレスは *PAT_address* /4904 になります。これが不可能な場合（そのポートが次の PAT アドレスで使用できない）、アルゴリズムは標準のラウンドロビンサイクルを続行することに注意してください。

（注） 明示的にラウンドロビン割り当てを指定しない場合、ポート割り当て循環は 8.4.2 以前のデバイスの説明に従って実行されます。

[Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ

ホスト、ネットワーク、またはアドレス範囲オブジェクトの追加または編集に使用するダイアログボックスのいずれかの [NAT] タブを使用して、オブジェクト NAT ルールを作成または更新します。この NAT 設定は、ASA 8.3+ デバイスでだけ使用されます。他のタイプのデバイスでこのオブジェクトを使用した場合、NAT 設定は無視されます。

NAT 設定は、デバイスのオーバーライドとして作成され、グローバル オブジェクトには保持されません。そのため、これらの NAT オプションを設定する場合は、[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択する必要があります（このオプションはダイアログボックスを閉じたときに、自動的に選択されます）。

この項では、[NAT] タブのフィールドについて説明します。[General] タブのフィールドの詳細については、[Add Network/Host]/[Edit Network/Host] ダイアログボックス （395 ページ）を参照してください。

ナビゲーション パス

ホスト、ネットワーク、またはアドレス範囲オブジェクトの作成時か編集時に、[Add Network/Host]/[Edit Network/Host] ダイアログボックス （395 ページ）の [NAT] タブを選択します。

フィールド リファレンス

表 318 : [Add Network/Host]/[Edit Network/Host] ダイアログボックスの [NAT] タブ

要素	説明
Add Automatic Address Translation NAT Rule	オンにすると、ネットワーク アドレス変換（NAT）規則が、ここでの定義に従って、[Translated By] フィールドで指定したデバイスに適用されます。ルールは、そのデバイスの [Translation Rules] テーブルの [Network Object NAT Rule] セクションに表示されます（[Translation Rules]：ASA 8.3+ （1352 ページ）を参照）。
Translated By	NAT ルールを設定するデバイス。[Select] をクリックして、リストからデバイスを選択します。リストは、ASA 8.3+ デバイスだけを表示するようにフィルタリングされています。
送信元インターフェイス（Source Interface）	パケットが発信されるインターフェイスの名前。これは「実際の」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。

要素	説明
Destination Interface	パケットが到着するインターフェイスの名前。これは「マッピングされた」インターフェイスです。デフォルトは、すべてのインターフェイスを表す [任意（Any）] です。
タイプ（Type）	作成する変換ルールのタイプ。 • [静的（Static）]：実際のアドレスからマッピングされたアドレスへのスタティックな割り当てを提供します。 • [PAT（非表示）（PAT (Hide)）]：複数のローカルアドレスから単一のグローバル IP アドレスおよび一意のポート番号へのダイナミックな割り当てをイネーブルにします。 • [ダイナミックNATおよびPAT（Dynamic NAT and PAT）]：実際のアドレスからマッピングされたアドレス、および実際のポートからマッピングされたポートへのダイナミックな割り当てを提供します。
送信元の変換	
Original value	このダイアログボックスの [General] タブで設定したアドレスが表示されます。これは、NAT ルールで変換する送信元アドレスです。アドレス範囲またはネットワークの場合は、範囲またはネットワーク内のすべてのアドレスが変換されます。
Translated Source Use Address Use Interface（スタティックおよびPAT にかぎり有効）	変換がデバイス上のアドレスまたはインターフェイスのどちらに基づくかを示します。 • [アドレスを使用（Use Address）]：指定したアドレスまたはネットワーク/ホストオブジェクトを使用して、元のアドレスを変換します。[アドレス（Address）] フィールドにアドレスまたはオブジェクト名を入力するか、または [選択（Select）] をクリックしてリストからオブジェクトを選択します。 • [インターフェイスを使用（Use Interface）]：[変換済み送信元（Translated Source）] フィールドで指定したインターフェイスに基づいて、元のアドレスを変換します。 （注） [Use Interface] オプションは、タイプとして [Static] または [PAT (Hide)] を選択している場合にだけ使用できます。

要素	説明
PAT Pool Address Translation	

要素	説明
	このオプションは、タイプとして [Dynamic NAT and PAT] を選択している場合に使用できます。関連パラメータを使用すると、PAT マッピングに使用されるアルゴリズムを変更できるだけでなく、特にポート アドレス変換に使用する IP アドレスの「プール」を指定することができます。これらの機能の詳細については、PAT プールおよびラウンド ロビン割り当て （1364 ページ）を参照してください。 [PAT Pool Address Translation] チェックボックスをオンにして、次のオプションをイネーブルにします。 • [アドレスを使用（Use Address）] または [インターフェイスを使用（Use Interface）] : [PATプールアドレス（PAT Pool Address）] フィールドに含まれているのが、PAT プールとして使用するネットワーク/ホスト（またはネットワーク/ホストオブジェクト）であることを示すには、[アドレスを使用（Use Address）] を選択します。フォールスルー インターフェイスを提供するには、[インターフェイスを使用（Use Interface）] を選択します。 • [PATプールアドレス（PAT Pool Address）] : 上記のアドレスまたはインターフェイスの選択に従って、目的のネットワーク/ホストまたはインターフェイスを入力するか、選択します。 • [PATプールにラウンドロビン割り当てを使用（Use Round Robin Allocation for PAT Pool）] : 「ラウンドロビン」アプローチを使用してアドレス/ポートをマッピングするには、このボックスをオンにします。このオプションの詳細については、PAT プールおよびラウンド ロビン割り当て （1364 ページ）を参照してください。 • [拡張PATテーブル（Extended PAT Table）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く） : 拡張 PAT を有効にするには、このボックスをオンにします。拡張 PAT では、変換情報の宛先アドレスとポートを含め、IP アドレスごとではなく、サービスごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。このオプションは、ASA 8.4(3) 以降（8.5(1) または 8.6(1) を除く）で使用できます。 • [フラットなポート範囲（Flat Port Range）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く） : ポートの割り当て時に 1024 ～ 65535 のポート範囲全体の使用を有効にするには、このボックスをオンにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポー

要素	説明
	ト番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用できない場合は、デフォルトで、マッピング ポートは実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、[予約済みポートを含める（Include Reserved Ports）] もオンにします。 • [予約済みポートを含める（Include Reserved Ports）]（ASA 8.4(3) 以降で使用可能、8.5(1) または 8.6(1) を除く）：PAT 範囲に予約ポート 1 ～ 1023 を含めるには、このボックスをオンにします。
Service Translation スタティック ポート アドレス変換を設定するには、[Advanced] パネルのこのセクションのオプションを使用します。 （スタティック ルールにかぎり有効） （注） [サービス変換（Service Translation）] と [このルールに一致するDNS応答を変換（Translate DNS replies that match this rule）] オプションは、同時には使用できません。	
プロトコル	TCP ポートか UDP ポートか。
元のポート	トラフィックがデバイスに着信するポート。
[変換されたポート（Translated Port）]	元のポート番号を交換するポート番号。
[オプション（Options）]	
このルールに一致する DNS 回答の変換	オンにすると、このルールに一致する DNS 応答に埋め込まれたアドレスが書き換えられます。 マッピングされたインターフェイスから実際のインターフェイスへの DNS 応答の場合、Address（または「A」）レコードはマッピングされた値から実際の値に書き換えられます。反対に、実際のインターフェイスからマッピングされたインターフェイスへの DNS 応答の場合、A レコードは実際の値からマッピングされた値に書き換えられます。この機能をサポートするには、DNS インスペクションをイネーブルにする必要があります。 （注） このオプションと [サービス変換（Service Translation）] は、同時には使用できません。

要素	説明
[インターフェイスPATへのフォールスルー(宛先インターフェイス)（Fallthrough to Interface PAT (Destination Interface)）]	オンにすると、ダイナミック PAT のバックアップが有効になります。ダイナミック NAT アドレスのプールが枯渇すると、[Use Address] フィールドで指定されたアドレス プールを使用して、ポート アドレス変換が実行されます。このオプションは、ルーテッド モードで稼働しているデバイスで、タイプとして [Dynamic NAT and PAT] を選択している場合にだけ使用できます。
IPv6	選択すると、インターフェイスの IPv6 アドレスが使用されます。
[IPv4からIPv6へのネット間マッピング（Net to net mapping of IPv4 to IPv6）]	オンにすると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に変換されます（以降も同様）。このオプションを指定しない場合、32 ビットの IPv4 アドレスが IPv6 プレフィックスの後に埋め込まれる IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このオプションを選択する必要があります。
[宛先インターフェイスでARPをプロキシしない（Do not proxy ARP on Destination Interface）]	指定した宛先インターフェイスでプロキシ ARP を無効にするには、このボックスをオンにします。このオプションは、ルールのタイプとして [スタティック（Static）] を選択している場合には使用できません。 デフォルトでは、すべての NAT ルールは、出力インターフェイスでプロキシ ARP が含まれます。NAT 免除ルールは出力インターフェイスを検出するときにルートの概要に依存する入力トラフィックと出力トラフィックの両方に対して NAT をバイパスするために使用されます。したがって、プロキシ ARP は、NAT 免除ルールを無効にする必要があります。（NAT 免除ルールが常に優先し、[Translation Rules] テーブルの他のすべての NAT ルールの上に表示されます。） （注） [No Proxy ARP] の設定 （2703 ページ）の説明に従って、個々のインターフェイスでプロキシ ARP を無効にすることもできます。
[宛先インターフェイスのルートルックアップの実行（Perform route lookup for Destination Interface）]	このオプションを選択すると、出力インターフェイスは、指定した宛先インターフェイスを使用する代わりにルートルックアップを使用して決定されます。NAT 免除ルールでは、このチェックボックスをオンにしてください。このオプションは、スタティック アイデンティティ NAT でだけサポートされています。 （注） このオプションは、トランスペアレント モードで動作しているデバイスでは使用できません。

Per-Session NAT ルール: ASA 9.0（1）+

[Per-Session NATルール（Per-Session NAT Rules）] ページを使用して、選択した ASA 9.0(1)+ デバイスで Per-Session PAT ルールを設定します。デフォルトでは、すべての TCP PAT トラフィッ

クおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。特定のトラフィックに Multi-session PAT を使用するように、Per-session ルールを設定できます。

Per-Session PAT と Multi-Session PAT の比較（バージョン 9.0(1) 以降）

Per-session PAT 機能によって PAT の拡張性が向上し、クラスタリングの場合に各メンバーユニットに独自の PAT 接続を使用できるようになります。Multi-Session PAT 接続は、制御ユニットに転送して制御ユニットを所有者とする必要があります。Per-Session PAT セッションの終了時に、ASA からリセットが送信され、即座に xlate が削除されます。このリセットによって、エンドノードは即座に接続を解放し、TIME_WAIT 状態を回避します。対照的に、Multi-Session PAT では、PAT タイムアウトが使用されます（デフォルトでは 30 秒）。「ヒットエンドラン」トラフィック、たとえば HTTP や HTTPS の場合は、Per-session 機能によって、1 アドレスでサポートされる接続率が大幅に増加することがあります。Per-session 機能を使用しない場合は、特定の IP プロトコルに対する 1 アドレスの最大接続率は約 2000/秒です。Per-session 機能を使用する場合は、特定の IP プロトコルに対する 1 アドレスの接続率は 65535/平均ライフタイムです。

デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックが、Per-session PAT xlate を使用します。Multi-Session PAT のメリットを活用できるトラフィック、たとえば H.323、SIP、Skinny に対して Per-session PAT をディセーブルにするには、Per-session 拒否ルールを作成します。

[Per-Session NATルール（Per-Session NAT Rules）] テーブルの一部の機能

この [Translation Rules] テーブルは、ルール テーブルの使用 （764 ページ）で示すような標準的な Security Manager のルール テーブルです。たとえば、カラムを移動、表示または非表示にしたり、ルールの順序を変更したり、特定のテーブルセルを右クリックしてそのパラメータを編集したりできます。

このテーブルに一覧表示されている NAT ルールは最初に一致したものから順に処理されます。そのため、順序は重要です。

関連項目

- [セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （1374 ページ）
- セキュリティ デバイスの NAT ポリシー （1326 ページ）
- ASA 8.3 以降のデバイスでの「簡易」NAT について （1311 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [NAT] > [Per-Session NATルール（Per-Session NAT Rules）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [NAT（PIX/ASA/FWSM）]>[Per-Session NATルール（Per-Session NAT Rules）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [変換ルール（Translation Rules）] を右クリックして新しいポリシーを作成します。

[Per-Session NATルール（Per-Session NAT Rules）] ページが表示されます。

ルールの追加、編集、および削除

Per-Session NAT ルールを**追加**するには：

1. ルールを追加するルールを選択します。見出しを選択しなかった場合、ルールはデフォルトでテーブルの末尾に追加されます。
2. [Per-Session NATルールの追加（Add Per-Session NAT Rule）] ダイアログボックスを開きます。テーブルの下部にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の任意の場所を右クリックしてポップアップメニューから [行の追加（Add Row）] を選択します。
3. ルールを定義してから [OK] をクリックしてダイアログボックスを閉じると、ルールがテーブルに追加されます。

[Per-Session NATルールの追加（Add Per-Session NAT Rule）] ダイアログボックスの詳細な説明については、[セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （1374 ページ）を参照してください。

Per-Session NAT ルールを**編集**するには：

1. 目的のルールの [Per-Session NATルールの編集（Edit Per-Session NAT Rule）] ダイアログボックスを開きます。[Per-Session NATルール（Per-Session NAT Rule）] テーブルでルールを選択してテーブルの下部にある [行の編集（Edit Row）] ボタンをクリックするか、または単に目的のルールエントリを右クリックしてポップアップメニューから [行の編集（Edit Row）] を選択します。
2. ルールを編集してから [OK] をクリックしてダイアログボックスを閉じます。

[Per-Session NATルールの編集（Edit Per-Session NAT Rule）] ダイアログボックスの詳細な説明については、[セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス （1374 ページ）を参照してください。

NAT ルールを**削除**するには、テーブルでルールを選択してテーブルの下部にある [行の削除（Delete Row）] ボタンをクリックするか、または単に目的のルールエントリを右クリックしてポップアップメニューから [行の削除（Delete Row）] を選択します。

ルールの有効化と無効化

次のように、1 つ以上の連続するルールをテーブルから削除せずにディセーブルにできます。

1. ディセーブルにするルールを選択します。連続したルールのブロックを選択する場合は、ブロックの最初のルールをクリックしてから、ブロックの最後のルールを Shift を押した状態でクリックします。
2. 選択したルールを右クリックして、ポップアップメニューから [無効化（Disable）] を選択します。

無効になっているルールは、テーブルでグレー表示されます。

無効になっている 1 つ以上の連続するルールを再度有効にするには、このプロセスを繰り返して、ポップアップメニューから [有効化（Enable）] を選択します。

[セッションごとのNATルールの追加（Add Per Session NAT Rule）]/[セッションごとのNATルールの編集（Edit Per Session NAT Rule）] ダイアログボックス

デフォルトでは、すべての TCP PAT トラフィックおよびすべての UDP DNS トラフィックが Per-Session PAT を使用します。トラフィックに Multi-Session PAT を使用するには、Per-Session PAT ルールを設定します。許可ルールで Per-Session PAT を使用し、拒否ルールで Multi-Session PAT を使用します。

Per-Session PAT と Multi-Session PAT の違いの詳細については、Per-Session NAT ルール: ASA 9.0（1）+ （1371 ページ）を参照してください。

デフォルト

デフォルトでは、次のルールがインストールされます。

- any（IPv4 および IPv6）から any（IPv4 および IPv6）への TCP を許可する
- any（IPv4 および IPv6）からドメインへの UDP を許可する

これらのルールは、ルール テーブルに表示されません。

（注） これらのルールは削除できません。これらのルールは常に、手動作成されたルールの後に存在します。ルールは順番に評価されるので、デフォルト ルールを無効にすることができます。たとえば、これらのルールを完全に無効にするには、次を追加できます。any（IPv4 および IPv6）から any（IPv4 および IPv6）への TCP を拒否する、any（IPv4 および IPv6）からドメインへの UDP を拒否する

ナビゲーション パス

Per-Session NAT ルール: ASA 9.0（1）+ （1371 ページ）ページから、次のいずれかを実行します。

- ルールを追加するには、ルールを追加するルールを選択してから、ルールテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の任意の場所を右クリックし、[行の追加（Add Row）] を選択して [Per-Session NATルールの追加（Add Per-Session NAT Rule）] ダイアログボックスを開きます。
- ルールを編集するには、ルールを選択して [行の編集（Edit Row）] ボタンをクリックするか、単にルールを右クリックし [行の編集（Edit Row）] を選択して、そのルールの [NATルールの編集（Edit NAT Rule）] ダイアログボックスを開きます。

関連項目

- Per-Session NAT ルール: ASA 9.0（1）+ （1371 ページ）
- [Translation Rules]：ASA 8.3+ （1352 ページ）
- [Add Network/Host]/[Edit Network/Host] ダイアログボックス - [NAT] タブ （1366 ページ）

フィールド リファレンス

表 *319 : [Add NAT Rule]/[Edit NAT Rule]* ダイアログボックス

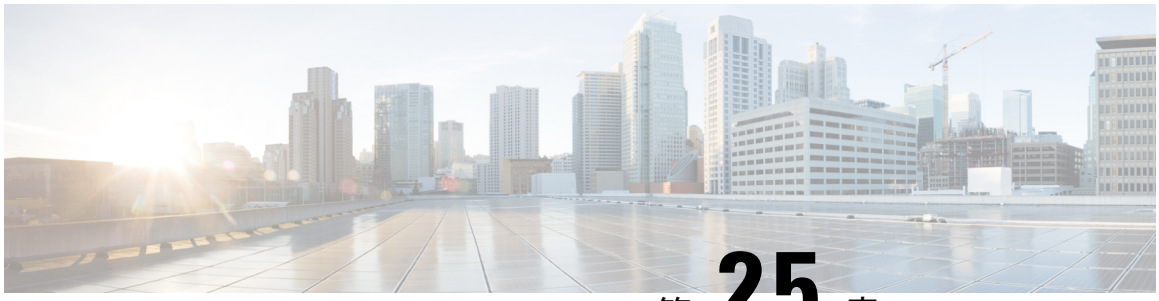
要素	説明
操作	このルールのアクション。許可または拒否します。 許可ルールは、per-session PAT を使用し、拒否ルールは multi-session PAT を使用します。
[元のネットワーク（Original Network）]	送信元アドレス、またはルールが適用されるアドレス（またはネットワーク/ホストオブジェクト）。アドレス範囲またはネットワークの場合は、範囲またはネットワーク内のすべてのアドレスが変換されます。
宛先ネットワーク	宛先アドレス、またはルールが適用されるアドレス（またはネットワーク/ホストオブジェクト）。
[サービス（TCP/UDPのみ）（Service (tcp/udp Only)）]	変換対象のサービスが定義されているサービスオブジェクトを入力するか、選択します。 これらのサービス オブジェクトは、サービス プロトコル（TCP または UDP）と 1 つ以上のポートを示します。サービス オブジェクトの設定の詳細については、サービスとサービス オブジェクトおよびポート リスト オブジェクトの理解と指定 （418 ページ）を参照してください。

要素	説明
カテゴリ	（任意）ルールに割り当てるカテゴリを選択します。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。 （注） このオプションは、ルールのタイプとして [Dynamic NAT and PAT] を選択している場合には使用できません。
説明	（任意）ルールの説明を入力します。

第 III 部

VPN の設定

- サイト間 VPN の管理：基本 （1379 ページ）
- IKE および IPsec ポリシーの設定 （1477 ページ）
- GRE および DM VPN （1575 ページ）
- Easy VPN （1599 ページ）
- Group Encrypted Transport（GET）VPN （1619 ページ）
- リモート アクセス VPN の管理の基礎 （1655 ページ）
- ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理 （1705 ページ）
- リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）（1827 ページ）
- IOS および PIX 6.3 デバイスでのリモートアクセス VPN の管理 （1891 ページ）
- リモート アクセス VPN 用のポリシー オブジェクトの設定 （1917 ページ）
- マップ ビューの使用 （2049 ページ）



第 25 章

サイト間 VPN の管理：基本

バーチャルプライベートネットワーク（VPN）は、インターネットなどのセキュアでないネットワーク経由で相互にプライベート データを安全に送信する、複数のリモート ピアで構成されています。サイト間 VPN は、トンネルを使用してデータ パケットを通常の IP パケット内でカプセル化し、IP ベースのネットワーク経由で転送するものです。その際、暗号化を使用してプライバシーを確保し、認証を使用してデータの整合性を確保します。

Cisco Security Manager では、サイト間 VPN は、VPN トポロジに割り当てられた IPsec ポリシーに基づいて実装されています。IPsec ポリシーとはパラメータのセットであり、これらのパラメータによって、IPsec トンネル内のトラフィックでセキュリティを確保するために使用されるセキュリティ プロトコルやアルゴリズムなど、サイト間 VPN の特性が定義されます。Security Manager は、IPsec ポリシーを、VPN トポロジ内のデバイスに展開可能な CLI コマンドに変換します。IPsec テクノロジーのタイプによっては、VPN トポロジに割り当て可能な完全な設定イメージを定義するために、複数のポリシー タイプが必要となる場合があります。

Site-to-Site VPN Manager では、Cisco IOS セキュリティ ルータ、PIX ファイアウォール、Catalyst VPN サービス モジュール、および Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）ファイアウォール デバイスにサイト間 VPN トポロジおよびポリシーが定義されて設定されます。

ヒント　ASA の資料では、サイト間 VPN は LAN-to-LAN VPN と呼ばれています。これらの用語は同義語であり、この資料では「サイト間 VPN」を使用します。

Site-to-Site VPN Manager にアクセスするには、**[管理（Manage）] > [サイト間VPN（Site-to-Site VPNs）]** を選択するか、またはツールバーの [Site-to-Site VPN Manager] ボタンをクリックします。

また、ポリシー ビューでの共有ポリシーの設定や、デバイス ビューでのトポロジの表示および設定も可能です。ポリシー ビューでは、IPsec ポリシーを VPN トポロジに割り当てることができます。

この章は次のトピックで構成されています。

- VPN トポロジについて　（1380 ページ）
- IPsec テクノロジーおよびポリシーについて　（1384 ページ）

- サイト間 VPN トポロジおよびポリシーへのアクセス （1403 ページ）
- サイト間 VPN ディスカバリ （1406 ページ）
- VPN トポロジの作成または編集 （1416 ページ）
- エクストラネット VPN の作成または編集 （1469 ページ）
- VPN トポロジの削除 （1475 ページ）

VPN トポロジについて

VPN トポロジでは、その VPN に属するピアとネットワーク、およびそれらの間の接続方法が指定されます。VPN トポロジを作成したあと、割り当てられた IPsec テクノロジーに応じて、VPN トポロジに適用可能なポリシーが設定に使用できるようになります。

Security Manager では、ハブアンドスポーク、ポイントツーポイント、完全メッシュという 3 種類の主要なトポロジがサポートされており、これらを使用してサイト間 VPN を作成できます。すべてのポリシーをすべての VPN トポロジに適用できるわけではありません。適用できるポリシーは、VPN トポロジに割り当てられた IPsec テクノロジーに応じて異なります。また、VPN に割り当てられる IPsec テクノロジーは、トポロジタイプに応じて異なります。たとえば、DMVPN および Easy VPN テクノロジーは、ハブアンドスポーク トポロジにだけ適用できます。

詳細については、IPsec テクノロジーおよびポリシーについて （1384 ページ）を参照してください。

ここでは、次の内容について説明します。

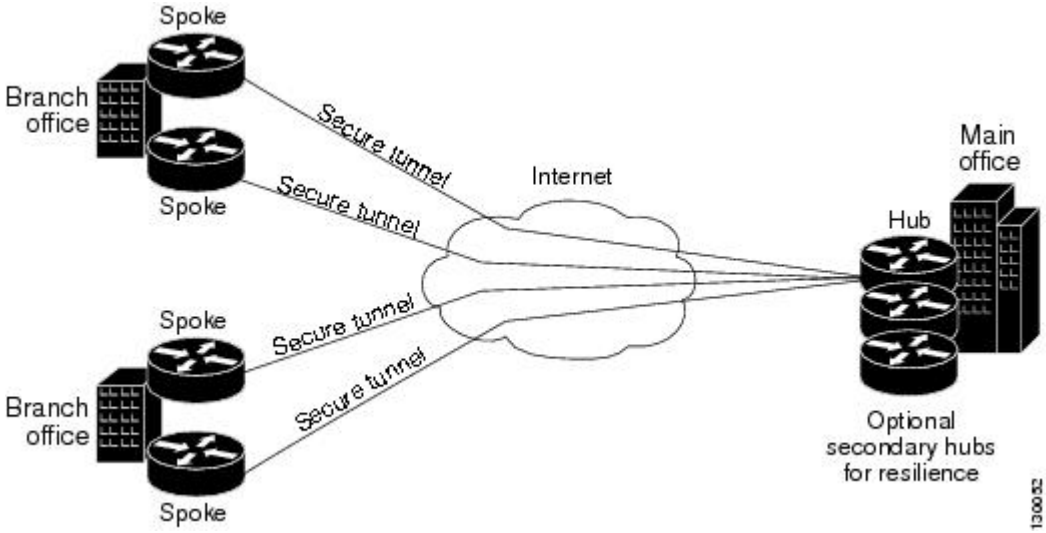
- ハブアンドスポーク VPN トポロジ （1380 ページ）
- ポイントツーポイント VPN トポロジ （1382 ページ）
- 完全メッシュ VPN トポロジ （1382 ページ）
- 暗黙的にサポートされるトポロジ （1384 ページ）

ハブアンドスポーク VPN トポロジ

ハブアンドスポーク VPN トポロジでは、複数のリモート デバイス（スポーク）が 1 つの中央のデバイス（ハブ）と安全に通信します。ハブと個別の各スポークとの間には、保護されたトンネルが個別に設定されます。

次の図に、一般的なハブアンドスポーク VPN トポロジを示します。

図 *30* : ハブアンドスポーク *VPN* トポロジ



通常、このトポロジは、サードパーティネットワークまたはインターネットへの永続的な接続を使用して、企業のメインオフィスとブランチオフィスを接続するイントラネット VPN を表しています。ハブアンドスポーク トポロジの VPN を使用することによって、どのような場所でリモートの業務を行うか、またはその規模や数に関係なく、すべての従業員が企業ネットワークに完全にアクセスできます。

ハブは、一般的には企業のメインオフィスに配置されます。スポークデバイスは、一般的には企業のブランチオフィスに配置されます。ハブアンドスポーク トポロジでは、ほとんどのトラフィックはスポーク サイトにあるホストによって開始されますが、一部のトラフィックは、セントラル サイト側で開始されてスポークに送られる場合もあります。

ハブアンドスポーク設定において何らかの理由でハブが利用できなくなると、IPsec フェールオーバーによって、すべてのスポークが使用するフェールオーバー（バックアップ）ハブにトンネル接続がシームレスに転送されます。1 台のプライマリ ハブに対して、複数のフェールオーバー ハブを設定できます。

ハブアンドスポーク VPN トポロジでは、GET VPN 以外のすべての IPsec テクノロジー タイプを割り当てることができます。

関連項目

- IPsec テクノロジーおよびポリシーについて （1384 ページ）
- 暗黙的にサポートされるトポロジ （1384 ページ）
- IKE および IPsec ポリシーの設定 （1477 ページ）

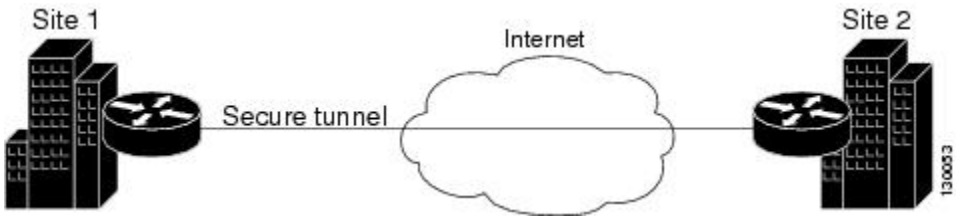
ポイントツーポイント VPN トポロジ

ポイントツーポイント VPN トポロジでは、2 つのデバイスが相互に直接通信します。ハブアンドスポーク設定の場合のような IPsec フェールオーバーのオプションはありません。ポイントツーポイント VPN トポロジを確立するためには、ピア デバイスとして 2 つのエンドポイントを指定します。これら 2 つのデバイスのどちらからでも接続を開始できるため、IPsec テクノロジー タイプとして通常の IPsec または IPsec/GRE のみを割り当てることができます。

Security Manager では、エクストラネットと呼ばれる、通常の IPsec ポイントツーポイント VPN の特殊タイプを設定できます。エクストラネット VPN は、管理対象ネットワーク内のデバイスと管理対象外デバイスの間の接続です。管理対象外デバイスは、サービスプロバイダーのネットワーク内のルータ、シスコ製以外のデバイス、または単に別のグループで管理される、ご使用のネットワーク内のデバイス（つまり、Security Manager インベントリには現れないデバイス）などです。

次の図に、一般的なポイントツーポイント VPN トポロジを示します。

図 *31* : ポイントツーポイントの *VPN* トポロジ



関連項目

- IPsec テクノロジーおよびポリシーについて （1384 ページ）
- 暗黙的にサポートされるトポロジ （1384 ページ）
- VPN トポロジの作成または編集 （1416 ページ）
- エクストラネット VPN の作成または編集 （1469 ページ）
- IKE および IPsec ポリシーの設定 （1477 ページ）

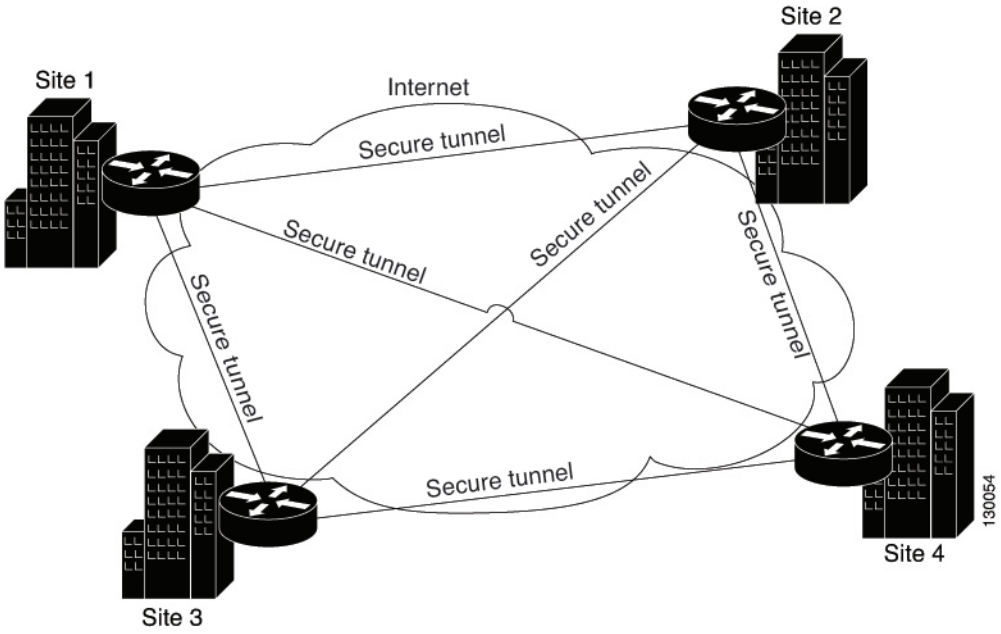
完全メッシュ VPN トポロジ

完全メッシュ トポロジは、すべてのピアが相互に通信する必要があるような複雑なネットワークに適しています。このトポロジ タイプでは、ネットワーク内のすべてのデバイスが固有の IPsec トンネルを経由して他のすべてのデバイスと通信します。すべてのデバイスが相互に直接のピア関係を持っているため、VPN ゲートウェイ デバイスでボトルネックが発生せず、デバイスにおける暗号化および復号化のオーバーヘッドを低減できます。

完全メッシュ VPN トポロジには、通常の IPsec、IPsec/GRE、および GET VPN テクノロジーだけを割り当てることができます。

次の図に、一般的な完全メッシュ VPN トポロジを示します。

図 *32* : フル メッシュ *VPN* トポロジ



完全メッシュ ネットワークは信頼性が高く、冗長性を備えています。GRE テクノロジーが割り当てられている場合は、1 つのデバイス（またはノード）が動作できなくなっても、他のすべてのデバイスは引き続き、直接または1つ以上の中間ノード経由で、相互に通信できます。通常の IPsec では、1 つのデバイスが動作できなくなった場合、保護対象のネットワークを指定するクリプト アクセス コントロール リスト（ACL）が 2 つのピアごとに作成されます。

GET VPN は、グループ トラスト モデルに基づいています。このモデルでは、グループ メンバーはキー サーバに登録されます。キー サーバは、Group Domain of Interpretation（GDOI）プロトコルを使用して、セキュリティ ポリシー、およびグループ メンバー間のトラフィックを暗号化するためのキーを配布します。プライマリ キー サーバと、プライマリ サーバとポリシーを同期するセカンダリ キー サーバを設定できるため、プライマリ キー サーバが利用できなくなった場合にはセカンダリ キー サーバが処理を引き継ぐことができます。

（注） 完全メッシュ トポロジ内のノード数が増加すると、スケーラビリティが問題となる可能性があります。つまり、デバイスが適度な CPU 使用率でサポートできるトンネル数が、制限要因となる可能性があります。

関連項目

- IPsec テクノロジーおよびポリシーについて （1384 ページ）
- 暗黙的にサポートされるトポロジ （1384 ページ）
- VPN トポロジの作成または編集 （1416 ページ）

- IKE および IPsec ポリシーの設定 （1477 ページ）

暗黙的にサポートされるトポロジ

3 つの主要な VPN トポロジに加えて、これらのトポロジを組み合わせた他のより複雑なトポロジを作成することもできます。具体的には以下のとおりです。

- 部分メッシュ：このネットワークでは、一部のデバイスはフル メッシュ トポロジに編成され、その他のデバイスは、フルメッシュ構成のデバイスのうちのいくつかとのハブアンドスポーク接続またはポイントツーポイント接続を形成します。部分メッシュには、フル メッシュ トポロジほどの冗長性はありませんが、導入コストがより低くなります。部分メッシュ トポロジは、通常、完全メッシュ構成のバックボーンに接続する境界ネットワークで使用されます。
- 階層型ハブアンドスポーク：このネットワークでは、あるデバイスが、1 つ以上のトポロジでハブとして動作し、他のトポロジではスパイクとして動作できます。スポーク グループからそれらの直近のハブへのトラフィックが許可されます。
- 結合ハブアンドスポーク：接続して 1 つのポイントツーポイント トンネルを形成する、2 つのトポロジ（ハブアンドスポーク、ポイントツーポイント、またはフル メッシュ）の組み合わせです。たとえば、2 つのハブアンドスポーク トポロジから構成され、それぞれのハブがポイントツーポイント トポロジのピア デバイスとして動作する結合ハブアンドスポーク トポロジを作成できます。

関連項目

- VPN トポロジの作成または編集 （1416 ページ）
- ハブアンドスポーク VPN トポロジ （1380 ページ）
- ポイントツーポイント VPN トポロジ （1382 ページ）
- 完全メッシュ VPN トポロジ （1382 ページ）

IPsec テクノロジーおよびポリシーについて

Security Manager には、サイト間 VPN トポロジのデバイスに設定できる 7 種類の IPsec テクノロジーが用意されています。それらは、通常の IPsec、IPsec/GRE、GRE ダイナミック IP、標準 DMVPN、大規模 DMVPN、Easy VPN、および GET VPN です。割り当てられたテクノロジーに応じて、VPN に対して設定できるポリシーが決まります。

VPN トポロジの作成時に VPN トポロジに IPsec テクノロジーを割り当てることができます。VPN トポロジに IPsec テクノロジーを割り当てたあとは、テクノロジーを変更できません。変更する場合は、いったん VPN トポロジを削除してから新たなトポロジを作成する必要があります。VPN トポロジの名前および IPsec テクノロジーの定義 （1420 ページ）を参照してください。

ここでは、IPsec テクノロジーおよびサイト間 VPN ポリシーのいくつかの基本的な概念について説明します。

- サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （1385 ページ）
- サイト間 VPN ポリシーの概要 （1388 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）
- VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）
- デバイスのオーバーライドを使用した VPN ポリシーのカスタマイズ （1398 ページ）
- VRF 対応 IPsec について （1398 ページ）

サイト間 VPN の必須ポリシーおよびオプションのポリシーについて

一部のサイト間 VPN ポリシーは必須です。つまり、VPN トポロジを作成したり、ポリシー編集時に変更内容を保存したりする場合には、これらのポリシーを設定する必要があります。ほとんどの必須ポリシーには定義済みのデフォルトが用意されています。このデフォルトを使用して VPN トポロジを定義することもできますが、通常はこれらのポリシーを編集して、ご使用のネットワークに適した設定にする必要があります。

オプションのポリシーは、それらのポリシーによって定義されるサービスを必要とする場合にだけ設定する必要があり、デフォルトは用意されていません。

ヒント 必要な設定を指定した共有ポリシーを作成し、VPN 作成時にこれらの共有ポリシーを選択することによって、独自の必須ポリシーのデフォルトを設定できます。共有ポリシーを Create VPN ウィザードのデフォルトとすることもできます。ただし、これらのデフォルト ポリシーはエクストラネット VPN の作成時には適用されません。エクストラネット VPN を使用する場合、常に通常のウィザード フローの一部として必須ポリシーの設定値を設定する必要があります。さらに、IKEv2 認証のデフォルト ポリシーは作成できません。詳細については、 VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。

一部の必須ポリシーは、特定の条件の下でだけ必須となります。たとえば、IKEv1 Preshared Key ポリシーは、デフォルトの（必須）IKEv1 プロポーザルで事前共有キー認証を使用する場合にだけ必須となります。選択された IKE 認証方式が証明書（RSA の署名）である場合は、IKEv1 Public Key Infrastructure ポリシーが必須となります（使用する認証方式の決定 （1486 ページ）を参照）。トポロジで IKEv2 ネゴシエーションを許可する場合、IKEv2 Authentication ポリシーは必須です。

次の表に、サイト間VPNトポロジ内のデバイスに割り当て可能な各定義済みテクノロジーの、必須ポリシーおよびオプションのポリシーを示します。

表 *320 :* サイト間 *VPN IPsec* テクノロジーおよびポリシー

テクノロジー	必須ポリシー	オプションのポリシー
通常の IPsec サイト間 VPN の IPsec プロポーザルについて （1500 ページ）を参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 を許可する場合、IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • IKEv2 を許可する場合、IKEv2 Authentication	• VPN Global Settings
IPsec/Generic Routing Encapsulation（GRE） GRE について （1577 ページ）を参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード	• VPN Global Settings
GRE ダイナミック IP 動的にアドレス指定されるスポークの GRE 設定について （1580 ページ）を参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード	• VPN Global Settings
ダイナミック マルチポイント VPN（DMVPN） DMVPN について （1587 ページ）を参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード	• VPN Global Settings
大規模 DMVPN 大規模 DMVPN の設定 （1595 ページ）を参照してください。	• IKE Proposal • IPsec プロポーザル • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • GRE モード • Server Load Balance	• VPN Global Settings

テクノロジー	必須ポリシー	オプションのポリシー
Easy VPN Easy VPN について （1599 ページ）を参照してください。	• IKE Proposal • Easy VPN IPsec Proposal • Client Connection Characteristics • いずれかのサーバが IOS または PIX 6.3 デバイスである場合、User Group • いずれかのサーバが ASA または PIX 7.0+ デバイスである場合、Connection Profiles	• IKEv1 Public Key Infrastructure（証明書を使用している場合は必須） • VPN Global Settings
GET VPN Group Encrypted Transport（GET）VPN について （1619 ページ）を参照してください。	• Group Encryption • IKE Proposal for GET VPN • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか	• Global Settings for GET VPN
通常の IPSec VTI トンネルインターフェイスの設定（2360ページ）を参照してください。	• IKE Proposal • ピア（Peers） • IKEv1 Preshared Key または IKEv1 Public Key Infrastructure のいずれか • IKEv2 認証 • IPsec プロファイルとのトンネルインターフェイス	

関連項目

- VPN トポロジの作成または編集 （1416 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）
- VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）
- IKE および IPsec ポリシーの設定 （1477 ページ）
- ポリシーについて （209 ページ）

サイト間 VPN ポリシーの概要

サイト間 VPN ポリシーにアクセスするには、[管理（Manage）] > [サイト間VPN（Site-To-Site VPNs）] を選択するか、ツールバーの [Site-To-Site VPN Manager] ボタンをクリックして、[サイト間VPN（Site-To-Site VPN）] ウィンドウのポリシーセレクタで必要なポリシーを選択します。また、デバイス ビューまたはポリシー ビューからサイト間 VPN ポリシーにアクセスすることもできます。詳細については、サイト間 VPN トポロジおよびポリシーへのアクセス （1403 ページ）を参照してください。

バージョン 4.21 以降、Cisco Security Manager は、IKEv2 のサイト間 VPN の複数ピアクリプトマップをサポートしています。ただし、複数ピアクリプトマップは FlexConfig を介してのみ設定できます。

（注） 複数ピアクリプトマップを設定し、VPN トポロジを展開して検出すると、シーケンス内の次のクリプトマップは生成されません。その後の展開では、単一ピアクリプトマップが無効になり、複数ピアクリプトマップが生成されます。

次に、すべてのサイト間 VPN ポリシーの要約を示します。このなかには、共有ポリシーとして作成できないポリシーもあります。一部のポリシーは、リモート アクセスとサイト間 VPN の両方で使用されるため、リモート アクセス VPN を説明するセクションに記載されていることに注意してください。ただし、これらのポリシーは、それぞれのタイプの VPN 用に別の設定する必要があります。

- Client Connection Characteristics。 Easy VPN のクライアント接続特性の設定 （1607 ページ）を参照してください。
- Connection Profiles。 Easy VPN のクライアント接続特性の設定 （1607 ページ）を参照してください。
- Easy VPN IPsec Proposal。 [Connection Profiles] ページ （1715 ページ）を参照してください。
- GRE Modes。 [GRE Modes] ページについて （1575 ページ）を参照してください。
- Group Encryption Policy。 GET VPN ピアの定義 （1461 ページ）を参照してください。
- Group Members。 GET VPN グループ メンバーの設定 （1645 ページ）を参照してください。
- IKE Proposal。 IKE プロポーザルの設定 （1488 ページ）を参照してください。
- IKE Proposal for GET VPN。 GET VPN の IKE プロポーザルの設定 （1638 ページ）を参照してください。
- IKEv2 Authentication。 [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）を参照してください。
- IPsec Proposal。 サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）を参照してください
- Key Servers。 GET VPN キー サーバの設定 （1642 ページ）を参照してください。

- セグメント分割　エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。
- IKEv1 Preshared Key。 IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。
- IKEv1 Public Key Infrastructure。 サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。
- Server Load Balance。 大規模 DMVPN でのサーバ ロード バランシングの設定 （1596 ページ）を参照してください。
- User Group Policy。 Easy VPN における User Group ポリシーの設定 （1617 ページ）を参照してください。
- VPN Global Settings。 VPN グローバル設定 （1517 ページ）を参照してください。
- Global Settings for GET VPN。 GET VPN のグローバル設定 （1640 ページ） を参照してください。

IKEv2 のサイト間 VPN での複数ピアクリプトマップの設定

バージョン 4.21 以降、Cisco Security Manager は、IKEv2 のサイト間 VPN の複数ピアクリプトマップをサポートしています。ただし、複数ピアクリプトマップは FlexConfig を介してのみ設定できます。P2P、ハブアンドスポーク、またはフルメッシュトポロジの複数ピアクリプトマップを作成できます。

この手順では、P2P、ハブアンドスポーク、およびフルメッシュトポロジのサイト間 VPN で複数ピアクリプトマップを設定する方法について説明します。サイト間 VPN トポロジおよびポリシーの詳細については、 サイト間 VPN トポロジおよびポリシーへのアクセス （1403 ページ）を参照してください。

ステップ 1　目的の VPN トポロジ（P2P、ハブアンドスポーク、またはフルメッシュ）を展開します。

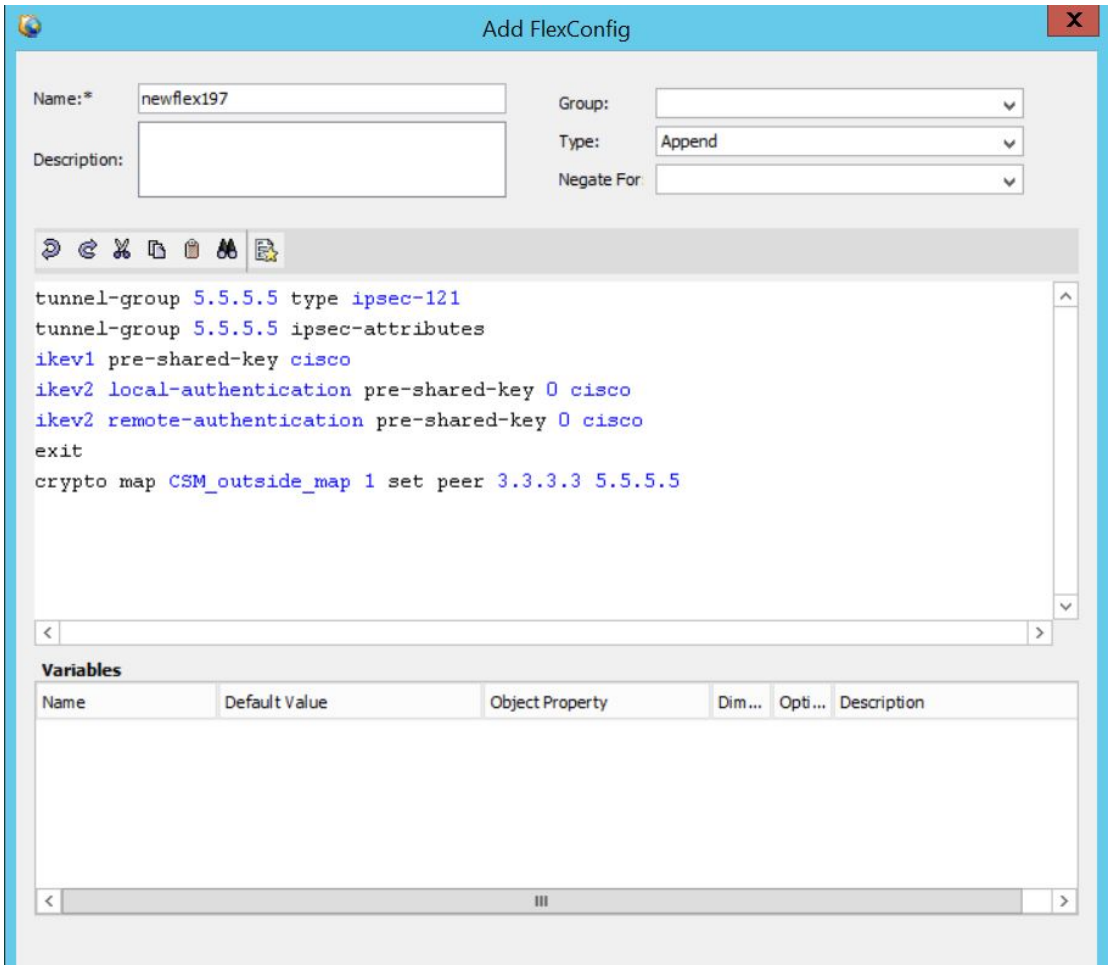
注：ハブアンドスポークトポロジを使用する場合は、ハブピアの**接続タイプ**が**双方向**に設定されていることを確認してください。

ステップ 2　[ツール（Tools）] > [Security Manager の管理（Security Manager Admin）] > [展開（Deployment）] で、[新規または変更済みの FlexConfig のみを展開する（Deploy only new or modified Flexconfigs）] チェックボックスをオフにします。

ステップ 3　[FlexConfig の追加（Add FlexConfig）] をクリックし、[タイプ（Type）] で [付加（Append）] を選択して、複数ピア CLI と対応するトンネルグループ CLI を入力します。

ステップ 4　図 33 : 複数ピア固有 CLI およびトンネルグループ CLIに示すように、複数ピアサポート固有 CLI を入力します。

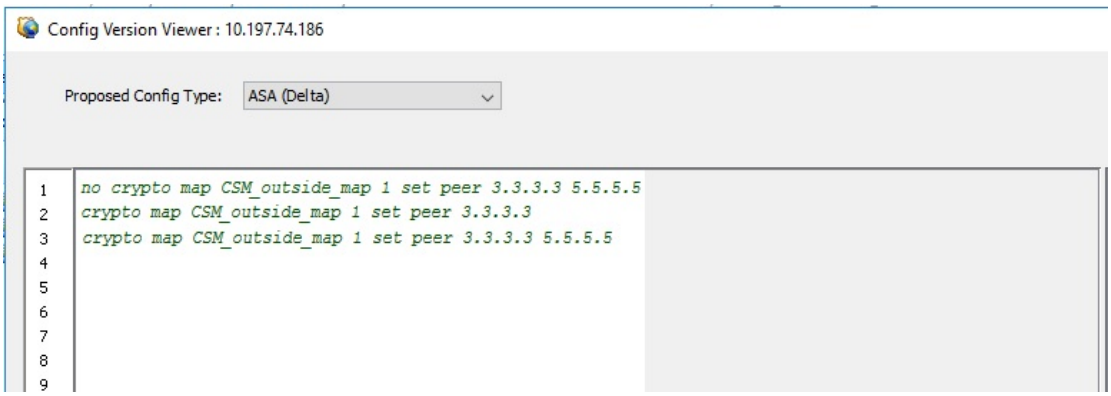
図 *33* : 複数ピア固有 *CLI* およびトンネルグループ *CLI*



ステップ 5 設定のプレビューを行い、新しい設定を展開して、[ポリシー（Policy）]>[VPN ポリシーの検出（Discover VPN Policies）] により、複数ピアクリプトマップを設定した VPN トポロジを再検出します。

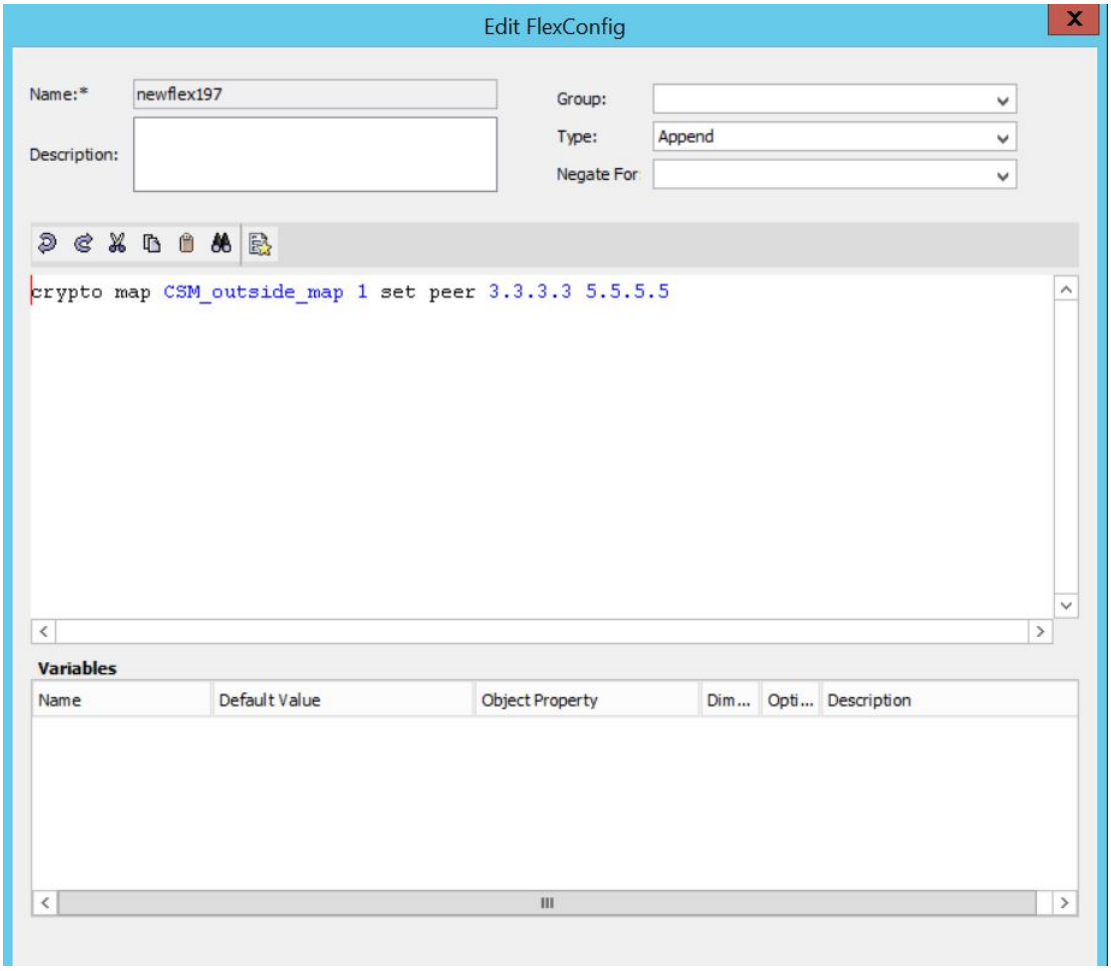
ステップ 6 VPN トポロジを再検出すると、複数ピアクリプトマップ CLI が無効になり、新しい展開が行われるたびに、追加されます。次の図を参照して、CLI がどのように無効になるのかを確認してください。

図 *34 : CLI* の無効化



ステップ 7 次の図に示すように、FlexConfig でトンネルグループ CLI が削除され、複数ピア CLI のみが保持されていることを確認します。

図 *35 :* 複数ピア固有 *CLI*



各 IPsec テクノロジーでサポートされるデバイスについて

各 IPsec テクノロジーでは、異なるデバイスがトポロジのメンバーとしてサポートされます。次の表に、基本的なデバイスのサポートについて示します。これらの要件は、VPN のデバイスを選択する場合に適用されます。場合によっては、デバイス リストは、サポートされているデバイスだけを表示するようフィルタリングされています。また、デバイスは、1 つのロール（スポークなど）としてはサポートされているが、他のロールとしてはサポートされていないことがあります。このような場合は、誤ったデバイス タイプを選択する可能性がありますが、変更内容を保存できないようになっています（メッセージが表示され、具体的な問題の説明が示されます）。

（注） バージョン 4.21 以降、Cisco Security Manager は、すべてのアグリゲーション サービス ルータ、統合サービス ルータ、組み込みサービス ルータ、および Cisco IOS ソフトウェアで動作するすべてのデバイスについて、バグ修正または拡張機能のサポートを含むサポート全体を終了します。

ヒント デバイスモデルによっては、VPN 設定をサポートしていない NO-VPN バージョンがあります。したがって、あるタイプの VPN で 3845 モデルがサポートされていても、3845 NOVPN モデルはサポートされません。さらに、Cisco Catalyst 6500 シリーズ ASA サービスモジュール（ソフトウェアリリース 8.5(x) を実行）は、どのタイプの VPN もサポートしていません。

表 *321* : 各 *IPsec* テクノロジーでサポートされるデバイス

テクノロジー	サポートされるプラットフォーム
通常の IPsec IKE および IPsec ポリシーの設定（1477ページ）を参照してください。	通常の IPsec ポリシーは、Cisco IOS セキュリティ ルータ（アグリゲーション サービス ルータ（ASR）を含む）、PIX ファイアウォール、および ASA 5500 シリーズ デバイスで設定できます。エクストラネット VPN の場合を除き、Catalyst VPN サービス モジュールもサポートされます。 IKEv2 は、ASA リリース 8.4(x) でのみサポートされます。トポロジを IKEv2 のみに制限する場合、すべてのデバイスが IKEv2 をサポートする必要があります。IKEv1 と IKEv2 の両方を許可する場合、IKEv2 をサポートしないデバイスは自動的に IKEv1 を使用します。
IPsec/GRE（Generic Routing Encapsulation）。 GRE について （1577 ページ）を参照してください。	GRE ポリシーは、Cisco IOS セキュリティ ルータ（ASR を含む）および Catalyst 6500/7600 デバイスに設定できます。

テクノロジー	サポートされるプラットフォーム
GRE ダイナミック IP。 動的にアドレス指定されるスポークの GRE 設定について（1580ページ）を参照してください。	GRE ダイナミック IP は、Cisco IOS セキュリティ ルータ（ASR を含む）および Catalyst 6500/7600 デバイスに設定できます。
Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）、大規模 DMVPN。 ダイナミック マルチポイント VPN（DMVPN）（1586 ページ）および大規模 DMVPN の設定（1595ページ）を参照してください。	DMVPN 設定は、Cisco IOS 12.3T 以降のデバイス、および Cisco IOS XE ソフトウェア 2.x 以降（Security Manager では 12.2(33)XNA+ と呼ばれる）を実行している ASR でサポートされます。大規模 DMVPN 設定は、IPsec ターミネータとして Catalyst 6500/7600 デバイスもサポートします。 スポーク間で DMVPN フェーズ 3 接続を使用するには、デバイスは IOS ソフトウェアリリース 12.4(6)T 以降を実行している必要があります。ASR は IOS XE ソフトウェアリリース 2.4（12.2(33)XND と呼ばれる）以降を実行している必要があります。
Easy VPN。 Easy VPN（1599ページ）を参照してください。	Easy VPN サーバーは、Cisco IOS セキュリティルータ（ASR を含む）、Catalyst 6500/7600（サポートされる VPN サービス モジュールまたはポートアダプタを使用）、PIX ファイア ウォール、または ASA 5500 シリーズ デバイスです。 Easy VPN クライアントは、PIX 6.3 を実行する PIX 501、506、506E Firewall、Cisco 800 ～ 3900 シリーズ ルータ、および OS バージョン 7.2 以降を実行する ASA 5505 デバイスでサポートされます。
GET VPN。 Group Encrypted Transport（GET）VPN（1619ページ）を参照してください。	キー サーバは、次のデバイスに設定できます。 • Cisco IOS ソフトウェア Release 12.4(15)T 以降を実行する Cisco 1800、2800、3800 シリーズ ISR、Cisco 7200 シリーズ ルータ、および Cisco 7301 ルータ • Release 15.0 以降を実行する Cisco 1900、2900、3900 シリーズ ISR グループ メンバーは、Cisco 1800、1900、2800、2900、3800、3900 シリーズ ISR、Cisco 7200 シリーズ ルータ、および Cisco 7301 ルータに設定できます。必要最小限のソフトウェア リリース要件は同じです。展開された GET VPN の IPsec SA の数が非常に少ない場合（1 ～ 3 の場合）は、Cisco 871 ISR もグループ メンバーとして使用できます。さらに、Cisco IOS XE ソフトウェア リリース 2.3（12.2(33)XNC）以降を使用する Cisco ASR ルータもグループ メンバーとして設定できます。

（注） Cisco Security Manager 4.21 以降では、ASA ソフトウェアの拡張機能とバグ修正は引き続きサポートされていますが、Cisco IOS ソフトウェアのサポートが終了しているため、ルータのハードウェア サポートは提供されません。

関連項目

- VPN トポロジの作成または編集 （1416 ページ）
- サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （1385 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）
- VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）
- VPN トポロジについて （1380 ページ）
- IKE および IPsec ポリシーの設定 （1477 ページ）
- ポリシーについて （209 ページ）

管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み

VPN には、Security Manager で管理できないデバイスや、Security Manager では管理しないデバイスが含まれることがあります。次のようなものがあります。

- Security Manager ではサポートされているが、ユーザの組織が担当していないシスコ デバイス。たとえば、VPN に、社内の他の部門が管理するネットワーク内のスポークや、サービス プロバイダーやパートナー ネットワークへの接続が含まれている場合があります。
- シスコ製以外のデバイス。Security Manager を使用して、シスコ製以外のデバイスに対する設定を作成したり、展開したりすることはできません。

これらの種類のデバイスを処理する方法は 2 つあります。

- 接続が通常の IPsec ポイントツーポイント接続である場合、エクストラネット VPN の作成または編集 （1469 ページ）で説明されているように、エクストラネット VPN として接続を設定できます。
- その他のタイプの接続の場合、これらのデバイスを「管理対象外」デバイスとして Cisco Security Manager インベントリに含めることができます。これらのデバイスは、VPN トポロジ内でエンドポイントとして機能できますが、Security Manager でデバイスから設定を検出したり、デバイスに設定を展開したりすることはできません。

エクストラネット VPN オプションが機能しない場合、管理対象外デバイスを VPN トポロジに追加する前に以下を実行する必要があります。

- 手動定義によるデバイスの追加 （116 ページ）の手順に従って、デバイスインベントリに管理対象外デバイスとして手動でデバイスを追加します。次の項目を選択する必要があります。
  - VPN でサポートされているテクノロジーという観点から、追加するデバイスに対応するシスコ デバイス タイプを選択します。デバイス タイプによって、デバイスを追加できる VPN トポロジのタイプが決まります。たとえば、GRE や DMVPN では、1800 シリーズや 2800 シリーズなどのサービス統合型ルータを選択できます。Easy VPN では、必要に応じて ASA デバイスや PIX デバイスも選択できます。
  - [Cisco Security Managerで管理（Manage in Cisco Security Manager）] オプションの選択を解除します。デフォルトではすべての新規デバイスが管理対象デバイスとなるため、この操作は重要です。デバイスの追加時にこの操作を行わなかった場合、後で [デバイスのプロパティ（Device Properties）] の [全般（General）] タブ（デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択）でこのオプションの選択を解除できます。
- デバイスのインターフェイス ポリシーを使用して、管理対象デバイスが指す外部 VPN インターフェイスを定義します。デバイスは管理対象外であるため、このポリシーに定義した内容はデバイスに設定されることはありません。単に、Security Manager の外部でデバイスに設定した内容を示すための定義です。

関連項目

- 各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）
- VPN トポロジのデバイスの選択 （1422 ページ）
- VPN トポロジの作成または編集 （1416 ページ）

VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定

Security Manager では、ほとんどの必須 VPN ポリシーに対してポリシーの「出荷時のデフォルト」設定が用意されています。これらのデフォルトは汎用的な内容になっており、ご使用のネットワークに対して適切でない可能性がありますが、デフォルトを使用することによって、必要な共有ポリシーが設定されていない場合に、毎回入力し直すことなく VPN を作成できるという利点があります。このため、必須ポリシーには、独自のデフォルト VPN ポリシーを作成する必要があります。また、特定のオプションのポリシーに対してデフォルトを作成することもできます。

新しいデフォルトを設定する前に、設定する予定の VPN のタイプを検討し、デフォルトを作成できるポリシーのタイプを確認します。[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [VPNポリシーのデフォルト（VPN Policy Defaults）] を選択します。目的の IPsec テクノロジーのタブを選択して、どのようなポリシーを利用できるかを確認します。ポリシーに出荷時のデフォルトが割り当てられている場

合、またはオプションがドロップダウン リストから選択可能な場合、そのポリシーは必須です。その他のポリシーはオプションです。リモート アクセス VPN およびサイト間のエンドポイント設定用のデフォルトポリシーを作成することもできます。選択したポリシーの横にある [コンテンツの表示（View Content）] ボタンをクリックして、ポリシー定義を確認します。

次の手順では、VPNポリシーのデフォルトを作成する方法および使用する方法について説明します。

ヒント

- VPN デフォルト ポリシーを設定すると、共有ポリシーを選択することになります。IPsec テクノロジーに従い、ポリシーごとに設定できるデフォルトは1つだけですが、ユーザは VPNの設定時にさまざまな共有ポリシーを選択できます。したがって、ユーザが選択できる複数の共有ポリシーを設定し、そのうち最も一般的に使用されるポリシーをデフォルトポリシーとして設定できます。VPN設定時にユーザがどのようにさまざまなポリシーを選択できるかの詳細については、新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て （1463 ページ）を参照してください。
- IKEv2 Authentication ポリシーは IKEv2 ネゴシエーションを許可するトポロジの場合は必須ポリシーですが、IKEv2 Authentication の出荷時のデフォルト設定は存在せず、IKEv2 Authentication 共有ポリシーを作成できません。したがって、トポロジで IKEv2 を許可する場合は必ず、トポロジが有効になる前に IKEv2 Authentication ポリシーを手動で設定する必要があります。
- 証明書認証を使用するように IKE Proposal ポリシーを設定する場合、IKEv1 に対して Public Key Infrastructure ポリシーが必須です。ただし、このポリシーに対する出荷時のデフォルト設定は存在しないため、IKEv1 で証明書認証を使用する場合は、デフォルトの Public Key Infrastructure ポリシーを作成することを考慮してください。
- 共有ポリシーを変更すると、そのポリシーを使用しているすべての VPN に影響があることに注意してください。このため、共有ポリシーは、すべての VPN に必要な全社的変更を導入する場合に便利です。ただし、VPN を作成したあと、ユーザは共有ポリシーからローカル ポリシーに切り替えることができます。この場合は、VPN トポロジに対して個別に設定を変更する必要があります。共有ポリシーの詳細については、ポリシー ビューにおける共有ポリシーの管理 （273 ページ）を参照してください。
- これらのデフォルト ポリシーは、エクストラネット VPN の作成時には適用されません。エクストラネット VPN を使用する場合、通常のウィザード フローの一部として必須ポリシーの設定値を必ず設定する必要があります。

ステップ 1 デフォルト ポリシーを作成します。すべてのデフォルト ポリシーは、共有ポリシーです。

a) ポリシービュー（[表示（View）]>[ポリシービュー（Policy View）] を選択）で、デフォルトを設定するポリシーを選択します。ポリシーは、[サイト間VPN（Site-to-Site VPN）] フォルダまたは [リモートアクセスVPN（Remote Access VPN）] フォルダにあります。

b) [共有ポリシー（shared policy）] セレクタの下部にある [ポリシーの作成（+） （Create a Policy(+)）] ボタンをクリックし、ポリシーの名前を入力して、[OK] をクリックします。

c) 必要な設定を行います。選択したポリシーで利用可能な設定についての情報を参照するには、ツールバーの [ヘルプ（?）（Help(?)）] ボタンをクリックします。

d) このプロセスを繰り返して、デフォルト ポリシーを定義する各ポリシーに対して少なくとも 1 つの共有ポリシーを作成します。

ステップ 2 必要に応じて、VPN エンドポイントのデフォルトを作成します。これらのデフォルトは、VPN 接続に使用されるインターフェイス名（GigabitEthernet0/1 など）を識別する、インターフェイス ロール オブジェクトです。内部および外部 VPN インターフェイスには、それぞれ別個のロールを作成します。

a) [管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択して、Policy Object Manager （290 ページ）を開きます。

b) コンテンツテーブルから [インターフェイスロール（Interface Roles）] を選択します。

c) [新規オブジェクト（+）（New Object(+)）] ボタンをクリックし、ネットワーク内の内部または外部 VPN インターフェイスで最も一般的に使用されるインターフェイスを識別するインターフェイス名のパターンを入力して、[OK] をクリックします。

インターフェイス ロール、およびそれらの設定時に使用するワイルドカードの詳細については、インターフェイス ロール オブジェクトについて （381 ページ）およびインターフェイス ロール オブジェクトの作成 （383 ページ）を参照してください。

ステップ 3 ポリシーおよびポリシー オブジェクトをデータベースに送信します。すべての検証エラーを解決する必要があります。

- Workflow 以外のモードで、[ファイル（File）]>[送信（Submit）] を選択します。
- アクティビティ承認者のいない Workflow モードの場合は、[アクティビティ（Activities）]>[承認アクティビティ（Approve Activity）] を選択します。
- アクティビティ承認者のいる Workflow モードの場合は、[アクティビティ（Activities）]>[アクティビティの送信（Submit Activity）] を選択します。アクティビティが承認されるまでは、ポリシーおよびオブジェクトをデフォルトとして選択できません。

ステップ 4 新しく設定したポリシーおよびポリシー オブジェクトを VPN ポリシーのデフォルトとして選択します。

a) [ツール（Tools）]>[Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [VPNポリシーのデフォルト（VPN Policy Defaults）] を選択します（[VPN Policy Defaults] ページ （743 ページ）を参照）。

b) 適切なタブを選択して、デフォルトを設定した必須またはオプションのポリシーそれぞれのドロップダウン リストから、設定したポリシーを選択します。

[S2S Endpoints] タブで、適切なインターフェイス ロール オブジェクトを選択します。

c) [保存（Save）] をクリックして、デフォルトを保存します。

次回ユーザが Create VPN ウィザードを実行すると、選択したデフォルトがウィザードのデフォルトとして使用されます。ユーザは、他の任意の共有ポリシーまたはインターフェイス ロールを選択して、デフォルトを上書きできます。

デバイスのオーバーライドを使用した VPN ポリシーのカスタマイズ

多くの VPN ポリシーでは、設定で Security Manager ポリシー オブジェクトが使用されます。ポリシー オブジェクトとは、再利用可能な設定を作成できるコンテナを指します。

VPN ポリシーは VPN トポロジ内のすべてのデバイスに適用されるため、VPN トポロジ内の特定のデバイスのポリシーで使用されるポリシー オブジェクトを変更する必要がある場合があります。場合によっては、トポロジ内のすべてのデバイスを変更する必要があることもあります。このような変更は、ポリシー オブジェクトに対するデバイス レベルのオーバーライドを使用して行います。

たとえば、PKI ポリシーを定義する場合は、PKI 登録オブジェクトを選択する必要があります。VPN のハブでスポークとは異なる CA サーバが使用されている場合は、デバイス レベルのオーバーライドを使用して、ハブで使用されている CA サーバを指定する必要があります。PKI ポリシーでは単一の PKI 登録オブジェクトが参照されますが、ハブの場合、定義するデバイス レベルのオーバーライドに基づいて、このオブジェクトで表される実際の CA サーバが異なるものとなります。

ポリシーオブジェクトのオーバーライドをイネーブルにするには、ポリシーオブジェクト定義で [デバイスごとのオーバーライドを許可（Allow Override per Device）] オプションを選択する必要があります。その後、デバイス レベルのオーバーライドを作成できます。デバイス レベルでの VPN ポリシー オブジェクトのオーバーライドの詳細については、次の項を参照してください。

- 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）
- 単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）
- 複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）

VRF 対応 IPsec について

ピアツーピア VPN を展開する場合、ルーティング テーブルの分離、および重複したアドレスの使用が障害となります。アドレスの重複は、通常、お客様のネットワークのプライベート IP アドレスを使用することが原因で起こります。この問題は、マルチプロトコル ラベル スイッチング（MPLS）VPN への IPsec トンネルのマッピングを導入する VRF 対応 IPsec 機能を使用することで解決できます。

VRF 対応 IPsec 機能を使用することによって、単一のパブリック向けアドレスを使用して、IPsec トンネルを Virtual Routing and Forwarding（VRF）インスタンスにマッピングできます。VRF インスタンスでは、プロバイダー エッジ（PE）ルータに接続されたカスタマー サイトの VPN メンバーシップが定義されます。VRF は、IP ルーティング テーブル、派生シスコ エクスプレス フォワーディング（CEF）テーブル、転送テーブルを使用するインターフェイスのセット、ルーティング テーブルに含まれる情報を制御するルールおよびルーティング プロトコル パラメータのセットで構成されています。ルーティング テーブルおよび CEF テーブルのセットは、MPLS/VPN ネットワーク全体で VPN カスタマーごとに保持されます。

各 VPN は、ルータに独自のルーティング テーブルおよび転送テーブルを持っているため、VPN に属するすべての顧客またはサイトは、そのテーブルに含まれているルートのセットにだけアクセスできます。すべての PE ルータには、VPN ごとに数多くのルーティング テーブルと、プロバイダー ネットワーク内の他のルータに到達するのに使用できる 1 つのグローバル ルーティング テーブルが保持されています。事実上、数多くの仮想ルータが単一の物理ルータに作成されます。MPLS コアから他の PE ルータへのルート全体にわたり、ルート識別子（RD）などの一意の VPN 識別子を追加することによって、このルーティングの分離は維持されます。

（注） VRF 対応 IPsec は、リモート アクセス VPN のデバイスにも設定できます。詳細については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス）（1900 ページ）を参照してください。

Security Manager では、ハブアンドスポーク VPN トポロジに VRF 対応 IPsec を設定できます。この場合、すべての機能を提供する単一のデバイスを使用することも（「1 ボックス」ソリューション）、それぞれが機能の一部を提供する複数のデバイスを使用することもできます（「2 ボックス」ソリューション）。1 つのデバイスですべての機能を提供するソリューションは、システムに過負荷がかかり、パフォーマンスに悪影響がある可能性があります。一方、2 ボックス ソリューションで機能を分離すると、各機能のスケーラビリティを高めることができます。

ここでは、次の内容について説明します。

- VRF 対応 IPsec 1 ボックス ソリューション （1399 ページ）
- VRF 対応 IPsec 2 ボックス ソリューション （1400 ページ）
- Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化 （1402 ページ）

VRF 対応 IPsec の設定の詳細については、VRF 対応 IPsec の設定 （1445 ページ）を参照してください。

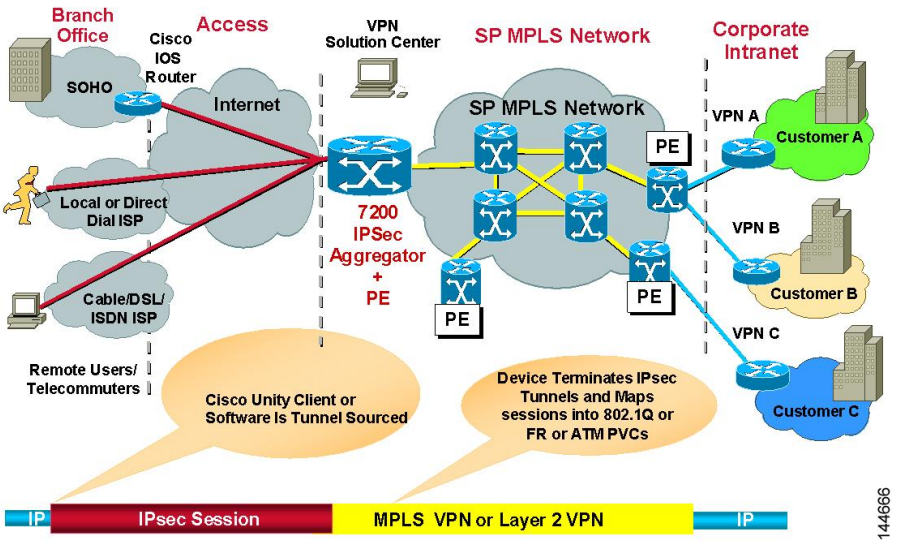
VRF 対応 IPsec 1 ボックス ソリューション

1 ボックス ソリューションでは、IPsec トンネルの終端が Cisco IOS ルータとなり、このルータがプロバイダー エッジ（PE）デバイスとして機能します。PE デバイスは、これらのトンネルを適切な MPLS/VPN ネットワークにマッピングし、カスタマー エッジ（CE）デバイスとの間で IPsec 暗号化および復号化を実行することによって IPsec Aggregator として機能します。

（注） PE デバイスと MPLS クラウドとの間のルーティングの設定は、Cisco IP Solution Center によって行われます。『Cisco IP Solution Center MPLS VPN User Guide』を参照してください。

次の図に、1 ボックス ソリューションのトポロジを示します。

図 *36 : VRF* 対応 *IPsec 1* ボックス ソリューション



関連項目

- VRF 対応 IPsec について （1398 ページ）
- VRF 対応 IPsec の設定 （1445 ページ）
- エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）

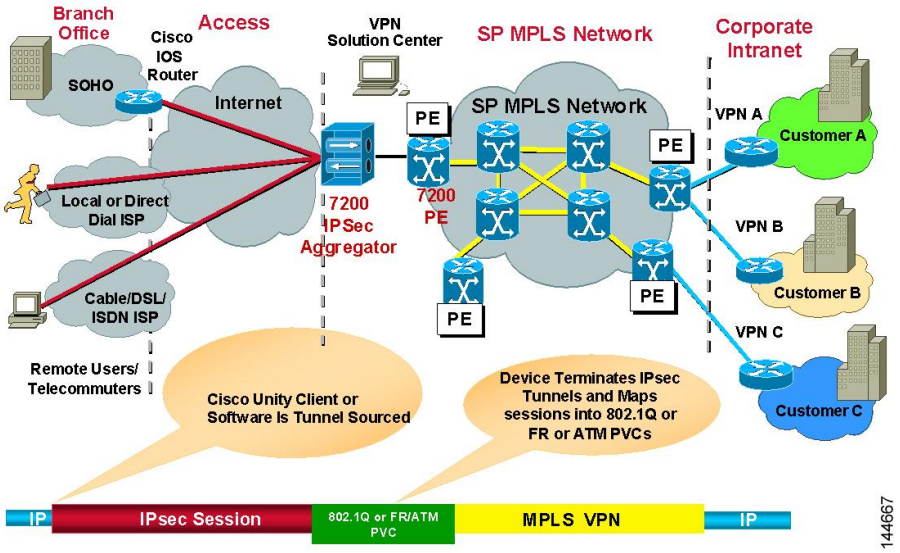
VRF 対応 IPsec 2 ボックス ソリューション

2 ボックス ソリューションでは、PE デバイスは MPLS マッピングだけを行います。CE との間の IPsec 暗号化および復号化は、別の IPsec Aggregator によって行われます。

（注） Security Manager は、PE デバイスへのルーティングも含め、IPsec Aggregator を完全に管理します。PE デバイスは、Cisco IP Solution Center によって完全に管理されます。これには、PE デバイスと MPLS クラウドとの間のルーティングや、PE から IPsec Aggregator へのルーティングが含まれます。詳細については、『Cisco IP Solution Center MPLS VPN User Guide』を参照してください。

次の図に、2 ボックス ソリューションのトポロジを示します。

図 *37 : VRF* 対応 *IPsec 2* ボックス ソリューション



2 ボックス ソリューションを使用して、次のように VPN トポロジのデバイスに VRF 対応 IPsec を設定します。

1. IPsec Aggregator と PE デバイスとの間の接続を設定します。

ハブアンドスポーク VPN トポロジを作成して、それに IPsec テクノロジーを割り当てます。このトポロジでは、ハブは IPsec Aggregator です。スポークは、Cisco IOS ルータ、PIX ファイアウォール、Catalyst VPN サービス モジュール、または Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスです。IPsec Aggregator は、セキュリティ ルータまたは Catalyst VPN サービス モジュールです。次に、ハブに VRF パラメータ（VRF 名および一意のルート識別子）を定義します。

（注） VRF 対応 IPsec では、Cisco IOS ルータおよび Catalyst VPN サービス モジュールへの IPsec、GRE、または Easy VPN テクノロジーの設定がサポートされています。DMVPN は、Cisco IOS ルータでだけサポートされています。

1. IPsec Aggregator と PE デバイスとの間の VRF 転送インターフェイス（または Catalyst VPN サービス モジュールの VLAN）を指定します。
2. IPsec Aggregator と PE との間で使用するルーティング プロトコルおよび自律システム（AS）番号を定義します。使用可能なルーティング プロトコルには、BGP、EIGRP、OSPF、RIPv2、スタティック ルートがあります。

IPsec Aggregator と PE との間に定義されたルーティング プロトコルが、保護された IGP で使用されるルーティング プロトコルと異なる場合、ルーティングはこのルーティング プロトコルと AS 番号を使用して保護された IGP に再配布されます。ルーティングは、保護された IGP から PE にも再配布されます。

（注） ルーティングの再配布は、選択されたテクノロジーが IPsec/GRE または DMVPN の場合にだけ関連します。

関連項目

- VRF 対応 IPsec について （1398 ページ）
- VRF 対応 IPsec の設定 （1445 ページ）
- エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）

Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチをサポートしますが、Cisco Catalyst スイッチはサポートが終了しているため、拡張機能はサポートされません。

既存のサイト間 VPN の Catalyst スイッチおよび 7600 ハブで Virtual Routing and Forwarding（VRF）モードを変更すると、展開に失敗します。たとえば、最初に Create VPN ウィザードで VRF を設定して展開したあと、Peers ポリシーに戻って [Enable VRF Settings] チェックボックスの選択を解除すると、展開に失敗します（この設定は、[エンドポイントの編集（Edit Endpoints）] ダイアログボックスの [VRF対応IPSec（VRF Aware IPSec）] タブにあります。VRF 対応 IPsec の設定 （1445 ページ）を参照してください）。最初に設定されていない VPN で VRF を有効にしようとすると、同様に展開が失敗します。

Catalyst 6500/7600 では、VPN の動作中には VRF モードを変更できません。この制限は、Catalyst 6500/7600 ハブに対してだけ適用されます。他のデバイス タイプには適用されません。

この制限は、VRF 設定自体に加えられる変更には適用されません。たとえば、VPN トポロジに VRF が設定されている場合、Peers ポリシーに戻って VRF 名やルート識別子を変更することができます。

VPN の VRF モードを変更する必要がある場合に、Catalyst 6500/7600 デバイスをハブとして使用しているときは、次の手順を実行します。

関連項目

- VRF 対応 IPsec について （1398 ページ）
- VRF 対応 IPsec 1 ボックス ソリューション （1399 ページ）
- VRF 対応 IPsec 2 ボックス ソリューション （1400 ページ）

ステップ 1 Security Manager から VPN トポロジを削除します。

ステップ 2 変更を展開します。

ステップ 3 Catalyst 6500/7600 デバイスをリロード（再起動）します。

ステップ 4 Security Manager でデバイスを右クリックして、[デバイスでポリシーを検出（Discover Policies on Device）] を選択します。完全なポリシー再検出を実行します。

ステップ 5 Create VPN ウィザードを開いて、VPN トポロジを再定義します。これで、異なる VRF モードを選択できるようになりました。VRF 対応 IPsec の設定 （1445 ページ）およびVPN トポロジの作成または編集 （1416 ページ）を参照してください。

サイト間 VPN トポロジおよびポリシーへのアクセス

次の方法を使用して、サイト間 VPN トポロジおよびポリシーへのアクセスおよび設定を行うことができます。

- Site-to-Site VPN Manager：VPN トポロジを設定するための主要なツールです。Security Manager で設定されているすべてのサイト間 VPN のリストを表示して、それらの設定やポリシー（デバイス メンバーシップを含む）を編集できます。このツールの使用方法の詳細については、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を参照してください。
- デバイス ビューの [サイト間VPN（Site-to-Site VPN）] ポリシー：デバイス ビューでデバイスを選択するときに、ポリシー セレクタで [サイト間VPN（Site-to-Site VPN）] ポリシーを選択して、デバイスが参加しているすべてのサイト間 VPN のリストを表示し、それらのトポロジを編集できます。新しい VPN を作成したり、VPN を選択して Site-to-Site VPN Manager を開き、選択した VPN のポリシーを編集したりすることもできます。このデバイス ビューのポリシーは、実質的には Site-to-Site VPN Manager へのショートカットです。このポリシーの使用方法の詳細については、デバイス ビューにおける VPN トポロジの設定 （1405 ページ）を参照してください。
- ポリシー ビューの [サイト間VPN（Site-to-Site VPN）] フォルダ：ポリシー ビューは、共有ポリシーを作成するために使用されます。多くのサイト間 VPN ポリシーは、共有可能です。したがって、Site-to-Site VPN Manager でトポロジを設定するときに、複数の VPN トポロジに割り当てることができる共有ポリシーを設定できます。VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）に説明したように、共有ポリシーを Create VPN ウィザードのデフォルトとして設定できます。

[Site-to-Site VPN Manager] ウィンドウでも、デバイス ビューのローカル ポリシーから作成する場合と同様に共有ポリシーを作成できますが、[Site-to-Site VPN Manager] ウィンドウにおいては、共有に関するすべてのコマンドは右クリックして表示されるコンテキスト メニューからだけ利用できます（共有可能ポリシーを右クリックします）。

ポリシー ビューにおける共有ポリシー作成の詳細については、ポリシー ビューにおける共有ポリシーの管理 （273 ページ）を参照してください。

[Site-to-Site VPN Manager] ウィンドウ

Site-to-Site VPN Manager には、Security Manager で設定されたすべてのサイト間 VPN が表示されます。ウィンドウの左上ペインにある VPN セレクタには、既存の VPN トポロジがすべて表示されます（VPN トポロジについて （1380 ページ）を参照）。アイコンは、VPN のタイプ（ハブアンドスポーク、ポイントツーポイント、または完全メッシュ）を示します。トポロジを表示または編集するには、トポロジを選択します。これにより、左下ペインのポリシーセレクタにそのポリシーがロードされます。ポリシーを選択すると、その定義が右側のペインに表示されます。

Site-to-Site VPN Manager を開くには、ツールバーの [Site-To-Site VPN Manager] ボタンをクリックするか、**[管理（Manage）] > [サイト間VPN（Site-To-Site VPNs）]** を選択します。

[Site-to-Site VPN Manager] ウィンドウを使用して、次のことを行うことができます。

- VPN トポロジを作成、編集、および削除します。
  - VPN トポロジを作成するには、VPN セレクタの上にある [VPN トポロジの作成（Create VPN Topology）]（+）ボタンをクリックし、表示されるオプションから、作成するトポロジのタイプを選択します。これにより、Create VPN ウィザードまたは Create Extranet VPN ウィザードが開きます。詳細については、VPN トポロジの作成または編集 （1416 ページ）またはエクストラネット VPN の作成または編集 （1469 ページ）を参照してください。
  - VPN トポロジを編集するには、トポロジを選択して [VPN トポロジの編集（Edit VPN Topology）]（鉛筆）ボタンをクリックするか、トポロジを右クリックして [編集（Edit）] を選択します。これにより、[Edit VPN] ダイアログボックスまたは [Edit Extranet VPN] ダイアログボックスが開きます。このダイアログボックスには、Create VPN ウィザードと同様のページのほとんどがタブ形式のレイアウトで表示されます。
  - VPN トポロジを削除するには、トポロジを選択して [VPN トポロジの削除（Delete VPN Topology）]（ゴミ箱）アイコンをクリックするか、トポロジを右クリックして [削除（Delete）] を選択します。削除の確認が求められます。VPN トポロジの削除 （1475 ページ）を参照してください。
- 各 VPN トポロジについての詳細情報を表示します。トポロジを選択して、[VPN Summary] ポリシーを選択します。[VPN トポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）] （1464 ページ）を参照してください。
- VPN トポロジに定義されたエンドポイントを表示および設定します。エンドポイントは、VPN トポロジ編集時に [エンドポイント（Endpoints）] タブで確認するか、または [ピア（Peers）] ポリシーを選択して確認します。GET VPN トポロジの場合、[ピア（Peers）] ポリシーはありません。代わりに、[キーサーバー（Key Servers）] ポリシーと [グループメンバー（Group Members）] ポリシーを使用して、エンドポイントを表示および設定します。エクストラネット VPN の場合、エンドポイントは VPN 編集時の [Device Selection] タブ、または [Peers] ポリシーにも表示されます。

- VPN トポロジに割り当てられたポリシーの表示と編集、共有ポリシーの割り当て、または既存のポリシーからの共有ポリシーの作成を行います。個別のポリシーの詳細については、サイト間 VPN ポリシーの概要 （1388 ページ）を参照してください。

Site-to-Site VPN Manager から共有ポリシーを設定する場合のオプションおよび方法は、デバイス ビューから設定する場合と同じです。これについては、デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）およびポリシー バナーの使用 （258 ページ）の項で説明しています。ポリシーの共有、割り当て、割り当て解除、割り当ての編集、および名前の変更を行うことができますが、VPN ポリシーの継承はできません。これらのタスクを実行するには、VPN トポロジを選択し、目的のポリシーを右クリックして、必要なコマンドを選択します。

ポリシー ビューを使用して共有 VPN ポリシーを設定することもできます。

デバイス ビューにおける VPN トポロジの設定

デバイスが属するサイト間 VPN トポロジがある場合は、デバイス ビューの Site-to-Site VPN ポリシーを使用して、サイト間 VPN トポロジを表示および編集できます。VPN ポリシーを編集したり、デバイスがトポロジに参加するかどうかを変更したりできます。また、新しい VPN トポロジを作成することもできます。

このポリシーは、実質的には Site-to-Site VPN Manager へのアクセス ポイントです（サイト間 VPN ディスカバリ （1406 ページ）を参照）。

このポリシーを開くには、デバイスビューで目的のデバイスを選択して、ポリシーセレクタから [サイト間VPN（Site-to-Site VPN）] を選択します。

VPN トポロジ テーブルには、このデバイスが属するすべてのサイト間 VPN が表示されます。VPN のタイプ、その名前、IPsec テクノロジー、説明などの情報が表示されます。バージョン 4.9 以降、Security Manager は VPN トポロジの最後に変更されたチケットの情報も表示します。チケット管理システムを使用して作成または編集された VPN トポロジには、このページで利用可能な最後に変更されたチケットの ID 情報があります。また、最後に変更されたチケットの ID で VPN トポロジをフィルタリングすることもできます。

- VPN を追加するには、[VPNトポロジの作成（Create VPN Topology）] ボタンをクリックするか、またはテーブルを右クリックして [VPNトポロジの作成（Create VPN Topology）] を選択し、表示されるオプションから作成するトポロジのタイプを選択します。これにより、Create VPN ウィザードまたは Create Extranet VPN ウィザードが開きます。詳細については、VPN トポロジの作成または編集 （1416 ページ）またはエクストラネット VPN の作成または編集 （1469 ページ）を参照してください。

- VPN を編集するには、VPN を選択して [VPNトポロジの編集（Edit VPN Topology）] ボタンをクリックするか、VPN を右クリックして [VPNトポロジの編集（Edit VPN Topology）] を選択するか、または単にエントリをダブルクリックします。これにより、[Edit VPN] ダイアログボックスまたは [Edit Extranet VPN] ダイアログボックスが開きます。このダイアログボックスは、Create VPN ウィザードのタブ形式バージョンです（VPN トポロジの作成または編集 （1416 ページ）またはエクストラネット VPN の作成または編集 （1469 ページ）を参照）。

- VPN のポリシーを編集するには、VPN を選択して、[VPNポリシーの編集（Edit VPN Policies）] ボタンをクリックします。VPN トポロジについての情報が表示された [Site-to-Site VPN] ウィンドウが開きます。ポリシー セレクタから目的のポリシーを選択して、編集します。
- VPN を削除するには、VPN を選択して [VPNトポロジの削除（Delete VPN Topology）] ボタンをクリックするか、または VPN を右クリックして [VPNトポロジの削除（Delete VPN Topology）] を選択します。削除の確認が求められます。詳細については、VPN トポロジの削除 （1475 ページ）を参照してください。

サイト間 VPN ディスカバリ

すでにネットワークに展開されている VPN トポロジを検出して、それらを Security Manager を使用して管理できます。VPN 設定が Security Manager に取り込まれて、サイト間 VPN ポリシーとして表示されます。

エクストラネット VPN の場合を除き、すでに Security Manager によって管理されている既存の VPN トポロジの設定を再検出することもできます。サイト間 VPN の再検出の詳細については、サイト間 VPN の再検出 （1415 ページ）を参照してください。

（注） また、すでにネットワークに展開されているリモート アクセス VPN のデバイスの設定も検出できます。リモート アクセス VPN ポリシーの検出 （1669 ページ）を参照してください。

次の各項では、サイト間 VPN ディスカバリについて説明します。

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ （1406 ページ）
- VPN ディスカバリの前提条件 （1408 ページ）
- VPN ディスカバリ ルール （1408 ページ）
- サイト間 VPN の検出 （1411 ページ）
- 検出された、複数のスポーク定義を持つ VPN の定義または修復 （1413 ページ）
- サイト間 VPN の再検出 （1415 ページ）

VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ

ここでは、Security Manager で検出できるテクノロジーとトポロジ、および Security Manager によってプロビジョニングされるが検出できない VPN 機能について説明します。

VPN ディスカバリでサポートされるテクノロジー

- IPsec（ASA デバイスの LAN-to-LAN 設定を含む）
- IPsec + GRE
- IPsec + GRE ダイナミック IP
- DMVPN
- Easy VPN
- GET VPN

VPN ディスカバリでサポートされるトポロジ

- ポイントツーポイント
- ハブアンドスポーク
- 完全メッシュ
- エクストラネット VPN（管理対象外デバイスに対するポイントツーポイント）

Security Manager によってプロビジョニングされるが VPN ディスカバリではサポートされていない VPN 機能

- IPsec ターミネータを使用した大規模 DMVPN（高集中ハブ）
- VRF 対応 IPSec
- ダイヤル バックアップ
- Easy VPN の IPsec および ISAKMP プロファイル
- ハイ アベイラビリティ Easy VPN

Security Manager を使用してこれらのタイプのポリシーを定義および展開すると、検出されなかったデバイス設定がポリシーによって上書きされます。したがって、Security Manager で既存の設定を管理する場合には、既存の設定と可能なかぎり一致するようにポリシーを定義する必要があります（[Tool（ツール）]>[設定のプレビュー（Preview Configuration）] を使用して、展開する前に結果を調べます）。VPN のプロビジョニングメカニズムでは、（既存の設定の内容が Cisco Security Manager で設定されたポリシーに一致するという前提で）可能なかぎり既存の設定の内容が利用されますが、CLI コマンドで使用される命名規則は維持されません。

関連項目

- VPN ディスカバリの前提条件 （1408 ページ）
- VPN ディスカバリ ルール （1408 ページ）
- サイト間 VPN の検出 （1411 ページ）

VPN ディスカバリの前提条件

正常に VPN を検出するためには、次の前提条件を満たしている必要があります。

- エクストラネット VPN の場合を除き、VPN に参加するすべてのデバイスを Security Manager インベントリに追加する必要があります。
- Security Manager で、VPN に関するいくつかの基本的な情報を指定する必要があります。VPN ディスカバリ ウィザードでは、次の情報の入力を求められます。
  - VPN トポロジ（ハブアンドスポーク、ポイントツーポイント、完全メッシュ、エクストラネット）。
  - VPN テクノロジー（通常の IPsec、IPsec/GRE、GRE ダイナミック IP、DMVPN、Easy VPN、GET VPN）。
  - VPN 内のデバイスおよびそのロール（ハブまたはスポーク）。エクストラネット VPN の場合、管理対象デバイスのみを指定します。
  - VPN 設定のソース。VPN は、ライブネットワークから直接検出することも、Security Manager の Configuration Archive から検出することもできます。
- VPN の各デバイスでは、物理インターフェイスにクリプト マップが関連付けられている必要があります。このルールは、エクストラネット VPN 内のリモート（管理対象外）デバイスには適用されません。
- VPN トポロジ内のルーティング プロトコルとして OSPF を使用する場合は、VPN 内のすべてのデバイスで同じ OSPF プロセス番号を使用する必要があります。
- Easy VPN トポロジ内の各 PIX 6.3 または ASA 5505 クライアント デバイスに vpnclient 設定が必要です。

関連項目

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ（1406 ページ）
- VPN ディスカバリ ルール （1408 ページ）
- サイト間 VPN の検出 （1411 ページ）

VPN ディスカバリ ルール

次の表に、Security Manager が VPN 設定を変換および検出する場合のルール、およびデバイスの設定が Security Manager によってサポートされている設定と一致しない場合の処理方法について示します。

ヒント　エクストラネット VPN 検出には単一デバイス（管理対象デバイス）の分析が含まれるため、これらのルールのほとんどはエクストラネット VPN 検出には適用されません。VPN 内のデバイス間の値の整合性を含むルールはすべて適用されません。

表 *322 : VPN* ディスカバリ ルール

条件	VPN ディスカバリの処理
Security Manager が、ライブ デバイス検出のために VPN 内のデバイスに接続できない	• デバイスが VPN 内の唯一のハブまたはスポークである場合、検出は失敗します。 • VPN 内に他のハブやスポークがある場合、検出は進行しますが、利用できないデバイスは検出されません。 • エクストラネット VPN の場合を除き、デバイスがポイントツーポイントトポロジのピアである場合、検出は失敗します。エクストラネット VPN の場合、管理対象デバイスにのみ接続し、接続できないと検出は失敗します。 • デバイスが完全メッシュ トポロジのピアであり、利用できないデバイスを含めてトポロジ内にデバイスが 2 つしかない場合、検出は失敗します。3 つ以上のデバイスがある場合、検出は進行しますが、利用できないデバイスは検出されません。
VPN が ASA 上の LAN-to-LAN VPN である	ASA の資料では、「サイト間」の同義語として「LAN-to-LAN」が使用されています。LAN-to-LAN VPN 設定では、ASA はトンネルグループを使用します。トンネルグループをリモートアクセス VPN 設定で使用すると、Security Manager は接続プロファイルとして検出します。 LAN-to-LAN（L2L）トンネル グループを使用する ASA でサイト間 VPN を検出する場合、Security Manager はサイト間 VPN トポロジを作成し、L2L トンネル グループはユーザに対して接続プロファイルとして表示されません。代わりに、VPN トポロジのプロパティを編集すると、展開中に、Security Manager が設定を適切な L2L トンネル グループのコマンドに変換します。

条件	VPN ディスカバリの処理
VPN 内のデバイス全体において、VPN 設定のポリシーまたは値に不整合がある	• ハブとスポークの値が異なる場合は、ハブの値が優先されます。 • いくつかのポリシーまたは値の候補から単に 1 つのポリシーや値を選択するだけで済み、機能的な問題が発生しない場合には、Security Manager によってすべてのデバイスに共通するポリシーまたは値が 1 つ選択されます。たとえば、デバイスには複数の IKE ポリシーを設定できますが、VPN では単一の IKE ポリシーだけを選択できます。 • 1 つの値を選択すると機能的な問題が発生する場合は、ポリシーに対して値が検出されず、展開時に確認メッセージが表示されます。 • 数値が異なる場合は、検出中にメッセージが表示され、小さい方の値が検出されます。たとえば、IPsec ポリシーにおいては、最小の SA ライフタイム値が検出されます。 • 上記いずれも実行できない場合、VPN ディスカバリは失敗します。
事前共有キー設定で、ピアのセットごとに異なるキーが存在する	Preshared Key ポリシーは検出されないため、検出完了後に設定する必要があります。Security Manager では、すべてのデバイスで事前共有キーの値が同じ場合にだけ Preshared Key ポリシーが検出されます。
デバイスに複数のクリプト マップ候補が存在する	VPN ディスカバリで選択されたすべてまたは大部分のデバイスに関連付けられているクリプト マップが使用されます。
スポークに、ハブに関連付けられたクリプト マップがない	VPN ディスカバリは進行しますが、スポークは検出されず、エラー メッセージが表示されます。
デバイスに、選択されたトランスフォーム セット値がない	VPN ディスカバリは進行しますが、デバイスは VPN トポロジから削除されることがあります。
デバイスに、選択された IKE プロポーザルがない	VPN ディスカバリは進行しますが、デバイスは VPN トポロジから削除されることがあります。
デバイスで DVTI がサポートされているが、DVTI またはクリプト マップが設定されていない	VPN ディスカバリは失敗します。

条件	VPN ディスカバリの処理
サーバで DVTI がサポートされているが、DVTI 設定に IP アドレスが設定されていない	VPN ディスカバリは進行しますが、警告が表示されます。
クライアントで DVTI がサポートされていない	ハブに DVTI が設定されている場合は、警告やエラーは表示されずに検出が進行します。
ハブアンドスポーク トポロジで、スポークがハブと同じ VPNSPA/VSPA スロットを使用していない（Catalyst 6500/7600）	VPN ディスカバリは失敗します。
キー サーバとグループ メンバーの同一のセットが複数の GET VPN に参加している	Security Manager では、トポロジのうち 1 つだけが検出されます。
User Group ポリシーで、IP アドレスではなくホスト名を使用してバックアップ サーバが設定されている	VPN ポリシー検出は失敗し、次のエラーが表示されます。 Policy Discovery Failed: com.cisco.nm.vms.discovery.DiscoveryException: Internal Error 正常に検出を行うには、ホスト名ではなく IP アドレスを使用して、デバイスの User Group ポリシーのバックアップ サーバを再設定する必要があります。

関連項目

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ（1406 ページ）
- VPN ディスカバリの前提条件 （1408 ページ）
- サイト間 VPN の検出 （1411 ページ）
- サイト間 VPN の再検出 （1415 ページ）

サイト間 VPN の検出

ここでは、すでにネットワークで稼働しているが、Security Manager には定義されていないサイト間 VPN を検出する方法について説明します。

関連項目

- サイト間 VPN の検出 （1411 ページ）
- ポリシーの検出 （223 ページ）

- VPN ディスカバリでサポートされる、およびサポートされないテクノロジーとトポロジ（1406 ページ）
- VPN ディスカバリの前提条件 （1408 ページ）
- VPN ディスカバリ ルール （1408 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）

ステップ 1 デバイスビューで、**[ポリシー（Policy）] > [VPNポリシーの検出（Discover VPN Polices）]** を選択して、[VPNポリシーの検出（Discover VPN Polices）] ウィザードの [名前とテクノロジー（Name and Technology）] ページを開きます。

ステップ 2 次の情報を指定します。

- [VPN名（VPN Name）]：検出する VPN の名前です。

エクストラネット VPN を検出する場合は名前を指定できません。代わりに、Security Manager がデバイス上に定義されているすべてのエクストラネットを検出し、各エクストラネットに対して、VPN 名はローカル IP アドレスとリモート IP アドレスがハイフンでつながれたものになります。たとえば、ローカルアドレスが 10.100.10.1、リモートアドレスが 10.100.11.1 である場合、エクストラネット VPN の名前は **10.100.10.1-10.100.11.1** と指定されます。

- [説明（Description）]：（任意）VPN の説明。エクストラネット VPN 検出に説明を追加することはできません。
- [トポロジ（Topology）]：検出する VPN のタイプ（[ハブアンドスポーク（Hub and Spoke）]、[ポイントツーポイント（Point to Point）]、[フルメッシュ（Full Mesh）]、または [エクストラネット（Extranet）]）です。
- [IPsecテクノロジー（IPsec Technology）]：VPN に割り当てられている IPsec テクノロジー（通常の IPsec、IPsec/GRE、GRE ダイナミック IP（サブテクノロジー）、DMVPN、Easy VPN、GET VPN、または通常の IPSEC VTI）です。選択するトポロジに応じて、このリストで利用可能な内容が変わります。

IPsec/GRE を選択した場合は、[標準（Standard）]（IPsec/GRE 用）または [ダイナミックIPを使用したスポーク（Spokes with Dynamic IP）]（GRE ダイナミック IP の設定用）のいずれかのタイプも指定する必要があります。

（注） ハブアンドスポークトポロジ、およびポイントツーポイントトポロジに適用可能なトンネルベースのルーティングには、通常の IPSEC VTI を選択できます。

- [検出元（Discover From）]：VPN は、ネットワークから直接検出することも、設定アーカイブから再検出することもできます。
  - [Network]：Security Manager は、すべてのライブ デバイスに接続してデバイス設定を取得します。エクストラネット VPN 検出の場合、Security Manager はユーザが指定する単一の管理対象デバイスに接続します。

- [Config Archive]：ライブ デバイスではなく設定ファイルに展開する場合は、Configuration Archive からの検出を推奨します。[Configuration Archive] 内のデバイス設定の最新バージョンがすべてのデバイスに使用されます。

ステップ 3 [次へ（Next）] をクリックして、[VPNポリシーの検出（Discover VPN Policies）] ウィザードの [デバイス選択（Device Selection）] ページを開きます。

ステップ 4 VPN に参加しているデバイス、およびそれらのデバイスの VPN 内でのトポロジタイプに応じたロール（ハブ、スポーク、ピア 1、ピア 2、ローカル デバイス、キー サーバ、グループ メンバー、または単に完全メッシュ VPN で選択されるデバイス）を選択します。Easy VPN トポロジの場合は、サーバがハブ、クライアントがスポークになります。

ハブアンドスポーク VPN に 2 つ以上の IPsec ターミネータがある場合は、上向きおよび下向き矢印ボタンを使用して、プライマリ ハブがリストの先頭にくるようにします。IPsec ターミネータが 1 つだけの場合は、同じ IPsec ターミネータにいくつのハブが接続されているかに関係なく、1 つのハブをプライマリ ハブとして指定できません。

VPN のデバイスの選択の詳細については、VPN トポロジのデバイスの選択 （1422 ページ）を参照してください。

ステップ 5 [終了（Finish）] をクリックしてウィザードを閉じ、検出プロセスを開始します。[Discovery Status] ウィンドウが開き、検出のステータスが表示されます。また、各デバイスの検出が成功したか、または失敗したかが示されます（ポリシー検出タスクのステータスの表示 （237 ページ）を参照）。問題の原因を示すためにエラーまたは警告メッセージが提供されます。問題の原因は、VPN に固有またはデバイスに固有の可能性があります。

エクストラネット検出の場合を除き、検出プロセスが正常に完了し、[Discovery Status] ダイアログボックスを閉じると、[Site-to-Site VPN Manager] ウィンドウが開き、検出された VPN の概要情報が表示されます。エクストラネット検出の場合、検出されたエクストラネット VPN のリストを参照するには、Site-to-Site VPN Manager を手動で開くか、またはデバイス ビューで Site-to-Site VPN ポリシーを選択する必要があります。

ステップ 6 VPN ポリシーが必要な内容となっていることを確認します。必要に応じて、ポリシーを編集します。

ヒント エクストラネット VPN を検出する場合、選択されたデバイスに定義されているすべてのエクストラネット VPN が検出されます。Security Manager で管理しないエクストラネット VPN は削除してください。

検出された、複数のスポーク定義を持つ VPN の定義または修復

各スポークに異なる定義が含まれる VPN を検出した場合（たとえば Easy VPN スポークのクライアント モードが異なる場合）、Security Manager では検出中に定義が変更されて、すべてのスポークに対して統一された定義が作成されます。Security Manager では、VPN トポロジに 1 セットのスポーク定義だけを含むことができるため、このような動作になります。

元の定義を維持する場合、または異なる定義を持つスポークで構成された新しい VPN を作成する場合は、次のいずれかの方法を実行します。

- Security Manager に複数の VPN トポロジを定義し、各トポロジには、一致するスポーク定義を含むスポークを設定します。
- 特殊な定義を含むFlexConfigポリシーを定義して、次の手順で説明するように、この定義を必要とするスポークにポリシーを割り当てます。

関連項目

- 新しい共有ポリシーの作成 （278 ページ）
- FlexConfig ポリシー オブジェクトの作成 （465 ページ）
- ポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）
- サイト間 VPN ディスカバリ （1406 ページ）
- サイト間 VPN の検出 （1411 ページ）
- VPN ディスカバリ ルール （1408 ページ）

ステップ 1 ポリシー ビューで、共有 FlexConfig ポリシーを作成します。

a) **[表示（View）] > [ポリシービュー（Policy View）]** を選択します。
b) ポリシータイプセレクタで [FlexConfigs] を右クリックして、[新しいFlexConfigポリシー（New FlexConfigs Policy）] を選択します。
c) ポリシーの名前を入力し、[OK] をクリックします。

ステップ 2 FlexConfig オブジェクトを作成および選択して、FlexConfig ポリシーを定義します。

a) ポリシービューの作業領域にある [詳細（Details）] タブで [追加（Add）] ボタンをクリックします。
b) FlexConfigs セレクタで、ウィンドウの左下隅にある [作成（Create）] ボタンをクリックして、 [Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を開きます。
c) 必要なクライアント定義を含む追加の FlexConfig オブジェクトを定義します。たとえば、Easy VPN スポークでクライアント モードを定義するには、次のコマンドを入力します。

```
crypto ipsec client ezvpn CSM_EASY_VPN_CLIENT_1
mode client
exit
```

d) FlexConfigオブジェクトを作成したあと、セレクタを使用してこのオブジェクトをFlexConfigポリシーに追加します。

ステップ 3 ポリシー ビューの作業領域にある [割り当て（Assignments）] タブを使用して、このポリシーを割り当てるスポークを選択し、[保存（Save）] をクリックします。

ステップ 4 ポリシーを展開します。

サイト間 VPN の再検出

ポリシーの変更をアプリケーションで再作成する必要がないように、すでに Security Manager で管理されている既存の VPN トポロジの設定を再検出できます。

Security Manager が VPN 設定を変換および検出する場合と同じルールが再検出にも適用されます。ただし、再検出は、VPN トポロジに参加するデバイスに対してだけ実行できます。また、IPsec テクノロジーやトポロジ タイプは変更できません。VPN インターフェイスや保護対象ネットワークなどのデバイス固有のポリシー、およびハブに設定される任意のハイ アベイラビリティ（HA）ポリシーの設定だけを再検出できます。IKE プロポーザルや PKI 登録などの VPN グローバル ポリシーは再検出できません。さらに、次のトポロジは再検出できません。

- ダイナミック VTI を使用する Easy VPN トポロジ
- エクストラネット VPN

ここでは、すでに Security Manager に存在するサイト間 VPN トポロジの設定を再検出する方法について説明します。

関連項目

- サイト間 VPN の検出 （1411 ページ）
- ポリシーの検出 （223 ページ）
- VPN ディスカバリの前提条件 （1408 ページ）
- VPN ディスカバリ ルール （1408 ページ）
- 各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）
- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）

ステップ 1 [Site-to-Site VPN Manager] ウィンドウで、設定を再検出する VPN トポロジを右クリックして、[ピアの再検出（Rediscover Peers）] を選択します。これにより、Rediscover VPN Policies ウィザードの [Name and Technology] ページが開きます。

このページには、トポロジのタイプ、および VPN で使用される IPsec テクノロジーが表示されますが、これらは変更できません。

ステップ 2 次の情報を指定します。

- [VPN検出名（VPN Discovery Name）]：VPN 再検出ジョブの名前です。
- [説明（Description）]：（任意）VPN の説明。
- [検出元（Discover From）]：VPN は、ネットワークから直接再検出することも、設定アーカイブから再検出することもできます。
  - [Network]：Security Manager は、すべてのライブ デバイスに接続してデバイス設定を取得します。

- [Config Archive]：ライブ デバイスではなく設定ファイルに展開する場合は、Configuration Archive からの再検出を推奨します。[Configuration Archive] 内のデバイス設定の最新バージョンがすべてのデバイスに使用されます。

ステップ 3 [次へ（Next）] をクリックして、[VPNポリシーの再検出（Rediscover VPN Policies）] ウィザードの [デバイス選択（Device Selection）] ページを開きます。

ステップ 4 ピア レベルのポリシーを再検出する必要があるデバイス、およびそれらのデバイスの VPN 内でのトポロジ タイプに応じたロール（ハブ、スポーク、ピア 1、ピア 2、キー サーバ、グループ メンバー、または単に完全メッシュ VPN で選択されるデバイス）を選択します。Easy VPN トポロジの場合は、サーバがハブ、クライアントがスポークになります。

ハブアンドスポーク VPN に 2 つ以上の IPsec ターミネータがある場合は、上向きおよび下向き矢印ボタンを使用して、プライマリ ハブがリストの先頭にくるようにします。IPsec ターミネータが 1 つだけの場合は、同じ IPsec ターミネータにいくつのハブが接続されているかに関係なく、1 つのハブをプライマリ ハブとして指定できません。

VPN のデバイスの選択の詳細については、VPN トポロジのデバイスの選択 （1422 ページ）を参照してください。

ステップ 5 [終了（Finish）] をクリックしてウィザードを閉じ、再検出プロセスを開始します。[Discovery Status] ウィンドウが開き、再検出のステータスが表示されます。また、各デバイスの再検出が成功したか、または失敗したかが示されます（ポリシー検出タスクのステータスの表示 （237 ページ）を参照）。問題の原因を示すためにエラーまたは警告メッセージが提供されます。問題の原因は、VPN に固有またはデバイスに固有の可能性があります。

再検出プロセスが正常に完了し、[Discovery Status] ダイアログボックスを閉じると、[Site-to-Site VPN Manager] ウィンドウが開き、再検出された VPN の概要情報が表示されます。

VPN トポロジの作成または編集

Security Manager では、サイト間 VPN を作成するための 3 つの基本的なトポロジ タイプがサポートされています。Create VPN ウィザードを使用して、複数のデバイス タイプにまたがるハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、または完全メッシュ VPN トポロジを作成できます。これらのトポロジの詳細については、VPN トポロジについて （1380 ページ）を参照してください。

ヒント エクストラネット ポイントツーポイント VPN を作成する場合は、このトピックではなく、エクストラネット VPN の作成または編集 （1469 ページ）を参照してください。

VPN トポロジを作成する場合は、サイト間 VPN を構成するデバイスおよびネットワークを指定します。デバイス、デバイスのロール（ハブ、スポーク、ピア、キー サーバ、グループ メンバーなど）、VPN トンネルの送信元エンドポイントおよび宛先エンドポイントとなる VPN インターフェイス、トンネルによって保護される保護対象ネットワークを定義します。VPN ト

ポロジを作成する場合は、トポロジに対して、定義済みのポリシーのセットが関連付けられた IPsec テクノロジー（通常の IPsec、IPsec/GRE、GRE ダイナミック IP、DMVPN、大規模 DMVPN、Easy VPN、GET VPN など）を割り当てます。サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （1385 ページ）を参照してください。

（注） Create VPN ウィザードを完了すると、Security Manager によって必須ポリシーに対してデフォルトが指定されるため、すぐにトポロジを展開可能になります。ただし、Security Manager のデフォルトを使用する場合は、ご使用のネットワークでその設定が適切に動作することを確認する必要があります。詳細については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。

VPN トポロジを編集する場合、[Edit VPN] ダイアログボックスには（[VPN defaults] ページを除いて）Create VPN ウィザードと同じページが含まれていますが、ウィザード形式ではなく、タブ形式でページがレイアウトされています。GET VPN トポロジだけは例外であり、トポロジの名前と説明だけを編集できます（トポロジの属性を変更するには、GET VPN ポリシーを編集する必要があります。GET VPN の設定 （1634 ページ）を参照してください）。ダイアログボックスの任意のタブで [OK] をクリックすると、すべてのタブの定義が保存されます。すべてのトポロジにおいて、当初 [VPN defaults] ページに表示された必須ポリシーおよびオプションのポリシーを直接編集する必要があります。

VPN トポロジを編集することによって、トポロジのデバイス構造の変更（デバイスの追加または削除）、デバイスに定義された VPN インターフェイスおよび保護対象ネットワークの変更、または VPN に割り当てられているポリシーの変更を行うことができます。たとえば、組織において新規サイトを頻繁にオープンする場合、既存のハブアンドスポーク VPN にスポークを追加して、新しいスポークに VPN のすべてのポリシーを適用する必要があります。また、1 つのハブだけを持つ VPN にセカンダリ ハブを追加して、耐障害性を高めることもできます。VPN トポロジの編集時に、トポロジに割り当てられたポリシーを変更する必要がある場合もあります。たとえば、IKE アルゴリズムをより安全なアルゴリズムに変更したり、VPN の DES 暗号化アルゴリズムを変更してより安全にしたりします。

ヒント トポロジを作成したあとは、VPN で使用されているテクノロジーを変更することはできません。テクノロジーを変更する場合は、古い VPN を削除してから、必要なテクノロジーを使用する新しい VPN を作成します。

Create VPN ウィザードを開始する、または既存の VPN トポロジを編集するには、次の手順を実行します。

- Create VPN ウィザードを開くには、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）または [サイト間VPNポリシー（Site-to-Site VPN Policy）] ページ（デバイスビュー）で、[新規VPNトポロジの作成（Create VPN Topology）]（+）ボタンをクリックして、作成する VPN トポロジのタイプを表示されるオプション（[ハブアンドスポーク（Hub and Spoke）]、[ポイントツーポイント（Point to Point）]、または [フルメッシュ（Full Mesh）]）から選択します。[Back] ボタンと [Next] ボタンを使用してページを移動します。終了したら、[Finish] をクリックして、トポロジを作成します。

- [VPNの編集（Edit VPN）] ダイアログボックスを開くには、[Site-to-Site VPN Manager] ウィンドウまたは[サイト間VPNポリシー（Site-to-Site VPN Policy）]ページ（デバイスビュー）で VPN トポロジを選択し、[PNトポロジの編集（Edit VPN Topology）]（鉛筆）ボタンをクリックします。

表示されるページまたはタブ、およびその順序は、作成する VPN トポロジのタイプに応じて異なります。それらについて、次の表に示します。

表 *323 : Create VPN/Edit VPN* ウィザードのページ

ページ	ハブアンドスポーク VPN	ポイントツーポイント VPN	完全メッシュ VPN
[Name and Technology] ページ。 VPN トポロジの名前および IPsec テクノロジーの定義 （1420 ページ）を参照してください。	ステップ 1	ステップ 1	ステップ 1
[Device Selection] ページ。 VPN トポロジのデバイスの選択 （1422 ページ）を参照してください。	ステップ 2	ステップ 2	ステップ 2
[Endpoints] ページ。 エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。 このページから、いくつかの高度な設定を作成することもできます。詳細については、表のあとにある説明を参照してください。	ステップ 3	ステップ 3	手順 3（通常の IPsec、IPsec GRE だけ）
[High Availability] ページ。 VPN トポロジにおけるハイ アベイラビリティの設定 （1450 ページ）を参照してください	ステップ 4：	—	—
[GET VPN Group Encryption Policy] ページ。 GET VPN グループ暗号化の定義 （1453 ページ）を参照してください。	—	—	手順 3（GET VPN だけ）
[GET VPN Peers] ページ。 GET VPN ピアの定義 （1461 ページ）を参照してください。	—	—	手順 4（GET VPN だけ）

ページ	ハブアンドスポーク VPN	ポイントツーポイント VPN	完全メッシュ VPN
[VPN Defaults] ページ。 新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て （1463 ページ）を参照してください。	ステップ 5	ステップ 4	手順 4（GET VPN では手順 5）
[Synchronize Keys] ダイアログボックス。GET VPN で Create VPN ウィザードを完了するときに、キーを同期するかどうかを尋ねられます。[はい（Yes）] をクリックすると、プロセスが開始されます。 RSA キーの生成と同期 （1636 ページ）を参照してください。	—	—	手順 6（GET VPN だけ）

VPN トポロジの作成中または作成後、エンドポイント編集時に、次の高度な設定を作成することもできます。

- ハブアンドスポーク トポロジでの、ハブにおける VRF 対応 IPsec（VRF 対応 IPsec の設定 （1445 ページ）を参照）
- ハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、または完全メッシュ VPN トポロジでの、Catalyst 6500/7600 における VPNSM または VPNSPA/VSPA（VPNSM または VPN SPA/VSPA エンドポイントの設定 （1436 ページ）を参照）
- ハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、または完全メッシュ VPN トポロジでの、VPN サービス モジュールまたは VPN SPA が設定された Catalyst 6500/7600 デバイスにおけるファイアウォール サービス モジュール（VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 （1443 ページ）を参照）

（注） マップ ビューでは、VPN トポロジをそのすべての要素とともに視覚的に表現できます。詳細については、マップ ビューにおける VPN トポロジの作成 （2075 ページ）を参照してください。

関連項目

- デバイス ビューにおける VPN トポロジの設定 （1405 ページ）
- IPsec テクノロジーおよびポリシーについて （1384 ページ）
- ウィザードの使用 （63 ページ）

VPN トポロジの名前および IPsec テクノロジーの定義

（注） このトピックは、エクストラネット VPN には適用されません。エクストラネット VPN の名前の設定については、エクストラネット VPN の作成または編集 （1469 ページ）を参照してください。

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [Name and Technology] ページ（またはタブ）を使用して、VPN トポロジの名前と説明を定義します。新しいトポロジを作成するときには、トポロジに割り当てる IPsec テクノロジーを選択する必要があります。ただし、既存のトポロジを編集するときにテクノロジーを変更することはできません。

Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開く方法については、VPN トポロジの作成または編集 （1416 ページ）を参照してください。

（注） 既存の VPN を編集する場合、割り当てられている IPsec テクノロジーおよびタイプが表示されますが、変更はできません。テクノロジーまたはタイプを変更するには、トポロジを削除してから新しいトポロジを作成する必要があります。

次の表に、名前およびテクノロジーを定義する場合に設定可能なオプションを示します。

表 *324 : [Name and Technology]* ページ

要素	説明
名前	VPN トポロジを識別する一意の名前です。
説明	VPN トポロジについての情報です。
IPsec Technology	VPN トポロジで使用される IPsec テクノロジーです。 • 通常の IPsec • IPsec/GRE • DMVPN（ハブアンドスポーク VPN だけ） • Easy VPN（ハブアンドスポーク VPN だけ） • GET VPN（完全メッシュ VPN だけ） • 通常の IPSec VTI

要素	説明
タイプ（Type）	選択された IPsec テクノロジーが IPsec/GRE またはハブアンドスポークトポロジにおける DMVPN の場合、テクノロジータイプフィールドが表示されます。 • [IPsec/GRE]：[標準（Standard）]（IPsec/GRE）または [ダイナミック IP を使用したスポーク（Spokes with Dynamic IP）]（GRE ダイナミック IP）を選択します。詳細については、動的にアドレス指定されるスポークの GRE 設定について （1580 ページ）を参照してください。 • [DMVPN]：[標準（Standard）]（通常の DMVPN）または [IPsec ターミネータを使用した大規模型（Large Scale with IPsec Terminator）]（大規模 DMVPN）を選択します。詳細については、大規模 DMVPN の設定 （1595 ページ）を参照してください。
IKE バージョン	IKE ネゴシエーションで許可するインターネット キー エクスチェンジ（IKE）バージョン。 通常の IPsec VTI トポロジを設定する場合、バージョン 1（[IKEv1]）またはバージョン 2（[IKEv2]）を許可できます。 通常の IPsec トポロジを設定する場合、バージョン 1（[IKEv1]）、バージョン 2（[IKEv2]）、または [IKEv1 と IKEv2（IKEv1 & IKEv2）] の両方を許可できます。 [IKEv1 と IKEv2（IKEv1 & IKEv2）] を選択すると、IKEv2 をサポートしないデバイスでは自動的に IKEv1 が使用されます。ただし、IKEv2 のみを選択する場合は、IKEv2 をサポートしていないデバイスを選択しないようにする必要があります（ウィザードは無効な選択を阻止しません）。間違ったオプションを選択した場合、VPN の作成後に IKE Proposal ポリシーと IPsec Proposal ポリシーを編集してサポートされる IKE バージョンを変更できます。 IKE について、および各バージョンの相違点については、IKE および IPsec 設定の概要 （1478 ページ）を参照してください。IKEv2 をサポートするデバイスについては、各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）を参照してください。 **ヒント** Create VPN ウィザード使用時に IKEv2 を許可するオプションを選択すると、ウィザードは有効なトポロジを作成しません。ウィザードの完了後、IKEv2 Authentication ポリシーを手動で設定して、設定を完了する必要があります。

関連項目

- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）

VPN トポロジのデバイスの選択

（注） このトピックは、エクストラネット VPN には適用されません。エクストラネット VPN でのデバイスの選択については、エクストラネット VPN の作成または編集 （1469 ページ）を参照してください。

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [Device Selection] ページ（またはタブ）を使用して、VPN トポロジに組み込むデバイスを選択します。このページの内容は、作成または編集する VPN トポロジがハブアンドスポーク、大規模 DMVPN、ポイントツーポイント、または完全メッシュのいずれであるかに応じて異なります。また、このページを使用して GET VPN のメンバーシップを編集することはできません（既存の GET VPN について作業する場合は、GET VPN グループ メンバーの設定 （1645 ページ）および GET VPN キー サーバの設定 （1642 ページ）を参照してください）。

Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開く方法については、VPN トポロジの作成または編集 （1416 ページ）を参照してください。

ほとんどの場合、[使用可能なデバイス（Available Devices）] リストには、選択した VPN トポロジタイプで使用できるデバイス、IPsec テクノロジータイプをサポートするデバイス、および表示する権限があるデバイスだけが表示されます。また、利用可能なデバイスは、選択した IPsec テクノロジーによっても異なります。たとえば、IPsec テクノロジーが IPsec/GRE、GRE ダイナミック IP、または DMVPN の場合、PIX ファイアウォールと ASA デバイスは表示されません。リストはトポロジでサポートする IKE バージョンを考慮するようには調整されません。ただし、通常の IPsec VTI トポロジ設定の場合、IKEv1 が選択されていると、ASA 9.7.1 以降のシングル コンテキスト デバイスが表示されます。IKEv2 の場合は、ASA 9.8.1 以降のシングル コンテキスト デバイスが表示されます。詳細については、各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）に説明されている、サポートされるプラットフォームを参照してください。

ヒント デバイスを選択する場合、デバイス グループを選択して、そのグループ内のすべての選択可能なデバイスを選択することができます。

次のリストに、トポロジのタイプに応じてデバイスを追加または削除する方法を示します。

- **通常の IPsec または IPsec/GRE テクノロジーを使用する完全メッシュ VPN トポロジでデバイスを選択するには、**[使用可能なデバイス（Available Devices）] リストでデバイスを選択して、[>>] をクリックします。
- **GET VPN テクノロジーを使用する完全メッシュ VPN トポロジでデバイスを選択するには、次の手順を実行します。**
  - キーサーバーとして定義するデバイスを選択して、[キーサーバー（Key Servers）] フィールドの横にある [>>] をクリックします。

複数のキーサーバーがある場合は、**上向き**および**下向き**の矢印ボタンを使用して、プライマリ キーサーバーを先頭に配置します。グループ メンバーは、リストの最初のキー サーバに登録されます。最初のキー サーバに到達できない場合は、2 番め以降のキー サーバに順番に登録が試みられます。

- グループメンバーとして定義するデバイスを選択して、[グループメンバー（Group Members）] フィールドの横にある [>>] をクリックします。
- **ハブアンドスポーク VPN トポロジでデバイスを選択するには、次の手順を実行します。**
  - ハブとして定義するデバイス（または Easy VPN 設定でサーバーとして定義するデバイス）を選択して、[ハブ（Hubs）] リストの横にある [>>] をクリックします。

複数のハブがある場合は、ハブ リストをプライオリティ順に並べて、プライマリ ハブを先頭に配置します。順序を変更するには、ハブを選択し、**上向き**および**下向き**の矢印ボタンをクリックして、デバイスを適切な順序に並べ替えます。

（注） プライマリ ハブは、2 つ以上の IPsec ターミネータがある場合にだけ選択する必要があります。IPsec ターミネータが 1 つだけの場合は、同じ IPsec ターミネータにいくつのハブが接続されているかに関係なく、1 つのハブをプライマリ ハブとして指定できません。

- スポークとして定義するデバイス（または Easy VPN 設定でクライアントとして定義するデバイス）を選択して、[スポーク（Spokes）] リストの横にある [>>] をクリックします。
- **IPsec ターミネータを使用した大規模 DMVPN** トポロジを設定する場合は、大規模 DMVPN 設定で **IPsec ターミネータ**となる Catalyst 6500/7600 デバイスを選択する必要もあります。2 つ以上の IPsec ターミネータを選択する場合は、**上向き**および**下向き**の矢印ボタンを使用して、プライオリティ順に並べ替えます。詳細については、大規模 DMVPN の設定（1595 ページ）を参照してください。
- **ポイントツーポイント VPN トポロジでデバイスを選択するには、次の手順を実行します。**
  - [デバイス（Devices）] リストから、**ピア 1** とするデバイスを選択して、[>>] をクリックします。
  - **ピア 2** とする別のデバイスを選択して、[>>] をクリックします。
- **（任意のトポロジまたはテクノロジーの組み合わせにおいて）デバイスを削除するには、**選択されたデバイスのいずれかのリストでデバイスを選択し、[<<] をクリックして、そのデバイスを [使用可能なデバイス（Available Devices）] リストに戻します。

既存の VPN トポロジを編集している場合は、VPN トポロジからデバイスを削除することはできますが、その結果として無効な VPN 設定となる場合には、変更内容を保存できません。デバイスを削除する場合、次の点に注意する必要があります。

- デバイスがハブアンドスポーク VPN トポロジにおける唯一のハブである場合、そのデバイスは削除できません。他のハブに置き換える必要があります。

- デバイスがポイントツーポイント VPN トポロジにおける 2 つのデバイスのいずれかである場合、そのデバイスは削除できません。他のハブに置き換える必要があります。
- 複数のハブ デバイスがある VPN トポロジでは、ハブを削除すると、そのハブを使用するトンネルが削除されます。
- VPN トポロジのすべてのスポークではなく一部のスポークが削除されると、ハブ側の crypto ステートメントが変更されて、削除内容が反映されます。
- GET VPN には、少なくとも 1 つのキー サーバと 1 つのグループ メンバーが必要です。

関連項目

- 管理対象外デバイスまたは非シスコ デバイスの VPN への組み込み （1394 ページ）

エンドポイントおよび保護対象ネットワークの定義

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [Endpoints] ページを使用して、VPN トポロジ内のデバイスを表示し、それらの VPN 特性および機能を定義または編集します。主に、VPN トポロジ内のデバイスの外部または内部 VPN インターフェイス、および保護対象ネットワークを定義します。VPN インターフェイスは、データを暗号化するインターフェイスです。保護対象ネットワークは、暗号化されるネットワークです。

[Endpoints] ページは、次のいずれかの方法で開きます。

- Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開きます。手順については、 VPN トポロジの作成または編集 （1416 ページ）を参照してください。
- Site-to-Site VPN Manager で目的の VPN トポロジを選択して（GET VPN トポロジを除く）、[ピア（Peers）] ポリシーを選択します。

ヒント：

- この設定は、GET VPN 以外のすべての IPsec テクノロジー タイプに適用されます。VPN 作成時に GET VPN エンドポイントを設定する方法については、 GET VPN ピアの定義 （1461 ページ）を参照してください。既存の GET VPN では、Key Servers ポリシーおよび Group Members ポリシーを使用してエンドポイントを設定します。 GET VPN キー サーバの設定 （1642 ページ）およびGET VPN グループ メンバーの設定 （1645 ページ）を参照してください。
- このページに表示されるデバイスは、[Device Selection] ページで選択します（VPN トポロジのデバイスの選択 （1422 ページ）を参照）。このリストは、Peers ポリシーの編集時にだけ変更できます。この場合、デバイスを選択し、[削除（Delete）]（ゴミ箱）ボタンをクリックして、デバイスを削除します。デバイスを追加するには、VPN トポロジ自体を編集する必要があります。
- Peers ポリシーを使用してエクストラネット VPN のエンドポイントを編集することはできますが、代わりに、[Edit Extranet VPN] ダイアログボックスで VPN トポロジを編集するこ

とによりエンドポイントを編集してください。Create Extranet VPN ウィザードには [Endpoints] ページは表示されません。

テーブルには、VPN における各デバイスのロール（ハブ、スポーク、ピア、または IPsec ターミネータ）、デバイス名、および VPN インターフェイスと保護対象ネットワークが表示されます。当初、VPN インターフェイスと保護対象ネットワークは、外部および内部インターフェイスに対して、Security Manager の管理設定で定義されたデフォルトのインターフェイス ロールに設定されています（[VPN Policy Defaults] ページ （743 ページ）を参照）。エンドポイント設定には、このテーブルに表示されない設定が含まれている場合もありますが、必須の設定は VPN インターフェイスと保護対象ネットワークだけです。

- デバイスのエンドポイント設定を変更するには、デバイスを選択して、テーブルの下にある [行の編集（Edit Row）] ボタンをクリックします。一度に複数のデバイスを選択して編集することもできますが、その場合、それらのデバイスのロールは同じである必要があります。複数のデバイスを選択する場合は、Catalyst 6500/7600 デバイスまたは VPN サービス モジュールを含めることはできません。エンドポイントの編集は [Edit Endpoints] ダイアログボックスで実行しますが、その内容は選択したデバイス タイプおよび IPsec テクノロジーに応じて異なります。

[Edit Endpoints] ダイアログボックスで設定できるオプションの詳細については、次の項を参照してください。

- - [VPNインターフェイス（VPN Interface）] タブ：VPN インターフェイスを設定し、その他の必要なインターフェイス設定を行います（VPN インターフェイス エンドポイントの設定 （1427 ページ）を参照）。ダイヤルバックアップも設定できる場合があります（ダイヤルバックアップの詳細については、ダイヤルバックアップの設定 （1432 ページ）を参照してください）。

Catalyst 6500/7600 デバイスでは、[VPN Interface] タブに、デバイス（大規模 DMVPN における IPsec ターミネータの場合もあります）に VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA ブレードを設定できる設定が表示されます。これについては、VPNSM または VPN SPA/VSPA エンドポイントの設定 （1436 ページ）を参照してください。

トンネルベースの VPN を設定する場合は、[VPNインターフェイス（VPN Interface）] タブのみが表示されます。[選択（Select）] ボタンを使用して、トンネルインターフェイスを選択します。

Easy VPN は、ASA の起動時に最高および最低のセキュリティレベルのインターフェイスを判別することによって機能します。VPN クライアントは、同じ最高セキュリティレベルの複数のインターフェイスを拒否します。BVI で、Easy VPN によって同じ最高セキュリティ レベルの複数のインターフェイスがあることが特定されると、VPN クライアントが無効になります。この問題を解決するために、ASA 9.9(2) 以降のすべての ASA 5506、5508、および 5512 [x/h/w] デバイスに vpnclient secure interface CLI が導入されました。そのため、Cisco Security Manager で CLI をサポートするために、バージョン 4.17 以降、新しいコンポーネント「VPN クライアント インターフェイス」がタイプ（Easy VPN）のハブアンドスポークトポロジに導入されました。

- [エクストラネットデバイスの詳細（Extranet Device Details）]：エクストラネット VPN 内のリモート（管理対象外）デバイスのエンドポイント設定値を設定します。このタブは、Peers ポリシーの場合にのみ表示されます。このタブで情報を編集する代わりに、VPN トポロジを編集して設定を変更する方法を推奨します。詳細については、エクストラネット VPN の作成または編集 （1469 ページ）を参照してください。
- [ハブインターフェイス（Hub Interface）] タブ：選択されたデバイスが大規模 DMVPN におけるハブである場合、IPsec ターミネータに接続されたインターフェイスを指定します。 大規模 DMVPN の設定 （1595 ページ）を参照してください。
- [保護対象ネットワーク（Protected Networks）] タブ：暗号化されるネットワークを定義します（エンドポイントの保護対象ネットワークの特定 （1441 ページ）を参照）。保護対象ネットワークは、インターフェイスロール、ネットワーク/ホストオブジェクト、または通常の IPsec の場合は ACL ポリシーオブジェクトです。
- [FWSM] タブ：Firewall Services Module（FWSM）と、Catalyst 6500/7600 デバイスにすでに設定されている IPsec VPN サービスモジュール（VPNSM）または VPNSPA/VSPA との間を接続できるようにするための設定を定義します。この設定は、ハブがこれらのモジュールがインストールされた Catalyst 6500/7600 デバイスであるハブアンドスポーク トポロジでだけ可能です。詳細については、 VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 （1443 ページ）を参照してください。
- [VRF対応IPsec（VRF Aware IPsec）] タブ：ハブアンドスポーク VPN トポロジにおいて、ハブ（IPsec アグリゲータ）に VRF-Aware IPsec ポリシーを設定します。詳細については、 VRF 対応 IPsec の設定 （1445 ページ）および VRF 対応 IPsec について （1398 ページ）を参照してください。
- [クリプトマップ（Crypto Map）] タブ：各ピアのクリプトマップ名とクリプト ACL 名を手動で設定します。これは、バージョン 4.7 以降の Security Manager でサポートされます。クリプトマップとクリプト ACL は、通常の IPSec テクノロジーでサポートされています。したがって、この設定は、通常の IPSec テクノロジーを使用するトポロジにのみ適用できます。詳細については、 クリプトマップの設定 （1448 ページ）を参照してください。

- 各デバイスのインターフェイスロールに関連付けられている実際のインターフェイスを表示するには、テーブルの下にある [表示（Show）] リストの [一致するインターフェイス（Matching Interfaces）] を選択します。一致するインターフェイスがない場合は、「一致なし（No Match）」と表示されます。デフォルトでは、インターフェイス ロール ポリシーオブジェクト名が表示されます。有効な VPN を作成するには、これらのロールがデバイスに定義されている実際のインターフェイスに一致する必要があります。

関連項目

- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

VPN インターフェイス エンドポイントの設定

[Edit Endpoints] ダイアログボックスの [VPN Interface] タブを使用して、[Endpoints] テーブルのデバイスに定義された VPN インターフェイスを編集します。ルータ デバイスのプライマリ VPN インターフェイスを定義する場合は、プライマリ ルート VPN インターフェイスの接続リンクが利用できなくなった場合にフォールバック リンクとして使用するバックアップ インターフェイスも設定できます。バックアップ インターフェイスは、ポイントツーポイント トポロジまたは完全メッシュ トポロジにある Cisco IOS セキュリティ ルータ、ハブアンドスポーク トポロジのスポークとなっている Cisco IOS セキュリティ ルータ、または Easy VPN トポロジのリモート クライアントとなっている Cisco IOS セキュリティ ルータで設定できます。詳細については、ダイヤル バックアップの設定 （1432 ページ）を参照してください。

ヒント

- デバイスが大規模 DMVPN のハブである場合、このタブは [ハブインターフェイス（Hub Interface）] と呼ばれます。[IPsecターミネータに接続されたハブインターフェイス（Hub Interface Toward the IPsec Terminator）] フィールドで、IPsec ターミネータに接続されているインターフェイスを指定します。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。詳細については、大規模 DMVPN の設定 （1595 ページ）を参照してください。
- デバイスが Catalyst 6500/7600 デバイスの場合、[VPN Interface] タブでは、デバイスの VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA ブレードを設定できます。Catalyst 6500/7600 デバイスの場合に [VPN Interface] タブに表示される要素の詳細については、VPNSM または VPN SPA/VSPA エンドポイントの設定 （1436 ページ）を参照してください。次の表では、デバイスが Catalyst 6500/7600 デバイスではない場合について示します。

ナビゲーション パス

[VPNの作成（Create VPN）] ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページ、あるいは [VPNピア（VPN Peers）] ポリシーでデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [VPNインターフェイス（VPN Interfaces）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義（1424 ページ）を参照してください。

フィールド リファレンス

表 *325 : [Edit Endpoints]* ダイアログボックスの *[VPN Interface]* タブ

要素	説明
Enable the VPN Interface Changes on All Selected Peers	[Endpoints] ページで編集用に複数のデバイスを選択した場合に使用可能です。 選択されている場合は、[VPN interface] タブで行った変更内容が、選択したすべてのデバイスに適用されます。
VPN Interface	選択したデバイスに定義された VPN インターフェイスです。インターフェイスを識別するインターフェイス ロール ポリシー オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか、新しいインターフェイス ロール オブジェクトを作成します。（インターフェイス ロール オブジェクトの作成 （383 ページ） を参照。） （注） デバイスでクリプトマップを手動で設定する場合は、ピアインターフェイスの名前ではなく IP アドレスを指定する必要があります。 デバイスが ASA 5505 バージョン 7.2(1) 以降である場合は、異なるセキュリティ レベルを持つ 2 つのインターフェイスを定義する必要があります。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください。
VPN クライアントインターフェイス	選択したデバイスに定義された VPN クライアント インターフェイスです。[選択（Select）] をクリックして、リストから選択します。Cisco Security Manager 4.17 から、Easy VPN のクライアント インターフェイスを指定できます。これは以下に適用されます。 • ASA 5506 デバイス以降 • BVI インターフェイスまたはその他の物理インターフェイス（BVI メンバーインターフェイス以外） • ハブ アンド スポーク トポロジのデバイス
VPN クライアントのセキュアインターフェイス	4.17 以降、Cisco Security Manager は ASA 9.9(2) の BVI に対する EzVPN 機能の対応をサポートします。このフィールドでは、保護されたインターフェースを定義できます。トンネル確立のために保護されたネットワークとして機能するインターフェースを選択します。この機能は、次の場合にのみ適用されます。 • EasyVPN トポロジ • スポークインターフェイス • ASA 9.9.2 デバイス以降

要素	説明
接続タイプ	選択したデバイスが ASA または PIX 7.0+ デバイスであり、かつ選択したテクノロジーが通常の IPsec の場合にだけ、ハブアンドスポーク VPN トポロジで使用できます。 SA ネゴシエーション中にハブまたはスポークが使用する接続のタイプを選択します。 • [応答のみ（Answer Only）]：ハブが、SA ネゴシエーションへの応答だけを行い、SA ネゴシエーションを開始しないように設定します。これは、ハブの場合のデフォルトです。 • [発信のみ（Originate Only）]：デバイスが、SA ネゴシエーションの開始だけを行い、SA ネゴシエーションには応答しないように設定します。これは、スポークの場合のデフォルトです。 • [双方向（Bidirectional）]：ハブまたはスポークが、SA ネゴシエーションの開始および SA ネゴシエーションへの応答の両方を行うように設定します。

要素	説明
Local Peer IPSec Termination	選択したテクノロジーが Easy VPN の場合は使用できません。 ローカル ルータの VPN インターフェイスの IP アドレスを指定します。次のいずれかのオプションを選択できます。 • [トンネル送信元のIPアドレス（Tunnel Source IP Address）]：トンネル送信元の IP アドレスを使用します。 • [VPNインターフェイスのIPアドレス（VPN Interface IP Address）]：選択した VPN インターフェイスに設定された IP アドレスを使用します。インターフェイス ロールに一致できるのは、1 つの VPN インターフェイスだけです。このオプションは、GRE Modes ポリシーで [各トンネルに一意のトンネル送信元を設定（Configure Unique Tunnel Source for each Tunnel）] を選択した場合にだけ使用できます。 （注） バージョン 4.9 以降、Security Manager では IPv6 アドレスを選択できます。この機能は、IPv6 アドレスを持つインターフェイスでサポートされており、ASA ソフトウェア バージョン 9.0 以降を実行しているデバイスに適用されます。また、IPv6 アドレスのオプションは、Regular IPSec テクノロジでのみ使用できます。 • [IPアドレス（IP Address）]：ローカルルータの VPN インターフェイスの IP アドレスを明示的に指定します。このオプションは、デバイスが NAT 境界の背後にあり、NAT IP アドレスを指定する場合に使用します。バージョン 4.9 以降、Security Manager では IPv6 アドレスを指定できます。 （注） VPN インターフェイスとしてトンネル ソースを選択した場合は、VPN インターフェイスに IP アドレスが動的に割り当てられている可能性があります。 • [別の既存のインターフェイスのIPアドレスをローカルアドレスとして使用（IP Address of Another Existing Interface to be Used as Local Address）]（IPsec テクノロジーが DMVPN の場合は使用不可）：任意のインターフェイスに設定された IP アドレスをローカルアドレスとして使用します（VPN インターフェイスにかぎりません）。提供されたフィールドにインターフェイスを入力します。 [選択（Select）] をクリックして、必要なインターフェイスを選択できます。すべての使用可能な定義済みのインターフェイス ロールが示されたダイアログボックスが表示されます。このダイアログボックスでは、インターフェイス ロール オブジェクトを作成できます。

要素	説明
トンネルの送信元	IPsec/GRE または DMVPN でだけ使用可能です。 **[GREモード（GRE Modes）] > [トンネルパラメータ（Tunnel Parameters）]** タブで、トンネルインターフェイスごとに一意のトンネルソースを使用する設定を有効にしている場合、[トンネルインターフェイスごとに一意のトンネルソースをオーバーライド（Override Unique Tunnel Source per Tunnel Interface）] チェックボックスが使用可能になります。このオプションを選択して、選択したデバイスに別のトンネル ソースを指定します。 スポーク側の GRE または DMVPN トンネルで使用するトンネル ソース アドレスを指定します。次のいずれかのオプションを選択できます。 • [VPNインターフェイス（VPN Interface）]：トンネルソースアドレスとして、VPN インターフェイスを使用します。 • [インターフェイス（Interface）]：任意のインターフェイスをトンネルソースアドレスとして使用します。VPN インターフェイスにかぎりません。インターフェイス名を入力します。または、[選択（Select）] をクリックして、インターフェイスを識別するインターフェイスロールを選択します（選択ダイアログボックスからロールを作成することもできます）。
Dial Backup Settings	
Enable Backup	選択したデバイスが、ポイントツーポイント トポロジまたは完全メッシュ トポロジにある IOS ルータ、ハブアンドスポーク トポロジのスポークとなっている IOS ルータ、または Easy VPN トポロジのリモート クライアントとなっている IOS ルータの場合に使用できます。 プライマリ ルート VPN インターフェイスの接続リンクが利用できなくなった場合にフォールバック リンクとして使用するバックアップ インターフェイスを設定するかどうかを指定します。 **ヒント** バックアップ インターフェイスを設定する前に、まずデバイスでダイヤラ インターフェイスを設定する必要があります。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）を参照してください。
ダイヤラ インターフェイス	ダイヤラ インターフェイスがアクティブになったときに、セカンダリ ルート トラフィックが送信される論理インターフェイスです。シリアルインターフェイス、非同期インターフェイス、または BRI インターフェイスを選択できます。 インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。

要素	説明
Primary Next Hop IP Address	選択されたテクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合にだけ使用できます。 プライマリ インターフェイスがアクティブな場合に接続する IP アドレスです。これは、ネクスト ホップ IP アドレスと呼ばれています。 ネクスト ホップ IP アドレスを指定しない場合、Security Manager は、VPN インターフェイス名を使用してスタティック ルートを設定します。VPN インターフェイスはポイントツーポイントである必要があります。それ以外の場合は、展開に失敗します。 [選択（Select）] をクリックして、必要な IP アドレスを選択できます。ネットワーク/ホスト セレクタが開き、そこで IP アドレスの割り当て元のネットワークを選択できます。
Tracking IP Address	プライマリ VPN インターフェイス接続からの接続を維持する必要がある宛先デバイスの IP アドレスです。Service Assurance Agent では、プライマリ ルートを経由してこのデバイスに対して ping を実行し、接続性を追跡します。このデバイスへの接続が失われた場合にバックアップ接続がトリガーされます。 IP アドレスを指定しない場合は、ハブアンドスポークまたは Easy VPN トポロジでプライマリ ハブ VPN インターフェイスが使用されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ピア VPN インターフェイスが使用されます。 [選択（Select）] をクリックして、必要な IP アドレスを選択できます。ネットワーク/ホスト セレクタが開き、そこで IP アドレスの割り当て元のネットワークを選択できます。
[Advanced] ボタン	選択したテクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合に使用できます。 [Dial Backup Settings] ダイアログボックス （1434 ページ）を使用して、追加のオプションの設定を行うには、このボタンをクリックします。

ダイヤル バックアップの設定

ダイヤルバックアップを使用すると、プライマリ リンクが利用できなくなった場合に備えて、直接のプライマリ接続に対するフォールバック リンクを提供できます。ダイヤル バックアップは、ポイントツーポイント、エクストラネット、または完全メッシュ VPN トポロジに参加している Cisco IOS セキュリティ ルータ、あるいはハブアンドスポーク トポロジのスポークとなっている Cisco IOS セキュリティ ルータで設定できます。Easy VPN トポロジにおいて IOS バージョン 12.3(14)T+ を実行するリモート クライアント ルータでも設定できます。

ダイヤル バックアップ機能は、次の 2 つのスタティック ルートが存在するという前提に基づいて実装されています。

- プライマリ ゲートウェイ経由の、最も高いプライオリティを持つプライマリ ルート

- セカンダリ ゲートウェイ経由の、低いプライオリティを持ち、プライマリ ゲートウェイがダウンしたときにだけルーティング テーブルに表示されるセカンダリ ルート

Security Manager によって、スポークに論理ダイヤラ インターフェイスが設定されます。このダイヤラインターフェイスは、物理的なバックアップインターフェイスに関連付けられます。プライマリ ルートがダウンすると、ダイヤラ インターフェイスがアクティブになり、トラフィックはこのバックアップ インターフェイス経由でセカンダリ ルートにリダイレクトされます。スポークとハブとの間のトラフィックが暗号化されるように、Security Manager によってダイヤラ インターフェイスに対してクリプト マップが適用されます。このクリプト マップは、VPN インターフェイス（プライマリ ルート インターフェイス）のクリプト マップと同一のものです。Easy VPN では、バックアップ設定は、ダイヤラ インターフェイスに追加されます。

IOS バージョンによっては、Response Time Reporter（RTR）または Service Level Agreement（SLA; サービス レベル契約）IOS テクノロジーを使用して、プライマリ ルートでのネットワークのパフォーマンス低下が検出されます。割り当てられている IPsec テクノロジーが DMVPN である場合は、Dialer Watch-List（DWL）が使用されます。

ISDN Basic Rate Interface（BRI; 基本インターフェイス）およびアナログ モデム インターフェイスを他のプライマリ インターフェイスに対するバックアップ インターフェイスとして設定できます。この場合、ISDN またはアナログ モデム接続は、プライマリ インターフェイスがダウンした場合に確立されます。プライマリ インターフェイスおよびその接続がダウンすると、ISDN またはアナログ モデム インターフェイスからすぐにダイヤルアウトが実行されて、ネットワーク サービスが停止しないように接続が確立されます。

はじめる前に

- Cisco IOS ルータでダイヤラ インターフェイスを設定します。このためには、物理 BRI および非同期インターフェイス間の関係、およびダイヤルバックアップを設定する場合に使用する仮想ダイヤラインターフェイスを定義する必要があります。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）を参照してください。
- プライマリ ルートが機能していることを確認します。
- エクストラネット VPN の場合、ローカル（管理対象）デバイスのみにダイヤルバックアップを設定できます。

ステップ 1 ほとんどの VPN トポロジの場合、サイト間 VPN の作成時または編集時にダイヤル バックアップを設定します。既存 VPN トポロジの Peers ポリシーを編集することもできます。エクストラネット VPN の場合、Peers ポリシーを介してのみダイヤル バックアップを設定できます。

次のいずれかを実行します。

- Create VPN ウィザードで、[Endpoints] ページに進みます（VPN トポロジの作成または編集 （1416 ページ）およびエンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照）。
- [VPN の編集（Edit VPN）] ダイアログボックスで、[エンドポイント（Endpoints）] タブをクリックします（VPN トポロジの作成または編集 （1416 ページ）およびエンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照）。

- エクストラネット VPN の場合、またはその他の VPN トポロジを編集する場合、[Peers] ポリシーを選択します。エンドポイント編集の一般情報については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。

ステップ 2 ダイヤルバックアップを設定するルータを選択して、[編集（Edit）]（鉛筆）ボタンをクリックします。同じダイヤラ設定を行うルータが複数ある場合は、それらを選択して、同時に編集できます。

これにより、[Edit Endpoints] ダイアログボックスが開きます。[VPN インターフェイス（VPN Interface）] タブが選択されていない場合は、このタブを選択します。

ステップ 3 [VPN Interface] タブで、ダイヤル バックアップに関する次のオプションを設定します。新しい VPN を作成している場合は、VPN インターフェイスなどの他の設定も行う必要があります。これらのオプションの詳細については、VPN インターフェイス エンドポイントの設定 （1427 ページ）を参照してください。

- [バックアップの有効化（Enable Backup）]：このオプションを選択します。
- [ダイヤラインターフェイス（Dialer Interface）]：論理ダイヤラインターフェイスがアクティブになったときに、セカンダリ ルート トラフィックが送信される物理インターフェイスを指定します。
- [プライマリネクストホップ IP アドレス（Primary Next Hop IP Address）]：選択した IPsec テクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合、ネクストホップ IP アドレスを入力します。ネクスト ホップ IP アドレスを入力しない場合、Security Manager は、インターフェイス名を使用してスタティック ルートを設定します。
- [追跡 IP アドレス（Tracking IP Address）]：プライマリ VPN インターフェイス接続からの接続を維持する必要がある宛先デバイスの IP アドレスを指定します。これは、接続性を追跡するために、プライマリ ルートを経由して ping が実行されるデバイスです。このデバイスへの接続が失われた場合にバックアップ接続がトリガーされます。

IP アドレスを指定しない場合は、ハブアンドスポークまたは Easy VPN トポロジでプライマリ ハブ VPN インターフェイスが使用されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ピア VPN インターフェイスが使用されます。

ステップ 4 選択した IPsec テクノロジーが通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN の場合は、[詳細設定（Advanced）] をクリックして、[ダイヤルバックアップ設定（Dial Backup Settings）] ダイアログボックスで追加の（任意の）設定を行います。これらの設定については、[Dial Backup Settings] ダイアログボックス （1434 ページ）で説明します。[OK] をクリックして変更を保存します。

ステップ 5 [エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [OK] をクリックします。

[Dial Backup Settings] ダイアログボックス

[Dial Backup Settings] ダイアログボックスを使用して、サイト間 VPN にダイヤル バックアップ ポリシーを設定するためのオプションの設定を定義します。これらの設定は、通常の IPsec、IPsec/GRE、GRE ダイナミック IP、または Easy VPN テクノロジーにおいて使用できます。

ダイヤル バックアップの必須の設定は、[Edit Endpoints] ダイアログボックスの [VPN Interface] タブで行います。VPN インターフェイス エンドポイントの設定 （1427 ページ）を参照してください。

（注） ダイヤラ インターフェイスを設定しないと、ダイヤル バックアップは正常に動作しません。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）を参照してください。

ナビゲーション パス

[ダイヤルバックアップ設定（Dial Backup Settings）] ダイアログボックスを開くには、ダイヤルバックアップを有効にして、[エンドポイントの編集（Edit Endpoints）] ダイアログボックスの [VPNインターフェイス（VPN Interface）] タブにある [詳細設定（Advanced）] をクリックします。[Edit Endpoints] ダイアログボックスを開く方法については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。

関連項目

- ダイヤル バックアップの設定 （1432 ページ）
- Easy VPN について （1599 ページ）

フィールド リファレンス

表 *326 : [Dial Backup Settings]* ダイアログボックス

要素	説明
Next Hop Forwarding Backup Next Hop IP Address	必要に応じて、ISDN BRI またはアナログ モデム バックアップ インターフェイスのネクスト ホップ IP アドレス（バックアップ インターフェイスがアクティブになったときに接続する IP アドレス）を入力します。IP アドレス、またはネットワーク/ホスト オブジェクトの名前を入力できます。または、[Select] をクリックして、IP アドレスを指定するネットワーク/オブジェクトを選択します。 ネクスト ホップ IP アドレスを入力しない場合、Security Manager は、インターフェイス名を使用してスタティック ルートを設定します。
Tracking Object Settings	
タイムアウト（Timeout）	Service Assurance Agent の動作において、宛先デバイスからの応答を受信するまで待機するミリ秒単位の時間です。デフォルトは 5000 ms です。
周波数（Frequency）	プライマリ ルートのパフォーマンスの低下を検出するために Response Time Reporter（RTR）を使用する頻度です。デフォルトは 60 秒ごとです。

要素	説明
[しきい値（Threshold）]	RTR 動作において、対応イベントを生成し、履歴情報を保存する、ミリ秒単位の上昇しきい値です。デフォルトは 5000 ms です。

VPNSM または VPN SPA/VSPA エンドポイントの設定

[Endpoints] テーブルで編集用に Catalyst 6500/7600 デバイスを選択した場合、[Edit Endpoints] ダイアログボックスの [VPN Interface] タブで、デバイスに Cisco VPN Services Module（VPNSM; VPN サービス モジュール）、Cisco VPN Shared Port Adapter（VPN SPA; VPN 共有ポート アダプタ）、および Cisco VPN Service Port Adapter（VSPA; VPN サービス ポート アダプタ）を設定できます。同時に複数の Catalyst 6500/7600 デバイスを選択できます。変更内容は、選択したすべてのデバイスに適用されます。

Security Manager によって管理されたポイントツーポイントまたは完全メッシュ VPN トポロジ内のデバイス、またはハブアンドスポーク VPN トポロジ内のハブやスポークをデバイスとして選択できます（Easy VPN では、スポークをデバイスとして選択することはできません）。これらの設定は、選択したデバイスが大規模 DMVPN における IPsec ターミネータである場合にも設定する必要がありますが、次に示すすべての設定が使用できるわけではありません。大規模 DMVPN の設定 （1595 ページ）を参照してください。

一般的な注意点

- Catalyst 6500/7600 デバイスには、3 ～ 13 のシャーシ スロットが備えられています。ブレードの設計上、スロットあたり 1 つの VPNSM または 2 つの VPNSPA/VSPA をインストールできます。VPNSPA/VSPA の位置は、スロット番号とサブスロット番号で識別されます。Security Manager は、この情報をインベントリに保存して、VPN トポロジを管理できるようにします。
- シャーシ内のハイ アベイラビリティを設定する場合は、同じデバイスで VPNSM ブレードと VPNSPA/VSPA ブレードをプライマリ ブレードおよびフェールオーバー ブレードとして使用することはできません。
- リモート アクセス VPN では、各 IPsec プロポーザルに対して 1 つのフェールオーバー装置だけを設定できます。[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス （1898 ページ）を参照してください。
- Catalyst 6500/7600 に Firewall Services Module（FWSM; ファイアウォール サービス モジュール）がある場合は、これらのモジュールと連携して動作するように設定できます。詳細については、VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定 （1443 ページ）を参照してください。
- デバイスで VRF 対応 IPsec とともに VPNSM または VPNSPA/VSPA を設定する場合、そのデバイスは、VRF 対応 IPsec が設定されていない別の VPN トポロジに属することができません。詳細については、VRF 対応 IPsec の設定 （1445 ページ）を参照してください。

- Catalyst 6500/7600 デバイスに内部 VLAN を作成するか、または既存のポートや VLAN 設定を編集します。デバイスに VRF 対応 IPsec が設定されている場合は、転送 VLAN を作成する必要があります。

VPNSM に関する注意点

- Security Manager では、Catalyst 6500/7600 デバイスにおける複数の VPNSM の設定がサポートされていますが、VPN トポロジあたり 1 つ（シャーシ内のハイ アベイラビリティを設定する場合は 2 つ）のモジュールだけを設定できます。
- VPNSM を設定する場合、親の Catalyst 6500/7600 デバイスで Cisco IOS ソフトウェア Release 12.2(18)SXD1 以降が実行されている必要があります。
- VPNSM 設定では、レイヤ 3 VLAN だけを使用できます。

VPNSPA/VSPA に関する注意点

- この設定は、大規模 DMVPN 設定で IPsec ターミネータを設定する場合にも適用されます。詳細については、大規模 DMVPN の設定 （1595 ページ）を参照してください。
- VPN SPA では、すべてのキー サイズ（128、192、および 256 ビット）の AES 暗号化アルゴリズム、および DES 暗号化アルゴリズムと 3DES 暗号化アルゴリズムがサポートされています。詳細については、使用する暗号化アルゴリズムの決定 （1483 ページ）を参照してください。

VRF モードでは、**crypto engine slot** *slot/subslot* {**inside** | **outside**} コマンドは内部および外部 VPN インターフェイスに展開されます。

- Catalyst 6500/7600 デバイスで、Cisco IOS ソフトウェア Release 12.2(18)SXE2 以降を実行している必要があります。
- 暗号接続代替モード（このモードでは、暗号化されたトラフィックが VPNSM/VPN SPA で受信された場合はパススルーされ、クリアテキストのトラフィックは迂回されます）を使用する予定の場合、Catalyst 6500 デバイスでは Cisco IOS ソフトウェア バージョン 12.2(33)SXH 以降が、7600 ルータでは 12.2(33)SRA 以降が実行されている必要があります。
- 複数のハブが参加する DMVPN トポロジで 1 つのハブに VPN SPA ブレードが設定されている場合は、スポークであるかハブであるかにかかわらず、いずれのデバイスにもトンネルキーを設定しないでください。このようなトポロジに参加するデバイスでは、キーなしでのトンネルをサポートするために Cisco IOS ソフトウェア バージョン 12.3T 以降が実行されている必要があります。

ナビゲーション パス

Create VPN ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページ、あるいは [VPNピア（VPN Peers）] ポリシーで Catalyst 6500/7600 デバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダ

イアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [FWSM] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。

フィールド リファレンス

表 *327 : [エンドポイントの編集（Edit Endpoints）] ダイアログボックス、[VPNインタフェース（VPN Interface）] タブの [VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）]*

要素	説明
Enable the VPN Interface Changes on All Selected Peers	（注） [Endpoints] ページで、編集用に複数の Catalyst 6500/7600 デバイスを選択した場合に使用できます。 選択されている場合は、[VPN interface] タブで行った変更内容が、選択したすべてのデバイスに適用されます。

要素	説明
VPNSM/VPN SPA/VSPA Settings	• [暗号接続代替の使用（Use Crypto Connect Alternate）]：選択されている場合、Catalyst 6500/7600 上の VPNSM/VPN SPA に入った暗号化されたトラフィックだけがパススルーされます。クリアテキストのトラフィックは、アダプタを通過しません（迂回されます）。このオプションを使用するには、Catalyst 6500 ではバージョン 12.2(33)SXH 以降が、7600 ルータでは 12.2(33)SRA 以降が実行されている必要があります。 このモードは、大規模な VPN トポロジをサポートする必要がある企業のお客様（金融機関など）や、暗号化されたチャネル上で大量のデータを送信する必要がある企業のお客様（インターネット上でのリモートディザスタリカバリやバックアップなど）にとって、暗号接続モードの代替選択肢として推奨されます。 • [内部VLAN（Inside VLAN）]：サービスモジュールまたはアダプタへの内部インターフェイスとして機能する VLAN です。また、VPN トンネルのハブ エンドポイントでもあります（デバイスに VRF 対応 IPsec が設定されていない場合）。VLAN またはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。 • [スロットとサブスロット（Slot and Subslot）]：VPNSM または VPNSPA/VSPA のスロット位置を指定する番号です。VPNSPA/VSPA を設定する場合は、サブスロット番号も必要です。 • [外部VLAN/外部ポート（Outside VLAN/External port）]：内部 VLAN に接続する外部ポートまたは VLAN です。VLAN またはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。内部 VLAN に選択したものとは異なるインターフェイスまたはインターフェイス ロールを選択する必要があります。 （注） VRF 対応 IPsec がデバイスに設定されている場合は、外部ポートまたは VLAN に IP アドレスが必要です。

要素	説明
トンネルの送信元	（注） 選択されたテクノロジーが IPsec/GRE または DMVPN の場合は、ハブに対してだけ使用できます。 スポーク側の GRE または DMVPN トンネルで使用するトンネル ソース アドレスを指定します。次のいずれかのオプションを選択できます。 • [トンネルインターフェイスごとに一意のトンネルソースをオーバーライド（Override Unique Tunnel Source per Tunnel Interface）]：[GREモード（GRE Modes）] > [トンネルパラメータ（Tunnel Parameters）] タブで、トンネルインターフェイスごとに一意のトンネルソースを使用する設定を有効にしている場合、このオプションが選択可能になります。このオプションを選択して、選択したデバイスに別のトンネル ソースを指定します。 • [外部VLAN/外部ポート（CCA/VRFが有効な場合）（Outside VLAN/External Port (When CCA/VRF is Enabled)）]：[暗号接続代替の使用（Use Crypto Connect Alternate）] チェックボックスがオンになっている場合、このオプションボタンが使用可能になります。選択されている場合、外部 VLAN または外部ポートがトンネル ソースとして指定されます。 • [内部VLAN（Inside VLAN）]：選択されている場合、内部 VLAN に設定されているインターフェイスがトンネルソースとして使用されます。 • [インタフェース（Interface）]：任意のインターフェイス（VPN インターフェイスとは限らない）をトンネルソースアドレスとして使用するには、インターフェイス名を入力するか、または [選択（Select）] をクリックしてインターフェイスを識別するインターフェイスロールを選択します。選択リストから新しいロールを作成することもできます。
Local Peer IPSec Termination	ローカル ルータに、VPN インターフェイスの IPsec 終端ポイントを定義します。 • [内部VLAN（Inside VLAN）]：内部 VLAN として設定されているインターフェイスを使用します。 • [IPアドレス（IP Address）]：ローカルルータの VPN インターフェイスの IP アドレスを使用します。IP アドレスを入力します。 （注） VPNインターフェイスとしてトンネル ソースを選択した場合は、VPN インターフェイスに IP アドレスが動的に割り当てられている可能性があります。

要素	説明
Enable Failover Blade	シャーシ内のハイ アベイラビリティを確保するために、フェールオーバー VPNSM または VPNSPA/VSPA ブレードを設定するかどうかを指定します。 （注） 同じデバイスで VPNSM ブレードと VPNSPA/VSPA ブレードをプライマリ ブレードおよびフェールオーバー ブレードとして使用することはできません。 次のように、フェールオーバー ブレードを指定します。 • [スロット（Slot）]：VPNSM ブレードまたは VPNSPA/VSPA ブレードの位置を特定するスロット番号です。 • [サブスロット（Subslot）]：VPNSPA/VSPA を設定する場合は、フェールオーバー VPN SPA ブレードがインストールされているサブスロットの番号（0 または 1）を選択します。 （注） VPNSM を設定している場合は、ブランク オプションを選択します。

エンドポイントの保護対象ネットワークの特定

[Edit Endpoints] ダイアログボックスの [Protected Networks] タブを使用して、[Endpoints] テーブルのデバイスに定義された保護対象ネットワークを編集します（エンドポイントおよび保護対象ネットワークの定義 （1424 ページ） を参照。）

保護対象ネットワークは、命名パターンがデバイスの内部 VPN インターフェイスと一致するインターフェイス ロールとして指定することも、1 つ以上のネットワークやホストの IP アドレス、インターフェイス、その他のネットワーク オブジェクトを含むネットワーク/ホスト グループ オブジェクトとして指定することも、（割り当てられているテクノロジーが通常の IPsec の場合には）アクセス コントロール リスト オブジェクトとして指定することもできます。

- 同時に複数のデバイスを編集している場合は、[選択したすべてのピアで保護されたネットワークの変更を有効にする（Enable the Protected Networks Changes on All Selected Peers）] を選択して、[保護されたネットワーク（Protected Networks）] タブで行ったすべての変更内容を選択されたすべてのデバイスに適用します。
- 保護されたネットワークを追加するには、[使用可能な保護されたネットワーク（Available Protected Networks）] リストからネットワークを選択し、[>>] をクリックして、[選択済みの保護されたネットワーク（Selected Protected Networks）] リストに移動します。インターフェイス ロール オブジェクト、（[Protected Networks] フォルダに表示された）ネットワーク/ホスト グループ オブジェクト、またはアクセス コントロール リスト オブジェクトの任意の組み合わせを使用して、デバイスの保護対象ネットワークを定義できます（ACL オブジェクトは、割り当てられたテクノロジーが通常の IPsec の場合にだけ使用できます）。

バージョン 4.9 以降、Security Manager では IPv6 アドレスがサポートされます。

- [保護されたネットワーク（Protected Networks）] フォルダでは、IPv6 オブジェクトがサポートされるようになりました。

- [アクセスコントロールリスト（Access Control Lists）] フォルダでは、拡張および統合 ACL がサポートされるようになりました。
- インターフェイスロールの場合、IPv6 が有効なインターフェイスを選択して [>>] をクリックすると、設定されているすべての IPv6 アドレスのリストを含むポップアップウィンドウが表示されます。リストからアドレスを選択し、[OK] をクリックして、そのアドレスを [選択済みの保護されたネットワーク（Selected Protected Networks）] リストに移動できます。アドレスを編集するには、[選択済みの保護されたネットワーク（Selected Protected Networks）] リストでアドレスを選択し、[選択の編集（Edit Selection）] リンクをクリックします。
- エクストラネット VPN の場合、リモートバックアップピアでは IPv6 アドレスがサポートされます。

（注） 割り当てられているテクノロジーが通常の IPsec であるハブアンドスポーク VPN トポロジで ACL オブジェクトを使用してスポークで保護対象ネットワークが定義されている場合、Security Manager によってハブ上のスポークの ACL オブジェクトが、一致するクリプトマップエントリにミラーリングされます。

クリプトマップエントリを指定しない場合、展開時に Security Manager は、ハブデバイスのクリプト ACL 名を、スポーク デバイスの ACL オブジェクト名に「_1」を付加して生成します。たとえば、スポークの ACL オブジェクト名が「spokeACL」である場合、Security Manager はハブデバイスのクリプト ACL 名を「spokeACL_1」として生成します。同じ ACL オブジェクト名を持つ複数のスポークデバイスが存在する場合、Security Manager はハブ デバイスのクリプト ACL 名を「ACLobjectName_spokeDisplayName_1」として生成します。

ここで、「ACLobjectName」はトポロジ内のすべてのスポークデバイスの ACL オブジェクト名であり、「spokeDisplayName」はスポークごとに異なるスポークデバイスの表示名です。

Cisco Security Manager は、次のいずれかを実行すると、トポロジタイプに関係なく、ASA デバイスの新しい ACL を作成します。

- 保護されたネットワークにエントリを追加する。
- 既存のハブアンドスポークトポロジの [VPN グローバル設定（VPN Global Setting）] > [全般設定（General Settings）] タブで、[スポーク間接続を有効にする（Enable Spoke to spoke connectivity）] チェックボックスをオンにする。
- 既存のハブアンドスポークトポロジに新しいピアを（スポークとして）追加する。

即座に生成されるこの新しい ACL は、VPN トラフィックを混乱させる可能性があります。したがって、保護されたネットワークで ACL 構成要素を使用して直接変更を行うことをお勧めします。

- 選択済みの保護されたネットワークを削除するには、ネットワークを選択して、[<<] ボタンをクリックします。

- オブジェクトの順序が問題となる場合は、上向き矢印ボタンと下向き矢印ボタンを使用して、必要に応じて選択されたオブジェクトのリスト内でオブジェクトのプライオリティの順序を調整できます。順序が問題とならない場合には、これらのボタンは使用できません。
- 保護されたネットワークを定義するために必要なオブジェクトがリストに表示されていない場合は、[作成（Create）]（+）ボタンをクリックしてオブジェクトを追加します。この場合、追加するオブジェクトのタイプを選択するように求められます。既存のオブジェクトを選択し、[編集（Edit）]（鉛筆）ボタンをクリックして、既存のオブジェクトの定義を変更することもできます。 詳細は、次のトピックを参照してください。
  - インターフェイス ロール オブジェクトについて （381 ページ）、インターフェイス ロール オブジェクトの作成 （383 ページ）
  - ネットワーク/ホストオブジェクトについて （391 ページ）、ネットワーク/ホストオブジェクトの作成 （394 ページ）
  - アクセス コントロール リスト オブジェクトの作成 （356 ページ）

ナビゲーション パス

VPNの作成（Create VPN）ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページ、あるいは [ピア（Peers）] ポリシーでデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [保護されたネットワーク（Protected Networks）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義（1424 ページ）を参照してください。

VPNSM または VPNSPA/VSPA が設定されたデバイスへのファイアウォール サービス モジュール（FWSM）インターフェイスの設定

（注） 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、FWSM はサポートが終了しているため、FWSM の拡張機能はサポートされません。

Security Manager では、Catalyst 6500/7600 デバイスに、IPsec VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA とともに Firewall Services Module（FWSM; ファイアウォールサービスモジュール）を設定できます。この機能を使用すると、VPNSM または VPN SPA/VSPA で内部ネットワークに対してセキュアなアクセスを提供するとともに、FWSM で信頼できないクライアントに対してファイアウォール ポリシーを適用できます。

FWSM と、Catalyst 6500/7600 デバイスにすでに設定されている VPNSM または VPNSPA/VSPA との間の接続を可能にする設定を定義するには、[Edit Endpoints] ダイアログボックスの [FWSM] タブを使用します。[FWSM] タブは、ハブアンドスポーク VPN トポロジにおいて、選択されたハブが Catalyst 6500/7600 デバイスの場合にだけ使用できます。

ヒント

- FWSM 設定を定義する前に、FWSM をホストする Catalyst 6500/7600 デバイスを Security Manager インベントリに追加して、FWSM とそのポリシーおよびセキュリティ コンテキストを検出する必要があります。ネットワークからのデバイスの追加 （100 ページ）およびセキュリティ コンテキストの管理 （2984 ページ）を参照してください。
- Catalyst 6500/7600 デバイスで内部インターフェイスがまだ作成されていない場合は、内部インターフェイスを作成する必要があります（VLAN の作成または編集 （3436 ページ）を参照）。その後、FWSM 内部インターフェイス（VLAN）を適切なセキュリティ コンテキストに割り当てるか、または FWSM ブレードに直接割り当てます。
- また、IPsec VPN Services Module（VPNSM; VPN サービス モジュール）または VPNSPA/VSPA に関連する設定を [VPN Interfaces] タブで行う必要があります。詳細については、VPNSM または VPN SPA/VSPA エンドポイントの設定 （1436 ページ）を参照してください。

ナビゲーション パス

VPN の作成（Create VPN） ウィザードの [エンドポイント（Endpoints）] ページ、または [VPN の編集（Edit VPN）] ダイアログボックス、または [VPN ピア（VPN Peers）] ポリシーで、FWSM を搭載した Catalyst 6500/7600 デバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [FWSM] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。

フィールド リファレンス

表 328 : [Edit Endpoints] ダイアログボックスの [FWSM] タブ

要素	説明
Enable FWSM Settings	Catalyst 6500/7600 デバイスで、Firewall Services Module（FWSM; ファイアウォール サービス モジュール）と VPN Services Module（VPNSM; VPN サービス モジュール）または VPN SPA との間に接続を設定するかどうかを指定します。
FWSM Inside VLAN	Firewall Services Module（FWSM; ファイアウォール サービス モジュール）への内部インターフェイスとして機能する VLAN です。インターフェイスまたはインターフェイス ロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか新しいインターフェイス ロール オブジェクトを作成します。
FWSM Blade	使用可能なブレードのリストから、選択した FWSM 内部 VLAN インターフェイスが接続されているブレード番号を選択します。

要素	説明
セキュリティコンテキスト	FWSM 内部 VLAN がセキュリティ コンテキストの一部である場合（つまり、FWSM がマルチ コンテキスト モードで実行されている場合）、このフィールドにセキュリティ コンテキスト名を指定します。名前では、大文字と小文字が区別されます。

VRF 対応 IPsec の設定

[Edit Endpoints] ダイアログボックスの [VRF-Aware IPsec] タブを使用して、ハブアンドスポーク VPN トポロジ内のハブに VRF-Aware IPsec ポリシーを設定します。VRF 対応 IPsec は、1 ボックス ソリューションまたは 2 ボックス ソリューションとして設定できます。VRF 対応 IPsec の詳細については、VRF 対応 IPsec について （1398 ページ）を参照してください。

ヒント

- VRF 対応 IPsec は、ハブアンドスポーク VPN トポロジのハブにだけ設定できます。
- 2 つのハブがある VPN トポロジでは、両方のデバイスに VRF 対応 IPsec を設定する必要があります。
- VRF 対応 IPsec が設定されていない他の VPN トポロジに属するデバイスに対して VRF 対応 IPsec を設定することはできません。
- ハイ アベイラビリティが設定されているハブに対して VRF 対応 IPsec を設定することはできません。VPN トポロジにおけるハイ アベイラビリティの設定 （1450 ページ）を参照してください。
- IPsec Aggregator が、既存の事前共有キー（keyring）コマンドと同じ **keyring** CLI コマンドを使用して設定されており、他のコマンドによって参照されていない場合には、展開に失敗する場合があります。この場合、Security Manager では VRF keyring CLI が使用されず、異なる名前でキーリングが生成されるため、展開に失敗します。設定を展開する前に、事前共有キー keyring コマンドを CLI から手動で削除する必要があります。

ナビゲーション パス

[VPNの作成（Create VPN）] ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページで、ハブアンドスポーク トポロジ内の VRF 対応 IPsec 設定をサポートするデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [VRF対応IPsec（VRF-Aware IPsec）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）および VPN トポロジの作成または編集 （1416 ページ）を参照してください。

フィールド リファレンス

表 329 : [Edit Endpoints] ダイアログボックスの [VRF Aware IPsec] タブ

要素	説明
Enable the VRF Settings Changes on All Selected Peers	[Endpoints] ページで編集用に複数のデバイスを選択した場合に使用できます。 選択されている場合、[VRF Settings] タブで行ったすべての変更内容が、選択したすべてのデバイスに適用されます。
Enable VRF Settings	デバイスで VRF の設定をイネーブルにするかどうかを指定します。 （注） このチェックボックスの選択を解除することによって、VPN トポロジに定義された VRF 設定を削除できます。ただし、Catalyst 6500/7600 デバイスに VRF 対応 IPsec が設定されている場合、VRF 設定をディセーブルにするには追加の手順が必要となります。 Catalyst スイッチおよび 7600 デバイスにおける VRF のイネーブル化およびディセーブル化 （1402 ページ）を参照してください。
VRF Solution	設定する VRF ソリューションのタイプを指定します。 • [1-Box]（IPsec Aggregator + MPLS PE）：1 ボックス ソリューションでは、1 つのデバイスが、パケットへの MPLS タギング、およびカスタマーエッジ（CE）デバイスとの間での IPsec 暗号化と復号化を行うプロバイダーエッジ（PE）ルータとして機能します。詳細については、 VRF 対応 IPsec 2 ボックス ソリューション （1400 ページ）を参照してください。 • [2-Box]（IPsec Aggregator だけ）：2 ボックス ソリューションでは、PE デバイスは MPLS タギングだけを行います。CE との間の IPsec 暗号化および復号化は、IPsec Aggregator によって行われます。詳細については、 VRF 対応 IPsec 2 ボックス ソリューション （1400 ページ）を参照してください。
[VRF名（VRF Name）]	IPsec Aggregator の VRF ルーティング テーブルの名前。VRF 名では、大文字と小文字が区別されます。

要素	説明
ルート識別子	IPsec Aggregator の VRF ルーティング テーブルの固有識別情報。この一意のルート識別子によって、MPLS コアおよび他の PE ルータにまたがる各 VPN のルーティングの分離が維持されます。 識別情報は次のいずれかの形式です。 • IP アドレス:X（X は 0 ～ 2147483647 の数値） • N:X（N は 0 ～ 65535 の数値、X は 0 ～ 2147483647 の数値） （注） VRF 設定をデバイスに展開したあとは RD 識別子を上書きできません。展開後に RD 識別子を変更するには、デバイス CLI を使用して手動で削除してから、再度展開する必要があります。
Interface Towards Provider Edge （2 ボックス ソリューションのみ）	IPsec Aggregator 上の、PE デバイスに向けた VRF 転送インターフェイス。IPsec Aggregator（ハブ）が Catalyst VPN サービス モジュールの場合は、VLAN を指定する必要があります。 インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか、新しいインターフェイス ロール オブジェクトを作成します。
ルーティング プロトコル（Routing Protocol） （2 ボックス ソリューションのみ）	IPsec Aggregator と PE との間で使用するルーティング プロトコル。オプションは、[BGP]、[EIGRP]、[OSPF]、[RIPv2]、または [Static route] です。デフォルトは BGP です。 保護された IGP で使用されるルーティング プロトコルが、IPsec Aggregator と PE との間で使用されるルーティング プロトコルと異なる場合は、保護された IGP へのルーティングの再配布に使用するルーティング プロトコルを選択します。 プロトコルの詳細については、ルータの管理（3001 ページ）を参照してください。 （注） 1 ボックス ソリューションでは、ルーティング プロトコルおよび AS 番号は指定する必要がないため、これらのフィールドは使用できません。1 ボックス ソリューションでは、BGP プロトコルだけがサポートされています。

要素	説明
AS 番号（AS Number） （2 ボックス ソリューション、BGP または EIGRP ルーティングだけ）	IPsec Aggregator と PE との間の自律システム（AS）領域の識別に使用する番号。AS 番号は、1 ～ 65535 の範囲である必要があります。 保護された IGP で使用されるルーティング プロトコルが、IPsec Aggregator と PE との間で使用されるルーティング プロトコルと異なる場合は、IPsec Aggregator および PE からルーティングが再配布される保護された IGP を識別するために使用する AS 番号を入力します。この設定は、IPsec/GRE または DMVPN が適用されている場合にだけ関連があります。
Process Number （2 ボックス ソリューション、OSPF ルーティングのみ）	OSPF ルーティングを使用している場合に、保護された IGP を識別するために使用するルーティング プロセス ID 番号。 範囲は 1 ～ 65535 です。
OSPF Area ID （2 ボックス ソリューション、OSPF ルーティングのみ）	パケットが属する領域の ID 番号。0 ～ 4294967295 の範囲の任意の番号を入力できます。 （注） すべての OSPF パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ領域 ID 番号が必要です。
Next Hop IP Address （2 ボックス ソリューション、スタティック ルーティングだけ）	スタティック ルーティングを使用している場合の、IPsec Aggregator に接続されているプロバイダーエッジ（PE）またはインターフェイスの IP アドレス。
Redistribute Static Route （2 ボックス ソリューション、スタティック ルーティング以外だけ）	IPsec Aggregator に設定されたルーティング プロトコルで、スタティック ルートを PE デバイスにアドバタイズするかどうかを指定します。

クリプトマップの設定

バージョン 4.7 以降、Cisco Security Manager では、VPN トポロジ内の各ピアデバイスのクリプトマップ名とクリプト ACL 名を手動で設定できます。この機能は、通常の IPsec トポロジでのみサポートされています。

[エンドポイントの編集（Edit Endpoints）] ダイアログボックスの [クリプトマップ（Crypto Map）] タブを使用して、ピアに設定されているクリプトマップ名とクリプト ACL 名とともにピアデバイスを一覧表示します。リストでピアデバイスを選択し、[編集（Edit）]（鉛筆）ボタンをクリックすると、[クリプトマップエントリの編集（Edit Crypto Map Entry）] ダイアログボックスが開きます。

（注） トポロジがダイナミッククリプトマップをサポートしている場合、[編集（Edit）] ボタンをクリックすると開くダイアログボックスで、ダイナミッククリプトマップ名を入力できます。

ナビゲーション パス

Create VPN ウィザードまたは [VPNの編集（Edit VPN）] ダイアログボックスの [エンドポイント（Endpoints）] ページでデバイスを選択し、[編集（Edit）] をクリックして [エンドポイントの編集（Edit Endpoints）] ダイアログボックスを開きます。[エンドポイントの編集（Edit Endpoints）] ダイアログボックスで [クリプトマップ（Crypto Map）] タブを選択します。これらのページおよびダイアログボックスへのアクセス方法については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。

フィールド リファレンス

表 *330 : [*エンドポイントの編集（*Edit Endpoints***）*]* ダイアログボックス、*[*クリプトマップ（***Crypto Map***）*]* タブ**

要素	デフォルト値（Default Value）
暗号マップ名（Crypto Map Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager はデバイスのクリプトマップ名を使用するか、または新しいクリプトマップ名を生成します。VPN インターフェイスにクリプトマップがすでに存在する場合、Cisco Security Manager は同じ名前を再利用します。
クリプトマップシーケンス（Crypto Map Sequence）	Cisco Security Manager は、管理対象ネットワークでデバイスを検出すると、このフィールドにデバイスのシーケンス番号を表示します。この値は編集できません。 新しい VPN トポロジを追加する場合、Cisco Security Manager は [シーケンス番号（Sequence Number）] フィールドに # の値を入力します。この値は編集できません。
クリプトACL名（Crypto ACL Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager は新しいクリプト ACL 名を生成します。
ダイナミッククリプトマップ名（Dynamic Crypto Map Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager はデバイスのクリプトマップ名を使用するか、または新しいクリプトマップ名を生成します。

- インターフェイスに適用できるクリプトマップは 1 つだけです。
- デバイスの複数のインターフェイスに同じクリプトマップ名を割り当てることはできません。

- デバイスの同じインターフェイスに異なるクリプトマップ名を割り当てることはできません。

[クリプトマップエントリの編集（Edit Crypto Map Entry）] ダイアログボックス

フィールド リファレンス

表 *331 : [クリプトマップエントリの編集（Edit Crypto Map Entry）] ダイアログボックス*

要素	デフォルト値（Default Value）
クリプトACL名（Crypto ACL Name）	デフォルト値はありません。値を入力しない場合、Cisco Security Manager は新しいクリプト ACL 名を生成します。
クリプトマップシーケンス（Crypto Map Sequence）	Cisco Security Manager は、管理対象ネットワークでデバイスを検出すると、このフィールドにデバイスのシーケンス番号を表示します。この値は編集できません。 新しい VPN トポロジを追加する場合、Cisco Security Manager は [シーケンス番号（Sequence Number）] フィールドに # の値を入力します。この値は編集できません。
暗号モード（Crypto Mode）	ASA デバイス バージョン 9.6(2) 以降向けの Cisco Security Manager バージョン 4.12 以降では、次の暗号モードからオプションを選択できます。 • [トンネル（Tunnel）] : デフォルト値。カプセル化モードがトンネルモードになります。 • [トランスポート（Transport）] : ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きのトランスポートモードになります。 • [トランスポート必須（Transport-Require）] : カプセル化モードはトランスポート必須モードのみになります。 （注） トランスポートおよびトランスポート必須モードは、IKEv2 でのみサポートされます。

VPN トポロジにおけるハイ アベイラビリティの設定

Create VPN ウィザードおよび [Edit VPN] ダイアログボックスの [High Availability] ページを使用して、ハブのグループをハイ アベイラビリティ（HA）グループとして定義します。ハイ アベイラビリティを設定するかどうかはオプションです。

Create VPN ウィザードまたは [Edit VPN] ダイアログボックスを開く方法については、VPN トポロジの作成または編集 （1416 ページ）を参照してください。

LAN 上で IP を実行する Cisco IOS ルータまたは Catalyst 6500/7600 デバイスにハイ アベイラビリティ（HA）ポリシーを設定すると、自動デバイス バックアップ機能を使用できます。ハイ アベイラビリティは、通常の IPsec または Easy VPN テクノロジーを使用するハブアンドスポーク VPN トポロジで設定できます。

Security Manager では、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブ デバイスで構成された HA グループによって HA がサポートされます。仮想 IP アドレスを共有することによって、HA グループのハブは、外観上は、LAN 上のホストに対して単一の仮想デバイスまたはデフォルト ゲートウェイになります。HA グループの 1 つのハブが常にアクティブになって仮想 IP アドレスを独占的に使用し、同時に他のハブはスタンバイ ハブになります。グループ内のハブは、アクティブ デバイスおよびスタンバイ デバイスから hello パケットが着信するのを待ちます。アクティブ デバイスが何らかの理由で使用できなくなると、スタンバイ ハブが仮想 IP アドレスの所有権を取得して、ハブの機能を引き継ぎます。この移行は、LAN 上のホストおよびピア デバイスに対してシームレスかつ透過的に実行されます。

HA グループを使用する場合は、次の点に注意します。

- ハイ アベイラビリティは、通常の IPsec または Easy VPN テクノロジーを使用するハブアンドスポーク VPN トポロジ内のハブに対してだけ設定できます。
- ハイ アベイラビリティは、Cisco IOS ルータまたは Catalyst 6500/7600 デバイスにだけ設定できます。ただし、HA グループには、Cisco IOS ルータと Catalyst 6500/7600 デバイスの両方を含むことはできません。
- ステートフル フェールオーバーを設定する場合、HA グループには 2 つのハブだけを含むことができます。これらのハブは、Cisco IOS ルータである必要があります。Catalyst 6500/7600 デバイスは使用できません。
- VRF 対応 IPsec が設定されたハブにはハイ アベイラビリティを設定できません。 VRF 対応 IPsec について （1398 ページ）を参照してください。
- HA グループには GRE を設定できません。
- HA グループ内のデバイスは、複数のハブアンドスポーク トポロジに属することができます。
- サイト間 VPN で HA が設定されたハブとして設定されているデバイスは、同じ外部インターフェイスを使用して、異なるサイト間 VPN で HA が設定されたハブとして設定できません。同様に、このようなデバイスは、同じ外部インターフェイスを使用して、HA が設定されたリモート アクセス VPN サーバとして設定できません。
- すべてのピアにおいて、同じ自動生成された事前共有キーを認証に使用する必要があります。Preshared Key ポリシーを設定するときにこのオプションの使用を指定していない場合、このオプションは、ハイ アベイラビリティの設定中に上書きされます。詳細については、 IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。
- 設定の生成中に、HA グループ内のすべてのハブは同じコマンドを受信します。コマンドは、HA グループ全体に対して展開する必要があります。グループ内の個別のハブに対して展開することはできません。

次の表に、ハイ アベイラビリティ設定用のオプションを示します。

表 *332 : [High Availability]* ページ

要素	説明
有効化（Enable）	ハブのグループに対してハイ アベイラビリティ設定をイネーブルにするかどうかを指定します。すでにハイ アベイラビリティを設定している場合は、このオプションの選択を解除することによって、設定を削除できます。
Inside Virtual IP	HA グループ内のハブによって共有され、HA グループの内部インターフェイスを表す IP アドレス。仮想 IP アドレスは、HA グループ内のハブの内部インターフェイスと同じサブネットである必要がありますが、これらのインターフェイスのいずれかと同じ IP アドレスにすることはできません。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
Inside Mask	内部仮想 IP アドレスのサブネット マスク。
VPN Virtual IP	HA グループ内のハブによって共有され、HA グループの VPN インターフェイスを表す IP アドレス。この IP アドレスは、VPN トンネルのハブ エンドポイントとして機能します。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
VPN Mask	VPN 仮想 IP アドレスのサブネット マスク。
Hello 間隔（Hello Interval）	ステータスと優先度を示すためにハブがグループ内の別のハブにエコー hello メッセージを送信する秒単位の間隔（1 ～ 254）。デフォルトは 5 秒です。
保留時間（Hold Time）	ハブがダウンしていると結論付ける前に、スタンバイ ハブがアクティブなハブから hello メッセージの受信を待機する秒単位の期間（2 ～ 255）。デフォルトは 15 秒です。
Standby Group Number (Inside)	HA グループ内のハブの内部仮想 IP サブネットと一致する内部ハブ インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 1 です。
Standby Group Number (Outside)	HA グループ内のハブの外部仮想 IP サブネットと一致する外部ハブ インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 2 です。 （注） 外部スタンバイ グループの番号と内部スタンバイ グループの番号は異なっている必要があります。

要素	説明
Enable Stateful Failover	ステートフル フェールオーバーをイネーブルにし、ステートフル スイッチオーバー（SSO）を使用して HA グループ内の HSRP デバイス間で状態情報が共有されるようにするかどうかを指定します。デバイスで障害が発生した場合、共有されている状態情報により、スタンバイデバイスは、トンネルの再確立またはセキュリティアソシエーションの再ネゴシエートを行わずに、IPsec セッションを維持できます。 ステートフル フェールオーバーは、Cisco IOS ルータである 2 つのハブを含む HA グループでだけ設定できます。このチェックボックスは、HA グループに 3 つ以上のハブが含まれる場合にディセーブルになります。 Easy VPN トポロジでは、ステートフル フェールオーバーを常に設定する必要があるため、このチェックボックスは選択されてディセーブルになります。 **ヒントTips:** • 通常の IPsec トポロジの場合に選択解除すると、HA グループにステートレス フェールオーバーが設定されます。ステートレス フェールオーバーは、HA グループに 3 つ以上のハブが含まれる場合にも設定されます。ステートレス フェールオーバーは、Cisco IOS ルータまたは Catalyst 6500/7600 デバイスに設定できます。 • ステートレス フェールオーバーは、IKE 認証方式が RSA の署名である場合には使用できません。 • Cisco IOS バージョン 12.3(14)T 以降が実行されているデバイスでだけ、ステートフル フェールオーバーと PKI を同時に設定できます。

関連項目

- ハブアンドスポーク VPN トポロジ （1380 ページ）
- Easy VPN について （1599 ページ）

GET VPN グループ暗号化の定義

[GET VPN Group Encryption] ページを使用して、GET VPN トポロジのグループ設定およびセキュリティ アソシエーションを定義します。

このページの内容は、Create VPN ウィザードを使用しているか、または Group Encryption ポリシーを編集しているかに応じて異なります。ウィザードのページはタブ形式ではありませんが、ポリシーはタブ形式で表示されます。ウィザードのページには追加のフィールドが用意されており、セキュリティ アソシエーションを設定できます。

[GET VPN Group Encryption] ページを開くには、次の手順を実行します。

- 新しい GET VPN を作成する場合は、Create VPN ウィザードを使用します。ウィザードの開始方法の詳細については、VPN トポロジの作成または編集 （1416 ページ）を参照してください。
- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））既存の GET VPN トポロジを選択して、ポリシーセレクタで [グループ暗号化ポリシー（Group Encryption Policy）] を選択します。
- （ポリシービュー）**[サイト間VPN（Site-to-Site VPN）]>[グループ暗号化ポリシー（Group Encryption Policy）]** を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

次の表に、GET VPN グループ暗号化設定を定義する場合に設定可能なオプションを示します。

表 *333 : [GET VPN Group Encryption Policy]* ページ

要素	説明
[Group Settings] タブ	
グループ名（Group Name）	Group Domain of Interpretation（GDOI）グループの名前。この名前は、VPN 名と同じです。
Group Identity	グループを識別するために使用されるパラメータ。すべてのキーサーバおよびグループ メンバーは、このパラメータを使用してグループを識別します。 ID には、番号（3333 など）または任意の IP アドレス（キーの再生成に使用するマルチキャスト アドレスなど）を使用できます。
受信のみ	イネーブルに設定すると、グループ メンバーによってトラフィックが復号化されて、クリア テキストで転送されます。この機能は、VPN のテストに役立ちます。通常の運用においては、このオプションを選択しないでください。詳細については、パッシブ モードを使用した GET VPN への移行 （1649 ページ）を参照してください。

要素	説明
セキュリティ ポリシー （Create VPN ウィザードだけ）	セキュリティ ポリシーとして使用される ACL ポリシー オブジェクト。このオブジェクトの内容の詳細な説明とグループ メンバーセキュリティ ポリシーとの関連については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。 このフィールドは、Create VPN ウィザードを使用している場合にだけ表示されます。Group Encryption ポリシーでは、[Security Associations] タブでセキュリティ ポリシーを設定します（後述の説明を参照）。 （注） キーの配布方法としてマルチキャストを使用している場合は、ACL ポリシー オブジェクトにマルチキャスト アドレスの拒否ルール（ACE）が含まれている必要があります。こうすると、マルチキャストを使用して送信されるキーの再生成パケットは、TEK によって暗号化されなくなります。このステートメントにより、グループ メンバーは、マルチキャスト プロトコルを使用して送信されたキーの再生成パケットを受信できます。
認証タイプ（Authorization Type）	グループで使用する認可メカニズムのタイプを [None]、[Certificates]、または [Preshared Key] から選択します。[Certificates] または [Preshared Key] を選択すると、権限のあるグループ メンバーだけがキー サーバに登録できるようになり、セキュリティが強化されます。キーサーバが複数の GDOI グループで使用される場合には、このような追加のセキュリティが必要となります。 [証明書（Certificates）] を選択した場合は、証明書フィルタのリストを作成する必要があります（識別名属性または完全修飾ドメイン名属性の組み合わせを使用）。このフィルタは、キー サーバに配置されて、GDOI グループに参加する権限がグループ メンバーにあるかどうかを確認するために使用される属性や値を指定します。証明書フィルタの名前を入力し、[行の追加（Add Row）]（+）ボタンをクリックして、[Add Certificate Filter] ダイアログボックス （1458 ページ）に入力します。 （注） 証明書認可を設定するには、GET VPN の Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーも設定する必要があります。使用する PKI 登録オブジェクトには、必要に応じて、同じ識別名が定義されているか、またはデバイスの完全修飾ドメイン名が含まれている必要があります。 [事前共有キー（Preshared Key）] を選択した場合は、権限のあるグループ メンバーを特定するための ACL ポリシーオブジェクトも選択します。許可ルールを使用して、グループ メンバーのホストまたはネットワーク アドレスを特定します。

要素	説明
Key Distribution	各グループ メンバーにキーを配布するために使用する転送方法（[unicast] または [multicast]）。どちらを使用するかを決定するのに役立つ情報については、キーの再生成転送メカニズムの選択 （1625 ページ）を参照してください。 [unicast] を選択した場合、キーサーバーは登録されている各グループメンバーに対してキーの再生成メッセージを送信し、確認応答を待機します。[multicast] を選択した場合、キー サーバはキーの再生成メッセージをすべてのグループ メンバーに一度に送信し、確認応答は待機しません。キーの再生成メッセージは、このポリシーに設定された再送信間隔経過後に再送信されます。 [multicast] を選択した場合、キーサーバーとして使用されているルータでマルチキャストがイネーブルになっていることを確認します。また、次のオプションを設定します。 • [グループIPアドレス（Group IP Address）]：キー配布に使用されるマルチキャストグループの IP アドレスです。 • [グループメンバーでStatic IGMP Joinsを使用（Use Static IGMP Joins on Group Members）]：このオプションを選択すると、静的な Source Specific Multicast（SSM）マッピングがイネーブルとなり、グループメンバーに対してマルチキャストトラフィックの送信元が通知されます。GET VPN の場合、グループ メンバーには、キー サーバのアドレスが通知されます。
RSA Key Label	さまざまなメッセージの暗号化に使用される、RSA キーのラベル。このキーは、デバイスにすでに存在している場合もありますが、使用されていない新しいラベルを指定することもできます。 新しい VPN を作成している場合、[VPNの作成（Create VPN）] ウィザードの最後にキーサーバー間でこのキーを同期するかどうかを尋ねられます。[はい（Yes）] をクリックすると、キーが存在していない場合には Security Manager によってキーが生成されます。既存の GET VPN でこの値を変更した場合は、Key Servers ポリシーからキーを同期する必要があります。このキーの用途、およびキーの生成と同期のプロセスの詳細については、RSA キーの生成と同期 （1636 ページ）を参照してください。

要素	説明
Lifetime (KEK)	Key Encryption Key（KEK; キー暗号化キー）が有効な秒数。このキーは、キーの再生成メッセージの暗号化に使用されます。このライフタイムが終了する前に、キーサーバからグループにキーの再生成メッセージが送信されます。このメッセージには、新しい KEK 暗号化キーとトランスフォーム、および新しい TEK 暗号化キーとトランスフォームが含まれています。 KEK ライフタイム値は、TEK ライフタイム値よりも大きい必要があります（KEK ライフタイム値は、TEK ライフタイム値の少なくとも 3 倍以上にすることが推奨されます）。通常は、デフォルト値である 86,400 秒が適しています。TEK ライフタイム値は、セキュリティ アソシエーションごとに設定します（ [Add New Security Association]/[Edit Security Association] ダイアログボックス （1459 ページ）を参照）。
暗号化アルゴリズム（Encryption Algorithm）	キー サーバからグループ メンバーへのキーの再生成メッセージを暗号化するために使用されるアルゴリズム。
Retransmits	1 つ以上のグループ メンバーがキーの再生成メッセージを受信しない場合にメッセージを送信できる回数。
インターバル	再試行間隔を表す秒数。
[Security Associations] タブ	
[Security Associations] テーブル	[Security Associations] テーブルを使用して、VPN のセキュリティ アソシエーションを定義します。テーブルのカラムには、エントリの設定の概要が表示されます。これらについては、 [Add New Security Association]/[Edit Security Association] ダイアログボックス （1459 ページ）で説明します。新しい VPN を作成する場合は、このタブではなく [Security Policy] フィールド（上記の説明を参照）を使用します。このタブは、ウィザードには表示されません。 セキュリティ アソシエーションを設定するには、次の手順を実行します。 • テーブルにエントリを追加するには、[追加（Add）] ボタンをクリックして、[新しいセキュリティアソシエーションの追加（Add New Security Association）] ダイアログボックスに入力します。 • エントリを選択し、[編集（Edit）] ボタンをクリックして、既存のエントリを編集します。 • エントリを選択し、[削除（Delete）] ボタンをクリックして削除します。

関連項目

- GET VPN 登録プロセスについて （1623 ページ）

- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）

[Add Certificate Filter] ダイアログボックス

[Add Certificate Filter] ダイアログボックスを使用して、GET VPN の Group Encryption ポリシー用の証明書フィルタを定義します。このフィルタは、キーサーバに配置されて、グループに参加する権限がグループメンバーにあるかどうかを確認するために使用される属性や値を指定します。

次のフィルタ タイプのいずれかを選択します。

- [dn]：（識別名。）[サブジェクト（Subject）] フィールドに、名前=値のペアのリストをカンマで区切って指定します。たとえば、OU=Cisco, C=US のように指定します。Public Key Infrastructure ポリシーを設定する場合は、選択する PKI 登録オブジェクトの [Certificate Subject Name] タブで同じ値が定義されている必要があります（[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）を参照）。識別名を使用すると、1 つのフィルタで複数のデバイスに一致させることができます。
- [fqdn]：（完全修飾ドメイン名。）[ドメイン名（Domain Name）] フィールドに、単一のデバイスの完全修飾ドメイン名（router1.example.com など）を指定します。公開鍵インフラストラクチャ ポリシーを設定する場合は、選択する PKI 登録オブジェクトで [デバイスの FQDNを含める（Include Device's FQDN）] オプションが選択されている必要があります。各デバイスは一意の名前を持つため、FQDN フィルタは単一のデバイスにだけ一致します。

ヒント 証明書認可を設定するには、GET VPN の Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーも設定する必要があります。PKI ポリシーは、VPN のすべてのデバイスに設定します。

ナビゲーション パス

[GET VPNグループ暗号化（GET VPN Group Encryption）] ページの [グループ設定（Group Settings）] タブで、認可タイプとして [証明書（Certificates）] を選択し、[認可フィルタ（Authorization Filter）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、フィルタを選択して [行の編集（Edit Row）] ボタンをクリックします。[Group Encryption] ページを開く方法については、GET VPN グループ暗号化の定義 （1453 ページ）を参照してください。

関連項目

- GET VPN 登録プロセスについて （1623 ページ）
- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）

[Add New Security Association]/[Edit Security Association] ダイアログボックス

[Add New Security Association]/[Edit Security Association] ダイアログボックスを使用して、選択した GET VPN トポロジで使用される IPsec プロファイル（名前とトランスフォーム セットだけ）およびセキュリティ ポリシーを定義します。

ナビゲーション パス

[新しいセキュリティアソシエーションの追加（Add New Security Association）] ダイアログボックスを開くには、[GET VPNグループ暗号化（GET VPN Group Encryption）] ページの [セキュリティアソシエーション（Security Associations）] タブで、[行の追加（Add Row）]（+）ボタンをクリックするか、または既存のアソシエーションを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。[Group Encryption] ページを開く方法については、GET VPN グループ暗号化の定義 （1453 ページ）を参照してください。

関連項目

- GET VPN 登録プロセスについて （1623 ページ）
- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）

フィールド リファレンス

表 334 : [Add New Security Association] ダイアログボックス

要素	説明
ID	プロファイルのシーケンス番号。この番号によって、セキュリティアソシエーションの相対的なプライオリティが定義されます（1が最も高いプライオリティです）。複数のセキュリティ アソシエーションがある場合、それぞれの ACL がこの番号で表された順序で連結（およびマージ）され、グループ メンバーは、連結された ACL を単一の ACL として処理します。 デフォルトの番号のままにするか、または新しい番号を入力します。
IPSec Profile Name	IPsec プロファイルの名前。
トランスフォーム セット（Transform Sets）	IPsecプロファイルに定義されたトランスフォーム セット ポリシー オブジェクト（セキュリティ プロトコル、アルゴリズム、およびその他の設定）。複数のエントリがある場合は、カンマで区切って、プライオリティ順に並べます。[選択（Select）]をクリックして定義済みのトランスフォームセットのリストから選択するか、または新しいトランスフォームセットを作成します。

要素	説明
セキュリティ ポリシー	セキュリティ アソシエーションに対して定義されているアクセス コントロール リスト ポリシー オブジェクト。[選択（Select）] をクリックして定義済みの ACL オブジェクトのリストから選択するか、または新しい ACL オブジェクトを作成します。このオブジェクトの内容の詳細な説明とグループ メンバー セキュリティ ポリシーとの関連については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。 （注） キーの配布方法としてマルチキャストを使用している場合は、ACL ポリシー オブジェクトにマルチキャスト アドレスの拒否ルール（ACE）が含まれている必要があります。こうすると、マルチキャストを使用して送信されるキーの再生成パケットは、TEK によって暗号化されなくなります。このステートメントにより、グループ メンバーは、マルチキャスト プロトコルを使用して送信されたキーの再生成パケットを受信できます。
Enable Anti-Replay	盗聴者がデータ ストリームにパケットを挿入できないようにするアンチリプレイ機能をイネーブルにするかどうかを指定します。アンチリプレイは、トラフィック カウンタまたは時間に基づいて設定できます。 • [カウンタ ウィンドウ サイズ（Counter Window Size）]：これがデフォルトですが、推奨されません。カウンタ ベースのアンチリプレイは、グループ メンバーが 2 つの場合（実質的にポイントツーポイント VPN の場合）にだけ役立ちます。ウィンドウ サイズを選択します。 • [時間ウィンドウ サイズ（Time Window Size）]：これが推奨される方法ですが、グループ メンバーが 3 つ以上必要です。Synchronous Anti-Replay（SAR; 同期アンチリプレイ）クロックの間隔を表す秒数を入力します。1 ～ 100 の範囲の値を入力します。デフォルト値は 100 です。時間ベースのアンチリプレイの詳細については、時間ベースのアンチリプレイについて（1633 ページ）を参照してください。 （注） カウンタ ベースのアンチリプレイにおいて、パケット レートが高い状態で暗号化を行う場合は、KEK ライフタイムまたは TEK ライフタイムをあまり長くしないでください。数時間でシーケンス番号が折り返す可能性があるためです。たとえば、パケット レートが 100 キロパケット/秒の場合、シーケンス番号が折り返す前に SA が使用されるように、ライフタイムを 11.93 時間未満に設定する必要があります。

要素	説明
Enable IPSec Lifetime	Global Settings for GET VPN ポリシーで設定されるグローバル設定を上書きする IPsec セキュリティ アソシエーション ライフタイムを設定するかどうかを指定します（GET VPN のグローバル設定 （1640 ページ）を参照）。このライフタイム値によって、キーの再生成が必要となるまでに、どの程度の時間 Traffic Encryption Key（TEK; トラフィック暗号化キー）を使用できるかが制御されます。 グループ メンバー間のトラフィック量（KB 単位）、秒数、またはその両方に基づいて値を設定します。いずれかの値に達するとキーが失効します。次の推奨事項を考慮してください。 • ライフタイムは、Key Encryption Key（KEK; キー暗号化キー）に使用されるライフタイムよりも大幅に短く（3 分の 1 程度に）する必要があります（ GET VPN グループ暗号化の定義 （1453 ページ）を参照）。 • トラフィック量が多い場合にはキーの再生成が頻繁に発生し、データが消失する危険性があるため、時間に基づくライフタイムを推奨します。 • グローバル設定を上書きしない場合は、フィールドを空白のままにします。

GET VPN ピアの定義

Create VPN ウィザードの [GET VPN Peers] ページを使用して、GET VPN トポロジ内のキー サーバおよびグループ メンバーのピア プロパティを設定します。トポロジを作成したあとは、[キーサーバー（Key Servers）] ポリシーおよび [グループメンバー（Group Members）] ポリシーを使用して、これらの設定を変更します。ポリシーは、キー サーバとグループ メンバーのテーブルが異なるポリシーに分割されている点を除いて、ウィザードのページと同じです。

ヒント キーサーバーおよびグループメンバーのリストには、ウィザードの [デバイスの選択（Device Selection）] ページで選択したデバイスが含まれます（VPN トポロジのデバイスの選択 （1422 ページ）を参照）。ただし、[追加（Add）]（+）ボタンおよび [削除（Delete）]（ゴミ箱）ボタンを使用して、このページのデバイスを追加または削除できます。

キー サーバとグループ メンバーのリストを確認して、デフォルト設定がご使用の VPN に適しているかどうかを判断します。各テーブルの下にある [表示（Show）] フィールドで [一致するインターフェイス（Matching Interfaces）] を選択して、デフォルトのインターフェイス ロールによって選択される実際のインターフェイスを表示できます。GET VPN 設定を有効にするには、インターフェイス ロールがデバイスの実際のインターフェイスに解決される必要があります。

はじめる前に

ここでは、新しい VPN を作成するときに GET VPN のピアを定義する方法、および GET VPN のピア設定について説明します。Create VPN ウィザードを開く方法については、VPN トポロジの作成または編集 （1416 ページ）を参照してください。

関連項目

- 登録の失敗時にも保護するためのフェールクローズの設定 （1628 ページ）
- パッシブ モードを使用した GET VPN への移行 （1649 ページ）
- GET VPN キー サーバの設定 （1642 ページ）
- GET VPN グループ メンバーの設定 （1645 ページ）

ステップ 1 デフォルト設定が適切でない場合は、キー サーバを設定します。

変更する各キーサーバーを選択し、テーブルの下にある [編集（Edit）]（鉛筆）ボタンをクリックして、少なくとも次の項目を設定します。使用可能なすべての設定については、[Edit Key Server] ダイアログボックス （1644 ページ）を参照してください。

- [アイデンティティインターフェイス（Identity Interface）]：グループメンバーがキーサーバーを識別し、キーサーバーに登録するために使用するインターフェイスを選択します。デフォルトは、キーサーバに定義されているすべてのループバック インターフェイスを識別するループバック インターフェイス ロールです。
- [プライオリティ（Priority）]：1 ～ 100 の範囲のプライオリティ値を入力することによって、キーサーバーのロールをプライマリまたはセカンダリとして定義します。最も高いプライオリティを持つキーサーバがプライマリ キー サーバとなります。2 つ以上のキー サーバに同じプライオリティ値が割り当てられている場合は、最も大きい IP アドレスを持つデバイスが使用されます。デフォルトのプライオリティは、最初のキー サーバに対しては 100、2 番めのキー サーバに対しては 95 などになります。

（注） ネットワークがパーティション化されている場合は、複数のプライマリ キー サーバが存在することがあります。

ステップ 2 テーブル内でキー サーバを上方または下方に移動して、グループ メンバーがキー サーバに登録する場合に使用する順序を指定します。グループ メンバーは、リストの最初のキー サーバに登録されます。最初のキー サーバに到達できない場合は、2 番め以降のキー サーバに順番に登録が試みられます。この順序は、どのキー サーバがプライマリ キー サーバであるかを判断するために使用される全体的なキー サーバのプライオリティを定義するものではないことに注意してください。

ステップ 3 デフォルト設定が適切でない場合は、グループ メンバーを設定します。

変更する各グループメンバーを選択し、テーブルの下にある [編集（Edit）]（鉛筆）ボタンをクリックして、少なくとも次の項目を設定します。

- [GET対応インターフェイス（GET-Enabled Interface）]：プロバイダーエッジ（PE）への VPN 対応外部インターフェイスです。このインターフェイスで発信または終了するトラフィックは、暗号化または復号化が適宜評価されます。複数のインターフェイスに解決されるインターフェイス ロール オブジェクトを選択することによって、複数のインターフェイスを設定できます。[選択（Select）]をクリックして、インターフェイス ロール オブジェクトを選択するか、新しいオブジェクトを作成します。

- [ローカルアドレスとして使用するインターフェイス（Interface To Be Used As Local Address）]：キーサーバーがキーの再生成情報などのデータを送信する場合にグループメンバーを識別するために使用する IP アドレスを持つインターフェイス。GET が 1 つのインターフェイスでだけイネーブルになっている場合は、ローカル アドレスとして使用するインターフェイスを指定する必要はありません。GET が複数のインターフェイスでイネーブルになっている場合は、ローカル アドレスとして使用するインターフェイスを指定する必要があります。インターフェイスまたはインターフェイスロールの名前を入力します。または [選択（Select）] をクリックしてインターフェイスロールを選択します。

他の使用可能な設定については、[Edit Group Member] ダイアログボックス （1646 ページ）を参照してください。

新しい VPN トポロジへの初期ポリシー（デフォルト）の割り当て

Create VPN ウィザードの [VPN Defaults] ページを使用して、作成する VPN トポロジに割り当てられる共有サイト間 VPN ポリシーを表示および選択します。このページには、選択した IPsec テクノロジーに応じて、VPN トポロジに割り当てることができるすべての使用可能な必須およびオプションのポリシーが表示されます（詳細については、サイト間 VPN の必須ポリシーおよびオプションのポリシーについて （1385 ページ）を参照してください。）

Create VPN ウィザードを開く方法については、VPN トポロジの作成または編集 （1416 ページ）を参照してください。トポロジを作成したあとは、これらのポリシーを直接編集できます。

各ポリシー タイプにおいて、VPN トポロジに割り当てる共有 VPN ポリシーを選択します。共有ポリシーだけを選択できます。次のヒントに従って選択します。

- このページに表示される初期デフォルトは、Security Manager Administration の [VPN Policy Defaults] ページ （743 ページ）で設定します。必須ポリシーに対して特定のデフォルトが設定されていない場合は、出荷時のポリシーが選択されます。デフォルトポリシーの設定の詳細については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。
- リストされる共有ポリシーは、データベースにコミットされた共有ポリシーのみです。たとえば、Create VPN ウィザードを使用する前に新規共有 IPsec Proposal ポリシーを作成したが、そのポリシーを事前に送信しない（および、必要に応じて承認した）場合、その新規ポリシーはリストに表示されません。新規ポリシーを使用する必要がある場合は、VPN を作成する前にそのポリシーを必ず送信してください。
- ポリシーが必須の場合は、必ず選択を行う必要があります。共有ポリシーがない場合は、出荷時のポリシーだけを選択できます。トポロジを作成したあと、いつでもポリシーを編集できます。

（注） 現在他のユーザによってロックされている共有ポリシーの選択を試みた場合は、ロックに関する問題が存在することを示す警告メッセージが表示されます。ロックを回避するには、別のポリシーを選択するか、またはロックが解除されるまで VPN トポロジの作成をキャンセルします。詳細については、ポリシーのロックについて （217 ページ）を参照してください。

- ポリシーがオプションであり、共有ポリシーがない場合は、何も選択できません。そのポリシーによって提供される機能が必要な場合は、トポロジ作成終了後に設定します。
- 読み取り専用ダイアログボックスでポリシーの内容を表示するには、ポリシーを選択して、ポリシーリストの横にある [コンテンツを表示（View Contents）] ボタンをクリックします。
- IKEv2 のみをサポートするトポロジを作成している場合でも、Create VPN ウィザードは、選択内容に従って IKEv1 Preshared Key ポリシーまたは IKEv1 Public Key Infrastructure ポリシーのいずれかを作成します。IKEv2 Authentication ポリシーに対するデフォルト設定はありません。IKEv2 をサポートすることを選択する場合は常に、VPN を作成したあとで IKEv2 Authentication ポリシーを手動で編集し、少なくともグローバル IKEv2 設定を定義する必要があります。ピア固有の IKEv2 オーバーライドを作成することもできます。IKEv2 のみをサポートする場合、ウィザードによって作成された IKEv1 固有のポリシーを割り当て解除できます。

完了したら、[終了（Finish）] をクリックして、新しい VPN トポロジを作成します。新しい VPN トポロジが [Site-to-Site VPN] ウィンドウの VPN セレクタに表示され、[VPN Summary] ページが表示されます。[VPNトポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）] （1464 ページ） を参照してください。

[VPNトポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）]

[VPN Summary] ページを使用して、選択した VPN トポロジの設定の概要を表示します。概要には、VPN トポロジのタイプ、トポロジ内のデバイス、割り当てられたテクノロジー、およびトポロジに設定されている特定のポリシーについての情報が含まれます。概要ページは、VPN トポロジ作成後に自動的に表示されます。エクストラネット VPN を作成する場合、Create Extranet VPN ウィザードの最後のステップとしても表示されます。

VPN トポロジの [VPN Summary] ページを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN トポロジを選択して、[ポリシー（Policies）] リストから [VPNサマリー（VPN Summary）] を選択します。
- （デバイスビュー）VPN に参加するデバイスを選択して、[ポリシー（Policies）] リストから [サイト間VPN（Site-to-Site VPN）] ポリシーを選択します。VPN トポロジを選択して、[VPNポリシーの編集（Edit VPN Policies）] ボタンをクリックします。これにより、そのトポロジが選択された状態で [Site-to-Site VPN Manager] ウィンドウが表示されます。こ

のウィンドウで、[ポリシー（Policies）] リストから [VPNサマリー（VPN Summary）] を選択できます。

次の表に、このページに表示される情報を示します。

（注） 標準 VPN の概要は、エクストラネット VPN の概要とは大きく異なります。このテーブルは 2 つに分かれていて、上半分では標準 VPN の概要が説明されており、下半分ではエクストラネット VPN の概要が説明されています。

表 *335 : [VPN Summary]* ページ

要素	説明
標準 VPN の概要情報	
名前	VPN トポロジの名前。
テクノロジー	VPN トポロジに割り当てられた IPsec テクノロジー。IPsec テクノロジーおよびポリシーについて （1384 ページ）を参照してください。
タイプ（Type）	VPN トポロジ タイプ（[Hub-and-Spoke]、[Point-to-Point]、または [Full Mesh]）。
説明	VPN トポロジの説明。
IPsec Terminator	VPN トポロジが大規模 DMVPN の場合に使用可能です。 大規模 DMVPN のハブ間で GRE トラフィックを負荷分散するために使用される IPsec ターミネータの名前。
Primary Hub	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク トポロジにおけるプライマリ ハブの名前。
Failover Hubs	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク トポロジに設定されたすべてのセカンダリ バックアップ ハブの名前。
Number of Spokes	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク トポロジに含まれるスポークの数。
ピア 1	VPN トポロジ タイプがポイントツーポイントの場合に使用可能です。 ポイントツーポイント VPN トポロジにおいてピア 1 として定義されるデバイスの名前。

要素	説明
ピア 2	VPN トポロジ タイプがポイントツーポイントの場合に使用可能です。 ポイントツーポイント VPN トポロジにおいてピア 2 として定義されるデバイスの名前。
Number of Peers	VPN トポロジ タイプが完全メッシュの場合に使用可能です。 完全メッシュ VPN トポロジに含まれているデバイスの数。
IKE Proposal	VPN トポロジに設定されている IKEv1 プロポーザルのセキュリティ パラメータ。 IKE プロポーザルの設定 （1488 ページ）を参照してください。 （注） IKEv2 プロポーザルは概要に表示されません。
Dynamic VTI	Easy VPN トポロジで使用可能です。 Easy VPN トポロジにおいて、デバイスにダイナミック仮想テンプレート インターフェイスが設定されているかどうかが表示されます。 Easy VPN に対するダイナミック VTI の設定 （1614 ページ）を参照してください。
トランスフォーム セット（Transform Sets）	VPN トンネル内のトラフィックを保護するために使用される認証および暗号化アルゴリズムを指定する IPsec IKEv1 トランスフォーム セット。 サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）を参照してください。 （注） IPsec IKEv2 トランスフォーム セットは概要に表示されません。
事前共有キー（Preshared Key）	選択したテクノロジーが Easy VPN の場合は使用できません。 IKEv1 Preshared Key ポリシーで使用する共有キーがユーザ定義であるか、または自動生成されたものであるかを指定します。 IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。 （注） IKEv2 事前共有キー設定は概要に表示されません。
公開キーインフラストラクチャ	VPN トポロジに IKEv1 Public Key Infrastructure ポリシーが設定されている場合に、Certificate Authority（CA; 認証局）サーバを指定します。 サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。 （注） IKEv2 PKI 設定は概要に表示されません。

要素	説明
ルーティング プロトコル（Routing Protocol）	選択したテクノロジーが IPsec/GRE、GRE ダイナミック IP、または DMVPN の場合にだけ使用可能です。 GRE、GRE ダイナミック IP、または DMVPN ルーティング ポリシーを設定するための、保護された IGP で使用されるルーティング プロトコルおよび自律システム（またはプロセス ID）番号です。 （注） Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、このルーティング プロトコルおよび自律システム（またはプロセス ID）番号を使用して、ルータ プラットフォーム ポリシーを作成する必要があります。 [GRE Modes] ページについて （1575 ページ）を参照してください。
Tunnel Subnet IP	選択したテクノロジーが IPsec/GRE、GRE ダイナミック IP、または DMVPN の場合にだけ使用可能です。 トンネル サブネットが定義されている場合に、一意のサブネット マスクを含む内部トンネル インターフェイス IP アドレスが表示されます。 [GRE Modes] ページについて （1575 ページ）を参照してください。
ユーザー グループ	Easy VPN トポロジで使用可能です。 Easy VPN トポロジ内のデバイスに User Group ポリシーが設定されている場合に、ポリシーの詳細が表示されます。 Easy VPN における User Group ポリシーの設定 （1617 ページ）を参照してください。
PIX7.0/ASA Tunnel Group	Easy VPN トポロジで使用可能です。 Easy VPN トポロジ内の PIX ファイアウォール バージョン 7.0+ または ASA アプライアンスに Connection Profile ポリシーが設定されている場合に、ポリシーの詳細が表示されます。
ハイ アベイラビリティ	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク VPN トポロジ内のデバイスに High Availability ポリシーが設定されている場合に、ポリシーの詳細が表示されます。 VPN トポロジにおけるハイ アベイラビリティの設定 （1450 ページ）を参照してください。
VRF 対応 IPSec	VPN トポロジ タイプがハブアンドスポークの場合に使用可能です。 ハブアンドスポーク VPN トポロジ内のハブに VRF-Aware IPsec ポリシーが設定されている場合に、VRF ソリューションのタイプ（1 ボックスまたは 2 ボックス）および VRF ポリシーの名前が表示されます。 VRF 対応 IPsec の設定 （1445 ページ）を参照してください。

要素	説明
エクストラネット VPN の概要情報	
[IKE Phase 1 Proposal] セクション	エクストラネットに対して割り当てられる IKE Proposal ポリシー オブジェクト内に定義される、IKE フェーズ 1 プロポーザルのパラメータ。設定値については、次のトピックを参照してください。 • [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ） • [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）
[IKE Phase 2 Proposal] セクション	IKE フェーズ 2 プロポーザルのパラメータ。これらのパラメータのほとんどは、エクストラネットに対して割り当てられる IPsec トランスフォーム セット ポリシー オブジェクトで設定されます。説明については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。 Lifetime 属性パラメータは VPN Global Settings ポリシーで定義されます。 VPN グローバル設定 （1517 ページ）を参照してください。Perfect Forward Secrecy パラメータは IPsec Proposal ポリシーで定義されます。サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）を参照してください。
[Authentication] セクション	接続の認証に使用される証明書を定義する事前共有キーまたは PKI 登録ポリシー オブジェクトの名前。 事前共有キーを使用している場合、[キーの表示/非表示（Show/Hide Key）] ボタンをクリックして、キーの表示とマスクを切り替えることができます。概要の印刷または PDF の生成を行う場合、キーはここでの選択内容に応じて表示または非表示になります。
ローカル（Local）	エクストラネット VPN のローカル（管理対象）エンドにあるデバイス。表示名、VPN インターフェイスの名前と IP アドレス、および保護対象ネットワークが含まれます。
リモート（Remote）	エクストラネット VPN のリモート（管理対象外）エンドにあるデバイス。デバイス名、VPN インターフェイスの IP アドレス、および保護対象ネットワークが含まれます。
[Print] ボタン	概要を印刷するには、このボタンをクリックします。事前共有キーは、ページに現在表示されている内容に基づいて、表示または非表示になります。 概要を印刷するには、Adobe Acrobat Reader がインストールされている必要があります。Security Manager は、概要の PDF を生成してから、Acrobat の印刷機能を使用して印刷します。

要素	説明
[Generate PDF] ボタン	概要の PDF を作成するには、このボタンをクリックします。事前共有キーは、ページに現在表示されている内容に基づいて、表示または非表示になります。PDF の保存先のファイル名と場所のプロンプトが表示されます。

関連項目

- IKE プロポーザルの設定 （1488 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）
- IKEv1 事前共有キー ポリシーの設定 （1540 ページ）
- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）
- GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定 （1582 ページ）
- DMVPN の [GRE Modes] の設定 （1590 ページ）
- 大規模 DMVPN の設定 （1595 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- Easy VPN における User Group ポリシーの設定 （1617 ページ）
- Easy VPN における Connection Profile ポリシーの設定 （1616 ページ）
- エクストラネット VPN の作成または編集 （1469 ページ）

エクストラネット VPN の作成または編集

Security Manager は、Security Manager で管理しているデバイスと管理対象外のデバイスの間に通常の IPsec ポイントツーポイント VPN を作成するための簡単な方式を提供します。このタイプの VPN は、エクストラネットと呼ばれます。

通常、エクストラネットは、ご使用のネットワークとパートナーまたはサービスプロバイダーのネットワークの間のサイト間 VPN 接続です。ただし、ユーザーの組織のネットワーク内の VPN 接続であっても、異なるグループにより管理されているデバイス間の VPN 接続、またはシスコ デバイスとシスコ製以外の（Security Manager では管理できない）デバイスの間の VPN 接続の場合もあります。

このタイプのポイントツーポイント VPN トポロジを作成するには、Create Extranet VPN ウィザードを使用します。エクストラネット VPN の作成には、デバイス、VPN トンネルのソースエンドポイントおよび宛先エンドポイントである VPN インターフェイス、およびトンネルで保護される保護対象ネットワークの指定が含まれます。セキュアな接続の完了のために必要な IKE プロポーザル、IPsec プロポーザル、および事前共有キーまたは証明書も指定します。

エクストラネット VPN トポロジを編集する場合、[Edit Extranet VPN] ダイアログボックスには（[IKE Proposal] ページを除いて）Create Extranet VPN ウィザードと同じページが含まれていますが、ウィザード形式ではなく、タブ形式でページがレイアウトされています。ダイアログボックスの任意のタブで [OK] をクリックすると、すべてのタブの定義が保存されます。IKE プロポーザル、IPsec プロポーザル、事前共有キー、および公開キー インフラストラクチャ証明書について、直接ポリシーを編集する必要があります。

ヒント

- VPN デフォルト ポリシーはエクストラネット VPN には適用されません。[Security Manager Administration] の [VPN Defaults] ページで定義された設定は無視されます。エクストラネット VPN 設定で使用する共有ポリシーがある場合は、Create Extranet VPN ウィザードで作成したあとで VPN に割り当てることができます。共有ポリシーを割り当てると、ウィザードで作成されたポリシーと置き換えられます。
- エクストラネット VPN を作成するときに事前定義 IKE プロポーザルまたは IPsec トランスフォーム セット ポリシー オブジェクトを選択することはできません。使用する既存オブジェクトがある場合は、VPN の作成後に関連ポリシーを編集し、オブジェクトを選択できます。その後、必要に応じて、Create Extranet VPN ウィザードで作成されたオブジェクトを削除できます。
- エクストラネット VPN の作成後、そのエクストラネット VPN を、VPN の両方のエンドを Security Manager で管理する標準ポイントツーポイント VPN に変換することはできません。代わりに、VPN を削除してから再作成する必要があります。
- エクストラネット VPN 接続は、通常の IPsec ポイントツーポイント接続に対してのみ設定できます。たとえば、サービスプロバイダーのネットワーク内に存在する GET VPN キー サーバーをこの方式を使用して識別することはできません。その他のすべてのタイプのエクストラネット接続を設定するには、管理対象外デバイスまたは非シスコデバイスの VPN への組み込み （1394 ページ）の説明に従って、Security Manager インベントリにダミーの管理対象外デバイスを追加する必要があります。

関連項目

- VPN トポロジについて （1380 ページ）
- デバイス ビューにおける VPN トポロジの設定 （1405 ページ）
- IPsec テクノロジーおよびポリシーについて （1384 ページ）
- ウィザードの使用 （63 ページ）

ステップ 1 次のいずれかを実行します。

- 新規エクストラネット VPN を作成するには、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）または [サイト間 VPN ポリシー（Site-to-Site VPN Policy）] ページ（デバイスビュー）で、[VPN トポロジの作成（Create VPN Topology）]（+）ボタンをクリックし、[エクストラネット VPN（Extranet VPN）] を選択します。Create Extranet VPN ウィザードが開始され、[Name and Technology] ページが表示されます。

- 既存のエクストラネット VPN を編集するには、[Site-to-Site VPN Manager] ウィンドウまたは [サイト間 VPN ポリシー（Site-to-Site VPN Policy）] ページ（デバイスビュー）で VPN トポロジを選択し、[VPN トポロジの編集（Edit VPN Topology）]（鉛筆）ボタンをクリックします。[Device Selection] タブに対して [Edit Extranet VPN] ダイアログボックスが開きます。

ステップ 2 [Name and Technology] ページまたはタブで、以下を設定します。名前のみが必須です。

- [名前（Name）]：VPN トポロジを識別する一意の名前。
- [説明（Description）]：最大 1024 文字の VPN の説明。
- [作成日（Creation Date）]：VPN が作成された日付。VPN を作成するときは、今日の日付がデフォルトです。ただし、編集ボックスの横のカレンダー アイコンをクリックして、希望する日付を選択できます。
- [チケット番号（Ticket Number）]：チケットシステムを使用していて、実行するアクションが追跡されている要件に関連する場合は、このフィールドに番号を入力します。Security Manager はこの番号を使用しません。内部追跡目的専用です。
- [最終変更者（Last Modified By）]：最後に VPN の設定を変更したユーザーの名前、ユーザー ID、電子メールアドレス、またはその他のインジケータ。Security Manager はこのフィールドを使用しません。内部追跡目的専用です。

ウィザードで、[次へ（Next）] をクリックします。[エクストラネット VPN の編集（Edit Extranet VPN）] ダイアログボックスで、[デバイスの選択（Device Selection）] タブをクリックします。

ステップ 3 [Device Selection] ページまたはタブで、接続の各エンドのデバイス、インターフェイス、および保護対象ネットワークを設定します。

- [ローカル（Local）]：これは、管理対象ネットワーク内のデバイスです。デバイスは、Security Manager インベントリ内にある必要があります。次のプロパティをすべて設定します。
  - [デバイス（Device）]：デバイスの表示名を入力するか、または [選択（Select）] をクリックしてインベントリ内のデバイスをリストから選択します。ASA 5500 シリーズデバイス、PIX ファイアウォール、または Cisco IOS ルータ（ASR を含む）を選択できます。
  - [VPN トンネルインターフェイス（VPN Tunnel Interface）]：VPN 接続の外部インターフェイスを識別するインターフェイスまたはインターフェイスロールの名前。[選択（Select）] をクリックして、既存のインターフェイスまたはインターフェイスロールを選択するか、または新規インターフェイスロールを作成します。

インターフェイスまたはロールを選択するときに、一致するインターフェイスの IP アドレスが [IP アドレス（IP Address）] フィールドの横あるドロップダウンリストにリストされます。バージョン 4.9 以降、Security Manager はエクストラネット VPN の IPv6 アドレスをサポートします。IPv4 アドレスと IPv6 アドレスのリストを表示できます。デフォルトでは IPv4 アドレスが表示されます。アドレスが表示されない場合、Security Manager は IP アドレスを判別できませんでした。設定またはオブジェクト選択内容を確認してください。

- - [保護されたネットワーク（Protected Networks）]：デバイスがこの VPN に対して保護しているネットワーク。[選択（Select）] をクリックして [保護されたネットワークの選択（Protected Network

Selection）] ダイアログボックスを表示します。このダイアログボックスでは、インターフェイス名、インターフェイス ロール オブジェクト、ネットワーク/ホストグループオブジェクト、または ACL オブジェクトを使用して、保護されたネットワークを指定できます。[保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを使用して、新しいネットワーク/ホストグループまたは ACL オブジェクトを定義することもできます。

（注） エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）の説明に従って、ローカルデバイス エンドポイント設定を編集することもできます。設定はこれらに似ていますが、インターフェイス ロール オブジェクトを定義する機能が追加されています。

- [クリプトマップ名（Crypto Map name）] : デバイスのクリプトマップ名を手動で入力できます。デフォルト値はありません。値を入力しない場合、Cisco Security Manager はデバイスのクリプトマップ名を使用するか、新しいクリプトマップ名を生成します。VPN インターフェイスにクリプトマップがすでに存在する場合、Cisco Security Manager は同じ名前を再利用します。
- [クリプト ACL 名（Crypto ACL name）] : デバイスのクリプト ACL 名を手動で入力できます。デフォルト値はありません。値を入力しない場合、Cisco Security Manager は新しいクリプト ACL 名を生成します。
- [クリプトマップシーケンス（Crypto Map Sequence）] : Cisco Security Manager は、管理対象ネットワークでデバイスを検出すると、このフィールドにデバイスのシーケンス番号を表示します。この値は編集できません。新しい VPN トポロジを追加する場合、Cisco Security Manager は [シーケンス番号（Sequence Number）] フィールドに # の値を入力します。この値は編集できません。

詳細については、以下を参照してください。 クリプトマップの設定 （1448 ページ）

- [クリプトモード（Crypto Mode）] : ASA デバイスバージョン 9.6(2) 以降向けの Cisco Security Manager バージョン 4.12 以降では、次のクリプトモードからオプションを選択できます。
  - [トンネル（Tunnel）] : デフォルト値。カプセル化モードがトンネルモードになります。
  - [トランスポート（Transport）] : ピアがサポートしていない場合、カプセル化モードは、トンネルモードにフォールバックするオプション付きのクリプトモードになります。
  - [トランスポート必須（Transport-Require）] : カプセル化モードはトランスポートモードのみになります。トランスポートモードは IKEv2 でのみサポートされています。
- [リモート（Remote）] : これは、Security Manager では管理しないデバイスです。次のプロパティをすべて設定します。
  - [名前（Name）] : デバイスの名前。Security Manager インベントリで使用される表示名に対応しています。
  - [IP アドレス（IP Address）] : デバイスの VPN インターフェイスの IP アドレス。スペースを区切り文字として使用して、最大 10 個の IP アドレスを入力できます。バージョン 4.9 以降、Security Manager は IPv4 アドレスに加えて IPv6 アドレスをサポートします。

（注） バージョン 4.8 以降、Security Manager では、同じエクストラネット VPN 構成に複数のピア IP アドレスを設定できます。これにより、最初のデバイスが VPN サービスに使用できない場合に、リスト内の次のピアデバイスがフェールオーバーとして機能できます。このバックアップピアサポートは、Cisco 適応型セキュリティアプライアンス（ASA）デバイスおよび Cisco IOS ルータで利用できます。

- • [保護されたネットワーク（Protected Networks）]：デバイスがこの VPN に対して保護しているネットワーク。[選択（Select）] をクリックして [保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを表示します。このダイアログボックスでは、ネットワーク/ホストグループオブジェクトまたは ACL オブジェクトを使用して、保護されたネットワークを指定できます。[保護されたネットワークの選択（Protected Network Selection）] ダイアログボックスを使用して、新しいネットワーク/ホストグループまたは ACL オブジェクトを定義することもできます。

（注） エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）の説明に従って、リモートデバイス エンドポイント設定を編集することもできます。ただし、設定値はこれらの設定値と同じであり、インターフェイス名またはインターフェイス ロール オブジェクトを使用して保護対象ネットワークを指定することはできません。

ウィザードで、[次へ（Next）] をクリックします。[Edit VPN] ダイアログボックスで終了します。残りの特性を編集するには、IKE Proposal、IPsec Proposal、IKEv1 Preshared Key、IKEv1 Public Key Infrastructure、IKEv2 Authentication、および VPN Global Settings の各ポリシーを編集して、次のステップで説明されている設定を変更する必要があります。

ステップ 4 Create Extranet VPN ウィザードの [IKE Proposal] ページで、IKE プロポーザル、IPsec プロポーザル、および事前共有キーまたは証明書のいずれかを定義します。

- [IKEv1] または [IKEv2] を選択します。リリース 8.4(1) を実行している ASA 5500 シリーズ デバイスでのみ IKEv2 を使用できます。

エクストラネット VPN を作成したあとで IKE バージョンを変更する場合は、これらのポリシーをすべて編集して以前の設定を割り当て解除または置換し、目的のバージョン（IKE Proposal、IPsec Proposal、IKEv1 Preshared Key、IKEv1 Public Key Infrastructure、IKEv2 Authentication、VPN Global Settings）のオプションを設定する必要があります。IKEv1 と IKEv2 の違いについては、IKE バージョン 1 と 2 の比較 （1481 ページ）を参照してください。

- IKE フェーズ 1 プロポーザルのパラメータを設定します。これらのパラメータは、*ExtranetName*_**ikeBB** という名前の IKE プロポーザル ポリシー オブジェクトの作成に使用されます。パラメータの説明については、[IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）または [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）を参照してください。

VPN を作成したあとでこれらの値を編集する場合は、そのオブジェクトを編集する必要があります。オブジェクトは Policy Object Manager で編集できます。または、VPN の IKE Proposal ポリシーを使用して直接編集できます。

（注） **DH Group** 属性（Diffie-Hellman 係数グループの場合）は、その他のポリシーやポリシーオブジェクトでは **Modulus Group** と呼ばれます。

- IKE フェーズ 2（IPsec）プロポーザルのパラメータを設定します。これらのパラメータのほとんどは、*ExtranetName*_**transformSet** という名前の IPsec トランスフォーム セット ポリシー オブジェクトの作成に使用されます。パラメータの説明については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。AH Hash Algorithm 設定はローカル デバイスがルータである場合にのみ使用できることに注意してください。

VPN を作成したあとでこれらの値を編集する場合は、そのオブジェクトを編集する必要があります。オブジェクトは Policy Object Manager で編集できます。または、VPN の IPsec Proposal ポリシーを使用して直接編集できます。

次の設定は、IPsec トランスフォーム セット オブジェクトには含まれません。

- • [Perfect Forward Secrecy、DH Group の有効化（Enable Perfect Forward Secrecy, DH Group）]：それぞれの暗号化された交換に対して固有のセッションキーを使用するかどうか。固有のセッションキーにより、攻撃者がトンネルの両方のエンドで使用される事前共有キーまたは秘密キーを知っている場合でも、その攻撃者がキャプチャされた交換を復号化できなくなります。このオプションを選択する場合は、キーの導出に使用する Diffie-Hellman（DH）係数グループも選択します。係数グループの詳細については、使用する Diffie-Hellman 係数グループの決定 （1485 ページ）を参照してください。

VPN を作成したあとでこのオプションを変更するには、IPsec Proposal ポリシーを編集します。

- • [ライフタイム（Lifetime）]：セキュリティ アソシエーションの期限切れまでの存在秒数。デフォルトは 3,600 秒（1 時間）です。

VPN を作成したあとでこのオプションを変更するには、VPN Global Settings ポリシーを編集します。

- 認証に [事前共有キー（Preshared Key）] を選択する場合は、リモートホストとの接続の認証に使用するキーを入力します。

VPN を作成したあとでキーを編集するには、ご使用の IKE バージョンに応じて IKEv1 Preshared Key ポリシーまたは IKEv2 Authentication ポリシーのいずれかを編集する必要があります。これらのポリシーではキーはマスクされていますが、[VPN Summary] ポリシーを選択し、事前共有キーの横にある [Show Key] ボタンをクリックすることにより、キーを表示できます。

- [証明書（Certificate）] を選択する場合は、証明書名を定義する PKI 登録オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合は、[<新規追加>（<Add New>）] を選択して [PKI の追加（Add PKI）] セレクタを開きます。そこで、新規 PKI 登録オブジェクトの追加、または既存の PKI 登録オブジェクトの編集を行うことができます。PKI 登録オブジェクトの詳細については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

VPN を作成したあとで証明書設定を編集するには、Policy Object Manager でオブジェクトを編集します。または、ご使用の IKE バージョンに応じて、IKEv1 Public Key Infrastructure ポリシーまたは IKEv2 Authentication ポリシーのいずれかを使用して直接編集します。

ウィザードで、[次へ（Next）] をクリックします。

ステップ 5 （Create Extranet VPN ウィザードのみ）[サマリー（Summary）] ページで、設定が正しいことを確認し、[完了（Finish）] をクリックします。

Security Manager は、トポロジおよび必要なポリシー オブジェクトを作成し、Site-to-Site VPN Manager の VPN のリストに VPN を追加します。

ステップ 6 ダイヤルバックアップを設定する場合は、[ピア（Peers）]ポリシーを選択し、ダイヤルバックアップの設定 （1432 ページ）の説明に従います。

VPN トポロジの削除

VPN トポロジを削除すると、サイト間 VPN に割り当てられているデバイスとネットワークから、ピア間の IPsec トンネルおよび VPN トポロジに関連付けられたすべての設定が削除されます。設定を展開するまでは、ネットワークから実際の VPN は削除されません。

ステップ 1 次のいずれかを実行します。

- [管理（Manage）] > [サイト間 VPN（Site-To-Site VPNs）] を選択して、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開きます。
- デバイスビューで、削除する VPN に参加しているデバイスを選択して、ポリシーセレクタから [サイト間 VPN（Site to Site VPN）] ポリシーを選択します（デバイス ビューにおける VPN トポロジの設定（1405 ページ）を参照）。

ステップ 2 削除する VPN トポロジを選択して、[VPN トポロジの削除（Delete VPN Topology）]（ゴミ箱）ボタンをクリックします。削除の確認が求められます。

第 26 章

IKE および IPsec ポリシーの設定

この章では、インターネットプロトコルセキュリティ（IPSec）および Internet Security Association and Key Management Protocol（ISAKMP または IKE）標準を設定して、サイト間およびリモートアクセス IPsec バーチャルプライベートネットワーク（VPN）を構築する方法について説明します。これらのポリシーは、VPN トンネルを構築するために通常の IPsec および他のタイプの IPsec ベースの VPN テクノロジーで使用されます。

トンネリングは、インターネットなどのパブリック TCP/IP ネットワークを使用して、リモートユーザーとプライベートな企業ネットワークとの間でセキュアな接続を構築することを可能にします。それぞれのセキュアな接続は、トンネルと呼ばれます。

IPsec ベースの VPN テクノロジーは、ISAKMP および IPsec トンネリング標準を使用して、トンネルの構築と管理を行います。ISAKMP と IPsec は、次を実現します。

- トンネル パラメータのネゴシエート。
- トンネルの確立。
- ユーザとデータの認証。
- セキュリティ キーの管理。
- データの暗号化と復号。
- トンネルを経由するデータ転送の管理。
- トンネルエンドポイントまたはルータとしてのインバウンドおよびアウトバウンドのデータ転送の管理。

VPN 内のデバイスは、双方向トンネル エンドポイントとして機能します。プライベートネットワークからプレーンパケットを受信し、それらをカプセル化して、トンネルを作成し、それらをトンネルの他端に送信できます。そこで、カプセル化が解除され、最終宛先へ送信されます。また、パブリック ネットワークからカプセル化されたパケットを受信し、それらをカプセル化解除して、プライベート ネットワーク上の最終宛先に送信することもできます。

ここでは、基本的な IKE および IPsec ポリシーと、その設定方法について説明します。

- IKE および IPsec 設定の概要　（1478 ページ）
- IKE について　（1482 ページ）

- IPsec プロポーザルについて （1499 ページ）
- VPN グローバル設定 （1517 ページ）
- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）
- Public Key Infrastructure ポリシーについて （1544 ページ）
- サイト間 VPN での IKEv2 認証の設定 （1567 ページ）

IKE および IPsec 設定の概要

インターネット キー エクスチェンジ（IKE）は、IPsec ピアを認証し、IPsec 暗号化キーをネゴシエートして配信し、IPsec セキュリティ アソシエーション（SA）を自動的に確立するために使用されるキー管理プロトコルです。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーションでは、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE プロポーザルは、2 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。IKE Version 1（IKEv1; IKE バージョン 1）では、IKE プロポーザルには、単一のアルゴリズム セットと係数グループが含まれています。各ピアにおいて、複数のポリシーをプライオリティ付きで作成して、少なくとも 1 つのポリシーがリモートピアのポリシーに一致するようにできます。IKEv1 と異なり、IKEv2 プロポーザルでは、フェーズ 1 ネゴシエーション中にピアが選択できる複数のアルゴリズムと係数グループを選択できます。これによって、単一の IKE プロポーザルの作成が可能になります（ただし、最も望ましいオプションにより高いプライオリティを設定するために、異なるプロポーザルが必要になる可能性があります）。1 つの VPN あたり複数の IKE プロポーザルを定義できます。

サイト間またはリモート アクセス VPN で通常の IPsec 接続を正常に確立するために必要な設定を定義するよう、いくつかのポリシーを設定する必要があります。次の手順には、設定を行うために必要な手順の概要が示されており、各手順の詳細情報が記載された他のトピックのリンクがあります。

関連項目

- IKE について （1482 ページ）
- IPsec プロポーザルについて （1499 ページ）
- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）
- Public Key Infrastructure ポリシーについて （1544 ページ）

ステップ 1 [IKEプロポーザル（IKE Proposal）] ポリシーを設定します。

[IKE Proposal] ポリシーでは、VPN 接続の確立に使用する IKE プロポーザル ポリシー オブジェクトを定義します。IKE プロポーザル オブジェクトの定義時に、IKE ネゴシエーションの暗号化と完全性チェックに使用するアルゴリズムと、暗号化アルゴリズムの実行に使用するデフィーヘルマン グループを選択します。IKEv1 では、事前共有キーまたは公開キー インフラストラクチャのいずれを使用するかも判別しますが、IKEv2 では、IKE プロポーザルには、認証モードの指定は含まれていません。

ここでは、[IKE Proposal] ポリシーの設定方法について説明します。

- IKE プロポーザルの設定 （1488 ページ）
  - [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）
  - [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）
- GET VPN の IKE プロポーザルの設定 （1638 ページ）

ステップ 2 認証モード設定を行います。

IKEv1 プロポーザルで認証モードに選択した項目、および IKEv2 に使用するよう決定したモードによって、認証モード設定を行うために必要な他のポリシーが制御されます。

- 事前共有キー：リモートアクセス IKEv1 IPsec VPN の場合は、[接続プロファイル（Connection Profiles）] ポリシーで事前共有キーを定義します。事前共有キーは、リモートアクセス VPN の IKEv2 ではサポートされません。サイト間 VPN の場合は、使用している IKE バージョンに基づいて [IKEv1事前共有キー（IKEv1 Preshared Keys）] または [IKEv2認証（IKEv2 Authentication）] ポリシーでキーを定義します。

ここでは、事前共有キー設定について説明します。

- [IPSec] タブ（[Connection Profiles]） （1730 ページ）
- IKEv1 事前共有キー ポリシーの設定 （1540 ページ）
- サイト間 VPN での IKEv2 認証の設定 （1567 ページ）
- 公開キーインフラストラクチャ認証局サーバー：Certificate Authority（CA; 認証局）サーバーを使用するよう IKE を設定する場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーを設定する必要があります。また、このポリシーを使用して、SSL VPN の公開キー インフラストラクチャを定義します。サイト間 VPN の場合は、使用している IKE バージョンに基づいて、ポリシーは [IKEv1公開キーインフラストラクチャ（IKEv1 Public Key Infrastructure）] または [IKEv2認証（IKEv2 Authentication）] です。

[Public Key Infrastructure] ポリシーは、認証局サーバを識別する PKI 登録オブジェクトを特定します。サイト間 VPN の場合は、単一の PKI 登録オブジェクトを選択できます。リモート アクセス VPN の場合は、リモート アクセス接続に必要なすべてのオブジェクトを選択できます。これらのトラストポイントは、（[IPsec] タブにある）リモートアクセスの [接続プロファイル（Connection Profiles）] ポリシーで識別されます。

ここでは、公開キー インフラストラクチャ設定について説明します。

- Public Key Infrastructure ポリシーについて （1544 ページ）
- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）

- サイト間 VPN での複数の IKEv1 CA サーバの定義 （1550 ページ）
- リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）
- [IPSec] タブ（[Connection Profiles]） （1730 ページ）
- サイト間 VPN での IKEv2 認証の設定 （1567 ページ）

ステップ 3 [IPsecプロポーザル（IPsec Proposal）] ポリシーを設定します。[IPsec Proposal] ポリシーは、VPN のセキュアな IPsec トンネルを作成するために使用される IPsec トランスフォーム セット ポリシー オブジェクトを定義します。

ここでは、[IPsec Proposal] ポリシーの設定方法について説明します。

- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）
  - サイト間 VPN におけるデバイスの IKE バージョンの選択 （1509 ページ）
  - IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス） （1759 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス） （1893 ページ）

ステップ 4 [グローバル設定（Global Settings）] ポリシーを設定します。

[グローバル設定（Global Settings）]（リモートアクセス）ポリシーおよび[VPNグローバル設定（VPN Global Settings）]（サイト間）ポリシーは、さまざまな ISAKMP、IKEv1、IKEv2、IPsec、NAT、フラグメンテーション、およびその他の設定を定義します。これらの設定には、多くの場合適切であるデフォルト値があるため、通常はデフォルト以外の動作が必要なときにかぎり [Global Settings] ポリシーを設定する必要があります。ただし、リモートアクセス IKEv2 IPsec VPN ではポリシーを設定する必要があります。これは、[IKEv2設定（IKEv2 Settings）] タブでリモート アクセス グローバル トラストポイントを指定する必要があるためです。

ここでは、[Global Settings] ポリシーの設定方法について説明します。

- VPN グローバル設定 （1517 ページ）
  - VPN グローバル ISAKMP/IPsec 設定 （1520 ページ）
  - VPN グローバル IKEv2 設定 （1526 ページ）
  - VPN グローバル NAT 設定 （1532 ページ）
  - VPN グローバル一般設定 （1534 ページ）
- GET VPN のグローバル設定 （1640 ページ）

ステップ 5 リモート アクセス IKEv2 IPsec VPN を設定する場合は、SSL VPN のいくつかのポリシーも設定する必要があります。IKEv2 は、SSL VPN といくつかの設定を共有します。設定する必要があるその他のポリシーに

ついては、 Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）を参照してください。

IKE バージョン 1 と 2 の比較

IKE には、バージョン 1（IKEv1）とバージョン 2（IKEv2）の 2 つのバージョンがあります。IKEv2 をサポートするデバイスで IKE を設定する場合は、いずれかのバージョンを単独で設定するか、両方のバージョンを一緒に設定するかを選択できます。デバイスが別のピアとの接続のネゴシエーションを試行する場合は、ユーザが許可したバージョンか、他のピアが受け入れるバージョンのどちらでも使用されます。両方のバージョンを許可すると、最初に選択したバージョン（IKEv2 は、設定されている場合は常に最初に試行されます）とのネゴシエーションが正常に行われなかった場合に、デバイスは他のバージョンに自動的にフォールバックします。ネゴシエーションで使用するには、両方のピアが IKEv2 をサポートする必要があります。

ヒント Security Manager は、ASA 8.4(1)+ だけで IKEv2 をサポートします。リモート アクセス IPsec VPN では、ユーザは AnyConnect 3.0+ クライアントを使用して、IKEv2 接続を実行する必要があり、IKEv2 接続は、SSL VPN 接続に使用される同じライセンス プールを使用します。ASA での IKEv1 リモート アクセス接続には従来の VPN クライアントが使用されます。VPN でのデバイス サポートの詳細については、各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）を参照してください。

IKEv2 は、次の方法で IKEv1 とは異なります。

- IKEv2 は、Photuris スタイルのクッキー メカニズムを修正します。
- IKEv2 では、IKEv1 よりも少ないラウンドトリップが行われます（基本的な交換では、IKEv1 の場合の 5 回に対して 2 回のラウンドトリップ）。
- トランスフォームオプションは論理和演算されます。これは、許可される組み合わせごとに別個の固有のプロポーザルを作成するのではなく、単一のプロポーザルで複数のオプションを指定できることを意味します。
- 組み込みの Dead Peer Detection（DPD; デッドピア検知）。
- 組み込みの設定ペイロードとユーザ認証モード。
- 組み込みの NAT Traversal（NAT-T; NAT 通過）。IKEv2 は、NAT-T にポート 500 と 4500 を使用します。
- 向上したキーの再生成とコリジョン処理。
- 単一の Security Association（SA; セキュリティ アソシエーション）は複数のサブネットを保護でき、これによってスケーラビリティが向上します。
- サイト間 VPN での非対称認証。トンネルのそれぞれの側に、異なる事前共有キーと異なる証明書を設定するか、片側にキー、もう片側に証明書を設定できます。

- リモート アクセス IPsec VPN では、リモート アクセス SSL VPN に対して設定する場合と同じ方法で IKEv2 接続に二重認証を設定できます。IKEv1 は二重認証をサポートしません。

関連項目

- IKE および IPsec 設定の概要 （1478 ページ）
- IKE プロポーザルの設定 （1488 ページ）

IKE について

Internet Key Exchange（IKE; インターネット キー交換）は、Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれ、2 つのホストが IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法に合意するためのネゴシエーション プロトコルです。これは、SA 属性のフォーマットに合意するための共通のフレームワークを提供します。これには、SA に関するピアとのネゴシエーション、および SA の変更または削除が含まれます。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーションの自動確立に使用される暗号キーを作成します。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートして、ピアがフェーズ 2 で安全に通信できるようにする最初のトンネルを作成し、その後の ISAKMP ネゴシエーション メッセージを保護します。フェーズ 2 のネゴシエーション中に、IKE によって IPsec などの他のアプリケーション用の SA が確立されます。これによって、ピア間で送信されるデータが保護されます。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。

IKE プロポーザルは、2 つのピア間の IKE ネゴシエーションを保護するためにこれらのピアで使用されるアルゴリズムのセットです。IKE ネゴシエーションは、共通（共有）IKE ポリシーに合意している各ピアによって開始されます。このポリシーは、後続の IKE ネゴシエーションを保護するために使用されるセキュリティ パラメータを示します。リモートアクセス IPsec VPN では、VPN ごとに複数の IKE プロポーザルを定義し、各ピアでポリシーに優先順位を付けて、少なくとも 1 つのポリシーがリモートピアのポリシーと一致するようにできます。サイト間 VPN では、単一の IKE プロポーザルを作成できます。

IKE プロポーザルを定義するには、次の内容を指定する必要があります。

- 一意のプライオリティ（1 ～ 65,543、1 が最高のプライオリティ）。
- データを保護し、プライバシーを確保するための IKE ネゴシエーションの暗号化方式。使用する暗号化アルゴリズムの決定 （1483 ページ）を参照してください。
- 送信者の ID を保証し、メッセージが伝送中に変更されないようにするためのハッシュメッセージ認証コード（HMAC）方式（IKEv2 では整合性アルゴリズムと呼ばれる）。使用するハッシュ アルゴリズムの決定 （1484 ページ）を参照してください。
- IKEv2 では、別個の Pseudo-Random Function（PRF; 疑似乱数関数）をアルゴリズムとして使用して、IKEv2 トンネルの暗号化に必要なキー関連情報とハッシュ操作を取得していま

した。オプションは、ハッシュ アルゴリズムに使用されるものと同じです。使用するハッシュ アルゴリズムの決定 （1484 ページ）を参照してください。

- 暗号化キー判別アルゴリズムの強度を決定する Diffie-Hellman グループ。デバイスは、このアルゴリズムを使用して、暗号化キーとハッシュ キーを派生させます。 使用する Diffie-Hellman 係数グループの決定 （1485 ページ）を参照してください。
- ピアの ID を確認する認証方式。 使用する認証方式の決定 （1486 ページ）を参照してください。
- デバイスが暗号化キーを交換するまでに使用できる時間制限。

（注） [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）

ヒント （ASA デバイスのみ）。IKEv1 ポリシーを使用して、パラメータごとに 1 つの値を設定します。IKEv2 では、複数の暗号化、整合性、PRF、およびデフィーヘルマン オプションを設定できます。ASA は、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを送信することなく、許可されるすべてのトランスフォームを伝送するために単一のプロポーザルを送信できます。

IKE ネゴシエーションが開始されると、ネゴシエーションを開始するピアがそのポリシーすべてをリモート ピアに送信します。リモート ピアは、一致するポリシーがないかどうか、所有するポリシーをプライオリティ順に検索します。

ピアが、暗号化、ハッシュ（IKEv2 の場合は整合性と PRF）、認証、Diffie-Hellman 値を保持し、さらに、送信されたポリシーのライフタイム以下である SA ライフタイムを保持している場合に、IKE ポリシー間に一致が存在します。ライフタイムが等しくない場合は、（リモート ピア ポリシーからの）短い方のライフタイムが適用されます。一致するポリシーがない場合、IKE はネゴシエーションを拒否し、IKE SA は確立されません。

ここでは、IKE プロポーザルの設定方法について説明します。

- IKE プロポーザルの設定 （1488 ページ）
- [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）
- [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）
- GET VPN の IKE プロポーザルの設定 （1638 ページ）

使用する暗号化アルゴリズムの決定

IKE プロポーザルで使用する暗号化およびハッシュ アルゴリズムを決定する場合、VPN 内のデバイスによってサポートされているアルゴリズムだけを選択できます。

次の暗号化アルゴリズムから選択できます。

- Data Encryption Standard（DES; データ暗号規格）は、対称秘密キー ブロック アルゴリズムです。3DES よりも高速であり、使用するシステム リソースも少ないですが、安全性も劣ります。堅牢なデータ機密保持が必要ない場合、およびシステム リソースや速度が重要である場合には、DES を選択します。
- 3DES（トリプル DES）では、毎回異なるキーを使用して各データ ブロックを 3 回処理するため、より安全です。ただし、使用するシステム リソースが多くなり、DES よりも速度が遅くなります。デバイスでサポートされている場合には、3DES 暗号化アルゴリズムを使用することを推奨します。
- AES（Advanced Encryption Standard）は DES よりも安全であり、3DES よりも効率的に計算できます。AES には、128 ビット、192 ビット、256 ビットの 3 種類のキー強度が用意されています。キーが長いほど安全になりますが、パフォーマンスは低下します。ルータで IKE を設定するには、AES を使用するために Cisco IOS ソフトウェア 12.3T 以降をルータで使用する必要があります。

（注） AES は、ハードウェア暗号化カードとともに使用することはできません。

関連項目

- IKE について （1482 ページ）
- IKE プロポーザルの設定 （1488 ページ）

使用するハッシュ アルゴリズムの決定

選択可能なハッシュ アルゴリズムは、次のとおりです。IKEv2 では、ハッシュ アルゴリズムは 2 つのオプションに分かれています。1 つは整合性アルゴリズムに使用され、もう 1 つは擬似乱数関数（PRF）に使用されます。

- Secure Hash Algorithm（SHA; セキュア ハッシュ アルゴリズム）には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。ただし、SHA は MD5 よりもリソース消費量が大きくなります。最大レベルのセキュリティを必要とする実装には、SHA ハッシュ アルゴリズムを使用してください。

標準の SHA では、160 ビットのダイジェストが生成されます。

よりセキュアな次のオプションは、ASA 8.4(2+) デバイスの IKEv2 設定で使用できます。

- SHA512：512 ビット キー
- SHA384：384 ビット キー
- SHA256：256 ビット キー

- MD5（Message Digest 5）では、128 ビットのダイジェストが生成され、SHA よりも処理時間が短く、全体的に高いパフォーマンスを発揮しますが、SHA よりもセキュリティ面で弱くなります。

関連項目

- IKE について （1482 ページ）
- IKE プロポーザルの設定 （1488 ページ）

使用する Diffie-Hellman 係数グループの決定

Security Manager では、IPsec Security Association（SA; セキュリティ アソシエーション）キーを生成するための次のデフィーヘルマン キー導出アルゴリズムがサポートされています。各グループでは、異なるサイズの係数が使用されます。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。両方のピアに、一致する係数グループが存在する必要があります。

ヒント AES 暗号化を選択する場合は、AES で必要な大きいキーサイズをサポートするために、ISAKMP ネゴシエーションで Diffie-Hellman（DH）グループ 5 以降を使用する必要があります。IKEv1 の場合、ASA デバイスはグループ 2 と 5 のみをサポートします。

- Diffie-Hellman グループ 1：768 ビットの係数。768 ビットの素数およびジェネレータ数を使用して IPsec SA キーを生成する場合に使用します。

（注） Cisco Security Manager 4.19 以降、IKEv1 および IKEv2 の DH グループ 1 は、ASA 9.12(1) 以降のデバイスではサポートされません。

- Diffie-Hellman グループ 2：1024 ビットの係数。1024 ビットの素数およびジェネレータ数を使用して IPsec SA キーを生成する場合に使用します。Cisco VPN Client バージョン 3.x 以降では、少なくともグループ 2 が必要です
- Diffie-Hellman グループ 5：1536 ビットの係数。2048 ビットの素数およびジェネレータ数を使用して IPsec SA キーを生成する場合に使用します。128 ビットのキーでは十分な保護レベルですが、グループ 14 の方がより安全です。
- デフィーヘルマン グループ 7：163 文字の楕円曲線フィールド サイズを使用して IPsec SA キーを生成する場合に使用します。グループ 7 は、VPNSM または VPN SPA が設定された Catalyst 6500/7600 デバイスではサポートされていません。
- Diffie-Hellman グループ 14：2048 ビットの係数。128 ビットのキーでは十分な保護レベルです。（ASA 9.0.1 以降のデバイスのみ）。

（注） Cisco Security Manager 4.20 以降では、DH グループ 14 がサポートされており、これが ASA 9.13(1) 以降のデバイスにおける IKEv1 および IKEv2 のデフォルト DH グループです。

- Diffie-Hellman 15：3072 ビットの係数。192 ビットのキーでは十分な保護レベルです。
- Diffie-Hellman グループ 16：4096 ビットの係数。256 ビットのキーでは十分な保護レベルです。

（注） Cisco Security Manager 4.20 以降、DH グループ 15 および 16 は、ASA 9.13(1) 以降のデバイスの IKEv2 でサポートされています。

- Diffie-Hellman グループ 19：（256 ビットの楕円曲線フィールドサイズ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 20：（384 ビットの楕円曲線フィールドサイズ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 21：（521 ビットの楕円曲線フィールドサイズ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 24：（2048 ビット係数および 256 ビット素数位数サブグループ）。（ASA 9.0.1 以降のデバイスのみ）。
- Diffie-Hellman グループ 31：（256 ビットの楕円曲線フィールドサイズ）。（ASA 9.16.1 以降のデバイスのみ）。

関連項目

- IKE について （1482 ページ）
- IKE プロポーザルの設定 （1488 ページ）

使用する認証方式の決定

Security Manager では、VPN 通信でのピア デバイス認証において 2 つの方式がサポートされています。

- [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。各ピアに同じ共有キーを設定する必要があります。同じキーが設定されていない場合は、IKE SA を確立できません。

このデバイス認証方式を使用して IKE を正常に使用するには、さまざまな事前共有キー パラメータを定義する必要があります。詳細については、次の適切なトピックを参照してください。

- サイト間 VPN、IKEv1 設定：IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。
- サイト間 VPN、IKEv2 設定：サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。
- リモート アクセス IPsec VPN、IKEv1：接続プロファイルの [IPsec] タブで設定されています。 [IPSec] タブ（[Connection Profiles]） （1730 ページ）を参照してください。
- リモート アクセス IPsec VPN、IKEv2：リモート アクセス IPSec VPN で IKEv2 を使用する場合は、事前共有キーを使用できません。証明書を使用する必要があります。
- **証明書**：IKE キー管理メッセージを署名および暗号化するために、RSA キーペアが使用される認証方式。証明書によって、2 つのピア間の通信の否認防止を実施します。つまり、実際に通信が行われたことを証明できます。この認証方式を使用する場合は、Certification Authority（CA; 認証局）からデジタル証明書を取得するようにピアを設定します。CA は、証明書要求を管理して、参加する IPsec ネットワーク デバイスに証明書を発行します。これらのサービスは、参加デバイスのキー管理を一元化して行います。

事前共有キーを使用した場合のスケーラビリティは高くありませんが、CA を使用することによって、IPsec ネットワークを容易に管理できるようになり、スケーラビリティが高まります。CA を使用する場合は、すべての暗号化デバイス間でキーを設定する必要がありません。代わりに、参加する各デバイスは CA に登録され、CA に対して証明書を要求します。自身の証明書と CA の公開キーを持つ各デバイスは、その CA のドメイン内にある他のすべてのデバイスを認証できます。

証明書認証方式を使用して IKE を正常に使用するには、CA 認証および登録用のパラメータを定義する必要があります。詳細については、次の適切なトピックを参照してください。

- サイト間 VPN、IKEv1 設定：Public Key Infrastructure ポリシーについて （1544 ページ）を参照してください。
- サイト間 VPN、IKEv2 設定：サイト間 VPN での IKEv2 認証の設定 （1567 ページ）。
- リモート アクセス IPsec VPN、IKEv1：[IPSec] タブ（[Connection Profiles]） （1730 ページ）で説明されているように、接続プロファイルの [IPsec] タブで設定されています。同じトラストポイントを使用して、公開キー インフラストラクチャ ポリシーも設定する必要があります。 Public Key Infrastructure ポリシーについて （1544 ページ）を参照してください。
- リモート アクセス IPsec VPN、IKEv2：VPN グローバル IKEv2 設定 （1526 ページ）で説明されているように、[Global Settings] ポリシーの [IKEv2 Settings] タブでグローバル トラストポイントを設定します。同じトラストポイントを使用して、公開キーインフラストラクチャ ポリシーも設定する必要があります。 Public Key Infrastructure ポリシーについて （1544 ページ）を参照してください。

関連項目

- IKE について （1482 ページ）
- IKE プロポーザルの設定 （1488 ページ）

IKE プロポーザルの設定

Security Manager では、サイト間またはリモート アクセス IPsec VPN を設定する場合は、IKE プロポーザルは必須ポリシーです。設定ウィザードを使用して、新しい IPsec VPN を作成する場合は、[IKE Proposal] ポリシーは VPN に自動的に割り当てられます。ポリシーは出荷時のデフォルトであるか、VPN 専用に選択された共有ポリシーです。Internet Key Exchange（IKE; インターネット キー交換）キー管理プロトコルの詳細については、IKE について （1482 ページ）を参照してください。

[IKE Proposal] ポリシーを使用して、現在の IKE プロポーザルを調べて、GET VPN トポロジを除く新しいプロポーザルを設定します。GET VPN については、 GET VPN の IKE プロポーザルの設定 （1638 ページ）を参照してください。

（注） Cisco Security Manager バージョン 4.17 以降では、ソフトウェアバージョン 9.9(2) 以降を実行している ASA マルチコンテキストデバイスで IKE プロポーザルポリシーを設定および展開できます。

ヒント

- サイト間 VPN では、IKE バージョンごとに最大 1 つの IKE プロポーザルを選択できます。リモート アクセス IPsec VPN では、IKE バージョンごとに複数のプロポーザルを選択できます。リモート アクセス VPN で許可されるすべての IKE プロポーザルを選択します。
- IKEv2（バージョン 2）を設定するには、デバイスは、ASA ソフトウェアリリース 8.4(1) 以降が実行されている ASA である必要があります。
- [IPsec Proposal] ポリシーでは、IKEv1、IKEv2、または両方が、このポリシーで設定する IKE プロポーザルと一致する必要があります。IPsec プロポーザルで IKEv2 を設定できない場合は、Easy VPN トポロジなどでは IKEv2 はサポートされません。詳細については、IPsec プロポーザルについて （1499 ページ）を参照してください。
- [IKEv1 Proposal] オブジェクトでは、認証に事前共有キーと証明書のいずれを使用するのかを指定します。IKEv1 プロポーザルオブジェクトが証明書認証タイプの場合は、IKEv1 公開キー インフラストラクチャ ポリシーで適切な CA サーバーを（ポリシーセレクタから）指定していることを確認します。事前共有キーの場合、IKEv1 事前共有キーポリシーが割り当てられていることを確認します。IKEv2 では、オブジェクトでは、事前共有キーまたは証明書のいずれを使用するのかは指定しませんが、他のポリシーでは認証要件を定義する必要があります。詳細については、使用する認証方式の決定 （1486 ページ）を参照してください。

- 通常の IPSec VTI テクノロジーの場合、IKE プロポーザルの 1 つ（IKEv1 プロポーザルまたは IKEv2 プロポーザル）のみを指定できます。つまり、（[IKEプロポーザル（IKE Proposal）] ウィンドウで）通常の IPSec VTI に IKE バージョン 1 を選択した場合、[IKEv1 プロポーザル（IKEv1 Proposal）] を指定し、[IKEv2プロポーザル（IKEv2 Proposal）] フィールドを空白のままにしておく必要があり、その逆も同様です。

関連項目

- 使用するハッシュ アルゴリズムの決定 （1484 ページ）
- 使用する Diffie-Hellman 係数グループの決定 （1485 ページ）
- 使用する認証方式の決定 （1486 ページ）

ステップ 1 設定する VPN のタイプに基づいて [IKE Proposal] ポリシーを開くには、次のいずれかを実行します。

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IKEプロポーザル（IKE Proposal）]** を選択します。
  - （ポリシービュー）ポリシータイプセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IKEプロポーザル（IKE Proposal）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタでトポロジ（GET VPN 以外）を選択して、ポリシーセレクタで [IKEプロポーザル（IKE Proposal）] を選択します。
  - （ポリシービュー）ポリシータイプセレクタで **[サイト間VPN（Site-to-Site VPN）] > [IKEプロポーザル（IKE Proposal）]** を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

ステップ 2 適切な IKE バージョンに対して [選択（Select）] をクリックして、IKE バージョン 1 またはバージョン 2 プロポーザルの設定を定義するポリシーオブジェクトを選択します。VPN でサポートされる IKE バージョンのプロポーザルだけを設定します。

（注） 4.16 以降、Cisco Security Manager は分散モードの Firepower 9300 デバイスの IKEv1 設定をサポートしていません。

- サイト間 VPN の IKE プロポーザルを選択するには、使用可能なプロポーザル リストで単に強調表示します。リモートアクセス IPsec VPN では、使用可能なプロポーザルリストで必要なオブジェクトを強調表示して、[>>] をクリックして選択したプロポーザルリストに移動します。
- リモートアクセス IPsec VPN の IKE プロポーザルを削除するには、選択したプロポーザルリストで強調表示し、[<<] をクリックして使用可能なプロポーザルリストに移動します。

- 新しいIKEプロポーザルを作成するには、使用可能なプロポーザルリストの下にある [作成（Create）]（+）ボタンをクリックします。[Add IKEv1 or IKEv2 Proposal] ダイアログボックスが開きます。オブジェクトの作成手順については、次のトピックを参照してください。
  - [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）
  - [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）
- オブジェクトを編集するか、オブジェクトの設定を表示するには、そのオブジェクトを選択して、リストの下にある [編集（Edit）]（鉛筆）ボタンをクリックします。

[IKEv1 Proposal] ポリシー オブジェクトの設定

[IKEv1 Proposal] ダイアログボックスを使用して、IKEv1 プロポーザル オブジェクトを作成、コピー、および編集します。

Internet Key Exchange（IKE; インターネット キー交換）バージョン 1 プロポーザル オブジェクトには、リモート アクセス VPN ポリシーおよびサイト間 VPN ポリシーを定義する場合に IKE1 プロポーザルに必要となるパラメータが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーション中に、IKE は、他のアプリケーション（IPsec など）用の Security Association（SA; セキュリティ アソシエーション）を確立します。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKE プロポーザルの詳細については、次の項を参照してください。

- IKE および IPsec 設定の概要 （1478 ページ）
- IKE バージョン 1 と 2 の比較 （1481 ページ）
- IKE について （1482 ページ）
- 使用する暗号化アルゴリズムの決定 （1483 ページ）
- 使用するハッシュ アルゴリズムの決定 （1484 ページ）
- 使用する Diffie-Hellman 係数グループの決定 （1485 ページ）
- 使用する認証方式の決定 （1486 ページ）

ナビゲーション パス

[管理（Manage）] > **[ポリシーオブジェクト（Policy Objects）]** を選択し、オブジェクトタイプセレクタから **[IKE プロポーザル（IKE Proposals）]** > **[IKEv1 プロポーザル（IKEv1 Proposals）]**

を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

ヒント　IKE プロポーザルの設定 （1488 ページ）の説明に従って [IKE Proposal] ポリシーを設定する際に、このダイアログボックスにアクセスすることもできます。

関連項目

- [IKEv2 Proposal] ポリシー オブジェクトの設定 （1494 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- Policy Object Manager （290 ページ）
- IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）

フィールド リファレンス

表 *336 : [IKEv1 Proposal]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。
[プライオリティ（Priority）]	IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 有効な値の範囲は 1 ～ 10000 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、Security Manager によって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。

要素	説明
暗号化アルゴリズム（Encryption Algorithm）	フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズム： • [AES-128]：128 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [DES]：56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。
ハッシュ アルゴリズム（Hash Algorithm）	IKE プロポーザルで使用されるハッシュ アルゴリズム。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。次のオプションがあります。 • SHA (Secure Hash Algorithm)：160 ビットのダイジェストを生成します。SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。

要素	説明
係数グループ（Modulus Group）	2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。次のオプションがあります。 ヒント　IKEv1 の場合、ASA デバイスは DH グループ 14 のみをサポートします。 • [1]：Diffie-Hellman グループ 1（768 ビット係数）。 （注）　Cisco Security Manager 4.19 以降、DH グループ 1 は ASA 9.12(1) 以降のデバイスではサポートされません。デフォルト値はグループ 2 です。 • [2]：Diffie-Hellman グループ 2（1024 ビット係数）。 • [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以降）を使用します。 • [7]：Diffie-Hellman グループ 7（163 ビットの楕円曲線フィールド サイズ）。 • [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。 （注）　Cisco Security Manager 4.20 以降では、DH グループ 14 がサポートされており、これが ASA 9.13(1) 以降のデバイスの IKEv1 のデフォルトの DH グループです。 • [15]：Diffie-Hellman グループ 15（3072 ビット係数。192 ビット キーの保護に推奨される）。 • [16]：Diffie-Hellman グループ 16（4096 ビット係数。256 ビット キーの保護に推奨される）。 （注）　Diffie-Hellman グループ 15 と 16 がリストされていますが、これらは IKEv1 ではサポートされていないため、IKEv1 ポリシーに選択すると検証エラーが発生します。
保存期間（Lifetime）	セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 60 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 です。

要素	説明
認証方式	2 つのピア間で使用する認証方式。設定する必要があるその他のポリシーをこの選択で判別する方法については、使用する認証方式の決定 （1486 ページ）を参照してください。次のいずれかを選択します。 • [事前共有キー（Preshared Key）]：事前共有キーを使用すると、秘密キーを 2 つのピア間で共有したり、認証フェーズ中に IKE で使用したりできます。参加ピアの 1 つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。 • 証明書：IKE キー管理メッセージを署名および暗号化するために、RSA キー ペアが使用される認証方式。この方式によって、2 つのピア間の通信の否認防止が提供されます。つまり、実際に通信が行われたことが証明されます。この認証方式を使用すると、ピアは、Certification Authority（CA; 証明局）からデジタル証明書を取得するように設定されます。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

[IKEv2 Proposal] ポリシー オブジェクトの設定

[IKEv2 Proposal] ダイアログボックスを使用して、IKEv2 プロポーザル オブジェクトを作成、コピー、および編集します。IKEv2 プロポーザルは、ASA ソフトウェア リリース 8.4(1)+ だけで使用できます。

Internet Key Exchange（IKE; インターネット キー交換）バージョン 2 プロポーザル オブジェクトには、リモート アクセス VPN ポリシーおよびサイト間 VPN ポリシーを定義する場合に IKEv2 プロポーザルに必要となるパラメータが含まれています。IKE は、IPsec ベースの通信の管理を簡易化するキー管理プロトコルです。IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec セキュリティ アソシエーション（SA）の自動確立に使用されます。

IKE ネゴシエーションは 2 つのフェーズで構成されています。フェーズ 1 では、2 つの IKE ピア間のセキュリティ アソシエーションをネゴシエートします。これにより、ピアはフェーズ 2 で安全に通信できるようになります。フェーズ 2 のネゴシエーション中に、IKE は、他のアプリケーション（IPsec など）用の Security Association（SA; セキュリティ アソシエーション）を確立します。両方のフェーズで接続のネゴシエーション時にプロポーザルが使用されます。IKEv1 とは異なり、IKEv2 プロポーザルでは、ピアがフェーズ 1 ネゴシエーション中に選択できる複数のアルゴリズムと係数グループを選択できます。IKE プロポーザルの詳細については、次の項を参照してください。

- IKE および IPsec 設定の概要 （1478 ページ）
- IKE バージョン 1 と 2 の比較 （1481 ページ）
- IKE について （1482 ページ）

- 使用する暗号化アルゴリズムの決定 （1483 ページ）
- 使用するハッシュ アルゴリズムの決定 （1484 ページ）
- 使用する Diffie-Hellman 係数グループの決定 （1485 ページ）

ヒント IKEv1 とは異なり、IKE プロポーザルで認証方式を指定しません。IKEv2 での認証方式の設定方法に関する詳細については、使用する認証方式の決定 （1486 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [IKEプロポーザル（IKE Proposals）] > [IKEv2プロポーザル（IKEv2 Proposals）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

ヒント IKE プロポーザルの設定 （1488 ページ）の説明に従って [IKE Proposal] ポリシーを設定する際に、このダイアログボックスにアクセスすることもできます。

関連項目

- [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- Policy Object Manager （290 ページ）
- IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）

フィールド リファレンス

表 *337 : [IKEv2 Proposal]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

要素	説明
[プライオリティ（Priority）]	IKE プロポーザルのプライオリティ値。このプライオリティ値によって、共通のセキュリティ アソシエーション（SA）の検出試行時に、ネゴシエーションする 2 つのピアを比較することで、IKE プロポーザルの順序が決定します。リモート IPsec ピアが、最初のプライオリティ ポリシーで選択されているパラメータをサポートしていない場合、デバイスは、次に低いプライオリティ番号を持つポリシーで定義されているパラメータの使用を試行します。 有効な値の範囲は 1 ～ 65535 です。値が小さいほど、プライオリティが高くなります。このフィールドをブランクのままにすると、Security Manager によって、まだ割り当てられていない最も小さい値が割り当てられます。値は 1 から始まり、次は 5 となり、その後は 5 ずつ増加します。
暗号化アルゴリズム（Encryption Algorithm）	フェーズ 2 ネゴシエーションを保護するためのフェーズ 1 SA の確立に使用される暗号化アルゴリズム。[選択（Select）] をクリックして、VPN で許可するすべてのアルゴリズムを選択します。 • [AES-GCM-256]：256 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（9.0.1+ を実行している ASA 5580 および ASA 5500-X シリーズ デバイスのみ）。 • [AES-GCM-192]：192 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（9.0.1+ を実行している ASA 5580 および ASA 5500-X シリーズ デバイスのみ）。 • [AES-GCM]：128 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（9.0.1+ を実行している ASA 5580 および ASA 5500-X シリーズ デバイスのみ）。 • [AES-256]：256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES]：128 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。 • [DES]：56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [Null]：暗号化アルゴリズムなし。

要素	説明
Integrity (Hash) Algorithm	IKE プロポーザルで使用するハッシュ アルゴリズムの整合性部分。このハッシュ アルゴリズムによって、メッセージの整合性の確保に使用されるメッセージ ダイジェストが作成されます。[選択（Select）] をクリックして、VPN で許可するすべてのアルゴリズムを選択します。 （注） AES-GCM、AES-GCM-192、または AES-GCM-256 を使用している場合は、整合性アルゴリズムとして Null を選択する必要があります。 • SHA（セキュア ハッシュ アルゴリズム）：SHA には、総当たり攻撃に対して、MD5 よりも高い耐性が備えられています。 標準の SHA では、160 ビットのダイジェストが生成されます。 よりセキュアな次のオプションは、ASA 8.4(2+) デバイスの IKEv2 設定で使用できます。 • SHA512：512 ビット キー • SHA384：384 ビット キー • SHA256：256 ビット キー • [MD5 (Message Digest 5)]：128 ビットのダイジェストを生成します。MD5 では、処理時間が SHA よりも少なくなります。 • [Null]：暗号化アルゴリズムなし。AES-GCM、AES-GCM-192、および AES-GCM-256 でのみ使用します。
Prf Algorithm	IKE プロポーザルで使用するハッシュ アルゴリズムの Pseudo-Random Function（PRF; 疑似乱数関数）部分。IKEv1 では、整合性と PRF アルゴリズムは別ですが、IKEv2 では、これらの要素に異なるアルゴリズムを指定できます。[選択（Select）] をクリックして、VPN で許可するすべてのアルゴリズムを選択します。オプションについては、上記の整合性アルゴリズムの項で説明されています。

要素	説明
係数グループ（Modulus Group）	2 つの IPsec ピア間の共有秘密キーを互いに送信することなく取得するために使用する Diffie-Hellman グループ。係数が大きいほどセキュリティが強化されますが、処理時間が長くなります。2 つのピアに、一致する係数グループが設定されている必要があります。[選択（Select）] をクリックして、VPN で許可するすべてのグループを選択します。 • [1]：Diffie-Hellman グループ 1（768 ビット係数）。 （注） Cisco Security Manager 4.19 以降、DH グループ 1 オプションは、ASA 9.12(1) 以降のデバイスではサポートされません。 • [2]：Diffie-Hellman グループ 2（1024 ビット係数）。 • [5]：Diffie-Hellman グループ 5（1536 ビット係数。128 ビット キーの保護に推奨されるが、グループ 14 の方がより強力）。AES 暗号化を使用する場合は、このグループ（またはそれ以降）を使用します。 • [14]：Diffie-Hellman グループ 14（2048 ビット係数。128 ビット キーの保護に推奨される）。（ASA 9.0.1 以降のデバイスのみ）。 （注） Cisco Security Manager 4.20 以降では、DH グループ 14 がサポートされており、これが ASA 9.13(1) 以降のデバイスにおける IKEv1 のデフォルト DH グループです。 • [15]：Diffie-Hellman グループ 15（3072 ビット係数。192 ビット キーの保護に推奨される）。（ASA 9.13.1 以降のデバイスのみ）。 • [16]：Diffie-Hellman グループ 16（4096 ビット係数。256 ビット キーの保護に推奨される）。（ASA 9.13.1 以降のデバイスのみ）。 • [19]：Diffie-Hellman グループ 19（256 ビットの楕円曲線フィールド サイズ）。（ASA 9.0.1 以降のデバイスのみ）。 • [20]：Diffie-Hellman グループ 20（384 ビットの楕円曲線フィールド サイズ）。（ASA 9.0.1 以降のデバイスのみ）。 • [21]：Diffie-Hellman グループ 21（521 ビットの楕円曲線フィールド サイズ）。（ASA 9.0.1 以降のデバイスのみ）。 • [24]：Diffie-Hellman グループ 24（2048 ビット係数および 256 ビット素数位数サブグループ）。（ASA 9.0.1 以降のデバイスのみ）。 • [31]：Diffie-Hellman グループ 31（256 ビットの楕円曲線フィールドサイズ）。（ASA 9.16.1 以降のデバイスのみ）。

要素	説明
保存期間（Lifetime）	セキュリティ アソシエーション（SA）のライフタイム（秒数）。このライフタイムを超えると、SA の期限が切れ、2 つのピア間で再ネゴシエーションを行う必要があります。一般的に、一定の限度に達するまで、ライフタイムが短いほど、IKE ネゴシエーションがセキュアになります。ただし、ライフタイムが長いと、今後の IPsec セキュリティ アソシエーションのセットアップが、短いライフタイムの場合よりも迅速に行われます。 120 ～ 2147483647 秒の値を指定できます。デフォルトは 86400 です。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

IPsec プロポーザルについて

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルは、2 つのピア間のセキュアな論理通信パスです。ピアは、サイト間 VPN 内のデバイスまたはリモート アクセス IPsec VPN 内のデバイスとユーザが考えられます。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

IPsec プロポーザルは、IKE について （1482 ページ）で説明されているように、IKE ネゴシエーションのフェーズ 2 で使用されます。プロポーザルの特定のコンテンツは、トポロジ タイプ（サイト間またはリモート アクセス）とデバイス タイプによって異なりますが、プロポーザルは大まかには似ていて、IPsec トランスフォーム セットなど、同じ要素を多数含んでいます。

次の項では、IPsec プロポーザルの概念と手順についてより詳細に説明します。

- サイト間 VPN の IPsec プロポーザルについて （1500 ページ）
  - クリプト マップについて （1500 ページ）
  - トランスフォーム セットの概要 （1501 ページ）
  - 逆ルート注入について （1503 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）
- IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）（1759 ページ）

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）

サイト間 VPN の IPsec プロポーザルについて

IPsec は、VPN を設定する場合の最も安全な方法の 1 つです。IPsec では、IP パケット レベルでのデータ暗号化が提供され、標準規格に準拠した堅牢なセキュリティ ソリューションが提供されます。基本 IPsec 設定では、ルーティング プロトコルを使用できません。作成されるポリシーは、基本 IPsec のプロビジョニングに使用されます。基本 IPsec は、Cisco IOS ルータ、PIX ファイアウォール、Catalyst VPN サービス モジュール、および Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスに設定できます。

IPsec では、データはトンネルを介してパブリック ネットワーク経由で送信されます。トンネルとは、2つのピア間のセキュアで論理的な通信パスです。IPsec トンネルを通過するトラフィックは、トランスフォーム セットと呼ばれるセキュリティ プロトコルとアルゴリズムの組み合わせによって保護されます。

Security Manager では、[IPsec Proposal] ポリシーを使用して、IPsec トンネルに必要な設定を定義します。IPsec プロポーザルとは、デバイスの VPN インターフェイスに適用される 1 つ以上のクリプト マップの集合です。クリプト マップには、トランスフォーム セットを含む、IPsec セキュリティ アソシエーションを設定するために必要なすべてのコンポーネントが含まれています。クリプト マップでは、Reverse Route Injection（RRI; 逆ルート注入）を設定することもできます。

詳細については、次の項を参照してください。

- クリプト マップについて （1500 ページ）
- トランスフォーム セットの概要 （1501 ページ）
- 逆ルート注入について （1503 ページ）

関連項目

- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）

クリプト マップについて

クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA を定義するために必要なその他のパラメータを含む、IPsec Security Associations（SA; セキュリティ アソシエーション）を設定するために必要なすべてのコンポーネントが組み合わされています。クリプト マップ エントリは、一連の CLI コマンドに名前が付けられた形式になっています。同じクリプト マップ名および異なるマップ シーケンス番号を持つ複数のクリプト マップ エントリは、1 つのクリプト マップ セットにグループ化されて、関連するデバイスの VPN インターフェイスに適用されます。インターフェイスを通過するすべての IP トラフィックは、適用されたクリプト マップ セットに対して評価されます。

2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップエントリが必要です。クリプトマップエントリに定義されたトランスフォームセットは、そのクリプトマップの IPsec ルールによって指定されたデータフローを保護するための IPsec セキュリティ ネゴシエーションで使用されます。

不明なリモート ピアがローカル ハブとの間の IPsec セキュリティ アソシエーションの開始を試みた場合、ダイナミック クリプト マップ ポリシーがサイト間 VPN で使用されます。ハブは、セキュリティ アソシエーション ネゴシエーションを開始できません。ダイナミック暗号ポリシーを使用することによって、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間で IPsec トラフィックを交換できます。ダイナミック クリプト ポリシーは、個別のハブ、またはハブを含むデバイス グループに作成できます。このポリシーは、ハブに対してだけ書き込まれ、グループにスポークが含まれていてもスポークには書き込まれません。実質的には、ダイナミック暗号マップ ポリシーによって、すべてのパラメータが設定されていない暗号マップエントリが作成されます。設定されていないパラメータは、IPsec ネゴシエーションの結果として、リモート ピアの要件に合うようにあとで動的に設定されます。ダイナミック クリプト マップまたはスタティック クリプト マップのピア アドレスは、VPN トポロジから推定されます。

ダイナミック クリプト マップ ポリシーは、ハブアンドスポーク VPN 設定にだけ適用されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、スタティック クリプト マップ ポリシーだけを適用できます。

（注） （サイト間 VPN）エクストラネット VPN を除き、Security Manager は、トンネルのピアが Security Manager によって管理されている場合だけ、既存の VPN トンネルを管理できます。このような場合、Security Manager では、ピアにおいてトンネルに同じクリプトマップ名が使用されます。以降の展開においては、Security Manager トンネルだけが管理されます（Security Manager では、設定されたすべてのトンネルのログが保持されます）。

関連項目

- IPsec プロポーザルについて （1499 ページ）
- トランスフォーム セットの概要 （1501 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）

トランスフォーム セットの概要

トランスフォームセットとは、IPsec トンネル内のトラフィックを保護するためのセキュリティ プロトコルおよびアルゴリズムの組み合わせです。IPsec Security Association（SA：セキュリティ アソシエーション）のネゴシエーション中に、ピアでは、両方のピアに共通するトランスフォーム セットが検索されます。そのようなトランスフォーム セットは、検出されると適用され、そのクリプトマップのアクセス リストでデータ フローを保護する SA が作成され、VPN でトラフィックが保護されます。

IKEv1 と IKEv2 には別個の IPsec トランスフォーム セットがあります。IKEv1 トランスフォームセットを使用して、パラメータごとに 1 つの値を設定します。IKEv2 トランスフォームセットでは、単一のプロポーザルに複数の暗号化アルゴリズムと統合アルゴリズムを設定できます。ASA デバイスは、設定をセキュア度が最も高いものから最も低いものに並べ替え、その順序を使用してピアとのネゴシエーションを行います。これによって、IKEv1 と同様に、許可される各組み合わせを個別に送信することなく、許可されるすべての組み合わせを伝送するために単一のプロポーザルを送信できます。

1 つの IPsec プロポーザル ポリシーごとに複数のトランスフォーム セットを指定できます。スポークまたはスポークのグループに対してポリシーを定義する場合は、通常、複数のトランスフォームセットを指定する必要はありません。これは、スポークに割り当てられたハブが、通常はより高性能なルータであり、スポークがサポートするすべてのトランスフォームセットをサポートできるためです。ただし、ハブでダイナミック クリプトに関してポリシーを定義している場合は、ハブと不明なスポークとの間でトランスフォームセットが一致するように、複数のトランスフォーム セットを指定する必要があります。選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。

Security Manager には、トンネル ポリシーで使用できる定義済みのトランスフォーム セットが用意されています。独自のトランスフォームセットを作成することもできます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。

IKEv1 トランスフォーム セットのトンネル モードの選択

IKEv1 トランスフォーム セットを定義する場合は、使用する IPsec の動作モード（トンネル モードまたはトランスポート モード）を指定する必要があります。AH プロトコルおよび ESP プロトコルを使用して、IP ペイロード全体を保護するか（トンネル モード）、IP ペイロードの上位層プロトコルだけを保護（トランスポート モード）できます。

トンネル モード（デフォルト）では、元の IP データグラム全体が暗号化され、その暗号化されたデータが新しい IP パケットのペイロードとなります。このモードでは、ルータは IPsec プロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元のルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先のルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの主な利点は、終端システムを変更しなくても IPsec を利用できる点です。また、トンネル モードを使用すると、トラフィック分析に対しても保護されます。トンネル モードを使用した場合、攻撃者は、トンネルのエンドポイントだけを特定できます。トンネルを通過するパケットの送信元と宛先がトンネルのエンドポイントと同じである場合でも、攻撃者はそのパケットの実際の送信元と宛先を特定できません。

トランスポート モードでは、IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。このモードの利点は、各パケットに追加されるのが数バイトだけである点です。また、パブリック ネットワーク上のデバイスは、パケットの実際の送信元と宛先を確認できます。ただし、IP ヘッダーがクリア テキストで渡されるため、トランスポート モードでは、攻撃者が一定のトラフィック分析を実行できます。たとえば、攻撃者は、会社の CEO が他のシニアエグゼクティブに多数のパケットを送信したタイミングを把握できます。ただし、攻撃者が把握できるのは、IP パケットが送信されたという事実だけです。パケットの内容は解読でき

ません。トランスポート モードでは、フローの宛先は IPsec 終端デバイスである必要があります。

（注） 通常の IPsec または Easy VPN を使用して、VPN トポロジにトランスポート モードを使用することはできません。

関連項目

- IPsec プロポーザルについて （1499 ページ）
- クリプト マップについて （1500 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）

逆ルート注入について

リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。保護されているこれらのホストおよびネットワークは、リモート プロキシ アイデンティティと呼ばれます。各ルートは、リモート プロキシ ネットワークとマスクを基にして作成され、リモート トンネル エンドポイントがこのネットワークへのネクスト ホップとなります。リモート VPN ルータをネクストホップとして使用することによって、トラフィックは強制的に暗号プロセスを通して暗号化されます。

VPN ルータでスタティック ルートが作成されたあと、この情報がアップストリーム デバイスに伝播されます。これにより、アップストリーム デバイスでは、IPsec 状態フローを維持するためのリターン トラフィックの送信先として適切な VPN ルータを特定できるようになります。この機能は、サイトで複数の VPN ルータを使用してロード バランシングやフェールオーバーを提供している場合や、デフォルト ルート経由でリモート VPN デバイスにアクセスできない場合に特に便利です。ルートは、グローバル ルーティング テーブルまたは適切な Virtual Routing and Forwarding（VRF）テーブルに作成されます。

（注） VRF 対応 IPsec が設定されている場合、Security Manager によって、ハイ アベイラビリティ（HA）が設定されているデバイスや IPsec Aggregator に自動的に RRI が設定されます。リモートアクセス VPN 内のデバイスのクリプトマップに RRI を設定することもできます。

Security Manager では、逆ルート注入を設定する場合に次のオプションを使用できます。

- ダイナミック クリプトマップでは、ルートは、リモートプロキシの IPsec Security Association（SA;セキュリティ アソシエーション）が正常に確立されたときに作成されます。リモート プロキシへのネクスト ホップは、リモート VPN ルータ経由となります。リモート VPN ルータのアドレスは、ダイナミック クリプト マップ テンプレートの作成中に学習および適用されます。ルートは、SA が削除されたあとに削除されます。

- [Remote Peer] オプション（IOS デバイスでだけ使用可能）を使用すると、リモート VPN デバイスへの明示的なネクストホップとして、インターフェイスまたはアドレスを指定できます。2 つのルートが作成されます。1 つめのルートは標準的なリモート プロキシ アイデンティティであり、ネクスト ホップはリモート VPN クライアントのトンネル アドレスとなります。2 つめのルートは、再帰検索において「ネクストホップ」経由でリモートエンドポイントに到達できることが強制される場合のリモート トンネル エンドポイントへの実際のルートです。実際のネクストホップ用の 2 つめのルートを作成することは、デフォルトルートをより明示的なルートで上書きする必要がある場合に VRF 対応 IPsec で非常に重要となります。

（注） VPN Services Module（VPNSM; VPN サービス モジュール）を使用するデバイスでは、ネクスト ホップはクリプト マップが適用されるインターフェイス、サブインターフェイス、または VLAN となります。リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）（1759 ページ）および リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）を参照してください。

- [Remote Peer IP]（IOS デバイスでだけ使用可能）の場合、ユーザ定義のネクスト ホップを経由したリモート プロキシへのルートが 1 つ作成されます。暗号化された発信パケットを適切に送信するために、ネクスト ホップを使用してデフォルト ルートを上書きできます。このオプションを使用すると、作成されるルートの数を減らすことができます。また、このオプションでは、ルート再帰を容易に使用できないプラットフォームがサポートされます。

関連項目

- IPsec プロポーザルについて （1499 ページ）
- クリプト マップについて （1500 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）

サイト間 VPN での IPsec プロポーザルの設定

[IPsec Proposal] ページを使用して、Easy VPN トポロジを除いて、サイト間 VPN トポロジの IKE フェーズ 2 ネゴシエーション中に使用される IPsec プロポーザルを設定します。

Easy VPN トポロジで使用される IPsec プロポーザルと、リモート アクセス VPN で使用される IPsec プロポーザルは、ここで説明する基本的なサイト間プロポーザルとは大幅に異なります。これらの他のトポロジで使用される IPsec プロポーザルについては、次の項を参照してください。

- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）（1759 ページ）

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタで Easy VPN 以外のトポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。必要に応じて、[IPsecプロポーザル（IPsec Proposal）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタで **[サイト間VPN（Site-to-Site VPN）] > [IPsecプロポーザル（IPsec Proposal）]** を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

関連項目

- IKE について （1482 ページ）
- サイト間 VPN の IPsec プロポーザルについて （1500 ページ）

フィールド リファレンス

表 *338 : [IPsec Proposal]* ページ、サイト間 *VPN*（*Easy VPN* を除く）

要素	説明
Crypto Map Type （ハブアンドスポーク トポロジと完全メッシュ トポロジだけ）	クリプト マップには、IPsec Security Association（SA; セキュリティ アソシエーション）を設定するために必要なすべてのコンポーネントが組み合わされています。2 つのピアが SA を確立しようとする場合は、それぞれに少なくとも 1 つの互換クリプト マップ エントリが必要です。詳細については、クリプトマップについて （1500 ページ）を参照してください。 生成するクリプト マップのタイプを選択します。 • [スタティック（Static）]：スタティック クリプト マップは、ポイントツーポイントまたは完全メッシュ VPN トポロジで使用します。 • [Dynamic]：ダイナミック クリプトマップは、ハブアンドスポーク VPN トポロジでだけ使用できます。ダイナミック クリプトマップ ポリシーを使用すると、ハブがリモートピアのアイデンティティを把握していない場合でも、リモートピアはローカルハブとの間で IPsec トラフィックを交換できます。

要素	説明
Enable IKEv1 Enable IKEv2	IKE ネゴシエーション中に使用する IKE バージョン。IKEv2 は、ASA ソフトウェア リリース 8.4(x) だけでサポートされます。同様に、4.16 以降、Cisco Security Manager は分散モードで構成された Firepower 9300 デバイスの IKEv1 構成をサポートしていません。必要に応じて、いずれかまたは両方のオプションを選択します。トポロジ内のデバイスが IKEv2 をサポートしない場合は、IKEv1 を選択する必要があります。 ハブアンドスポーク トポロジまたは完全メッシュ トポロジで両方のオプションを選択すると、Security Manager は、デバイスで使用される OS のタイプとバージョンに基づいて IKE バージョンをデバイスに自動的に割り当てます。これらの割り当てを変更するには、[IKEバージョン（IKE Version）] タブをクリックして、[IKEv1対応ピア（IKEv1 Enabled Peers）] または [IKEv2対応ピア（IKEv2 Enabled Peers）] の下にある [選択（Select）] ボタンをクリックして、デバイスに割り当てられているバージョンを変更します。各バージョンをサポートするデバイスだけについて割り当てを変更できます。他のデバイスは選択できません。詳細については、サイト間 VPN におけるデバイスの IKE バージョンの選択 （1509 ページ）を参照してください。
トランスフォーム セット（Transform Sets） IKEv2 トランスフォーム セット	トンネルポリシーで使用するトランスフォームセット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。トランスフォーム セットは、各 IKE バージョンで異なるため、サポートされているバージョンごとにオブジェクトを選択します。それぞれ最大 11 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要 （1501 ページ）を参照してください。 選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォームセット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。 （注） IKEv1 トランスフォームセットでは、トンネル モードまたはトランスポート モードの IPsec 動作を使用できます。ただし、IPsec または Easy VPN トポロジではトランスポート モードを使用できません。

要素	説明
Perfect Forward Secrecy の有効化（Enable Perfect Forward Secrecy） 係数グループ（Modulus Group）	暗号化された交換ごとに一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS）を使用するかどうかを指定します。固有のセッション キーを使用することで、後続の復号から交換が保護されます。また、交換全体が記録されていて、攻撃者がエンドポイント デバイスで使用されている事前共有キーや秘密キーを入手している場合であっても保護されます。 このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッションキーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （1485 ページ）を参照してください。 （注） DH グループ 1 は廃止され、以降の ASA バージョンで削除されます。以降の ASA バージョンでは、デフォルト値はグループ 2 になります。
Lifetime (sec) ライフタイム（KB）（Lifetime (kbytes)）	暗号化 IPsec Security Association（SA; セキュリティ アソシエーション）のグローバルなライフタイム設定。IPsec ライフタイムは、秒、KB、またはその両方で指定できます。 • [Seconds (sec)]：SA が期限切れになるまでに存続できる秒数。デフォルトは 3600 秒（1 時間）です。 • [Kilobytes (kbytes)]：特定の SA が期限切れになる前にその SA を使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。有効な値は、デバイス タイプに応じて異なります。入力できる値の範囲は、IOS ルータでは 10 ～ 2147483647、ASA/PIX7.0+ デバイスでは 2560 ～ 536870912 です。 デフォルト値は 4,608,000 KB です。
QoS Preclassify	7600 デバイスを除く Cisco IOS ルータでサポートされます。 選択されている場合、トンネリングおよび暗号化実行前にパケットを分類できます。 VPN の Quality of Service（QoS）機能を使用すると、インターフェイスで Cisco IOS QoS サービスとトンネリングおよび暗号化を同時に実行できます。出力インターフェイスの QoS 機能によって、データが暗号化およびトンネリングされる前にパケットが分類されて、適切な QoS サービスが適用されます。これにより、輻輳した環境でのトラフィック フローの調整が可能となり、より効率的なパケットのトンネリングを実現できます。

要素	説明
Reverse Route	ASA デバイス、PIX 7.0+ デバイス、および 7600 デバイス以外の Cisco IOS ルータでサポートされます。 リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入について （1503ページ）を参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None）]：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]（ASA、PIX 7.0 以降、IOS デバイス）：クリプトマップアクセス制御リスト（ACL）に定義された宛先情報に基づいてルートを作成します。これがデフォルトのオプションです。 • [リモートピア（Remote Peer）]（IOS デバイスのみ）：リモートエンドポイント用に 1 つ、クリプトマップが適用されるインターフェイス経由でのリモートエンドポイントへのルート再帰用に 1 つ、合計 2 つのルートを作成します。 • [リモートピアIP（Remote Peer IP）]：アドレスをリモート VPN デバイスへの明示的なネクストホップとして指定します。IP アドレス、またはアドレスを指定するネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックして、リストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） ネットワークまたはホストオブジェクトを使用する場合は、オブジェクトで [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択し、必要に応じて、このオブジェクトを使用する特定のデバイスの IP アドレスをオーバーライドできます。
動的RRIの有効化（Enable Dynamic RRI）	（注） このオプションは、ASA 9.7(1) 以降でサポートされています。これは、IKEV2 が有効になっているか、静的クリプトマップが選択されている場合にのみ適用されます。 有効にすると、設定中はクリプトマップによって逆ルートはインストールされず、IPsec セキュリティ アソシエーション（SA）が起動するまで延期されます。
ESPv3 設定（ASA 9.0.1 以降のみ） 着信 ICMP エラーメッセージの検証先（暗号化マップまたはダイナミック暗号化マップ）を指定し、セキュリティ単位のアソシエーションポリシーを設定するか、トラフィックフローパケットを有効にします。	

要素	説明
着信ICMPのエラーメッセージを検証（Validate incoming ICMP error messages）	IPsec トンネル経由で受信し、プライベートネットワーク上の内部ホストが宛先である ICMP エラーメッセージを検証するかどうかを指定します。
フラグメント禁止ポリシーを有効にする（Enable Do Not Fragment (DF) Policy）	IP ヘッダーに Do-Not-Fragment（DF）ビットセットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。次のいずれかを実行します。 • 設定（Set）：DF ビットを設定して使用します。 • コピー（Copy）：DF ビットを保持します。 • クリア（Clear）：DF ビットを無視します。
トラフィック フロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）	トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。 （注） TFC を有効にする前に、[トンネルポリシー（クリプトマップ）（Tunnel Policy (Crypto Map)）] の [基本（Basic）] タブで IKE v2 IPsec プロポーザルを設定しておく必要があります。IKEv1 が有効になっている場合、トラフィックフローの機密性は利用できません。 バースト、ペイロードサイズ、およびタイムアウト パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

サイト間 VPN におけるデバイスの IKE バージョンの選択

[IPsec Proposal] ページで [IKE Version] タブを使用して、ハブアンドスポークまたは完全メッシュ サイト間 VPN でデバイスごとに使用する IKE のバージョンを選択します。このタブは、Site-to-Site VPN Manager だけで表示されます。ポリシー ビューではオプションを設定できません。これらのオプションは、VPN トポロジ内の実際のデバイスに固有であるためです。

[IKE Version] タブには、[IKEv1 Enabled Peers] と [IKEv2 Enabled Peers] の 2 つのリストが含まれています。サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）の説明に従って IPsec プロポーザルを設定する際に、VPN で許可する IKE バージョン（バージョン 1、バージョン 2、または両方）を選択します。Security Manager は、デバイスによって使用される OS バージョンに基づいてデバイスに使用する IKE バージョンを自動的に選択します。たとえば、IOS ルータは、[IKEv1 Enabled Peers] リストに常に表示されます。デバイスで IKEv1 と IKEv2 の両方がサポートされる場合は、両方のリストに表示されます。

選択を変更する必要があるのは、VPN で両方の IKE バージョンを許可していて、一部の IKEv2 対応デバイスがいずれかの IKE バージョンを使用するのを明示的に防止する場合だけです。

デバイスで許可する IKE バージョンを変更するには、デバイスを削除する（または以前に削除したデバイスを追加する）リストの下にある [選択（Select）] ボタンをクリックします。次の作業を行うことができる選択ダイアログボックスが開きます（選択を確認するには、[OK] をクリックします）。

- デバイスを削除して、IKE バージョンを使用できなくするには、[選択されたピア（Selected Peers）] リストでそのデバイスを強調表示して、[<<] をクリックして [使用可能なピア（Available Peers）] リストに移動します。
- デバイスを追加して、IKE バージョンの使用を許可するには、[使用可能なピア（Available Peers）] リストでそのデバイスを強調表示して、[>>] をクリックして [選択されたピア（Selected Peers）、] リストに移動します。

ヒント　単一のバージョンをサポートするデバイスのバージョン選択は変更できないため、選択リストには、両方の IKE バージョンをサポートするデバイスだけが含まれています。IKEv2 は、ASA ソフトウェア 8.4(1)+ でサポートされます。

ナビゲーション パス

（[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタで non-Easy VPN 以外のトポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。[IKEバージョン（IKE Version）] タブをクリックします。

関連項目

- IKE について （1482 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）

IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定

[Add IPSec Transform Set]/[Edit IPSec Transform Set] ダイアログボックスを使用して、IKE ネゴシエーションで使用する IPSec トランスフォーム セットを設定します。

サイト間 VPN およびリモート アクセス VPN における IPSec 保護トラフィックを定義するときに、IPSec プロポーザルに使用する IPSec トランスフォーム セット オブジェクトを作成できます。IPSec セキュリティ アソシエーションのネゴシエーション中、ピアは、特定のデータ フローを保護する場合に特定のトランスフォーム セットを使用することを合意します。

2 つの異なるセキュリティ プロトコルが、IPSec 標準に含まれています。

- [Encapsulating Security Protocol (ESP)]：認証、暗号化、およびアンチリプレイの各サービスを提供します。ESP は、IP プロトコル タイプ 50 です。

- [Authentication Header (AH)]：認証サービスとアンチリプレイ サービスを提供します。AH では暗号化が提供されず、通常は、ESP の方が優先されます。また、ルータだけでサポートされます。AH は、IP プロトコル タイプ 51 です。

（注） IPSec トンネルで暗号化と認証の両方を使用することを推奨します。

IKE バージョン（IKEv1 または IKEv2）に基づいて、別個の IPsec トランスフォーム セット オブジェクトがあります。

- IPSec IKEv1 トランスフォーム セット オブジェクトを作成する場合、IPSec が動作するモードを選択し、必要な暗号化タイプおよび認証タイプを定義します。また、トランスフォームセットに圧縮を含めるかどうかを選択できます。アルゴリズムに単一のオプションを選択できるため、VPN で複数の組み合わせをサポートするには、複数の IPsec IKEv1 トランスフォーム セット オブジェクトを作成する必要があります。
- IPSec IKEv2 トランスフォーム セット オブジェクトを作成する際に、VPN で許可するすべての暗号化アルゴリズムとハッシュ アルゴリズムを選択できます。IKEv2 ネゴシエーション中に、ピアは、それぞれでサポートされる最適なオプションを選択します。

（注） デバイスで IPsec IKEv1 または IKEv2 プロポーザルを設定する場合は、そのデバイスに設定されたプロポーザルを使用する必要があります。たとえば、サイト間（ポイントツーポイント）VPN 構成では、IPsec プロポーザルで構成されたエンドポイント（インターフェイス）をクリプトマップの生成に使用できます。ただし、設定されたプロポーザルが Security Manager によってそのデバイスに使用されない場合、後続の設定のプレビューでは、Security Manager は negate コマンドを生成し、設定された IPsec プロポーザルは Security Manager によって否定されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、オブジェクトタイプセレクタから **[IPSecトランスフォームセット（IPSec Transform Sets）] > [IPSec IKEv1トランスフォームセット（IPSec IKEv1 Transform Sets）]**、または **[IPSec トランスフォームセット（IPSec Transform Sets）] > [IPSec IKEv2トランスフォームセット（IPSec IKEv2 Transform Sets）]** を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- トランスフォーム セットの概要 （1501 ページ）
- IKE および IPsec 設定の概要 （1478 ページ）
- IKE バージョン 1 と 2 の比較 （1481 ページ）

- IKE について （1482 ページ）
- IPsec プロポーザルについて （1499 ページ）
- [IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス） （1761 ページ）
- IPsec Proposal Editor（IOS、PIX 6.3 デバイス） （1895 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）（1759 ページ）
- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）
- サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- [IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *339 : [IPSec IKEv1 or IKEv2 Transform Set]* ダイアログボックス

要素	説明
名前	ポリシー オブジェクトの名前。最大 128 文字を使用できます。
説明	ポリシー オブジェクトの説明。最大 1024 文字を使用できます。

要素	説明
[モード（Mode）] （IKEv1 のみ）	IPSec トンネルが動作するモード： • [Tunnel]：トンネルモードによって、IP パケット全体がカプセル化されます。IPSec ヘッダーが、元の IP ヘッダーと新しい IP ヘッダーとの間に追加されます。これがデフォルトです。 トンネルモードは、ファイアウォールの背後にあるホストとの間で送受信されるトラフィックをファイアウォールが保護する場合に使用します。トンネルモードは、インターネットなどの非信頼ネットワークを介して接続されている 2 つのファイアウォール（またはその他のセキュリティ ゲートウェイ）間で通常の IPSec が実装される標準の方法です。 • [Transport]：トランスポート モードでは、IP パケットの上位層プロトコルだけがカプセル化されます。IPSec ヘッダーは、IP ヘッダーと上位層プロトコル ヘッダー（TCP など）との間に挿入されます。 トランスポート モードでは、送信元ホストと宛先ホストの両方が IPSec をサポートしている必要があります。また、トランスポート モードは、トンネルの宛先ピアが IP パケットの最終宛先である場合にだけ使用されます。一般的に、トランスポート モードは、レイヤ 2 またはレイヤ 3 のトンネリング プロトコル（GRE、L2TP、DLSW など）を保護する場合にだけ使用されます。

要素	説明
ESP 暗号化（ESP Encryption）	

要素	説明
	トランスフォーム セットが使用する Encapsulating Security Protocol（ESP; カプセル化セキュリティ プロトコル）暗号化アルゴリズム。次のオプションの詳細については、使用する暗号化アルゴリズムの決定 （1483 ページ）を参照してください。 IKEv1 では、次のいずれかのオプションを選択します。IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。 （注） AES-GCM/GMAC は、5580 以降の ASA プラットフォームでのみ設定できます。 • （空白）：ESP 暗号化を使用しません。 • [DES]：56 ビット キーを使用するデータ暗号規格に従って暗号化を実行します。 • [3DES]：56 ビット キーを使用して暗号化を 3 回実行します。3DES は DES よりも強力なセキュリティを確保しますが、暗号化と復号化に多くの処理を必要とします。AES に比べるとセキュリティは低くなります。このオプションを使用するには 3DES のライセンスが必要です。 （注） バージョン 4.22 以降、Cisco Security Manager は、IPsec IKEv1 プロポーザルの DES および 3DES ESP 暗号化アルゴリズムをサポートしません。これらは、現代の脅威に対して安全であると見なされなくなったためです。 • [AES-128 (AES)]：128 ビットキーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-192]：192 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [AES-256]：256 ビット キーを使用する高度暗号化規格に従って暗号化を実行します。 • [ESP-Null (NULL)]：ヌル暗号化アルゴリズム。[ESP-Null] を使用して定義されたトランスフォーム セットでは、暗号化なしの認証を提供します。一般的に、テスト目的にだけ使用されます。 • [AES-GCM]（IKEv2のみ）：128 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（ASA 9.0.1 以降のデバイスのみ）。 • [AES-GCM-19]（IKEv2のみ）：192 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（ASA 9.0.1 以降のデバイスのみ）。 • [AES-GCM-256]（IKEv2のみ）：256 ビットキーを使用する Galois/Counter モードの高度暗号化規格に従って暗号化を実行します（ASA 9.0.1 以降の

要素	説明
	デバイスのみ）。 • [AES-GMAC]（IKEv2のみ）：128 ビットキーを使用する高度暗号化規格 Galois メッセージ認証コードに従って暗号化を実行します • [AES-GMAC-192]（IKEv2のみ）：192 ビットキーを使用する高度暗号化規格 Galois メッセージ認証コードに従って暗号化を実行します • [AES-GMAC-256]（IKEv2のみ）：256 ビットキーを使用する高度暗号化規格 Galois メッセージ認証コードに従って暗号化を実行します
ESP Hash Algorithm (IKEv1) ESP Integration Algorithm (IKEv2) AH Hash Algorithm (IKEv1 only)	認証のためにトランスフォームセットで使用するハッシュアルゴリズムまたは整合性アルゴリズム。IKEv1 の場合、デフォルトでは、ESP 認証用の SHA を使用し、AH認証は使用しません。IKEv2には、デフォルトはありません。AH ハッシュ アルゴリズムは、ルータだけで使用されます。 IKEv1 では、次のいずれかのオプションを選択します。IKEv2 では、[選択（Select）] をクリックして、サポートするすべてのオプションを選択できるダイアログボックスを開きます。 • [None]：ESP または AH 認証を実行しません。 • [SHA, SHA-1 (Secure Hash Algorithm version 1)]：160 ビットのダイジェストを生成します。SHA は、総当たり攻撃に対して、MD5 よりも高い耐性がありますが、より長い処理時間を必要とします。 よりセキュアな次のオプションは、ASA 8.4(2+) デバイスの IKEv2 設定で使用できます。 • SHA512：512 ビット キー • SHA384：384 ビット キー • SHA256：256 ビット キー • MD5 (Message Digest 5)：128 ビットのダイジェストを生成します。MD5 では、SHA よりも処理時間が短くなりますが、セキュリティは低くなります。 • [Null]：暗号化アルゴリズムなし。AES-GCM、AES-GCM-192、AES-GCM-256、AES-GMAC、AES-GMAC-192、および AES-GMAC-256 でのみ使用します。
圧縮 （IKEv1 だけ、IOS デバイスだけ）	Lempel-Ziv-Stac（LZS）アルゴリズムを使用して IPSec トンネル内のデータを圧縮するかどうかを指定します。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用（304 ページ） を参照してください。

VPN グローバル設定

リモート アクセスまたはサイト間 VPN トポロジ内のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネット キー交換）、IKEv2、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、ほとんどの場合、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合や、リモート アクセス IPsec VPN で IKEv2 ネゴシエーションをサポートする場合だけ設定します

（注） サイト間 VPN の [VPN Global Settings] ポリシーは、GET VPN を除くすべてのテクノロジーに適用されます。GET VPN のグローバル設定の説明については、GET VPN のグローバル設定 （1640 ページ）を参照してください。

ステップ 1 設定する VPN のタイプに基づいてグローバル設定ポリシーを開くには、次のいずれかを実行します。

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）]** を選択します。
  - （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。
  - （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

ステップ 2 必要なタブを選択して、必要に応じて設定を行います。

- [ISAKMP/IPsec設定（ISAKMP/IPsec Settings）]：IKE と IPsec のグローバル設定を行います。オプションの詳細については、 VPN グローバル ISAKMP/IPsec 設定 （1520 ページ）を参照してください。

- [IKEv2設定（IKEv2 Settings）]：IKE バージョン 2 ネゴシエーションのグローバル設定を行います。オプションの詳細については、VPN グローバル IKEv2 設定 （1526 ページ）を参照してください。
- [NAT設定（NAT Settings）]：NAT の動作を設定します。オプションの詳細については、VPN グローバル NAT 設定 （1532 ページ）を参照してください。VPN での NAT について （1530 ページ）も参照してください。
- [アドレス割り当て（Address Assignment）]：リモートクライアントへのアドレス割り当ての 方法を 1 つ以上指定するには、VPN グローバルアドレス割り当て設定の設定 （1518 ページ）を参照してください。アドレスの割り当ては、リモートアクセス VPN にのみ適用されます。
- [全般設定（General Settings）]：フラグメンテーションの動作とその他の一部の各種オプションを設定します。オプションの詳細については、VPN グローバル一般設定 （1534 ページ）を参照してください。

VPN グローバルアドレス割り当て設定の設定

[VPN グローバル設定（VPN Global Settings）]ページの [アドレス割り当て（Address Assignment）] タブを使用して、リモートクライアントへのアドレス割り当ての方法を 1 つ以上指定します。使用可能な方法は次のとおりです。

- 認証サーバーから IP アドレスを取得します。
- DHCP サーバーから IP アドレスを取得します。
- 内部設定されたプールから IP アドレスを取得します。

（注） ASA ソフトウェアバージョン 7.0(1) 以降を実行しているデバイスでアドレス割り当てを設定できます。デフォルトでは、すべての方法が有効になっています。

アドレス割り当ては、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [グローバル設定（Global Settings）] を選択します。[アドレス割り当て（Address Assignment）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [グローバル設定（Global Settings）] を選択します。既存のポリシーを選択するか新しいポリシーを作成して、[アドレス割り当て（Address Assignment）] タブをクリックします。

関連項目

- VPN グローバル設定 （1517 ページ）

フィールド リファレンス

表 *340 : [VPN* グローバル設定（*VPN Global Settings*）*]* ページ、*[*アドレス割り当て（*Address Assignment*）*]* タブ

要素	説明
[IPv4 アドレス割り当ての優先順位（IPv4 Address Assignment Priority）]	
[認証サーバーを使用する（Use Authentication Server）]	認証サーバーから取得した IPv4 アドレスをユーザー単位で割り当てる場合は、オンにします。IPv4 アドレスが設定された認証サーバー（外部または内部）を使用している場合は、この方式を使用することを推奨します。このオプションをオンにする場合は、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA] ポリシーを使用して、ユーザーアクセスの認証に使用する AAA サーバーグループを定義します。この方法は IPv4 および IPv6 の割り当てポリシーに使用できます。
DHCP を使用する	DHCP サーバーから IP アドレスを取得する場合に選択します。DHCP を使用する場合は、デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP サーバー（DHCP Server）] を使用してサーバーを設定する必要があります。また、DHCP サーバーで使用可能な IP アドレスの範囲も定義する必要があります。この方法は IPv4 の割り当てポリシーに使用できます。
[内部アドレスプールを使用する（Use internal address pools）]	内部設定されたプールから IPv4 アドレスを割り当てる場合は、オンにします。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、IP アドレスプールを設定する必要があります。IP アドレスプールを設定するには、デバイスビューで、デバイスポリシーセレクタから [NAT] > [アドレスプール（Address Pools）] を選択します。または、ポリシービューで、ポリシータイプセレクタから [NAT（PIX/ASA/FWSM）] > [アドレスプール（Address Pools）] を選択し、共有ポリシーセレクタから既存のポリシーを選択するか、[アドレスプール（Address Pools）] を右クリックして新しいポリシーを作成します。

要素	説明
[IP アドレスが解放されてから - 分後に IP アドレスの再利用を許可する（Allow the reuse of an IP address - minutes after it is released）]	IP アドレスがアドレスプールに返された後、IP アドレスの再利用を遅らせます。遅延時間を設けることにより、IP アドレスがすぐに再割り当てされることによって発生する問題がファイアウォールで生じないようにできます。デフォルトでは、これはチェックされません。つまり、ASA は遅延時間を課しません。遅延を追加する場合は、チェックボックスをオンにし、IP アドレスを再割り当てするまでの時間を 0 ～ 480 の範囲で指定します。 （注） この機能は、ASA ソフトウェアバージョン 8.0(3) 以降を実行しているデバイスで使用できます。
[IPv6 アドレス割り当ての優先順位（IPv6 Address Assignment Priority）]：バージョン 9.0 以降を実行している ASA デバイスの場合は Security Manager 4.12 以降	
[認証サーバーを使用する（Use Authentication Server）]	認証サーバーから取得した IPv6 アドレスをユーザー単位で割り当てる場合は、オンにします。IPv6 アドレスが設定された認証サーバー（外部または内部）を使用している場合は、この方式を使用することを推奨します。このオプションをオンにする場合は、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA] ポリシーを使用して、ユーザーアクセスの認証に使用する AAA サーバーグループを定義します。
[内部アドレスプールを使用する（Use internal address pools）]	内部設定されたプールから IPv6 アドレスを割り当てる場合は、オンにします。内部的に設定されたアドレス プールは、最も設定が簡単なアドレス プール割り当て方式です。この方法を使用する場合は、IP アドレスプールを設定する必要があります。IPv6 アドレスプールを設定するには、デバイスビューで、デバイスポリシーセレクタから [NAT] > [アドレスプール（Address Pools）] を選択します。または、ポリシービューで、ポリシータイプセレクタから [NAT（PIX/ASA/FWSM）] > [アドレスプール（Address Pools）] を選択し、共有ポリシーセレクタから既存のポリシーを選択するか、[アドレスプール（Address Pools）] を右クリックして新しいポリシーを作成します。

VPN グローバル ISAKMP/IPsec 設定

[VPN Global Settings] ページの [ISAKMP/IPsec Settings] タブを使用して、Internet Key Exchange（IKE; インターネット キー交換）および IPsec のグローバル設定を指定します。

Internet Key Exchange（IKE; インターネット キー交換）プロトコルは、Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれ、2 つのホスト間で IPsec セキュリティ アソシエーションの構築方法について合意するためのネゴシエーション プロトコルです。各 ISAKMP ネゴシエーションは、フェーズ 1 とフェーズ 2 の 2 段階に分けられます。フェーズ 1

では、ISAKMP ネゴシエーション メッセージを保護する最初のトンネルが作成されます。フェーズ 2 では、データを保護するトンネルが作成されます。

ISAKMP ネゴシエーションの条件を設定するために、IKE プロポーザルを作成します。詳細については、IKE プロポーザルの設定 （1488 ページ）を参照してください。

IKE キープアライブについて

IKE キープアライブでは、トンネル ピア間で、トンネル経由でデータを送受信できることを示すメッセージが交換されます。キープアライブ メッセージは、設定された間隔で送信されます。この時間内にメッセージが送信されない場合は、バックアップ デバイスを使用して新しいトンネルが作成されます。

耐障害性を確保するために IKE キープアライブを使用しているデバイスでは、他の情報を交換しているかどうかにかかわらず、キープアライブ メッセージが送信されます。そのため、これらのキープアライブ メッセージによって、若干ではあるものの追加の負荷がネットワークにかかります。

キープアライブ（DPD）と呼ばれる IKE キープアライブのバリエーションでは、着信トラフィックを受信しておらず、発信トラフィックを送信する必要がある場合にだけ、ピア デバイス間でキープアライブ メッセージが送信されます。発信トラフィックがあるかどうかにかかわらず、着信トラフィックを受信していない場合に DPD キープアライブ メッセージを送信する場合は、[Periodic] オプションを使用してこのことを指定します。

ナビゲーション パス

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）] を選択します。[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタから、[Remote Access VPN] > [Global Settings] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しいポリシーを作成し、[ISAKMP/IPsec設定（ISAKMP/IPsec Settings）] タブをクリックします。

関連項目

- VPN グローバル設定 （1517 ページ）

- IKE について （1482 ページ）
- IPsec プロポーザルについて （1499 ページ）

フィールド リファレンス

表 *341 : [VPN Global Settings]* ページ、*[ISAKMP/IPsec Settings]* タブ

要素	説明
ISAKMP 設定（ISAKMP Settings）	
Enable Keepalive	Dead-Peer Detection（DPD; デッドピア検知）設定を行うかどうかを指定します。ピアが応答に失敗する場合は、ピアが使用できなくなっていることを前提に新しいトンネルが構築されます。IKE キープアライブは、ハブアンドスポーク VPN トポロジ内のスポーク、ポイントツーポイント VPN トポロジ内の両方のデバイス、またはリモート アクセス VPN 設定に定義します。 次のオプションを設定します。 • [Interval]：キープアライブのモニタリングを開始するまでピアがアイドル状態を維持できる秒数。範囲は 10 ～ 3600 秒です。デフォルトは 10 ですが、リモート アクセス グループの ASA デバイスのデフォルトは 300 です。 • [Retry]：キープアライブ応答が受信されなくなった後のリトライ間の間隔（秒単位）。範囲は、ASA では 2 ～ 10 秒で、IOS デバイスでは 2 ～ 60 です。デフォルト値は 2 秒です。 • [Periodic]：（IOS ソフトウェアバージョン 12.3(7)T 以降を実行しているルータ、7600 デバイスを除く）IPsec トラフィックに関係なく、一定の間隔で DPD キープアライブメッセージを送信するかどうか。これによって、間隔値が使用される方法が変更されます。 • [Infinite]：（ASA のみ）間隔と再試行設定を無視するかどうか、およびピアを無制限にアイドル状態にできるかどうか。

要素	説明
ID（Identity）	フェーズ I の IKE ネゴシエーション中に、ピアは相互に識別する必要があります。次のいずれかを選択します。 • [Address]：ISAKMP アイデンティティ情報を交換するホストの IP アドレスを使用します。これがデフォルトです。 • [Hostname]：ISAKMP アイデンティティ情報を交換するホストの完全修飾ドメイン名を使用します。 • [Auto/DN]：デバイス タイプに基づいて自動選択または識別名を使用します。 • [Distinguished Name]（IOS デバイスだけ）：Distinguished Name（DN; 識別名）を使用して、ユーザ グループ名を識別します。 • [Auto]（ASA デバイスだけ）：接続タイプによって ISAKMP ネゴシエーションを決定します。事前共有キーに対しては IP アドレスを、証明書認証に対しては識別名を使用します。
SA Requests System Limit	Cisco IOS ソフトウェア リリース 12.3(8)T 以降を実行しているルータ（7600 ルータを除く）でサポートされます。 IKE が SA 要求の拒否を開始する前に許可される SA 要求の最大数。0 ～ 99999 です。ピアの数以上の値を指定する必要があります。ピアの数未満の値を指定した場合は、VPN トンネルが切断される可能性があります。
SA Requests System Threshold	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 IKE が新規 SA 要求の拒否を開始する前に使用できるシステム リソースのパーセンテージ。デフォルトは 75% です。
アグレッシブ モードの有効化（Enable Aggressive Mode） （サイト間 VPN だけ）	ASA デバイスおよび PIX 7.0+ デバイスでサポートされます。 選択されている場合、ISAKMP ネゴシエーションでアグレッシブ モードを使用できます。アグレッシブ モードは、デフォルトでイネーブルになっています。
IPsec 設定	

要素	説明
Enable Lifetime	サイト間またはリモートアクセスVPNのデバイスでクリプトIPsec Security Association（SA; セキュリティ アソシエーション）のグローバル ライフタイム設定を行えるようにする場合は、これを選択します。次を設定します。 • [Lifetime (secs)]：セキュリティ アソシエーションが期限切れになるまでに存続できる秒数。デフォルトは 3,600 秒（1 時間）です。 • [Lifetime (kbytes)]：特定のセキュリティ アソシエーションが期限切れになるまでにそのセキュリティ アソシエーションを使用して IPsec ピア間を通過できるトラフィック量（KB 単位）。デフォルトは 4,608,000 KB です。
Xauth Timeout	リモート アクセス VPN トポロジと Easy VPN トポロジの Cisco IOS ルータおよび Catalyst 6500/7600 デバイスだけでサポートされます。 システムが Xauth チャレンジに応答するまでにデバイスが待機する秒数。 リモート アクセスまたは Easy VPN 設定内に IPsec トンネルを確立するためにトンネル パラメータをネゴシエートする場合、Xauth によって、IPsec 接続を要求するユーザを識別する別の認証レベルが追加されます。Xauth 機能を使用すると、クライアントは IKE SA の確立後、「ユーザ名/パスワード」（Xauth）チャレンジを待機します。エンドユーザがチャレンジに応答すると、その応答は IPsec ピアに転送され、さらに上のレベルの認証が行われます。
最大セッション数（Max Sessions）	ASA デバイスおよび PIX 7.0+ デバイスでサポートされます。 デバイスで同時にイネーブルにできる Security Association（SA; セキュリティ アソシエーション）の最大数。最大数は、デバイス モデルによって異なります。ASA デバイスでは制限は次のとおりです。 • 5505：10 セッション。 • 5510：250 セッション。 • 5520：750 セッション。 • 5540、5550、5585-X（SSP）：10 ～ 5000 セッション。 • 5580、5585-X（その他のモデル）：10000 セッション。

要素	説明
Enable IPsec via Sysopt	ASA デバイスおよび PIX ファイアウォール バージョン 6.3 または 7.0+ でサポートされます。 VPN インターフェイスで VPN トラフィックに対して定義されているアクセス ルールをバイパスするかどうか。 デフォルトでは、デバイスによって VPN トラフィックをインターフェイスで終端させることが許可されています。IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストで許可する必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスのインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端されたため、この機能によって、設定が簡略化され、デバイスのパフォーマンスはセキュリティ リスクを負うことなく最大化されます。（グループ ポリシーおよびユーザー単位の認可アクセス リストは、引き続きトラフィックに適用されます）。 このオプションの選択を解除すると、インターフェイス アクセス ルールが VPN トラフィックにも適用されます。アクセス リストは、ローカル IP アドレスに適用され、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。適用されるコマンドは **no sysopt connection permit-vpn** です。
Enable IPsec inner routing lookup （ASA デバイス 9.6(2) 以降の Security Manager バージョン 4.12 以降）	IPSec 内部パケットに対してパケット単位のルーティングルックアップをイネーブルにします。このチェックボックスは、デフォルトでは選択解除されています。
Enable SPI Recovery （サイト間 VPN だけ）	IOS バージョン 12.3(2)T 以降を実行するルータ、およびバージョン 12.2(18)SXE 以降を実行する Catalyst 6500/7600 デバイスでサポートされます。 選択されている場合、SPI リカバリ機能で、Security Parameter Index（SPI; セキュリティ パラメータ インデックス）が無効であっても IKE SA が開始されるようにデバイスを設定できるようになります。 SPI は、宛先 IP アドレスおよびセキュリティ プロトコルを組み合わせて、特定のセキュリティ アソシエーションを一意に識別する番号です。IKE を使用してセキュリティ アソシエーションを確立する場合、各セキュリティ アソシエーションの SPI は、疑似乱数によって導出された番号となります。IKE を使用しない場合、SPI は、手動で各セキュリティ アソシエーションに指定されます。IPsec パケット処理中に無効な SPI が検出された場合は、SPI リカバリ機能によって、IKE SA が確立されます。

要素	説明
ESPv3 設定（ESPv3 Settings）	
Enable PMTU (Path Maximum Transmission Unit) Aging	ASA デバイスバージョン 9.0.1 以降の IKEv2 でサポートされます。 パスの最大伝送ユニットのエージングをイネーブルにするかどうか。 このオプションを選択した場合、PMTU 値が元の値にリセットされる間隔を分単位で設定します。値は 10 ～ 30 分で設定できます。デフォルトは 10 分です。

VPN グローバル IKEv2 設定

[VPN Global Settings] ページの [IKEv2 Settings] タブを使用して、Internet Key Exchange（IKE; インターネット キー交換）バージョン 2 のグローバル設定を指定します。これらの設定は、ASA 8.4(x) デバイスだけに適用されます。

Internet Key Exchange（IKE; インターネット キー交換）は、Internet Security Association and Key Management Protocol（ISAKMP）とも呼ばれ、2 つのホストが IPsec Security Association（SA; セキュリティ アソシエーション）の構築方法に合意するためのネゴシエーション プロトコルです。

IKEv2 オープン SA を制限することで DoS 攻撃を防止

着信 Security Association（SA; セキュリティ アソシエーション）のクッキー チャレンジを常に行うか、オープンな SA の数を制限して追加の接続のクッキー チャレンジを行うことによって、IPsec IKEv2 接続の Denial of Service（DoS; サービス拒否）攻撃を防止できます。デフォルトでは、ASA は、オープンな SA の数を制限せず、SA のクッキー チャレンジを行うことはありません。

許可される SA の数を制限することもできます。これによって、接続がさらにネゴシエーションされないようにして、クッキー チャレンジ機能が阻止できない可能性があるメモリまたは CPU 攻撃から保護します。SA の最大数を制限すると、現在の接続を保護できます。

DoS 攻撃では、攻撃者は、ピア デバイスが SA 初期パケットを送信し、ASA がその応答を送信すると攻撃を開始しますが、ピア デバイスはこれ以上応答しません。ピア デバイスがこれを継続的に行うと、応答を停止するまで ASA で許可されるすべての SA 要求を使用できます。

クッキー チャレンジのしきい値パーセンテージをイネーブルにすると、オープンな SA ネゴシエーションの数が制限されます。たとえば、デフォルト設定の 50 % では、許可される SA の 50 % がネゴシエーション中（オープン）のときに、ASA は、到着した追加の SA 初期パケットのクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5580 では、5000 個の SA がオープンになると、その後すべての着信 SA のクッキー チャレンジが行われます。

[ネゴシエーションでの最大SA数（Maximum SAs in Negotiation）] オプションとともに使用する場合は、低いクッキーチャレンジしきい値を設定します。

ナビゲーション パス

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）]** を選択します。[IKEv2設定（IKEv2 Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[IKEv2設定（IKEv2 Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[IKEv2設定（IKEv2 Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しい共有ポリシーを作成し、[IKEv2設定（IKEv2 Settings）] タブをクリックします。

関連項目

- VPN グローバル設定 （1517 ページ）
- IKE について （1482 ページ）
- IPsec プロポーザルについて （1499 ページ）
- グループのロードバランスポリシーの設定（ASA） （1711 ページ）

フィールド リファレンス

表 342 : [VPN Global Settings] ページ、[IKEv2 Settings] タブ

要素	説明
Maximum SAs	デバイスで許可される IKEv2 接続（セキュリティ アソシエーション）の数。デフォルトの制限は、デバイス ライセンスによって指定された接続の最大数で、これはデバイス モデルによって異なります。 デバイス ライセンスよりも低い制限を作成する場合にかぎり、数を指定します。範囲は 1 ～ 10000 です。

要素	説明
Maximum SAs in Negotiation	許可される最大の Security Association（SA; セキュリティ アソシエーション）のパーセンテージとして指定する、いつでもネゴシエーション中にできる IKEv2 SA の最大数。デフォルトでは、ネゴシエーション中の SA に関する制限はないため、すべての使用可能な SA をネゴシエーション中にできます。範囲は 1 ～ 100 % です。 このオプションを設定する場合に、カスタムのクッキーチャレンジもイネーブルにするときは、この制限よりも低いクッキーチャレンジしきい値を設定します。
Enable Cookie Challenge	SA 開始パケットの応答としてピア デバイスにクッキー チャレンジを送信するかどうかを指定します。これは、サービス妨害（DoS）攻撃の防止に役立つことがあります。デフォルトでは、使用可能な SA の 50% がネゴシエーション中である場合にクッキーチャレンジを使用します。次のオプションのいずれか 1 つを選択します。 • [カスタム（Custom）]：ネゴシエーション中の SA の数が、パーセンテージ（ネゴシエーション中の SA が許可された総SA数に対する割合）に基づいて、デバイスで許可された SA の総数を超えると、クッキーチャレンジを行います。[Custom Cookie Challenge] に、将来の SA ネゴシエーションでクッキー チャレンジをトリガーするパーセンテージを入力します。範囲は 1 ～ 100 % です。デフォルトは 50% です。 • [常にしない（Never）]：デバイスではクッキーチャレンジを使用しません。 • [常時（Always）]：デバイスでは、ネゴシエーション中の SA のパーセンテージに関係なく、常にクッキーチャレンジを使用します。
Remote Access Authentication RA Trustpoint （リモート アクセス VPN だけ）	（IKEv2 ネゴシエーションをサポートする場合は必須）デバイスがリモートユーザに対して自身を認証するために使用できる Certificate Authority（CA; 認証局）サーバーを識別する PKI 登録オブジェクト。この認可は、ユーザが接続プロファイルを選択して、VPN にログインする前に必要です。この CA サーバは、リモートアクセス IKEv2 IPsec VPN だけで使用されます。[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9(2) 以降のマルチコンテキストデバイスでリモートアクセス認証を設定できます。 ヒント この PKI 登録オブジェクトは、[Remote Access VPN] > [Public Key Infrastructure] ポリシーでも選択する必要があります。

要素	説明
Load Balancing Settings Redirect Connections During （リモート アクセス VPN だけ）	ロードバランシングを設定する場合は、[ASAグループロードバランス（ASA Group Load Balance）] ポリシーを使用して、ユーザをグループ内の別のデバイスにリダイレクトできるIKEv2ネゴシエーションフェーズを指定できます。次のオプションのいずれか 1 つを選択します。 • [INIT]：グループまたはユーザ認証の前に、未認証の開始要求（最初の IKEv2 メッセージ IKE_SA_INIT）をリダイレクトします。 • 長所：このオプションを使用すると、メインサーバーは、接続をリダイレクトする前に、最小の処理を行って、（CPU とメモリを使用して）状態を維持できます。 • [Cons]：このオプションは、（セキュリティ リスクは最小ですが）[AUTH] ほどセキュアではありません。これは、誰でも、完全に認証なしでリダイレクトされるIPアドレスを取得できるためです。 • [AUTH]（デフォルト）：認証中（IKE_AUTH 中）にリダイレクトします。デバイスは、この時点ではまだユーザを識別または認証していませんが、クライアントは、サーバを認証して、受信するリダイレクトを信頼できることを確認できます。 • [Pros]：応答は IKEv2 トンネルで暗号化され、クライアント側はサーバを認証してから、リダイレクトされるIPアドレスで試行できるため、このオプションはよりセキュアです。これによって、INITオプションよりもさらにDoSから保護されます。 • [Cons]：このオプションでは、リダイレクト前に IKEv2 トンネルをほとんど起動する必要があるため、さらに処理が必要です。ただし、子 SA とデータ トンネルを起動する必要はありません。クライアントは、まったく認証されません。トンネルの両方の側のグループ認証後に、IKEv1 リダイレクトが行われることに注意してください。
無効なセレクタの通知を有効にする（Enable Invalid Selectors Notification）	着信パケットが、SAのトラフィックセレクタと一致しないSAで受信された場合にIKE通知のピアへの送信をイネーブルにします。この機能は、バージョン9.4(1)以降のASAデバイスで、Security Managerバージョン 4.9 以降で使用できます。
フラグメンテーション設定（Fragmentation Settings）（ASA デバイス 9.6(1) 以降）	

要素	説明
暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation before Encryption）	IKEv2 メッセージのフラグメンテーションをイネーブルにするかどうかを指定します。インターネット キー エクスチェンジ バージョン 2（IKEv2）フラグメンテーション プロトコルは、大きな IKEv2 メッセージを IKE フラグメント メッセージと呼ばれる一連の小さなメッセージに分割します。 フラグメンテーションは、ソフトウェアバージョン 9.6(1) 以降を実行している ASA デバイスでサポートされています。
ローカルMTUサイズ（ASA）（Local MTU Size (ASA)）	MTUサイズの値を入力します。MTUサイズは、クリアテキストパケットをチャンクに分割するために使用されます。使用するMTU値には、IPヘッダー+UDPヘッダーのサイズが含まれます。デフォルトのMTUサイズは 576 です。
フラグメンテーションモード（ASA）（Fragmentation Mode (ASA)）	次のいずれかを選択します。 • [CSCO]：現在のシスコ独自のフラグメンテーション方式を指します。 • [IETF]： IETF 標準で定義されている方式を指します（draft-ietf-ipsecme-ikev2-fragmentation）。デフォルトでは、IETF が選択されています。

VPN での NAT について

ネットワーク アドレス変換（NAT）によって、内部IPアドレスを使用するデバイスがインターネット経由でデータを送受信できるようになります。NAT では、デバイスがインターネット上のデータへのアクセスを試みたときに、プライベートな内部 LAN アドレスが、グローバルにルーティング可能な IP アドレスに変換されます。このように、NAT を使用すると、少ない数のパブリック IP アドレスで多数のホストにグローバル接続を提供できます。

NAT では、ハブアンドスポーク VPN トンネルまたはリモート アクセス接続における安定性が向上します。これは、VPN 接続に必要なリソースが他の目的に使用されず、VPN トンネルが完全なセキュリティを必要とするトラフィックに対して継続して使用可能になるためです。VPN 内部のサイトでは、スプリット トンネル経由で NAT を使用して外部デバイスとセキュアでないトラフィックを交換できます。重要でないトラフィックを VPN トンネル経由で送信することによって、VPN 帯域幅を浪費したり、トンネル ヘッドエンドのハブに過負荷をかけたりすることがありません。

Security Manager では、ダイナミック IP アドレッシングによる NAT だけがサポートされており、ポート レベルの NAT またはポート アドレス変換（PAT）と呼ばれる方式を可能にするオーバーロード機能に適用されます。PAT では、ポート アドレッシングを使用して、何千ものプライベート NAT アドレスが少数のパブリック IP アドレスのグループに関連付けられます。PAT は、ネットワークのアドレッシング要件がダイナミック NAT プールで使用可能なアドレスを超える場合に使用されます。

（注） Cisco IOS ルータで PAT をイネーブルにすると、展開時に、スプリット トンネリングされるトラフィック用に追加の NAT ルールが暗黙的に作成されます。（外部インターフェイスを IP アドレス プールとして使用して）VPN トンネリングされるトラフィックを拒否し、他のすべてのトラフィックを許可するこの NAT ルールは、ルータ プラットフォーム ポリシーとしては反映されません。この機能をディセーブルにすることによって、NAT ルールを削除できます。詳細については、[NAT] ページ - [Dynamic Rules] （1319 ページ）を参照してください。

サイト間 VPN トラフィックで NAT 設定を無視するようにトラフィックを設定できます。Cisco IOS ルータで NAT 設定を無視するには、[NAT ダイナミック ルール（NAT Dynamic Rule）] プラットフォーム ポリシーで [VPN トラフィックを返還しない（Do Not Translate VPN Traffic）] オプションが選択されていることを確認します（[Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照）。PIX ファイアウォールまたは ASA デバイスで NAT を除外するには、[NAT Translation Options] プラットフォーム ポリシーでこのオプションが選択されていることを確認します（[Translation Options] ページ （1329 ページ）を参照）。

NAT 通過について

NAT 通過は、VPN 接続ハブアンドスポークの間にデバイス（中間デバイス）があり、そのデバイスが IPsec フローで NAT を実行する場合に、キープアライブ メッセージの送信に使用されます。

スポークの VPN インターフェイスの IP アドレスがグローバルにルーティング可能でない場合、中間デバイスにおける NAT でこのアドレスが新しいグローバルにルーティング可能な IP アドレスに置換されます。この変更は、IPsec ヘッダーで行われるため、スポークのチェックサムが無効となり、ハブにおけるチェックサムの計算が一致しなくなります。これにより、ハブとスポークとの間の接続が失われます。

NAT 通過を使用すると、スポークでペイロードに UDP ヘッダーが追加されます。中間デバイスにおける NAT では、この UDP ヘッダーの IP アドレスが変更され、IPsec ヘッダーおよびチェックサムは変更されないままとなります。スタティック NAT を使用する中間デバイスでは、（グローバルにルーティング可能な）スタティック NAT IP アドレスを内部インターフェイスに指定する必要があります。スタティック NAT IP アドレスは、そのインターフェイスを通過し NAT を必要とするすべてのトラフィックに提供されます。ただし、NAT IP アドレスが不明なダイナミック NAT を中間デバイスで使用する場合は、スポークからのすべての接続要求に対応できるように、ハブにダイナミック クリプトを定義する必要があります。Security Manager によって、スポークに必要なトンネル設定が生成されます。

（注） NAT 通過は、IOS バージョン 12.3T 以降を実行するルータではデフォルトでイネーブルになっています。NAT 通過機能をディセーブルにする場合は、デバイスで手動でディセーブルにするか、FlexConfig を使用してディセーブルにする必要があります（FlexConfig の管理 （431 ページ）を参照）。

VPN グローバル NAT 設定 （1532 ページ）の説明に従って、[Global VPN Settings] ページの [NAT Settings] タブで、グローバルな NAT 設定を定義できます。

VPN グローバル NAT 設定

[Global Settings] ページの [NAT Settings] タブを使用して、グローバル ネットワーク アドレス変換（NAT）設定を定義します。これにより、内部 IP アドレスを使用するデバイスがインターネット経由でデータを送受信できるようになります。

（注） サイト間 VPN では、IOS ルータで NAT 設定を無視する場合は、[NATダイナミックルール（NAT Dynamic Rule）] プラットフォームポリシーで [VPNトラフィックを変換しない（Do Not Translate VPN Traffic）] オプションが選択されていることを確認します（ [Add NAT Dynamic Rule]/[Edit NAT Dynamic Rule] ダイアログボックス （1321 ページ）を参照）。PIX ファイアウォールまたは ASA デバイスで NAT を除外するには、[NAT Translation Options] プラットフォーム ポリシーでこのオプションが選択されていることを確認します（ [Translation Options] ページ （1329 ページ）を参照）。

ナビゲーション パス

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）]** を選択します。[NAT設定（NAT Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[NAT設定（NAT Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPNセレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[NAT設定（NAT Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しいポリシーを作成し、[NAT設定（NAT Settings）] タブをクリックします。

関連項目

- VPN での NAT について （1530 ページ）

• VPN グローバル設定 （1517 ページ）

フィールド リファレンス

表 343 : [VPN Global Settings] ページ、[NAT Settings] タブ

要素	説明
Enable Traversal Keepalive インターバル	NAT 通過キープアライブをイネーブルにするかどうかを指定します。VPN接続ハブとスポークとの間にデバイス（中間デバイス）が配置されている場合、キープアライブ メッセージを転送するためにNAT トラバーサル キープアライブを使用します。このデバイスでは、IPsec フローで NAT を実行します。 このオプションを選択する場合は、セッションがアクティブであることを示すためにスポークと中間デバイス間でキープアライブ信号が送信される間隔（秒）を設定します。値は、5 ～ 3600 秒の範囲で指定します。デフォルトは 10 秒です。 （注） Cisco IOS ルータでは、NAT 通過がデフォルトでイネーブルになります。NAT 通過機能をディセーブルにする場合は、デバイスで手動でディセーブルにするか、FlexConfig を使用してディセーブルにする必要があります。
Enable Traversal over TCP TCP ポート（TCP Ports） （リモート アクセス VPN だけ）	ASA および PIX 7.0+ デバイスでサポートされます。 選択すると、IKE プロトコルと IPsec プロトコルの両方が TCP パケット内にカプセル化され、NAT デバイスと PAT デバイスおよびファイアウォールの両方を経由するセキュアなトンネリングがイネーブルになります。 このオプションを選択する場合は、NAT Traversal（NAT-T; NAT 通過）をイネーブルにする TCP ポートを指定します。リモート クライアントおよび VPN デバイスで TCP ポートを設定する必要があります。クライアント設定には、セキュリティ アプライアンスに対して設定したポートを少なくとも 1 つ含める必要があります。最大 10 個のポートを入力できます。 ヒント これらのポートは、IKEv1 接続だけに使用されます。IKEv2 は、NAT-T にポート 500 と 4500 を使用します。指定するすべてのポートが、適切なインターフェイスのアクセスルールで開いていることを確認します。

要素	説明
Enable PAT (Port Address Translation) on Split Tunneling for Spokes （サイト間 VPN だけ）	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 選択されている場合、VPN トポロジのスポークで、スプリット トンネリングされるトラフィックでのポート アドレス変換（PAT）の使用がイネーブルになります。 PAT では、ポート アドレッシングを使用して、何千ものプライベート NAT アドレスを少数のパブリック IP アドレスのグループに関連付けることができます。PAT は、ネットワークのアドレッシング要件がダイナミック NAT プールで使用可能なアドレスを超える場合に使用されます。 （注） このオプションを選択する場合、Security Manager では、展開時に、スプリット トンネリングされるトラフィック用に追加の NAT ルールが暗黙的に作成されます。（外部インターフェイスを IP アドレス プールとして使用して）VPN トンネリングされるトラフィックを拒否し、他のすべてのトラフィックを許可するこの NAT ルールは、ルータ プラットフォーム ポリシーとしては反映されません。 ダイナミック NAT ルールをルータ プラットフォーム ポリシーとして作成または編集する詳細については、[NAT] ページ - [Dynamic Rules]（1319 ページ）を参照してください。

VPN グローバル一般設定

[VPN Global Settings] ページの [General Settings] タブを使用して、サイト間およびリモート アクセス VPN の最大伝送単位（MTU）処理パラメータを含む、フラグメンテーション設定を定義します。

フラグメンテーションでは、パケットの元のサイズをサポートできない物理インターフェイス経由でパケットが送信されるときに、パケットがより小さな単位に分割されます。フラグメンテーションを使用することによって、分割しないと大きすぎて送信できない保護対象パケットを送信できるようになるため、VPN トンネルにおけるパケット損失を最小限に抑えることができます。このことは、特に GRE を使用する場合に当てはまります。IPsec と GRE を組み合わせて使用するとパケットのペイロードに 80 バイトが追加されますが、1420 バイトを超えるパケットにはこのための余裕がヘッダーにないためです。

最大伝送単位（MTU）によって、インターフェイスが処理できる最大パケット サイズがバイト単位で指定されます。通常、パケットが MTU を超える場合は、暗号化のあとにパケットがフラグメント化されます。Do Not Fragment（DF）ビットが設定されている場合、パケットはドロップされます。DF ビットは、デバイスでパケットをフラグメント化できるかどうかを示す、IP ヘッダー内にあるビットです。カプセル化されたヘッダーの DF ビットをデバイスでクリア、設定、またはコピーできるかどうかを指定する必要があります。

暗号化されたパケットを再構築することは困難であるため、フラグメンテーションによってネットワークのパフォーマンスが低下する可能性があります。ネットワークパフォーマンスの

問題を回避するには、[暗号化前のフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）] を選択して、暗号化前にフラグメンテーションが行われるように設定できます。

ナビゲーション パス

- リモート アクセス VPN の場合は、次のいずれかを実行します。
  - （デバイスビュー）ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [グローバル設定（Global Settings）] を選択します。[一般設定（General Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [グローバル設定（Global Settings）] を選択します。既存のポリシーを選択するか新しいポリシーを作成してから、[全般設定（General Settings）] タブをクリックします。
- サイト間 VPN の場合は、次のいずれかを実行します。
  - [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタでトポロジを選択して、ポリシーセレクタで [VPNグローバル設定（VPN Global Settings）] を選択します。[全般設定（General Settings）] タブをクリックします。
  - （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [VPNグローバル設定（VPN Global Settings）] を選択します。既存の共有ポリシーを選択するか新しい共有ポリシーを作成してから、[全般設定（General Settings）] タブをクリックします。

関連項目

- VPN グローバル設定 （1517 ページ）

フィールド リファレンス

表 344 : [VPN Global Settings] ページ、[General Settings] タブ

要素	説明
Fragmentation Settings	

要素	説明
Fragmentation Mode Local MTU Size	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 フラグメンテーションを行うと、パケットの元のサイズをサポートできない物理インターフェイスを介してパケットが送信されるときの、VPN トンネル内のパケット損失が最小限に抑えられます。フラグメンテーション モードを選択します。 • [フラグメンテーションなし（No Fragmentation）]：IPsec 暗号化の前にフラグメント化しません。カプセル化のあと、デバイスで、MTU 設定を超えるパケットがフラグメント化されたあと、パブリック インターフェイスを介して送信されます。 • [エンドツーエンドMTUの検出（End to End MTU Discovery）]：ICMP メッセージを使用して、最大 MTU を判別します。このオプションは、IPsec VPN で使用します。 エンドツーエンドMTUディスカバリでは、インターネット制御メッセージプロトコル（ICMP）メッセージを使用して、フラグメンテーションを発生させずにホストが VPN トンネルを介してパケットを送信するために使用できる最大 MTU を決定します。送信パス内の各リンクの MTU 設定がチェックされて、送信されるいずれのパケットもそのパス内の最小MTUを超えていないことが確認されます。検出されたMTUを使用して、フラグメンテーションが必要であるかどうかが決定されます。ICMP がブロックされている場合は、MTU ディスカバリに失敗し、パケットが失われるか（DF ビットが設定されている場合）、または暗号化のあとにパケットがフラグメント化されます（DF ビットが設定されていない場合）。 （注） （サイト間 VPN）Catalyst 6500/7600 デバイスでは、エンドツーエンド パス MTU ディスカバリはイメージ 12.2(33)SRA、12.2(33)SRB、12.2(33)SXH、12.2(33)SXI またはそれ以降だけでサポートされています。 • [ローカルMTU処理（Local MTU Handling）]：デバイスでMTUをローカルに設定します。このオプションは通常、ICMP がブロックされているか、サイト間 IPsec/GRE VPN 内にある場合に使用されます。このオプションを選択する場合は、ローカル MTU サイズを指定します。この値には、VPN インターフェイスに応じて 68 ～ 65535 バイトを指定できます。

要素	説明
DF ビット（DF Bit）	Cisco IOS ルータ、Catalyst 6500/7600 デバイス、PIX 7.0+、および ASA デバイスでサポートされます。 IP ヘッダー内の Do Not Fragment（DF）ビットによって、デバイスでパケットのフラグメント化が許可されているかどうかが決定されます。DF ビットの処理方法を選択します。 • [コピー（Copy）]：現在のパケットのカプセル化されたヘッダーの DF ビットを、すべてのデバイスのパケットにコピーします。パケットの DF ビットがフラグメント化を許可するように設定されている場合、以降のすべてのパケットはフラグメント化されます。これがデフォルトのオプションです。 • [設定（Set）]：送信するパケットの DF ビットを設定します。MTU を超える大きなパケットはドロップされ、パケットの送信者に ICMP メッセージが送信されます。 • [クリア（Clear）]：元の DF ビット設定にかかわらず、パケットをフラグメント化します。ICMP がブロックされていると、MTU ディスカバリは失敗し、パケットは暗号化されたあとでだけフラグメント化されます。
暗号化の前にフラグメンテーションを有効にする（Enable Fragmentation Before Encryption）	Cisco IOS ルータ、Catalyst 6500/7600 デバイス、PIX 7.0+、および ASA デバイスでサポートされます。 選択されている場合、想定されるパケット サイズが MTU を超えるときには暗号化の前にフラグメント化できます。 Look Ahead Fragmentation（LAF）は、IPsec SA に設定されているトランスフォーム セットに応じて、暗号化後のパケット サイズを計算するために暗号化の実行前に使用されます。パケット サイズが指定した MTU を超える場合は、暗号化の前にパケットがフラグメント化されます。
Enable Notification on Disconnection	ASA および PIX 7.0+ デバイスでサポートされます。 選択されている場合、デバイスは、認定されたピアに、切断されようとしているセッションを通知できます。アラートを受け取ったピアは、理由をデコードし、イベント ログまたはポップアップ ウィンドウにそれを表示します。この機能は、デフォルトではディセーブルになっています。 IPsec セッションがドロップされる理由としては、セキュリティ アプライアンスのシャットダウンまたはリブート、セッション アイドル タイムアウト、最大接続時間の超過、管理者による切断などが考えられます。

要素	説明
Enable Split Tunneling （サイト間VPNだけ）	選択されている場合（デフォルト）、サイト間 VPN トポロジでスプリット トンネリングを設定できます。 スプリット トンネリングを使用すると、同じインターフェイスで、保護されるトラフィックと保護されないトラフィックの両方を送信できます。スプリット トンネリングを使用する場合は、保護対象のトラフィック、およびそのトラフィックの宛先を正確に指定して、指定したトラフィックだけが IPsec トンネルに入り、その他のトラフィックはパブリック ネットワークに暗号化なしで送信されるようにする必要があります。
Enable Spoke-to-Spoke Connectivity through the Hub	ASA および PIX 7.0+ デバイスでサポートされます。 選択すると、ハブアンドスポーク VPN トポロジ内のスポーク間のダイレクト通信がイネーブルになります。ここでのハブは ASA または PIX 7.0+ デバイスです。
Enable Default Route	Cisco IOS ルータおよび Catalyst 6500/7600 デバイスでサポートされます。 選択されている場合、デバイスは、設定された外部インターフェイスをすべての着信トラフィックのデフォルトの発信ルートとして使用します。
[すべてのセッションが終了するまで再起動しない（ASA）（Do not reboot until all the sessions are terminated (ASA)）]	すべてのアクティブセッションが終了するまで、スケジュールされた再起動を ASA で延期する場合は、このオプションを選択します。この機能は、デフォルトではディセーブルになっています。 （注） ASA ソフトウェアの **crypto isakmp reload-wait** コマンドは、マルチコンテキストモードの ASA デバイスのシステムコンテキストでのみサポートされます。ただし、VPN 設定ではシステムコンテキストがサポートされないため、Security Manager は、VPN 設定に含まれるマルチコンテキストモードのデバイスに対してこのコマンドを生成しません。マルチコンテキストモードのデバイスで **crypto isakmp reload-wait** コマンドを機能させるには、システムコンテキストで FlexConfig ポリシーを使用する必要があります。FlexConfig ポリシーを使用すると、Security Manager ではサポートされていないデバイス コマンドを設定できます。詳細については、FlexConfig の管理 （431 ページ）を参照してください。

サイト間 VPN での IKEv1 事前共有キー ポリシーについて

IKEv1 ネゴシエーションの認証方式として事前共有キーを使用する場合は、2 つのピア間のトンネルごとに共有キーを定義する必要があります。この共有キーは、接続を認証するための共有秘密となります。キーはピアごとに設定されます。トンネルの両方のピアのキーが同じでない場合は、接続を確立できません。事前共有キーの設定に必要なピア アドレスは、VPN トポロジから推定されます。

ヒント　IKEv2 ネゴシエーションに事前共有キーを使用することもできますが、ルールと要件があるため、設定は、IKEv1 に使用する設定とは異なります。IKEv2 ネゴシエーションの事前共有キーの設定については、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。

事前共有キーは、スポークに設定されます。ハブアンドスポーク VPN トポロジでは、スポークとハブのキーが同じものになるように、Security Manager によってスポークの事前共有キーがミラーリングされ、割り当てられているハブに設定されます。ポイントツーポイント VPN トポロジでは、両方のピアに同じ事前共有キーを設定する必要があります。完全メッシュ VPN トポロジでは、接続される任意の 2 つのデバイスが同じ事前共有キーを持っている必要があります。

Preshared Key ポリシーでは、特定のキーを使用することも、各通信セッションに参加するピアに対して自動的に生成されたキーを使用することもできます。VPN 内のすべての接続で同じ事前共有キーを使用するとセキュリティが侵害される可能性があるため、自動的にキーを生成する方法（デフォルトの方法）を推奨します。

4.16 以降、Cisco Security Manager は分散モードの Firepower 9300 デバイスの IKEv1 関連の設定をサポートしていません。

デバイスの 1 つがクラスタ分散モード（IKEv2 が設定されている）であり、他のデバイスが非クラスタモード（IKEv1 および IKEv2 が設定されている）である VPN トポロジを検出しているときに、Cisco Security Manager はエラーを表示しません。ただし、プレビュー設定中に、IKEv1 関連の設定を削除するためのアクティビティ検証エラーが表示されます。

キー情報のネゴシエーションおよび IKE Security Association（SA; セキュリティ アソシエーション）の設定には、3 種類の方式があります。

- メイン モード（アドレス）：IP アドレスに基づいてネゴシエーションが行われます。メイン モードは、発信側と受信側の間に 3 つの双方向交換を持つため、最も高いセキュリティを提供します。これはデフォルトのネゴシエーション方式です。

この方式では、キーを作成するための 3 つのオプションがあります。

- 各ピアの一意の IP アドレスに基づいて各ピアに対してキーを作成できます。このオプションを使用すると、高いセキュリティが確保されます。
- ハブアンドスポーク VPN トポロジ内のハブにグループ事前共有キーを作成して、指定したサブネット内の任意のデバイスとの通信で使用できます。各ピアは、デバイスの IP アドレスが不明である場合でも、サブネットによって識別されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、グループ事前共有キーがピアに作成されます。
- ハブアンドスポーク VPN トポロジ内のハブ、またはハブを含むグループに対して、ワイルドカード キーを作成できます。ワイルドカード キーは、スポークが固定 IP アドレスを持っていない場合や、特定のサブネットに属していない場合にダイナミック クリプトで使用されます。ハブに接続するすべてのスポークは同じ事前共有キーを持っているため、セキュリティが侵害される可能性があります。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ワイルドカード キーがピアに作成されます。

（注） DMVPN にスポーク間での直接接続を設定する場合は、スポークにワイルドカード キーを作成します。

- メインモード（Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名））：IP アドレスに依存しないで、DNS 解決に基づいてネゴシエーションが行われます。このオプションは、ホストで DNS 解決サービスが利用できる場合にだけ使用できます。このオプションは、ダイナミック IP アドレスを使用する、DNS 解決機能を持つデバイスを管理する場合に役立ちます。
- アグレッシブ モード：ホスト名（DNS 解決は行いません）およびドメイン名に基づいてネゴシエーションが行われます。アグレッシブ モードで提供されるセキュリティは、メイン モードよりも低くなります。ただし、ホストの VPN インターフェイスの IP アドレスが不明であり、ダイナミック IP ピアの FQDN が DNS で解決できない場合には、グループ事前共有キーを使用するよりも高いセキュリティが提供されます。このネゴシエーション方式は、GRE ダイナミック IP または DMVPN フェールオーバーおよびルーティング ポリシーでの使用が推奨されます。

関連項目

- 使用する認証方式の決定 （1486 ページ）
- IKEv1 事前共有キー ポリシーの設定 （1540 ページ）

IKEv1 事前共有キー ポリシーの設定

[IKEv1 Preshared Key] ページを使用して、サイト間 VPN トポロジでの IKEv1 の使用時に事前共有キー設定を定義します。IKEv2 を使用する場合の事前共有キーの設定については、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。

（注） Preshared Key ポリシーは、Easy VPN トポロジには適用されません。

（注） 4.16 以降、Cisco Security Manager は、分散モードの Firepower 9300 デバイスの IKEv1 事前共有キー設定をサポートしていません。

[IKEv1 Preshared Key] ページを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタでトポロジを選択して、ポリシーセレクタで [IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。

- （ポリシービュー）ポリシータイプセレクタで[サイト間VPN（Site-to-Site VPN）]>[IKEv1事前共有キー（IKEv1 Preshared Key）]を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

次の表で、このポリシーで定義できる設定について説明します。

表 *345 : [IKEv1 Preshared Key]* ページ

要素	説明
Key Specification キーを手動で定義する（[User Defined]）か、キーを自動的に生成するかを選択します。自動生成キーの使用時に設定できる追加のオプションがあります。	
ユーザー定義	選択されている場合、手動で定義した事前共有キーを使用できます。 [キー（Key）] フィールドに必要な事前共有キーを入力して、[確認（Confirm）] フィールドに再度そのキーを入力します。
Auto Generated	選択されている場合、参加するピアにランダムなキーが割り当てられます。生成されるキーは、ハブとスポークとの間の接続ごとに異なるため、セキュリティが確保されます。[Auto Generated] がデフォルトの選択です。 [Auto generated] は、VPN（たとえば、エクストラネット VPN の場合）内のすべてのノードを管理しないときは有効なオプションではありません。 （注） キーは、デバイスへの最初の展開時に割り当てられ、[Regenerate Key (Only in Next Deployment)] チェックボックスを選択するまでは、同じデバイスに対するそれ以降のすべての展開で常にこのキーが使用されます。
キーの長さ（Key Length）	自動生成する事前共有キーの必要な長さ（1 ～ 127）です。デフォルトは 24 です。
Same Key for All Tunnels	ポイントツーポイント VPN トポロジでは使用できません。 選択されている場合、すべてのトンネルで自動生成された同じキーを使用できます。 （注） このオプションを選択しない場合は、トンネルで異なるキーが使用されます。ただし、DMVPN設定など、同じネットワーク内の異なるマルチポイント GRE インターフェイスで同じ事前共有キーを使用する必要がある場合を除きます。

要素	説明
Regenerate Key (Only in Next Deployment)	選択されている場合、デバイスに対する次の展開時に Security Manager によって新しいキーが生成されます。キーの機密性が侵害された可能性がある場合に役立ちます。 ジョブを展開用に送信すると、このチェックボックスはクリアされます。新しいキーは、新しい展開に対してだけ生成され、以降の展開では（再度チェックボックスを選択しないかぎり）生成されないため、このチェックボックスがクリアされます。
Negotiation Method ネゴシエーション方式のタイプを選択します。方式については、サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）で詳細に説明します。	

要素	説明
Main Mode Address	デバイスの IP アドレスが判明している場合は、このネゴシエーション方式を使用してキー情報を交換します。IP アドレスに基づいてネゴシエーションが行われます。メインモードは、発信側と受信側の間に 3 つの双方向交換を持つため、最も高いセキュリティを提供します。メインモード（アドレス）がデフォルトのネゴシエーション方式です。 ネゴシエーション アドレス タイプを定義するには、次のいずれかのオプションを選択します。 • [ピアアドレス（Peer Address）]：各ピアの一意の IP アドレスに基づいてネゴシエーションが行われます。キーはピアごとに作成されるため、高いセキュリティが確保されます。これがデフォルトです。 • [サブネット（Subnet）]：ハブアンドスポークトポロジ内のハブでグループ事前共有キーを作成して、指定したサブネット内の任意のデバイスとの通信に使用します。デバイスの IP アドレスが不明な場合でも使用できます。各ピアは、それぞれのサブネットによって識別されます。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、グループ事前共有キーがピアに作成されます。表示されるフィールドにサブネットを入力します（たとえば、10.10.10.0/24）。 • [ワイルドカード（Wildcard）]：ハブアンドスポークトポロジ内のハブまたはハブのグループに対してワイルドカードキーを作成して、スポークが固定 IP アドレスを持っていない場合や、特定のサブネットに属していない場合に使用します。この場合、ハブに接続するすべてのスポークは同じ事前共有キーを持っているため、セキュリティが侵害される可能性があります。ハブアンドスポーク VPN トポロジ内のスポークでダイナミック IP アドレスが使用されている場合にこのオプションを使用します。ポイントツーポイントまたは完全メッシュ VPN トポロジでは、ワイルドカード キーがピアに作成されます。 （注） DMVPN にスポーク間での直接接続を設定する場合は、スポークにワイルドカード キーを作成します。
Main Mode FQDN	IP アドレスが不明であり、デバイスで DNS 解決を使用できる場合は、このネゴシエーション方式を選択してキー情報を交換します。IP アドレスに依存しないで、DNS 解決に基づいてネゴシエーションが行われます。

要素	説明
Aggressive Mode	ハブアンドスポーク VPN トポロジでのみ使用できます。 IP アドレスが不明であり、デバイスで DNS 解決を使用できない可能性がある場合は、このネゴシエーション方式を選択してキー情報を交換します。ホスト名およびドメイン名に基づいてネゴシエーションが行われます。 （注） スポーク間での直接のトンネリングがイネーブルになっている場合には、アグレッシブ モードを使用できません。

関連項目

- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）

Public Key Infrastructure ポリシーについて

Security Manager では、証明書要求を管理し、VPN トポロジ内のデバイスに対して証明書を発行する、Certification Authority（CA; 認証局）サーバでの IPsec 設定がサポートされています。Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。これにより、参加するデバイスについてキーを中央で管理できます。

CA サーバ（トラストポイントとも呼ばれます）では、公開 CA 証明書要求を管理して、参加する IPsec ネットワーク デバイスに対して証明書を発行します。IKE プロポーザル ポリシーおよび IPsec プロポーザル ポリシーの認証方式として証明書を使用する場合、ピアは CA サーバからデジタル証明書を入手するように設定されます。CA サーバでは、すべての暗号化デバイス間にキーを設定する必要はありません。代わりに、参加する各デバイスを CA サーバに個別に登録します。CA サーバは、アイデンティティを確認し、デバイスのデジタル証明書を作成することを明示的に信任されています。登録が完了すると、参加する各ピアは、もう一方の参加するピアのアイデンティティを確認し、証明書に含まれている公開キーを使用して暗号化されたセッションを確立できます。

また、CA では、IPsec VPN トポロジに参加しなくなったピアの証明書を無効化することもできます。無効化された証明書は、Online Certificate Status Protocol（OCSP; オンライン証明書状態プロトコル）サーバで管理されるか、または LDAP サーバに格納されている Certificate Revocation List（CRL; 証明書失効リスト）に記載されます。各ピアでは、他のピアからの証明書を受け入れる前に、この CRL をチェックできます。

PKI 登録は、複数の CA で構成される階層型フレームワークに設定できます。階層の最上位にはルート CA があり、自己署名証明書を保持しています。階層全体の信頼性は、ルート CA の RSA キー ペアから導出されます。階層内の下位 CA は、ルート CA または他の下位 CA に登録できます。階層型 PKI 内では、ピア間で信頼できるルート CA 証明書または共通の下位 CA が共有されている場合、登録されたすべてのピアが相互の証明書を確認できます。

次の点を考慮してください。

- PKI ポリシーは、バージョン 12.3(7)T 以降を実行する Cisco IOS ルータ、PIX ファイアウォール、およびサイト間およびリモート アクセス VPN の Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスに設定できます。
- サイト間 VPN では、[IKEv1 Public Key Infrastructure] ポリシーを使用して、IKEv1 ネゴシエーション専用の CA サーバを特定します。IKEv2 ネゴシエーションでは、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）の説明に従って、[IKEv2 Authentication] ポリシーで CA サーバを特定します。
- リロード間に RSA キーペアと CA 証明書を PIX Firewall リリース 6.3 のフラッシュメモリに永続的に保存するには、**ca save all** コマンドを設定する必要があります。この操作は、デバイスで手動で行うか、FlexConfig を使用して行うことができます。

CA サーバの認証方式

次のいずれかの方式を使用して CA サーバを認証できます。

- Simple Certificate Enrollment Protocol（SCEP）を使用して、CA サーバーから CA の証明書を取得します。SCEP を使用すると、デバイスと CA サーバとの間に直接接続を確立できます。登録プロセスを開始する前に、デバイスが CA サーバに接続されていることを確認してください。この方式を使用してルータの CA 証明書を取得する場合は、対話形式の操作が必要となるため、PKI ポリシーをライブデバイスだけに展開できます。ファイルには展開できません。

（注） SCEP を使用する場合は、CA サーバのフィンガープリントを入力する必要があります。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。サーバーに直接アクセスして、または Web ブラウザにアドレス（**http://<URLHostName>/certsrv/mscep/mscep.dll**）を入力して、CA のフィンガープリントを取得できます。

- CA サーバーの証明書を他のデバイスからコピーすることによって、オフラインで CA サーバーに送信できる登録要求を手動で作成します。

この方式は、デバイスが CA サーバへの直接接続を確立できない場合、またはいったん登録要求を生成してから、あとで登録要求をサーバに送信する場合に使用します。

（注） この方式を使用すると、デバイスまたはファイルに PKI ポリシーを展開できます。

詳細については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

（注） Cisco Secure Device Provisioning（SDP; セキュア デバイス プロビジョニング）を使用して、ルータの証明書を登録することもできます。SDP を使用した証明書登録の詳細については、Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）を参照してください。

ここでは、公開キー インフラストラクチャ設定についてより詳細に説明します。

- PKI 登録を正常に行うための前提条件 （1546 ページ）
- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）
- サイト間 VPN での複数の IKEv1 CA サーバの定義 （1550 ページ）
- リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）
- [PKI Enrollment] ダイアログボックス （1554 ページ）

PKI 登録を正常に行うための前提条件

ネットワークに PKI ポリシーを設定するためには、次の前提条件が必要です。

- IKEv1 では、IKE プロポーザルで、IKE 認証方式の証明書を指定する必要があります。[IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）を参照してください。
- PKI 登録を正常に行うには、デバイスにドメイン名が定義されている必要があります（CA サーバのニックネームを指定する場合を除く）。
- CA サーバーに直接登録するには、サーバーの登録 URL を指定する必要があります。
- TFTP サーバを使用して CA サーバに登録するには、TFTP サーバに CA 証明書ファイルが保存されている必要があります。PKI ポリシーを展開したあと、TFTP サーバから CA サーバに証明書要求をコピーする必要があります。
- 登録要求で使用する RSA 公開キーを指定できます。RSA キー ペアを指定しない場合は、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）キーが使用されます。

RSA キーを使用する場合は、証明書が承認されると、証明書に公開キーが組み込まれます。ピアは、この公開キーを使用して、デバイスに送信するデータを暗号化できます。秘密キーはデバイスに保持されて、ピアから送信されるデータの復号化、およびピアとのネゴシエーション時のトランザクションのデジタル署名に使用されます。既存のキーペアを使用することも、新しいキー ペアを生成することもできます。ルータ デバイスの証明書で使用する新しいキー ペアを生成する場合は、キーのサイズを特定する係数も指定する必要があります。

詳細については、[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （1561 ページ）を参照してください。

- Cisco Easy VPN IPsec リモート アクセス システムで PKI 登録要求を行う場合は、各リモート コンポーネント（スポーク）に、接続するユーザ グループの名前を設定する必要があります。この情報は、[PKI Enrollment Editor] ダイアログボックスの [Certificate Subject Name] タブにある [Organization Unit (OU)] フィールドで指定します。

（注） ハブ（Easy VPN サーバ）にユーザ グループの名前を設定する必要はありません。

詳細については、[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）を参照してください。

- PKI ポリシーを（ライブ デバイスではなく）ファイルに展開する場合は、次の前提条件を満たしている必要があります。
  - ルータは、Cisco IOS ソフトウェア 12.3(7)T 以降を実行している必要があります。
  - CA 認証が対話形式で行われず、ライブ デバイスとの通信が必要とならないように、CA 認証証明書を Security Manager ユーザ インターフェイスにカット アンド ペーストする必要があります。
- ライブ デバイスに展開する場合、PKI サーバがオンラインである必要があります。
- Security Manager では、Microsoft、VeriSign、および Entrust の PKI がサポートされています。
- Security Manager では、Cisco IOS 証明書サーバがサポートされています。Cisco IOS 証明書サーバ機能では、限定的な CA 機能を持つ簡易証明書サーバが Cisco IOS ソフトウェアに組み込まれます。IOS 証明書サーバは、FlexConfig ポリシーとして設定できます。詳細については、FlexConfig の管理 （431 ページ）を参照してください。
- IOS ルータにおいて、PKI に被認証者名全体を使用する AAA 認可を設定するには、IOS_PKI_WITH_AAA という名前の定義済み FlexConfig オブジェクトを使用します。

TFTP を使用した PKI 登録の前提条件

CA サーバに継続的に直接アクセスしていない場合は、デバイスが Cisco IOS ソフトウェア 12.3(7)T 以降を実行するルータであれば、TFTP を使用して登録を行うことができます。

展開時に、Security Manager によって対応する CA トラストポイント コマンドおよび認証コマンドが生成されます。トラストポイント コマンドは、TFTP を使用して CA 証明書を取得するための登録 URL tftp://<certserver> <file_specification> のエントリを使用して設定されます。file_specification が指定されていない場合は、ルータの FQDN が使用されます。

このオプションを使用する前に、TFTP サーバに CA 証明書ファイル（.ca）が保存されている必要があります。このためには、次の手順を実行します。

1. http://servername/certsrv に接続します。servername は、アクセスする CA がある Windows 2000 Web サーバの名前です。

2. [CA証明書または証明書失効リストの取得（Retrieve the CA certificate or certificate revocation list）] を選択して、[次へ（Next）] をクリックします。
3. [Base 64エンコード済み（Base 64 encoded）] をクリックして、[CA証明書をダウンロード（Download CA certificate）] をクリックします。
4. ブラウザの別名保存機能を使用して、.crt ファイルを .ca ファイルとして TFTP サーバーに保存します。

展開後、TFTP サーバーの Security Manager が生成した証明書要求を CA に転送し、デバイスの証明書を CA からデバイスに転送する必要があります。

TFTP サーバから CA サーバへの証明書要求の転送

Security Manager によって、TFTP サーバに PKCS#10 フォーマットの登録要求（.req）が作成されます。次の手順を実行して、この登録要求を PKI サーバに転送する必要があります。

1. http://servername/certsrv に接続します。servername は、アクセスする CA がある Windows 2000 Web サーバの名前です。
2. [証明書の要求（Request a certificate）] を選択し、[次へ（Next）] をクリックします。
3. [詳細な要求（Advanced request）] を選択して、[次へ（Next）] をクリックします。
4. [base64エンコード済みPKCS #10ファイルを使用して証明書要求を送信またはbase64エンコード済みPKCS #7ファイルを使用して更新要求を送信（Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file）] を選択して、[次へ（Next）] をクリックします。
5. ファイルの参照を選択して TFTP サーバを参照し .req ファイルを選択するか、または先ほど TFTP で受信した .req ファイルをワードパッドまたはメモ帳で開いてその内容を最初のウィンドウにコピーアンドペーストします。
6. CA から .crt ファイルをエクスポートして、TFTP サーバに配置します。
7. 「crypto ca import <label> certificate」を設定して、tftp サーバーからデバイスの証明書をインポートします。

関連項目

- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）
- リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）
- [PKI Enrollment] ダイアログボックス （1554 ページ）
- Easy VPN における User Group ポリシーの設定 （1617 ページ）

サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定

Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、VPN トポロジ内の参加デバイスに対して証明書を発行するために使用されます。

Security Manager では、CA サーバは、PKI ポリシーで使用できる PKI 登録オブジェクトとして事前に定義されています。PKI 登録オブジェクトには、CA 証明書の登録要求を作成するために必要なサーバ情報および登録パラメータが含まれています。

Public Key Infrastructure ポリシーの詳細については、Public Key Infrastructure ポリシーについて（1544 ページ）を参照してください。

この手順では、VPN トポロジで IKEv1 Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーの作成に使用する CA サーバを指定する方法について説明します。

ヒント IKEv2 ネゴシエーションで使用する CA サーバの指定については、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。

はじめる前に

PKI の正常な設定に関する重要な情報については、PKI 登録を正常に行うための前提条件 （1546 ページ）を参照してください。

関連項目

- サイト間 VPN での複数の IKEv1 CA サーバの定義 （1550 ページ）
- 使用する認証方式の決定 （1486 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

ステップ 1 次のいずれかを実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））既存のトポロジを選択して、ポリシーセレクタで [IKEv1公開キーインフラストラクチャ（IKEv1 Public Key Infrastructure）] を選択します。
- （ポリシービュー）**[サイト間VPN（Site-to-Site VPN）]>[IKEv1公開キーインフラストラクチャ（IKEv1 Public Key Infrastructure）]** を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

[公開キーインフラストラクチャ（Public Key Infrastructure）] ページが開き、[選択済み（Selected）] フィールドに、現在選択されている CA サーバー（存在する場合）が表示されます。

ステップ 2 [Available CA Servers] リストで必要な CA サーバを定義する PKI 登録ポリシー オブジェクトを選択します。リストされているオブジェクトを変更するには、次の手順を実行できます。

- 新しい PKI 登録オブジェクトを追加するには、[作成（Create）]（+）ボタンをクリックします。[Add PKI Enrollment] ダイアログボックスが開きます。PKI 登録オブジェクトの属性に関する詳細については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。
- 既存のオブジェクトの設定を変更するには、そのオブジェクトを選択して、[編集（Edit）]（鉛筆）ボタンをクリックします。

（注） Easy VPN トポロジで PKI 登録要求を行う場合は、各リモート コンポーネント（スポーク）に、接続するユーザ グループの名前を設定する必要があります。この情報は、[PKI Enrollment] ダイアログボックスの [Certificate Subject Name] タブにある [Organization Unit (OU)] フィールドで指定します。ハブ（Easy VPN サーバ）にユーザ グループの名前を設定する必要はありません。詳細については、[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）を参照してください。

サイト間 VPN での複数の IKEv1 CA サーバの定義

サイト間 VPN で IKEv1 Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーを定義する場合は、1 つの CA サーバだけを選択できます。このことは、IKEv1 の使用時に VPN 内のデバイスが異なる CA サーバに登録するときに問題となります。たとえば、スポーク デバイスとハブ デバイスとで異なる CA サーバに登録する場合や、VPN のある部分のスポークが VPN の他の部分のスポークとは異なる CA サーバに登録する場合があります。

ヒント IKEv2 の使用時に、PKI 登録ポリシー オブジェクトにデバイス レベルのオーバーライドを作成する代わりに、[IKEv2 Authentication] ポリシー グローバル設定のオーバーライドを作成することによって、さまざまなデバイスに異なる CA サーバを設定できます。ただし、ここでの説明に従って、IKEv2 にデバイス レベルのオーバーライドを使用することもできます。IKEv2 の CA サーバの設定については、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。

IKEv1 PKI ポリシーを定義するには、デバイスが登録する CA サーバを指定する PKI 登録オブジェクトを選択します。デフォルトでは、ポリシー オブジェクトは単一の CA サーバをグローバルに参照していますが、デバイス レベルのオーバーライドを使用して、選択したデバイスにおいて異なる CA サーバをオブジェクトが参照するように設定できます。

たとえば、PKI 登録オブジェクト PKI_1 が CA_1 という CA サーバを参照している場合、PKI_1 を持つ選択したデバイスにデバイス レベルのオーバーライドを作成して、CA_2 などの異なる CA サーバを参照できます。理論的には、オーバーライドを使用して、VPN 内の各デバイスに異なる CA サーバを定義することもできます。

この手順では、PKI 登録オブジェクトにオーバーライドを作成するための基本的な手順について説明します。

（注） 共通の信頼できる CA サーバの下の PKI 階層に CA サーバが配置されている場合でも、デバイスレベルのオーバーライドを使用できます。このためには、[PKI Enrollment] ダイアログボックスの [Trusted CA Hierarchy] タブで、オブジェクトのグローバル定義およびデバイスレベルのオーバーライドの両方によって、信頼できる CA サーバが指定されている必要があります。[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （1566 ページ） を参照してください。

関連項目

- Public Key Infrastructure ポリシーについて （1544 ページ）
- 使用する認証方式の決定 （1486 ページ）

ステップ 1 PKI 登録オブジェクトを作成するには、[PKI Enrollment] ダイアログボックスを開きます。このダイアログボックスには、次の 2 つの方法でアクセスできます。

- [公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーから：[選択済み（Selected）] フィールドの下にある [作成（Create）]（+）ボタンをクリックします。サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。
- Policy Object Manager から（[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択します）：オブジェクトタイプセレクタから [PKI 登録（PKI Enrollments）] を選択して、[新規オブジェクト（New Object）]（+）ボタンをクリックします。

ステップ 2 オブジェクトが参照する CA サーバを含む、PKI 登録オブジェクトのグローバル定義を設定します。[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を必ず選択します。このオプションによって、個別のデバイスでオブジェクトをオーバーライドできるようになります。[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

オブジェクトのグローバル定義では、VPN 内の最も多くのデバイスで使用される CA サーバを使用します。これにより、必要となるデバイスレベルのオーバーライドの数を減らすことができます。

ステップ 3 PKI 登録オブジェクトの定義が終了したら、[OK] をクリックします。そのため、次の点に注意してください。

- PKI ポリシーからダイアログボックスにアクセスした場合は、ポリシーページの [Selected] フィールドに新しいオブジェクトが表示されます。
- Policy Object Manager を使用してダイアログボックスにアクセスした場合は、[Policy Object Manager] ウィンドウの作業領域に新しいオブジェクトが表示されます。[Overridable] カラムに緑色のチェックマークが表示されている場合、このオブジェクトに対してデバイスレベルのオーバーライドを作成できることを示しています（このチェック マークは、オーバーライドが実際に存在しているかどうかを示すものではありません）。

ステップ 4 PKI 登録オブジェクトに対してデバイスレベルのオーバーライドを作成します。この処理は、次の 2 つの方法のいずれかで実行できます。

- [デバイスのプロパティ（Device Properties）]（デバイスビューでデバイスが選択された状態で、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択）から：単一のデバイスに対してデバイスレベルのオーバーライドを作成する場合は、このオプションを推奨します。[デバイスのプロパティ（Device Properties）] で、[ポリシー オブジェクト オーバーライド（Policy Object Overrides）] > [PKI 登録（PKI Enrollments）] を選択し、オーバーライドする PKI 登録オブジェクトを選択して、[オーバーライドの作成（Create Override）] ボタンをクリックします。その後、オブジェクトによって定義された CA サーバを含むオーバーライドの内容を定義できます。

詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）を参照してください。

- Policy Object Manager から：このオプションは、複数のデバイスに対して同時にデバイスレベルのオーバーライドを作成する場合に推奨します。[Overridable] カラムの緑色のチェック マークをダブルクリックし、オーバーライドを適用する必要があるデバイスを選択して、オブジェクトによって定義された CA サーバを含むオーバーライドの内容を定義します。

詳細については、複数デバイスのオブジェクト オーバーライドの一括での作成または編集 （313 ページ）を参照してください。

リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定

Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用されます。

Security Manager では、CA サーバは、PKI ポリシーで使用できる PKI 登録オブジェクトとして事前に定義されています。PKI 登録オブジェクトには、CA 証明書の登録要求を作成するために必要なサーバ情報および登録パラメータが含まれています。

Public Key Infrastructure ポリシーの詳細については、Public Key Infrastructure ポリシーについて（1544 ページ）を参照してください。

（注） バージョン 4.12 以降、Cisco Security Manager は、ソフトウェアバージョン 9.5(2) 以降を実行している ASA マルチコンテキストデバイスの公開キー インフラストラクチャ ポリシーのサポートを提供します。

ここでは、リモート アクセス VPN で Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）ポリシーの作成に使用する CA サーバを指定する方法について説明します。

はじめる前に

次の点を考慮してください。

- PKI の正常な設定に関する重要な情報については、 PKI 登録を正常に行うための前提条件（1546 ページ）を参照してください。
- IPsec リモートアクセス VPN の [IKEプロポーザル（IKE Proposal）] ポリシーでは、IKEv1 の設定時に証明書認可を必要とする IKE プロポーザルオブジェクトを使用する必要があります。
- ASA または PIX 7.x+ デバイスで定義されるリモート アクセス VPN では、[Public Key Infrastructure] ポリシーは次のポリシーに直接関連していることに注意してください。これらのポリシーで定義されるすべてのトラストポイントも [Public Key Infrastructure] ポリシーで選択する必要があります。これはポリシーに自動的に追加されません。最初に、リモート アクセス VPN で必要な PKI 登録オブジェクトを判別するようこれらのポリシーを設定することもできます。
  - [接続プロファイル（Connection Profiles）] : CA トラストポイントを使用する必要がある IPsec 接続プロファイルの作成時に、[IPsec] タブでトラストポイントを識別する PKI 登録オブジェクトを選択します。
  - [SSL VPNアクセス（SSL VPN Access）] : インターフェイスごとにトラストポイントを設定して、フォールバック トラストポイントも設定できます。
  - [グローバル設定、IKEv2設定（Global Settings, IKEv2 Settings）] タブ : IKEv2 IPsec では、グローバルトラストポイントを指定する必要があります。

関連項目

- 使用する認証方式の決定 （1486 ページ）
- セレクタ内の項目のフィルタリング （60 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [公開キーインフラストラクチャ（Public Key Infrastructure）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [公開キーインフラストラクチャ（Public Key Infrastructure）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Public Key Infrastructure] ページが開き、現在使用可能な CA サーバと選択されている CA サーバ（PKI 登録オブジェクト）（存在する場合）が表示されます。

ステップ 2 必要な CA サーバーを定義する PKI 登録ポリシーオブジェクトを [使用可能なCAサーバー（Available CA Servers）] リストで選択して、[>>] をクリックして、[選択済みCAサーバー（Selected CA Servers）] リストに移動します。不要なオブジェクトを削除するには、選択済みリストでオブジェクトを選択して [<<] をクリックします。

（注） [サイト間VPN（Site-to-Site VPN）] で IKEv2 を設定し、認証方式として PKI を選択する場合、ここに表示される必要があるオブジェクト名を [選択済みCAサーバー（Selected CA Servers）] の下で指定する必要があります（サイト間 VPN での IKEv2 認証の設定 （1567 ページ）のステップ 2 を参照）。したがって、必要な CA サーバーが [選択済みCAサーバー（Selected CA Servers）] リストに含まれていることを確認してください。

ASA および PIX 7.x+ デバイスでは、選択されている PKI 登録オブジェクトのリストには、リモート アクセス VPN に対して定義されている接続プロファイルで指定されたすべてのオブジェクトが含まれている必要があります。接続プロファイルの詳細については、接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照してください。また、[Global Settings] ポリシーで IKEv2 に対して設定されているすべてのトラストポイントも含まれている必要があります。VPN グローバル IKEv2 設定 （1526 ページ）を参照してください。

リストされているオブジェクトを変更するには、次の手順を実行できます。

- 新しい PKI 登録オブジェクトを追加するには、使用可能なサーバーのリストの下にある [作成（Create）]（+）ボタンをクリックします。[Add PKI Enrollment] ダイアログボックスが開きます。PKI 登録オブジェクトの属性に関する詳細については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。
- 既存のオブジェクトの設定を変更するには、いずれかのリストでそのオブジェクトを選択して、[編集（Edit）]（鉛筆）ボタンをクリックします。

[PKI Enrollment] ダイアログボックス

[PKI Enrollment] ダイアログボックスを使用して、Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）登録オブジェクトを表示、作成、コピー、または編集します。PKI 登録オブジェクトは、ネットワーク内のデバイスからの証明書要求に応答する外部 Certification Authority（CA; 証明局）サーバを表します。

PKI 登録オブジェクトを作成して、デバイスが IPsec ネットワークの一部として証明書を交換するときに使用する CA サーバのプロパティを定義します。PKI 登録オブジェクトを作成する場合は、登録用のサーバ名および URL を定義します。このサーバーに登録するデバイスが、Simple Certificate Enrollment Process（SCEP）を使用して CA サーバー独自の証明書を取得するか、またはデバイス設定に手動で入力した証明書を使用するかを指定する必要があります。CA サーバが失効確認に使用するサポート方式も選択する必要があります。

（注） Security Manager でトラストポイントを作成またはインポートするために登録パラメータを定義する必要はありません。

さらに、任意で次を定義できます。

- CA サーバが Registration Authority（RA; 登録局）サーバとして機能するかどうかを指定します。

- 再試行の設定および RSA キー ペアの設定を含む、登録パラメータ。
- 証明書要求に含める追加の属性。
- PKI 階層においてこのサーバの上位に位置する、信頼できる CA サーバのリスト。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから [PKI登録（PKI Enrollments）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

ヒント このダイアログボックスは、リモートアクセスまたはサイト間 VPN の [公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーから開くこともできます。

関連項目

- Public Key Infrastructure ポリシーについて （1544 ページ）
- PKI 登録を正常に行うための前提条件 （1546 ページ）
- サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）
- サイト間 VPN での IKEv2 認証の設定 （1567 ページ）
- リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *346 : [PKI Enrollment]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
[CA Information] タブ	このタブを使用して、認証局サーバ、その証明書、およびその失効確認サポート レベルに関する設定値を入力します。特定の設定については、 [PKI Enrollment] ダイアログボックス - [CA Information] タブ （1556 ページ）を参照してください。

要素	説明
[Enrollment Parameters] タブ	このタブを使用して、PKI 登録に関する設定を入力します。特定の設定については、[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （1561 ページ）を参照してください。 （注） Security Manager でトラストポイントを作成またはインポートするために登録パラメータを定義する必要はありません。
[Certificate Subject Name] タブ	このタブを使用して、サブジェクト属性など、証明書に含める任意の情報を入力します。特定の設定については、[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）を参照してください。
[Trusted CA Hierarchy] タブ	このタブを使用して、階層フレームワークに配置する、信頼できる CA サーバを定義します。特定の設定については、[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （1566 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[PKI Enrollment] ダイアログボックス - [CA Information] タブ

[PKI Enrollment] ダイアログボックスの [CA Information] タブを使用して、次のことを実行できます。

- 外部 Certificate Authority（CA; 認証局）サーバの名前と位置を定義する。
- 証明書を手動で貼り付ける（既知の場合）。
- サーバーの失効確認サポートレベルを定義する。

ナビゲーション パス

[PKI 登録（PKI Enrollment）] ダイアログボックスに移動して、[CA 情報（CA Information）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （1561 ページ）
- [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）
- [PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （1566 ページ）

フィールド リファレンス

表 *347 : [PKI Enrollment]* ダイアログボックス - *[CA Information]* タブ

要素	説明
CA Server Nickname	証明書要求内の CA サーバの識別に使用する名前。このフィールドを空白のままにすると、ドメイン名が使用されます。Verisign CA の場合は、このフィールドを空白のままにする必要があります。また、次の点を考慮してください。 • 名前は同じであるが、URL が異なる 2 つの CA サーバは、同じデバイス上で設定できません。 • この CA 名は、同じ PKI 登録オブジェクトの一部として設定されている信頼できる CA の名前（[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （1566 ページ）で定義）と同じにできません。 • デバイスが VPN の一部として設定されている場合、いずれかのピアで使用される CA サーバ名と同じ CA サーバ名を使用する、デバイスレベルのオーバーライドを設定しないでください（これは、デバイスおよびそのピアが階層化された PKI 階層を使用する場合は問題になりません）。
Enrollment Type	実行する登録のタイプ。Security Manager は、URL 登録を設定している場合にだけ登録を実行します。別のタイプを選択する場合、独自の方法を使用して登録を実行する必要があります。 • [自己署名証明書（Self-Signed Certificate）]（ASA のみ）：**enrollment self** コマンドを設定する場合。 • [端末（Terminal）]（ASA のみ）：**enrollment terminal** コマンドを設定する場合。 • [URL]：CA サーバの URL を設定することで、自動登録を実行する場合。 • [None]：登録コマンドを設定しない場合。
プロトコル	SCEP CA URL または CMP CA URL のどちらを設定するかを指定します。

要素	説明
Enrollment URL （URL 登録のみ）	デバイスが登録を試行する先の CA サーバの URL。この URL は次の形式になります。 • [SCEP]：**http://CA_name:port** の形式の HTTP URL を使用します。ここで、CA_name は CA サーバーのホスト DNS 名または IP アドレスです。ポート番号は必須です。 • [TFTP]：**tftp://certserver/file_specification** の形式を使用します。CA サーバに直接アクセスできないときにこのオプションを使用します。TFTP サーバが、証明書要求および証明書を転送します。 • サポートされているその他の形式には、bootflash、cns、flash、ftp、null、nvram、rcp、scp、system などがあります。 （注） CA での CA cgi-bin スクリプト位置がデフォルト（/cgi-bin/pkiclient.exe）でない場合は、その標準以外のスクリプト位置を **http://CA_name:port/script_location** の形式で URL に含める必要があります。ここで、script_location は CA スクリプトへのフルパスです。

要素	説明
CA Certificate Source フィンガープリント（Fingerprint） 証明書 （URL 登録のみ）	証明書の取得方法： • [SCEP を使用した CA 証明書の取得（Retrieve CA Certificate Using SCEP）]（デフォルト）：ルータが、Simple Certificate Enrollment Process（SCEP）を使用して CA サーバーから証明書を取得するようにします。CA サーバのフィンガープリントを 16 進数形式で入力します。入力した値が証明書のフィンガープリントと一致しない場合、証明書は拒否されます。 フィンガープリントを使用して CA の証明書の真正性を確認すると、不正な第三者が、本物の証明書を偽の証明書に置き換えることを阻止できます。 ヒント　サーバーに直接アクセスして、または Web ブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、CA のフィンガープリントを取得できます。フィンガープリントの使用は、Cisco IOS ソフトウェアリリース 12.3(12) 以降、12.3(14)T 以降、12.4 以降（15.x を含む）、12.2(33)XNA 以降だけでサポートされます。 • [CA サーバーからの CA 証明書を手動で入力する（Enter CA Certificate from CA Server Manually）]：別のデバイスから最大 3 つの証明書をコピーし、[証明書（Certificate）] フィールドに貼り付けます（ブラウザの貼り付け機能、またはキーボードショートカット Ctrl+V を使用します）。PKI 登録オブジェクトが定義済み証明書を表すようにするには、このオプションを使用します。各証明書は、「certificate」という単語で始まり、「quit」という単語で終わる必要があります。CMP 認証では、認証に Base 64 でエンコードされた CA 証明書が必要です。CMP の場合、このフィールドで、Base 64 でエンコードされた CA 証明書を設定できます。Base 64 でエンコードされた CA 証明書を CA サーバーからコピーして貼り付け、最後に「quit」という単語を付けます。 （注）　証明書の詳細を「-----BEGIN CERTIFICATE----」という文字列と「----END CERTIFICATE----」という文字列の間に入力します。
CA 証明書のチェック	デフォルトでは、CA フラグのない証明書を CA 証明書として ASA にインストールできなくなりました。基本制約拡張は、証明書のサブジェクトが CA で、この証明書を含む有効な認証パスの最大深さかどうかを示すものです。バージョン 4.9 以降、Security Manager を使用すると、必要に応じて、これらの証明書のインストールを許可するように ASA を設定できます。この機能は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスでのみサポートされています。 デフォルトでは CA 証明書のチェックは有効になっています。

要素	説明
Revocation Check Support	実行する証明書失効確認のタイプ。 • [Checking Not Performed]：これがデフォルトです。デバイスは、CRL がデバイス上に存在する場合も、失効確認を実行しません。 • [CRL Check Required]：デバイスは CRL を確認する必要があります。デバイス上に CRL が存在せず、デバイスが CRL を取得できない場合、証明書は拒否され、トンネルは確立されません。 • [OCSP Check Required]：デバイスは、OCSP サーバからの失効ステータスをチェックする必要があります。チェックに失敗すると、その証明書は拒否されます。 • [CRL Check Attempted]：デバイスは、指定された LDAP サーバから最新の CRL をダウンロードしようとします。ダウンロードに失敗しても、証明書は受け入れられます。 • [OCSP Check Attempted]：デバイスは、OCSP サーバからの失効ステータスをチェックしようとします。チェックに失敗した場合でも、証明書は受け入れられます。 • [CRL or OCSP Check Required]：デバイスは最初に CRL に対するチェックを行います。CRL が存在しない、または取得できない場合、デバイスは OCSP サーバからの失効ステータスをチェックしようとします。両方のオプションが失敗した場合、証明書は拒否されます。 • [OCSP or CRL Check Required]：デバイスは、最初に OCSP サーバからの失効ステータスをチェックしようとします。このチェックが失敗すると、デバイスは CRL をチェックします。両方のオプションが失敗した場合、証明書は拒否されます。 • [CRL and OCSP Checks Attempted]：デバイスは、最初に CRL をチェックします。CRL が存在しない、または取得できない場合、デバイスは OCSP サーバからの失効ステータスをチェックしようとします。両方のオプションが失敗した場合でも、証明書は受け入れられます。 • [OCSP and CRL Checks Attempted]：デバイスは、最初に OCSP サーバからの失効ステータスをチェックしようとします。このチェックが失敗すると、デバイスは最新の CRL をダウンロードしようとします。両方のオプションが失敗した場合でも、証明書は受け入れられます。
OCSP Server URL	OCSP チェックを必須としている場合に、失効をチェックする OCSP サーバの URL。この URL は、**http://** で始まる必要があります。

要素	説明
CRL Server URL	CRL チェックを必須としている場合に、CRL をダウンロードできる LDAP サーバの URL。この URL は、**ldap://** で始まる必要があります。 （注） AAA サーバを ASA デバイスで使用する場合は、ポート番号を URL に含める必要があります。含めないと、LDAP が失敗します。
Enable Registration Authority Mode (PIX 6.3)	PIX 6.3 デバイスの場合に、CA サーバが Registration Authority（RA; 登録局）モードで動作するかどうかを指定します。登録局は、実際の CA のプロキシとして動作するサーバであるため、CA サーバがオフラインの場合でも CA の運用を続行できます。 （注） Cisco IOS ルータは、必要に応じて、RA モードを自動的に設定します。

[PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ

[PKI Enrollment] ダイアログボックスの [Enrollment Parameters] タブを使用して、デバイスが CA サーバに接続するときに使用する再試行設定、および証明書に関連付ける RSA キー ペアを生成するための設定を定義します。

PKI 登録オブジェクトが Microsoft CA を表す場合、ルータのアイデンティティの検証に必要なチャレンジパスワードを定義できます。

（注） Security Manager でトラストポイントを作成またはインポートするために登録パラメータを定義する必要はありません。

ナビゲーション パス

[PKI登録（PKI Enrollment）] ダイアログボックスに移動して、[登録パラメータ（Enrollment Parameters）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [CA Information] タブ （1556 ページ）
- [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）
- [PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （1566 ページ）

フィールド リファレンス

表 348 : [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ

要素	説明
Challenge Password 確認（Confirm）	CA サーバがデバイスの ID を検証するために使用するパスワード。このパスワードは、PIX 6.3 デバイスの場合は必須ですが、PIX/ASA 7.0+ デバイスおよび Cisco IOS ルータの場合は任意です。 CA サーバに直接アクセスして、または Web ブラウザにアドレス（**http://URLHostName/certsrv/mscep/mscep.dll**）を入力して、パスワードを取得できます。このパスワードは、CA サーバから取得した時間から 60 分間有効です。したがって、パスワードは、作成後、できるだけ迅速に配布する必要があります。 （注） 各パスワードは、単一デバイスごとの単一登録に対して有効です。このため、VPN の各デバイスにデバイスレベルのオーバーライドを最初に設定している場合を除き、このフィールドが VPN に対して定義されている PKI 登録オブジェクトを割り当てることは推奨しません。詳細については、個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。
Retry Period	証明書要求の試行間隔（分数）。値には 1 ～ 60 分を指定できます。デフォルトは 1 分です。
再試行回数（Retry Count）	最初の要求時に証明書が発行されていない場合、実行する再試行回数。値には 1 ～ 100 を指定できます。デフォルトは 10 です。
Certificate Auto-Enrollment （IOS デバイスのみ）	現在の証明書のライフタイムのパーセンテージです。ルータは、このパーセンテージに達してから新しい証明書を要求します。たとえば、70 を入力した場合、ルータは、現在の証明書のライフタイムが 70% に達成したあとに、新しい証明書を要求します。値の範囲は 10 ～ 100 % です。 値を指定しない場合、ルータは、古い証明書が期限切れになってから、新しい証明書を要求します。
自動登録の有効化（Enable Auto-Enrollment）	有効にすると、設定可能なトリガーに基づいて証明書が自動的に要求されます。 次の具体的なパラメータを設定することもできます。 • CMPv2 アップデートを使用するかどうか • いつトリガーするか • 現在のキーペアが使用されるか、新しいキーペアが生成されるか

要素	説明
Certificate Auto-Enrollment （ASA 9.7.1 以降）	現在の証明書のライフタイムのパーセンテージです。ルータは、このパーセンテージに達してから新しい証明書を要求します。たとえば、50 と入力した場合、ルータは、現在の証明書のライフタイムが 50% に達してから新しい証明書を要求します。値の範囲は 10 ～ 99% です。 値を指定しない場合、ルータは、古い証明書が期限切れになってから、新しい証明書を要求します。 （注） デフォルト値は 70% です。
自動登録再生成キー（Auto Enroll Regenerate Key）（ASA 9.7.1 以降）	選択して、証明書を更新する際に新しいキーを生成します。
キー ペアの再生成（Regenerate Key Pair）（ASA 9.7.1 以降）	選択して、トラストポイント要求を登録する前に、新しいキー ペアを再生成します。
共有キー（Shared Key）（ASA 9.7.1 以降）	アウトオブバンドで CA から取得したユーザーログイン情報を指定します。この情報は、CA および ASA が交換するメッセージの信頼性および整合性を確認するために使用されます。キー長は、64 文字以下です。 （注） 共有キーは「参照:共有キー」の形式にする必要があります。
証明書の署名（Signing Certificate）（ASA 9.7.1 以降）	CMP 登録要求に署名するために使用された、以前の発行済みデバイス証明書を含むトラストポイントの名前を指定します。
（注） CMP プロトコルの場合、セキュリティ上の理由から、[証明書（Certificate）]、[共有キー（Shared Key）]、[証明書の署名（Signing Certificate）] などのオプションは検出されません。その結果、PKI 登録ダイアログでは再検出時にオーバーライドが作成されます。	
キーペア（Key Pair）	すべての CMP 手動および自動登録用に自動的に新しいキーペアが生成されます。この機能をサポートするために、トラストポイントでキーペアパラメータを設定する機能が追加されました。 キー ペアの生成に使用するアルゴリズム（RSA または EDCSA）を選択します。 （注） RSA アルゴリズムには、係数オプション（1024| 2048| 4096| 512|768）があります。EDCSA アルゴリズムには、キーペアを生成するための楕円曲線オプション（256|384|521）があります。

要素	説明
デバイスのシリアル番号を含める（Include Device's Serial Number）	デバイスのシリアル番号を証明書に含めるかどうかを指定します。 ヒント CA は、このシリアル番号を使用して、証明書を認証するか、またはあとで証明書を特定のデバイスに関連付けます。シリアル番号を含めるかどうか判断できない場合は、デバッグに役立つため、含めてください。
RSA Key Pair Name （PIX 7.0+、ASA、IOS デバイスのみ）	証明書に関連付けるキー ペアがすでに存在する場合、このフィールドでは、そのキー ペアの名前を指定します。 キー ペアが存在しない場合、このフィールドでは、登録時に生成されるキー ペアに割り当てる名前を指定します。 （注） RSA キー ペアを指定しない場合、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が代わりに使用されます。PIX デバイスおよび ASA デバイスでは、展開の前にデバイス上にキーペアが存在する必要があります。
RSA Key Size （IOS デバイスのみ）	キー ペアが存在しない場合は、必要なキー サイズ（係数）をビットで定義します。512 ～ 1024 の係数が必要な場合は、64 の倍数となる整数を入力します。1024 よりも大きい値が必要な場合は、1536 または 2048 を入力します。推奨サイズは 1024 です。 （注） 係数のサイズが大きくなるほど、キーがよりセキュアになります。ただし、係数のサイズが大きいキーほど、生成に時間がかかり（512 ビットより大きい場合は 1 分以上）、交換するときの処理にも時間がかかります。
RSA Encryption Key Size （IOS デバイスのみ）	個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ。

要素	説明
送信元インターフェイス（Source Interface） （IOS デバイスおよび ASA 9.5(1) 以降）	認証中、登録中、および失効リストの取得時に、CA または LDAP サーバに送信されるすべての発信接続の送信元アドレス。このパラメータは、CA サーバまたは LDAP サーバが、（ファイアウォールなどが原因で）接続の生成元のアドレスに応答できない場合に必要となる場合があります。 このフィールドで値を定義しない場合、発信インターフェイスのアドレスが使用されます。 インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） Cisco Security Manager 4.9 は、ASA 9.5(1) 以降を実行しているデバイスの管理トラフィック用に個別のルーティングテーブルをサポートしています。この機能により、ASA 上の他のデータトラフィックから管理トラフィックを完全に分離できます。IOS デバイスとは別に、ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスを選択できるようになりました。

[PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ

[PKI Enrollment] ダイアログボックスの [Certificate Subject Name] タブを使用して、CA サーバに送信される証明書要求内のデバイスに関する追加情報を任意で定義します。この情報は、証明書に格納され、このルータから証明書を受信するすべての第三者が表示できます。

標準の LDAP X.500 形式を使用して、すべての情報を入力します。

ナビゲーション パス

[PKI登録（PKI Enrollment）] ダイアログボックスに移動して、[証明書のサブジェクト名（Certificate Subject Name）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [CA Information] タブ （1556 ページ）
- [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （1561 ページ）
- [PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ （1566 ページ）

フィールド リファレンス

表 349 : [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ

要素	説明
FQDN を含める	デバイスの完全修飾ドメイン名（FQDN）を証明書要求に含めるかどうかを指定します。 この名前は、[Hostname] ポリシーから取得されます（有効な完全修飾ドメイン名を取得するには、このポリシーでホスト名とドメイン名の両方を必ず指定してください）。ホスト名ポリシーを設定しない場合、この名前は Security Manager のデバイスの表示名 *display_name*.**null** から取得されますが、望ましい結果を得られない可能性が高くなります。
デバイスの IP アドレスを含める	IP アドレスが証明書要求に含まれているインターフェイス。 インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Common Name（CN）	証明書に含める X.500 共通名。
Organization Unit (OU)	証明書に含める組織単位の名前（部門名など）。 （注） Cisco Easy VPN Remote コンポーネントの PKI 登録オブジェクトを設定する場合、このフィールドには、コンポーネントが接続するクライアント グループの名前を含める必要があります。含めないと、このコンポーネントは接続できません。ただし、この情報は、設定の問題は発生しないなどの理由から、Easy VPN サーバでは必須ではありません。Easy VPN の詳細については、Easy VPN について （1599 ページ）を参照してください。
Organization（O）	証明書に含める組織名または会社名。
Locality（L）	証明書に含める都市。
州（State）（ST）	証明書に含める州。
Country（C）	証明書に含める国。
Email (E)	証明書に含める電子メール アドレス。

[PKI Enrollment] ダイアログボックス - [Trusted CA Hierarchy] タブ

[PKI Enrollment] ダイアログボックスの [Trusted CA Hierarchy] タブを使用して、階層 PKI フレームワーク内に信頼できる CA サーバを定義します。このフレームワーク内で、すべての登録済

みピアは、信頼できるルート CA 証明書または共通の下位 CA を共有している場合、互いの証明書を検証できます。

（PKI 登録オブジェクトとして定義されている）CA サーバを選択して [Available Servers] リストの階層に含め、[>>] をクリックしてそれらのサーバを選択済みリストに移動します。サーバを削除するには、この反対を実行します。

必要な PKI 登録オブジェクトをまだ定義していない場合は、使用可能なサーバーリストの下の [作成（Create）]（+）ボタンをクリックして、オブジェクトを作成します。必要な場合は、オブジェクトを選択し、[編集（Edit）] ボタンをクリックして、オブジェクトの定義を変更することもできます。

ナビゲーション パス

[PKI登録（PKI Enrollment）] ダイアログボックスに移動して、[信頼できるCA階層（Trusted CA Hierarchy）] タブをクリックします。このダイアログボックスを開く方法については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。

関連項目

- [PKI Enrollment] ダイアログボックス - [CA Information] タブ （1556 ページ）
- [PKI Enrollment] ダイアログボックス - [Enrollment Parameters] タブ （1561 ページ）
- [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）

サイト間 VPN での IKEv2 認証の設定

サイト間 VPN で IKE Version 2（IKEv2; IKE バージョン 2）を設定する場合は、認証設定を定義するよう [IKEv2 Authentication] ポリシーを設定する必要があります。IKEv1 と異なり、認証設定は、IKEv2 プロポーザルの一部ではありません。

Security Manager では、サイト間 VPN の IKEv2 認証を設定する際に、VPN トポロジで使用するデフォルト設定を行います。例外をデフォルトに設定して、VPN の特定のセグメントに異なる事前共有キーまたはトラストポイントを指定できます。事前共有キーとトラストポイントの混合を使用できます。たとえば、グローバル事前共有キーを設定して、VPN の選択したメンバーにはトラストポイントを設定できます。

IKEv2 トンネルの非対称認証の設定

IKEv2 を使用すると、IKEv1 とは異なり非対称認証を使用できます。これは、2 つのピアが、異なる事前共有キーまたは異なるトラストポイントを使用したり、1 つのピアが事前共有キーを使用して、他のピアがトラストポイントを使用したりできることを意味します。Security Manager では、次の操作を行って、非対称認証を設定できます。

- [グローバルIKEv2認証設定（Global IKEv2 Authentication Settings）] タブで、自動生成キーを選択して、[すべてのトンネルに同じキー（Same Keys for All Tunnel）] または [トンネルのエンドポイントに同じキー（Same Key at Tunnel Endpoints）] オプションを選択**しない**場

合は、異なる事前共有キーを設定できます。各トンネルの終端ごとに異なる事前共有キーが生成されます。

- [Override IKEv2 Authentication Settings] タブで、グローバル設定のオーバーライドを作成できます。ローカル ピアとリモート ピアのサブセットに異なるキーまたはトラストポイントを指定するオーバーライドを追加します。デバイスまたは特定のトンネルに複数のオーバーライドを作成できるため、ピアが認証する事前共有キーとトラストポイントのセットを設定できます。

ヒント [IKEv2 Authentication] ポリシーは共有ポリシーではありません。IKEv2 ネゴシエーションをサポートする VPN トポロジごとにポリシーを設定する必要があります。すべての VPN トポロジで使用するグローバル IKEv2 認証オプションは設定できません。[Create VPN] ウィザードの使用時に、IKEv2 をサポートするよう選択する場合でも、[IKEv2 Authentication] ポリシーが設定されることはありません。

はじめる前に

[IKEv2 Authentication] ポリシーは、[IKE Proposal] ポリシーと [IPsec Proposal] ポリシーの VPN で IKEv2 をイネーブルにする場合、およびトポロジ内の少なくとも一部のデバイスが IKEv2 をサポートする場合にかぎり使用されます。

IKEv2 を設定するには、デバイスは、ASA ソフトウェアリリース 8.4(1) 以降が実行されている ASA でなければなりません。デバイス サポートの詳細については、各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）を参照してください。

ヒント トポロジで IKEv2 だけをサポートする場合は、検証の警告を回避するために、[IKEv1 Preshared Keys] ポリシーと [IKEv1 Public Key Infrastructure] ポリシーの割り当てを解除してください。

関連項目

- IKE について （1482 ページ）
- 使用する認証方式の決定 （1486 ページ）

ステップ 1 [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタで（IKEv2 をサポートする）通常の IPsec トポロジを選択して、ポリシーセレクタで [IKEv2認証（IKEv2 Authentication）] を選択します。

ポリシーの参照情報については、[IKEv2 Authentication] ポリシー （1570 ページ）を参照してください。

ステップ 2 [グローバルIKEv2認証設定（Global IKEv2 Authentication Settings）] タブで、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブでオーバーライドが設定されていない VPN 内のデバイスに使用する必要がある認証タイプを設定します。VPN 内のほとんどのデバイスで使用されるオプションを選択します。グローバル事前共有キーまたはトラストポイントを設定できます。

- [グローバル事前共有キー（Global Preshared Keys）]：グローバル事前共有キーを設定するには、[キーの仕様（Key Specification）] を選択して、次のいずれかのオプションを設定します。
  - [User Defined]：必要なグローバル キーを入力して、[Confirm] フィールドに再度入力します。
  - [Auto Generated]：生成する必要があるキーの長さを入力して、すべてのトンネルに同じキーを使用するか、単一のトンネルの両方の終端で同じキーを使用するかを選択します。いずれのオプションも選択しない場合は、すべてのエンド ポイントで固有のキーが生成されます。

新しいキーを生成するには、[キーの登録（次回の展開時）（Regenerate Key (On Next Deployment)）] を選択することもできます。これによって、VPN のキーを定期的に再生成できます。このチェックボックスは、次回に展開が正常に行われたあとでオフにされます。

- [グローバルトラストポイント（CAサーバー）（Global Trustpoint (CA Servers)）]：トラストポイント証明書認可を設定するには、[PKIの仕様（PKI Specification）] を選択して、認証局（CA）サーバーを識別する PKI 登録オブジェクトの名前を入力します。

（注） PKI ポリシーで展開されたものと同じオブジェクト名を入力していることを確認します（リモートアクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）のステップ 2 を参照）。

[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

- [IKEv2認証ペイロードにSHA1で署名（Sign IKEv2 Authentication Payload with SHA1）]：IKEv2 ペイロードで SHA1 認証を有効にするには、このチェックボックスをオンにします。このオプションは、Cisco Security Manager 4.19 および ASA 9.12(1) 以降のデバイスでのみ使用できます。

ステップ 3 特定のデバイスのグローバル IKEv2 認証設定をオーバーライドする場合は、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブをクリックして、次のいずれかを実行します。

- オーバーライドを追加するには、[行の追加（+）（Add Row (+)）] ボタンをクリックし、[IKEv2認証（IKEv2 Authentication）] ダイアログボックスに入力します。オーバーライドを作成するローカル ピアとリモート ピアを選択して、使用する必要がある CA サーバの事前共有キーを指定します。[IKEv2 Authentication (Override)] ダイアログボックス （1572 ページ）を参照してください。
- オーバーライドを編集するには、テーブルでそのオーバーライドを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- オーバーライドを削除するには、テーブルでオーバーライドを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

（注） オーバーライド IKEV2 認証設定は、ハブアンドスポーク VPN およびフルメッシュ VPN トポロジにのみ適用されます。

（注） サイト間 VPN で非対称認証を設定できます。ここでは、トンネルの両側で異なる事前共有キーを使用できます。サイト間トポロジの一部であるピアデバイスごとに、IKEv2 認証用の非対称キーを作成するには、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに 2 つの行を追加する必要があります。詳細については、[IKEv2 Authentication (Override)] ダイアログボックス （1572 ページ）を参照してください。

[IKEv2 Authentication] ポリシー

[IKEv2 Authentication] ポリシーを使用して、サイト間 VPN で Internet Key Exchange（IKE; インターネット キー交換）バージョン 2 のデバイス認証設定を行います。これらの設定は、ASA 8.4(1)+ デバイスだけに適用されます。IKEv2 認証の設定の詳細については、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。

ポリシーには 2 つのタブが含まれています。

- [Global IKEv2 Authentication Settings]：グローバル設定は、[Overrides] タブでオーバーライドが設定されている場合を除き、VPN 内のすべてのデバイスに適用されます。VPN 内のほとんどのデバイスで使用される認証スキームを表すグローバル設定を行います。
- [Override IKEv2 Authentication Settings]：オーバーライド設定によって、固有の認証設定が特定のトンネルに適用され、VPN内のさまざまなトンネルで必要な固有の事前共有キーとトラストポイントの組み合わせを作成できます。このタブで行う設定は、最初に使用され、常にグローバル設定に優先されます。

ナビゲーション パス

[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開き、VPN セレクタで（IKEv2 をサポートする）通常の IPsec トポロジを選択して、ポリシーセレクタで [IKEv2認証（IKEv2 Authentication）] を選択します。

このポリシーは、共有ポリシーとしては使用できません。

関連項目

- IKE について （1482 ページ）
- サイト間 VPN の IPsec プロポーザルについて （1500 ページ）
- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

フィールド リファレンス

表 *350 : [IKEv2 Authentication]* ポリシー

要素	説明
[Global IKEv2 Authentication Settings] タブ	
Key Specification	VPN での認証に事前共有キーを使用します。次のいずれかを設定します。 • [ユーザー定義（User Defined）]：必要なグローバルキーを入力して、[確認（Confirm）] フィールドに再度入力します。キーは 1 ～ 128 文字の範囲で指定できます。 • [自動生成（Auto Generated）]：Security Manager にキーを生成させます。キーを生成する方法を示す次のオプションを指定します。 • [キーの長さ（Key Length）]：生成するキーの長さ（1 ～ 128）。 • [すべてのトンネルに同じキーを生成（Same Keys for All Tunnels）]：VPN 内のすべてのトンネルに同じキーを生成するには、このオプションを選択します。このオプションを選択しない場合は、トンネルごとに異なるキーまたはキー ペア（[Same Key for Tunnel Endpoints] を選択した場合）が使用されます。 • [トンネルエンドポイントに同じキーを生成（Same Key for Tunnel Endpoints）]：VPN 内の各トンネルの各終端で同じキーを生成するには、このオプションを選択します。このオプションを選択しない場合は、トンネルの各終端で異なるキーが生成されます。 • [キーの再生成（次の展開時）（Regenerate Key (On Next Deployment)）]：デバイスへの次の展開で新しいキーを生成するには、このオプションを選択します。これによって、VPN のキーを容易に再生成できます。 展開が正常に行われたあとで、後続の展開でキーが再生成されないように、このチェックボックスはオフにされます。VPN のキーを再生成するたびに、このオプションを選択します。
PKI Specification	IKEv2 接続のトラストポイントを定義する PKI 登録ポリシー オブジェクトの名前。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。PKI 登録オブジェクトを選択する場合や、新しいオブジェクトを作成する場合は、[選択（Select）] をクリックします。

要素	説明
[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブ	このテーブルには、VPN に対して定義されている IKEv2 認証オーバーライドがリストされます。これらのポリシーは、グローバル設定で定義された事前共有キーまたは PKI 設定に優先されます。オーバーライドを設定するには、次のいずれかを実行します。 • オーバーライドを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[IKEv2認証（IKEv2 Authentication）] ダイアログボックスに入力します。オーバーライドを作成するローカル ピアとリモート ピアを選択して、使用する必要がある CA サーバの事前共有キーを指定します。[IKEv2 Authentication (Override)] ダイアログボックス （1572 ページ）を参照してください。 • オーバーライドを編集するには、テーブルでオーバーライドを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • オーバーライドを削除するには、テーブルでオーバーライドを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。 （注） サイト間 VPN で非対称認証を設定できます。サイト間 VPN では、トンネルの各側で異なる事前共有キーを使用できます。サイト間トポロジの一部であるピアデバイスごとに IKEv2 認証用の非対称キーを作成するには、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに 2 つの行を追加する必要があります。詳細については、「[IKEv2 Authentication (Override)] ダイアログボックス （1572 ページ）」を参照してください。

[IKEv2 Authentication (Override)] ダイアログボックス

[IKEv2 Authentication] ダイアログボックスを使用して、サイト間 VPN の IKEv2 認証グローバル設定に対するオーバーライドを設定します。IKEv2 グローバル認証設定とオーバーライド認証設定の詳細については、サイト間 VPN での IKEv2 認証の設定 （1567 ページ）を参照してください。

ナビゲーション パス

[IKEv2認証（IKEv2 Authentication）] ポリシーの [IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブ（[IKEv2 Authentication] ポリシー （1570 ページ）を参照）で、[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルでオーバーライドを選択して [行の編集（Edit Row）]（鉛筆）をクリックします。

フィールド リファレンス

表 351 : [IKEv2 Authentication] ダイアログボックス

要素	説明
Local Peers Remote Peers	このオーバーライドを定義するトンネルのローカル側とリモート側。 リストにデバイスを追加するには、リストの右側にある [選択（Select）] ボタンをクリックして、[ローカルまたはリモートピアの選択（Local or Remote Peer Selection）] ダイアログボックスを開きます。このダイアログボックスで、[選択可能（Available）] リストで必要なピアを選択して、[>>] をクリックして [選択済み（Selected）] リストに移動します。逆の操作を行って（[<<] ボタンを使用して）、デバイスの選択を解除できます。 使用可能なデバイスのリストには、IKEv2 接続をサポートするデバイスだけが含まれています。これは、VPN 内のすべてのデバイスではないことがあります。
IKEv2 Authentication Mode	選択したローカル ピアとリモート ピア間で使用する IKEv2 認証モード。次のいずれかを選択します。 • [Key Specification]：ユーザ定義の事前共有キー（1 ～ 128 文字）。必要なキーを入力して、[Confirm] フィールドに再度入力します。 • [PKI Specification]：IKEv2 接続のトラストポイントを定義する PKI 登録ポリシー オブジェクトの名前。PKI 登録オブジェクトを選択する場合や、新しいオブジェクトを作成する場合は、[選択（Select）] をクリックします。

IKEv2 認証用の非対称キーの設定

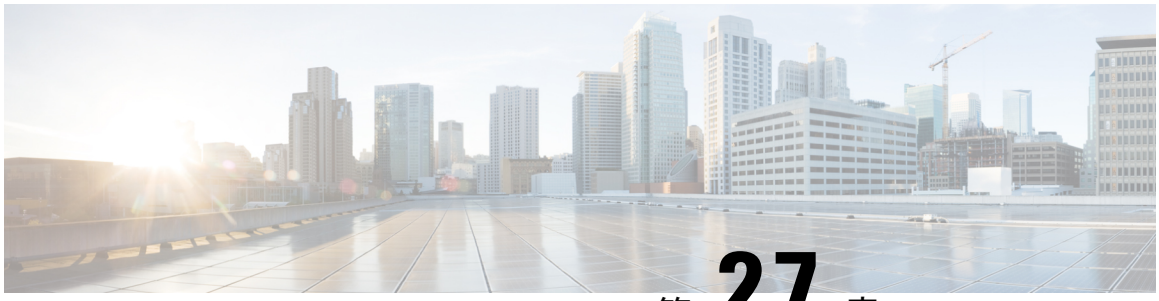
サイト間 VPN で非対称認証を設定できます。サイト間 VPN では、トンネルの各側で異なる事前共有キーを使用できます。サイト間トポロジの一部であるピアデバイスごとに、IKEv2 認証用の非対称キーを作成するには、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに 2 つの行を追加する必要があります。次の手順を実行します。

1. [IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブをクリックしてから、[行の追加（Add Row）]（+）ボタンをクリックします。[IKE認証（IKE Authentication）] ダイアログボックスが開きます。ピアの指定で、サイト間 VPN トポロジの一部であるローカルピアデバイスとリモートピアデバイスを選択します。[IKEv2認証モード（IKEv2 Authentication Mode）] で [キーの指定（Key Specification）] を選択し、キーを指定して確認します。Security Manager は、このキーを、選択したローカルピアデバイスのローカル事前共有キーと見なし、選択したリモートピアデバイスのリモート事前共有キーとも見なします。[OK] をクリックして、[IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブに戻ります。
2. [IKEv2認証設定のオーバーライド（Override IKEv2 Authentication Settings）] タブを選択した状態で、[行の追加（Add Row）]（+）ボタンをクリックします。[IKE認証（IKE

Authentication）] ダイアログボックスが開きます。ピアの指定で、ローカルピアの場合はステップ 1 のリモートピアデバイスを選択し、リモートピアの場合はステップ 1 のローカルピアデバイスを選択します。[IKEv2認証モード（IKEv2 Authentication Mode）] で [キーの指定（Key Specification）] を選択し、キーを指定して確認します。このキーは、ステップ 1 で指定したキーとは異なる必要があります。

次の表は、IKEv2 認証用の非対称キーの設定を示しています。

	ローカルピアデバイス	リモートピアデバイス	認証方式（事前共有キー）
行 1 を追加	ピア 1	Peer2	test123
行 2 を追加	Peer2	ピア 1	sample123



第 27 章

GRE および DM VPN

総称ルーティング カプセル化（GRE）、および GRE モード設定を含む Dynamic Multipoint（DM; ダイナミック マルチポイント）VPN を設定できます。ハブアンドスポーク トポロジ、ポイントツーポイント トポロジ、および完全メッシュ VPN トポロジに IPsec GRE VPN を設定できます。DMVPN は、ハブアンドスポーク トポロジだけで使用可能です。

この章は次のトピックで構成されています。

- [GRE Modes] ページについて （1575 ページ）
- GRE およびダイナミック GRE VPN （1576 ページ）
- ダイナミック マルチポイント VPN（DMVPN） （1586 ページ）

[GRE Modes] ページについて

[GRE Modes] ページを使用して、GRE、GRE ダイナミック IP、および DMVPN のポリシーで IPsec トンネリングについてルーティング パラメータおよびトンネル パラメータを定義します。

ポリシーの内容は、アクセスする方法によって異なります。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））GRE VPN または DMVPN を選択する場合は、[GRE Modes] ポリシーには、VPN で使用されるテクノロジーとテクノロジー タイプに関連するプロパティが含まれています。
- （ポリシービュー）[サイト間 VPN（Site-to-Site VPN）] > [GRE モード（GRE Modes）] を選択して、新しいポリシーを作成するか既存のポリシーを選択する場合は、ポリシーには [GRE 方式（GRE Method）] という追加のフィールドがあります。[GRE Method] リストから、ポリシーを定義する VPN テクノロジーとテクノロジー タイプとして [IPsec/GRE]、[GRE Dynamic IP]、[DMVPN]、または [Large Scale DMVPN] を選択する必要があります。このオプションは、ポリシーに表示されるフィールドを制御します。ポリシーの保存後は [GRE Method] を変更できません。

共有される [GRE モード（GRE Modes）] ポリシーを VPN に割り当てる場合は、[GRE 方式（GRE Method）] および VPN のテクノロジーとタイプが一致する必要があります。一致しな

い場合は、ポリシーを選択できません。たとえば、共有される [DMVPN GRE Modes] ポリシーを IPsec/GRE VPN に割り当てることはできません。

次のトピックで、選択した [GRE Methods] に基づいて [GRE Modes] ポリシーについて詳細に説明します。

- [IPsec/GRE] または [GRE Dynamic IP]： GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定 （1582 ページ）を参照してください。
- [DMVPN] または [Large Scale DMVPN]： DMVPN の [GRE Modes] の設定 （1590 ページ）を参照してください。

（注） IPsec/GRE、GRE ダイナミック IP、または DMVPN のルーティング ポリシーを設定する場合、Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、同じルーティング プロトコルと、[GRE Modes] ポリシーで定義した自律システム（またはプロセス ID）番号を使用して（各メンバー デバイスで）ルータ プラットフォーム ポリシーを作成する必要があります。

関連項目

- GRE について （1577 ページ）
- 動的にアドレス指定されるスポークの GRE 設定について （1580 ページ）
- DMVPN について （1587 ページ）
- IPsec テクノロジーおよびポリシーについて （1384 ページ）

GRE およびダイナミック GRE VPN

Generic Routing Encapsulation（GRE）を使用して、ハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、完全メッシュ VPN トポロジにおいて Cisco IOS セキュリティ ルータおよび Catalyst 6500/7600 デバイスを使用する VPN を作成できます。

ここでは、次の内容について説明します。

- GRE について （1577 ページ）
- IPsec GRE VPN の設定 （1581 ページ）
- GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定 （1582 ページ）

GRE について

Generic Routing Encapsulation（GRE）は、IP トンネルにさまざまなプロトコル パケット タイプをカプセル化し、IP ネットワーク経由でリモート ポイントのデバイスへの仮想的なポイントツーポイント接続を作成するトンネリング プロトコルです。このテクノロジーでは、GRE によって、IPsec 処理の前に元のパケット全体が標準 IP ヘッダーおよび GRE ヘッダーでカプセル化されます。その後、IPsec では、GRE パケットは通常の IP パケットであると認識されて、IKE のネゴシエーションされたパラメータに従って暗号化サービスおよび認証サービスが実行されます。GRE ではマルチキャスト トラフィックおよびブロードキャスト トラフィックを伝送できるため、仮想 GRE トンネルにルーティング プロトコルを設定できます。ルーティング プロトコルによって接続の切断が検出されると、パケットはバックアップ GRE トンネルに再ルーティングされるため、高い耐障害性が提供されます。

VPN の耐障害性を確保するためには、スポークにおいて、プライマリ ハブとバックアップ ハブへの 2 つの GRE トンネルを設定する必要があります。どちらの GRE トンネルも、IPsec によって保護されます。各トンネルは、独自の IKE Security Association（SA; セキュリティ アソシエーション）および IPsec SA のペアを持っています。関連付けられたルーティング プロトコルによって、フェールオーバー メカニズムが自動化され、仮想リンクの切断が検出されるとバックアップ トンネルに転送されます。

（注） GRE は、ハブアンドスポーク VPN トポロジ、ポイントツーポイント VPN トポロジ、および完全メッシュ VPN トポロジの Cisco IOS セキュリティ ルータと Catalyst 6500/7600 デバイスに設定できます。

ここでは、次の内容について説明します。

- GRE を使用した IPsec トンネリングの利点 （1577 ページ）
- Security Manager における GRE の実装 （1578 ページ）
- GRE を正常に設定するための前提条件 （1578 ページ）
- 動的にアドレス指定されるスポークの GRE 設定について （1580 ページ）

GRE を使用した IPsec トンネリングの利点

GRE を使用した IPsec トンネリングの主な利点は次のとおりです。

- GRE では、すべての IPsec ピアが他のすべてのピアのステータスを常に把握できるルーティング プロトコルが使用されます。
- GRE では、IKE キープアライブよりも高い耐障害性が実現されます。
- GRE を使用すると、スポーク間の接続がサポートされます。
- GRE では、マルチキャスト伝送およびブロードキャスト伝送がサポートされます。

（注） GRE では、ダイナミック クリプト トンネルの使用はサポートされていません。

Security Manager における GRE の実装

Security Manager では、GRE 用に追加の Interior Gateway Protocol（IGP）ソリューションが実装されています。IGP とは、ルーティング プロトコル（EIGRP、OSPF、または RIP）によって相互にルーティング更新を受信するデバイスのグループを指しています。各「ルーティンググループ」は、論理番号によって識別されます。一般的なルーティングのために、ネットワーク内のルータのインターフェイスは 1 つの IGP に属しています。Security Manager によって、IPsec および GRE によって保護された通信専用の追加の IGP が追加されます。この追加の IGP が保護された IGP です。既存の IGP（保護されていない IGP）は、暗号化を必要としないトラフィックのルーティングに使用されます。

GRE トンネルを確立するために、Security Manager によって各デバイスに仮想インターフェイスが設定されます。これらの仮想インターフェイスは、GRE トンネルのエンドポイントとなります。それぞれの仮想インターフェイスは固有です。GRE トンネル インターフェイスには、Security Manager によって作成されるインターフェイスから取得された IP アドレス（内部トンネル IP アドレス）が設定されます。GRE トンネルは、各デバイスの物理インターフェイスまたはループバック インターフェイスのいずれかの送信元 IP アドレスおよび宛先 IP アドレスを指しています。GRE 仮想インターフェイスは、内部インターフェイスと同様に保護された IGP に属しています。保護された IGP 内でのルーティング更新は、GRE でカプセル化され、IPsec が適用されます。保護されたインターフェイス宛のフロー（保護された IGP のルーティング更新によって判断されます）は、GRE インターフェイスから送信されます。このフローは、GRE インターフェイスで GRE によってカプセル化されて、クリプト ACL に対して評価されます。クリプト ACL に一致すると、GRE および VPN トンネル経由でルーティングされます。

GRE を正常に設定するための前提条件

ネットワークで GRE を使用する前に、次の前提条件を考慮してください。

- デバイスの内部インターフェイス（デバイスを内部サブネットおよび内部ネットワークに接続するデバイス上の物理インターフェイス）を特定する必要があります。
- GRE をイネーブルにする場合は、常にルーティング プロトコル（IGP と呼ばれています）またはスタティック ルートを選択する必要があります。

Security Manager では、EIGRP、OSPF、RIPv2 というダイナミック ルーティング プロトコル、および GRE スタティック ルートがサポートされています。

- • EIGRP：Enhanced Interior Gateway Routing Protocol を使用すると、自律システム内でルーティング情報を交換でき、大規模な異種ネットワークにおけるルーティングに関連するいくつかのより困難な問題に対処できます。他のプロトコルと比較して、EIGRP にはより優れたコンバージェンス特性が備えられています。また、効率的な運用が可能で、複数の異なるプロトコルの利点を兼ね備えています。詳細については、Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）を参照してください。

- OSPF：Open Shortest Path First は、最小コストでのルーティング機能、マルチパス ルーティング機能、およびロード バランシング機能を備えた、階層型リンク ステート プロトコルです。

OSPF を使用すると、ルーティング テーブルの変更を取得したホスト、またはネットワークの変更を検出したホストは、その情報をすぐにネットワーク内の他のすべてのホストにマルチキャストするため、すべてのホストが同じルーティング テーブル情報を保持できます。詳細については、Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）を参照してください。

- RIPv2：Routing Information Protocol は、定期的にルーティング更新メッセージを送信する距離ベクトル プロトコルです。ネットワーク トポロジが変更された場合にもルーティング更新メッセージが送信されます。

RIPv2 を使用すると、（ルータ機能を備えた）ゲートウェイ ホストは、30 秒ごとに最も近いネイバー ホストにルーティング テーブル全体を送信します。そのネイバー ホストからも次のネイバーに情報が渡され、最終的にネットワーク内のすべてのホストに同じルーティング パス情報が渡されます。RIPv2 では、ホップ カウントを使用してネットワーク上の距離が判断されます。ネットワーク内のルータ機能を備えた各ホストは、ルーティング テーブル情報を使用して、指定した宛先へのパケットをルーティングする次のホストを判断します。

RIP は、小規模な同種ネットワークにおいて効率的なソリューションです。RIP では 30 秒ごとにルーティング テーブル全体が送信されるため、より複雑で大規模なネットワークにおいては、ネットワーク上に大量の余剰トラフィックが流れる可能性があります。詳細については、Cisco IOS ルータにおける RIP ルーティング （3384 ページ）を参照してください。

- スタティック ルート：2 つのデバイス間に固定されて変更されないルートがある場合には、スタティック ルーティング ポリシーを使用して、IPsec によって保護され、堅牢かつ安定した GRE トンネルを提供できます。各デバイスのサブネットでは、対応するトンネル インターフェイスを指すスタティック ルートがデバイスに作成されます。詳細については、Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）を参照してください。

- IGP プロセス番号を指定する必要があります。IGP プロセス番号によって、デバイスの内部インターフェイスが属する IGP プロセスが特定されます。GRE の実装時には、これは保護された IGP となります。セキュアな通信を行うために、VPN 内のデバイスの内部インターフェイスでは同じ IGP プロセスを使用する必要があります。IGP プロセス番号は、指定された範囲内である必要があります。デバイスに、この範囲内ではあるが、GRE 設定に指定された IGP プロセス番号とは異なる既存の IGP プロセスがある場合、Security Manager によって既存の IGP プロセスが削除されます。GRE 設定に指定された番号に一致する既存の IGP プロセスがある場合、既存の IGP プロセスに含まれ、指定された内部インターフェイスに一致しないすべてのネットワークは削除されます。
- デバイスの内部インターフェイスが、GRE 設定に指定された IGP プロセス以外の IGP プロセスを使用するように設定されている場合（つまり、インターフェイスが保護されていない IGP に属している場合）は、次の作業を行います。

- スポークの場合：GRE を設定する前に、デバイス CLI を使用して、保護されていない IGP から内部インターフェイスを手動で削除します。
- ハブの場合：ハブの内部インターフェイスが Security Manager のネットワーク アクセス ポイントとして使用されている場合は、展開時に、このインターフェイスが保護された IGP と保護されていない IGP の両方にアドバタイズされます。スポーク ピアで保護された IGP だけが使用されるようにするには、保護されていない IGP に手動で auto-summary コマンドを追加するか、またはその内部インターフェイスの保護されていない IGP を手動で削除します。

- ループバックには、一意でグローバルにルーティング可能でないサブネットを指定する必要があります。このサブネットは、GRE のループバックの実装をサポートするためにだけ使用する必要があります。ループバック インターフェイスは、Security Manager によってだけ作成、維持、および使用されます。他のいかなる目的にも使用できません。
- 保護されていない IGP ではないスタティック ルートを使用する場合は、ハブの内部インターフェイス経由のスタティック ルートをスポークに設定する必要があります。

（注） 上記の設定は、IPsec テクノロジーとして IPsec/GRE が選択されている場合に、[GRE Modes] ページで設定できます。

動的にアドレス指定されるスポークの GRE 設定について

スポークにダイナミック IP アドレスがある場合、（スポーク側で GRE トンネルによって使用される）固定の GRE トンネル ソース アドレスまたは（ハブ側で GRE トンネルによって使用される）送信先アドレスはありません。そのため、Security Manager によってハブおよびスポークに追加のループバック インターフェイスが作成されて、GRE トンネル エンドポイントとして使用されます。Security Manager がループバック インターフェイスの IP アドレスを割り当てることのできるサブネットを指定する必要があります。

（注） GRE ダイナミック IP は、ハブアンドスポーク VPN トポロジの Cisco IOS ルータおよび Catalyst 6500/7600 デバイスにだけ設定できます。

Security Manager は、Cisco Configuration Engine を使用して、動的にアドレス指定されるデバイスからデバイスの IP アドレスやその他の情報を取得します。ダイナミック IP アドレスを持つデバイスは定期的に Configuration Engine マネージャに接続して、デバイス設定ファイルをアップグレードし、デバイス情報およびステータス情報を渡します。

詳細については、Auto Update Server または Configuration Engine の追加、編集、または削除（130 ページ）を参照してください。

（注） GRE ダイナミック IP 設定は、IPsec テクノロジーとして GRE ダイナミック IP が選択されている場合に、[GRE Modes] ページで設定できます。

関連項目

- GRE について （1577 ページ）
- DMVPN の [GRE Modes] の設定 （1590 ページ）

IPsec GRE VPN の設定

IPsec Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）VPN を設定するには、エクストラネット VPN の作成または編集 （1469 ページ）の説明に従って [Create VPN] ウィザードを使用します。説明されている手順を使用して、VPN のメンバーシップ、またはそのポリシーの一部を編集することもできます。動的にアドレス指定されたスポークを使用してハブアンドスポーク VPN を作成する場合は、動的にアドレス指定されるスポークの GRE 設定について （1580 ページ）も参照してください。

他のポリシーや設定を変更する必要がある場合は、[Site-to-Site Manager] ページで次のようにポリシーを開きます。

- ISAKMP および IPSec 設定の場合は、[VPNグローバル設定（VPN Global Settings）] を選択します。 VPN グローバル設定 （1517 ページ）を参照してください。
- IKE プロポーザルポリシーの場合は、[IKEプロポーザル（IKE Proposal）] を選択します。 IKE プロポーザルの設定 （1488 ページ）を参照してください。
- IPSec プロポーザルの場合は、[IPsecプロポーザル（IPsec Proposal）] を選択します。 サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）を参照してください。
- 事前共有キーポリシーの場合は、[IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。 IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。
- 公開キー（PKI）ポリシーの場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] を選択します。 サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。
- 総称ルーティングカプセル化の設定では、[GREモード（GRE Modes）] を選択します。 DMVPN の [GRE Modes] の設定 （1590 ページ） を参照してください。

関連項目

- IKE について （1482 ページ）
- GRE について （1577 ページ）
- GRE を正常に設定するための前提条件 （1578 ページ）

• GRE を使用した IPsec トンネリングの利点 （1577 ページ）

GRE または GRE ダイナミック IP VPN の [GRE Modes] の設定

[GRE Modes] ポリシーを使用して、GRE または GRE ダイナミック IP VPN で IPsec トンネリングのルーティング パラメータおよびトンネル パラメータを定義します。

[GRE Modes] ポリシーを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））[IPsec/GRE] または [GREダイナミックIP（GRE Dynamic IP）] トポロジを選択して、ポリシーリストから [GREモード（GRE Modes）] を選択します。
- （ポリシービュー）[サイト間VPN（Site-to-Site VPN）] > [GREモード（GRE Modes）] を選択して、新しいポリシーを作成するか、既存のポリシーを選択します。その後、[GRE メソッド（GRE Method）] リストから [IPsec/GRE] または [ダイナミックGRE（Dynamic GRE）] のいずれかを選択します。

次の表に、GRE または GRE ダイナミック IP に IPsec トンネリングを設定するための [GRE Modes] ページの要素を示します。

（注） GRE ルーティング ポリシーを設定する場合、Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、同じルーティング プロトコルと、[GRE Modes] ポリシーで定義した自律システム（またはプロセス ID）番号を使用して（各メンバー デバイスで）ルータ プラットフォーム ポリシーを作成する必要があります。

表 *352 : GRE* または *GRE* ダイナミック *IP VPN* の *[GRE Modes]* ページ

要素	説明
[Routing Parameters] タブ	
ルーティング プロトコル（Routing Protocol）	GRE または GRE ダイナミック IP に使用する、必要なダイナミック ルーティング プロトコル（EIGRP、OSPF、または RIPv2）、あるいはスタティック ルートを選択します。 デフォルトのルーティング プロトコルは EIGRP です。 これらのプロトコルの設定の詳細については、GRE を正常に設定するための前提条件 （1578 ページ）を参照してください。

要素	説明
AS 番号（AS Number） （EIGRP だけ）	EIGRP パケットが属する自律システム（AS）領域の識別に使用する数値。範囲は 1 ～ 65535 です。デフォルトは 110 です。 自律システム（AS）は、共通のルーティング ストラテジを共有するネットワークのコレクションです。AS は、連続したネットワークおよび接続ホストのグループであるいくつかの領域に分割できます。複数のインターフェイスがあるルータは、複数の領域に参加できます。AS ID は、パケットが属する領域を識別します。すべての EIGRP パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ AS 番号が必要です。
Hello 間隔（Hello Interval） （EIGRP だけ）	インターフェイスで送信される hello パケットの間隔を 1 ～ 65535 秒の間で指定します。デフォルトは 5 秒です。
保留時間（Hold Time） （EIGRP だけ）	ルータが接続を無効化する前に hello メッセージの受信を待機する秒数。範囲は 1 ～ 65535 です。デフォルトのホールド時間は 15 秒（hello の間隔の 3 倍）です。
遅延 （EIGRP だけ）	プライマリ ルート インターフェイスのスループット遅延（マイクロ秒単位）。トンネル遅延時間の範囲は 1 ～ 16777215 です。デフォルトは 1000 です。
Failover Delay （EIGRP だけ）	フェールオーバー ルート インターフェイスのスループット遅延（マイクロ秒単位）。トンネル遅延時間の範囲は 1 ～ 16777215 です。デフォルト値は 1500 です。
帯域幅 （EIGRP だけ）	プライマリ ルート インターフェイスで EIGRP パケットに使用可能な帯域幅の量。プライマリ ルートが他のルートよりも優先されるように値を入力する必要があります。 1 ～ 10000000 kb の値を入力できます。デフォルトは 1000 kb です。 （注） デフォルトでは、インターフェイスでパケットを送信する場合のコストは帯域幅に基づいて計算されます。帯域幅が広いほど、コストは低くなります。
Failover Bandwidth （EIGRP だけ）	フェールオーバー ルート インターフェイスで EIGRP パケットに使用可能な帯域幅の量。 1 ～ 10000000 kb の値を入力します。デフォルトは 1000 kb です。

要素	説明
Process Number （OSPF だけ）	Security Manager が GRE の設定時に追加する保護された IGP の識別に使用されるルーティング プロセス ID 番号。 範囲は 1 ～ 65535 です。デフォルトは 110 です。 Security Manager によって、IPsec および GRE によって保護された通信専用の追加の Interior Gateway Protocol（IGP）が追加されます。IGP とは、ルーティング プロトコルによって相互にルーティング更新を受信するデバイスのグループを指しています。各「ルーティンググループ」は、プロセス番号によって識別されます。 詳細については、GRE について （1577 ページ）を参照してください。
Hub Network Area ID （OSPF だけ）	トンネルサブネットを含めて、ハブの保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を指定できます。デフォルトは 0 です。
Spoke Protected Network Area ID （OSPF だけ）	トンネル サブネットを含め、リモート保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を指定できます。デフォルトは 1 です。
認証 （OSPF または RIPv2 だけ）	OSPF または RIPv2 認証キーを指定する文字列。文字列は最大 8 文字の長さにすることができます。
コスト（Cost） （OSPF または RIPv2 だけ）	プライマリ ルート インターフェイスでのパケットの送信コスト。 選択したプロトコルが OSPF の場合は、1 ～ 65535 の範囲の値を入力します。デフォルトは 100 です。 選択したプロトコルが RIPv2 の場合は、1 ～ 15 の範囲の値を入力します。デフォルトは 1 です。
Failover Cost （OSPF または RIPv2 だけ）	セカンダリ（フェールオーバー）ルート インターフェイスでのパケットの送信コスト。 OSPF では 1 ～ 65535 の値（デフォルトは 125）を、RIPv2 では 1 ～ 15 の値（デフォルトは 2）を入力できます。
Filter Dynamic Updates on Spokes	選択されている場合、スポークにおけるすべてのダイナミック ルーティング更新をフィルタリングする再配布リストの作成がイネーブルになります。これにより、スポーク デバイスは他の IP アドレスではなく固有の保護サブネットだけをアドバタイズ（ハブ デバイスで読み込み）するよう強制されます。
[Tunnel Parameters] タブ	

要素	説明
Tunnel IP	GRE または GRE ダイナミック IP トンネル インターフェイスの IP アドレスを指定する必要なオプションを選択します。 • [物理インターフェイスを使用（Use Physical Interface）]：選択されている場合、保護ネットワークから取得されたトンネルのプライベート IP アドレスが使用されます。 • [サブネットを使用（Use Subnet）]：選択されている場合、IP 範囲から取得されたトンネル IP アドレスが使用されます。これがデフォルトです。 [Subnet] フィールドに、一意のサブネット マスクを含むプライベート IP アドレスを入力します（デフォルトは 1.1.1.0/24 です）。 ダイヤル バックアップ インターフェイスも設定する場合は、用意された [Dial Backup Subnet] フィールドにそのサブネットを入力します（デフォルトは 1.1.2.0/24 です）。 （注） ほとんどの場合、サブネットを使用して GRE トンネル インターフェイスの IP アドレスを指定すると、Security Manager によって、トンネルの IP アドレスに使用されるループバック インターフェイスがデバイスに作成されます。Security Manager によって設定が検出された VPN トポロジにデバイスが属しており、デバイスの GRE トンネルに直接 IP アドレスを設定する場合は、Security Manager によってその設定が維持されて、デバイスにループバック インターフェイスは作成されません。ただし、VPN トポロジ内のハブには常にループバックが設定されます。複数のハブがあるハブアンドスポーク VPN トポロジでは、スポークにもループバック インターフェイスが設定されます。 • [ループバックインターフェイスを使用（Use Loopback Interface）]：選択されている場合、既存のループバック インターフェイスから取得されたトンネル IP アドレスが使用されます。[ロール（Role）] フィールドに、ループバック インターフェイス名を定義するインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 （注） 新しい GRE トンネルまたはループバック インターフェイスを [Router Interfaces] ページに表示するには、VPN をデバイスに正常に展開したあとでデバイス インベントリの詳細を再検出する必要があります。

要素	説明
Configure Unique Tunnel Source for each Tunnel	イネーブルになっている場合、VPN の各 GRE トンネル インターフェイスに一意のトンネル ソースが割り当てられます。[トンネルソースのIP範囲（Tunnel Source IP Range）] フィールドに、トンネルソースとして使用するサブネット IP を入力します。 （注） イネーブルになっている場合、この機能は、VPN 内のすべての GRE トンネル インターフェイスに設定されます。1 つのインターフェイスに特定のトンネル ソースを割り当てる場合は、Peers ポリシーを使用して、目的のデバイスにエンドポイントを設定します。エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。
Tunnel Source IP Range （GRE ダイナミック IP だけ）	一意のサブネット マスクを含む、GRE のループバックをサポートするプライベート IP アドレス。GRE トンネル インターフェイスの IP アドレス（内部トンネル IP アドレス）は、Security Manager がループバック専用に作成するループバック インターフェイスから取得されます。 スポークにダイナミック IP アドレスがある場合、（スポーク側で GRE トンネルによって使用される）固定の GRE トンネル ソース アドレスまたは（ハブ側で GRE トンネルによって使用される）送信先アドレスはありません。そのため、Security Manager によってハブおよびスポークに追加のループバック インターフェイスが作成されて、GRE トンネル エンドポイントとして使用されます。Security Manager がループバック インターフェイスの IP アドレスを割り当てることのできるサブネットを指定する必要があります。
Enable IP Multicast	選択されている場合は、GRE トンネル間でマルチキャスト送信をイネーブルにします。IP マルチキャストは、最小限のネットワーク帯域幅を使用して、送信元または受信側に負荷をかけることなく複数の受信側にアプリケーション ソース トラフィックを配信します。
ランデブー ポイント	[Enable IP Multicast] チェックボックスをオンにした場合にだけ使用可能です。 必要に応じて、マルチキャスト送信のランデブー ポイント（RP）として機能するインターフェイスの IP アドレスを入力できます。送信元は RP にトラフィックを送信します。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。

ダイナミック マルチポイント VPN（DMVPN）

Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）とは、Generic Routing Encapsulation（GRE）トンネル、IP Security（IPsec; IP セキュリティ）暗号化、および Next Hop Resolution Protocol（NHRP）ルーティングを組み合わせることによって、大規模および小規模

な IPsec VPN におけるスケーラビリティを向上できるハブアンドスポーク VPN テクノロジーです。

ここでは、次の内容について説明します。

- DMVPN について （1587 ページ）
- DMVPN の設定 （1589 ページ）
- DMVPN の [GRE Modes] の設定 （1590 ページ）
- 大規模 DMVPN の設定 （1595 ページ）
- 大規模 DMVPN でのサーバ ロード バランシングの設定 （1596 ページ）

DMVPN について

Dynamic Multipoint VPN（DMVPN; ダイナミック マルチポイント VPN）では、Generic Routing Encapsulation（GRE）トンネル、IP Security（IPsec; IP セキュリティ）暗号化、および Next Hop Resolution Protocol（NHRP）ルーティングを組み合わせることによって、大規模および小規模な IPsec VPN におけるスケーラビリティを向上できます（大規模 DMVPN の詳細については、大規模 DMVPN の設定 （1595 ページ）を参照してください）。

Security Manager では、EIGRP、OSPF、RIPv2 というダイナミック ルーティング プロトコル、および GRE スタティック ルートを使用する DMVPN がサポートされています。On-Demand Routing（ODR; オンデマンド ルーティング）もサポートされています。ODR は、ルーティング プロトコルではありません。ハブアンドスポーク VPN トポロジにおいて、スポーク ルータがハブ以外の他のルータに接続していない場合に使用できます。ダイナミック プロトコルを実行しているネットワーク環境では、ODR は適していません。

DMVPN は、ハブアンドスポーク VPN トポロジにおいて、Cisco IOS ソフトウェア リリース 12.3T デバイス以降を実行するデバイス、または Cisco IOS XE ソフトウェア 2.x 以降（Security Manager では 12.2(33)XNA+ と呼ばれています）を実行する ASR だけで使用できます。DMVPN は、Catalyst VPN サービス モジュール デバイス、またはハイ アベイラビリティ（HA）グループではサポートされていません。デバイスで DMVPN がサポートされていない場合は、GRE ダイナミック IP を使用して、動的にアドレス指定されるスポークに GRE を設定します。動的にアドレス指定されるスポークの GRE 設定について （1580 ページ）を参照してください。

次のトピックでは、DMVPN の概要について説明します。

- DMVPN トポロジでのスポーク間接続のイネーブル化 （1588 ページ）
- DMVPN を使用した GRE の利点 （1589 ページ）

Cisco.com の次のマニュアルには、DMVPN の詳細が記載されています。

- 『*Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications*』：DMVPN テクノロジーおよびこのテクノロジーを使用する場所と理由が説明されています。このデータ シートでは、DMVPN とともに使用されるテクノロジー、およびこれらのテクノロジーによって得られる利点について説明します。

- 『*Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3*』：フェーズ 2 およびフェーズ 3 のスポーク間接続の違いが説明されています。スポーク間接続の作成は、DMVPN での設定オプションです。フェーズ 3 では、ショートカット スイッチングという拡張機能を使用して、ネットワークのパフォーマンスとスケーラビリティを向上できます。
- 追加のホワイトペーパーとプレゼンテーションは、http://www.cisco.com/en/US/products/ps6658/prod_literature.html で入手できます。

DMVPN トポロジでのスポーク間接続のイネーブル化

DMVPN を使用して、従来のハブアンドスポーク接続が、スポーク間に動的に作成された直接の IPsec トンネルによって補われる完全メッシュ VPN を実質的に作成できます。直接のスポーク間トンネルでは、リモート サイト間のトラフィックは、ハブを通過する必要はありません。これによって、追加の遅延がなくなり、WAN 帯域幅を節約できます。スポーク間機能は、シングルハブまたはマルチハブ環境でサポートされます。マルチハブ展開では、スポーク間の復元力と冗長性が向上します。

80:20 トラフィック ルールを使用して、基本のハブアンドスポーク トポロジを使用するか、直接のスポーク間接続を許可するかを判別できます。

- スポークからの 80 % 以上のトラフィックをハブ ネットワーク自体に転送する場合は、ハブアンドスポーク モデルを展開します。
- 20 % を超えるトラフィックが他のスポーク用である場合は、スポーク間モデルを検討します。

IP マルチキャスト トラフィックが大量にあるネットワークでは、通常ハブアンドスポーク モデルが推奨されます。

DMVPN の [GRE Modes] ポリシーを設定する場合は、これらの直接接続を作成するためにスポークを許可することを選択できます。これらの接続に使用する DMVPN フェーズを選択する必要があります。

- [フェーズ2（Phase 2）]：スポーク間接続はリージョナルハブを通過し、ハブからスポークへのルーティングプロトコル更新はサマライズされません。
- [フェーズ3（Phase 3）]（デフォルト）：スポークは、相互の直接接続を作成でき、ハブからスポークへのルーティング更新はサマライズされます。このオプションを使用すると、スケーラビリティが最大になり、遅延が低減されます。デバイスは IOS ソフトウェア リリース 12.4(6)T 以降を実行している必要があります。ASR は IOS XE ソフトウェア リリース 2.4（12.2(33)XND と呼ばれる）以降を実行している必要があります。Security Manager は、それより低い OS バージョンが実行されているデバイスではフェーズ 2 設定を自動的に作成します。

[GRE Modes] ポリシーの設定に関する詳細については、DMVPN の [GRE Modes] の設定 （1590 ページ）を参照してください。

関連項目

- DMVPN について （1587 ページ）
- 『*Cisco Dynamic Multipoint VPN: Simple and Secure Branch-to-Branch Communications*』
- 『*Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3*』

DMVPN を使用した GRE の利点

DMVPN を使用した GRE には、次の利点があります。

- **ハブにおける GRE 設定の簡素化**

GRE では、ハブにおいて、接続された各スポークに対してトンネルが設定されます。GRE と DMVPN を使用すると、すべての接続されたスポークに対してトンネルが 1 つだけ設定されます。

- **動的にアドレス指定されるスポークのサポート**

GRE を使用する場合、ハブ ルータを設定するときに、スポーク ルータの物理インターフェイス IP アドレスを GRE トンネルの宛先アドレスとして設定する必要があります。DMVPN を使用すると、スポーク ルータに動的な外部インターフェイス IP アドレスを設定できます。また、外部インターフェイス IP アドレスが変更された場合でも設定をデバイスに再展開する必要がなく、設定が堅固になります。スポークがオンラインになると、スポークの物理インターフェイス IP アドレスが含まれた登録パケットをハブに対して送信します。

- **直接のスポーク間通信用のダイナミック トンネルの作成**

NHRP では、スポーク ルータは、VPN ネットワーク内のルータの外部インターフェイス IP アドレスを動的に学習できます。NHRP を使用すると、ハブにすべてのスポーク（クライアント）のパブリック インターフェイス アドレスの NHRP データベースが保持されます。各スポークは、起動時にハブに対してスポークの実際のアドレスを登録します。

スポークは、他のスポークにパケットを送信する必要がある場合、NHRP を使用して、宛先スポークの必要な宛先アドレスを動的に決定できます。ハブは、送信元スポークの要求を処理する NHRP サーバとして動作します。これにより、ハブ ルータを経由せずにスポーク ルータ間で直接の IPsec および GRE トンネルを動的に作成でき、それによりハブにおいて複数回暗号化と復号化を繰り返すことによる遅延を低減できます。

DMVPN の設定

ハブアンドスポーク ダイナミック マルチポイント VPN を設定するには、 VPN トポロジの作成または編集 （1416 ページ）の説明に従って [Create VPN] ウィザードを使用します。説明されている手順を使用して、VPN のメンバーシップ、またはそのポリシーの一部を編集することもできます。大規模 DMVPN を作成する場合は、 大規模 DMVPN の設定 （1595 ページ）も参照してください。

他のポリシーや設定を変更する必要がある場合は、[Site-to-Site Manager] ページで次のようにポリシーを開きます。

- ISAKMP および IPSec 設定の場合は、[VPNグローバル設定（VPN Global Settings）] を選択します。 VPN グローバル設定 （1517 ページ）を参照してください。
- IKE プロポーザルポリシーの場合は、[IKEプロポーザル（IKE Proposal）] を選択します。 IKE プロポーザルの設定 （1488 ページ）を参照してください。
- IPSec プロポーザルの場合は、[IPsecプロポーザル（IPsec Proposal）] を選択します。 サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）を参照してください。
- 事前共有キーポリシーの場合は、[IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。 IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。
- 公開キー（PKI）ポリシーの場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] を選択します。 サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。
- スポーク間のフェーズ 2 または 3 接続の選択を含め、Generic Routing Encapsulation の設定では、[GREモード（GRE Modes）] を選択します。 DMVPN の [GRE Modes] の設定 （1590 ページ）を参照してください。
- 大規模 DMVPN とともに使用するサーバー ロードバランシング ポリシーでは、[サーバーロードバランシング（Server Load Balance）] を選択します。 大規模 DMVPN でのサーバ ロード バランシングの設定 （1596 ページ） を参照してください。

関連項目

- IKE について （1482 ページ）
- DMVPN について （1587 ページ）
- DMVPN トポロジでのスポーク間接続のイネーブル化 （1588 ページ）
- DMVPN を使用した GRE の利点 （1589 ページ）

DMVPN の [GRE Modes] の設定

[GRE Modes] ポリシーを使用して、DMVPN で IPsec トンネリングのルーティング パラメータおよびトンネル パラメータを定義します。

[GRE Modes] ポリシーを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））[DMVPN] または [大規模DMVPN（Large Scale DMVPN）] トポロジを選択して、ポリシーリストから [GREモード（GRE Modes）] を選択します。
- （ポリシービュー）[サイト間VPN（Site-to-Site VPN）] > [GREモード（GRE Modes）] を選択して、新しいポリシーを作成するか、既存のポリシーを選択します。その後、[GRE

メソッド（GRE Method）] リストから [DMVPN] または [大規模DMVPN（Large Scale DMVPN）] のいずれかを選択します。

次の表に、DMVPN を設定するための [GRE Modes] ページの要素を示します。

（注） DMVPN ルーティング ポリシーを設定する場合、Security Manager によって、展開時に、保護された IGP 内のすべてのデバイスにルーティング プロトコルが追加されます。この保護された IGP を維持する場合は、同じルーティング プロトコルと、[GRE Modes] ポリシーで定義した自律システム（またはプロセス ID）番号を使用して（各メンバー デバイスで）ルータ プラットフォーム ポリシーを作成する必要があります。

表 *353 : [DMVPN] の [GRE Modes] ページ*

要素	説明
[Routing Parameters] タブ	
ルーティング プロトコル（Routing Protocol）	DMVPN トンネルで使用する、必要なダイナミック ルーティング プロトコルまたはスタティック ルートを選択します。 オプションには、EIGRP、OSPF、RIPv2 というダイナミック ルーティング プロトコル、および GRE スタティック ルートがあります。On-Demand Routing（ODR; オンデマンド ルーティング）もサポートされています。オンデマンド ルーティングは、ルーティング プロトコルではありません。ハブアンドスポーク VPN トポロジにおいて、スポーク ルータがハブ以外の他のルータに接続していない場合に使用できます。ダイナミック プロトコルを実行しているネットワーク環境では、オンデマンド ルーティングは適していません。 詳細については、GREについて （1577ページ）を参照してください。
AS 番号（AS Number） （EIGRP だけ）	EIGRP パケットが属する自律システム（AS）領域の識別に使用する数値。範囲は 1 ～ 65535 です。デフォルトは 110 です。 自律システム（AS）は、共通のルーティング ストラテジを共有するネットワークのコレクションです。AS は、連続したネットワークおよび接続ホストのグループであるいくつかの領域に分割できます。複数のインターフェイスがあるルータは、複数の領域に参加できます。AS ID は、パケットが属する領域を識別します。すべての EIGRP パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ AS 番号が必要です。
Hello 間隔（Hello Interval） （EIGRP だけ）	インターフェイスで送信される hello パケットの間隔を 1 ～ 65535 秒の間で指定します。デフォルトは 5 秒です。

要素	説明
保留時間（Hold Time） （EIGRP だけ）	ルータが接続を無効化する前にhelloメッセージの受信を待機する秒数。範囲は 1 ～ 65535 です。デフォルトのホールド時間は 15 秒（hello の間隔の 3 倍）です。
遅延 （EIGRP だけ）	プライマリ ルート インターフェイスのスループット遅延（マイクロ秒単位）。トンネル遅延時間の範囲は 1 ～ 16777215 です。デフォルトは 1000 です。
Bandwidth （EIGRP だけ）	プライマリ ルート インターフェイスの帯域幅（キロビット単位）。帯域幅の範囲は 1 ～ 10000000 です。デフォルトは 1000 です。
Bandwidth （EIGRP だけ）	プライマリ ルート インターフェイスでEIGRP パケットに使用可能な帯域幅の量。プライマリ ルートが他のルートよりも優先されるように値を入力する必要があります。 1 ～ 10000000 kb の値を入力できます。デフォルトは 1000 kb です。 （注） デフォルトでは、インターフェイスでパケットを送信する場合のコストは帯域幅に基づいて計算されます。帯域幅が広いほど、コストは低くなります。
Process Number （OSPF だけ）	Security Manager が DMVPN の設定時に追加する保護された IGP の識別に使用されるルーティング プロセス ID 番号。 いずれのプロトコルにおいても、有効な範囲は1 ～ 65535 です。デフォルトは 110 です。
Hub Network Area ID （OSPF だけ）	トンネルサブネットを含めて、ハブの保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を入力できます。デフォルトは 0 です。
Spoke Protected Network Area ID （OSPF だけ）	トンネル サブネットを含め、リモート保護ネットワークがアドバタイズされる領域の ID 番号。任意の数値を入力できます。デフォルトは 1 です。
認証キー（Authentication Key） （OSPF と RIPv2）	OSPF または RIPv2 認証キーを指定する文字列。文字列は最大 8 文字の長さにすることができます。
コスト（Cost） （OSPF と RIPv2）	プライマリ ルート インターフェイスでのパケットの送信コスト。 選択したプロトコルが OSPF の場合は、1 ～ 65535 の範囲の値を入力します。デフォルトは 100 です。 選択したプロトコルが RIPv2 の場合は、1 ～ 15 の範囲の値を入力します。デフォルトは 1 です。

要素	説明
Allow Direct Spoke to Spoke Connectivity	ハブを経由せずにスポーク間で直接通信を可能にするかどうか。使用する DMVPN フェーズを選択します。これにより、スポークが行うことができる接続のタイプが決定されます。 • [フェーズ2（Phase 2）]：スポーク間接続はリージョナルハブを通過し、ハブからスポークへのルーティングプロトコル更新はサマライズされません。 • [フェーズ3（Phase 3）]（デフォルト）：スポークは、相互の直接接続を作成でき、ハブからスポークへのルーティング更新はサマライズされます。このオプションを使用すると、スケーラビリティが最大になり、遅延が低減されます。デバイスは IOS ソフトウェアリリース 12.4(6)T 以降を実行している必要があります。ASR は IOS XE ソフトウェアリリース 2.4（12.2(33)XND と呼ばれる）以降を実行している必要があります。Security Manager は、それより低い OS バージョンが実行されているデバイスではフェーズ 2 設定を自動的に作成します。 フェーズ 2 と 3 の違いの詳細については、Cisco.com の『Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3』を参照してください。 （注） 直接のスポーク間通信を使用する場合は、事前共有キー ネゴシエーションで [Main Mode Address] オプションを使用する必要があります。詳細については、サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）を参照してください。
Filter Dynamic Updates On Spokes	DMVPN トンネルでオンデマンドルーティングまたはスタティック ルートを使用している場合には使用できません。 選択されている場合、スポークにおけるすべてのダイナミック ルーティング更新（EIGRP、OSPF、および RIPv2）をフィルタリングする再配布リストの作成がイネーブルになります。これにより、スポーク デバイスは他の IP アドレスではなく固有の保護サブネットだけをアドバタイズ（ハブ デバイスで読み込み）するよう強制されます。
[Tunnel Parameters] タブ	
Tunnel IP Range	一意のサブネット マスクを含む、内部トンネル インターフェイスの IP アドレスの IP アドレス範囲。このフィールドは、10.1.1.0/24 などのサブネットを定義します。 （注） トンネルインターフェイスの IP アドレスがデバイスにすでに存在すること、およびその IP アドレスがトンネルの IP サブネットのフィールドに一致することが Security Manager によって検出された場合は、そのインターフェイスが GRE トンネルとして使用されます。

要素	説明
Dial Backup Tunnel IP Range	ダイヤル バックアップ インターフェイスを設定する場合は、一意のサブネット マスクを含む、その内部トンネル インターフェイスの IP アドレス範囲を入力します。このフィールドはサブネットを定義します。
Server Load Balance	選択されている場合、複数のハブを使用する設定においてハブとして機能している Cisco IOS ルータでのロードバランシングの設定がイネーブルとなります。 サーバ ロード バランシングを使用すると、作業負荷を分散することによって、複数のハブを使用する設定においてパフォーマンスが最適化されます。この設定では、複数の DMVPN サーバ ハブが同じトンネル IP および送信元 IP アドレスを共有し、VPN トポロジのスパイクによって単一のデバイスのように認識されます。
Enable IP Multicast	選択されている場合は、GRE トンネル間でマルチキャスト送信をイネーブルにします。 IP マルチキャストは、最小限のネットワーク帯域幅を使用して、送信元または受信側に負荷をかけることなく複数の受信側にアプリケーション ソース トラフィックを配信します。
ランデブー ポイント	[Enable IP Multicast] チェックボックスをオンにした場合にだけ使用可能です。 必要に応じて、マルチキャスト送信のランデブー ポイント（RP）として機能するインターフェイスの IP アドレスを入力できます。送信元は RP にトラフィックを送信します。このトラフィックは、それから共有配信ツリーを下ってレシーバに転送されます。
トンネル キー（Tunnel Key）	トンネル キーを示す番号。デフォルトは 1 です。 トンネル キーは、multipoint GRE（mGRE; マルチポイント GRE）トンネル Non Broadcast Multiple Access（NBMA; 非ブロードキャスト マルチアクセス）ネットワークごとに異なります。同じ NBMA ネットワーク内のすべての mGRE インターフェイスでは同じトンネル キーの値を使用する必要があります。同じルータに 2 つの mGRE インターフェイスがある場合、これらのインターフェイスでは異なるトンネル キーの値を使用する必要があります。 （注） 新規に作成したトンネル インターフェイスを、VPN のメンバーであるルータの [Router Interfaces] ページに表示するには、VPN をデバイスに正常に展開したあとでデバイス インベントリの詳細を再検出する必要があります。
NHRP Parameters	

要素	説明
ネットワーク ID（Network ID）	1 つの論理 Non-Broadcast Multi-Access（NBMA; 非ブロードキャスト マルチアクセス）ネットワーク内のすべての Next Hop Resolution Protocol（NHRP）ステーションには、同じネットワーク ID を設定する必要があります。1 ～ 4294967295 の範囲の、グローバルに一意な 32 ビットのネットワーク ID を入力します。
保留時間	正規の NHRP 応答に指定されている情報をルータで保持する時間（秒数）。ホールド時間を経過すると、キャッシュされた IP から NBMA へのアドレス マッピング エントリは廃棄されます。 デフォルトは 300 秒です。
認証	送信元および宛先 NHRP ステーション間で相互に通信できるかどうかを制御する認証文字列。NHRP を使用している同じネットワーク内のすべてのルータが同じ認証文字列を共有する必要があります。文字列は最大 8 文字の長さにすることができます。

大規模 DMVPN の設定

数千のスポークで構成される可能性がある大規模な展開について DMVPN を設定できます。大規模 DMVPN トポロジでは、Server Load Balance（SLB; サーバ ロード バランス）デバイスとも呼ばれる IPsec ターミネータがスポークとハブとの間に設置されます。ハブは、IPsec ターミネータに直接接続されている必要があり、ハブと IPsec ターミネータとの間にはその他のデバイスは設置できません。

IPsec ターミネータ（Catalyst 6500/7600 デバイス）では暗号化および復号化が実行され、ハブでは Next Hop Resolution Protocol（NHRP）および multipoint Generic Routing Encapsulation（mGRE; マルチポイント GRE）に関連するすべてのタスクが処理されます。IPsec ターミネータは、ハブへの GRE トラフィックのロード バランスを特化して行うように設定されます。また、IPsec ターミネータには、任意のプロキシを経由する任意のスポークを受け入れるようにダイナミック クリプトが設定されます。スポークでトンネル保護を使用する場合、これらのプロキシは、GRE トラフィックに一致するように自動的に設定されます。スポークには、1 つの GRE トンネルが設定されます。同じ IPsec ターミネータに接続するすべてのハブは、同じトンネル IP アドレスを使用し、トンネル ソースは IPsec ターミネータの仮想 IP アドレスとなります。

Security Manager では、VPN トポロジの作成または編集 （1416 ページ）の説明に従って、新規ハブアンドスポーク VPN トポロジの作成中に大規模 DMVPN を設定します。既存の標準の DMVPN は編集できず、大規模 DMVPN に変換できません。大規模 DMVPN を作成する場合は、次の点に注意してください。

- VPN のテクノロジーを定義する場合は、テクノロジーとして [DMVPN]、タイプとして [IPsecターミネータを使用した大規模型（Large Scale with IPsec Terminator）] を選択します。手順については、VPN トポロジの名前および IPsec テクノロジーの定義 （1420 ページ）を参照してください。

- VPN のデバイスを選択する場合は、必要な IPsec ターミネータ（Catalyst 6500/7600 デバイス）、ハブ、およびすべてのスポークを選択します。手順については、 VPN トポロジのデバイスの選択 （1422 ページ）を参照してください。

IPsec ターミネータとハブは直接接続されている必要があります。

- エンドポイントを設定する場合は、 エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）の説明に従って、[Edit Endpoints] ダイアログボックスで次の項目を設定します。
  - [Hub Interface] タブで、各ハブ デバイスに対して、IPsec ターミネータに接続するインターフェイスを選択します。それぞれのハブは、1 つの IPsec ターミネータにだけ接続できます。また、保護されたネットワークを識別します。大規模 DMVPN 内の各ハブは自身と保護されたネットワークを識別する必要があります。
  - 大規模 DMVPN 内の IPsec ターミネータごとに、VPN 外部インターフェイス、暗号化エンジン スロット、および内部 VLAN を指定します。IPsec ターミネータでは、保護対象ネットワークは設定されません。

大規模 DMVPN トポロジの作成後、[Server Load Balance] ポリシーが、必要なすべてのパラメータを使用して IPsec ターミネータで設定されます。パラメータは、必要に応じて編集できます。最初に、すべてのハブに VPN 接続の同じプライオリティと番号が指定されます。[Server Load Balance] ポリシーの設定については、 大規模 DMVPN でのサーバ ロード バランシングの設定 （1596 ページ）を参照してください。

（注） 大規模 DMVPN では、VRF 対応 IPsec は設定できません。

関連項目

- DMVPN について （1587 ページ）
- DMVPN の設定 （1589 ページ）

大規模 DMVPN でのサーバ ロード バランシングの設定

[Server Load Balance] ページを使用して、大規模 DMVPN 内の IPsec ターミネータに設定される Server Load Balance ポリシーを表示または編集します。サーバ ロード バランシングを使用すると、ハブのグループ間で作業負荷を共有することによって、複数のハブアンドスポーク VPN トポロジにおけるパフォーマンスが最適化されます。大規模 DMVPN 設定では、IPsec ターミネータはトラフィックのロードバランシングを実行します。詳細については、大規模 DMVPN の設定 （1595 ページ）を参照してください。

Weighted Round Robin（WRR; 重み付けラウンドロビン）スケジューリング アルゴリズムを使用して、出力送信キューに割り当てられる帯域幅が制御されます。重み付けは、インターフェ

イスの各送信キューで使用される帯域幅の量に基づいて行われます。容量の大きいキューからのパケットは、容量の小さいキューからのパケットよりも高い頻度で送信されます。

[サーバーロードバランス（Server Load Balance）] ポリシーを開くには、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）で既存の大規模 DMVPN トポロジを選択して、[ポリシー（Policies）] リストから [サーバーロードバランス（Server Load Balance）] を選択します。

表には、VPN 内のハブ、同じ IPsec ターミネータに接続されているその他のハブに対するハブの相対的な重量、ハブで許可されるアクティブな接続の最大数が表示されます。重量または最大接続を変更するには、ハブを選択して、表の真下にある [Edit]（鉛筆）ボタンをクリックして、[Edit Load Balancing Parameters] ダイアログボックス （1597 ページ）を開きます。

関連項目

- 大規模 DMVPN の設定 （1595 ページ）
- テーブルのフィルタリング （64 ページ）

[Edit Load Balancing Parameters] ダイアログボックス

大規模 DMVPN において IPsec ターミネータに接続されているハブに設定されたサーバ ロード バランス パラメータを変更するには、[Edit Load Balancing Parameters] ダイアログボックスを使用します。

ナビゲーション パス

[Server Load Balance] ポリシーで、ハブを選択して、表の下にある **[Edit]（鉛筆）**ボタンをクリックします。[Server Load Balance] ポリシーを開く方法については、大規模 DMVPN でのサーバ ロード バランシングの設定 （1596 ページ）を参照してください。

関連項目

- 大規模 DMVPN の設定 （1595 ページ）

フィールド リファレンス

表 354 : [Edit Load Balancing Parameters] ダイアログボックス

要素	説明
重量	Weighted Round Robin（WRR; 重み付けラウンドロビン）スケジューリング アルゴリズムに基づいて、IPsec ターミネータに接続されている他のハブに対する、ハブの相対的な容量。 1 ～ 255 の値を入力できます。デフォルトは 1 です。
最大接続数（Max Connections）	ハブから IPsec ターミネータに対して許可されるアクティブな接続の最大数。 1 ～ 65535 の値を入力できます。デフォルトは 500 です。

第 28 章

Easy VPN

Easy VPN は、さまざまなルータ、PIX、および ASA デバイスで使用できるハブアンドスポーク VPN トポロジです。ほとんどのポリシーはハブで定義され、リモート スポーク VPN デバイスにプッシュされるため、クライアントには、セキュアな接続を確立する前に確実に最新のポリシーが配置されます。

この章は次のトピックで構成されています。

- Easy VPN について （1599 ページ）
- Easy VPN のクライアント接続特性の設定 （1607 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- Easy VPN における Connection Profile ポリシーの設定 （1616 ページ）
- Easy VPN における User Group ポリシーの設定 （1617 ページ）

Easy VPN について

Easy VPN を使用すると、リモート オフィスの VPN 展開が容易になります。Easy VPN では、ヘッドエンドに定義されたセキュリティ ポリシーがリモート VPN デバイスにプッシュされるため、クライアントには、セキュアな接続を確立する前に確実に最新のポリシーが配置されます。

Security Manager では、ハブアンドスポーク VPN トポロジにおける Easy VPN ポリシーの設定がサポートされています。このような設定では、ほとんどの VPN パラメータは、ハブ デバイスとして機能する Easy VPN サーバに定義されます。集中管理された IPsec ポリシーは、サーバによって Easy VPN クライアント デバイスにプッシュされるため、リモート（スパイク）デバイス設定を最小限に抑えることができます。

Easy VPN サーバーは、Cisco IOS ルータ、PIX ファイアウォール、または ASA 5500 シリーズ デバイスです。Easy VPN クライアントは、PIX 6.3 を実行する PIX 501、506、506E Firewall、Cisco 800 ～ 3900 シリーズ ルータ、および ASA ソフトウェア リリース 7.2 以降を実行する ASA 5505 デバイスでサポートされます。

バージョン 4.17 以降、Cisco Security Manager は BVI による Easy VPN のサポートを提供します。通常、Easy VPN は、ASA の起動時に最高および最低のセキュリティレベルのインターフェイスを判別します。最も低いセキュリティレベルのインターフェイスは、VPN クライアントが

ヘッドエンドへのトンネリングを開始する外部インターフェイスとして使用され、最も高いセキュリティレベルのインターフェイスは、内部のセキュリティで保護されたインターフェイスとして使用されます。

ASA5506 プラットフォームでは、デフォルト設定に、最高セキュリティ レベル インターフェイスを示す 100 に設定された BVI（そのメンバーインターフェイスもレベル 100 に設定）と、セキュリティレベルが 0 の外部インターフェイスが含まれます。VPN クライアントは、同じ最高セキュリティレベルの複数のインターフェイスを拒否します。Easy VPN によって同じ最高セキュリティレベルの複数のインターフェイスがあることが特定され、VPN クライアントが無効になります。

この問題を解決するために、ASA 9.9(2) 以降のすべての ASA 5506、5508、および 5512 [x/h/w] デバイスに vpnclient secure interface CLI が導入されました。そのため、Cisco Security Manager で CLI をサポートするために、バージョン 4.17 以降、新しいコンポーネント「VPN クライアント インターフェイス」がタイプ（Easy VPN）のハブアンドスポークトポロジに導入されました。

（注） Easy VPN トポロジで使用されるポリシーの中には、リモート アクセス VPN で使用されるポリシーに類似しているものもあります。リモート アクセス VPN では、ポリシーはサーバと VPN クライアント ソフトウェアを実行するモバイル リモート PC との間に設定されますが、サイト間 Easy VPN トポロジでは、クライアントはハードウェア デバイスです。

ここでは、次の内容について説明します。

- Easy VPN とダイヤル バックアップ （1600 ページ）
- ハイ アベイラビリティ Easy VPN （1601 ページ）
- Easy VPN とダイナミック仮想トンネル インターフェイス （1601 ページ）
- Easy VPN コンフィギュレーション モード （1602 ページ）
- Easy VPN および IKE 拡張認証（Xauth） （1603 ページ）
- Easy VPN の設定の概要 （1605 ページ）
- Easy VPN 設定に関する重要事項 （1606 ページ）

Easy VPN とダイヤル バックアップ

Easy VPN のダイヤル バックアップを使用すると、リモート クライアント デバイスにダイヤル バックアップ トンネル接続を設定できます。このバックアップ機能は、実際のトラフィックの送信準備が完了したときにだけアクティブになります。これにより、トラフィックがない場合に高価なダイヤルアップまたは ISDN リンクを作成および維持する必要がなくなります。

（注） Easy VPN ダイヤル バックアップは、IOS バージョン 12.3(14)T 以降を実行するルータであるリモート クライアントにだけ設定できます。

Easy VPN 設定では、リモート デバイスがサーバへの接続を試み、追跡された IP がアクセスできない場合には、プライマリ接続がティアダウンされて、Easy VPN バックアップ トンネル経由でサーバへの新しい接続が確立されます。プライマリ ハブに到達できない場合は、プライマリ設定が、バックアップ設定ではなく、同じプライマリ設定を持つフェールオーバー ハブに切り替えられます。

各プライマリ Easy VPN 設定では、1 つのバックアップ設定だけがサポートされています。各内部インターフェイスでは、プライマリおよびバックアップの Easy VPN 設定を指定する必要があります。Easy VPN リモート デバイスでダイヤル バックアップが動作するためには、IP スタティック ルート トラッキングが設定されている必要があります。オブジェクト トラッキング設定は、Easy VPN リモート ダイヤル バックアップ設定とは独立しています。オブジェクト トラッキングの詳細は、スポークの [エンドポイントの編集（Edit Endpoints）] ダイアログボックスで指定します。

ダイヤル バックアップの詳細については、ダイヤル バックアップの設定 （1432 ページ）を参照してください。

ハイ アベイラビリティ Easy VPN

Easy VPN トポロジ内のデバイスにハイ アベイラビリティ（HA）を設定できます。LAN 上で IP を実行する Cisco IOS ルータまたは Catalyst 6500/7600 デバイスに High Availability（HA; ハイ アベイラビリティ）を設定すると、自動デバイス バックアップ機能を使用できます。Easy VPN に、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブ デバイスで構成された HA グループを作成できます。詳細については、VPN トポロジにおけるハイ アベイラビリティの設定 （1450 ページ）を参照してください。

Easy VPN とダイナミック仮想トンネル インターフェイス

IPsec Virtual Tunnel Interface（VTI; 仮想トンネル インターフェイス）機能を使用すると、IPsec によって保護する必要がある、リモート アクセス リンク用の GRE トンネルの設定が簡素化されます。VTI は、IPsec トンネリングをサポートするインターフェイスです。VTI を使用すると、IPsec トンネルに直接インターフェイス コマンドを適用できます。仮想トンネル インターフェイスの設定では、クリプトマップが適用されている特定の物理インターフェイスに対する IPsec セッションのスタティック マッピングが不要であるため、オーバーヘッドが低減されます。

IPsec VTI では、任意の物理インターフェイスにおいて、ユニキャストとマルチキャストの両方の暗号化されたトラフィックがサポートされます（複数のパスがある場合など）。トラフィックは、トンネル インターフェイスから転送されるときに暗号化され、トンネル インターフェイスに転送されると復号化されます。また、IP ルーティング テーブルによって管理されます。

ダイナミックまたはスタティック IP ルーティングを使用して、仮想トンネル インターフェイスにトラフィックをルーティングできます。IP ルーティングを使用してトンネルインターフェイスにトラフィックを転送することによって、アクセス コントロール リスト（ACL）とクリプト マップを使用する複雑なプロセスと比較して IPsec VPN 設定が簡素化されます。ダイナミック VTI は、他のすべての実際のインターフェイスと同様に機能するため、トンネルがアクティブになるとすぐに Quality of Service（QoS）、ファイアウォール、およびその他のセキュリティ サービスを適用できます。

ダイナミック VTI では、IPsec インターフェイスの動的なインスタンス化および管理のために、仮想テンプレート インフラストラクチャが使用されます。Easy VPN トポロジでは、Security Manager によって暗黙的にデバイスに仮想テンプレートインターフェイスが作成されます。デバイスがハブの場合、ユーザは、ハブに仮想テンプレートインターフェイスとして使用される IP アドレスを指定する必要があります。この IP アドレスには、サブネット（アドレスのプール）、既存のループバック インターフェイス、または既存の物理インターフェイスを指定できます。スポークでは、仮想テンプレートインターフェイスは IP アドレスなしで作成されます。

Security Manager では、[Easy VPN IPsec Proposal] ページでダイナミック VTI を設定します。Easy VPN に対するダイナミック VTI の設定 （1614 ページ）を参照してください。

注記

- ダイナミック VTI は、ハブアンドスポーク VPN トポロジにおいて、IOS バージョン 12.4(2)T 以降を実行する 7600 デバイスを除くルータでだけ設定できます。PIX ファイアウォール、ASA デバイス、または Catalyst 6000 シリーズ スイッチではサポートされていません。
- 検出またはプロビジョニング中に、すべてのハブおよびスポークにダイナミック VTI 設定が必要なわけではありません。（dVTI をサポートしていないルータを含む）既存の Easy VPN トポロジを拡張して、dVTI をサポートするルータを追加できます。
- ダイナミック VTI は、サーバのみ、クライアントのみ（サーバが dVTI をサポートしていない場合）、およびクライアントとサーバの両方でサポートされます。
- dVTI が設定されたハブ（サーバ）には、ハイ アベイラビリティを設定できません。
- リモート アクセス VPN でもダイナミック VTI を設定できます。詳細については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （1900 ページ）を参照してください。

Easy VPN コンフィギュレーション モード

Easy VPN は、Client、Network Extension、および Network Extension Plus の 3 つのモードで設定できます。

- Client モード：クライアント サイトのデバイスがセントラル サイトのリソースにアクセスできるデフォルトの設定です。ただし、セントラル サイトからクライアント サイトのリソースへはアクセスできません。Client モードでは、VPN 接続が確立されると、単一の IP アドレスがサーバからリモート クライアントにプッシュされます。通常、このアドレスは、お客様のネットワークのプライベート アドレス空間内でルーティング可能なアドレス

です。Easy VPN トンネルを通過するすべてのトラフィックでは、そのプッシュされた単一の IP アドレスへのポート アドレス変換（PAT）が実行されます。

- Network Extension モード：セントラル サイトのユーザは、クライアント サイトのネットワーク リソースにアクセスできます。また、クライアント PC およびホストは、セントラル サイトの PC およびホストに直接アクセスできます。Network Extension モードでは、宛先ネットワークで完全にルーティング可能で、宛先ネットワークから到達可能な IP アドレスを VPN トンネルのクライアント側終端にあるホストに設定することが指定されます。接続の両端のデバイスは、一体となって 1 つの論理ネットワークを形成します。PAT は使用されないため、クライアント側終端のホストは、宛先ネットワークのホストに直接アクセスできます。つまり、ルーティング可能なアドレスが Easy VPN サーバ（ハブ）から Easy VPN クライアント（スポーク）に設定され、クライアントの背後にある LAN において PAT は実行されません。
- Network Extension Plus モード：Network Extension モードを機能拡張したもので、IOS ルータにだけ設定できます。モード設定を介して受信した IP アドレスを、使用可能なループバック インターフェイスに自動的に割り当てることができます。この IP アドレスを使用してルータに接続し、リモート管理およびトラブルシューティング（ping、Telnet、およびセキュア シェル）を行うことができます。このオプションの選択時に一部のクライアントが IOS ルータでない場合、それらのクライアントは Network Extension モードで設定されません。

（注） すべての動作モードで、スプリット トンネリングをサポートすることもできます。スプリット トンネリングを使用すると、VPN トンネル経由で企業リソースに安全にアクセスできることに加えて、ISP などのサービスへの接続を使用したインターネット アクセスも可能となります（そのため、Web アクセス用のパスから企業ネットワークを除外できます）。

Easy VPN のクライアント接続特性の設定 （1607 ページ）の説明に従って、Client Connection Characteristics ポリシー内のモードを設定します。

関連項目

- Easy VPN 設定に関する重要事項 （1606 ページ）
- Easy VPN について （1599 ページ）

Easy VPN および IKE 拡張認証（Xauth）

Easy VPN 設定で IPsec トンネルを確立するためのトンネル パラメータをネゴシエートする場合、IKE Extended Authentication（Xauth; 拡張認証）によって、IPsec 接続を要求するユーザを識別する、追加の認証レベルが追加されます。VPN サーバに Xauth が設定されている場合、IKE Security Association（SA; セキュリティ アソシエーション）の確立後、クライアントは「ユー

ザ名/パスワード」チャレンジを待機します。エンド ユーザがチャレンジに応答すると、その応答は IPsec ピアに転送され、さらに上のレベルの認証が行われます。

入力された情報は、RADIUS や TACACS+ などの認証、許可、アカウンティング（AAA）プロトコルを使用して認証エンティティに照らしてチェックされます。トークン カードは、AAA プロキシを介して使用することもできます。Xauth 中、ユーザのクレデンシャルが RADIUS を介して検証される場合に、そのユーザに固有の属性を取得できます。

（注） リモート クライアントを処理するように設定されている VPN サーバは、ユーザ認証を実行するように常に設定されている必要があります。

Security Manager では、Easy VPN トンネルを確立するたびにこれらのクレデンシャルを手動で入力する必要がないように、デバイス自体に Xauth ユーザ名およびパスワードを保存できます。情報は、デバイスの設定ファイルに保存され、トンネルが確立されるたびに使用されます。クレデンシャルをデバイスの設定ファイルに保存する方法は、一般的に、デバイスを複数の PC で共有し、VPN トンネルを常にアップ状態にする場合や、送信するトラフィックがある場合は常に自動的にデバイスでトンネルを確立する場合に使用します。

ただし、デバイスの設定ファイルにクレデンシャルを保存すると、デバイス設定にアクセスできるすべてのユーザーがこの情報を入手できるため、セキュリティ上のリスクとなる可能性があります。Xauth 認証のもう 1 つの方法として、Xauth が要求されるたびにユーザ名とパスワードを手動で入力する方法があります。クレデンシャルの入力に Web ブラウザ ウィンドウまたはルータ コンソールのどちらを使用するかを選択できます。Web ベースの対話形式を使用すると、ログインページが表示され、そのページで VPN トンネルを認証するためのクレデンシャルを入力できます。VPN トンネルが確立されると、このリモート サイトの背後のすべてのユーザは、再度ユーザ名とパスワードを求められることなく企業 LAN にアクセスできます。または、VPN トンネルを迂回して、インターネットにだけ接続することもできます。この場合、パスワードは必要ありません。

Easy VPN トンネル アクティベーション

デバイスのクレデンシャル（Xauth ユーザ名とパスワード）がデバイス自体に保存されている場合は、IOS ルータ クライアントのトンネルのアクティベーション方法を選択する必要があります。2 つのオプションから選択できます。

- [Auto]：Easy VPN トンネルは、Easy VPN 設定がデバイス設定ファイルに配信されると自動的に確立されます。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、無制限に再試行します。これがデフォルトのオプションです。
- [Traffic Triggered Activation]：Easy VPN トンネルは、発信ローカル（LAN 側）トラフィックが検出されるたびに確立されます。トンネル経由で送信するトラフィックがある場合にだけバックアップ トンネルがアクティブになるように、Easy VPN ダイヤル バックアップ設定では [Traffic Triggered Activation] を使用することを推奨します。このオプションを使用している場合は、「対象の」トラフィックを定義するアクセスコントロールリスト（ACL）を指定する必要があります。

（注） Xauth パスワードを対話形式で設定することを選択した場合は、手動によるトンネルのアクティベーションが暗黙的に設定されます。この場合、デバイスは、Easy VPN リモート接続の確立を試みる前にコマンドを待機します。トンネルでタイムアウトまたは障害が発生した場合は、後続の接続においてもコマンドを待機する必要があります。

Easy VPN のクライアント接続特性の設定 （1607 ページ）の説明に従って、Client Connection Characteristics ポリシー内の xauth およびトンネル アクティベーション モードを設定します。

関連項目

- Easy VPN 設定に関する重要事項 （1606 ページ）
- Easy VPN について （1599 ページ）
- クレデンシャル ポリシー オブジェクトの設定 （1610 ページ）

Easy VPN の設定の概要

リモート クライアントから VPN サーバに接続が開始されると、IKE を使用したピア間でのデバイス認証、IKE Extended Authentication（Xauth; 拡張認証）を使用したユーザ認証、VPN ポリシーのプッシュ（Client、Network Extension、または Network Extension Plus モード）、および IPsec Security Association（SA; セキュリティ アソシエーション）の作成が順に実行されます。

次に、このプロセスの概要を示します。

1. 認証に事前共有キーが使用される場合はアグレッシブ モードを、デジタル証明書が使用される場合はメイン モードを使用して、クライアントによって IKE フェーズ 1 が開始されます。クライアントが自身を事前共有キーによって識別する場合は、付随するユーザ グループ名（設定時に定義されます）を使用して、このクライアントに関連付けられているグループ プロファイルが特定されます。デジタル証明書が使用される場合は、Distinguished Name（DN; 識別名）の Organizational Unit（OU; 組織ユニット）フィールドを使用してユーザ グループ名が特定されます。 [PKI Enrollment] ダイアログボックス - [Certificate Subject Name] タブ （1565 ページ）を参照してください。

（注） クライアントで、IKE アグレッシブ モードが開始される事前共有キー認証が設定される可能性があるため、管理者は、crypto isakmp identity hostname コマンドを使用して、VPN デバイスのアイデンティティを変更する必要があります。この操作は、IKE メイン モードを使用した証明書認証には影響しません。

1. クライアントは、クライアントのパブリック IP アドレスと VPN サーバのパブリック IP アドレスとの間で IKE SA の確立を試みます。クライアントに手動で設定する作業量を減らすために、暗号化アルゴリズム、ハッシュ アルゴリズム、認証方式、および D-H グループ サイズのあらゆる組み合わせが提案されます。

2. IKE ポリシー設定に応じて、VPN サーバはどのプロポーザルを受け入れてフェーズ 1 のネゴシエーションを続行するかを判断します。

（注） この時点でデバイス認証が終了し、ユーザ認証が開始されます。

1. IKE SA が正常に確立され、VPN サーバーに Xauth が設定されている場合、クライアントは「ユーザー名/パスワード」チャレンジを待機して、ピアのチャレンジに応答します。入力された情報は、RADIUS や TACACS+ などの認証、許可、アカウンティング（AAA）プロトコルを使用して認証エンティティに照らしてチェックされます。トークンカードは、AAA プロキシを介して使用することもできます。Xauth 中、ユーザのクレデンシャルが RADIUS を介して検証される場合に、そのユーザに固有の属性を取得できます。

（注） リモート クライアントを処理するように設定されている VPN サーバは、ユーザ認証を実行するように常に設定されている必要があります。

1. サーバから認証が成功したことを通知されると、クライアントはさらにピアから設定パラメータを要求します。残りのシステム パラメータ（IP アドレス、DNS、スプリット トンネル属性など）が、Client モードまたは Network Extension モード設定を使用してクライアントにプッシュされます。

（注） （Rivest, Shamir, and Adelman（RSA）の署名が使用されていない場合）IP アドレス プールおよびグループ事前共有キーだけがグループ プロファイルで必要なパラメータです。その他すべてのパラメータはオプションです。

1. モード設定を介して各クライアントに内部 IP アドレスが割り当てられたあと、Reverse Route Injection（RRI; 逆ルート注入）によってデバイスの各クライアント内部 IP アドレスに対してスタティック ルートが作成されます（RRI が設定されている場合）。
2. IKE クイック モードが開始されて、IPsec SA のネゴシエーションおよび作成が行われます。

これで、接続が完了します。

Easy VPN 設定に関する重要事項

トポロジに Easy VPN ポリシーを設定する前に、次の事項を把握しておく必要があります。

- Easy VPN トポロジ設定では、リモート クライアント デバイスとして 72xx シリーズ ルータが使用されていると展開に失敗します。Easy VPN クライアントは、PIX 6.3 を実行する

PIX 501、506、506E Firewall、Cisco 800 ～ 3900 シリーズ ルータ、および ASA ソフトウェア リリース 7.2 以降を実行する ASA 5505 デバイスでサポートされます。

- Easy VPN トポロジ設定において PIX 6.3 リモート クライアントに Public Key Infrastructure（PKI）ポリシーの設定を試みると、展開に失敗します。このデバイスに正常に展開するには、最初に CA サーバに PKI 証明書を発行してから、再度デバイスの展開を試みます。PKI ポリシーの詳細については、Public Key Infrastructure ポリシーについて （1544 ページ）を参照してください。
- 外部インターフェイスではなく NAT（または PAT）内部インターフェイスにクリプトマップが設定されている場合は、Easy VPN クライアントとして機能するデバイスで展開が失敗する場合があります。一部のプラットフォームでは、内部インターフェイスと外部インターフェイスが固定されています。たとえば、Cisco 1700 シリーズルータでは、VPN インターフェイスはデバイスの FastEthernet0 インターフェイスである必要があります。Cisco 800 シリーズルータでは、VPN インターフェイスは設定に応じてデバイスの Ethernet0 インターフェイスまたは Dialer1 インターフェイスのいずれかです。Cisco uBR905 および uBR925 ケーブル アクセス ルータでは、VPN インターフェイスは Ethernet0 インターフェイスである必要があります。

Easy VPN のクライアント接続特性の設定

[Client Connection Characteristics] ページを使用して、Easy VPN トポロジにおけるトラフィックのルーティング方法、および VPN トンネルの確立方法を指定します。このポリシーで定義する特性は、リモート クライアントに対して設定されます。このポリシーを設定する前に、次のトピックを参照してください。

- Easy VPN コンフィギュレーション モード （1602 ページ）
- Easy VPN および IKE 拡張認証（Xauth） （1603 ページ）

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [クライアント接続特性（Client Connection Characteristics）] を選択します。
- （ポリシービュー）[サイト間VPN（Site-to-Site VPN）] > [クライアント接続特性（Client Connection Characteristics）] を選択して新しいポリシーを作成するか、既存のポリシーを編集します。

関連項目

- Easy VPN について （1599 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- Easy VPN 設定に関する重要事項 （1606 ページ）

フィールド リファレンス

表 *355 : [Easy VPN Client Connection Characteristics]* ページ

要素	説明
[モード（Mode）]	リモート デバイスのコンフィギュレーション モード： • [クライアント（Client）]：リモートクライアントの内部ネットワークからのすべてのトラフィックに対して、接続時にヘッドエンドサーバーによってデバイスに割り当てられた単一 IP アドレスへのポートアドレス変換（PAT）を実行することを指定します。 • [ネットワーク拡張（Network Extension）]：宛先ネットワークで完全にルーティング可能で、宛先ネットワークから到達可能な IP アドレスを VPN トンネルのクライアント側終端にある PC およびその他のホストに設定することを指定します。PAT は使用されないため、クライアント PC およびホストは、宛先ネットワークの PC およびホストに直接アクセスできます。 • [ネットワーク拡張プラス（Network Extension Plus）]：ネットワーク拡張モードを機能拡張したもので、モード設定を介して受信した IP アドレスを、使用可能なループバック インターフェイスに自動的に割り当てることができます。この IP アドレスの IPsec SA は、Easy VPN クライアントによって自動的に作成されます。通常、IP アドレスは、（ping、Telnet、およびセキュア シェルを使用した）トラブルシューティングに使用されます。 [Network Extension Plus] を選択する場合、このモードは IOS ルータに対してのみ設定されます。PIX デバイスまたは ASA デバイスであるクライアントは、Network Extension モードで設定されます。 詳細については、Easy VPN コンフィギュレーション モード （1602 ページ）を参照してください。
Xauth Credentials Source	サーバとの VPN 接続を確立する場合にユーザ認証用の Xauth クレデンシャルを入力する方法を次のように選択します。 • [デバイスに保存されたクレデンシャル（Device Stored Credentials）]（デフォルト）：ユーザ名とパスワードはデバイス自体のデバイスの設定ファイルに保存され、トンネルが確立されるたびにこの情報が使用されます。 • [Interactive Entered Credentials]：Web ブラウザのウィンドウまたはルータ コンソールで、Xauth が要求されるたびに手動でユーザ名とパスワードを入力できます。 詳細については、Easy VPN および IKE 拡張認証（Xauth） （1603 ページ）を参照してください。

要素	説明
Xauth Credentials	[Xauthクレデンシャルソース（Xauth Credentials Source）] として [デバイスに保存されたクレデンシャル（Device Stored Credentials）] を選択した場合にだけ使用できます。 デフォルトの Xauth クレデンシャルを定義するクレデンシャル ポリシー オブジェクトです。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、クレデンシャル ポリシー オブジェクトの設定 （1610 ページ）を参照してください。 （注） リモートクライアントに異なる Xauth クレデンシャルを設定する場合は、オーバーライドを許可するようにクレデンシャル ポリシー オブジェクトを設定する必要があります（オブジェクト定義で [デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択します）。
Tunnel Activation（IOS）	Xauth パスワードソースに対して [デバイスに保存されたクレデンシャル（Device Stored Credentials）] オプションを選択した場合にのみ使用できます。 IOS ルータ クライアントについて、トンネルのアクティベーション方法を選択します。 • [自動（Auto）]（デフォルト）：Easy VPN トンネルは、Easy VPN 設定がデバイス設定ファイルに配信されると自動的に確立されます。トンネルでタイムアウトまたは障害が発生した場合、トンネルは自動的に再接続し、無制限に再試行します。 • [トラフィックトリガーアクティベーション（Traffic Triggered Activation）]：Easy VPN トンネルは、発信ローカル（LAN 側）トラフィックが検出されるたびに確立されます。[Traffic Triggered Activation] を選択する場合は、トンネルをアクティブにするトラフィックを定義するアクセス コントロール リスト（ACL）ポリシーオブジェクトの名前も入力します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。 トンネル経由で送信するトラフィックがある場合にだけバックアップ トンネルがアクティブになるように、Easy VPN ダイヤル バックアップ設定では [Traffic Triggered Activation] を使用することを推奨します。 （注） Xauth パスワードを対話形式で設定することを選択した場合は、手動によるトンネルのアクティベーションが暗黙的に設定されます。

要素	説明
User Authentication Method（IOS）	Xauth クレデンシャルソースに対して [インタラクティブに入力されたクレデンシャル（Interactive Entered Credentials）] オプションを選択した場合にのみ使用できます。このオプションは、リモート IOS ルータにのみ適用されます。 Xauth 認証が要求されるたびに対話形式で Xauth ユーザ名とパスワードを入力するための方法として、次のいずれかを選択します。 • [Web Browser]（デフォルト）：Web ブラウザ ウィンドウで手動で入力します。 • [ルータコンソール（Router Console）]：ルータのコマンド行から手動で入力します。

クレデンシャル ポリシー オブジェクトの設定

[Credentials] ダイアログボックスを使用して、クレデンシャル オブジェクトを作成、コピー、および編集します。

クレデンシャル オブジェクトは、認証ユーザがネットワークおよびネットワーク サービスにアクセスする場合の IKE Extended Authentication（Xauth; 拡張認証）中に、Easy VPN 設定で使用されます。Easy VPN 設定で IPsec トンネルを確立するためのトンネル パラメータをネゴシエートする場合、Xauth によって IPsec 接続を要求するユーザが識別されます。VPN サーバーに Xauth が設定されている場合、IKE SA の確立後、クライアントは「ユーザー名/パスワード」チャレンジを待機します。エンドユーザがチャレンジに応答すると、その応答は IPsec ピアに転送され、さらに上のレベルの認証が行われます。Xauth クレデンシャル（ユーザ名とパスワード）はデバイス自体に保存できるため、Easy VPN トンネルが確立されるたびに Xauth クレデンシャルを手動で入力する必要はありません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [ログイン情報（Credentials）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

• Easy VPN および IKE 拡張認証（Xauth） （1603 ページ）
• Easy VPN のクライアント接続特性の設定 （1607 ページ）
• Policy Object Manager （290 ページ）

フィールド リファレンス

表 *356 : [Credentials]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。
ユーザー名	Xauth 認証時にユーザの識別に使用される名前。
パスワード 確認（Confirm）	両方のフィールドに入力される、ユーザのパスワード。パスワードは、英数字で、最大 128 文字である必要があります。スペースは使用できません。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）]フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

Easy VPN での IPsec プロポーザルの設定

[Easy VPN IPsec Proposal] ページを使用して、Easy VPN トポロジの IKE フェーズ 2 ネゴシエーション中に使用される IPsec プロポーザルを設定します。IPsec プロポーザルは [IPSec Proposal] タブで設定されます。オプションについては、以下に説明されています。

Easy VPN トポロジでは、[Dynamic VTI] タブでダイナミック仮想インターフェイスを設定することもできます。dVTI 設定の説明については、 Easy VPN に対するダイナミック VTI の設定 （1614 ページ）を参照してください。

（注） このトピックでは、サイト間 VPN テクノロジーが Easy VPN である場合の [IPsec Proposal] ページを説明します。サイト間 VPN テクノロジーが異なる場合の [IPsecプロポーザル（IPsec Proposal）] ページの説明については、 サイト間 VPN での IPsec プロポーザルの設定 （1504 ページ）を参照してください。

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。[IPsecプロポーザル（IPsec Proposal）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）]>[簡単なIPsecプロポーザル（Easy IPsec Proposal）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。[IPsecプロポーザル（IPsec Proposal）] タブをクリックします。

関連項目

- Easy VPN について （1599 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- IPsec プロポーザルについて （1499 ページ）

フィールド リファレンス

表 *357 : [Easy VPN IPsec Proposal]* タブ

要素	説明
IKEv1 トランスフォーム セット	トンネル ポリシーで使用するトランスフォーム セット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。最大 11 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要 （1501 ページ）を参照してください。 トランスフォーム セットでは、トンネル モードの IPsec 動作だけを使用できます。 選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクト リストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、 IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。

要素	説明
Reverse Route	ASA 5500 シリーズ デバイス、PIX 7.0+ デバイス、および 7600 デバイス以外の Cisco IOS ルータでサポートされます。 リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入について （1503 ページ）を参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None）]：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]（ASA、PIX 7.0+、IOS デバイス）：クリプトマップアクセス制御リスト（ACL）に定義された宛先情報に基づいてルートを作成します。これがデフォルトのオプションです。 • [リモートピア（Remote Peer）]（IOS デバイスのみ）：リモートエンドポイント用に 1 つ、クリプトマップが適用されるインターフェイス経由でのリモートエンドポイントへのルート再帰用に 1 つ、合計 2 つのルートを作成します。 • [リモートピア IP（Remote Peer IP）]（IOS デバイスのみ）：アドレスをリモート VPN デバイスへの明示的なネクストホップとして指定します。IP アドレス、またはアドレスを指定するネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックして、リストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） ネットワークまたはホストオブジェクトを使用する場合は、オブジェクトで [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択し、必要に応じて、このオブジェクトを使用する特定のデバイスの IP アドレスをオーバーライドできます。
Enable Network Address Translation Traversal	PIX 7.0+ および ASA 5500 シリーズ デバイスでサポートされます。 ネットワーク アドレス変換（NAT）通過を許可するかどうか。 NAT 通過は、VPN 接続されたハブとスポークの間に、IPsec トラフィックに対してネットワーク アドレス変換（NAT）を実行するデバイスがある場合に使用します。NAT 通過については、VPN での NAT について （1530 ページ）を参照してください。

要素	説明
Group Policy Lookup/AAA Authorization Method	Cisco IOS ルータでだけサポートされます。 グループ ポリシーを検索する順序を定義するために使用される AAA 認可方式リスト。グループ ポリシーは、ローカル サーバまたは外部 AAA サーバ上に設定できます。リモート ユーザはグループ化され、リモート クライアントから VPN サーバに接続が正常に確立されたときに、その特定のユーザ グループのグループ ポリシーがユーザ グループに属するすべてのクライアントにプッシュされます。 [選択（Select）] をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。
User Authentication (Xauth)/AAA Authentication Method	Cisco IOS ルータおよび PIX 6.3 ファイアウォールのみでサポートされます。 ユーザ アカウントの検索順序を定義するために使用される AAA または Xauth ユーザ認証方式。 Xauth では、すべての AAA 認証方式で、IKE 認証フェーズ 1 の交換後に別のフェーズでユーザ認証を実行できます。ユーザ認証が実行されるためには、AAA 設定リスト名が Xauth 設定リスト名と一致する必要があります。 デバイスに Xauth が設定されている場合、クライアントは、IKE SA が正常に確立されたあとで、「ユーザ名/パスワード」チャレンジを待機して、ピアのチャレンジに応答します。入力された情報は、RADIUS や TACACS+ などの認証、許可、アカウンティング（AAA）プロトコルを使用して認証エンティティに照らしてチェックされます。 [選択（Select）] をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。

Easy VPN に対するダイナミック VTI の設定

[Easy VPN IPSec Proposal] ポリシーの [Use the Dynamic VTI] タブを使用して、ハブアンドスポーク Easy VPN トポロジ内のデバイスにダイナミック仮想トンネル インターフェイスを設定します。詳細については、Easy VPN とダイナミック仮想トンネル インターフェイス （1601 ページ）を参照してください。

（注） ダイナミック VTI は、IOS バージョン 12.4(2)T 以降を実行する 7600 デバイスを除く IOS ルータでだけ設定できます。

ナビゲーション パス

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [IPsecプロポーザル（IPsec Proposal）] を選択します。[ダイナミックVTI（Dynamic VTI）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）]>[簡単なIPsecプロポーザル（Easy IPsec Proposal）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。[ダイナミックVTI（Dynamic VTI）] タブをクリックします。

関連項目

- Easy VPN について （1599 ページ）
- Easy VPN での IPsec プロポーザルの設定 （1611 ページ）

フィールド リファレンス

表 358 : [Easy VPN IPSec Proposal]、[Dynamic VTI] タブ

要素	説明
Enable Dynamic VTI	選択されている場合、Security Manager は、デバイスにダイナミック仮想テンプレート インターフェイスを暗黙的に作成できます。 デバイスが、ダイナミック VTI をサポートしないハブ サーバである場合は、警告メッセージが表示されて、ダイナミック VTI なしでクリプト マップが展開されます。クライアント デバイスの場合は、エラー メッセージが表示されます。
Virtual Template IP	トポロジのハブにダイナミック VTI を設定している場合は、サブネット アドレスまたはインターフェイス ロールを指定します。 • [サブネット（Subnet）] : アドレスのプールから取得された IP アドレスを使用します。サブネット マスクを含むプライベート IP アドレスを入力します（たとえば 10.1.1.0/24）。 • [インターフェイスロール（Interface Role）] : デバイスの物理インターフェイスまたはループバックインターフェイスを使用します。必要に応じて、[選択（Select）] をクリックしてインターフェイスセレクタを開きます。そこで、目的のインターフェイスを識別するインターフェイス ロール オブジェクトを選択できます。適切なオブジェクトがまだ存在していない場合は、選択ダイアログボックスで作成できます。 トポロジのスポークにダイナミック VTI を設定している場合は、[なし（None）] を選択します。

Easy VPN における Connection Profile ポリシーの設定

接続プロファイルは、IPsec トンネル接続ポリシーを含むレコードのセットで構成されます。接続プロファイル、またはトンネル グループは、特定の接続のグループ ポリシーを示しており、ユーザ指向の属性を含んでいます。ユーザーに対して特定のグループ ポリシーを割り当てない場合は、接続のデフォルト グループ ポリシーが適用されます。正常に接続するためには、リモート クライアントのユーザ名がデータベースに存在している必要があります。データベースに存在しない場合は、接続が拒否されます。

サイト間 VPN では、Easy VPN サーバ（PIX ファイアウォール バージョン 7.0+ デバイスまたは ASA 5500 シリーズ デバイス）に Connection Profile ポリシーを設定します。Easy VPN Connection Profile ポリシーは、リモート アクセス VPN で使用されるプロファイルに類似しています。どの Easy VPN サーバも ASA デバイスまたは PIX 7.0+ デバイスでない場合、Connection Profile ポリシーを割り当て解除できます。

Connection Profile ポリシーの作成には、次の指定が含まれます。

- グループ ポリシー：デバイス内部または外部の RADIUS サーバや LDAP サーバに保存されるユーザ指向の属性の集合。
- グローバル AAA 設定：認証、許可、アカウンティング サーバ。
- クライアント アドレスの割り当てに使用される DHCP サーバ、および IP アドレスの割り当て元となるアドレス プール。
- Internet Key Exchange（IKE; インターネット キー交換）および IPsec の設定（事前共有キーなど）。

[PIX7.0+/ASA Connection Profiles] ページで、Easy VPN サーバ上の接続プロファイルを設定できます。

関連項目

- VPN トポロジの作成または編集 （1416 ページ）
- IPsec テクノロジーおよびポリシーについて （1384 ページ）
- Easy VPN について （1599 ページ）

ステップ 1 次のいずれかを実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））VPN セレクタで Easy VPN トポロジを選択し、ポリシー セレクタで [接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX 7.0/ASA)）] を選択します。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）] > [接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX 7.0/ASA)）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

ポリシーについては、 [Connection Profiles] ページ （1715 ページ）を参照してください。

ステップ 2 [全般（General）] タブで、接続プロファイル名およびグループポリシーを指定して、使用するアドレス割り当て方式を選択します。使用可能なプロパティの詳細については、 [General] タブ（[Connection Profiles]）（1718 ページ）を参照してください。

ステップ 3 [AAA] タブをクリックして、接続プロファイルの AAA 認証パラメータを指定します。タブの要素の詳細については、 [AAA] タブ（[Connection Profiles]） （1721 ページ）を参照してください。

ステップ 4 [IPsec] タブをクリックして、接続プロファイルの IPsec および IKE パラメータを指定します。タブの要素の詳細については、 [IPSec] タブ（[Connection Profiles]） （1730 ページ）を参照してください。

Easy VPN における User Group ポリシーの設定

[User Group Policy] ページを使用して、Easy VPN サーバの User Group ポリシーを作成または編集します。Easy VPN サーバを設定するときに、リモート クライアントが属するユーザ グループを作成します。Easy VPN ユーザ グループ ポリシーは、Cisco IOS セキュリティ ルータ、PIX 6.3 Firewall、または Catalyst 6500/7600 デバイスに設定できます。どの Easy VPN サーバも、IOS ルータ、Catalyst 6500/7600 デバイス、または PIX 6.3 ファイアウォールでない場合、ユーザ グループ ポリシーを割り当て解除できます。

リモート クライアントは、サーバ デバイスに接続するためには、サーバに設定されているユーザ グループと同じグループ名を持っている必要があります。同じグループ名を持たない場合、接続は確立されません。リモート クライアントから VPN サーバに接続が正常に確立されたときに、その特定のユーザ グループのグループ ポリシーがユーザ グループに属するすべてのクライアントにプッシュされます。

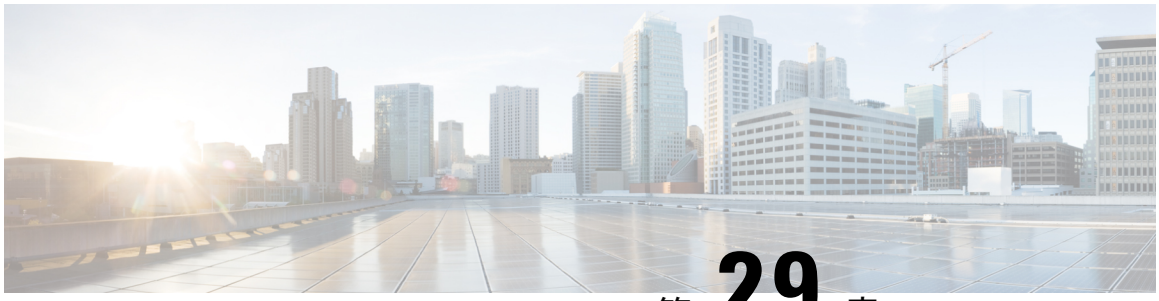
[Available User Groups] リストで、ポリシーで使用するユーザ グループ ポリシー オブジェクトを選択します。[作成（Create）] （+）ボタンをクリックして、新しいユーザー グループ オブジェクトを作成できます。また、既存のグループを選択し、[編集（Edit）]（鉛筆アイコン）ボタンをクリックして既存のグループを編集できます。ユーザ グループ オブジェクトの設定については、 [Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）を参照してください。

ナビゲーション パス

- （ [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）） VPN セレクタで Easy VPN トポロジを選択して、ポリシーセレクタで [ユーザーグループポリシー（User Group Policy）] を選択します。
- （ポリシービュー）ポリシータイプセレクタで [サイト間VPN（Site-to-Site VPN）]>[ユーザーグループポリシー（User Group Policy）] を選択します。既存の共有ポリシーを選択するか、新しい共有ポリシーを作成します。

関連項目

- Easy VPN について （1599 ページ）



第 29 章

Group Encrypted Transport（GET）VPN

Cisco Group Encrypted Transport Virtual Private Network（GET VPN; Group Encrypted Transport バーチャルプライベートネットワーク）は、IPやマルチプロトコルラベルスイッチング（MPLS）を含むさまざまなWAN環境で使用できる、完全メッシュVPNテクノロジーです。GET VPNは、プライベートWAN上で、Cisco IOSデバイスから発信される、またはCisco IOSデバイスを通過するIPマルチキャストグループトラフィックまたはユニキャストトラフィックを保護するために必要な機能のセットで構成されています。GET VPNでは、キー管理プロトコルであるGroup Domain of Interpretation（GDOI）とIP Security（IPsec; IPセキュリティ）暗号化が組み合わせて使用され、IPマルチキャストまたはユニキャストトラフィックを保護するための効率的な方法がユーザに対して提供されます。GET VPNでは、ルータによって、トンネル化されていない（つまり「ネイティブな」）IPマルチキャストおよびユニキャストパケットに対して暗号化を適用できるので、マルチキャストおよびユニキャストトラフィックを保護するためにトンネルを設定する必要がありません。

- Group Encrypted Transport（GET）VPNについて （1619ページ）
- GET VPN登録プロセスについて （1623ページ）
- GET VPNセキュリティポリシーおよびセキュリティアソシエーションについて （1631ページ）
- GET VPNの設定 （1634ページ）
- RSAキーの生成と同期 （1636ページ）
- GET VPNのIKEプロポーザルの設定 （1638ページ）
- GET VPNのグローバル設定 （1640ページ）
- GET VPNキーサーバの設定 （1642ページ）
- GET VPNグループメンバーの設定 （1645ページ）
- パッシブモードを使用したGET VPNへの移行 （1649ページ）
- GET VPN設定のトラブルシューティング （1652ページ）

Group Encrypted Transport（GET）VPNについて

音声やビデオなどのネットワークを利用するアプリケーションによって、即時に通信可能で各ブランチが相互接続された、QoS対応WANの必要性が増しています。これらのアプリケーションは分散して配置されるため、スケーラビリティに対する要求も高まります。同時に、企

業の WAN テクノロジーにおいては、QoS 対応ブランチ間相互接続と転送のセキュリティとの間でトレードオフが発生します。現在ネットワーク セキュリティのリスクが増加し、規制への準拠が重要となりつつありますが、WAN 暗号化テクノロジーである Group Encrypted Transport VPN（GET VPN）を使用すると、ネットワーク インテリジェンスとデータ プライバシーのいずれかを犠牲にする必要がなくなります。

GET では、トンネルなしの VPN が提供されるため、IPsec トンネルは必要ありません。ポイントツーポイント トンネルが不要になったことにより、メッシュ構造のネットワークのスケーラビリティが高まり、音声およびビデオの品質にとって重要なネットワーク インテリジェンス機能が維持されます。GET は、信頼グループの概念に基づき、ポイントツーポイント IPsec トンネルおよびそれに関連するオーバーレイ ルーティングが不要な、標準規格に準拠したセキュリティ モデルです。信頼グループ メンバーは、グループ SA と呼ばれる共通の Security Association（SA; セキュリティ アソシエーション）を共有します。これにより、グループ メンバーは、他の任意のグループ メンバーが暗号化したトラフィックを復号化できます。ポイントツーポイント トンネルではなく信頼グループを使用することによって、完全メッシュ ネットワークのスケーラビリティが高まり、音声およびビデオの品質にとって重要なネットワーク インテリジェンス機能（QoS、ルーティング、マルチキャストなど）が維持されます。

GET ベースのネットワークは、IP やマルチプロトコル ラベル スイッチング（MPLS）を含むさまざまな WAN 環境で使用できます。この暗号化テクノロジーを使用する MPLS VPN はスケーラビリティ、管理性、コストに優れており、政府によって義務付けられている暗号化要件が満たされます。GET は柔軟であるため、セキュリティを必要とする企業では、サービス プロバイダー WAN サービスにおいて独自のネットワーク セキュリティを管理することも、暗号化サービスをプロバイダーに委託することもできます。GET によって、部分メッシュ接続または完全メッシュ接続を必要とする大規模なレイヤ 2 または MPLS ネットワークの保護が簡易化されます。

既存の IKE、IPsec、およびマルチキャスト テクノロジーを利用できることに加えて、GET VPN トポロジには、次のような主要な要素および機能が備えられています。

- グループ メンバー：VPN 内で実際のトラフィックを交換するルータは、グループ メンバーと呼ばれます。グループ メンバーによって、トラフィックに対して暗号化サービスが提供されます。暗号化ポリシーは、キー サーバに集中的に定義されて、登録時にグループ メンバーにダウンロードされます。グループ メンバーは、このようにダウンロードされたポリシーに基づいて、トラフィックで暗号化または復号化が必要であるかどうか、および使用するキーを決定します。

グループ メンバーは、主にキー サーバから暗号化ポリシーを取得しますが、グループ メンバーにローカル サービス ポリシー ACL を設定して、ローカル要件に基づいて特定のトラフィックを暗号化から除外することができます。詳細については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。

（注） デバイスは、複数のグループのグループ メンバーとなることができます。

- キー サーバ：キー サーバとして動作するルータは、トポロジへのゲートキーパーとなります。グループ メンバーが VPN のアクティブなメンバーとなるには、まずキー サーバに

正常に登録される必要があります。キー サーバは共有サービス ポリシーを管理し、キーを生成して、グループ メンバーに対してキーを送信します。キー サーバ自体はグループ メンバーとなることができませんが、1 つのキー サーバが複数のトポロジのキー サーバとなることができます。詳細については、GET VPN 登録プロセスについて （1623 ページ）を参照してください。

- Group Domain of Interpretation（GDOI）グループ キー管理プロトコルを使用して、デバイスのグループに対して暗号キーおよびポリシーのセットが提供されます。GET VPN ネットワークでは、GDOI を使用して、安全に通信する必要がある企業 VPN ゲートウェイ（グループ メンバー）のグループに対して共通の IPsec キーが配布されます。キーサーバーとして指定されたデバイスは、「キーの再生成」と呼ばれるプロセスを使用して、定期的にキーをリフレッシュし、グループメンバーに最新のキーを送信します。

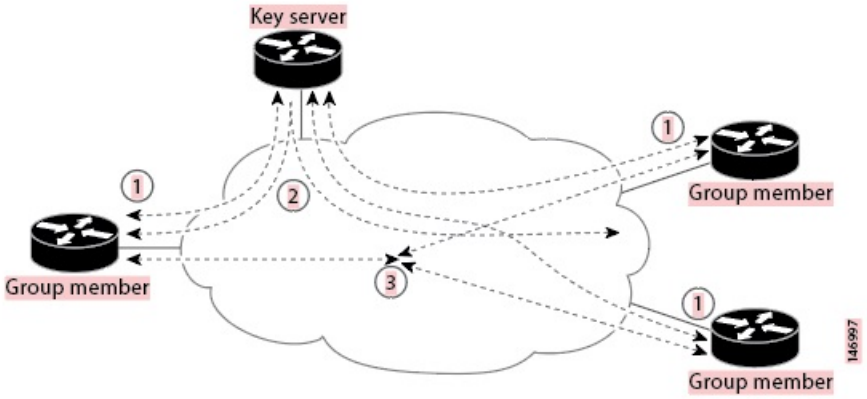
GDOI プロトコルでは、フェーズ 1 Internet Key Exchange（IKE; インターネット キー交換）SA が使用されます。参加するすべての VPN ゲートウェイは、キーを提供するデバイスに対して IKE を使用して自身を認証します。初期認証では、Pre-Shared Key（PSK; 事前共有キー）や Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）などのすべての IKE 認証方式がサポートされています。IKE SA を使用して VPN ゲートウェイが認証され、適切なセキュリティ キーが提供されたあと、IKE SA は期限切れとなります。これ以降は、GDOI を使用して、よりスケーラブルで効率的な方法でグループ メンバーが更新されます。GDOI の詳細については、RFC 3547 を参照してください。

- アドレスの維持：IPsec で保護されたデータ パケットでは、外側の IP ヘッダーで元の送信元と宛先が伝送されます。トンネルエンドポイントのアドレスには置換されません。GET VPN では、アドレスが維持されるため、コア ネットワーク内のルーティング機能を使用できます。アドレスの維持によって、ネットワーク内の、宛先アドレスへのルートをアドバタイズする任意のカスタマー エッジ（CE）デバイスにパケットを配送するルーティングが可能となります。グループのポリシーに一致するすべての送信元および宛先は、同様に処理されます。アドレスの維持は、IPsec ピア間のリンクが利用できない状況では、トラフィックの「ブラックホール」状況に対処するのに役立ちます。

また、ヘッダーが維持されることによって、企業のアドレス空間全体および WAN においてルーティングの継続性が維持されます。その結果、キャンパスのエンド ホスト アドレスは WAN に公開されます（MPLS では、これは WAN のエッジに適用されます）。このため、GET VPN は、WAN ネットワークが「プライベート」ネットワークとして動作する場合にだけ適用できます（MPLS ネットワークなど）。

次の図に、GET VPN トポロジの一般的な動作を示します。

図 *38 :* 一般的な *GET VPN* の動作



1. グループ メンバーは、Group Domain of Interpretation（GDOI）プロトコルを使用して、キー サーバに登録します。キー サーバは、グループ メンバーを認証および認可して、IP マルチキャストおよびユニキャスト パケットの暗号化と復号化に必要な IPsec ポリシーとキーをメンバーにダウンロードします。登録プロセスでは、ユニキャストまたはマルチキャスト通信を使用できます。
2. グループ メンバーは、IPsec を使用して暗号化された IP パケットを交換します。グループ メンバーだけが VPN のアクティブな要素となります。
3. 必要に応じて、キー サーバからグループ メンバーに対してキーの再生成メッセージがプッシュされます。キーの再生成メッセージには、古い IPsec Security Association（SA; セキュリティ アソシエーション）が期限切れとなった場合に使用する新しい IPsec ポリシーとキーが含まれています。常に有効なグループ キーが使用できるように、キーの再生成メッセージは SA の期限が切れる前に送信されます。

Security Manager を使用して GET VPN をプロビジョニングする場合には、次の点に注意します。

- GET VPN 対応 VRF はサポートされていません。
- Security Manager においてトンネル保護なしで DMVPN を定義する方法がないため、DMVPN と GET を併用することはできません。
- グループ メンバーを手動で設定してマルチキャスト グループに参加させること（ip igmp join-group）はできません。Security Manager では、静的な Source-Specific Multicast（SSM）マッピングだけがプロビジョニングされます。

関連項目

- GET VPN 登録プロセスについて （1623 ページ）
- GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）
- GET VPN の設定 （1634 ページ）

GET VPN 登録プロセスについて

GET VPN では、VPN トポロジはグループ メンバーによって構成されます。VPN 内のトラフィックは、グループ メンバー間のトラフィックです。デバイスがグループ メンバーとなるには、デバイスはキー サーバに正常に登録される必要があります。キー サーバでは、Security Association（SA; セキュリティ アソシエーション）ポリシーが保持され、グループ用のキーが作成および保持されます。グループ メンバーが登録されると、キー サーバはグループ メンバーにポリシーとキーをダウンロードします。また、キー サーバは、既存のキーの期限が切れる前にグループに対してキーの再生成を実行します。

キー サーバには、登録要求の処理およびキーの再生成の送信という 2 つの機能があります。グループ メンバーはいつでも登録可能で、最新のポリシーおよびキーを受信できます。グループ メンバーがキー サーバに登録する場合、キー サーバによって、グループ メンバーが参加を試みているグループ ID が確認されます。グループ ID が有効な場合、キー サーバはグループ メンバーに対してセキュリティ アソシエーション ポリシーを送信します。ダウンロードされたポリシーを処理できることがグループ メンバーによって確認されると、キー サーバから各キーがダウンロードされます。

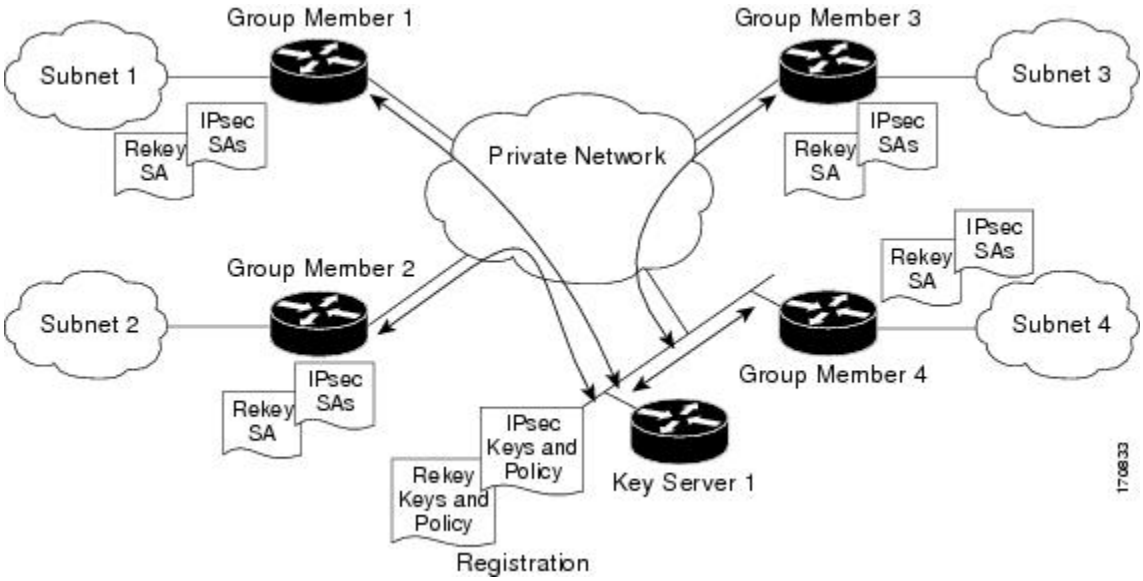
キー サーバおよびグループ メンバー間の通信は暗号化され、Traffic Encryption Key（TEK; トラフィック暗号キー）および Key Encryption Key（KEK; キー暗号キー）という 2 種類のキーを使用して保護されます。TEK は、キー サーバからすべてのグループ メンバーにダウンロードされます。ダウンロードされた TEK は、グループ メンバー間で安全に通信するためにすべてのグループ メンバーで使用されます。このキーは、実質的には、すべてのグループ メンバーによって共有されるグループ キーとなります。グループ ポリシーおよび IPsec SA は、グループ メンバーへの定期的なキーの再生成メッセージを使用して、キー サーバによってリフレッ

シュされます。KEK もキー サーバによってダウンロードされ、グループ メンバーによって、キー サーバから受信するキーの再生成メッセージの復号化に使用されます。

キー サーバは、近々 IPsec SA の期限が切れる場合や、キー サーバでセキュリティ ポリシーが変更された場合に、キーの再生成メッセージを送信します。KEK タイマーの期限が切れた場合もキーの再生成が実行されます（キー サーバは KEK キーの再生成を送信します）。キーの再生成メッセージは、パケット損失が発生した場合に備えて定期的に再送信される場合もあります。キーの再生成メカニズムがマルチキャストである場合は、受信者がキーの再生成メッセージを受信できなかったことを示す有効なフィードバック メカニズムがないため、定期的に再送信することによってすべての受信者が最新の情報を受信できるようにします。キーの再生成メカニズムがユニキャストである場合、受信者は確認応答メッセージを送信します。

キー サーバは、GDOI グループ用のグループ ポリシーおよび IPsec Security Association（SA; セキュリティ アソシエーション）を生成します。キー サーバによって生成される情報には、複数の TEK 属性、トラフィック暗号化ポリシー、ライフタイム、送信元と宛先、各 TEK に関連付けられるセキュリティ パラメータ インデックス（SPI）ID、キーの再生成ポリシー（1 つの KEK）などがあります。グループ メンバーにローカル セキュリティ ポリシーが設定され、ダウンロードされたポリシーとマージして使用されることがあります。詳細については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。

次の図に、グループ メンバーおよびキー サーバ間の通信フローを示します。キー サーバは、グループ メンバーからの登録メッセージを受信したあと、グループ ポリシーと新しい IPsec SA を含む情報を生成します。次に、新しい IPsec SA がグループ メンバーにダウンロードされます。キー サーバでは、グループごとに、各グループ メンバーの IP アドレスを含むテーブルが保持されます。グループ メンバーが登録されると、キー サーバはメンバーの IP アドレスを関連するグループのテーブルに追加します。これにより、キー サーバは、アクティブなグループ メンバーをモニタできるようになります。1 つのキー サーバで複数のグループをサポートできます。また、1 つのグループ メンバーは、複数のグループに属することができます。



GET VPN トポロジを設定する場合、次の登録関連機能を設定できます。

- グループ登録およびキーの再生成にユニキャストまたはマルチキャストのいずれを使用するかを決定します。詳細については、キーの再生成転送メカニズムの選択 （1625 ページ）を参照してください。

（注） マルチキャストを使用する場合は、キー サーバおよびグループ メンバーで手動でマルチキャストをイネーブルにする必要があります。マルチキャスト コマンドは、Security Manager によってプロビジョニングされません。

- 複数のキー サーバを設定して、冗長性を確保し、ロード バランシングを行うかどうかを決定します。詳細については、協調キー サーバを使用した冗長性の設定 （1627 ページ）を参照してください。
- キー サーバに正常に登録される前にグループ メンバーのトラフィックを保護するためにグループ メンバーにフェールクローズ モードを設定するかどうかを決定します。詳細については、登録の失敗時にも保護するためのフェールクローズの設定 （1628 ページ）を参照してください。
- グループ メンバーがグループに参加するときに認可が必要かどうかを決定します。証明書認可（Public Key Infrastructure ポリシーも設定する必要があります）または事前共有キーを使用できます。キー サーバが複数のグループに対応する場合は、認可を設定する必要があります。設定オプションの詳細については、GET VPN グループ暗号化の定義 （1453 ページ）の [Authorization Type] 設定を参照してください。

関連項目

- RSA キーの生成と同期 （1636 ページ）
- GET VPN の設定 （1634 ページ）

キーの再生成転送メカニズムの選択

Group Encryption ポリシーでキーの再生成設定を設定する場合（GET VPN グループ暗号化の定義 （1453 ページ）を参照）、キーの再生成転送メカニズムとしてマルチキャストまたはユニキャストのいずれを使用するかを選択する必要があります。キー サーバは、グループ メンバーまたは他のキー サーバに対して新しいキーおよび IPsec Security Association（SA; セキュリティ アソシエーション）を送信する場合には常にこの方法を使用します。それぞれの方法には利点と欠点があります。

マルチキャストが標準的な選択肢です。マルチキャストを使用した場合、キー サーバは、各キーの再生成メッセージの 1 つのコピーを、マルチキャスト グループ アドレスを使用してすべてのグループ メンバーに一度に送信します。そのため、キーの再生成で遅延は発生せず、グループ メンバーは更新されたセキュリティ ポリシーをほぼ同時にインストールできます（通常のネットワーク遅延を除く）。ただし、一部のネットワークでは、マルチキャスト機能を使用すると余分のコストが発生したり、マルチキャスト機能が許可されていない場合がありま

す。マルチキャストを設定する場合は、GET VPN トポロジで使用されるマルチキャスト アドレスを指定する必要があります。

マルチキャストが使用できない場合や、マルチキャストの使用が望ましくない場合は、**ユニキャスト**を使用できます。ユニキャストを使用した場合、キー サーバは、個別のグループ メンバーに対してキーの再生成および IPsec SA を送信します。各グループ メンバーはメッセージを受信したことを示す確認応答を送信します。ユニキャストでは、メッセージを直接送信したり、確認応答を受信したりする必要があるため、キー サーバはサブネットごとに順番にグループ メンバーに対してユニキャスト メッセージを送信します（ただし、グループ メンバー数が 30 未満などの比較的小規模な VPN では、すべてのグループ メンバーに同時にメッセージが送信されることがあります）。

したがって、マルチキャストとユニキャストを比較した場合の利点は次のようになります。

- マルチキャストでは、キー サーバはグループ メンバーがメッセージを受信したかどうかを把握できません。一方、ユニキャストでは、確認応答が送信されます。ユニキャストでは、キー サーバが確認応答を受信できない場合、メッセージが再送信されます。
- マルチキャストはユニキャストよりも高速です。特に、数百のグループ メンバーがあるような大規模なトポロジでは高速になります。マルチキャストのキーの再生成では、グループ内のグループ メンバー数が 1 つの場合でも数千の場合でも、CPU のオーバーヘッドは変わらず、いずれの場合も低くなります。
- ユニキャストでは、グループ メンバーが連続して確認応答を送信しないと、キー サーバはグループ メンバーが存在しないと判断して、キーの再生成メッセージの送信を停止します。そのため、キー サーバには常にアクティブなグループ メンバーのリストが保持されています。応答しなくなったグループ メンバーが GET VPN トポロジに再度参加するためには、もう一度登録が必要です。マルチキャストでは確認応答が使用されないため、グループ メンバーが応答しなくなってもキー サーバでは把握できず、アクティブなグループ メンバーのリストも保持されません。

ヒント マルチキャストを使用するには、キー サーバおよびグループ メンバーでマルチキャストをイネーブルにする必要があります。これらのコマンドは、Security Manager によってプロビジョニングされません。Security Manager では、マルチキャストによるキーの再生成だけがイネーブルにされ、ルータでのマルチキャスト トラフィックの送受信はイネーブルにされません。そのため、デバイスで手動でマルチキャストをイネーブルにするか、または FlexConfig ポリシーを使用してコマンドをプロビジョニングする必要があります（FlexConfig ポリシー オブジェクトの作成 （465 ページ）を参照）。

すべてのキー サーバでマルチキャストがサポートされている場合は、単一の GET VPN トポロジ内でマルチキャストとユニキャストの混在させることができます。どちらの転送メカニズムを使用するかを決定する場合には、次の推奨事項を考慮してください。

- すべてのキー サーバ、すべてのグループ メンバー、およびネットワークでマルチキャストがサポートされている場合は、マルチキャストを使用します。

- すべてのキー サーバとほとんどのグループ メンバーでマルチキャストがサポートされており、少数のグループ メンバーでマルチキャストがサポートされていない場合は、マルチキャストを使用します。マルチキャストをサポートしないグループ メンバーは、キーの再生成およびIPsec SA更新を受信しません。ただし、これらの項目のライフタイム設定の期限が切れる前に、ユニキャスト グループ メンバーはキー サーバに再登録し、新しいキーと IPsec SA を取得します。
- どのグループ メンバーでもマルチキャストがサポートされていない場合や、少数のグループ メンバーだけがマルチキャストをサポートしている場合は、ユニキャストを使用します。この場合、グループ メンバーは、キー サーバからキーの再生成と IPsec SA 更新を受信するため、キー サーバに再登録する必要はありません。

関連項目

- GET VPN 登録プロセスについて （1623 ページ）
- RSA キーの生成と同期 （1636 ページ）
- GET VPN の設定 （1634 ページ）

協調キー サーバを使用した冗長性の設定

GET VPN ネットワークでは、キー サーバがコントロール プレーンとなるため、キー サーバがこのネットワークにおける最も重要なエンティティとなります。したがって、キー サーバが 1 台しかない場合は、このキー サーバが GET VPN ネットワーク全体のシングル ポイント障害となります。キー サーバにおいて冗長性を考慮することは重要であるため、GET VPN では、Cooperative（COOP; 協調）キー サーバと呼ばれる複数のキー サーバを用意して、キー サーバのうちの 1 つで障害が発生したり、到達不能になったりした場合に、シームレスな障害回復を行うことができます。

すべてのCOOPキーサーバのリストから使用可能な任意のキーサーバに登録するようにグループ メンバーを設定できます。グループ メンバーの設定によって、登録の順序が決まります（GET VPN グループ メンバーの設定 （1645 ページ）および[Edit Group Member] ダイアログボックス （1646 ページ）を参照）。最初に定義されたキー サーバに対して接続が試みられ、その後、定義された順番でキー サーバへの接続が試みられます。すべての使用可能な COOP キー サーバにグループ メンバーの登録を分散して、1 つのキー サーバにおける IKE 処理の負荷を低減することを推奨します。キーの再生成メッセージを送信するのは、プライマリ キー サーバだけです。

COOPキーサーバーが起動すると、すべてのキーサーバーはセカンダリとしての役割を担い、選定プロセスが開始されます。通常は、最も高いプライオリティを持つキーサーバーが、プライマリ キーサーバーとして選定されます。他のキーサーバは、セカンダリのままとなります。プライマリ キー サーバは、グループ ポリシーを作成してすべてのグループ メンバーに配布する処理、およびCOOP キー サーバを定期的に同期する処理を担当します。

協調キー サーバは、（プライマリからセカンダリへの）一方向の通知メッセージを交換します。セカンダリ キー サーバが、一定期間プライマリ キー サーバから通知を受信しない場合、

セカンダリ キー サーバはプライマリ キー サーバへの接続を試みて、更新情報を要求します。プライマリ キー サーバが応答しない場合（セカンダリ キー サーバがプライマリ キー サーバから情報を受信しない場合）は、COOP キー サーバの再選定がトリガーされて、新しいプライマリ キー サーバが選定されます。

最大 8 台のキー サーバを COOP キー サーバとして定義できますが、5 台以上の COOP キー サーバが必要となることはほとんどありません。キーの再生成情報は単一のプライマリ キー サーバによって生成および配布されるため、3 台以上のキー サーバを展開することの利点は、ネットワークの障害が発生した場合の登録の負荷に対応でき、同時に再登録も実行できることにあります。Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）を使用する IKE ネゴシエーションは、Pre-Shared Key（PSK; 事前共有キー）を使用する IKE ネゴシエーションと比較してはるかに多くの CPU パワーを必要とするため、このことは PKI によるグループ メンバー認可を使用する場合に特に重要となります。

ヒント

- RSA キーはすべての協調キー サーバで同じである必要があります。RSA キーの同期の詳細については、RSA キーの生成と同期 （1636 ページ）を参照してください。
- キー サーバ間での定期的な ISAKMP キープアライブをイネーブルにして、プライマリ キー サーバで他のセカンダリ キー サーバの状態を追跡および表示できるようにすることを推奨します。グループ メンバーとキー サーバとの間の IKE キープアライブは必要ではなく、またサポートもされていません。キープアライブの設定の詳細については、GET VPN のグローバル設定 （1640 ページ）を参照してください。
- COOP プロトコルは、GDOI グループごとに設定されます。複数の GDOI グループが設定されたキー サーバでは、異なるキー サーバとの固有の COOP 関係を複数維持できます。

登録の失敗時にも保護するためのフェールクローズの設定

グループ メンバーは、GET VPN のメンバーとなるためにはキー サーバに登録する必要があります。グループメンバーがキーサーバーに正常に登録されるまでは、グループメンバーの GET VPN インターフェイス経由で送受信されるトラフィックは暗号化されません。クリア テキストでの伝送が行われる期間は、登録に成功すると短い期間で済みますが、何らかの理由でグループ メンバーが登録に失敗すると、長くなる可能性があります。

このデフォルトの動作はフェールオープンと呼ばれています。いかなる場合でもトラフィックがクリアテキストで送信されることをセキュリティ標準違反であると見なす場合は、フェールクローズモードを設定して、登録前（または登録中）のトラフィックを保護できます。フェールクローズモードを使用すると、インターフェイスを経由するトラフィックのうち、フェールクローズ ACL で明示的に特定したトラフィック以外のすべてのトラフィックがドロップされます。フェールクローズ モードでは、グループ メンバーがキー サーバに正常に登録されて、必要なキー、セキュリティ ポリシー、およびセキュリティ アソシエーションがダウンロードされるまでは、インターフェイスが実質的にシャットダウンされます。フェールクローズモードを使用するには、Cisco IOS ソフトウェア Release 12.4(22)T または 15.0 以上が必要です。また、フェールクローズモードは、サポートされているすべての ASR に設定できます（各 IPsec テクノロジーでサポートされるデバイスについて （1392 ページ）を参照）。

フェールクローズ モードは、最初の登録時にだけ使用されます。グループ メンバーがすでに正常に登録されている場合、そのグループ メンバーは、その後登録に失敗しても、キー サーバからダウンロードされたポリシーを保持し続けます。ただし、グループメンバーに対して **clear crypto gdoi** コマンドを使用した場合は、そのあとに行われる登録の試行が 1 回めの登録であると見なされて、フェールクローズモードが適用されます。

GET VPN グループ メンバーの設定 （1645 ページ）で説明するように、フェールクローズ モードは、個別のグループ メンバーに対して設定します。したがって、すべてのグループ メンバーでモードをイネーブルにせずに、選択したグループ メンバーに対してモードをイネーブルにできます。ユーザ（および Security Manager）がデバイスからロックアウトされ、登録が成功するまで設定の更新やメンテナンスができなくなる事態を回避するためには、フェールクローズ ACL を指定する必要があります。

フェールクローズ ACL は拡張 ACL ポリシー オブジェクトであり、デバイスにクリプト マップの一部として設定されます。ルールは、グループ メンバーの観点から設定します。次のヒントを参照して、適切なフェールクローズ ACL の作成に役立ててください。

- **permit** ステートメントと **deny** ステートメントの両方を設定できます。フェールクローズ ACL では、「permit」は「このトラフィックを送信しない」を意味し、「deny」は「このトラフィックをクリアテキストで送信する」ことを意味します。この動作は、ステートメントが次の意味を持つ通常のクリプトマップ ACL の動作とは異なります。
  - **Permit**：このトラフィックを暗号化する」ことを意味します。グループメンバーは、登録前にはトラフィックを暗号化するために必要な IPsec セキュリティ アソシエーションを持っていないため、結果としてトラフィックはドロップされます。
  - **deny**：「このトラフィックを暗号化しない」ことを意味します。一般的なクリプト マップ ACL では、deny ステートメントを使用すると、条件に一致したパケットは、デバイスに設定されている次のクリプトマップ ACL と比較されます（設定されている場合）。ただし、トラフィックがフェールクローズ ACL 内の deny ステートメントに一致した場合、すべてのクリプト マップ ACL 処理が終了し、クリア テキストでのトラフィックの送信が許可されます。

フェールクローズ モードで deny がこのように動作するのは、フェールクローズでは、クリプトマップ ACL のリストの最後に暗黙的に ACL ステートメントが追加されているためです。そのステートメントは **permit ip any any** であり、すべてのトラフィックに一致します。登録がまだ完了していないため IPsec セキュリティ アソシエーションがなく、どの条件にも一致しなかったトラフィックは、暗号化する方法が存在せずに、ドロップされます。

この最後の permit ip any any ステートメントによって、フェールクローズ ACL では deny ステートメントだけを設定することが可能となります。

- フェールクローズ ACL は、オプションのグループ メンバー セキュリティ ポリシー ACL のあとに続いて処理されます。ただし、グループ メンバー セキュリティ ポリシー ACL 内のすべてのステートメントは deny ステートメントである必要があります。これにより、一致するトラフィックがクリアテキストで送信される必要があることが指定されます。セキュリティ ポリシーは、通常のクリプト マップ ルールに従って処理されるため、deny ステートメントに一致するトラフィックは、そのあとでフェールクローズ ACL と比較されます。フェールクローズ ACL 内に一致する deny ステートメントがない場合、トラフィッ

クは、フェールクローズの暗黙的な最後の permit ip any any ステートメントによってドロップされます。

したがって、グループ メンバー セキュリティ ポリシー ACL を使用し、グループ メンバーの登録ステータスにかかわらず特定のトラフィックをクリアテキストで送信する場合、フェールクローズ ACL には、少なくともセキュリティ ポリシー ACL に含まれているものと同じステートメントがすべて含まれている必要があります。両方の ACL に同じ ACL オブジェクトを使用することもできます。

グループ メンバー セキュリティ ポリシーの詳細については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。

- フェールクローズ ACL は、最後のクリプト マップ ACL として挿入されます。したがって、クリプト マップを使用する他の機能を GET VPN インターフェイスに設定する場合は、それらの他の ACL 内の deny ステートメントで特定されるすべてのトラフィックも、フェールクローズ ACL および暗黙的な最後の permit ip any any ステートメントによってトラップ（およびドロップ）されます。そのため、GET VPN にフェールクローズ モードを設定すると、そのインターフェイスに設定する GET VPN 以外のサービスにも影響を与えることがあります。
- 登録に成功すると、フェールクローズ ACL および暗黙的な最後の permit ip any any ステートメントはクリプトマップから削除されます。これらのポリシーは、永続的ではありません。
- フェールクローズ ACL ポリシー オブジェクトでは、次のルールを含めることを検討する必要があります。これらのルールは、グループ メンバーの観点からのものであることに注意してください。
  - SSH および SSL（HTTPS）トラフィック：ユーザおよび Security Manager は、デバイスにアクセスして、デバイスを設定できる必要があります。デバイスをロックすることがないように、SSH および SSL 用の deny ステートメントを含めます。SSH 用には、**deny tcp any eq 22 <host or network address>** ステートメントを含めます。SSL 用には、**deny tcp any eq 443 <host or network address>** ステートメントを含めます。ホストのアドレスを指定する場合は、Security Manager サーバもホストの 1 つとして含めます。
  - ルーティング トラフィック：ルーティングをイネーブルにするには、ルーティング プロセスのトラフィックを許可します。たとえば、OSPF を使用している場合は、**deny ospf any any** を含めます。
  - GDOI トラフィック：デバイスでは、フェールクローズ ACL の内容にかかわらず GDOI 登録メッセージが検索されるため、正常に登録するためには明示的にこれらのメッセージを許可する必要はありません。ただし、グループ メンバー（1）がキー サーバと他のグループ メンバー（2）との間のパス上に位置している場合、グループ メンバー（1）が登録に失敗すると、グループ メンバー（2）がブロックされて、正常に登録できなくなります。グループ メンバー（2）が正常に登録されるためには、グループ メンバー（1）に、GDOI トラフィックの通過を許可するフェールクローズ ACL を設定する必要があります。したがって、フェールクローズ ACL に **deny udp any eq 848 any eq 848** を含めて、GDOI トラフィックを許可することを推奨します。

関連項目

- GET VPN の設定 （1634 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- 拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）

GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて

GET VPN では、クリプト マップ アクセス コントロール リスト（ACL）を使用して、VPN で暗号化される必要があるトラフィックが特定されます。これらの ACL では、暗号化する代わりにクリア テキストとして送信する必要があるトラフィック（実質的に VPN 外部となるトラフィック）も指定されます。これらの ACL の集合によって、VPN のセキュリティ ポリシーが定義されます。

GET VPN では、多階層のセキュリティ ポリシーが提供されます。VPN 全体の一般的なポリシーはキー サーバに定義しますが、グループ メンバーに個別のセキュリティ ポリシーを定義して、ローカルのバリエーションを用意することもできます。グループ メンバー セキュリティ ポリシーは、キー サーバから受信したポリシーよりも常に優先されます。グループメンバーがキーサーバーに登録されると、グループメンバーはキーサーバーのセキュリティポリシーとセキュリティアソシエーションをダウンロードします。次に、グループメンバーは、1 番めにグループメンバーの ACL、2 番めにキーサーバーの 1 つめの ACL、3 番め以降も同様にキーサーバーのすべての ACL をキーサーバーに定義されている順序で連結することによって、新しい単一のセキュリティ ポリシー クリプトマップ ACL を作成します。これらのマージされた ACL は単一の ACL として処理されることを理解することが重要です。これらは別個の ACL として検索されるわけではありません。したがって、トラフィックがグループメンバーの ACL の deny ステートメントに一致した場合、そのトラフィックは、キーサーバーからダウンロードされたどの ACL ルールに対してもテストされることはありません。

ヒント グループ メンバーが GET VPN から離脱すると、キー サーバからダウンロードされた ACL は削除されますが、グループ メンバー セキュリティ ポリシー ACL は維持されて、デバイスに設定されたままとなります。

GET VPN セキュリティ ポリシー ACL（およびクリプト マップ ACL 全般）では、permit キーワードと deny キーワードには特別な意味があります。

- **Permit**：このトラフィックを暗号化する」ことを意味します。permit エントリは、キーサーバーの [グループ暗号化ポリシー（Group Encryption Policy）] で定義されるセキュリティポリシー ACL にだけ設定できます。これは、暗号化されるトラフィックには、トラフィックの暗号化に使用されるトランスフォームセット、アンチリプレイ設定、IPsec ライフタイム設定を含む、完全な IPsec セキュリティ アソシエーションが存在する必要があ

るためです。パケットが permit エントリに一致するが、そのパケットに IPsec SA がない場合、そのパケットはドロップされます。

通常、permit ルールは対称的である必要があります。つまり、送信元アドレスと宛先アドレスは同じである必要があります。異なる送信元アドレスと宛先アドレスを指定する必要がある場合は、2 つのルールを作成する必要があります。2 つめのルールは、1 つめのルールの送信元アドレスと宛先アドレスを入れ替えた、対称的なルールとする必要があります。

- **deny**：「このトラフィックを暗号化しない」ことを意味します。実際には、通常、deny ステートメントに一致するトラフィックがクリアテキストで送信されることを意味します。ただし、クリプトマップを使用する他の機能を設定した場合、「拒否された」トラフィックは後続の（プライオリティの低い）クリプトマップ ACL と比較されて、一致するエントリがあるかどうかが確認されます。deny ルールに対しては、IPsec Security Association（SA; セキュリティ アソシエーション）は生成されません。

次に、設定できるセキュリティ ポリシーをプライオリティ順にまとめます。

- **グループ メンバー セキュリティ ポリシー**：グループメンバーの設定時に（GET VPN グループ メンバーの設定 （1645 ページ）を参照）、ローカル グループ メンバー セキュリティ ポリシーを定義する ACL ポリシーオブジェクトをオプションで選択できます。

このグループ メンバー ACL ポリシー オブジェクトには、deny ステートメントだけを設定できます。この ACL を使用して、暗号化から除外し、クリア テキストで送信するトラフィックを特定できます。たとえば、グループ内の一部のグループメンバーが通常とは異なるルーティングプロトコルを実行している場合、キーサーバーレベルでグローバルにポリシーを定義する代わりに、これらのグループメンバーのセキュリティポリシー ACL にローカルエントリを設定して、ルーティング プロトコル トラフィックの暗号化を回避できます。

- **キー サーバー セキュリティ ポリシーおよびセキュリティ アソシエーション**：GET VPN に Group Encryption ポリシーを設定する場合（GET VPN グループ暗号化の定義 （1453 ページ）を参照）、VPN で暗号化および保護する必要があるトラフィックを特定する ACL を設定します。

キー サーバのセキュリティ ポリシーと、トランスフォーム セットやその他の設定が組み合わされて、セキュリティ アソシエーションが定義されます。実際には、ACL 内の各ルールに対して 2 つの IPsec Security Association（SA; セキュリティ アソシエーション）が設定され、これらの SA によって、選択されたトラフィックの暗号化方法が定義されます。したがって、すべてのグループ メンバーで同じグループ SA が使用されるため、グループ メンバー間で SA をネゴシエートする必要がありません。

キーサーバーのポリシーはグループメンバーのポリシーに付加されるため、ポリシーは**permit ip any any**のようなシンプルなものになるかもしれません。つまりグループメンバーポリシーによって除外されていないすべてのトラフィックを暗号化します。

ただし、異なるトランスフォームセットに関連付けられて異なるタイプの暗号化を定義する、いくつかの別個の ACL ポリシー オブジェクトを設定して、より複雑なセキュリティ ポリシーとセキュリティ アソシエーションのセットを作成することもできます。

複数のセキュリティ アソシエーションを作成する場合は、順序を指定する必要があります。セキュリティ アソシエーションは、指定された順序でグループ ポリシーに追加されます。追加された結果単一の ACL が作成されるため、最初の ACL に deny ステートメントを含めると、後続のセキュリティ アソシエーションにおける同じトラフィックに対するすべての permit ルールは無視されて、トラフィックは暗号化されずにクリア テキストで送信されます。

（注） Group Encryption ポリシーに定義されるセキュリティ アソシエーションを全体としては、最大 100 の ACL permit エントリを定義できます。各 permit エントリによって、IPsec SA のペアが作成されます。グループ内の IPsec SA の最大数は 200 を超えることができません。対象のトラフィックを可能なかぎり少ない permit エントリにまとめ、送信元アドレスと宛先アドレスが同じである対称的なポリシーを構築することを推奨します。一意の送信元アドレス範囲と宛先アドレス範囲を定義する必要がある通常の IPsec ポリシーとは異なり、送信元アドレス範囲と宛先アドレス範囲が同じである場合に GET VPN は最適化されます。送信元アドレスと宛先アドレスが異なるルールを設定する場合は、（送信元アドレスと宛先アドレスを入れ替えた）対称的なルールも設定する必要があります。この場合、4 つの SA が使用されます。

これらのセキュリティ ポリシー以外に、グループ メンバーにフェールクローズ モードを設定した場合にトラフィック パターンに影響を与える追加のフェールクローズ ACL もあります。詳細については、登録の失敗時にも保護するためのフェールクローズの設定 （1628 ページ）を参照してください。

関連項目

- GET VPN の設定 （1634 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- 拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）

時間ベースのアンチリプレイについて

アンチリプレイは、IPsec（RFC 2401）などのデータ暗号化プロトコルにおける重要な機能です。アンチリプレイを使用すると、第三者が IPsec 通信やパケットを盗聴して、あとでこれらのパケットをセッションに挿入することを防止できます。時間ベースのアンチリプレイ メカニズムは、すでに過去の時点で到着しているパケットの再送を検出することによって、無効なパケットを廃棄できます。

GET VPN では、Synchronous Anti-Replay（SAR; 同期アンチリプレイ）メカニズムを使用して、複数の送信者からのトラフィックに対するアンチリプレイ保護が提供されます。SAR は、実社会のネットワーク タイム プロトコル（NTP）クロックや、シーケンシャル カウンタ メカニズム（パケットが送信順に受信されて処理されることを保証するメカニズム）とは独立しています。SAR クロックは、ルール正しく進みます。このクロックによって追跡される時間は、疑似時間と呼ばれます。疑似時間はキー サーバによって管理され、キーの再生成メッセージ内の pseudoTimeStamp と呼ばれるタイムスタンプ フィールドとしてグループ メンバーに定期的に送

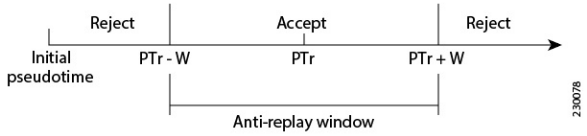
信されます。グループ メンバーは、定期的にキー サーバの疑似時間に再同期される必要があります。キー サーバの疑似時間は、最初のグループ メンバーが登録されたときから進み始めます。最初は、登録プロセス中に、キー サーバからグループ メンバーに対して、キー サーバの現在の疑似時間の値およびウィンドウ サイズが送信されます。時間ベースのリプレイ対応情報、ウィンドウ サイズ、キー サーバの疑似時間などの新しい属性は、SA ペイロード（TEK）で送信されます。

グループ メンバーは、疑似時間を使用して次のようにリプレイを防止します。pseudoTimeStampには、送信者がパケットを作成したときの疑似時間の値が含まれています。受信者は、送信者の疑似時間の値と自身の疑似時間の値を比較して、パケットが再送されたパケットであるかどうかを判断します。受信者は、時間ベースのアンチリプレイ ウィンドウを使用して、そのウィンドウ内のタイムスタンプ値を含むパケットを受け入れます。ウィンドウ サイズは、キーサーバで設定されて、すべてのグループ メンバーに送信されます。

次の図は、アンチリプレイ ウィンドウを示しています。値PTrは受信者のローカルの疑似時間を、W はウィンドウ サイズを示しています。

アンチリプレイは、Group Encryption ポリシーのセキュリティ アソシエーション定義に設定します。詳細については、 GET VPN グループ暗号化の定義 （1453 ページ）および [Add New Security Association]/[Edit Security Association] ダイアログボックス （1459 ページ）を参照してください。

図 *39* : アンチリプレイ ウィンドウ



GET VPN の設定

Group Encrypted Transport（GET）を使用して完全メッシュ VPN を設定するには、 VPN トポロジの作成または編集 （1416 ページ）の説明に従ってCreate VPN ウィザードを使用します。ウィ

ザードが終了したら、RSA キーを同期するかどうかを尋ねられます。RSA キーの同期は、VPN が正常に動作するために必要です。詳細については、RSA キーの生成と同期 （1636 ページ）を参照してください。

キーの再生成転送メカニズムとしてマルチキャストを選択した場合は、すべてのキーサーバおよび必要なグループメンバーにおいてマルチキャストをイネーブルにする必要があります。詳細については、キーの再生成転送メカニズムの選択 （1625 ページ）を参照してください。

Edit VPN ウィザードを使用すると、GET VPN の名前と説明だけを変更できます。他のポリシーや設定を変更する必要がある場合は、[Site-to-Site Manager] ページで次のようにポリシーを開きます。

- ISAKMP および IPsec 設定の場合は、[GET VPNのグローバル設定（Global Settings for GET VPN）] を選択します。GET VPN のグローバル設定 （1640 ページ）を参照してください。
- IKE プロポーザルポリシーの場合は、[GET VPNのIKEAプロポーザルポリシー（IKE Proposal Policy for GET VPN）] を選択します。GET VPN の IKE プロポーザルの設定 （1638 ページ）を参照してください。
- セキュリティ アソシエーション（ACL ルール）および IPsec ポリシーの場合は、[グループ暗号化ポリシー（Group Encryption Policy）]>[セキュリティアソシエーション（Security Associations）] を選択します。GET VPN グループ暗号化の定義 （1453 ページ）を参照してください。
- 事前共有キーポリシーの場合は、[IKEv1事前共有キー（IKEv1 Preshared Key）] を選択します。IKEv1 事前共有キー ポリシーの設定 （1540 ページ）を参照してください。
- 公開キー（PKI）ポリシーの場合は、[公開キーインフラストラクチャ（Public Key Infrastructure）] を選択します。サイト間 VPN での IKEv1 公開キー インフラストラクチャ ポリシーの設定 （1549 ページ）を参照してください。
- キーの再生成設定の場合は、[グループ暗号化ポリシー（Group Encryption Policy）]>[グループ設定（Group Settings）] を選択します。GET VPN グループ暗号化の定義 （1453 ページ）およびRSA キーの生成と同期 （1636 ページ）を参照してください。
- RSA キーの同期を含むキー サーバーの設定の場合は、[キーサーバー（Key Servers）] を選択します。GET VPN キー サーバの設定 （1642 ページ）およびRSA キーの生成と同期 （1636 ページ）を参照してください。
- グループメンバーシップおよびエンドポイント設定の場合は、[グループメンバー（Group Members）] を選択します。GET VPN グループ メンバーの設定 （1645 ページ）を参照してください。

関連項目

- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN 登録プロセスについて （1623 ページ）
- GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）

- GET VPN 設定のトラブルシューティング （1652 ページ）
- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）

RSA キーの生成と同期

Group Encryption ポリシーで RSA キーラベルを指定する場合（ GET VPN グループ暗号化の定義 （1453 ページ）を参照）、対応する RSA キー（公開キーと秘密キー）が GET VPN トポロジ内のすべてのキーサーバーに設定されている必要があります。キーは、デバイスに定義した既存のキー、または新しいキー ラベルを指定できます。Security Manager によってキーが生成されて、すべてのキー サーバが同じキーを使用するように同期されます。

Security Manager で RSA キーを生成して同期するには、次の方法を使用できます。

- Create VPN ウィザードを使用して新しい GET VPN を作成する場合は、ウィザードの最後に、キーを同期するかどうかを尋ねられます。[はい（Yes）] をクリックすると、Security Manager によってすぐにキーの同期が実行され、キーがまだ存在していない場合には新しいキーが生成されます。Create VPN ウィザードの使用方法の詳細については、 VPN トポロジの作成または編集 （1416 ページ）を参照してください。
- 既存の GET VPN では、キーサーバーポリシーで [キーの同期（Synchronize Keys）] ボタンをクリックできます。キー サーバを追加する場合や、プライマリ キー サーバで新しいキーを生成する場合には、必ずこのプロセスを使用します。既存のトポロジにおけるキー サーバの設定の詳細については、GET VPN キー サーバの設定 （1642 ページ）を参照してください。

ヒント 既存の GET VPN トポロジで新しい RSA キーを生成する場合は、Group Encryption ポリシーを更新して新しい未使用の RSA キー ラベルを指定し、Key Servers ポリシーで [Synchronize Keys] ボタンをクリックするのが最も簡単な方法です。キーはどのキー サーバにも存在しないため、Security Manager によって新しいキーが生成されて、すべてのキー サーバにインポートされます。その後、各キー サーバから古いキーを手動で削除できます。

RSA キーは、次のように使用されます。

- キー サーバは、RSA 秘密キーを使用して、グループ メンバーからのキーの再生成メッセージを認証します。
- キー サーバは、登録時にグループ メンバーに対して RSA 公開キーを提供します。
- キー サーバは、秘密キーを使用して、Key Encryption Key（KEK; キー暗号キー）および Traffic Encryption Key（TEK; トラフィック暗号キー）に署名します。RSA キーがないと、キー サーバは KEK および TEK を作成できません。
- RSA キーは、協調キー サーバ間のメッセージの署名にも使用されます。

RSA キー同期プロセスを開始すると、[Synchronize Keys] ダイアログボックスが開き、全体的な経過および各キー サーバにおける結果が表示されます（ [停止（Abort）] ボタンをクリックすると、プロセスをいつでも停止できます）。Security Manager によって次の手順が実行されます。

1. すべてのキー サーバにログインして、VPN に設定された RSA キー ラベルに対応する RSA キー情報が各サーバから取得されます。
2. いずれかのキー サーバに、必要なラベルを持つキーが存在しているかどうかが判断されます。
   - どのキー サーバにも必要なラベルを持つ RSA キーがない場合は、Security Manager によってプライマリ キー サーバ（最も高いプライオリティを持つサーバ）にキーが生成されます。
   - 1 つ以上のキー サーバにキーがなく、キーがあるすべてのキー サーバのキーが同じものである場合は、Security Manager によって、キーがある任意のサーバの既存のキーが使用されます。
   - 複数のキー サーバにキーがあるが、キーの内容がサーバ間で異なる場合は、Security Manager がキーを上書きしてもよいかどうかを尋ねられます。[はい（Yes）] をクリックすると、Security Manager では、プライマリキーサーバーの既存のキーが使用されます。

[いいえ（No）] をクリックした場合は、Security Manager 外部でキーサーバーにログインして、必要に応じて手動でキーを調整できます。ただし、すべてのキー サーバの RSA キーの内容は同じである必要があります。このプロセスについては、後述の説明を参照してください。

1. キーのエクスポート可能なバージョンが作成されます。
2. キーが、残りの各キー サーバにインポートされます。

ヒント　同期プロセスが成功するためには、デバイスがオンラインかつ到達可能であり、ユーザに展開権限がある必要があります。デバイスへの接続が失敗したり、タイムアウトしたりした場合は、Security Manager サーバからキー サーバに対する ping が成功することを確認します。ライブ デバイスではなくファイルに展開する場合は、後述の説明に従って手動でキーを生成および同期する必要がある場合があります。十分な権限がない場合は、プロセスを開始できないため、他のユーザにプロセスの実行を依頼する必要があります。

RSA キーの手動での生成と同期

Security Manager でキーを生成および同期しない場合、または何らかの理由で Security Manager においてプロセスを完了できない場合には、特権 EXEC（イネーブル）コンフィギュレーション モードで次の手順を使用して手動でキーを生成および同期できます。

1. 次のコマンドを使用して、キーサーバーにキーを生成します。**rekeyrsa** はキーの名前です（任意の名前を指定できます）。キーは、エクスポート可能にする必要があります。

crypto key generate rsa general-keys label rekeyrsa modulus 1024 exportable

1. 次のコマンドを使用して、キーのエクスポート可能なコピーを作成します。**passphrase** は、インポート用にキーを暗号化するために使用される文字列です（任意のパスフレーズを指定できます）。

crypto key export rsa rekeyrsa pem terminal 3des passphrase

このコマンドによって、公開キーと秘密キーが端末に出力されます。これらをクリップボードにコピーして、他のキー サーバへのインポートに使用できます。キーは **----BEGIN/END PUBLIC KEY----** と **----BEGIN/END RSA PRIVATE KEY----** によって区切られています。また、URL にエクスポートすることもできます。コマンドの使用方法の詳細については、Cisco.com の『*Cisco IOS Security Command Reference*』を参照してください。

1. 次のコマンドを使用して、他の各キー サーバにキーをインポートします。

crypto key import rsa rekeyrsa pem exportable terminal passphrase

キーをコピー アンド ペーストする場合は、BEGIN と END の行を含めます。

GET VPN の IKE プロポーザルの設定

[IKE Proposal for GET VPN] ページを使用して、GET VPN トポロジで使用される IKE プロポーザルを定義します。IKE プロポーザルは、キー サーバおよびグループ メンバーに設定されます。

これらの設定は、ISAKMP Security Association（SA; セキュリティ アソシエーション）用の設定です。単一のキー サーバを使用している場合、最初のグループ メンバー登録後には ISAKMP SA は使用されません。複数のキー サーバ（協調キー サーバ）を使用している場合は、キー サーバ間の通信で ISAKMP SA が必要です。

[IKE Proposal for GET VPN] ページを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））既存の GET VPN トポロジを選択して、ポリシーセレクタで [GET VPN の IKE プロポーザル（IKE Proposal for GET VPN）] を選択します。
- （ポリシービュー）[サイト間 VPN（Site-to-Site VPN）] > [GET VPN の IKE プロポーザル（IKE Proposal for GET VPN）] を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

次の表で、このポリシーで定義できる設定について説明します。

表 *359 : IKE Proposal for GET VPN* ポリシー

要素	説明
IKE Proposal	使用する設定を定義した IKE プロポーザル ポリシー オブジェクト。そのまま使用できる定義済みのオブジェクトもいくつか用意されています。 [選択（Select）] をクリックして、既存の IKE プロポーザルオブジェクトのリストを開きます。選択するオブジェクトでは、グループに設定する認可方式と同じ方式が使用されている必要があります（たとえば、事前共有キーを使用する場合はプレフィックス **preshared** を持つオブジェクト名を、Public Key Infrastructure（PKI）証明書を使用する場合はプレフィックス **cert** を持つオブジェクト名を選択します）。 オブジェクトを選択して [OK] をクリックすると、オブジェクトに定義されている設定が [IKE プロポーザルの設定（IKE Proposal Settings）] 表示フィールドに表示されます。また、選択リストで編集することによっても設定を確認できます。適切な既存のオブジェクトが見つからない場合は、選択リストの [追加（Add）]（+）ボタンをクリックして、新しいオブジェクトを作成します（詳細およびオプションの詳細な説明については、[IKEv1 Proposal] ポリシー オブジェクトの設定 （1490 ページ）を参照してください）。
IKE Proposal Overrides	キー サーバおよびグループ メンバーの ISAKMP SA の有効秒数。ライフタイムを超えると、SA の期限が切れ、ピア間で再ネゴシエートする必要があります。1 ～ 86400 の値を指定できます。 • 協調キー サーバ（複数のキー サーバ）を使用している場合は、キー サーバのライフタイムを高く設定します。デフォルトの 86400 が適切です。 • 単一のキー サーバを使用している場合は、必要以上に長く ISAKMP SA が保持されないようにライフタイムを低く設定します（ただし、60 秒未満には設定しないでください）。グループ メンバー登録後は使用されません。 • 特に協調キー サーバが設定されている場合には、キー サーバのライフタイムと比較してグループ メンバーのライフタイムを低く設定することを推奨します。

関連項目

- IKE について （1482 ページ）
- サイト間 VPN での IKEv1 事前共有キー ポリシーについて （1538 ページ）
- GET VPN グループ暗号化の定義 （1453 ページ）
- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）

GET VPN のグローバル設定

[Global Settings for GET VPN] ページを使用して、GET VPN トポロジ内のデバイスに適用する ISAKMP および IPsec のグローバル設定を定義します。

（注） このポリシー内のライフタイム設定は、キー サーバおよびグループ メンバーの ISAKMP セキュリティ アソシエーションのライフタイムには適用されません。これらのライフタイム値は、IKE Proposal for GET VPN ポリシーで設定されます。詳細については、GET VPN の IKE プロポーザルの設定 （1638 ページ）を参照してください。

[Global Settings for GET VPN] ページを開くには、次の手順を実行します。

- （[Site-to-Site VPN Manager] ウィンドウ （1404 ページ））既存の GET VPN トポロジを選択して、ポリシーセレクタで [GET VPN のグローバル設定（Global Settings for GET VPN）] を選択します。
- （ポリシービュー）[サイト間 VPN（Site-to-Site VPN）] > [GET VPN のグローバル設定（Global Settings for GET VPN）] を選択して、既存のポリシーを選択するか、または新しいポリシーを作成します。

次の表で、このポリシーで定義できる設定について説明します。

表 *360 : Global Settings for GET VPN*

要素	説明
Enable Keepalive（キーサーバだけ）	キー サーバ間で Dead Peer Detection（DPD）キープアライブ メッセージをイネーブルにするかどうかを指定します。複数のキーサーバー（協調キーサーバー）がある場合は、定期的なキープアライブをイネーブルにして、サーバー間で相互のステータスを把握し、必要に応じて新しいプライマリサーバーを選定できるようにする必要があります。次を設定します。 • [間隔（Interval）] : [定期（Periodic）] も選択した場合は、DPD メッセージ間の秒数です。[Periodic] を選択しない場合は、トラフィックがピアから受信されない場合に DPD リトライ メッセージが送信されるまでの秒数です。範囲は 10 ～ 3600 秒です。 • [リトライ（Retry）] : DPD リトライメッセージに対するピアからの応答がない場合の DPD リトライメッセージ間の秒数です。値の範囲は 2 ～ 60 秒です。デフォルトで、DPD リトライ メッセージは 2 秒ごとに送信されます。5 回 DPD リトライ メッセージを送信しても応答がない場合、そのキー サーバはダウンとマークされます。 • [定期（Periodic）] :（他のキーサーバーからトラフィックを受信しているかどうかにかかわらず）DPD メッセージを定期的に送信するかどうかを指定します。GET VPN では、[Periodic] を選択する必要があります。
アイデンティティ（Identity）	フェーズ I の IKE ネゴシエーション中に、ピアは相互に識別する必要があります。使用する ISAKMP アイデンティティを選択します。 • [Address]（デフォルト）：IKE ネゴシエーションに参加するインターフェイスの IP アドレス。アドレスは、1 つのインターフェイスだけがネゴシエーションに参加し、その IP アドレスが既知である（スタティックである）場合に使用します。 • [Hostname]：完全修飾ホスト名（router1.example.com など）。 • [識別名（Distinguished Name）]
SA Requests System Limit	IKE が SA 要求の拒否を開始する前に許可される SA 要求の最大数。ピアの数以上の値を指定する必要があります。ピアの数未満の値を指定した場合は、VPN トンネルが切断される可能性があります。 0 ～ 99999 の値を入力できます。
SA Requests System Threshold	IKE が新規 SA 要求の拒否を開始する前に使用できるシステム リソースのパーセンテージ。デフォルトは 75% です。

要素	説明
IPsec 設定	IPsec SA のデフォルトのライフタイム設定を変更する場合は、[ライフタイムを有効化（Enable Lifetime）] を選択します。グループ メンバー間のトラフィック量（KB 単位）、秒数、またはその両方に基づいてライフタイムを設定できます。いずれかの値に達するとキーが失効します。デフォルトは次のとおりです（これらのデフォルトは、このオプションを選択しない場合でも設定されています）。 • [ライフタイム（秒）（Lifetime（secs））]：3600 秒（1 時間）。 • [ライフタイム（KB）（Lifetime (kbytes)）]：4,608,000 KB。 ヒント　セキュリティアソシエーションの設定時に、トラフィック暗号キー用のこれらの値を上書きできます。GET VPN グループ暗号化の定義 （1453 ページ）および [Add New Security Association]/[Edit Security Association] ダイアログボックス （1459 ページ）を参照してください。

関連項目

- IKE について （1482 ページ）
- サイト間 VPN の IPsec プロポーザルについて （1500 ページ）
- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）

GET VPN キー サーバの設定

Key Servers ポリシーを使用して、GET VPN トポロジで使用するキー サーバを定義します。

Key Servers ポリシーを開くには、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）で既存の GET VPN トポロジを選択して、[ポリシー（Policies）] リストから [キーサーバー（Key Servers）] を選択します。

テーブルに、VPN で使用されているキーサーバが表示され、デバイス名、アイデンティティ、プライオリティ、および登録インターフェイスが表示されます。これらの属性の詳細については、 [Edit Key Server] ダイアログボックス （1644 ページ）を参照してください。

- テーブルにキーサーバーを追加するには、[行の追加（Add Row）] ボタンをクリックして、表示されるリストからデバイスを選択します。キーサーバとして含めることができるデバイスだけが表示されます。
- キーサーバーの特性を編集するには、キーサーバーを選択して、[行の編集（Edit Row）] ボタンをクリックします。[Edit Key Server] ダイアログボックスに入力します（ [Edit Key Server] ダイアログボックス （1644 ページ）を参照）。

- キーサーバーを削除するには、キーサーバーを選択して、[行の削除（Delete Row）] ボタンをクリックします。
- キーサーバー間で RSA キーを同期して、すべてのサーバーで同じキーが使用されるようにするには、[キーの同期（Synchronize Keys）] ボタンをクリックします。キーの同期が必要なタイミングや理由を含むキー同期プロセスの詳細については、RSA キーの生成と同期 （1636 ページ）を参照してください。

  協調キー サーバを使用する場合のキー サーバの順序を変更するには、キー サーバを選択して、上向きまたは下向きの矢印ボタンをクリックします。この順序では、どのサーバがプライマリ キー サーバであるかは定義されません（プライマリ キー サーバは、[Priority] の値によって決定されます。値が大きいほど、そのサーバがプライマリ キー サーバとして選定される確率が高くなります）。

代わりに、グループ メンバーがキー サーバへの登録を試みるデフォルトの順序が決定されます。グループ メンバーは、リストの最初のキー サーバに登録されます。最初のキー サーバに到達できない場合、グループ メンバーは、2 番め以降のキー サーバに順番に登録を試みます。キー サーバの冗長性の詳細については、協調キー サーバを使用した冗長性の設定 （1627 ページ）を参照してください。個別のグループ メンバーでこの順序を上書きできます。GET VPN グループ メンバーの設定 （1645 ページ）および[Edit Group Member] ダイアログボックス （1646 ページ）を参照してください。

ヒント テーブルの下にある [表示（Show）] フィールドを使用して、[アイデンティティ（Identity）] カラムおよび [インターフェイス（interfaces）] カラムに、インターフェイスロールを表示するか、またはこれらのロールによって定義されている実際のインターフェイスを表示するかを切り替えることができます。

関連項目

- GET VPN 登録プロセスについて （1623 ページ）
- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）
- デバイス ビューにおける VPN トポロジの設定 （1405 ページ）
- テーブルのフィルタリング （64 ページ）

[Add Key Server]、[Add Group Member] ダイアログボックス

[Add Key Server] ダイアログボックスおよび [Add Group Member] ダイアログボックスを使用して、GET VPN トポロジで使用されるキー サーバまたはグループ メンバーを選択します。目的のデバイスの横にあるチェックボックスを選択して、[OK] をクリックします。

ナビゲーション パス

GET VPN トポロジにキーサーバーまたはグループメンバーを追加するには、[VPNの作成（Create VPN）] ウィザードの [VPNピアの取得（GET VPN Peers）] ページにある [キーサーバーまたはグループメンバー（Key Server or Group Member）] テーブルの下の [行の追加（Add Row）]（+）をクリックします。既存のトポロジの場合は、[キーサーバー（Key Servers）] ポリシーまたは [グループメンバー（Group Members）] ポリシーを使用します。詳細については、次の項を参照してください。

- GET VPN ピアの定義 （1461 ページ）
- GET VPN キー サーバの設定 （1642 ページ）
- GET VPN グループ メンバーの設定 （1645 ページ）

[Edit Key Server] ダイアログボックス

[Edit Key Servers] ダイアログボックスを使用して、GET VPN トポロジのキー サーバに定義されている属性を変更します。

ナビゲーション パス

- （Create VPN ウィザード）[GET VPNピア（GET VPN Peers）] ページに移動し、キーサーバーを選択して、[行の編集（Edit Row）] ボタンをクリックします。 GET VPN ピアの定義 （1461 ページ）を参照してください。
- （ [Site-to-Site VPN Manager] ウィンドウ （1404 ページ））[キーサーバー（Key Servers）] ポリシーを選択し、キーサーバーを選択して、[行の編集（Edit Row）] ボタンをクリックします。 GET VPN キー サーバの設定 （1642 ページ） を参照してください。

関連項目

- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）

フィールド リファレンス

表 *361 : [Edit Key Server]* ダイアログボックス

要素	説明
Identity Interface	グループ メンバーがキー サーバを識別し、キー サーバに登録するために使用するインターフェイス。デフォルトは、すべてのループバック インターフェイスを識別するループバック インターフェイス ロールです。

要素	説明
プライオリティ	キー サーバのロール（プライマリまたはセカンダリ）を指定する、1～100 の数値。最も高い数値を持つキー サーバがプライマリ キー サーバとなります。2つ以上のキー サーバに同じプライオリティが割り当てられている場合は、最も大きい IP アドレスを持つデバイスが使用されます。デフォルトのプライオリティは、最初のキー サーバに対しては 100、2 番めのキー サーバに対しては 95 などになります。 （注） ネットワークがパーティション化されている場合は、複数のプライマリ キー サーバが存在することがあります。
登録インターフェイス（Registration Interface）	Group Domain of Interpretation（GDOI）登録を受け入れることができるインターフェイス。登録インターフェイスを指定しない場合、GDOI 登録は任意のインターフェイスで実行できます。

GET VPN グループ メンバーの設定

Group Members ポリシーを使用して、GET VPN トポロジ内のグループ メンバーを定義します。

Group Members ポリシーを開くには、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）で既存の GET VPN トポロジを選択して、[ポリシー（Policies）] リストから [グループメンバー（Group Members）] を選択します。

グループ メンバーのテーブルには、GET VPN のメンバーが表示され、デバイス名、GET 対応インターフェイス、ローカル インターフェイス、およびセキュリティ ポリシーが表示されます。これらの属性の詳細については、[Edit Group Member] ダイアログボックス （1646 ページ）を参照してください。

- テーブルにグループメンバーを追加するには、[行の追加（Add Row）] ボタンをクリックして、表示されるリストからデバイスを選択します。グループ メンバーとして含めることができるデバイスだけが表示されます。
- グループメンバーのエンドポイント特性を編集するには、グループメンバーを選択して、[行の編集（Edit Row）] ボタンをクリックします。[Edit Group Member] ダイアログボックスに入力します（ [Edit Group Member] ダイアログボックス （1646 ページ）を参照）。

テーブル内の複数のグループ メンバーを選択した場合は、右クリックして次のコマンドを選択することによって、それぞれに示す属性だけを編集することもできます。

- [キーサーバー順序の編集（Edit Key Server Order）]：選択したグループメンバーのキーサーバーリストおよび優先順位を変更します。
- [パッシブSAモードの編集（Edit Passive SA Mode）]：選択したグループメンバーでパッシブ SA モードを使用するかどうかを変更します。
- グループメンバーを削除するには、グループメンバーを選択して、[行の削除（Delete Row）] ボタンをクリックします。

ヒント　テーブルの下にある [表示（Show）] フィールドを使用して、[インターフェイス（Interfaces）] 列に、インターフェイスロールを表示するか、またはそれらのロールによって定義されている実際のインターフェイスを表示するかを切り替えることができます。

関連項目

- 登録の失敗時にも保護するためのフェールクローズの設定　（1628 ページ）
- パッシブ モードを使用した GET VPN への移行　（1649 ページ）
- Group Encrypted Transport（GET）VPN について　（1619 ページ）
- GET VPN の設定　（1634 ページ）
- デバイス ビューにおける VPN トポロジの設定　（1405 ページ）
- テーブルのフィルタリング　（64 ページ）

[Edit Group Member] ダイアログボックス

[Edit Group Members] ダイアログボックスを使用して、GET VPN トポロジのグループ メンバーに定義されている属性を変更します。

ヒント　複数のデバイスを選択して、右クリック メニューから編集コマンドを選択すると、このダイアログボックスには選択した編集コマンドに関連するオプションだけが表示されます。

ナビゲーション パス

- （Create VPN ウィザード）[GET VPN ピア（GET VPN Peers）] ページに移動し、グループメンバーを選択して、[行の編集（Edit Row）] ボタンをクリックします。 GET VPN ピアの定義　（1461 ページ）を参照してください。
- （[Site-to-Site VPN Manager] ウィンドウ　（1404 ページ））GET VPN トポロジを選択して、[グループメンバー（Group Members）] ポリシーを選択します。グループメンバーを選択して、[行の編集（Edit Row）] ボタンをクリックします。 GET VPN グループ メンバーの設定　（1645 ページ）を参照してください。

関連項目

- Group Encrypted Transport（GET）VPN について　（1619 ページ）
- GET VPN の設定　（1634 ページ）

フィールド リファレンス

表 *362 : [Edit Group Member]* ダイアログボックス

要素	説明
GET-Enabled Interface	プロバイダー エッジ（PE）への VPN 対応外部インターフェイス。このインターフェイスで発信または終了するトラフィックは、暗号化または復号化が適宜評価されます。複数のインターフェイスを設定できます。 インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。
Interface to be used as local address	キーの再生成情報などのデータを送信するために、キー サーバでグループ メンバーを識別する場合に IP アドレスが使用されるインターフェイス。GET が 1 つのインターフェイスでだけイネーブルになっている場合は、ローカル アドレスとして使用するインターフェイスを指定する必要はありません。GET が複数のインターフェイスでイネーブルになっている場合は、ローカル アドレスとして使用するインターフェイスを指定する必要があります。 インターフェイスまたはインターフェイスロールの名前を入力するか、あるいは [選択（Select）] をクリックして、リストから名前を選択するか、新しいインターフェイスロールを作成します。
セキュリティ ポリシー	キー サーバからダウンロードされたセキュリティ ACL よりも優先される、一部のグループ メンバー固有のトラフィックを拒否するために使用されるローカルのグループ メンバー セキュリティ ACL。拒否されたトラフィックは、暗号化されずにクリア テキストで送信されます。詳細については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ） を参照してください。 ACL オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックして、リストから選択するか、または新しいオブジェクトを作成します。

要素	説明
Enable Fail Close フェール クローズ ACL（Fail Close ACL）	デバイスがキー サーバに正常に登録される前に、デバイスからクリア テキストのトラフィックが送信されることを防止するフェールクローズ モードをデバイスでイネーブルにするかどうかを指定します。フェールクローズ モードを使用するには、Cisco IOS ソフトウェア Release 12.4(22)T または 15.0 以上が必要です。また、フェールクローズ モードは、サポートされているすべての ASR に設定できます。 ヒント　フェールクローズ モードは複雑な機能であり、慎重にフェールクローズ ACL を作成しないとデバイスからロックアウトされる可能性があります。フェールクローズモードをイネーブルにする前に、登録の失敗時にも保護するためのフェールクローズの設定 （1628ページ）を参照してください。 設定の更新が可能となるように、Security Manager サーバとの SSH 通信や SSL 通信などの許可するクリアテキストのトラフィックを指定した ACL ポリシー オブジェクトを選択する必要があります（deny ステートメントを使用）。オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックして、オブジェクトを選択するか、または新しいオブジェクトを作成します。
Override Key Servers	この特定のグループ メンバーにおいて、GET VPN トポロジ全体に設定されているキー サーバ リストを上書きするかどうかを指定します。 このオプションを選択した場合は、トポロジに設定されているキー サーバのうち、選択したグループ メンバーで使用されるサブセットを選択できます。また、それらのサーバのプライオリティ順も変更できます。この設定は、複数の協調キーサーバ間で登録アクティビティを負荷分散するのに役立ちます。詳細については、協調キー サーバを使用した冗長性の設定 （1627ページ）を参照してください。 [選択（Select）] をクリックし、[キーサーバーの選択（Key Servers Selection）] ダイアログボックスを使用して、キーサーバーリストおよびキーサーバーのプライオリティ順を変更します。グループ メンバーでのキー サーバの使用方法を変更する前に、GET VPN トポロジにそのキー サーバが定義されている必要があります。

要素	説明
Enable Passive SA Mode	グループ メンバーをパッシブ Security Association（SA; セキュリティ アソシエーション）モードに設定するかどうかを指定します。このモードでは、グループ メンバーは SA をインバウンド方向でだけインストールします。つまり、グループ メンバーは、暗号化されたデータを受信することができますが、クリア テキストのデータだけを送信します。このモードは、主に既存の VPN から GET VPN に移行する場合に、VPN のテスト目的でだけ役立ちます（このモードを使用するには、グループ メンバーは、Cisco IOS ソフトウェア バージョン 12.4(22)T または 15.0 以上を実行しているか、あるいはサポートされている ASR である必要があります）。 この設定は、Group Encryption ポリシーの [受信のみ（Receive Only）] 設定（トポロジ全体に適用されます）と似ています。このグループ メンバー オプションは、Group Encryption ポリシーの設定よりも優先されます。 これらのパッシブ モード機能を使用して GET VPN への移行または GET VPN のテストを行う方法の詳細については、パッシブ モードを使用した GET VPN への移行 （1649 ページ）を参照してください。

パッシブ モードを使用した GET VPN への移行

既存の VPN（特にクリア テキストを使用する VPN）から GET VPN テクノロジーに移行する場合は、2 つの機能を使用して、ネットワークのダウンタイムを回避するために段階的な移行を行うことができます。これらの機能はほぼ同じものであり、暗号化されたトラフィックを受動的に受け入れるものですが、GET VPN 内の異なる種類のデバイスに設定できます。

通常、完全に展開された GET VPN では、トラフィックは双方向に暗号化されます（双方向 Security Association（SA; セキュリティ アソシエーション））。ただし、テスト中にはパッシブ モードを使用できます。パッシブ モードでは、グループ メンバーは SA をインバウンド方向でだけインストールします。これにより、グループ メンバーは、暗号化されたトラフィックを受信できますが、トラフィックの送信はクリア テキストで行います。その後、VPN をテストし、期待どおりに動作していることを確認してから、完全な暗号化をオンにできます。

GET VPN にパッシブ モードを設定するには、次の機能を使用します。

- **SA 受信専用モード**：受信専用モードは、Group Encryption ポリシーを使用して、トポロジ内のキーサーバーのセキュリティ アソシエーションに設定します。したがって、この設定はトポロジ全体に適用されます。
- **パッシブ SA モード**：パッシブ セキュリティ アソシエーション モードは、個別のグループメンバーに設定します。この設定は、SA受信専用設定よりも優先されます。そのため、トポロジ全体に対して完全な暗号化をオンにして、一部のグループ メンバーをパッシブ モードのままにできます。これにより、グループ メンバーを段階的にテストして、すべてのメンバー デバイスを確認してから完全な暗号化をイネーブルにできます。

ヒント　グループ メンバーにパッシブ SA モードを設定するには、Cisco IOS ソフトウェア Release 12.4(22)T+ または 15.0+、あるいは ASR では Release 2.3（12.2(33)XNC）+ が必要です。

ここでは、これらのパッシブ モード機能を使用して GET VPN に移行する場合に使用できる、エンドツーエンドの移行プロセスの例を示します。

関連項目

- Group Encrypted Transport（GET）VPN について　（1619 ページ）
- GET VPN の設定　（1634 ページ）

ステップ 1　Create VPN ウィザードを使用して、Security Manager に新しい GET VPN トポロジを作成します。ウィザードでは、次のように選択します。

- デバイスを選択するときには、トポロジのキー サーバを選択します。グループ メンバーについては、移行するグループ メンバーのうち最初のセットを選択します。詳細については、 VPN トポロジのデバイスの選択　（1422 ページ）を参照してください。
- グループ暗号化を設定するときは、[受信専用（Receive Only）] を選択します。これにより、トポロジ全体で SA 受信専用機能がイネーブルになります。詳細については、 GET VPN グループ暗号化の定義（1453 ページ）を参照してください。

VPN 作成の詳細については、 VPN トポロジの作成または編集　（1416 ページ）を参照してください。

ステップ 2　VPN のすべてのデバイスに設定を展開します。これで、グループ メンバーは暗号化されたトラフィックの受信はできますが、送信はできなくなります。展開プロセスの詳細については、使用している Workflow モードに応じて次の項を参照してください。

- Workflow 以外のモードでの設定の展開　（515 ページ）
- Workflow モードでの設定の展開　（523 ページ）

ステップ 3　Security Manager の外部で、すべてのグループ メンバーが正常に動作していることを確認します。

たとえば、グループ メンバー デバイスでいくつかの CLI コマンドを使用して、グループ メンバーで暗号化されたパケットを送受信できるかどうかをテストできます。

- グループメンバー 1 で、次のコマンドを設定します。「groupexample」は、VPN の GDOI グループの名前です。このコマンドによって、暗号化されたテキストまたはクリア テキストを受信できるが、クリア テキストだけを送信できるようにデバイスが設定されます。

crypto gdoi gm group groupexample ipsec direction inbound only

- グループ メンバー 2 で、次のコマンドを設定します。このコマンドによって、暗号化されたテキストまたはクリア テキストを受信でき、暗号化されたテキストを送信できるようにデバイスが設定されます。

crypto gdoi gm group groupexample ipsec direction inbound optional

- グループ メンバー 2 からグループ メンバー 1 に ping を実行します。パケットは、グループ メンバー 2 から送信される前に暗号化されます。グループ メンバー 1 は、このパケットを受け入れて、復号化します。メンバー 1 からメンバー 2 に ping を実行した場合、ping はクリア テキストで送信されて、メンバー 2 によって受け入れられます。ACL で ping が許可されていることを確認してください。

ステップ 4 Cisco Security Manager で、[管理（Manage）]>[サイト間VPN（Site-to-Site VPNs）] を選択します（[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を参照）。

GET VPN トポロジを選択して、[グループメンバー（Group Members）] を選択します。

トポロジに追加する残りのグループメンバーを追加します（[グループメンバーの追加（Add Group Member）]（+）ボタンをクリックし、デバイスを選択して、[OK] をクリックします）。

完全な暗号化を有効にする前に、パッシブモードを使用して新しいグループメンバーをテストする場合は、グループメンバーの設定時に [パッシブSAモードの有効化（Enable Passive SA Mode）] を選択します。

- 個別のグループメンバーを設定するには、メンバーを選択して、[グループメンバーの編集（Edit Group Member）]（鉛筆）ボタンをクリックします。
- 一度に複数のデバイスでパッシブモードを有効にするには、Shift または Ctrl を押しながらクリックして複数のデバイスを選択し、右クリックして [パッシブSAモードの編集（Edit Passive SA Mode）] を選択します。その後、オプションを選択して [OK] をクリックします。

グループ メンバーの設定の詳細については、GET VPN グループ メンバーの設定 （1645 ページ）を参照してください。

ステップ 5 設定変更を VPN のすべてのデバイスに展開します。この時点で、すべてのデバイスはパッシブ モードで動作しています。

ステップ 6 Site-to-Site VPN Manager で、GET VPN トポロジを選択して、[Group Encryptionポリシー（Group Encryption Policy）] を選択します。

[受信専用（Receive Only）] の選択を解除します。これにより、トポロジ レベルで SA 受信専用モードがオフになります。

ステップ 7 設定変更を VPN のすべてのデバイスに展開します。テストした最初のグループ メンバーでは、GET VPN は完全暗号化モードで動作しています。パッシブ SA モードをイネーブルにして追加した新しいメンバーは、暗号化されたトラフィックを受信し、クリア テキストのトラフィックを送信しています。

ステップ 8 次の手順を使用して、新しいデバイスを確認し、パッシブ モードをオフにします。この手順は、すべての新しいデバイスに対して同時に実行することも、小さなグループに分けて段階的に実行することもできます。また、ネットワークを拡張したときに新しいグループ メンバーに対してこの手順を実行することもできます。必要に応じて次の手順を繰り返してください。

a) 最初のグループ メンバーを確認したときと同じ方法を使用して、新しいグループ メンバーが正常に動作していることを確認します。

b) グループメンバーのセットを完全暗号化モードに移行する準備が整ったら、Site-to-Site VPN Manager で GET VPN トポロジを選択して、[グループメンバー（Group Members）] を選択します。

c) 完全な暗号化を使用する必要があるすべてのパッシブモードのグループメンバーを選択し、右クリックして、[パッシブSAモードの編集（Edit Passive SA Mode）] を選択します。[パッシブSAモードの有効化（Enable Passive SA Mode）] オプションの選択を解除して、[OK] をクリックします。

d) パッシブ モードを変更したデバイスだけではなく、VPN のすべてのデバイスに設定を展開します。通常は、VPN 内のすべてのデバイスに展開する必要があります。

GET VPN 設定のトラブルシューティング

Security Manager を使用して GET VPN をプロビジョニングおよび展開したあとに GET VPN が動作しない場合は、次の項目をチェックします。

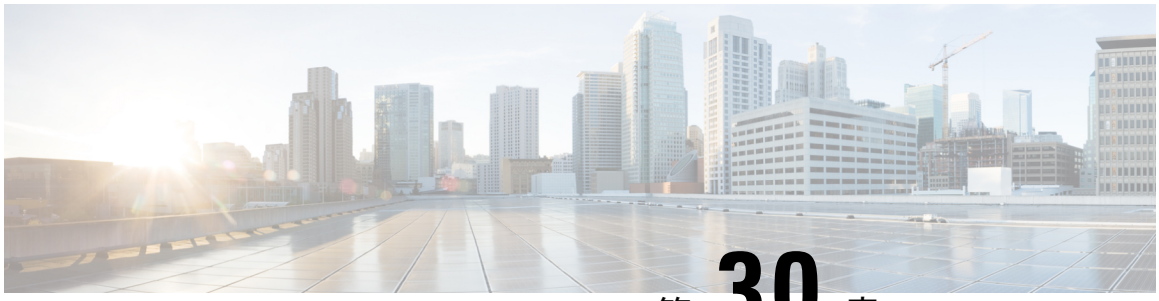
- すべての協調キー サーバ間で RSA キーが同期されていること、つまり RSA キーが同じであることを確認します。キーの同期方法の詳細については、RSA キーの生成と同期 （1636 ページ）を参照してください。
- 目的のトラフィックが暗号化されない場合は、キー サーバのセキュリティ ポリシー ACL（セキュリティ アソシエーション）に目的のトラフィックの permit ACE があることを確認します。非対称の ACE の場合（送信元アドレスと宛先アドレスが異なる場合）は、対称的な ACE（送信元アドレスと宛先アドレスを入れ替えた ACE）が存在することを確認します。詳細については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。
- マルチキャストのキーの再生成を使用する場合は、ネットワーク、すべてのキー サーバ、およびほとんどのグループ メンバーでマルチキャストがイネーブルになっていることを確認します。マルチキャストは、デバイスで直接イネーブルにする必要があります。マルチキャストをイネーブルにするために必要なコマンドは、Security Manager によってプロビジョニングされません。詳細については、キーの再生成転送メカニズムの選択 （1625 ページ）を参照してください。
- マルチキャストのキーの再生成を使用する場合は、キー サーバのセキュリティ ACL にマルチキャスト グループ アドレス用の deny ACE があり、マルチキャストのキーの再生成メッセージが暗号化されないことを確認します。
- グループ メンバーのローカル セキュリティ ACL には deny ACE だけがあることを確認します。暗号化するトラフィックを特定するために permit ステートメントを含めると、対応する IPsec SA がないため、一致するトラフィックは実際にはドロップされます。permit エントリがグループ メンバーにあるため、キー サーバはそのエントリを認識できず、必要な IPsec SA を生成できません。詳細については、GET VPN セキュリティ ポリシーおよびセキュリティ アソシエーションについて （1631 ページ）を参照してください。
- 証明書を使用してグループ メンバーを認可する場合は、ISAKMP 認証で証明書が使用されており、PKI ポリシーが設定されていることを確認します。グループ メンバーおよびキー サーバの ISAKMP アイデンティティは、Distinguished Name（DN; 識別名）を使用するように設定する必要があります。

- 通常、GET VPN が展開されるタイプの WAN 環境では、ネットワーク アドレス変換（NAT）は使用されません。ただし、NAT を使用する場合には、変換されるアドレス用の permit ステートメントがセキュリティ ポリシー ACL にあることを確認します。また、Network Address Translation-Traversal（NAT-T; ネットワーク アドレス変換通過）を使用する場合、GDOI プロトコル ポートは 4500 に変更されます。
- Cisco IOS ソフトウェア Release 12.4(15)T10、12.4(22)T3、12.4(24)T2、15.0(1)M、および 12.2(33)XNE には、コントロール プレーン リプライ保護メカニズムが追加されました。このメカニズムは下位互換性がないため、ネットワーク内のいずれかの GET VPN グループ メンバーがこれらのいずれかの（またはそれ以上の）リリースを実行している場合には、すべてのキー サーバをこれらの（またはそれ以上の）リリースにアップグレードする必要があります。アップグレードしない場合は、キーの再生成に失敗してネットワークが切断される可能性があります。この場合、次のいずれかのシステム ロギング（syslog）メッセージが表示されます。
  - %GDOI-3-GDOI_REKEY_SEQ_FAILURE: Failed to process rekey seq # 2 in seq payload for group get-group, last seq # 6
  - %GDOI-3-PSEUDO_TIME_TOO_OLD: Rekey received in group get-group is too old and failed PST check: my_pst is 184 sec, peer_pst is 25 sec, allowable_skew is 10 sec

ヒント　便利な **show** コマンドの情報を含む、CLI 設定の観点からの追加のトラブルシューティングのヒントについては、Cisco.com の『Cisco Group Encrypted Transport VPN』を参照してください。

関連項目

- Group Encrypted Transport（GET）VPN について （1619 ページ）
- GET VPN の設定 （1634 ページ）



第 30 章

リモート アクセス VPN の管理の基礎

Cisco Security Manager を使用すると、リモート アクセス IPSec VPN およびリモート アクセス SSL VPN の両方を設定できます。Security Manager では、リモート アクセス VPN を次のように柔軟に設定および管理できます。

既存のライブ デバイス、または設定ファイルから、既存のリモート アクセス VPN 設定ポリシーを検出できる。その後、必要に応じて、新しいポリシーまたは更新されたポリシーを変更および展開できます。

設定ウィザードを使用して、これらの 2 種類のリモート アクセス VPN に基本機能をすばやく簡単に設定できる。

ネットワークに必要な機能を把握している場合は、リモート アクセス VPN を独立して設定できる。ウィザードを使用して基本となるリモート アクセス VPN を作成してから、ウィザードに含まれていない追加機能を別途設定することもできます。

また、Cisco Security Manager に備えられているデバイス ビューまたはポリシー ビューによって、リモート アクセス VPN 設定ポリシーの割り当てを柔軟に行うことができます。

一部のポリシーでは、出荷時のデフォルト ポリシー（プライベート ポリシー）または Security Manager を使用して作成した共有ポリシーのいずれかを割り当てることもできます。

この章は次のトピックで構成されています。

- リモート アクセス VPN について （1655 ページ）
- 各リモートアクセスVPNテクノロジーでサポートされるデバイスについて （1665ページ）
- リモート アクセス VPN ポリシーの概要 （1666 ページ）
- リモート アクセス VPN ポリシーの検出 （1669 ページ）
- Remote Access VPN Configuration ウィザードの使用 （1671 ページ）

リモート アクセス VPN について

Security Manager では、IPSec と SSL の 2 種類のリモート アクセス VPN をサポートしています。

ここでは、次の内容について説明します。

- リモート アクセス IPSec VPN について （1656 ページ）
- リモート アクセス SSL VPN について （1657 ページ）

リモート アクセス IPSec VPN について

リモートアクセス IPSec VPN では、企業のプライベートネットワークとリモートユーザーの間で、暗号化されたセキュアな接続が可能になります。これは、ブロードバンドケーブル接続、DSL 接続、ダイヤルアップ接続などの接続を使用して、インターネットに暗号化された IPSec トンネルを確立して実現されます。

リモート アクセス IPSec VPN は、VPN クライアント、および VPN ヘッドエンド デバイスまたは VPN ゲートウェイで構成されます。VPN クライアントソフトウェアはユーザーのワークステーション上にインストールされ、企業ネットワークへの VPN トンネルアクセスを開始します。VPN トンネルの一方の端が、企業サイトのエッジに位置する VPN ゲートウェイとなります。

VPN クライアントが VPN ゲートウェイ デバイスへの接続を開始すると、Internet Key Exchange（IKE; インターネット キー交換）によるデバイスの認証と、続く IKE Extended Authentication（Xauth; 拡張認証）によるユーザの認証からなるネゴシエーションが行われます。次に、モード設定を使用してグループ プロファイルが VPN クライアントにプッシュされ、IPsec Security Association（SA; セキュリティ アソシエーション）が作成されて VPN 接続が完了します。

ヒント ASA 8.4(1) 以降のデバイスでホストされるリモートアクセス IPsec VPN には、IKE バージョン 2（IKEv2）を設定するオプションがあります。IKEv2 を使用する場合、通常の IPSec ポリシーに加えて、いくつかの SSL VPN ポリシーを設定する必要があります。また、ユーザは AnyConnect 3.0 以降の VPN クライアントを使用して、IKEv2 接続を確立する必要があります。詳細については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）を参照してください。

リモート アクセス IPSec VPN の場合は、AAA（認証、許可、アカウンティング）を使用してセキュアなアクセスを行います。ユーザ認証を行う場合、接続を完了するには有効なユーザ名およびパスワードを入力する必要があります。ユーザ名とパスワードは、VPN デバイス自体に格納することも、他の多数のデータベースに認証を提供できる外部 AAA サーバに格納することもできます。AAA サーバの使用の詳細については、AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）を参照してください。

（注） サイト間 Easy VPN トポロジでは、リモート アクセス IPsec VPN で使用するものと同じポリシーとポリシー オブジェクトの一部が使用されますが、そのポリシーはリモート アクセス ポリシーとは別に保存されます。Easy VPN でのリモート クライアントは、ルータなどのハードウェア クライアントです。一方、リモート アクセス IPSec VPN でのリモート クライアントは、VPN クライアント ソフトウェアを使用するワークステーションやその他のデバイスです。詳細については、Easy VPN について （1599 ページ）を参照してください。

関連項目

- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （1703 ページ）
- リモート アクセス VPN ポリシーの概要 （1666 ページ）
- リモート アクセス VPN ポリシーの検出 （1669 ページ）

リモート アクセス SSL VPN について

SSL VPN を使用すると、ユーザはインターネットが利用できる任意の場所から企業のネットワークにアクセスできます。ユーザは Secure Socket Layer（SSL）暗号化をネイティブでサポートする Web ブラウザのみを使用して、クライアントレス接続を確立できます。また、フル クライアント（AnyConnect など）やシン クライアントを使用して接続を確立することもできます。

（注） SSL VPN をサポートするのは、ソフトウェア バージョン 8.0 以降が実行され、シングル コンテキスト モードとルータ モードで動作する ASA 5500 デバイス、ソフトウェア バージョン 12.4(6)T 以降が実行されている Cisco 870、880、890、1800、2800、3700、3800、7200、7301 シリーズのルータ、およびソフトウェア バージョン 15.0(1)M 以降が実行されている Cisco 1900、2900、3900 シリーズのルータです。880 シリーズ ルータの場合、ソフトウェアの最小バージョンは 12.4(15)XZ です。これは、Security Manager では 12.4(20)T にマッピングされます。

IOS デバイスでは、SSL 対応の VPN ゲートウェイを介してリモート アクセスが提供されます。リモート ユーザは SSL 対応の Web ブラウザを使用して、SSL VPN ゲートウェイへの接続を確立します。リモート ユーザが Web ブラウザ経由でセキュア ゲートウェイに対して認証されると SSL VPN セッションが確立され、ユーザは企業ネットワーク内部にアクセスできるようになります。ポータル ページを使用すると、SSL VPN ネットワークで使用可能なすべてのリソースにアクセスできます。

ASA デバイスでは、リモート ユーザは Web ブラウザを使用して、セキュリティ アプライアンスへのセキュアなリモート アクセス VPN トンネルを確立します。中央サイトで設定した特定のサポート対象内部リソースとリモート ユーザ間のセキュアな接続は、SSL プロトコルによって実現されます。セキュリティ アプライアンスはプロキシ処理が必要な接続を認識し、HTTP ユーザーは認証サブシステムと通信してユーザーを認証します。

ユーザ認証は、ユーザ名とパスワード、証明書、あるいはその両方を使用して行われます。

（注） ネットワーク管理者は、SSL VPN リソースへのユーザ アクセスを、個々のユーザ単位ではなくグループ単位で指定します。

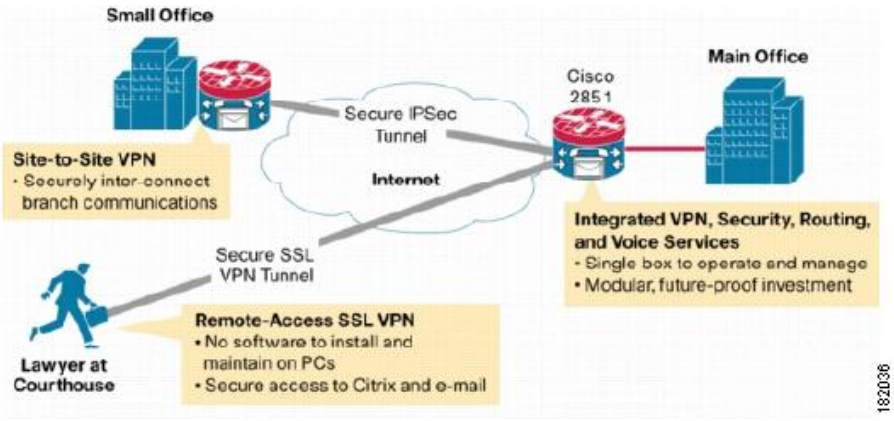
ここでは、次の内容について説明します。

- リモート アクセス SSL VPN の例 （1658 ページ）
- SSL VPN アクセスのモード （1659 ページ）
- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- SSL VPN を設定するための前提条件 （1663 ページ）
- SSL VPN の制限 （1664 ページ）

リモート アクセス SSL VPN の例

次の図では、モバイル ワーカーが、保護されたリソースにメイン オフィスやブランチ オフィスからアクセスする方法を示します。メイン サイトとリモート サイト間のサイト間 IPSec 接続に変更はありません。モバイル ワーカーが企業ネットワークに安全にアクセスするときに必要なものは、インターネット アクセスとサポートされているソフトウェア（Web ブラウザとオペレーティング システム）だけです。

図 *40* : セキュアな *SSL VPN* アクセスの例



SSL VPN アクセスのモード

SSL VPN には、IOS ルータにリモート アクセスする 3 つのモード（クライアントレス、シン クライアント、およびフル クライアント）が用意されています。ASA デバイスでは、クライアントレス（クライアントレスとシン クライアント ポート転送を含む）および AnyConnect クライアント（フル クライアント）の 2 つのモードがあります。

クライアントレス アクセス モード

クライアントレス モードでは、リモート ユーザは、クライアント マシンの Web ブラウザを使用して、内部ネットワークまたは企業ネットワークにアクセスします。アプレットのダウンロードは必要ありません。

クライアントレス モードは、インターネット アクセス、データベース、および Web インターフェイスを使用するオンライン ツールなど、想定されるほとんどのコンテンツに Web ブラウザでアクセスする場合に有効です。このモードでは（HTTP および HTTPS による）Web ブラウジング、Common Internet File System（CIFS）によるファイル共有、および Outlook Web Access（OWA）の電子メールをサポートします。クライアントレスモードが正しく動作するには、リモートユーザーの PC で Windows 2000、Windows XP、または Linux オペレーティングシステムが実行されている必要があります。

Windows オペレーティング システムからブラウザを使用して接続する SSL VPN ユーザは共有ファイル システムを参照でき、フォルダの表示、フォルダとファイルのプロパティの表示、作成、移動、コピー、ローカル ホストからリモート ホストへのコピー、リモート ホストからローカル ホストへのコピー、削除などの操作を実行できます。Web フォルダにアクセスできるようになると、Internet Explorer にそのことが表示されます。このフォルダにアクセスすると、別のウィンドウが開いて共有フォルダが表示されます。フォルダおよびドキュメントのプロパティで許可されている場合、ユーザーはここで Web フォルダの機能を実行できます。

シン クライアント アクセス モード

シン クライアント モードは TCP ポート転送とも呼ばれ、クライアント アプリケーションが TCP を使用して、既知のサーバおよびポートに接続することを前提としています。このモードでは、リモート ユーザはポータル ページに表示されたリンクをクリックして、Java アプレットをダウンロードします。この Java アプレットは、SSL VPN ゲートウェイに設定されているサービスに対する、クライアント マシン上の TCP プロキシとして機能します。Java アプレットは、すべてのクライアント接続に対して新しい SSL 接続を開始します。

Java アプレットは、リモート ユーザ クライアントから SSL VPN ゲートウェイへの HTTP 要求を開始します。HTTP 要求には、内部電子メール サーバの名前およびポート番号が格納されます。SSL VPN ゲートウェイは、その内部電子メール サーバおよびポートに対して TCP 接続を確立します。

シン クライアント モードによって、TCP ベースのアプリケーション（Post Office Protocol Version 3（POP3）、Simple Mail Transfer Protocol（SMTP）、Internet Message Access Protocol（IMAP）、Telnet、Secure Shell（SSH; セキュア シェル）など）へのリモート アクセスがイネーブルになるように Web ブラウザの暗号化機能が拡張されます。

（注） TCP ポート転送プロキシは、Sun の Java ランタイム環境（JRE）バージョン 1.4 以降でのみ動作します。Java アプレットはブラウザを介してロードされ、JRE のバージョンがブラウザで検証されます。互換性のある JRE バージョンが検出されなかった場合、Java アプレットは実行されません。

シン クライアント モードを使用する場合は、次の点に注意する必要があります。

- リモート ユーザが Java アプレットのダウンロードおよびインストールを許可する必要がある。
- TCP ポート転送アプリケーションをシームレスに動作させるには、リモート ユーザの管理権限をイネーブルにする必要がある。
- ポートを動的にネゴシエートする FTP などのアプリケーションには、シン クライアント モードを使用できない。つまり、TCP ポート転送を使用できるのは、スタティックなポートを使用する場合のみです。

フル トンネル クライアント アクセス モード

フル トンネル クライアント モードを使用すると、ネットワーク（IP）レイヤでデータを移動するために使用される SSL VPN トンネルを介して、企業ネットワークにフル アクセスできます。このモードは、Microsoft Outlook、Microsoft Exchange、Lotus Notes E-mail、および Telnet など、ほとんどの IP ベース アプリケーションをサポートします。SSL VPN に接続していることは、クライアントで実行されるアプリケーションに対して完全に透過的です。クライアント ホストと SSL VPN ゲートウェイ間のトンネリングを処理するために、Java アプレットがダウンロードされます。ユーザは、クライアント ホストが内部ネットワークに存在するかのように、任意のアプリケーションを使用できます。

トンネル接続は、グループ ポリシー設定によって指定されます。SSL VPN Client（SVC）または AnyConnect クライアントがリモート クライアントにダウンロードおよびインストールされ、リモート ユーザが SSL VPN ゲートウェイにログインしたときにトンネル接続が確立されます。デフォルトでは、接続を閉じるとクライアント ソフトウェアはリモート クライアントから削除されますが、必要に応じてクライアント ソフトウェアをインストールしたままにしておくことができます。

（注） フル トンネル SSL VPN アクセスには、リモート クライアントでの管理権限が必要です。

SSL VPN サポート ファイルの概要と管理

SSL VPN では、デバイスのフラッシュストレージにサポートファイルが存在する必要がある場合があります。これは特に、ASA デバイスに設定されている SSL VPN の場合に該当します。サポート ファイルには、Cisco Secure Desktop（CSD）パッケージ、AnyConnect クライアント イメージ、およびプラグイン ファイルが含まれています。Security Manager には多数のサポート ファイルが同梱されているため、ユーザはそれらのファイルを使用できます。ただし、ポー

タル ページに使用するグラフィック ファイル、または AnyConnect クライアントに使用するクライアント プロファイルなどの一部のサポート ファイルは、Security Manager では提供されません。

通常は、ファイル オブジェクトを作成してサポート ファイルを指定してから、そのファイル オブジェクトを参照するポリシーを作成するときに、そのファイル オブジェクトを選択する必要があります。必要なファイル オブジェクトは、ポリシーを作成するときに作成することも、ポリシーの定義を開始する前に作成することもできます。詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。

デバイスにポリシーを展開すると、ポリシーで参照されるすべてのサポート ファイルがデバイスにコピーされ、フラッシュ メモリの \csm フォルダに配置されます。ほとんどの場合、このための手動による作業は特に必要ありません。次に、手動の作業が必要となり得る状況をいくつか示します。

- 既存の SSL VPN ポリシーを検出または再検出しようとしている場合は、SSL VPN ポリシーからのファイル参照が正しいものである必要があります。ポリシー検出時にサポート ファイルを処理する方法については、リモート アクセス VPN ポリシーの検出 （1669 ページ）を参照してください。
- アクティブ/フェールオーバー設定の ASA デバイスの場合は、フェールオーバー デバイスにサポート ファイルを配置する必要があります。サポート ファイルは、フェールオーバー時にフェールオーバー デバイスにコピーされません。フェールオーバー デバイスにファイルを配置するには、次の方法を選択できます。
  - アクティブ装置の \csm フォルダからフェールオーバー装置にファイルを手動でコピーする。
  - アクティブ装置にポリシーを展開した後、フェールオーバーを強制実行して、アクティブになった装置にポリシーを再展開する。
- VPN クラスタを使用してロード バランシングを行っている場合は、クラスタ内のすべてのデバイスに同じサポート ファイルが展開されている必要があります。

Cisco Secure Desktop（CSD）パッケージ

このパッケージは ASA SSL VPN に使用します。Dynamic Access ポリシーでパッケージを選択します。選択するパッケージには、デバイスで実行されている ASA オペレーティング システムのバージョンとの互換性が必要です。ASA デバイスのダイナミック アクセス ポリシーを作成する場合は、そのデバイスのオペレーティングシステムと互換性のあるバージョン番号が [バージョン（Version）] フィールドに表示されます。

CSD パッケージは、Program Files\CSCOpx\files\vms\repository\ にあります。ファイル名の形式は、securedesktop-asa_k9-version.pkg または csd_version.pkg です。ここで、version は CSD バージョン番号（3.5.1077 など）です。

次に、Security Manager に付属する CSD パッケージについて、CSD と ASA バージョンの互換性を示します。

- csd_3_6_181-3.6.181.pkg：ASA 8.4 以降。

- csd_3_5_2008-3.5.2008.pkg：ASA 8.0(4) 以降。
- csd_3_5_2001-3.5.2001.pkg：ASA 8.0(4) 以降。
- csd_3_5_1077-3.5.1077.pkg - ASA 8.0(4) 以降
- csd_3_5_841-3.5.841.pkg - ASA 8.0(4) 以降
- csd_3_4_2048-3.4.2048.pkg - ASA 8.0(4) 以降
- csd_3_4_1108-3.4.1108.pkg - ASA 8.0(4) 以降
- securedesktop_asa_k9-3.3.0.151.pkg - ASA 8.0(3.1) 以降
- securedesktop_asa-k9-3.3.0.118.pkg - ASA 8.0(3.1) 以降
- securedesktop-asa-k9-3.2.1.126.pkg - ASA 8.0(3) 以降
- securedesktop-asa_k9-3.2.0.136.pkg - ASA 8.0(2) 以降

CSD バージョンと ASA バージョンの互換性については、Cisco.com にある CSD リリースノート（ http://www.cisco.com/en/US/products/ps6742/prod_release_notes_list.html）および「Supported VPN Platforms」を参照してください。

ダイナミック アクセス ポリシーを作成して CSD を指定する方法については、ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）を参照してください。

AnyConnect クライアント イメージ

これらのイメージは、ASA でホストされるリモート アクセス SSL および IKEv2 IPsec VPN 用です。AnyConnect クライアントはユーザーの PC にダウンロードされ、クライアントの VPN 接続を管理します。Cisco Security Manager には、いくつかの AnyConnect イメージが含まれています。各イメージは Program Files\CSCOpx\files\vms\repository\ に格納されています。パッケージ名には、ワークステーションのオペレーティングシステムと AnyConnect のリリース番号が、anyconnect-client_OS_information-anyconnect_release.pkg といういう一般的なパターンで示されます。たとえば、anyconnect-win-3.0.0610-k9-3.0.0610.pkg は、Windows ワークステーション用の AnyConnect 3.0(0610) クライアントです。k9 はパッケージに暗号化が含まれることを示します。この例では、AnyConnect のリリース番号が繰り返されています。一部のファイル名では、このリリース番号が一度だけ表示される場合もあります。

パッケージは次のワークステーションの Operating System（OS; オペレーティング システム）で使用できます。各クライアントがサポートする OS バージョン固有の情報については、Cisco.com にある AnyConnect クライアントのマニュアルを参照してください。

- Linux：パッケージは anyconnect-linux で始まります。64 ビットバージョンの場合は anyconnect-linux-64 で始まります。
- Mac OS：i386 ワークステーション上の Mac OS X では、パッケージは anyconnect-macosx で始まります。Power PC ワークステーション上の Mac OS X では、anyconnect-macosx-powerpc で始まります。
- Windows：パッケージは anyconnect-win で始まります。

他の AnyConnect クライアントパッケージを Cisco Security Manager サーバーまたはローカルの Cisco Security Manager クライアントにダウンロードして、リモートアクセスポリシーで使用することもできます。Security Manager ではこれらのクライアントのより新しいパラメータを設定できない場合があります。ただし、FlexConfigs を使用してより新しいパラメータを設定できる場合もあります。

AnyConnect クライアント、クライアントのプロファイル、およびデバイスにクライアントをロードするようにポリシーを設定する方法の詳細については、次の項を参照してください。

- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- AnyConnect プロファイルエディタ （1791 ページ）

プラグイン ファイル

これらのファイルは、ブラウザ プラグインとして使用されます。プラグインファイルは、Program Files\CSCOpx\files\vms\repository\ にあります。使用可能なファイルの詳細については、SSL VPN ブラウザ プラグインの設定（ASA） （1787 ページ）を参照してください。

SSL VPN を設定するための前提条件

リモート ユーザが SSL VPN ゲートウェイの背後にあるプライベート ネットワークのリソースに安全にアクセスするには、次の前提条件を満たす必要があります。

- ユーザ アカウント（ログイン名およびパスワード）。
- SSL 対応ブラウザ（Internet Explorer、Netscape、Mozilla、または Firefox など）。
- 電子メール クライアント（Eudora、Microsoft Outlook、または Netscape Mail など）。
- 次のいずれかのオペレーティング システム。
  - Microsoft Windows 2000 または Windows XP。Windows 用の JRE バージョン 1.4 以降、または ActiveX コントロールをサポートするブラウザのいずれかを搭載。
  - Linux。Linux 用の JRE バージョン 1.4 以降を搭載。クライアントレス リモート アクセス モードで Linux から Microsoft の共有ファイルにアクセスするには、Samba のインストールも必要です。

関連項目

- SSL VPN アクセスのモード （1659 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（1672 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）

SSL VPN の制限

Security Manager の SSL VPN 設定には、次の制限があります。

- SSL VPN ライセンス情報を Security Manager にインポートできない。このため、**vpn sessiondb** および **max-webvpn-session-limit** などの特定のコマンドパラメータを検証できません。
- クライアントレス SSL VPN を使用するには、トポロジ内のデバイスごとに DNS を設定する必要がある。DNS の設定がない場合、デバイスは指定された URL を取得できませんが、IP アドレスで指定された URL だけは取得できます。
- 複数の ASA デバイス間で Connection Profiles ポリシーを共有する場合は、すべてのデバイスが同じアドレス プールを共有することに留意する。ただし、デバイス レベルのオブジェクト オーバーライドを使用して、グローバル定義をデバイスごとの一意なアドレス プールに置き換える場合は除きます。NAT を使用していないデバイスでアドレスが重複しないようにするには、一意なアドレス プールが必要です。
- Cisco Security Manager では、CSM_ で始まる名前（Cisco Security Manager で使用される命名ルール）の SSL VPN のアドレスプールがデバイス設定に含まれる場合、そのプール内のアドレスが SSL VPN ポリシーに設定されたプールと重複するかどうかを検出できない（たとえば、異なる Security Manager インストールでユーザーがプールを設定した場合に発生する可能性があります）。この場合は、展開中にエラーが発生する可能性があります。したがって、Security Manager 内のネットワークまたはホスト オブジェクトと同じ IP アドレス プールを設定し、それを SSL VPN ポリシーの一部として定義することを推奨します。このようにすると、検証が正しく行われるようになります。
- 同じ IP アドレスおよびポート番号を、同じ IOS デバイス上の複数の SSL VPN ゲートウェイで共有できない。このため、重複したゲートウェイがデバイス設定に存在しても、Security Manager のインターフェイスを使用して再定義されなかった場合は、展開エラーが発生する可能性があります。このようなエラーが発生した場合は、別の IP アドレスおよびポート番号を選択して再展開する必要があります。
- SSL VPN ポリシーの一部として AAA 認証またはアカウンティングを定義した場合は、AAA サービスをイネーブルにするために **aaa new-model** コマンドが展開される。SSL VPN ポリシーをあとで削除した場合でも、このコマンドは削除されないことに留意してください。これは、デバイス設定の他の部分で、AAA サービスに **aaa new-model** コマンドが必要な場合があるためです。

（注） また、デバイスには、権限レベルを 15 に指定したローカル ユーザを少なくとも 1 人は定義することを推奨します。この定義により、関連する AAA サーバーを指定しないで **aaa new-model** コマンドを設定した場合でも、デバイスからロックアウトされることがなくなります。

関連項目

- SSL VPN アクセスのモード （1659 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（1672 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）

各リモートアクセスVPNテクノロジーでサポートされるデバイスについて

リモート アクセス VPN には、IKE Version 1（IKEv1; IKE バージョン 1）IPsec、IKE Version 2（IKEv2; IKE バージョン 2）IPsec、SSL の 3 つのタイプがあります。これらのテクノロジーを設定できるデバイスは異なります。一般的に、IOS/PIX 6.3 デバイスと比較して、ASA/PIX 7.0 以降では各 VPN タイプの設定は異なります。

次の表に、基本的なデバイスのサポートについて示します。デバイスを選択すると、デバイス タイプによって表示または設定可能なリモート アクセス ポリシーが決まります。

ヒント　デバイスモデルによっては、VPN 設定をサポートしていない NO-VPN バージョンがあります。したがって、あるタイプの VPN で 3845 モデルがサポートされていても、3845 NOVPN モデルはサポートされません。さらに、Cisco Catalyst 6500 シリーズ ASA サービスモジュール（ソフトウェアリリース 8.5(x) を実行）は、どのタイプの VPN もサポートしていません。

表 *363*：各リモート アクセス テクノロジーでサポートされているデバイス

テクノロジー	サポートされるプラットフォーム
IKE バージョン 1 IPsec	• ASA/PIX 7.0 以降：シングルコンテキスト モードおよびルータ モードで実行している ASA 5500 シリーズおよび PIX 515、515E、525、535（PIX ソフトウェア 7.0 以降（8.0 以降を含む）を搭載）。 • IOS/PIX 6.3：PIX ソフトウェア 6.3 のみを実行している Cisco IOS セキュリティ ルータ（Aggregation Services Router（ASR; アグリゲーション サービス ルータ）を含む）、Catalyst 6500/7600、および PIX ファイアウォール。
IKE バージョン 2 IPsec	ASA ソフトウェア 8.4(x) のみを実行している ASA 5500 シリーズのみ。

テクノロジー	サポートされるプラットフォーム
SSL	• ASA：ソフトウェアバージョン 8.0 以降を実行し、シングルコンテキストモードおよびルータモードで実行中の ASA 5500 シリーズ デバイス。 • IOS：ソフトウェア バージョン 12.4(6)T 以降を実行している Cisco 870、880、890、1800、2800、3700、3800、7200、7301 シリーズ ルータ、およびソフトウェア バージョン 15.0(1)M 以降を実行している Cisco 1900、2900、3900 シリーズ ルータ。880 シリーズ ルータの場合、ソフトウェアの最小バージョンは 12.4(15)XZ です。これは、Security Manager では 12.4(20)T にマッピングされます。 ヒント　SSL VPN 設定をサポートしている PIX のバージョンはありません。

関連項目

- リモート アクセス IPSec VPN について　（1656 ページ）
- リモート アクセス SSL VPN について　（1657 ページ）
- Remote Access VPN Configuration ウィザードの使用　（1671 ページ）
- ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要　（1706 ページ）
- IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要　（1892 ページ）

リモート アクセス VPN ポリシーの概要

次のリストでは、VPN で使用されているテクノロジーに基づいて、リモート アクセス VPN 設定で使用されているさまざまなポリシーの概要を説明します。可能なリモート アクセス VPN タイプは、IKE Version 1（IKEv1; IKE バージョン 1）IPsec、IKE Version 2（IKEv2; IKE バージョン 2）IPsec および SSL です。これらのポリシーの多くは、特定のデバイス タイプにのみ適用されます。その場合は、そのデバイス タイプが示されます。デバイス タイプごとにまとめられたこのリストについては、次の項を参照してください。

- ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要　（1706 ページ）
- IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要　（1892 ページ）

（注）　PIX デバイスでは SSL VPN を設定できません。PIX デバイスでは、リモート アクセス IKEv1 IPsec VPN だけをサポートしています。

（注） ダイナミック アクセス ポリシーなどの特定のリモートアクセス VPN ポリシーで、統合 ACL オブジェクト即座にを作成できます。ただし、即座に統合 ACL オブジェクトを作成すると、Cisco Security Manager にエラーメッセージが表示されます。この問題を解決するには、作成した ACL をセレクタウィンドウで選択し、ポリシーを保存する必要があります。

- **リモート アクセス IKEv1 と IKEv2 IPsec および SSL VPN で使用されているポリシー**：
  - **ASA グループロードバランシング**（ASA/PIX 7.0 以降）：リモート クライアント コンフィギュレーションで、複数のデバイスを同じネットワークに接続してリモート セッションを処理している場合、それらのデバイスでセッション負荷を分担するように設定できます。この機能は、ロード バランシングと呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッショントラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングは、ASA デバイスで開始されたリモート セッションの場合にだけ有効です。詳細については、グループのロードバランシングについて（ASA） （1710 ページ）を参照してください。
  - **接続プロファイル**（ASA/PIX 7.0 以降）：接続プロファイルは、トンネル自体の作成に関連する属性を含む、VPN トンネルの接続ポリシーが格納されたレコードのセットです。接続プロファイルでは、ユーザ指向の属性が含まれる特定の接続のグループ ポリシーを識別します。詳細については、接続プロファイルの設定（ASA、PIX 7.0+）（1713 ページ）を参照してください。
  - **ダイナミックアクセス**（ASA 8.0 以降）：個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザが持つさまざまなロール、および設定とセキュリティレベルが異なるリモートアクセスサイトからのログインなど、複数の変数が影響する可能性があります。Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）により、これらの多くの変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。詳細については、リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）（1827 ページ）を参照してください。
  - **グローバル設定**：リモートアクセス VPN のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネット キー交換）、IKEv2、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、ほとんどの場合、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合、または IKEv2 ネゴシエーションをサポートする場合だけ設定してください。詳細については、VPN グローバル設定 （1517 ページ）を参照してください。
  - **グループポリシー**（ASA/PIX 7.0 以降）：リモートアクセス VPN 接続プロファイルに定義されているユーザグループポリシーを表示できます。このページから、新しい ASA ユーザ グループを指定したり、既存の ASA ユーザ グループを編集したりできま

す。接続プロファイルを作成するときに、デバイスで使用されていないグループ ポリシーを指定した場合、このグループ ポリシーは自動的に [Group Policies] ページに追加されます。接続プロファイルを作成する前に、このポリシーに追加する必要はありません。詳細については、リモート アクセス VPN のグループ ポリシーの設定 （1740 ページ）を参照してください。

- **Public Key Infrastructure**：Public Key Infrastructure（PKI）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用されます。詳細については、Public Key Infrastructure ポリシーについて （1544 ページ）およびリモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定（1552 ページ）を参照してください。

- **リモート アクセス IPsec VPN だけで使用されるポリシー**：
  - **証明書から接続プロファイルへのマップ、ポリシーとルール**（IKEv1 IPSec のみ、ASA/PIX 7.0 以降のみ）：証明書から接続プロファイルへのマップポリシーを使用すると、指定したフィールドに基づいて、ユーザの証明書を権限グループと照合するルールを定義できます。認証を確立するため、証明書の任意のフィールドを使用することも、またはすべての証明書ユーザが権限グループを共有することもできます。グループは、DN ルール、[Organization Unit (OU)] フィールド、IKE ID、またはピア IP アドレスから照合できます。これらの方式のいずれかまたはすべてを使用できます。詳細については、Certificate to Connection Profile Map ポリシーの設定（ASA） （1754 ページ）を参照してください。
  - **IKE プロポーザル**：インターネット キー エクスチェンジ（IKE）は、ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーション プロトコルです。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。IKE プロポーザル ポリシーは、IKE ネゴシエーションのフェーズ 1 の要件を定義するときに使用します。詳細については、IKE プロポーザルの設定 （1488 ページ）を参照してください。
  - **IPsec プロポーザル（ASA/PIX 7.x）**：IPsec プロポーザルは、1 つ以上のクリプト マップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス） （1759 ページ）を参照してください。
  - **IPsec プロポーザル（IOS/PIX 6.x）**：IPsec プロポーザルは、1 つ以上のクリプト マップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設

定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス） （1893 ページ）を参照してください。

- **ハイアベイラビリティ**（IOS/PIX 6.3）：ハイアベイラビリティ（HA）グループを作成すると HA がサポートされます。HA グループは、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを実現する、複数のハブデバイスで構成されます。詳細については、リモートアクセス VPN での高可用性の設定（IOS） （1904 ページ）を参照してください。
- **ユーザーグループ（IOS/PIX 6.x）**：ユーザーグループポリシーには、VPN へのユーザーアクセスおよびVPNの使用を決定する属性を指定します。詳細については、ユーザ グループ ポリシーの設定 （1906 ページ）を参照してください。

- **リモート アクセス IKEv2 IPSec および SSL VPN だけで使用されるポリシー**：
  - **アクセス**（ASA のみ）：アクセス ポリシーには、リモートアクセス SSL または IKEv2 IPsec VPN 接続プロファイルをイネーブルにできるセキュリティアプライアンスのインターフェイス、接続プロファイルで使用するポート、Datagram Transport Layer Security（DTLS）設定、SSL VPN セッションタイムアウト、および最大セッション数を指定します。AnyConnect VPN クライアントまたは AnyConnect Essentials クライアントを使用するかどうかも指定できます。詳細については、SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）を参照してください。
  - **その他の設定**（ASA のみ）：[SSL VPNのその他の設定（SSL VPN Other Settings）] ポリシーは、キャッシング、コンテンツの書き換え、文字エンコード、プロキシとプロキシバイパス定義、ブラウザプラグイン、AnyConnect クライアントのイメージとプロファイル、Kerberos の制約付き委任、およびその他いくつかの高度な設定などを定義します。詳細については、他の SSL VPN 設定の定義（ASA） （1774 ページ）を参照してください。
  - **共有ライセンス**（ASA のみ）：[SSL VPN共有ライセンス（SSL VPN Shared License）] ページを使用して、SSL VPN 共有ライセンスを設定します。詳細については、SSL VPN 共有ライセンスの設定（ASA 8.2+） （1806 ページ）を参照してください。
  - **SSL VPN**（IOS デバイスのみ）：SSL VPN ポリシーテーブルには、SSL VPN の仮想設定を定義するすべてのコンテキストが一覧表示されます。各コンテキストには、ゲートウェイ、ドメインまたは仮想ホスト名、およびユーザ グループ ポリシーが含まれます。詳細については、SSL VPN ポリシーの設定（IOS） （1908 ページ）を参照してください。

リモート アクセス VPN ポリシーの検出

Security Manager を使用すると、ポリシー検出中にリモート アクセス IPSec VPN のポリシー設定をインポートできます。また、ASA デバイス上の SSL VPN ポリシーを検出できます。ただ

し、IOS デバイス上のポリシーは検出できません。リモートアクセス VPN ポリシーを検出するには、デバイスをインベントリに追加するときや、すでにインベントリにあるデバイス上のポリシーを検出するときに、[デバイスの検出（Discover Device）] 設定で [RA VPNポリシー（RA VPN Policies）] オプションを選択します。デバイスの追加やポリシーの検出の詳細については、次の項を参照してください。

- デバイス インベントリへのデバイスの追加 （94 ページ）
- Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）

リモートアクセスVPNネットワークに配置済みのデバイスの設定を検出して、Security Managerでその設定を管理できます。これらの設定は、リモートアクセスVPNポリシーとしてSecurity Manager にインポートされます。リモート アクセス VPN ポリシーの検出は、ライブ デバイスの設定をインポートするか、または設定ファイルをインポートして実行されます。ただし、設定ファイルからは、フラッシュ ストレージ内のファイルを参照する SSL VPN ポリシーを検出できません。したがって、設定ファイルからは SSL VPN を検出しないことを推奨します。

リモート アクセス VPN 内のデバイスのポリシー検出を開始すると、デバイスの設定が分析され、この設定がSecurity Managerポリシーに変換されてデバイスを管理できるようになります。インポートした設定によって一部のポリシーだけが定義される場合、警告が表示されます。追加の設定が必要な場合は、Security Manager インターフェイスの関連するページに移動して、ポリシー定義を完了する必要があります。すでに Security Manager で管理しているデバイスの設定を再検出することもできます。

SSL VPN ポリシーを検出すると、SSL VPN ポリシーで参照される、フラッシュ ストレージに保存されているファイルが Security Manager サーバにコピーされ、Security Manager からポリシーが展開されると、ターゲットデバイスの /csm ディレクトリに格納されます。使用するファイルがフラッシュ ストレージに格納されていても、そのファイルが SSL VPN ポリシーから参照されていない場合は、ファイルを参照するコマンドを設定するか、または Security Manager サーバにファイルを手動でコピーします。デバイスの SSL VPN ポリシーが、フラッシュから削除されたファイルを参照している場合、ポリシーの検出は失敗します。失敗した場合、デバイス検出の前に設定を直接修正するか、またはデバイスを追加するときに [RA VPNポリシー（RA VPN Policies）] オプションの選択を解除して、Cisco Security Manager で適切な SSL VPN 設定を作成します。

ヒント

- デバイスでポリシーを検出したら、ポリシーを変更する前またはデバイスからポリシーの割り当てを解除する前に、ただちに展開を実行する必要があります。すぐに展開を実行しないと、Security Manager で設定した変更が、デバイスに展開されない場合があります。
- ASA および PIX 7.0 以降のデバイスでは、デフォルトの接続プロファイルとグループ ポリシーが検出され、[Connection Profiles] と [Group Policies] ポリシーに追加されます。これらのデフォルト プロファイルとグループは変更できますが、削除はできません。
  - DefaultRAGroup：リモート アクセス IPsec VPN のデフォルトの接続プロファイル。
  - DefaultWEBVPNGroup：SSL VPN のデフォルトの接続プロファイル。この接続プロファイルは、ASA 8.0+ デバイスだけで検出されます。

- DfltGrpPolicy：デフォルトのグループ ポリシーです。デフォルトの接続プロファイルで使用されます。検出されると、Cisco Security Manager では <device_display_name> DfltGrpPolicy という名前が使用されます。ただし、設定を展開すると、デバイスの表示名は削除され、DfltGrpPolicy が使用されます。

グループ ポリシーは共有ポリシー オブジェクトとしてモデル化され、デフォルトグループ ポリシーをデバイス上で変更している可能性があるため、この命名ルールは必要です。ただし、この命名ルールにより、デフォルトのグループポリシーが組み込まれている共有ポリシーが使用できなくなることはありません。デバイス表示名は、割り当てられているデバイスにかかわらず、オブジェクト名から削除されます。たとえば、デバイス 10.200.11.1 でオブジェクト 10.100.10.1DfltGrpPolicy を使用する場合、Cisco Security Manager は設定内で引き続き「DfltGrpPolicy」を使用します。

重要 共有ポリシーを接続プロファイルやグループポリシーに割り当てる場合は、デフォルトのグループポリシーに複数エントリが存在しないように、最初に接続プロファイルに割り当て、次にグループポリシーに割り当てます。

（注） これらのデフォルト接続プロファイルでは、SSL VPN ポータル カスタマイゼーションに DfltCustomization オブジェクトを使用しますが、Security Manager では検出されません。DfltCustomization を変更するには、デバイス上で直接変更する必要があります。ただし、単にカスタマイゼーション オブジェクトを作成して、そのオブジェクトをデフォルト接続プロファイルに指定し、デフォルト以外の設定を使用できます。

関連項目

- ポリシーの検出 （223 ページ）
- サイト間 VPN ディスカバリ （1406 ページ）
- VPN ディスカバリ ルール （1408 ページ）

Remote Access VPN Configuration ウィザードの使用

Remote Access VPN Configuration ウィザードを使用して、基本的な IPsec または SSL VPN の設定に必要なポリシーを作成できます。このウィザードで示される簡単なオプションを使用して、基本の項目を設定できます。したがって、ウィザードを使用したあとに、個別のリモートアクセス VPN ポリシーで、追加の設定を行う必要が生じることがあります。

ヒント このウィザードでは有効な IKEv2 IPSec VPN は作成されません。IKEv2 設定を完了するには、常に追加のポリシーを設定する必要があります。

（注） リモートアクセス VPN マルチコンテキストモードの場合、ソフトウェアバージョン 9.5(2) 以降を実行している ASA デバイスでは、リモートアクセス SSL VPN のみがサポートされます。

このウィザードには、デバイス タイプおよび VPN タイプ（IPSec または SSL）に応じて、基本的なリモート アクセス VPN を設定する手順が示されます。

Remote Access Configuration ウィザードにアクセスするには、次の手順を実行します。

1. デバイス ビューで、リモート アクセス サーバとして設定するデバイスをデバイス セレクタから選択します。
2. ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [構成ウィザード（Configuration Wizard）] を選択します。
3. 作成するリモートアクセス VPN のタイプに対応するオプションボタン（[リモートアクセスSSL VPN（Remote Access SSL VPN）] または [リモートアクセスIPSec VPN（Remote Access IPSec VPN）]）を選択します。
4. [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックして、適切なウィザードを開きます。

ウィザードの各バージョンの使用方法については、次の項を参照してください。

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（1672 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （1703 ページ）

Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）

ここでは、Remote Access SSL VPN Configuration ウィザードを使用して、ASA デバイスで SSL VPN を作成または編集する方法について説明します。

関連項目

- リモート アクセス SSL VPN について （1657 ページ）
- 各リモートアクセスVPNテクノロジーでサポートされるデバイスについて （1665ページ）

ステップ 1 デバイス ビューで、目的の ASA デバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）]>[構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセスSSL VPN（Remote Access SSL VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[Access] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Access] ページ（ASA） （1675 ページ）を参照してください。

ステップ 5 SSL VPN 接続をイネーブルにするインターフェイスを指定します。[選択（Select）] をクリックして、インターフェイス、またはインターフェイスを識別するインターフェイス ロール オブジェクトを選択します。

ステップ 6 SSL VPN セッションに使用するポート番号を指定します。ポート番号を入力するか、番号を定義するポートリストオブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。

HTTPS トラフィックの場合、デフォルト ポートは 443 です。ポート番号は 443 にすることも、1024 ～ 65535 の範囲で指定することもできます。ポート番号を変更すると、現在の SSL VPN 接続がすべて終了するため、現在のユーザは再接続が必要になります。

（注） HTTP ポート リダイレクションがイネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。

ステップ 7 ログイン時に、ユーザーがデバイスに設定されたトンネルグループ接続プロファイルのリストからトンネルグループを選択できるようにするには、[ユーザーにポータルページでの接続プロファイルの選択を許可する（Allow Users to Select Connection Profile in Portal Page)] オプションを選択します。

ステップ 8 ユーザーが AnyConnect VPN クライアントを使用して SSL VPN に接続できるようにするには、[AnyConnect アクセスの有効化（Enable AnyConnect Access）] チェックボックスをオンにします。

ステップ 9 [次へ（Next）] をクリックします。[Connection Profile] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Connection Profile] ページ（ASA） （1676 ページ）を参照してください。

ステップ 10 [接続プロファイル名（Connection Profile Name）] で、接続プロファイルの名前を入力します。これはトンネル グループの名前であり、[Remote Access VPN] > [Connection Profiles] ポリシーに表示されます。Connection Profile ポリシーの詳細については、接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照してください。

ステップ 11 [Connection Profile] ページで、あとで接続プロファイルの [General] タブに表示されるこれらのオプションを設定します（[General] タブ（[Connection Profiles]） （1718 ページ）を参照）。

- [グループポリシー（Group Policy）]：接続プロファイルのデフォルトグループになる [ASAグループポリシー（ASA Group Policy）] ポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合、[選択（Select）] をクリックしてから、[ASAユーザーグループセレクタ（ASA User Groups Selector）] ダイアログボックスで [作成（Create）]（+）ボタンをクリックすると、作成プロセスを実行できるウィザードが開きます（Create Group Policy ウィザードによるユーザ グループの作成 （1680 ページ）の説明を参照）。

ASA グループ ポリシー オブジェクトの詳細については、[ASA Group Policies] ダイアログボックス （1918 ページ）を参照してください。

- [グループポリシー（Group Policies）]：このテーブルには、SSL または IPsec VPN に関係なく、現在デバイスで使用されているすべてのグループポリシーが一覧表示されます。[編集（Edit）] をクリックすると、他のグループポリシーを追加できます。
- [グローバルIPアドレスプール（Global IP Address Pool）]：IP アドレスが割り当てられるアドレスプールを入力します。サーバはこれらのアドレス プールをリスト内の順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。

アドレスの範囲またはアドレスの範囲が含まれるネットワークまたはホストオブジェクトとして、Start_Address -End_Address の形式でプールを指定します（例：10.100.10.2-10.100.10.254）。[選択（Select）] をクリックして、ネットワークまたはホストオブジェクトを選択するか、または新しいオブジェクトを作成します。

ステップ 12 [Connection Profile] ページで、あとで接続プロファイルの [SSL VPN] タブに表示されるこれらのオプションを設定します（ [SSL] タブ（[Connection Profiles]） （1734 ページ）を参照）。

- [ポータルページカスタマイゼーション（Portal Page Customization）]：VPN のデフォルトのポータル ページを定義する SSL VPN カスタマイゼーション ポリシー オブジェクトの名前。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。

（注） カスタマイゼーションプロファイルとトンネル グループの組み合わせを使用することで、個々のグループにそれぞれ異なるログイン ウィンドウを設定できます。たとえば、salesgui という名前のカスタマイゼーションプロファイルを作成済みである場合、そのカスタマイゼーションプロファイルを使用する sales という名前の SSL VPN トンネル グループを作成できます。

- [接続URL（Connection URL）]：接続プロファイルの URL。ユーザは、この URL を使用して、カスタマイズ済みのポータル ページにダイレクト アクセスできます。リストからプロトコル（[http] または [https]）を選択し、表示されたフィールドで、接続プロファイルの名前が含まれている URL を指定します。

URL は、ASA デバイスのホスト名または IP アドレス、ポート番号、および SSL VPN 接続プロファイルを識別するためのエイリアスで構成されています。

（注） URL を指定しない場合は、ポータル ページの URL を入力し、デバイスに設定されている設定済みの接続プロファイルエイリアス リストから接続プロファイルエイリアスを選択することによって、ポータル ページにアクセスできます。 SSL VPN Configuration ウィザード：[Access] ページ（ASA） （1675 ページ）を参照してください。

ステップ 13 [Connection Profile] ページで、認証、許可、アカウンティングおよびセカンダリ認証の AAA オプションを設定します。このオプションはあとで接続プロファイルの [AAA] タブおよび [Secondary AAA] タブに表示されます（ [AAA] タブ（[Connection Profiles]） （1721 ページ）および [Secondary AAA] タブ（[Connection Profiles]） （1727 ページ）を参照）。

ステップ 14 [終了（Finish）] をクリックして変更を保存します。

SSL VPN Configuration ウィザード：[Access] ページ（ASA）

SSL VPN Configuration ウィザードの [Access] ページを使用して、SSL VPN セッションのセキュリティ アプライアンス インターフェイスを設定します。ウィザードを完了したら、後で SSL VPN アクセスポリシーで設定を編集できます。[SSL VPN Access Policy] ページ （1766 ページ）を参照してください。

ナビゲーション パス

（デバイス ビュー）ASA デバイスでリモート アクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照）。最初に表示されるページは [Access] ページです。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（1672 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *364 : SSL VPN* ウィザード：*[Access]* ページ（*ASA*）

要素	説明
Interfaces to Enable SSL VPN Service	SSL VPN 接続をイネーブルにするインターフェイス、またはインターフェイスを識別するインターフェイス ロール。[選択（Select）] をクリックして、インターフェイスまたはインターフェイスロールを選択するか、または新しいインターフェイスロールを作成します。
ポート番号（Port Number）	SSL VPN セッションに使用するポート番号。ポート番号またはポートリストオブジェクト名を入力します。または、[選択（Select）] をクリックしてポート定義するオブジェクトを選択するか、または新しいオブジェクトを作成します。 HTTPS トラフィックの場合、デフォルト ポートは 443 です。ポート番号は 443 にすることも、1024 ～ 65535 の範囲で指定することもできます。ポート番号を変更すると、現在の SSL VPN 接続がすべて終了するため、現在のユーザは再接続が必要になります。 （注） HTTP ポート リダイレクションがイネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。
Portal Page URLs	VPN に接続するためにユーザが使用する URL。インターフェイスとポート番号を指定すると、URL が表示されます。

要素	説明
Allow Users to Select Connection Profile in Portal Page	ログイン時（たとえば、SSL VPN ポータル ページ）にユーザが適切なプロファイルを選択するときに使用できる設定済み接続プロファイル（トンネル グループ）のリストを提供するかどうかを指定します。このオプションを選択しない場合、ユーザはプロファイルを選択できず、接続にはデフォルト プロファイルを使用する必要があります。
Enable AnyConnect Access	ユーザが AnyConnect VPN クライアントを使用して SSL または IKEv2 IPSec VPN 接続を確立できるようにするかどうかを指定します。このオプションは、デフォルトでオンになっています。AnyConnect VPN クライアントの詳細については、 SSL VPN AnyConnect クライアント設定について （1789 ページ）を参照してください。 （注） AnyConnect Essentials をイネーブルにするには、[Remote Access VPN] > [SSL VPN] > [Access] を選択します。詳細については、Access ポリシーの設定 （1772 ページ） を参照してください。

SSL VPN Configuration ウィザード：[Connection Profile] ページ（ASA）

SSL VPN Configuration ウィザードの [Connection Profile] ページを使用して、セキュリティ アプライアンスでトンネル グループ ポリシーを設定します。追加するトンネル接続プロファイル ポリシーの名前を指定し、ユーザ グループ ポリシーを選択できます。また、このポリシーのアドレス プールを指定し、認証サーバ グループ設定を指定できます。

ナビゲーション パス

（デバイスビュー）ASA デバイスでリモートアクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（ Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照）。次に、このページが表示されるまで [次へ（Next）] をクリックします。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（1672 ページ）
- [ASA Group Policies] ダイアログボックス （1918 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

フィールド リファレンス

表 *365 : SSL VPN Configuration* ウィザード、*[Connection Profile]* ページ（*ASA*）

要素	説明
Connection Profile Name	接続プロファイルの名前（トンネル グループ）。
[グループ ポリシー（Group Policy）]	デバイスに関連付けられているデフォルトの ASA ユーザ グループ。ASA ユーザーグループポリシーを入力します。または、[選択（Select）] をクリックしてリストからポリシーを選択するか、新しいポリシーを作成します。 必要な場合、接続プロファイルに関連付けられているデフォルトユーザ グループを定義する ASA グループ ポリシー オブジェクトの名前。グループポリシーはユーザ指向の属性と値のペアの集合であり、デバイスで内部的に、または RADIUS/LDAP サーバで外部的に格納されます。 [選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。グループポリシーの選択ダイアログボックスで [作成（Create）]（+）ボタンをクリックすると、Create Group Policy ウィザードによるユーザ グループの作成 （1680 ページ）に説明されているように、ウィザードを使用してグループ作成手順を実行できます。
Full Tunnel	[Group Policy] フィールドで選択されているオブジェクトにフル トンネル アクセス モードが設定されているかどうかを示す読み取り専用フィールド。
グループ ポリシー	デバイスに設定されているすべての ASA ユーザ グループ ポリシーの名前（IPSec VPN 接続にのみ設定されているポリシーも含む）。このテーブルの内容は、[Remote Access VPN] > [Group Policies] ポリシーの内容と同じです。テーブルには、グループ ポリシーごとにフル トンネル アクセス モードがイネーブルかディセーブルかが示されます。 [編集（Edit）] をクリックして、リストを変更できます。[Edit] をクリックすると、ダイアログボックスが開きます。このダイアログボックスでは、追加のグループポリシーを選択したり、現在選択されているポリシーの選択を解除したりできます（他の接続プロファイルで使用されているポリシーの選択は解除しないでください）。また、新しいグループポリシーを作成したり（使用可能なグループポリシーリストの下にある [作成（Create）]（+）ボタンをクリック）、グループ ポリシー オブジェクトを選択してから、いずれかのリストの下にある [編集（Edit）]（鉛筆）ボタンをクリックして、グループポリシーを編集したりできます。 新しいグループ ポリシーを作成する場合、[Create Group Policy] ウィザードを使用して手順を実行できます。Create Group Policy ウィザードによるユーザ グループの作成 （1680 ページ）を参照してください。

要素	説明
Portal Page Customization	VPN のデフォルト ポータル ページを定義する [SSL VPN Customization] ポリシー オブジェクトの名前。このプロファイルでは、リモート ユーザが SSL VPN 上で使用可能なすべてのリソースにアクセスできるようにするためのポータル ページの外観を定義します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。
Connection URL	接続プロファイルの URL。ユーザは、この URL を使用して、カスタマイズ済みのポータル ページにダイレクト アクセスできます。 リストからプロトコル（[http] または [https]）を選択し、URL を指定します。URL には、ASA デバイスのホスト名または IP アドレス、ポート番号、および SSL VPN 接続プロファイルの識別に使用するエイリアスを含めます。 （注） URL を指定しない場合は、ポータル ページの URL を入力し、デバイスに設定されている設定済みの接続プロファイル エイリアス リストから接続プロファイル エイリアスを選択することによって、ポータル ページにアクセスできます。SSL VPN Configuration ウィザード：[Access] ページ（ASA） （1675 ページ）を参照してください。
[グローバル IPv4 アドレスプール（Global IPv4 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv4 アドレスをクライアントに割り当てるために使用されるアドレスプール。アドレス プールは、アドレスの範囲として入力します（10.100.12.2-10.100.12.254 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレス プール範囲を入力するか、これらのプールを定義するネットワークまたはホスト オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
[グローバル IPv6 アドレスプール（Global IPv6 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv6 アドレスをクライアントに割り当てるために使用されるアドレスプール。アドレスプールは、アドレスの範囲として入力します（2001:db8::1-2001:db8::2:1 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。。 アドレス プール範囲を入力するか、これらのプールを定義するネットワークまたはホスト オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
Authentication Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合はLOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Authorization Server Group	認可サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合はLOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Accounting Server Group	アカウンティング サーバ グループの名前。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

要素	説明
Secondary Authentication	リモートアクセスVPN接続を完了する前に、ユーザに2つのクレデンシャルセット（ユーザ名とパスワード）を要求する二重認証をイネーブルにするかどうか。 • [セカンダリ認証を有効化（Enable Secondary Authentication）]：二重認証を要求するには、このオプションを選択します。 • [認証サーバーグループ（Authentication Server Group）]：2 番めのクレデンシャルセットで使用する認証サーバーグループの名前（トンネルグループがローカルデバイスに設定されている場合はLOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 • [サーバーグループに障害が発生した場合はローカルを使用（Use LOCAL if Server Group Fails）]：選択した認証サーバーグループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。

Create Group Policy ウィザードによるユーザ グループの作成

Remote Access SSL VPN Configuration ウィザードを使用して、ASA または IOS デバイス上で SSL VPN を作成する場合、ウィザードを使用して、新しい ASA グループ ポリシーまたは IOS ユーザ グループ オブジェクトを作成できます。このウィザードを使用すると、グループの選択要素を設定できるため、オブジェクトを作成したあとに、そのオブジェクトを編集して追加の設定を行う必要が生じる場合があります。

Create Group Policy ウィザードは、Remote Access SSL VPN Configuration ウィザードからのみ使用できます。このウィザードの起動および使用方法については、次の項を参照してください。

次の手順では、次の項の説明に従って、すでに Remote Access SSL VPN Configuration ウィザードを実行していることを前提とします。

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス）（1672 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）

関連項目

- SSL VPN アクセスのモード （1659 ページ）

ステップ 1 SSL VPN に Remote Access VPN Configuration ウィザードを使用する場合、グループ ポリシーを選択するページに進みます。このページでは、次のようにしてユーザ グループの選択ページを開くことができます。

- ASA デバイス：ウィザードの [接続プロファイル（Connection Profile）] ページで、[グループポリシー（Group Policy）] フィールドの隣にある [選択（Select）] をクリックします。または、[グループポリシー（Group Policies）] テーブルの隣にある [編集（Edit）] をクリックします。
- IOS デバイス：ウィザードの [ゲートウェイとコンテキスト（Gateway and Context）] ページで、[グループポリシー（Group Policies）] テーブルの隣にある [編集（Edit）] をクリックします。

ステップ 2 [グループポリシーセレクタ（Group Policy Selector）] ダイアログボックスで、使用可能なグループポリシーのリストの下にある [作成（Create）]（+）ボタンをクリックして、Create Group Policy ウィザードを起動します。このウィザードは、[Group Policy] ページから始まります。

グループ ポリシー セレクタでは、次の項目も実行できます。

- 既存のグループを選択して [>>] をクリックし、グループを SSL VPN で使用する。ASA のデフォルト グループ用にグループを選択する場合は（[Group Policy] フィールド）、単にそのオブジェクトをリストからクリックします。
- 既存のグループを選択して [編集（Edit）]（鉛筆）をクリックし、既存のグループのプロパティを変更する。

ステップ 3 [Group Policy] ページで、次のオプションを設定します。

- [名前（Name）]：ユーザーグループの名前。最大 128 文字を入力します。大文字、小文字、およびほとんどの英数字または記号を使用できます。
- [アクセス方式（Access Method）]：目的のリモートアクセス方式オプションを、次から選択します。
  - [フルトンネル（Full Tunnel）]：SSL VPN トンネルを介して企業ネットワークにフルアクセスします。これは推奨オプションです。
  - [クライアントレス（Clientless）]：クライアントマシンで Web ブラウザを使用して内部ネットワーク、または企業ネットワークにアクセスします。
  - [シンクライアント（Thin Client）]：クライアントマシンで TCP プロキシとして機能する Java アプレットをダウンロードします。

ステップ 4 [次へ（Next）] をクリックします。次に開くページは、選択したアクセス方式によって異なります。この手順では、すべての方式を選択したと想定します。この場合は、[Full Client] ページが開きます。

ステップ 5 [Full Client] ページで、フル トンネルのみにアクセスを制限するか、またはフル クライアントのダウンロードに失敗した場合、他のアクセス方式を許可するかどうかを選択します。また、DNS および WINS サーバ情報を指定し、スプリット トンネリングを許可する場合は設定します。オプションの説明については、Create Group Policy ウィザード：[Full Tunnel] ページ （1682 ページ）を参照してください。

ステップ 6 [次へ（Next）] をクリックします。[Clientless and Thin Client] ページが開きます。

ステップ 7 [Clientless and Thin Client] ページで、これらのアクセス モードを設定します。オプションの説明については、Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ （1686 ページ）を参照してください。

ステップ 8 [終了（Finish）] をクリックして、グループ ポリシー オブジェクトを作成します。

ステップ 9 ウィザードを完了すると、使用可能なグループリストにグループポリシーが追加されますが、（設定してるグループがASAのデフォルトグループではない限り）そのグループは選択されていません。グループを選択するには、使用可能なグループリストで強調表示して、[>>] をクリックし、そのグループを選択したグループリストに移動します。

（注） ユーザーグループをデフォルトユーザーグループとして指定するには、ユーザーグループを選択し、[デフォルトとして設定（Set As Default）] をクリックします。このオプションは、IOSルータの場合にのみ使用可能です。

ステップ 10 [グループポリシーセレクタ（Group Policy Selector）] ページで [OK] をクリックして変更を保存し、Remote Access SSL VPN Configuration ウィザードに戻ります。

Create Group Policy ウィザード：[Full Tunnel] ページ

（注） このページは、Create Group Policy ウィザードの [グループポリシー（Group Policy）] で [フルクライアント（Full Client）] オプションを選択した場合にのみ使用可能です。

このページでは、企業ネットワークへのアクセスに使用するモードを設定できます。

ナビゲーション パス

Create Group Policy ウィザードの開始については、Create Group Policy ウィザードによるユーザグループの作成 （1680 ページ）を参照してください。

フィールド リファレンス

表 *366 : Create User Group* ウィザード：*[Full Tunnel]* ページ

要素	説明
[モード（Mode）]	SSL VPN で許可するアクセス モード。次のいずれかを選択します。 • [SSL VPN クライアントのダウンロードに失敗した場合に他のアクセスモードを使用する（Use Other Access Modes if SSL VPN Client Download Fails）]：VPN クライアントのダウンロードに失敗した場合に、リモートクライアントでクライアントレス アクセス モードまたはシン クライアント アクセス モードの使用を許可します。 • [フルトンネルのみ（Full Tunnel Only）]：クライアントレスまたはシンクライアントアクセスを禁止します。ユーザは、フル クライアントをインストールし、VPN への接続に使用できるようにしておく必要があります。 デバイス上でフル クライアント イメージを必ず設定してください。ASA デバイスでは、SSL VPN の [Client Settings] タブ > [Other Settings] ポリシーを使用します。SSL VPN AnyConnect クライアント設定の定義（ASA）（1792 ページ）を参照してください。IOS デバイスでは、クライアントは [FlexConfig] ポリシーを使用して管理されます。定義済みの FlexConfig ポリシー オブジェクト （454 ページ）を参照してください。
Client IP Address Pools （IOS デバイスのみ）	フル トンネル クライアントがログインしたときに取得するアドレス プールの IP アドレス範囲。このアドレスプールは、デバイスのインターフェイス IP アドレスのいずれかと同じサブネットに存在する必要があります。 アドレス範囲を指定する場合は、最初と最後の IP アドレスをハイフンで区切って入力します。たとえば、10.100.10.2-10.100.10.255 です。1 つのアドレスを入力した場合、プールには 1 つのアドレスだけが含まれます。サブネット指定は入力しないでください。 範囲を定義するネットワーク/ホストポリシーオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成することもできます。複数の範囲を指定する場合は、カンマで区切ります。
プライマリ IPv4 DNS サーバー	グループのプライマリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
セカンダリ IPv4 DNS サーバー	グループのセカンダリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
プライマリ IPv6 DNS サーバー	グループのプライマリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
セカンダリ IPv6 DNS サーバー	グループのセカンダリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
デフォルト DNS ドメイン	フルクライアント SSL VPN 接続に使用される DNS サーバのドメイン名。
プライマリ WINS サーバ（Primary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
セカンダリ WINS サーバ（Secondary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
Split Tunnel Option	IPv4 トラフィックのスプリットトンネリングを許可するかどうかを指定し、許可する場合は、保護するトラフィック、または暗号化されずにパブリックネットワークを介して送信するトラフィックを指定します。 • [無効（Disabled）]（デフォルト）：IPv4 トラフィックは、暗号化されずに送信されることがないか、またはゲートウェイ以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカルネットワークにはアクセスできません。 • [指定されたトラフィックをトンネル化（Tunnel Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過するすべての IPv4 トラフィックをトンネル化します。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。 • [指定されたトラフィックを除外（Exclude Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過する IPv4 トラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。

要素	説明
[IPv6 スプリットトンネルオプション（IPv6 Split Tunnel Option）]	IPv6 トラフィックのスプリットトンネリングを許可するかどうかを指定し、許可する場合は、保護するトラフィック、または暗号化されずにパブリックネットワークを介して送信するトラフィックを指定します。 • [無効（Disabled）]（デフォルト）：IPv6 トラフィックは、暗号化されずに送信されることがないか、またはゲートウェイ以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカルネットワークにはアクセスできません。 • [指定されたトラフィックをトンネル化（Tunnel Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過するすべてのトラフィックをトンネル化します。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。 • [指定されたトラフィックを除外（Exclude Specified Traffic）]：[ネットワーク（Networks）] または [宛先（Destinations）] フィールドに一覧表示されているアドレスを通過するトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。
ネットワーク （ASA デバイスのみ）	[Split Tunnel Option] で [Tunnel Specified Traffic] または [Exclude Specified] トラフィックを選択する場合、トンネルを通過するトラフィックまたは除外されるトラフィックを定義する ACL オブジェクトの名前を入力します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。
宛先 （IOS デバイスのみ）	[Split Tunnel Option] で [Tunnel Specified Traffic] または [Exclude Specified] トラフィックを選択する場合、トンネルを通過するトラフィックまたは除外されるトラフィックを定義する IP アドレスを指定します。 10.100.10.0/24 などのネットワーク アドレスまたは 10.100.10.12 などのホストアドレスを入力します。ネットワーク/ホストポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成することもできます。カンマで複数のアドレスを区切ります。

要素	説明
Exclude Local LANs （IOS デバイスのみ）	ローカル LAN を暗号化されたトンネルから除外するかどうかを指定します。このオプションは、[指定されたトラフィックを除外（Exclude Specified Traffic）] スプリット トンネル オプションを選択している場合にのみ選択できます。このオプションを選択すると、LAN に接続しているシステム（プリンタなど）との通信をユーザに許可するために、ローカル LAN アドレスを宛先フィールドに入力する必要がなくなります。 選択した場合、この属性によって、クライアントと同時にローカル サブネットワークにアクセスする非スプリット トンネリング接続が許可されなくなります。
Split DNS Names	スプリット トンネルを介してプライベート ネットワークに解決されるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを使用して解決されます。 ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ

Create Group Policy ウィザードの [Clientless and Thin Client] ページで、SSL VPN で企業ネットワークにアクセスするために使用する [Clientless] モードおよび [Thin Client] クライアント モードを設定できます。

（注） このページは、Create Group Policy ウィザードの手順 1 で [クライアントレス（Clientless）] オプションまたは [シンクライアント（Thin Client）] オプションを選択した場合にのみ表示されます。

ナビゲーション パス

Create Group Policy ウィザードの開始については、Create Group Policy ウィザードによるユーザ グループの作成 （1680 ページ）を参照してください。

関連項目

- SSL VPN アクセスのモード （1659 ページ）
- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）
- [Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス （1977 ページ）

フィールド リファレンス

表 *367 : Create User Group* ウィザード：*[Clientless and Thin Client]* ページ

要素	説明
[クライアントレス（Clientless）]：ウィザードの手順 1 で [クライアントレス（Clientless）] を選択した場合にのみ表示されます。	
Portal Page Websites	ポータル ページ上に表示する Web サイト URL が含まれる SSL VPN ブックマーク ポリシー オブジェクトの名前。これらの Web サイトを使用すると、ユーザは目的のリソースにアクセスできます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Allow Users to Enter Websites	ブラウザへの Web サイト URL の直接入力をリモート ユーザに許可するかどうかを指定します。このオプションを選択しない場合、ユーザはポータルに表示されている URL だけにアクセスできます。
[シンクライアント（Thin Client）]：ウィザードの手順 1 で [シンクライアント（Thin Client）] を選択した場合にのみ表示されます。	
Port Forwarding List	このグループに割り当てるポート転送リスト ポリシー オブジェクトの名前。ポート転送リストには、クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートを介してアクセスできるアプリケーションのセットが含まれます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Port Forwarding Applet Name （ASA デバイスのみ）	ポータル上の [Port Forwarding Java] アプレット画面に表示されるアプリケーション名または短い説明。最大 64 文字です。これは、ユーザがダウンロードするアプレットの名前です。このアプレットは、SSL VPN ゲートウェイで設定したサービス用の TCP プロキシとしてクライアント マシン上で動作します。
Download Port Forwarding Applet on Client Login	ユーザが SSL VPN にログインしたときに、ポート転送 Java アプレットがクライアントに自動的にダウンロードされるかどうかを指定します。アプレットを自動的にダウンロードしない場合、ユーザがログイン後に手動でダウンロードする必要があります。

Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

ここでは、Remote Access VPN Configuration ウィザードを使用して、ASA または PIX 7.0 以降のデバイスで IPSec VPN を作成する方法について説明します。

ヒント このウィザードの [Defaults] ページ（ウィザードの最後のステップ）では、VPN で使用する共有ポリシーを選択できます。この機能を使用する場合、必要なすべての共有ポリシーがデータベースに設定および送信されていることを最初に確認する必要があります。共有ポリシーと VPN ポリシーのデフォルトの設定については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。

関連項目

- リモート アクセス IPSec VPN について （1656 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （1665 ページ）

ステップ 1 [Device] ビューで、目的の ASA または PIX 7.0 以降のデバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）]>[構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセスIPSec VPN（Remote Access IPSec VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[Connection Profile] ページが開きます。このページに表示されるオプションの説明については、Remote Access VPN Configuration ウィザード：[IPSec VPN Connection Profile] ページ（ASA） （1692 ページ）を参照してください。

ステップ 5 [Connection Profile] ページで、これらの基本オプションを設定します。

- [接続プロファイル名（Connection Profile Name）]：接続プロファイルの名前を入力します。これはトンネル グループの名前であり、[Remote Access VPN] > [Connection Profiles] ポリシーに表示されます。Connection Profile ポリシーの詳細については、接続プロファイルの設定（ASA、PIX 7.0+）（1713 ページ）を参照してください。
- [IKEバージョン（IKE Versions）]：IKE ネゴシエーション中に VPN サーバーとリモートユーザー間で使用する IKE バージョン（バージョン 1、2 または両方）を選択します。IKEv2 は、ASA ソフトウェア リリース 8.4(1)+ だけでサポートされます。

ステップ 6 [Connection Profile] ページで、あとで接続プロファイルの [General] タブに表示されるこれらのオプションを設定します（ [General] タブ（[Connection Profiles]） （1718 ページ）を参照）。

- [グループポリシー（Group Policy）]：接続プロファイルのデフォルトグループになる [ASAグループポリシー（ASA Group Policy）] ポリシーオブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択します。必要なオブジェクトがまだ存在しない場合、[選択（Select）] をクリックしてから、[ASAユーザーグループセレクタ（ASA User Groups Selector）] ダイアログボックスで [作成（Create）]（+）ボタンをクリックすると、これらのオブジェクトを作成するために使用するダイアログボックスが開きます。

新しいグループ ポリシー オブジェクトを作成する場合、ウィザードの [Connection Profile] ページで選択する IKE バージョンと同じバージョンを選択する必要があります。これらのオプションは [Add ASA Group Policies] ダイアログボックスの [Technology] ページにあります。オプションは、[Easy VPN]、[IPSec IKEv1] および [Easy VPN/IPSec IKEv2] です。

ASA グループ ポリシー オブジェクトの詳細については、[ASA Group Policies] ダイアログボックス （1918 ページ）を参照してください。

- [グローバルIPアドレスプール（Global IP Address Pool）]：IP アドレスが割り当てられるアドレスプールを入力します。サーバはこれらのアドレス プールをリスト内の順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。

アドレスの範囲またはアドレスの範囲が含まれるネットワークまたはホストオブジェクトとして、Start_Address -End_Address の形式でプールを指定します（例：10.100.10.2-10.100.10.254）。[選択（Select）] をクリックして、ネットワークまたはホストオブジェクトを選択するか、または新しいオブジェクトを作成します。

ステップ 7 [Connection Profile] ページで、認証、許可、アカウンティングの AAA オプションを設定します。このオプションはあとで接続プロファイルの [AAA] タブに表示されます（ [AAA] タブ（[Connection Profiles]） （1721 ページ）を参照）。

ステップ 8 [次へ（Next）] をクリックして、[IPsec設定（IPsec Settings）] ページに移動します。

ステップ 9 [IPSec Settings] ページで、IPSec のオプションを設定します。このオプションはあとで接続プロファイルの [IPSec] タブに表示されます（ [IPSec] タブ（[Connection Profiles]） （1730 ページ）を参照）。これらの設定の一部は IKEv1 にのみ適用されます。

- [事前共有キー（Preshared Key）]、[確認（Confirm）]：各フィールドに、トンネルグループの IKEv1 事前共有キーを入力します。事前共有キーの最大長は 127 文字です。

リモート アクセス IKEv2 IPsec VPN に事前共有キーは設定できません。

- [トラストポイント名（Trustpoint Name）]：トラストポイントが設定されている場合、IKEv1 接続用のトラストポイント名を定義する PKI 登録ポリシーオブジェクトの名前を入力します。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

IKEv2 の場合、トラストポイント名はここではなく、[Global Settings] ポリシーの [IKEv2 Settings] タブで設定します。設定は、この手順の後半で説明されています。

- 他のオプション（クライアント テーブル以外）は IKEv1 と IKEv2 の両方に適用されます。デフォルト以外の動作が必要な場合は、設定を変更します。クライアント ソフトウェアの更新テーブルなどのオプションの説明については、Remote Access VPN Configuration ウィザード：[IPSec Settings] ページ（ASA） （1694 ページ）を参照してください。

ステップ 10 [次へ（Next）] をクリックして、[VPNデフォルト（VPN Defaults）] ページに移動します。

ステップ 11 [Defaults] ページで、VPN に割り当てる追加の共有ポリシーを選択します。最初から一覧表示されているポリシーは、[Security Manager Administration] の [VPN Defaults] ページで選択されているポリシーです。

これらのポリシーの選択については、Remote Access VPN Configuration ウィザード：[Defaults] ページ（1695 ページ）を参照してください。

ステップ 12 [終了（Finish）] をクリックして変更を保存します。

ウィザードでは、設定可能なすべてのオプションを設定するわけではないため、作成したポリシーを調べて、実装するオプションを追加で設定します。

サポート対象 IKE バージョンとして IKE バージョン 2 を選択した場合や IPsec トラストポイントを指定した場合、これ以降の手順は必須です。

ステップ 13 （IKEv2 で任意）必要に応じて、グループエイリアスと二重認証を設定します。

a) [Connection Profiles] ポリシーを選択します。

b) ウィザードで設定した接続プロファイルを選択して、[行の編集（Edit Row）]（鉛筆）ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。

- 二重認証を設定する場合は、[Secondary AAA] タブを選択して、必要な値を設定します。詳細については、[Secondary AAA] タブ（[Connection Profiles]） （1727 ページ）を参照してください。
- ログイン中にユーザが正しいプロファイルを選択できるようにするため、プロファイルにエイリアスを設定する場合、[SSL] タブを選択して、エイリアステーブルを設定します。詳細については、[SSL] タブ（[Connection Profiles]） （1734 ページ）を参照してください。
- ウィザードでは設定されない追加の接続プロファイル設定がいくつかあります。[Connection Profile] ダイアログボックスのタブを調べて、追加の変更が必要かどうかを決定します。

c) [接続プロファイル（Connection Profiles）] ダイアログボックスで [OK] をクリックして、変更を保存します。

ステップ 14 （IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（Access）] ポリシーを選択して、少なくとも次の項目を設定します。[Access] ポリシーの設定については、SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）を参照してください。

- リモート アクセス VPN インターフェイスをアクセス インターフェイス テーブルに追加します。
- [ユーザーにポータルページでの接続プロファイルの選択を許可する（Allow Users to Select Connection Profile in Portal Page）] を選択します。
- [Anyconnectアクセスを有効化（Enable AnyConnect Access）] を選択します。

ステップ 15 （IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシーを選択して、[クライアント設定（Client Settings）] タブをクリックします。

[AnyConnectクライアントイメージ（AnyConnect Client Image）] テーブルで、IKEv2 ネゴシエーションをサポートしている AnyConnect 3.0 以降のクライアントイメージを追加します。

クライアントイメージの設定については、VPN グローバル IKEv2 設定 （1526 ページ）を参照してください。

ステップ 16 （IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [グローバル設定（Global Settings）] ポリシーを選択して、[IKEv2設定（IKEv2 Settings）] タブをクリックします。

少なくとも、リモートアクセス IKEv2 認証用に [RA トラストポイント（RA Trustpoint）] を設定します。認証局（CA）サーバーを識別する PKI 登録オブジェクトの名前を入力するか、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。

IKEv2 グローバル設定については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス） （1761 ページ）を参照してください。

ステップ 17 （IKEv1、IKEv2 で必須）[リモートアクセスVPN（Remote Access VPN）] > [公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーを選択して、次の PKI 登録オブジェクトが選択されていることを確認します。

- （IKEv1）トラストポイントが設定されている場合、接続プロファイルの [IPSec] タブで指定したオブジェクト。
- （IKEv2）[Global Settings] ポリシーの [IKEv2 Settings] タブで指定したオブジェクト。

（注） これらのオブジェクトをすでに指定している共有の [Public Key Infrastructure] ポリシーは、ウィザードによって適用されている場合もあります。

ステップ 18 （IKEv2 で任意）IKEv2 接続には、AnyConnect 3.0 以降のクライアントを使用する必要があります。AnyConnect クライアントでは、場合によっては、ソフトウェアアップグレード、プロファイル、ローカリゼーションファイルおよびカスタマイゼーションファイル、CSD、SCEP などのファイルをダウンロードする必要があります。ウィザードでは、これらのタイプのダウンロードがイネーブルにされません。

AnyConnect でファイルのダウンロードをイネーブルにする手順は次のとおりです。

a) [リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPSecプロポーザル（IPSec Proposal）] を選択します。
b) ウィザードで作成された IPSec プロポーザルを選択して、[行の編集（Edit Row）]（鉛筆）をクリックして IPSec Proposal Editor を開きます。さまざまなオプションの詳細については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス） （1761 ページ）を参照してください。
c) デフォルトのポート 443 を使用しない場合は、[クライアントサービスの有効化（Enable Client Services）] オプションを選択して、ポート番号を入力します。（SSL VPN や他の SSL が使用するポート番号と同じ番号を使用できます）。
d) [OK] をクリックして変更を保存します。

Remote Access VPN Configuration ウィザード：[IPSec VPN Connection Profile] ページ（ASA）

Remote Access VPN Configuration ウィザードの [Connection Profile] ページを使用して、リモート アクセス IPSec VPN 用の Connection Profile ポリシーをセキュリティ アプライアンスで設定します。追加する Connection Profile ポリシーの名前を指定し、IKE ネゴシエーション中に許可する IKE バージョンを選択し、ユーザ グループ ポリシーを選択できます。また、このポリシーのアドレス プールを指定し、認証、許可、アカウンティングのサーバ グループ設定を指定できます。

このウィザードを使用した ASA でのリモート アクセス IPsec VPN の設定については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）（1688 ページ）を参照してください。

ナビゲーション パス

（デバイス ビュー）ASA または PIX 7.0 以降のデバイスでリモート アクセス IPsec VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照）。最初に表示されるページは [IPSec Connection Profile] ページです。

フィールド リファレンス

表 *368 : Remote Access VPN Configuration* ウィザード、*[IPSec VPN Connection Profile]* ページ（*ASA*）

要素	説明
Connection Profile Name	接続プロファイルの名前（トンネル グループ）。
IKE Versions	IKE ネゴシエーション中に VPN サーバとリモート ユーザ間で使用する IKE バージョン。IKEv2 は、ASA ソフトウェア リリース 8.4(1)+ だけでサポートされます。他のタイプのデバイスでは、オプションの選択を変更できません。 [IKEバージョン1（IKE Version 1）]、[IKEバージョン2（IKE Version 2）]、または [両方（Both）]（どちらのバージョンも許可する場合）を選択します。IKEv2 接続は Anyconnect クライアントを使用してのみ許可されます。

要素	説明
[グループポリシー（Group Policy）]	必要な場合、接続プロファイルに関連付けられているデフォルト ユーザ グループを定義する ASA グループ ポリシー オブジェクトの名前。グループ ポリシーはユーザ指向の属性と値のペアの集合であり、デバイスで内部的に、または RADIUS/LDAP サーバで外部的に格納されます。 [選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。 ヒント　この VPN で IKEv2 をイネーブルにする場合、選択するグループ ポリシーには特別の考慮事項が必要です。詳細については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス）（1688 ページ）を参照してください。
Global IP Address Pool	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IP アドレスをクライアントに割り当てるために使用されるアドレス プール。アドレス プールは、アドレスの範囲として入力します（10.100.12.2-10.100.12.254 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレス プール範囲を入力するか、これらのプールを定義するネットワークまたはホスト オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
Authentication Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Authorization Server Group	認可サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Accounting Server Group	アカウンティング サーバ グループの名前。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

Remote Access VPN Configuration ウィザード：[IPSec Settings] ページ（ASA）

Remote Access VPN Configuration ウィザードの [IPSec Settings] ページを使用して、リモート アクセス IPSec VPN 用の IPSec をセキュリティ アプライアンスで設定します。これらの設定の一部は IKE Version 1（IKEv1; IKE バージョン 1）にのみ適用されます。IKEv2 のみの VPN を設定している場合、これらのフィールドはグレー表示され、設定できません。

このウィザードを使用した ASA でのリモート アクセス IPsec VPN の設定については、Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）を参照してください。

ナビゲーション パス

（デバイスビュー）ASA または PIX 7.0 以降のデバイスでリモートアクセス IPsec VPN を設定するための Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照）。その後、このページが表示されるまで [次へ（Next）] をクリックします。

フィールド リファレンス

表 *369 : Remote Access VPN Configuration* ウィザード、*IPSec VPN* ウィザード：*IPSec Settings*（*ASA*）

要素	説明
事前共有キー（Preshared Key） （IKEv1 のみ）	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。 **ヒント** IKEv2 リモート アクセス VPN に事前共有キーを設定できません。
Trustpoint Name （IKEv1 のみ）	トラストポイント名を定義する PKI 登録ポリシー オブジェクトの名前（トラストポイントが IKEv1 接続で設定されている場合）。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。 [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** このトラストポイントは IKEv1 ネゴシエーションにのみ使用されます。IKEv2 ネゴシエーションにグローバル トラストポイントを設定するには、[Global Settings] ポリシーの [IKEv2 Settings] タブを使用します。VPN グローバル IKEv2 設定（1526 ページ）を参照してください。

要素	説明
IKE Peer ID Validation	IKE ピア ID 検証を無視する（確認しない）か、必須とするか、または証明書によってサポートされている場合にかぎり確認するかを選択します。IKE ネゴシエーション中、ピアは互いに自身を識別する必要があります。
Enable Sending Certificate Chain	認可の証明書チェーンの送信をイネーブルにするかどうか。証明書チェーンには、ルート CA 証明書、ID 証明書、およびキー ペアが含まれます。
Enable Password Update with RADIUS Authentication	選択すると、RADIUS 認証プロトコルを使用してパスワードを更新できます。 RADIUS認証プロトコルを使用してパスワードを更新できるかどうか。詳細については、サポートされる AAA サーバ タイプ （324 ページ）を参照してください。
ISAKMP Keepalive	ISAKMP キープアライブをモニタするかどうか。[キープアライブのモニター（Monitor Keepalive）] オプションを選択した場合、デフォルトのフェールオーバーおよびルーティングのメカニズムとして IKE キープアライブを設定できます。次のパラメータを入力します。 • [信頼間隔（Confidence Interval）]：IKE キープアライブパケット送信から次の送信までのデバイスの待機時間（秒単位）。 • [再試行間隔（Retry Interval）]：デバイスがリモートピアとの IKE 接続の確立を試行する間隔（秒単位）。デフォルト値は2秒です。 詳細については、VPN グローバル ISAKMP/IPsec 設定 （1520 ページ）を参照してください。
[Client Software Update] テーブル （IKEv1 のみ）	クライアント プラットフォームの VPN クライアントのリビジョン レベルおよび URL。すべての [All Windows Platforms]、[Windows 95/98/ME]、[Windows NT4.0/2000/XP]、または [VPN3002 Hardware Client] に対して別々のリビジョン レベルを設定できます。 プラットフォームにクライアントを設定するには、クライアントを選択して [行の編集（Edit Row）] ボタンをクリックし、[IPSec Client Software Update] ダイアログボックス （1734 ページ）に入力します。

Remote Access VPN Configuration ウィザード：[Defaults] ページ

Remote Access VPN Configuration ウィザードの [Defaults] ページを使用して、リモート アクセス IPSec VPN に割り当てる共有ポリシーを選択します。最初から選択されているポリシーは、リモート アクセス VPN 用に [Security Manager Administration] の [VPN Defaults] で設定されているポリシーです。これらのデフォルトを設定する方法については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。

必須のポリシーでは、常にポリシーが 1 つ選択されている必要があります。「Factory Default」が表示されている場合、適用されているポリシーは共有ポリシーではなく、Security Manager で指定されるデフォルトポリシー設定です。空のオプションを選択できる場合、ポリシーはオプションであり、関連機能が必要な場合にのみオプションを設定する必要があります。

ポリシーを割り当てる場合、割り当てるポリシーを検討するときには、次の点を考慮してください。

- 各ポリシー タイプのドロップダウン リストには、選択可能な既存の共有ポリシーが一覧表示されます。選択できる共有ポリシーは、Security Manager データベースにコミットされている（また、Workflow モードでアプルーバを使用している場合は承認されている）ポリシーだけです。共有ポリシーを作成して、送信前に使用することはできません。
- ポリシーの内容を表示するには、ポリシーを選択して [View Content（コンテンツの表示）] ボタンをクリックします。ポリシーが読み取り専用で表示されます。この表示を使用して、目的のポリシーを選択していることを確認します。

（注） 別のユーザによって現在ロックされているデフォルト ポリシーを選択しようとすると、ロックの問題を警告するメッセージが表示されます。ロックを回避するには、別のポリシーを選択するか、またはロックが解除されるまで VPN の作成をキャンセルします。詳細については、ポリシーのロックについて （217 ページ）を参照してください。

ナビゲーション パス

（デバイスビュー）リモートアクセス IPsec VPN を設定するための Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照）。その後、このページが表示されるまで [次へ（Next）] をクリックします。

関連項目

- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）
- Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （1703 ページ）
- リモート アクセス VPN ポリシーの概要 （1666 ページ）

フィールド リファレンス

表 *370 : Remote Access VPN Configuration* ウィザード、*[Defaults]* ページ

要素	説明
ASA グループの負荷分散	リモート アクセス VPN にある ASA デバイスのロード バランシングを定義します。

要素	説明
ハイ アベイラビリティ	リモート アクセス VPN の Cisco IOS ルータのハイ アベイラビリティ（HA）ポリシーを定義します。
Certificate to Connection Profile Map Policy	（IKEv1 のみ）リモートアクセス VPN にある ASA デバイスの証明書/接続プロファイル マップ オプションを定義します。
IKE Proposal	2 つのピアの間の IKE ネゴシエーションを保護するために使用するアルゴリズム セットを定義します。
IPSec Proposal	IPsec Security Associations（SA; セキュリティ アソシエーション）の設定に必要なクリプト マップを定義します。この定義内容には、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要なその他のパラメータが含まれます。
公開キーインフラストラクチャ	Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）証明書および RSA キーに対する PKI 登録要求の生成に使用する PKI ポリシーを定義します。
VPN Global Settings	リモートアクセス VPN にあるデバイスに適用される IKE、IPsec、IKEv2、NAT、およびフラグメンテーションのグローバル設定を定義します。

Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）

ここでは、Remote Access SSL VPN Configuration ウィザードを使用して、IOS デバイスで SSL VPN を作成または編集する方法について説明します。

関連項目

- リモート アクセス SSL VPN について （1657 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （1665 ページ）

ステップ 1 デバイス ビューで、目的の IOS デバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセス VPN（Remote Access VPN）]>[構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセス SSL VPN（Remote Access SSL VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[Gateway and Context] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） （1699 ページ）を参照してください。

ステップ 5 SSL VPN 内の保護されたリソースに接続する場合のプロキシとして使用するゲートウェイを選択します。次のオプションがあります。

- [既存のゲートウェイを使用（Use Existing Gateway）]：既存のゲートウェイオブジェクトを使用できます。このオプションを選択する場合、ゲートウェイを定義する [SSL VPN Gateway] ポリシー オブジェクトの名前を指定します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。
- [IP アドレスを使用して作成（Create Using IP Address）]：ルータ上の到達可能な（パブリックスタティック）IP アドレスを使用して、新しいゲートウェイオブジェクトを設定できます。IP アドレスを入力します。
- [インターフェイスを使用して作成（Create Using Interface）]：ルータインターフェイスのパブリックスタティック IP アドレスを使用して、新しいゲートウェイを設定できます。インターフェイスまたはインターフェイス ロール オブジェクトを選択します。

IP アドレスやインターフェイスを使用して新しいゲートウェイを作成することを選択した場合は、次の手順を実行します。

- ゲートウェイ名を指定します。
- HTTPS トラフィックを伝送するポート番号を指定します。HTTP ポート リダイレクトがイネーブルになっていない限り、デフォルトは 443 です。イネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。別のポートを使用する場合、1024 ～ 65535 の間で指定する必要があります。

ステップ 6 SSL VPN の仮想設定を定義するコンテキストの名前を入力します。

ステップ 7 SSL VPN ポリシー内で使用されるユーザ グループを選択します。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。テーブルには、そのグループでフルクライアント アクセスがイネーブルであるかどうかが示されます。[編集（Edit）] をクリックして、目的のグループを選択するか、新しいグループを作成します。

ステップ 8 認証、認証ドメイン、およびアカウンティング用の AAA オプションを設定します。詳細については、SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） （1699 ページ）を参照してください。

ステップ 9 [次へ（Next）] をクリックします。[Portal Page Customization] ページが開きます。このページの要素の詳細については、SSL VPN Configuration ウィザード：[Portal Page Customization] ページ（IOS） （1702 ページ）を参照してください。

ステップ 10 [Portal Customization] ページで、次のオプションを設定します。ページの下部には、ポータルページの外観のプレビューが、選択内容に応じて表示されます。このプレビューを使用して選択内容を調整します。

- [タイトル（Title）]：ページの上部に表示されるポータルページの名前。
- [ロゴ（Logo）]：ページのタイトル領域に表示されるグラフィック。[なし（None）]、[デフォルト（Default）]（Cisco のロゴグラフィック）、[カスタム（Custom）] から選択できます。[カスタム（Custom）] を選択する場合、[選択（Select）] をクリックして、Security Manager サーバー上にあるグラフィックを選択します。ポータル カスタマイゼーションでカスタム グラフィックを使用する前に、そのグラフィックをサーバにコピーする必要があります。

ロゴのソース イメージ ファイルに指定できるのは、GIF ファイル、JPG ファイル、または PNG ファイルです。ファイル名は最大 255 文字、サイズは最大 100 KB です。

- [ログインメッセージ（Login Message）]：ログインプロンプトの上に表示されるテキスト。

- [タイトルとテキストの色（Title and Text Colors）]：タイトルとログイン領域に使用する色とフォント。

ステップ 11　[終了（Finish）] をクリックして変更を保存します。

SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS）

（注）　バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

リモート ユーザが SSL VPN の背後にあるプライベート ネットワーク上のリソースにアクセスできるように、デバイスでゲートウェイおよびコンテキストをあらかじめ設定しておく必要があります。SSL VPN Configuration ウィザードのこの手順を使用して、ユーザにポータル ページへのアクセスを許可する情報を含むゲートウェイおよびコンテキスト設定を指定します。

ナビゲーション パス

（デバイス ビュー）IOS デバイスでリモート アクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用　（1671 ページ）を参照）。最初に表示されるページは [Gateway and Context] ページです。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス　（2011 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて　（323 ページ）

フィールド リファレンス

表 *371 : SSL VPN Configuration* ウィザード、*[Gateway and Context]* ページ

要素	説明
ゲートウェイ	SSL VPN 内の保護されたリソースに接続する場合のプロキシとして使用するゲートウェイ。次のオプションがあります。 • [既存のゲートウェイを使用（Use Existing Gateway）]：選択すると、SSL VPN に既存のゲートウェイを使用できます。 • [IPアドレスを使用して作成（Create Using IP Address）]：選択すると、ルータ上の到達可能な（パブリックスタティック）IP アドレスを使用して、新しいゲートウェイを設定できます。 • [インターフェイスを使用して作成（Create Using Interface）]：選択すると、ルータインターフェイスのパブリックスタティック IP アドレスを使用して、新しいゲートウェイを設定できます。
ゲートウェイ名	ゲートウェイを定義する [SSL VPN Gateway] ポリシー オブジェクトの名前。 • [既存のゲートウェイを使用（Use Existing Gateway）] を選択した場合、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） ゲートウェイを選択すると、セキュアな接続の確立に必要なポート番号とデジタル証明書が、関連するフィールドに表示されます。 • [Create Using IP Address] または [Interface] を選択した場合は、作成するオブジェクトの名前を入力します（最大 128 文字）。
IPアドレス	IP アドレスを使用してゲートウェイを作成するように選択した場合にのみ使用できます。 ゲートウェイ アドレスとして使用されるルータの IP アドレスです。
インターフェイス	インターフェイスを使用してゲートウェイを作成するように選択した場合にのみ使用できます。 SSL VPN ゲートウェイとして使用されるインターフェイスの名前、またはインターフェイスを定義するインターフェイス ロール オブジェクト。[選択（Select）] をクリックして、インターフェイスまたはインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。

要素	説明
[ポート（Port）]	SSL VPN 接続に使用するポート番号。HTTP ポート リダイレクトがイネーブルになっていない限り、デフォルトは 443 です。イネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。別の番号を入力する場合、1024 ～ 65535 の間で指定する必要があります。 • [Use Existing Gateway] を選択した場合、このフィールドは読み取り専用になり、選択したオブジェクトに設定されているポート番号が示されます。 • [IPアドレスを使用して作成（Create Using IP Address）] または [インターフェイス（Interface）] を選択した場合、ポート番号、または番号を指定するポートリストオブジェクトの名前を入力するか、[選択（Select）] をクリックしてポートリストオブジェクトを選択します。
Trustpoint	セキュアな接続を確立するために必要なデジタル証明書。SSL VPN ゲートウェイがアクティブな場合は、自己署名証明書が生成されます。
Context Name	SSL VPN の仮想設定を定義するコンテキストの名前。 （注） 多数のコンテキスト設定の管理を簡素化するには、コンテキスト名をドメインまたは仮想ホスト名と同じ名前にします。
Portal Page URL	SSL VPN の URL。ゲートウェイ オブジェクトを選択（または定義）すると入力されます。ユーザは、この URL に接続して VPN に入ります。
グループ ポリシー	SSL VPN ポリシー内で使用されるユーザ グループ。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。テーブルには、そのグループでフル クライアント アクセスがイネーブルであるかどうかが示されます。[編集（Edit）] をクリックして、目的のグループを選択するか、新しいグループを作成します。
Authentication Server Group	認証サーバ グループ。リストは、プライオリティ順に表示されます。認証は最初のグループを使用して試行され、ユーザが認証または拒否されるまで、リスト内のグループが順に使用されます。ゲートウェイ自体でユーザが定義されている場合は、LOCAL グループを使用します。 AAA サーバ グループの名前を入力します。複数のエントリはカンマで区切ります。[選択（Select）] をクリックして、グループを選択するか、新しいグループを作成します。
認証ドメイン（Authentication Domain）	SSL VPN リモート ユーザ認証のリストまたは方式。リストも方式も指定しない場合、ゲートウェイではリモート ユーザ認証にグローバル AAA パラメータが使用されます。
Accounting Server Group	アカウンティング サーバ グループ。AAA サーバー グループ ポリシー オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

SSL VPN Configuration ウィザード：[Portal Page Customization] ページ（IOS）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

SSL VPN Configuration ウィザードのこの手順を使用して、リモート ユーザが SSL VPN に接続すると表示されるポータル ページの外観を定義します。リモートユーザーは、このポータル ページから SSL VPN ネットワーク上で使用可能なすべての Web サイトにアクセスできます。

ナビゲーション パス

（デバイスビュー）ASA デバイスでリモートアクセス SSL VPN を設定するために Remote Access VPN Configuration ウィザードを開きます（Remote Access VPN Configuration ウィザードの使用（1671 ページ）を参照）。次に、このページが表示されるまで [次へ（Next）] をクリックします。

関連項目

- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）

フィールド リファレンス

表 *372 : SSL VPN Configuration* ウィザード：*[Portal Page Customization]* ページ

要素	説明
Title	ページの上部に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Primary] 設定を使用して色を制御します。
ロゴ	タイトルの隣に表示されるグラフィック。[None]、[Default]、または [Custom] を選択します。カスタムグラフィックを設定するには、目的のグラフィックを Cisco Security Manager サーバーにコピーし、[参照（Browse）] をクリックしてファイルを選択する必要があります。サポートされるグラフィック タイプは、GIF、JPG、および PNG で、最大サイズは 100 KB です。
ログイン メッセージ（Login Message）	ログイン プロンプトのすぐ上に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Secondary] 設定を使用して色を制御します。

要素	説明
Title Color テキストの色	タイトルとログイン領域に使用される色とテキスト。 • [Primary]：タイトル、ログインボックスのタイトル、およびこれらの領域のテキスト。 • [Secondary]：ログインボックスのユーザ名とパスワード、およびこの領域のテキスト。 [選択（Select）] をクリックして背景色を選択します。テキストでは、テキスト リストから [Black] または [White] を選択します。
プレビュー	選択内容に基づいたポータル ページの外観のプレビュー。

Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco IOS、FWSM、IPS、および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、Remote Access VPN Configuration ウィザードを使用して、IOS デバイスおよび PIX 6.3 デバイスで IPSec VPN を作成または編集する方法について説明します。

ヒント このウィザードの [Defaults] ページ（ウィザードの最後のステップ）では、VPN で使用する共有ポリシーを選択できます。この機能を使用する場合、必要なすべての共有ポリシーがデータベースに設定および送信されていることを最初に確認する必要があります。共有ポリシーと VPN ポリシーのデフォルトの設定については、VPN デフォルト ポリシーについて、および VPN デフォルト ポリシーの設定 （1395 ページ）を参照してください。

関連項目

- リモート アクセス IPSec VPN について （1656 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （1665 ページ）

ステップ 1 [Device] ビューで、目的の IOS または PIX 6.3 デバイスを選択します。

ステップ 2 ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [構成ウィザード（Configuration Wizard）] を選択します。

ステップ 3 [リモートアクセスIPSec VPN（Remote Access IPSec VPN）] オプションボタンを選択します。

ステップ 4 [リモートアクセス構成ウィザード（Remote Access Configuration Wizard）] をクリックします。[User Group Policy] ページが開きます。

ステップ 5 [利用可能なユーザーグループ（Available User Groups）] リストから必要なユーザ グループを選択して、[>>] をクリックします。

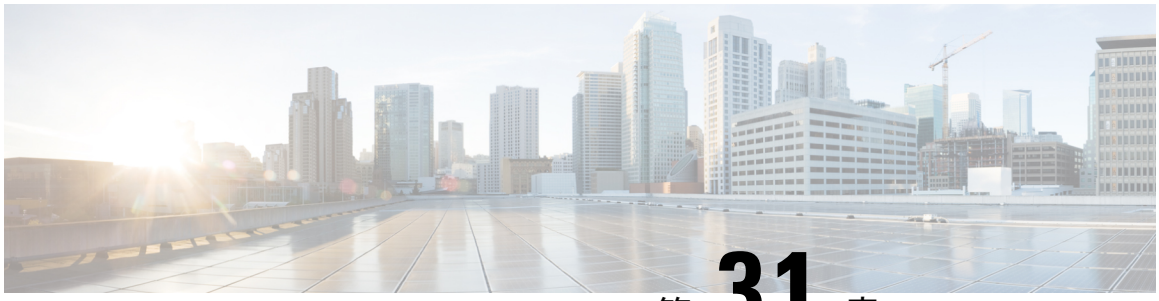
- 必要なユーザーグループがリストにない場合、[作成（Create）]（+）をクリックして[ユーザーグループの追加（Add User Groups）] ダイアログボックスを開きます。このダイアログボックスでは、ユーザー グループ オブジェクトを作成または編集できます。 [Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）を参照してください。
- 既存のユーザーグループをいずれかのリストで選択して [編集（Edit）]（鉛筆）をクリックすると、ユーザーグループを編集できます。
- ユーザーグループの選択を解除するには、ユーザーグループを選択して、[<<] をクリックします。

ステップ 6 [次へ（Next）] をクリックします。[Defaults] ページが開きます。

ステップ 7 VPN に割り当てる共有ポリシーを選択します。最初から選択されているポリシーは、[Security Manager Administration] の [VPN Defaults] ページで設定されているポリシーです。デフォルトを使用することも、使用可能なポリシーがある場合は別のポリシーを選択することもできます。これらのポリシーデフォルトの詳細については、 Remote Access VPN Configuration ウィザード：[Defaults] ページ （1695 ページ）を参照してください。

ステップ 8 [終了（Finish）] をクリックして変更を保存します。

作成したポリシーを調べて、実装するオプションを追加で設定します。



第 31 章

ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

Cisco ASA ソフトウェアまたは PIX 7.0+ を実行するデバイスのリモート アクセス IPsec、および ASA 8.0+ デバイス（PIX デバイスではありません）の SSL VPN を設定および管理できます。また、ASA 8.4(x) デバイスでは、リモートアクセス IPsec VPN で IKE バージョン 2（IKEv2）ネゴシエーションを使用できます。

（注） Cisco Catalyst 6500 シリーズ ASA サービスモジュール、およびモジュールで使用される ASA ソフトウェアリリース 8.5(x) では、VPN 設定はサポートされていません。

これらのリモートアクセス VPN の設定は、これらのデバイスタイプで同じです。IOS および PIX 6.3+ デバイスは、リモートアクセス VPN に異なる設定を使用します。

この章のトピックでは、ASA および PIX 7.0+ デバイスに固有のポリシーを設定する方法を説明します。リモート アクセス VPN の詳細については、次のトピックを参照してください。

- リモート アクセス VPN について （1655 ページ）
- 各リモートアクセス VPN テクノロジーでサポートされるデバイスについて （1665 ページ）
- リモート アクセス VPN ポリシーの検出 （1669 ページ）
- Remote Access VPN Configuration ウィザードの使用 （1671 ページ）
  - Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（ASA および PIX 7.0 以降のデバイス） （1688 ページ）
  - Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（ASA デバイス） （1672 ページ）

- リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）（1827 ページ）

この章は次のトピックで構成されています。

- ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要 （1706 ページ）
- グループのロードバランシングについて（ASA） （1710 ページ）
- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）
- リモート アクセス VPN のグループ ポリシーの設定 （1740 ページ）
- SSL VPN サーバー検証（ASA）について （1745 ページ）
- [スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （1751 ページ）
- IPSec VPN ポリシーの使用 （1753 ページ）
- SSL および IKEv2 IPSec VPN ポリシーの使用 （1764 ページ）
- クライアントレス SSL VPN ポータルのカスタマイズ （1811 ページ）

ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ASA または PIX 7.0 以降のデバイスでリモートアクセス VPN を設定する場合、設定する VPN のタイプに基づいて、以下のポリシーを使用します。可能なリモートアクセス VPN タイプは、IKE Version 1（IKEv1; IKE バージョン 1）IPsec、IKE Version 2（IKEv2; IKE バージョン 2）IPsec および SSL です。IKEv2 は、ソフトウェアバージョン 8.4(x) 以降を実行している ASA デバイスでサポートされています。これらのポリシーが必須または任意である条件については、表 373 : ASA デバイスのリモート アクセス VPN ポリシー要件 （1709 ページ）を参照してください。

（注） PIX デバイスでは SSL VPN を設定できません。PIX デバイスでは、リモート アクセス IKEv1 IPsec VPN だけをサポートしています。

- **リモート アクセス IKEv1 と IKEv2 IPsec および SSL VPN で使用されているポリシー**：
  - **ASA グループ ロード バランシング**：リモート クライアント コンフィギュレーションで、複数のデバイスを同じネットワークに接続してリモートセッションを処理している場合、それらのデバイスでセッション負荷を分担するように設定できます。この機能は、ロード バランシングと呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロードバランシングは、ASA デバイスで開始されたリモー

トセッションの場合にだけ有効です。詳細については、グループのロードバランシングについて（ASA） （1710 ページ）を参照してください。

- **接続プロファイル**：接続プロファイルは、トンネル自体の作成に関連する属性を含む、VPN トンネルの接続ポリシーが格納されたレコードセットです。接続プロファイルでは、ユーザ指向の属性が含まれる特定の接続のグループ ポリシーを識別します。詳細については、接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照してください。
- **ダイナミックアクセス**：各 VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティレベルが異なるリモートアクセスサイトからのログインなど、複数の変数が影響する可能性があります。Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）により、これらの多くの変数に対処する認可機能を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。詳細については、リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス） （1827 ページ）を参照してください。

（注） マルチコンテキスト ASA デバイスの場合、ダイナミック アクセス ポリシーは、Cisco Security Manager バージョン 4.12 および ASA バージョン 9.6(2) 以降でのみサポートされます。

- **グローバル設定**：リモートアクセス VPN のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネット キー交換）、IKEv2、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、ほとんどの場合、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合、または IKEv2 ネゴシエーションをサポートする場合だけ設定してください。詳細については、VPN グローバル設定 （1517 ページ）を参照してください。
- **グループポリシー**：リモートアクセス VPN 接続プロファイルに定義されているユーザーグループポリシーを表示できます。このページから、新しい ASA ユーザ グループを指定したり、既存の ASA ユーザ グループを編集したりできます。接続プロファイルを作成するときに、デバイスで使用されていないグループポリシーを指定した場合、このグループ ポリシーは自動的に [Group Policies] ページに追加されます。接続プロファイルを作成する前に、このポリシーに追加する必要はありません。詳細については、リモートアクセス VPN のグループ ポリシーの設定 （1740 ページ）を参照してください。
- **Public Key Infrastructure**：Public Key Infrastructure（PKI）ポリシーを作成して、CA 証明書および RSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用され

ます。詳細については、Public Key Infrastructure ポリシーについて （1544 ページ）および リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定（1552 ページ）を参照してください。

（注） マルチコンテキスト ASA デバイスの場合、Public Key Infrastructure ポリシーは、Cisco Security Manager バージョン 4.12 および ASA バージョン 9.6(2) 以降でのみサポートされます。

- **証明書スクリプトのユーザー名**：このポリシーを使用して、証明書のユーザー名のマッピングに使用するスクリプトを定義できます。詳細については、[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （1751 ページ）を参照してください。

（注） マルチコンテキスト ASA デバイスの場合、証明書スクリプトポリシーのユーザー名は、Cisco Security Manager バージョン 4.12 および ASA バージョン 9.6(2) 以降でのみサポートされます。

- **リモート アクセス IPsec VPN だけで使用されるポリシー**：
  - **証明書から接続プロファイルへのマップ、ポリシーとルール**（IKEv1 IPSec のみ）：証明書から接続プロファイルへのマップポリシーを使用すると、指定したフィールドに基づいて、ユーザーの証明書を権限グループと照合するルールを定義できます。認証を確立するため、証明書の任意のフィールドを使用することも、またはすべての証明書ユーザが権限グループを共有することもできます。グループは、DN ルール、[Organization Unit (OU)] フィールド、IKE ID、またはピア IP アドレスから照合できます。これらの方式のいずれかまたはすべてを使用できます。詳細については、Certificate to Connection Profile Map ポリシーの設定（ASA） （1754 ページ）を参照してください。
  - **IKE プロポーザル**：インターネットキーエクスチェンジ（IKE）は、ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。IKE プロポーザル ポリシーは、IKE ネゴシエーションのフェーズ 1 の要件を定義するときに使用します。詳細については、IKE プロポーザルの設定 （1488 ページ）を参照してください。
  - **IPsec プロポーザル（ASA/PIX 7.x）**：IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE

フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス） （1759 ページ）を参照してください。

- **リモート アクセス IKEv2 IPSec および SSL VPN だけで使用されるポリシー**：
  - **アクセス**：アクセスポリシーには、リモートアクセス SSL または IKEv2 IPsec VPN 接続プロファイルを有効にできるセキュリティアプライアンスのインターフェイス、接続プロファイルで使用するポート、Datagram Transport Layer Security（DTLS）設定、SSL VPN セッションタイムアウト、および最大セッション数を指定します。AnyConnect VPN クライアントまたは AnyConnect Essentials クライアントを使用するかどうかも指定できます。詳細については、SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）を参照してください。
  - **その他の設定**：SSL VPN のその他の設定ポリシーでは、キャッシング、コンテンツの書き換え、文字エンコード、プロキシとプロキシバイパス定義、ブラウザプラグイン、AnyConnect クライアントのイメージとプロファイル、Kerberos の制約付き委任、およびその他の詳細設定を定義します。詳細については、他の SSL VPN 設定の定義（ASA） （1774 ページ）を参照してください。
  - **共有ライセンス**：[SSL VPN共有ライセンス（SSL VPN Shared License）] ページを使用して、SSL VPN 共有ライセンスを設定します。詳細については、SSL VPN 共有ライセンスの設定（ASA 8.2+） （1806 ページ）を参照してください。

次の表に、特定のタイプの VPN でポリシーが必須か任意かについて説明します。

表 *373 : ASA* デバイスのリモート アクセス *VPN* ポリシー要件

ポリシー	必須、任意
ASA グループロードバランシング	**任意**：すべての VPN タイプ。
Dynamic Access	**任意**：すべての VPN タイプ。
Dynamic Access	**任意**：すべての VPN タイプ。
グローバル設定	**必須**：IKEv2 IPsec。 **任意**：IKEv1 IPsec、SSL。
グループ ポリシー	**必須**：すべての VPN タイプ。
公開キー インフラストラクチャ	**必須**：IKEv2 IPsec。 IKEv1 IPsec または SSL VPN 用のトラストポイントを設定する場合にも必須。これ以外の場合はオプションです。
Certificate To Connection Profile Maps, Policy and Rules	**任意**：IKEv1 IPsec。 **未使用**：IKEv2 IPsec、SSL。

ポリシー	必須、任意
IKE Proposal	**必須**：IKEv1 IPsec、IKEv2 IPsec。 **未使用**：SSL。
[IPsec Proposal](ASA/PIX 7.x)	**必須**：IKEv1 IPsec、IKEv2 IPsec。 **未使用**：SSL。
アクセス（Access）	**必須**：IKEv2 IPsec。SSL。 **未使用**：IKEv1 IPsec。
その他の設定（Other Settings）	**必須**：IKEv2 IPsec。SSL。 **未使用**：IKEv1 IPsec。
Shared License	**任意**：IKEv2 IPsec、SSL。 **未使用**：IKEv1 IPsec。

グループのロードバランシングについて（ASA）

リモートクライアント設定で、同じネットワークに接続された2つ以上のデバイスを使用してリモートセッションを処理するようになっている場合は、そのセッションの負荷が分散されるようにこれらのデバイスを設定できます。この機能は、ロード バランシングと呼ばれます。ロード バランシングでは、最も負荷の低いデバイスにセッション トラフィックが送信されます。このため、すべてのデバイス間で負荷が分散されます。ロード バランシングは、ASA デバイスで開始されたリモート セッションの場合にだけ有効です。

ロード バランシングを実装するには、同じプライベート LAN-to-LAN ネットワークの 2 つ以上のデバイスを、仮想クラスタにグループ化する必要があります。セッションの負荷は、仮想クラスタ内のすべてのデバイスに分散されます。仮想クラスタ内の1つのデバイス（仮想ディレクタと呼ばれる）が、着信コールを他のデバイス（セカンダリデバイスと呼ばれる）に転送します。仮想クラスタディレクタは、クラスタ内のすべてのデバイスをモニターし、各デバイスの負荷を追跡して、その負荷に基づいてセッションの負荷を分散します。

仮想クラスタは、外部のクライアントには単一の仮想グループ IP アドレスとして表示されます。この IP アドレスは、特定の物理デバイスに関連付けられたアドレスではなく、現在の仮想ディレクタに属するアドレスです。接続を確立しようとする VPN クライアントは、最初にこの仮想グループ IP アドレスに接続します。仮想クラスタディレクタは、クラスタ内で使用できるホストのうち、最も負荷の低いホストのパブリック IP アドレスをクライアントに返します。2 回めのトランザクション（ユーザーに対しては透過的）になると、クライアントはホストに直接接続します。仮想ディレクタは、このようにしてリソース全体に均等かつ効率的にトラフィックを転送します。

仮想ディレクタの役割は、1 つの物理デバイスに結び付けられるものではなく、デバイス間でシフトできます。クラスタ内のマシンで障害が発生すると、終了されたセッションはただちに

仮想グループ IP アドレスに再接続できます。次に、仮想ディレクタは、クラスタ内の別のアクティブデバイスにこれらの接続を転送します。仮想ディレクタ自身に障害が発生した場合は、クラスタ内のセカンダリデバイスが、新しい仮想セッションディレクタをただちに引き継ぎます。クラスタ内の複数のデバイスで障害が発生しても、クラスタ内のデバイスが 1 つでも使用可能である限り、ユーザはクラスタに引き続き接続できます。

Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用したリダイレクションについて

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、セカンダリ デバイスにリダイレクトされるとその証明書は無効になります。セキュリティアプライアンスは、VPN ディレクタとして、VPN クライアント接続をクラスタデバイス（クラスタ内の別のセキュリティアプライアンス）にリダイレクトする場合に、そのグループデバイスの完全修飾ドメイン名（FQDN）を送信できます。セキュリティ アプライアンスは、逆 DNS ルックアップを使用してデバイスの FQDN を外部 IP アドレスに解決し、接続を転送して VPN ロード バランシングを実行します。グループ内のロードバランシングデバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

FQDN によるロード バランシングをイネーブルにしたあと、ASA 外部インターフェイスごとにエントリが存在しない場合は、このエントリを DNS サーバに追加します。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。ASA での DNS ルックアップをイネーブルにし、ASA 上で DNS サーバの IP アドレスを定義します。

グループロードバランシングの設定手順については、グループのロードバランスポリシーの設定（ASA） （1711 ページ）を参照してください。

グループのロードバランスポリシーの設定（ASA）

[ASAクラスタロードバランス（ASA Cluster Load Balance）] ページを使用して、リモートアクセス VPN の ASA デバイスのロードバランシングを有効にします。ロードバランシングはデフォルトでは無効になっているので、明示的に有効にする必要があります。クラスタに参加するすべてのデバイスは、同じクラスタ固有の値（IP アドレス、暗号化設定、暗号キー、およびポート）を共有する必要があります。クラスタ ロードバランシングの詳細については、グループのロードバランシングについて（ASA） （1710 ページ）を参照してください。

（注） ロードバランシングには、アクティブな 3DES/AES ライセンス、および Plus ライセンス付きの ASA モデル 5510、または ASA モデル 5520 以降が必要です。ASA デバイスでは、ロード バランシングをイネーブルにする前に、このクリプト ライセンスが存在するかをチェックします。アクティブな 3DES または AES ライセンスを検出できない場合、デバイスは、ロード バランシングを回避し、さらにライセンスがこの使用を許可していないかぎり、ロード バランシング システムによる 3DES の内部コンフィギュレーションも回避します。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [ASAグループロードバランス（ASA Group Load Balance）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [リモートアクセスVPN（Remote Access VPN）] > [ASAグループロードバランス（ASA Group Load Balance）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[ASAグループロードバランス（ASA Group Load Balance）] ページが開きます。

ステップ 2 [ロードバランシングクラスタに参加（Participate in Load Balancing Cluster）] を選択して、デバイスがロードバランシングクラスタに属することを示します。

ステップ 3 [VPNグループの設定（VPN Group Configuration）] オプションを設定します。

- [グループIPv4/IPv6アドレス（Group IPv4/IPv6 Address）]：仮想クラスタ全体を表す単一の IP アドレスを指定します。外部インターフェイスと同じサブネット内にある IP アドレスを選択します。バージョン 4.12 以降、Security Manager は、IPv4 アドレスに加えて、IPv6 グループの IPv6 アドレスをサポートします。これはバージョン 9.0 以降を実行している ASA デバイスに適用されます。
- [UDPポート（UDP Port）]：デバイスが属する仮想クラスタの UDP 宛先ポートを指定します。通常、ポート番号は 9023 です。ただし、このポートが別のアプリケーションで使用されている場合、ロードバランシングに使用する UDP 宛先ポート番号を入力します。
- [IPSec暗号化を有効にする（Enable IPSec Encryption）]、[IPSec共有秘密（IPSec Shared Secret）]：必要に応じて、[IPSec暗号化を有効にする（Enable IPSec Encryption）] を選択し、デバイス間で通信されるすべてのロードバランシング情報が暗号化されるようにします。このオプションを選択した場合は、共有秘密パスワードも入力（および確認）します。これは、スペースを含まない 4 ～ 16 文字の値で、大文字と小文字が区別されます。仮想グループのセキュリティアプライアンスは、IPsec を使用して LAN-to-LAN トンネルを介して通信します。このパスワードは、クライアントから渡されるパスワードと一致する必要があります。

ステップ 4 [NAT設定（NAT Configuration）] オプションを設定します。

- [NAT IPアドレスIPv4/IPv6（NAT IP Address IPv4/IPv6）]：単一の NAT IP アドレスを指定します。バージョン 4.24 以降、CSM は IPv4 および IPv6 NAT IP アドレス設定をサポートします。

ステップ 5 クラスタ内のサーバーの優先順位を設定します。次のオプションのいずれかを選択します。

- [デバイスのデフォルト値を受け入れる（Accept default device value）]：デバイスに割り当てられたデフォルトの優先順位の値を受け入れます。
- [クラスタ内のすべてのデバイスに同じ優先順位を設定（Configure same priority on all devices in the cluster）]：クラスタ内のすべてのデバイスに同じ優先順位の値を設定します。次に優先順位番号（1 ～ 10）を入力します。この番号は、起動時または既存のディレクタで障害が発生したときに、デバイスが仮想ディレクタになる可能性を表します。

ステップ 6 サーバ上で使用するパブリックおよびプライベート インターフェイスを指定します。

- [パブリックインターフェイス（Public Interfaces）]：サーバーで使用されるパブリックインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。
- [プライベートインターフェイス（Private Interfaces）]：サーバーで使用されるプライベート インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択するか、あるいは新しいロールを作成します。

ステップ 7 必要に応じて、[リダイレクト時にIPアドレスではなくFQDNを送信する（Send FQDN to client instead of an IP address when redirecting）] を選択し、完全修飾ドメイン名を使用したリダイレクションを有効にします。このオプションは、8.0(2) 移行が動作する ASA デバイスでのみ使用できます。詳細については、グループのロードバランシングについて（ASA） （1710 ページ）を参照してください。

接続プロファイルの設定（ASA、PIX 7.0+）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

接続プロファイルは、VPN トンネル接続プロファイルポリシーを含む一連のレコードです。このレコードには、トンネルそのものの作成に関連する属性も含まれます。接続プロファイルでは、ユーザ指向の属性が含まれる特定の接続のグループ ポリシーを識別します。ユーザにグループ ポリシーを割り当てない場合、接続にはデフォルトの接続プロファイルが適用されます。環境に固有の接続プロファイルを 1 つ以上作成できます。ローカル リモート アクセス VPN サーバまたは外部 AAA サーバ上で接続プロファイルを設定できます。

デバイスでリモート アクセス VPN ポリシーを検出すると、Security Manager により、デフォルト接続プロファイルがポリシーに追加されます。これらのプロファイル、および関連する DlftGrpPolicy（Security Manager では *<device_display_name>* DfltGrpPolicy という名前に変更されています）を編集できますが、削除はできません。次に、Security Manager でサポートされているデフォルト接続プロファイルを示します。

- DefaultRAGroup：リモート アクセス IPsec VPN のデフォルトの接続プロファイル。
- DefaultWEBVPNGroup：SSL VPN のデフォルトの接続プロファイル。この接続プロファイルは、ASA 8.0+ デバイスだけで検出されます。

ASA デバイス上で接続プロファイルを設定する場合には、二重認証を設定するオプションがあります。二重認証機能では、Payment Card Industry Standards Council Data Security Standard に従って、ネットワークへのリモート アクセスに対して 2 つの要素からなる認証を実行します。この機能では、ユーザーはログイン ページで異なる 2 組のログイン クレデンシャルを入力する必要があります。たとえば、プライマリ認証をワンタイム パスワード、セカンダリ認証をドメイ

ン（Active Directory）クレデンシャルとする場合が考えられます。プライマリクレデンシャル認証が失敗すると、セキュリティ アプライアンスはセカンダリ クレデンシャルの確認を試行しません。いずれかの認証に失敗すると、接続が拒否されます。AnyConnect VPN クライアント（SSL VPN または IKEv2 IPSec VPN）およびクライアントレス SSL VPN の両方で二重認証がサポートされています。AnyConnect クライアントでは、Windows コンピュータ（サポート対象 Windows Mobile 装置および Start Before Login など）、Mac コンピュータ、および Linux コンピュータで二重認証がサポートされています。

ここでは、Connection Profile ポリシーを使用して、リモート アクセス VPN サーバで接続プロファイルを作成または編集する方法について説明します。

（注） Remote Access VPN Configuration ウィザードから、接続プロファイルを作成することもできます（Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照）。Easy VPN サイト間トポロジについては、Easy VPN における Connection Profile ポリシーの設定 （1616 ページ）を参照してください。

関連項目

- リモート アクセス VPN ポリシーの検出 （1669 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA または PIX 7.0 以降のデバイスを選択し、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（ASA）（Connection Profiles (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Connection Profiles] ページが開きます。このポリシーでは、すべての接続プロファイルのリストが示され、プロファイルで使用されるグループ ポリシーが表示されます。詳細については、[Connection Profiles] ページ （1715 ページ）を参照してください。

ステップ 2 テーブルの下にある [行の追加（Add Row）]（+）をクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）をクリックします。[Connection Profiles] ダイアログボックスが開きます。

ステップ 3 （すべてのリモートアクセス VPN タイプ）[General] タブで、接続プロファイル名およびグループ ポリシーを指定して、使用するアドレス割り当て方式を選択します。設定の詳細については、[General] タブ（[Connection Profiles]） （1718 ページ）を参照してください。

ステップ 4 （すべてのリモートアクセス VPN タイプ）[AAA] タブをクリックして、接続プロファイルの AAA 認証パラメータを指定します。設定の詳細については、[AAA] タブ（[Connection Profiles]） （1721 ページ）を参照してください。

ステップ 5 （リモートアクセス IKEv2 IPsec および SSL VPN のみ）ASA デバイスで接続プロファイルを設定している場合は、セカンダリ認証を設定できます。これを行うには、[セカンダリAAA（Secondary AAA）] タブを

クリックします。設定の詳細については、[Secondary AAA] タブ（[Connection Profiles]） （1727 ページ）を参照してください。

ステップ 6 （リモートアクセス IPsec VPN のみ）[IPsec] タブをクリックして、接続プロファイルの IPsec および IKE パラメータを指定します。これらの一部の設定は、IKEv1 接続には適用されますが、IKEv2 接続には適用されません。設定の詳細については、[IPSec] タブ（[Connection Profiles]） （1730 ページ）を参照してください。

（注） IKEv2 設定を行うには、[Global Settings] ポリシーの [IKEv2 Settings] タブを使用します。 VPN グローバル IKEv2 設定 （1526 ページ）を参照してください。

ステップ 7 （リモートアクセス SSL VPN のみ）[SSL] タブをクリックして接続プロファイルポリシーの WINS サーバーを指定し、SSL VPN エンドユーザログオン Web ページのカスタマイズ済みルックアンドフィールを選択し、クライアントアドレスの割り当てに使用する DHCP サーバーを指定し、インターフェイスとクライアント IP アドレスプール間のアソシエーションを設定します。設定の詳細については、[SSL] タブ（[Connection Profiles]） （1734 ページ）を参照してください。

ステップ 8 [OK] をクリックします。

[Connection Profiles] ページ

リモート アクセス VPN または Easy VPN トポロジの接続プロファイル ポリシーを管理するには、[Connection Profiles] ページを使用します。[接続プロファイル（Connection Profiles）] ページには、設定されている接続プロファイルが一覧表示され、それらの接続プロファイルに関連付けられたグループポリシーが表示されます。また、接続プロファイルが 、トンネルネゴシエーション中に特定のトンネルグループが識別されない場合に Citrix クライアントに使用されるデフォルトの接続プロファイルであるかどうかが示されます。

このポリシーの使用法は、設定する VPN のタイプによって異なります。

- [Remote access SSL VPN]：ポリシーは、ASA デバイスに対してだけ使用されます。複数のプロファイルを作成し、[Connection Profiles] ダイアログボックスのすべてのタブの値を設定できます。
- [Remote access IPSec VPN]：ポリシーは、PIX 7.0+ ソフトウェアを実行している ASA デバイスおよびPIX ファイアウォールに対して使用されます。複数のプロファイルを作成できますが、[Connection Profiles] ダイアログボックスの [General]、[AAA]、および [IPSec] タブだけがこの設定に適用されます（場合によってはこれらのタブだけが表示されます）。
- [Easy VPN topologies]：ポリシーは、PIX 7.0+ ソフトウェアを実行している ASA デバイスまたは PIX ファイアウォールである Easy VPN サーバ（ハブ）に対して使用されます。ポリシー ページが [Connection Profiles] ダイアログボックスが実際に埋め込まれるように、単一のプロファイルを作成できます。これにより、プロファイルを定義するタブに直接アクセスできます。[General]、[AAA]、および [IPSec] タブだけが適用されます。

リモート アクセス IPSec および SSL VPN では、次のように行います。

- プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスに入力します。

- 既存のプロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。

接続プロファイルは、次のタブで構成されます。これらのタブには、設定する VPN のタイプに適した値を設定してください。

- [General] タブ（[Connection Profiles]） （1718 ページ）
- [AAA] タブ（[Connection Profiles]） （1721 ページ）
- [Secondary AAA] タブ（[Connection Profiles]） （1727 ページ）（SSL VPN および IKEv2 IPsec VPN のみ）
- [IPSec] タブ（[Connection Profiles]） （1730 ページ）（これらの設定の一部は、IKEv1 接続には適用されますが、IKEv2 接続には適用されません。）
- [SSL] タブ（[Connection Profiles]） （1734 ページ）（SSL VPN のみ）

ナビゲーション パス

リモートアクセス VPN：

- （デバイスビュー）ASA または PIX 7+ デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [接続プロファイル（ASA）（Connection Profiles (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

Easy VPN では、次のように行います。

- [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）から Easy VPN トポロジを選択し、[接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX7.0/ASA)）] を選択します。
- （デバイスビュー）Easy VPN トポロジに参加するデバイスを選択し、ポリシーセレクタから [サイト間VPN（Site to Site VPN）] を選択します。Easy VPN トポロジを選択して [VPN ポリシーの編集（Edit VPN Policies）] をクリックし、[Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を開いてポリシーを選択します。
- （ポリシービュー）**[サイト間VPN（Site-to-Site VPN）] > [接続プロファイル（PIX7.0/ASA）（Connection Profiles (PIX7.0/ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ここでは、次の内容について説明します。

- [General] タブ（[Connection Profiles]） （1718 ページ）
- [AAA] タブ（[Connection Profiles]） （1721 ページ）

• [Secondary AAA] タブ（[Connection Profiles]） （1727 ページ）
• [IPSec] タブ（[Connection Profiles]） （1730 ページ）
• [SSL] タブ（[Connection Profiles]） （1734 ページ）

リモートアクセス VPN マルチコンテキスト モードでサポートされる CLI - 接続プロファイル

次の CLI は、マルチコンテキストモードのリモートアクセス VPN の接続プロファイル用 ASA 9.5(2) でサポートされています。これらの CLI は、トンネルグループの管理およびユーザコンテキストでサポートされています。

DefaultWEBVPNGroup は、デフォルトの接続プロファイルです。DefaultRAGroup は、ASA 9.5(2) リモートアクセス VPN マルチコンテキストモードではサポートされていません。

（注） サポートされていない設定の場合、Security Manager は無視できる警告メッセージを表示します。デルタは生成されません。

- Type remote-access
- General-attributes
  - Accounting-server-group
  - Address-pool
  - 注釈（Annotation）
  - Authenticated-session-username
  - Authentication-attr-from-server
  - Authentication-server-group
  - Authorization-required
  - Authorization-server-group
  - Default-group-policy
  - Dhcp-server
  - 終了（Exit）
  - Ipv6-address-pool
  - Nat-assigned-to-public-ip
  - Password-management
  - Secondary-authentication-server-group

- Webvpn-attributes
  - 認証
  - 終了（Exit）
  - Group-alias
  - Group-url
  - なし
  - Radius-reject-message

[General] タブ（[Connection Profiles]）

[Connection Profiles] ダイアログボックスの [General] タブを使用して、VPN Connection Profile ポリシーの基本プロパティを設定します。これらのプロパティは、リモートアクセス IPsec および SSL VPN、あるいはサイト間 Easy VPN トポロジで使用されます。

[全般（General）] タブは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

- リモートアクセス VPN：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （1715 ページ）を参照）から、[行の追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。必要に応じて、[全般（General）] タブをクリックします。
- Easy VPN トポロジ：Easy VPN トポロジを選択して、ポリシー ビューまたはサイト間 VPN Manager のいずれかでサイト間 VPN Connection Profile ポリシーを選択します（[Connection Profiles] ページ （1715 ページ）を参照）。必要に応じて、[全般（General）] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）
- [ASA Group Policies] ダイアログボックス （1918 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- Easy VPN について （1599 ページ）
- Easy VPN における Connection Profile ポリシーの設定 （1616 ページ）

フィールド リファレンス

表 374 : [Connection Profile] の [General] タブ

要素	説明
Connection Profile Name	接続プロファイルの名前（トンネル グループ）。
[グループ ポリシー（Group Policy）]	必要な場合、接続プロファイルに関連付けられているデフォルト ユーザ グループを定義する ASA グループ ポリシー オブジェクトの名前。グループ ポリシーはユーザ指向の属性と値のペアの集合であり、デバイスで内部的に、または RADIUS/LDAP サーバで外部的に格納されます。 [選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。
Client Address Assignment	
DHCP サーバ（DHCP Servers）	クライアント アドレス割り当てに使用される DHCP サーバ。これらのサーバは、リスト内の順序で使用されます。 DHCP サーバの IP アドレス、または DHCP サーバのアドレスを定義するネットワーク/ホスト ポリシー オブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[グローバル IPv4 アドレスプール（Global IPv4 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv4 アドレスをクライアントに割り当てるために使用されるアドレスプール。アドレス プールは、アドレスの範囲として入力します（10.100.12.2-10.100.12.254 など）。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレスプール範囲を入力するか、これらのプールを定義するネットワークまたはホストオブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
[グローバル IPv6 アドレスプール（Global IPv6 Address Pool）]	クライアントの接続先のインターフェイスにプールが指定されていない場合に、IPv6 アドレスをクライアントに割り当てるために使用されるアドレスプール。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。アドレスプールはアドレスの範囲として入力します（例：fe80::60/5 4）。ここで、fe80::60/5 は IPv6 アドレスとプレフィックス長、4 はカウント（アドレスの数）です。サーバはこれらのプールを一覧表示されている順序で使用します。最初のプールのアドレスがすべて割り当て済みの場合は、次のプールを使用するというように続きます。最大で 6 つのプールを指定できます。 アドレスプール範囲を入力するか、これらのプールを定義するネットワークまたはホストオブジェクトの名前を入力します。[選択（Select）] をクリックして、既存のネットワークまたはホストオブジェクトを選択するか、新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
[Interface-Specific Address Pools] テーブル	特定のインターフェイスを介して接続するクライアントがグローバル グループとは異なるプールを使用するように、そのインターフェイスに対して個別の IP アドレス プールを設定する場合は、そのインターフェイスをこのテーブルに追加し、個別のプールを設定します。このテーブルに表示されていないインターフェイスはすべて、グローバル プールを使用します。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。したがって、IPv6 アドレスプールの追加の列が表示されます。 • インターフェイス固有のアドレス プールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックス （1720 ページ）に入力します。 • インターフェイス プールを編集するには、インターフェイス プールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。

[Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックス

[Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools] ダイアログボックスを使用して、Connection Profile ポリシーに対してインターフェイス固有のクライアント アドレス プールを設定します。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [全般（General）] タブ（[General] タブ（[Connection Profiles]） （1718 ページ）を参照）を開き、[インターフェイス固有のアドレスプール（Interface-Specific Address Pools）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブルから行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- ネットワーク/ホストオブジェクトの作成 （394 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）

フィールド リファレンス

表 *375 : [Add Interface Specific Client Address Pools]/[Edit Interface Specific Client Address Pools]* ダイアログボックス

要素	説明
インターフェイス（Interface）	アドレス プールを割り当てるインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）]をクリックしてインターフェイスまたはオブジェクトを選択するか、または新しいオブジェクトを作成します。
IPv4 アドレスプール（IPv4 Address Pool）	インターフェイスに割り当てる IPv4 アドレスプール。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。アドレス プールは、プールの開始および終了 IP アドレスを使用して指定されます。たとえば、10.100.10.2-10.100.10.254 です。IP アドレス範囲を入力するか、アドレス範囲を指定するネットワーク/ホスト オブジェクトを使用できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。
IPv6アドレスプール（IPv6 Address Pool）	インターフェイスに割り当てる IPv6 アドレスプール。IPv6 アドレスプールは、IPv6 アドレスとプレフィックス長、およびその後に続くカウントを使用して指定されます。カウントはプール内のアドレスの数を示します。IP アドレス範囲を入力するか、アドレス範囲を指定するネットワーク/ホスト オブジェクトを使用できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。

[AAA] タブ（[Connection Profiles]）

[Connection Profile] ダイアログボックスの [AAA] タブを使用して、Connection Profile ポリシーに AAA 認証パラメータを設定します。

AAA の場合、識別名認証設定ポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされません。

ただし、Security Manager バージョン 4.12 以降、このポリシーはマルチコンテキストモードの ASA 9.6(2) リモートアクセス VPN でサポートされます。管理およびユーザーコンテキストでサポートされる CLI は次のとおりです。

- Tunnel-group General-attributes
  - Secondary-username-from-certificate
  - Username-from-certificate

ナビゲーション パス

- リモートアクセス VPN：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （1715 ページ）を参照）から、[行を追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックし、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[AAA] タブをクリックします。
- Easy VPN トポロジ：Easy VPN トポロジを選択して、ポリシー ビューまたはサイト間 VPN Manager のいずれかでサイト間 VPN Connection Profile ポリシーを選択します（[Connection Profiles] ページ （1715 ページ）を参照）。[AAA] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- Easy VPN における Connection Profile ポリシーの設定 （1616 ページ）
- Easy VPN について （1599 ページ）

フィールド リファレンス

表 376 : [Connection Profile] の [AAA] タブ

要素	説明
認証方式	AAA、証明書、またはその両方、複数の証明書、AAA と複数の証明書、およびSAML を使用して接続を認証するかどうか。[証明書（Certificate）] を選択すると、必要な詳細が証明書から取得されるため、ダイアログボックスのオプションの多くが無効になります。 バージョン 4.10 以降、Security Manager では、認証方法として SAML ID プロバイダーを選択できます。これは、現在のトンネルグループに対して SAML サービスプロバイダーを有効にするためです。SAML ID プロバイダーは、トンネルグループに適用されるまで使用されません。SAML 認証は相互排他認証方式です。詳細については、SAML ID プロバイダの構成 （415 ページ）を参照してください。 バージョン 4.13 以降、Security Manager では、認証方式として複数の証明書、または AAA と複数の証明書を選択できます。この方式は、ASA 9.7.1 デバイスの複数証明書認証機能をサポートする目的で有効になっています。9.7.1 リリースより前の ASA デバイスに対してこの方式を選択すると、検証エラーメッセージが表示されます。詳細については、複数証明書認証のサポート （577 ページ）を参照してください。
Authentication Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 クライアントの接続先のインターフェイスに基づいて別の認証サーバ グループを使用する場合は、このタブの一番下にある [Interface-Specific Authentication Server Groups] テーブルでサーバ グループを設定します（後述の説明を参照）。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Authorization Server Group	認可サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Users must exist in the authorization database to connect	正常に接続するために、クライアントのユーザ名が認可データベース内に存在することを要求するかどうか。ユーザー名が承認データベース内に存在しない場合、接続が拒否されます。

要素	説明
Accounting Server Group	アカウンティング サーバ グループの名前。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
Strip Realm from Username Strip Group from Username	ユーザ名を AAA サーバに渡す前に、ユーザ名からレルムまたはグループ名を削除するかどうか。レルムとは管理ドメインのことです。これらのオプションを有効にすると、ユーザ名だけに基づいて認証できます。 これらのオプションを任意に組み合わせて有効にできます。ただし、サーバーが区切り文字を解析できない場合は、両方のチェックボックスをオンにする必要があります。
Override Account-Disabled Indication from AAA Server	AAA サーバーからの「account-disabled」インジケータをオーバーライドするかどうか。この設定は、「account-disabled」インジケータを返すサーバー（NT LDAP を使用する RADIUS、Kerberos など）で有効です。 認証に LDAP ディレクトリ サーバーを使用している場合、パスワード管理は Sun Microsystems JAVA System Directory Server（旧名称は Sun ONE Directory Server）および Microsoft Active Directory を使用してサポートされます。 • **Sun**：Sunディレクトリサーバーにアクセスするためにセキュリティ アプライアンスで設定されている DN は、そのサーバー上のデフォルトのパスワードポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルトパスワード ポリシーに ACI を設定できます。 • **Microsoft**：Microsoft Active Directory でパスワード管理を有効にするには、LDAP over SSL を設定する必要があります。
Enable Notification Upon Password Expiration to Allow User to Change Password Enable Notification Prior to Expiration Notify Prior to Expiration	セキュリティ アプライアンスが、リモートユーザのログイン時に、現在のパスワードの期限切れが近づいていること、または期限が切れていることを通知し、パスワードを変更する機会を提供するかどうか。 パスワードの期限切れが近づいていることを前もってユーザーに警告する場合には、[期限切れ前の通知の有効化（Enable Notification Prior to Expiration）] を選択して、通知を開始する期限切れ前の日数（1 ～ 180）を指定します。このオプションは、RADIUS、RADIUS 対応 NT サーバ、および LDAP サーバなど、このような通知をサポートする AAA サーバで使用できます。他の種類のサーバーについては、事前の通知はありません。

要素	説明
Distinguished Name (DN) Authorization Settings	認可用の識別名を使用する方法。Distinguished Name（DN; 識別名）は、個々のフィールドから構成される一意の識別子であり、ユーザをトンネル グループと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。認可中の DN の使用方法を決定するには、以下のオプションを選択します。 • [DN全体をユーザー名として使用（Use Entire DN as the Username）]：特定のフィールドに焦点を当てることなく、DN 全体を使用します。 • [個々のDNフィールドをユーザー名として指定（Specify Individual DN fields as the Username）]：特定のフィールドに焦点を当てます。プライマリ フィールドを選択し、オプションでセカンダリ フィールドを選択します。デフォルトでは、Common Name（CN; 共通名）をプライマリとして使用し、Organizational Unit（OU; 組織ユニット）をセカンダリとして使用します。 • [ユーザー名選択にスクリプトを使用（Use Script to Select Username）]：バージョン 4.7 以降、Security Manager では、証明書からのユーザー名のマッピングに使用するスクリプトを定義できます。ドロップダウンリストから、定義したスクリプトを選択します。詳細については、[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （1751 ページ）を参照してください。
[Interface-Specific Authentication Server Groups] テーブル	特定のインターフェイスを介して接続するクライアントがグローバル プールとは異なるサーバ グループを使用するように、そのインターフェイスに対して個別の認証サーバ グループを設定する場合は、そのインターフェイスをこのテーブルに追加し、個別のグループを設定します。ここに記載されていないインターフェイスでは、グローバル認証サーバ グループを使用します。この表には、サーバ グループと、サーバ グループが使用可能でない場合にローカル認証を使用するかどうかを示します。 • インターフェイス固有の認証グループをリストに追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックス （1726 ページ）に入力します。 • インターフェイス設定を編集するには、インターフェイス設定を選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイス設定を削除するには、インターフェイス設定を選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックス

[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックスを使用して、Connection Profile ポリシーにインターフェイス固有の認証を設定します。指定されたインターフェイスにクライアントが接続すると、グローバル認証サーバ グループの設定がこの設定によって上書きされます。

ASA デバイスで SSL VPN のセカンダリ AAA サーバを設定する場合、その設定は、ユーザが入力するセカンダリ クレデンシャル セットに対して使用されます。これは、ダイアログボックスの名前に反映されます。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [AAA] または [セカンダリ AAA] タブ（[AAA] タブ（[Connection Profiles]） （1721 ページ）または [Secondary AAA] タブ（[Connection Profiles]） （1727 ページ）を参照）を開き、[インターフェイス固有のアドレス プール（Interface-Specific Address Pools）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブル内の行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- インターフェイス ロール オブジェクトについて （381 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

フィールド リファレンス

表 377 : [Add (Secondary) Interface Specific Authentication Server Groups]/[Edit (Secondary) Interface Specific Authentication Server Groups]

要素	説明
インターフェイス（Interface）	認証サーバ グループを設定するインターフェイスまたは（インターフェイスを識別する）インターフェイス ロールの名前。[選択（Select）] をクリックして、インターフェイスまたはインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。
Server Group	認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 セカンダリ AAA を設定する場合、2 番めのクレデンシャルに対してこのグループが使用されます。プライマリ クレデンシャルとセカンダリ クレデンシャルには別々のサーバ グループを指定できます。

要素	説明
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Use Primary Username （セカンダリ認証のみ。ASA 8.2+ でのリモート アクセス SSL または IKEv2 IPSec VPN にかぎります）	プライマリ クレデンシャルに使用したのと同じユーザ名をセカンダリ クレデンシャルに使用するかどうか。このオプションを選択した場合、ユーザは、プライマリ クレデンシャルで認証された後、セカンダリ パスワードだけを要求されます。このオプションを選択しない場合は、セカンダリ プロンプトによってユーザ名とパスワードの両方が要求されます。

[Secondary AAA] タブ（[Connection Profiles]）

[Secondary AAA] タブを使用して、ASA 8.2+ デバイスで使用するリモート アクセス SSL VPN Connection Profile ポリシーまたは ASA 8.4(1)+ デバイスで使用するリモート アクセス IKEv2 IPSec VPN Connection Profile ポリシーにセカンダリ AAA 認証パラメータを設定します。これらの設定は、リモート アクセス IKEv1 IPSec VPN や Easy VPN トポロジ、またはその他のデバイス タイプには適用されません。

ナビゲーション パス

リモートアクセス VPN のみ：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （1715 ページ）を参照）から、[行の追加（+）（Add Row(+)）] ボタンをクリックするか、プロファイルを選択して、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックして、[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[セカンダリ AAA（Secondary AAA）] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）

フィールド リファレンス

表 378 : [Connection Profile] の [Secondary AAA] タブ

要素	説明
Enable Double Authentication	リモート アクセス VPN 接続を完了する前に、ユーザに 2 つのクレデンシャル セット（ユーザ名とパスワード）を要求する二重認証をイネーブルにするかどうか。

要素	説明
Secondary Authentication Server Group	2 番めのクレデンシャルセットで使用する認証サーバ グループの名前（トンネル グループがローカル デバイスに設定されている場合は LOCAL です）。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 クライアントの接続先のインターフェイスに基づいて別の認証サーバ グループを使用する場合は、このタブの一番下にある [Secondary Interface-Specific Authentication Server Groups] テーブルでサーバ グループを設定します（後述の説明を参照）。
Use LOCAL if Server Group Fails	選択した認証サーバ グループで障害が発生した場合に、ローカルの認証データベースに切り替えるかどうか。
Use Primary Username for Secondary Authentication	プライマリ クレデンシャルに使用したのと同じユーザ名をセカンダリ クレデンシャルに使用するかどうか。このオプションを選択した場合、ユーザは、プライマリ クレデンシャルで認証された後、セカンダリ パスワードだけを要求されます。このオプションを選択しない場合は、セカンダリ プロンプトによってユーザ名とパスワードの両方が要求されます。
Username for Session	ソフトウェアがユーザ セッションに使用するユーザ名。プライマリ名かセカンダリ名のいずれかとなります。プライマリ名だけを要求する場合は、プライマリを選択します。 （注） デフォルトでは、複数のユーザ名が存在する場合、AnyConnect では、複数のセッションの間、両方のユーザ名を記憶します。さらに、ヘッドエンド デバイスでは、クライアントが両方のユーザ名を記憶するか、または両方とも記憶しないかの管理制御を行う機能が提供される場合があります。
Authorization Authentication Server	認可に使用するサーバ。（[AAA] タブで定義されている）プライマリ認証サーバか、このタブで設定されているセカンダリ認証サーバのいずれかです。

要素	説明
Distinguished Name (DN) Secondary Authorization Setting	認可用の識別名を使用する方法。Distinguished Name（DN; 識別名）は、個々のフィールドから構成される一意の識別子であり、ユーザをトンネルグループと照合するときに識別子として使用できます。DN ルールは、拡張証明書認証に使用されます。認可中の DN の使用方法を決定するには、以下のオプションを選択します。 • [DN全体をユーザー名として使用（Use Entire DN as the Username）]：特定のフィールドに焦点を当てることなく、DN 全体を使用します。 • [個々のDNフィールドをユーザー名として指定（Specify Individual DN fields as the Username）]：特定のフィールドに焦点を当てます。プライマリ フィールドを選択し、オプションでセカンダリ フィールドを選択します。デフォルトでは、User Identification（UID; ユーザ ID）フィールドだけを使用します。 • [ユーザー名選択にスクリプトを使用（Use Script to Select Username）]：バージョン 4.7 以降、Security Manager では、証明書からのユーザー名のマッピングに使用するスクリプトを定義できます。ドロップダウンリストから、定義したスクリプトを選択します。詳細については、[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス （1751 ページ）を参照してください。 （注） Distinguished Name (DN) Secondary Authorization Settings は、マルチコンテキストモードでバージョン 9.6(2) を実行している ASA デバイスの Security Manager バージョン 4.12 からサポートされています。管理およびユーザコンテキストでサポートされる CLI は次のとおりです。 • Tunnel-group General-attributes • Secondary-username-from-certificate • Username-from-certificate

要素	説明
[Secondary Interface-Specific Authentication Server Groups] テーブル	特定のインターフェイスを介して接続するクライアントがグローバルプールとは異なるサーバ グループを使用するように、そのインターフェイスに対して個別のセカンダリ認証サーバ グループを設定する場合は、そのインターフェイスをこのテーブルに追加し、個別のグループを設定します。ここに記載されていないインターフェイスでは、グローバル認証サーバ グループを使用します。この表には、サーバ グループと、サーバ グループが使用可能でない場合にローカル認証を使用するかどうかを示します。 • セカンダリインターフェイス固有の認証グループをリストに追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add Interface Specific Authentication Server Groups]/[Edit Interface Specific Authentication Server Groups] ダイアログボックス （1726 ページ）に入力します。 • インターフェイス設定を編集するには、そのインターフェイス設定を選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイス設定を削除するには、そのインターフェイス設定を選択し、[行の削除（Delete Row）] ボタンをクリックします。

[IPSec] タブ（[Connection Profiles]）

[Connection Profiles] ページの [IPsec] タブを使用して、接続ポリシーに IPsec および IKE パラメータを指定します。

バージョン 4.8 以降の Security Manager では、AnyConnect に加え、標準ベースでサードパーティの IKEv2 リモート アクセス クライアントを介した VPN 接続がサポートされます。認証では、事前共有キー、証明書、拡張認証プロトコル（EAP）を介したユーザ認証などがサポートされます。

IPSec は、マルチコンテキスト モードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。Cisco Security Manager バージョン 4.17 以降、IPSec は ASA 9.9(2) 以降のマルチコンテキストデバイスでサポートされています。ただし、[接続プロファイル（Connection Profile）] > [IPSec] タブにある次の属性は、ASA 9.9(2) 以降のマルチコンテキストデバイスではサポートされていません。

- IKEv2 Mobike RRCを有効にする（Enable IKEv2 Mobike RRC）
- クライアントソフトウェアの更新テーブル（Client Software Update Table）

ナビゲーション パス

- リモートアクセス VPN：[接続プロファイル（Connection Profiles）] ページ（ [Connection Profiles] ページ （1715 ページ）を参照）から、[行の追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックし、

[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[IPSec] タブをクリックします。

- Easy VPN トポロジ：Easy VPN トポロジを選択して、ポリシー ビューまたはサイト間 VPN Manager のいずれかでサイト間 VPN Connection Profile ポリシーを選択します（[Connection Profiles] ページ （1715 ページ）を参照）。[IPSec] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）
- Easy VPN における Connection Profile ポリシーの設定 （1616 ページ）
- Easy VPN について （1599 ページ）

フィールド リファレンス

表 379 : [Connection Profiles] の [IPsec] タブ

要素	説明
IKEv1 ピア認証	
事前共有キー（Preshared Key）	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。
Trustpoint Name	トラストポイント名を定義する PKI 登録ポリシー オブジェクトの名前（トラストポイントが IKEv1 接続で設定されている場合）。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。 [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** トラストポイントを指定した場合、公開キーインフラストラクチャ ポリシーで同じ PKI 登録オブジェクトを選択する必要があります。詳細については、 リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）を参照してください。
IKEv2 ピア認証 事前共有キー、証明書、EAP などの 1 つ以上の認証オプションをリモート認証用に構成できます。	
事前共有キー（Preshared Key）	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。

要素	説明
証明書認証の有効化（Enable Certificate Authentication）	オンにすると、認証に証明書を使用できます。
EAP 認証の有効化（Enable EAP Authentication）	オンにすると、認証に EAP を使用できます。 （注） このチェックボックスをオンにした場合は、ローカル認証に証明書を使用する必要があります。EAP認証では、サーバーは証明書を使用して認証する必要があるためです。
EAP アイデンティティ要求をクライアントに送信する（Send EAP identity request to the client）	リモートアクセス VPN クライアントに EAP 認証要求を送信できます。
IKEv2 ローカル認証 ローカル認証には、事前共有キーまたはトラストポイント名を設定できます。	
事前共有キー	接続プロファイルの事前共有キー。事前共有キーの最大長は 127 文字です。確認フィールドでもう一度キーを入力します。
Trustpoint Name	トラストポイント名を定義する PKI 登録ポリシー オブジェクトの名前（トラストポイントが IKEv2 接続で設定されている場合）。トラストポイントは Certificate Authority（CA; 認証局）と ID のペアを表し、CA の ID、CA 固有の設定パラメータ、および登録されている 1 つの ID 証明書との関連付けが含まれます。 [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） リモート認証に EAP を選択した場合は、ローカル認証で証明書を使用する必要があります。
IKEv2 Mobike RRCを有効にする（Enable IKEv2 Mobike RRC）	選択すると、Mobike が有効になっている IKE/IPSEC セキュリティ アソシエーションにおけるダイナミック IP アドレス変更のリターン ルータビリティ チェックを有効にします。デフォルトでは、Mobike RRC は無効になっています。 （注） 動的 IP アドレス変更のリターン ルータビリティ チェックは、ASA 9.8.1 以降でのみイネーブルにできます。 （注） このオプションは、ASA 9.9(2) 以降のマルチコンテキストデバイスではサポートされていません。

要素	説明
IKEv2 RSA署名SHA-1を有効にする（Enable IKEv2 RSA Signature SHA-1）	IKEv2 認証の RSA 署名 SHA-1 を有効にする場合に選択します。デフォルトでは、RSA 署名 SHA-1 は無効になっています。 （注） このオプションは、Cisco Security Manager 4.19 以降および ASA 9.12(1) 以降のデバイスでサポートされています。
IKE Peer ID Validation	IKE ピア ID 検証を無視する（確認しない）か、必須とするか、または証明書によってサポートされている場合にかぎり確認するかを選択します。IKE ネゴシエーション中、ピアは互いに自身を識別する必要があります。
Enable Sending Certificate Chain	認可の証明書チェーンの送信をイネーブルにするかどうか。証明書チェーンには、ルート CA 証明書、ID 証明書、およびキー ペアが含まれます。
Enable Password Update with RADIUS Authentication	RADIUS 認証プロトコルを使用してパスワードを更新できるかどうか。詳細については、サポートされる AAA サーバ タイプ （324 ページ）を参照してください。
ISAKMP Keepalive	ISAKMP キープアライブをモニタするかどうか。[キープアライブのモニター（Monitor Keepalive）] オプションを選択した場合、デフォルトのフェールオーバーおよびルーティングのメカニズムとして IKE キープアライブを設定できます。次のパラメータを入力します。 • [信頼間隔（Confidence Interval）]：IKE キープアライブパケット送信から次の送信までのデバイスの待機時間（秒単位）。 • [再試行間隔（Retry Interval）]：デバイスがリモートピアとの IKE 接続の確立を試行する間隔（秒単位）。デフォルト値は 2 秒です。 詳細については、VPN グローバル ISAKMP/IPsec 設定 （1520 ページ）を参照してください。
[Client Software Update] テーブル	クライアント プラットフォームの VPN クライアントのリビジョン レベルおよび URL。すべての [All Windows Platforms]、[Windows 95/98/ME]、[Windows NT4.0/2000/XP]、または [VPN3002 Hardware Client] に対して別々のリビジョン レベルを設定できます。 プラットフォームにクライアントを設定するには、クライアントを選択して [行の編集（Edit Row）] ボタンをクリックし、[IPSec Client Software Update] ダイアログボックス （1734 ページ）に入力します。 （注） このオプションは、ASA 9.9(2) 以降のマルチコンテキスト デバイスではサポートされていません。

[IPSec Client Software Update] ダイアログボックス

[IPsec Client Software Update] ダイアログボックスを使用して、VPN クライアントの特定のリビジョン レベルおよびイメージ URL を設定します。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [IPSec] タブを開き（[IPSec] タブ（[Connection Profiles]） （1730 ページ）を参照）、[クライアントソフトウェアの更新（Client Software Update）] テーブルからクライアントタイプを選択して、[行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *380 : [IPSec Client Software Update]* ダイアログボックス

要素	説明
Client Type	変更するクライアントのタイプ。
Client Revisions	クライアントのリビジョン レベル。
イメージ URL	クライアント ソフトウェア イメージの URL。

[SSL] タブ（[Connection Profiles]）

[Connection Profile] ダイアログボックスの [SSL] タブを使用して、Connection Profile ポリシーの WINS サーバの設定、SSL VPN エンドユーザ ログイン Web ページのカスタマイズ済みルックアンド フィールの選択、クライアント アドレス割り当てに使用する DHCP サーバの選択、およびインターフェイスとクライアント IP アドレス プールの関連付けの確立を行います。接続プロファイル エイリアスなどの一部の設定は、リモート アクセス IKEv2 IPsec VPN には適用されますが、これらの設定は、リモート アクセス IKEv1 IPSec VPN または Easy VPN トポロジには適用されません。

次のポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN の [SSL] タブでサポートされています。

- Radius-Reject-Message
- Connection alias
- Group-url
- Group-alias

ナビゲーション パス

リモートアクセス VPN のみ：[接続プロファイル（Connection Profiles）] ページ（[Connection Profiles] ページ （1715 ページ）を参照）から、[行の追加（Add Row）]（+）ボタンをクリックするか、プロファイルを選択して、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、

[接続プロファイル（Connection Profiles）] ダイアログボックスを開きます。[SSL] タブをクリックします。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+）　（1713 ページ）
- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化　（1825 ページ）
- ネットワーク/ホストオブジェクトについて　（391 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定　（1811 ページ）

フィールド リファレンス

表 381 : [Connection Profile] の [SSL] タブ

要素	説明
WINS Servers List	CIFS 名前解決に使用する Windows Internet Naming Server（WINS）サーバ リストの名前。[選択（Select）] をクリックして WINS サーバーリストからポリシーオブジェクトを選択するか、または新しいオブジェクトを作成します。 SSL VPN は、CIFS プロトコルを使用して、リモート システムのファイルにアクセスまたは共有します。Windows コンピュータの名前を使用してそのコンピュータへのファイル共有接続を試行する場合、指定するファイル サーバは、ネットワーク上のリソースを識別する特定の WINS サーバ名と対応しています。 WINS サーバ リストは、Windows ファイル サーバ名を IP アドレスに変換するために使用される WINS サーバのリストを定義するものです。セキュリティ アプライアンスは、WINS サーバを照会して、WINS 名を IP アドレスにマップします。少なくとも 1 台の WINS サーバを設定する必要があります。冗長性のために最大 3 台設定できます。セキュリティ アプライアンスは、リストの最初のサーバを WINS/CIFS 名前解決に使用します。クエリーが失敗すると、次のサーバーが使用されます。

要素	説明
DNS Group	SSL VPN トンネル グループに使用する DNS グループ。DNS グループは、ホスト名をトンネル グループに適した DNS サーバに解決します。リストから目的のグループを選択します。DefaultDNS グループは、デバイスで常に使用できるデフォルト グループです。 ヒント　DNS グループは、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS] ポリシーで定義されます。DNS ポリシーを使用して、グループで定義されているサーバを変更するか、グループを追加または削除します。[DNS] ページ （2616 ページ）を参照してください。
Portal Page Customization	VPN のデフォルト ポータル ページを定義する [SSL VPN Customization] ポリシー オブジェクトの名前。このプロファイルでは、リモート ユーザが SSL VPN 上で使用可能なすべてのリソースにアクセスできるようにするためのポータル ページの外観を定義します。[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注）　カスタマイゼーション プロファイルとグループの組み合わせを使用することで、個々のグループにそれぞれ異なるログイン ウィンドウを設定できます。たとえば、salesgui という名前のカスタマイゼーション プロファイルを作成してあるとすると、そのカスタマイゼーション プロファイルを使用する sales という名前の SSL VPN グループを作成できます。次に、[SSL VPN] > [Settings] タブのグループ ポリシー オブジェクトで、SSL VPN カスタマイゼーション オブジェクトを指定します（ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照）。
SAML ID プロバイダー	[SAML IDプロバイダー（SAML Identity Provider）] を選択します。SAML IDプロバイダーは、トンネルグループで適用されるまで使用されません。詳細については、SAML ID プロバイダの構成 （415 ページ）を参照してください。
Override SVC Download (ASA 8.0(2) 以降のみ)	特定のトンネルグループでログインしているクライアントレス ユーザには、ダウンロード プロンプトが終了するまで待たせることなく、クライアントレス SSL VPN ホームページを表示するかどうかを指定します。表示する場合、これらのユーザには即時にクライアントレス SSL VPN ホームページが表示されます。
Reject Radius Message (ASA 8.0(2) 以降のみ)	認証の失敗に関する RADIUS メッセージをリモート ユーザに表示するかどうかを指定します。

要素	説明
[Connection Aliases] テーブル	トンネル グループを参照できる代替名のリスト。このステータスは、名前がイネーブル（使用できる）またはディセーブル（使用できない）かを示します。 グループ エイリアスにより、ユーザがトンネル グループの参照に使用できる 1 つ以上の代替名が作成されます。この機能は、同じグループが複数の通常名（「Devtest」や「QA」など）で指定されている場合に便利です。トンネル グループの実際の名前をこのリストに表示する場合は、その名前をエイリアスとして指定する必要があります。ここで指定したグループ エイリアスは、ログイン ページに表示されます。各トンネル グループには複数のエイリアスがあることも、エイリアスがまったくないこともあります。 • エイリアスを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックして、[Add Connection Alias]/[Edit Connection Alias] ダイアログボックス （1738 ページ）に入力します。 • エイリアスを編集するには、エイリアスを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • エイリアスを削除するには、エイリアスを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。
[Group URLs] テーブル	トンネル グループ接続プロファイルに関連付けられる URL のリスト。このステータスは、URL が使用できるかどうかを示します。使用できる場合、ユーザは、URL を使用できるため、ログイン中にグループを選択する必要がなくなります。 1 つのトンネル グループに対して複数の URL を設定できます。または、URL を設定しないこともできます。各 URL は、個別にイネーブルまたはディセーブルにできます。URL ごとに、HTTP または HTTPS プロトコルを使用して URL 全部を指定することにより、個別の指定を使用する必要があります。 • URL を追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックして、[Add Connection URL]/[Edit Connection URL] ダイアログボックス （1739 ページ）に入力します。 • URL を編集するには、URL を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • URL を削除するには、URL を選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

要素	説明
デフォルトの Citrix クライアントプロファイル （ASA 9.1(4) 以降のみ）	トンネルネゴシエーション時に特定のトンネルグループが識別されない場合にこの接続プロファイルを Citrix クライアントに使用するデフォルトの接続プロファイルにするかどうかを定義します。 （注） デフォルトの Citrix クライアントプロファイルとして設定できる接続プロファイルは 1 つだけです。ある接続プロファイルがすでにデフォルトの Citrix クライアントプロファイルとして設定されている場合に、別の接続プロファイルをデフォルトとして設定しようとすると、警告メッセージが表示されます。操作を続行すると、選択した接続プロファイルがデフォルトの Citrix クライアントプロファイルになり、デフォルトの Citrix クライアントプロファイルとして選択されていた他の接続プロファイルは選択解除されます。
Disable CSD （ASA 8.2(0) 以降のみ） [クライアントレスと AnyConnect の両方（Both Clientless and AnyConnect）] [AnyConnect のみ（AnyConnect only）]	この接続プロファイルで Cisco Secure Desktop（CSD）をディセーブルにするかどうかを指定します。Security Manager は、ASA ソフトウェアバージョン 8.2(0) 以降を実行しているすべてのデバイスでこの機能をサポートします。 （注） CSD を無効にする場合、デフォルトでは、Security Manager は「SSL クライアントレス VPN と AnyConnect の両方」のオプションを選択します。

[Add Connection Alias]/[Edit Connection Alias] ダイアログボックス

[Add Connection Alias]/[Edit Connection Alias] ダイアログボックスを使用して、SSL または IKEv2 IPsec VPN 接続プロファイルの接続エイリアスを作成または編集します。接続エイリアスを指定すると、ユーザがトンネル グループの参照に使用できる 1 つ以上の代替名が作成されます。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [SSL] タブ（ [SSL] タブ（[Connection Profiles]） （1734 ページ）を参照）を開き、[接続エイリアス（Connection Alias）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブルからエイリアスを選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 382 : [Add Connection Alias]/[Edit Connection Alias] ダイアログボックス

要素	説明
有効	接続エイリアスをイネーブルにするかどうか指定します。エイリアスを使用するユーザには、エイリアスをイネーブルにする必要があります。
Connection Alias	接続プロファイルの代替名。 ここで指定する接続エイリアスは、ユーザーのログインページにあるリストに表示されます。

[Add Connection URL]/[Edit Connection URL] ダイアログボックス

このダイアログボックスを使用して、トンネル グループに着信 URL を指定します。トンネル グループ内の接続 URL がイネーブルになっている場合、ユーザがその URL を使用して接続すると、セキュリティ アプライアンスにより、関連付けられたトンネル グループが選択され、ログイン ウィンドウ内にユーザ名フィールドとパスワード フィールドだけが表示されます。

ヒント

- 1 つのグループに対して複数の URL またはアドレスを設定できます（何も設定しないこともできます）。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにできます。
- 同じ URL またはアドレスを複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネル グループの URL またはアドレスを受け入れる前に、URL またはアドレスの一意性を検証します。

ナビゲーション パス

[接続プロファイル（Connection Profiles）] ダイアログボックスの [SSL] タブ（[SSL] タブ（[Connection Profiles]） （1734 ページ）を参照）を開き、[グループURL（Group URLs）] テーブルの下の [行の追加（Add Row）] をクリックするか、テーブルから URL を選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 383 : [Add Connection URL]/[Edit Connection URL] ダイアログボックス

要素	説明
有効	接続エイリアスをイネーブルにするかどうか指定します。エイリアスを使用するユーザには、エイリアスをイネーブルにする必要があります。
Connection URL	リストからプロトコル（[http] または [https]）を選択し、接続の着信 URL を指定します。

リモート アクセス VPN のグループ ポリシーの設定

[Group Policies] ページでは、ASA リモート アクセス VPN 接続プロファイルに定義されているユーザ グループ ポリシーを参照できます。このページから、新しい ASA ユーザ グループを指定したり、既存の ASA ユーザ グループを編集したりできます。接続プロファイルを作成するときに、デバイスで使用されていないグループ ポリシーを指定した場合、このグループ ポリシーは自動的に [Group Policies] ページに追加されます。接続プロファイルを作成する前に、このポリシーに追加する必要はありません。接続プロファイルの作成については、接続プロファイルの設定（ASA、PIX 7.0+）（1713 ページ）を参照してください。

グループ ポリシーの詳細については、グループ ポリシーについて（ASA）（1741 ページ）を参照してください。

ヒント　ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

テーブル内の各行は、ASA グループ ポリシー オブジェクトを表します。これには、リモート アクセス VPN 接続プロファイルに割り当てられているポリシー オブジェクトの名前、そのポリシー オブジェクトが ASA デバイス自体（[Internal]）または AAA サーバ（[External]）のいずれに格納されるか、および、そのグループが IKEv1（IPsec）、IKEv2（IPsec）または SSL、あるいはすべてのタイプの VPN に対応しているかが表示されます。外部グループの場合、プロトコルは認識されず、N/A として表示されます。

- ASA グループ ポリシー オブジェクトを追加するには、[行の追加（Add Row）]ボタンをクリックします。これにより、オブジェクトセレクタが開きます。ここから、既存のポリシー オブジェクトを選択するか、[作成（Create）] ボタンをクリックして新しいオブジェクトを作成します。グループ ポリシーの作成の詳細については、グループ ポリシーの作成（ASA、PIX 7.0+）（1743 ページ）を参照してください。

（注）　名前に DfltGrpPolicy を含むグループ ポリシーを複数作成することはできません。DfltGrpPolicy は、デバイスで定義されているデフォルトのポリシーです。Security Manager が、リモートアクセスポリシー検出中にこのグループを検出すると、このグループは、リスト内の <device_display_name> DfltGrpPolicy という名前の下に表示されます。設定をデバイスに展開すると、DfltGrpPolicy が正しく更新されるため、表示名プレフィックスが削除されます。詳細については、リモートアクセス VPN ポリシーの検出（1669 ページ）を参照してください。

- オブジェクトを編集するには、オブジェクトを選択して [行の編集（Edit Row）] ボタンをクリックし、[ASA Group Policies] ダイアログボックス（1918 ページ）を開きます。

- オブジェクトをポリシーから削除するには、オブジェクトを選択して [行の削除（Delete Row）]ボタンをクリックします。関連付けられたポリシーオブジェクトは、このポリシーから取り除かれるだけで、削除されません。

（注） デフォルトのグループ ポリシーを削除することはできません。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [グループポリシー（Group Policies）]** を選択します。
- （ポリシービュー）ポリシーセレクタから、**[リモートアクセス VPN（Remote Access VPN）] > [グループポリシー（ASA）（Group Policies (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） Cisco Security Manager 4.24 以降では、ASA デバイス検出時に [グループポリシー（Group Policy）] に vpn-tunnel-protocol を設定しない場合、CSM は [DfltGrpPolicy] から vpn-tunnel-protocol 値を継承することで [グループポリシー（Group Policy）] の検出を行います。

グループ ポリシーについて（ASA）

リモート アクセス IPSec VPN 接続またはリモート アクセス SSL VPN 接続を設定する場合は、リモート クライアントが属するユーザ グループを作成する必要があります。ユーザ グループポリシーは、リモート アクセス VPN 接続のためのユーザ指向の属性と値のペアのセットで構成され、デバイス内部（ローカル）または外部の AAA サーバに保存されます。接続プロファイルは、接続確立後のユーザ接続条件を設定するユーザ グループ ポリシーを使用します。グループポリシーを使用すると、ユーザーまたはユーザーのグループに属性セット全体を適用できるので、ユーザーごとに各属性を個別に指定する必要がありません。

ヒント ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

ASA ユーザ グループは、次の属性で構成されます。

- グループポリシーソース。ユーザーグループの属性および値を、セキュリティアプライアンスの内部（ローカル）に格納するか、外部の AAA サーバーに格納するかどうかを指定します。ユーザ グループを外部タイプとした場合は、そのユーザ グループにその他の設

定をする必要はありません。詳細については、[ASA Group Policies] ダイアログボックス（1918 ページ）を参照してください。

- クライアント設定。Easy VPN またはリモート アクセス VPN でユーザ グループの Cisco クライアント パラメータを指定します。詳細については、ASA グループ ポリシーのクライアント設定 （1925 ページ）を参照してください。
- クライアント ファイアウォール属性。Easy VPN またはリモート アクセス VPN で VPN クライアントのファイアウォール設定を行います。詳細については、ASA グループ ポリシーのクライアント ファイアウォール属性 （1926 ページ）を参照してください。
- ハードウェア クライアント属性。Easy VPN またはリモート アクセス VPN で VPN 3002 ハードウェア クライアント設定を行います。詳細については、ASA グループ ポリシーのハードウェア クライアント属性 （1928 ページ）を参照してください。
- IPsec 設定。Easy VPN またはリモート アクセス VPN のユーザ グループにトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定します。詳細については、ASA グループ ポリシーの IPSec 設定 （1930 ページ）を参照してください。
- ASA ユーザ グループのクライアントレス設定。SSL VPN で企業ネットワークへのクライアントレス アクセス モードを設定します。詳細については、ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）を参照してください。
- ASA ユーザ グループのフル クライアント設定。SSL VPN で企業ネットワークへのフル クライアント アクセス モードを設定します。詳細については、ASA グループ ポリシーの SSL VPN フル クライアント設定 （1945 ページ）を参照してください。
- 一般設定。SSL VPN でのクライアントレス/ポート転送に必要です。詳細については、ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照してください。
- DNS/WINS 設定。DNS サーバと WINS サーバ、および ASA ユーザ グループに関連付けられたリモート クライアントにプッシュされるドメイン名を定義します。詳細については、ASA グループ ポリシーの DNS/WINS 設定 （1963 ページ）を参照してください。
- スプリット トンネリング。条件に応じて、リモート クライアントがパケットを暗号化された形式で IPsec VPN または SSL VPN トンネル上を送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。詳細については、ASA グループ ポリシーのスプリット トンネリング設定 （1965 ページ）を参照してください。
- ASA ユーザ グループのリモート アクセスまたは SSL の VPN セッション接続設定。詳細については、ASA グループ ポリシーの接続設定 （1967 ページ）を参照してください。

関連項目

- グループ ポリシーの作成（ASA、PIX 7.0+） （1743 ページ）
- リモート アクセス VPN のグループ ポリシーの設定 （1740 ページ）

グループ ポリシーの作成（ASA、PIX 7.0+）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[Group Policies] ページを使用して、リモート アクセス IPSec VPN で使用される ASA または PIX 7.0+ デバイス、あるいはリモート アクセス SSL VPN で使用される ASA デバイスのグループ ポリシーを作成します。グループ ポリシーについては、次を参照してください。

- グループ ポリシーについて（ASA） （1741 ページ）
- リモート アクセス VPN のグループ ポリシーの設定 （1740 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA または PIX 7.0+ デバイスを選択し、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [グループポリシー（ASA） （Group Policies (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Group Policies] ページが開きます。このテーブルには、既存のグループ ポリシーと、それらがデバイスで内部的に定義されるか AAA サーバで外部的に定義されるか、およびグループのプロトコル（IKEv1（IPsec）、IKEv2（IPsec）、または SSL）のリストが示されます。

ステップ 2 [行の追加（Add Row）]（+）をクリックするとダイアログボックスが開き、このダイアログボックスで、定義済みの ASA ユーザー グループ オブジェクトのリストからユーザーグループを選択したり、必要に応じて新しいユーザーグループを作成したりできます。新しいグループを作成するには、ダイアログボックスの [作成（Create）]（+）ボタンをクリックします。

ステップ 3 必要な ASA ユーザーグループをリストから選択して [OK] をクリックします。必要なグループがすでに存在する場合は終了です。

必要な ASA ユーザーグループが存在しない場合、[作成（Create）]（+）をクリックして作成します。[Add ASA User Group] ダイアログボックスが開き、ASA ユーザ グループ オブジェクトに設定可能な設定のリストが表示されます。このダイアログボックスの要素の詳細については、[ASA Group Policies] ダイアログボックス （1918 ページ）を参照してください。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 ASA ユーザーグループの属性と値をデバイスのローカルに保存するか、外部サーバーに保存するかを選択します。

（注） ASA ユーザーグループの属性を外部サーバーに保存することを選択した場合は、テクノロジー設定を行う必要はありません。認証に使用する AAA サーバーグループと AAA サーバーのパスワードを指定して [OK] をクリックし、オブジェクトセレクタでグループを選択して [OK] をクリックすることで、ポリシーにグループを追加します。

ステップ 6 ASA ユーザーグループの属性をデバイスのローカルに保存することを選択した場合は、[テクノロジー（Technology）] リストから、ASA ユーザーグループを作成する VPN のタイプを選択します。

- [Easy VPN/IPSec IKEv1]：IKE バージョン 1 ネゴシエーションを使用するリモート アクセス IPsec VPN 用。
- [Easy VPN/IPSec IKEv2]：（ASA のみ）IKE バージョン 2 ネゴシエーションを使用するリモートアクセス IPsec VPN 用。
- [SSL クライアントレス（SSL Clientless）]：（ASA のみ）SSL VPN、すべてのアクセスモード用（クライアントレスだけではない）。

ステップ 7 Easy VPN/IPSec IKEv1 および Easy VPN/IPSec IKEv2 のユーザ グループを設定するには、[Settings] ペインの [Easy VPN/IPSec VPN] フォルダから次のことを実行します。

a) [クライアント設定（Client Configuration）] を選択して、Cisco クライアントパラメータを設定します。これらの設定の詳細については、ASA グループ ポリシーのクライアント設定 （1925 ページ）を参照してください。

b) [クライアントのファイアウォール属性（Client Firewall Attributes）] を選択して、VPN クライアントのファイアウォール設定を行います。これらの設定の詳細については、ASA グループ ポリシーのクライアント ファイアウォール属性 （1926 ページ）を参照してください。

c) [ハードウェアクライアント属性（Hardware Client Attributes）] を選択して、VPN 3002 ハードウェア クライアント設定を行います。これらの設定の詳細については、ASA グループ ポリシーのハードウェア クライアント属性 （1928 ページ）を参照してください。

d) [IPsec] を選択して、トンネリングプロトコル、フィルタ、接続設定、およびサーバーを指定します。これらの設定の詳細については、ASA グループ ポリシーの IPSec 設定 （1930 ページ）を参照してください。

ステップ 8 SSL VPN のユーザ グループを設定するには、[Settings] ペインの SSL VPN フォルダから次の手順を実行します。

a) [クライアントレス（Clientless）] を選択して、SSL VPN で企業ネットワークへのクライアントレス アクセスモードを設定します。これらの設定の詳細については、ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）を参照してください。

b) [フルクライアント（Full Client）] を選択して、SSL VPN で企業ネットワークへのフル クライアント アクセスモードを設定します。これらの設定の詳細については、ASA グループ ポリシーの SSL VPN フル クライアント設定 （1945 ページ）を参照してください。

c) [設定（Settings）] を選択して、SSL VPN のクライアントレス アクセス モードおよびシンクライアント（ポートフォワーディング）アクセスモードに必要な全般設定を行います。これらの設定の詳細については、ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照してください。

ステップ 9 [Settings] ペインの Easy VPN/IPSec IKEv1 または IKEv2 VPN および SSL VPN 設定で、ASA ユーザ グループに次の設定を指定します。

a) [DNS/WINS] を選択して、DNS サーバーと WINS サーバー、および ASA ユーザーグループに関連付けられたクライアントにプッシュされるドメイン名を定義します。これらの設定の詳細については、ASA グループ ポリシーの DNS/WINS 設定 （1963 ページ）を参照してください。

b) [スプリットトンネリング（Split Tunneling）] を選択して、条件に応じてリモートクライアントが暗号化されたパケットをセキュアトンネル経由でセントラルサイトに送信できるようにし、同時にネットワーク インターフェイスを介したインターネットへのクリアテキストトンネルを許可します。これらの設定の詳細については、ASA グループ ポリシーのスプリット トンネリング設定 （1965 ページ）を参照してください。

c) [接続設定（Connection Settings）] を選択して、セッション、アイドルタイムアウト、およびバナーテキストなど、ASA ユーザーグループの SSL VPN 接続設定を行います。これらの設定の詳細については、ASA グループ ポリシーの接続設定 （1967 ページ）を参照してください。

ステップ 10 [OK] をクリック

ステップ 11 ASA ユーザーグループをリストから選択して [OK] をクリックします。

SSL VPN サーバー検証（ASA）について

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために CA が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が付属しています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

ブラウザが証明書管理の機能を提供するのと同様に、ASA も信頼できる証明書のプール管理機能の形式を提供します（trustpools）。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には、Web ブラウザで提供されるのと同様のデフォルトの証明書のバンドルが含まれますが、管理者がアクティブにするまで非アクティブとなります。

（注） すでに Cisco IOS の trustpools に精通している場合、ASA バージョンが、似ているが同じではないことがわかります。

信頼できる証明書の管理の詳細については、次のトピックを参照してください。

- SSL VPN サーバー検証の設定（ASA） （1805 ページ）
- 信頼できるプール設定の設定（ASA） （1746 ページ）
- Trustpool Manager の使用 （1748 ページ）

信頼できるプール設定の設定（ASA）

[信頼できるプールの設定（Trusted Pool Settings）] ページを使用して、証明書失効のオプションを設定します。Trustpool Manager を起動することもできます。

ナビゲーション パス

（デバイスビューのみ）ASA デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [信頼できるプール（Trusted Pool）]** を選択します。

関連項目

- SSL VPN サーバー検証の設定（ASA）　（1805 ページ）
- Trustpool Manager の使用　（1748 ページ）

フィールド リファレンス

表 *384 : [*信頼できるプール（*Trusted Pool*）*]* ページ

要素	説明
失効チェック	証明書の失効をチェックするかどうかを指定します。適切なオプションを選択します。 • [証明書をチェックする（Check Certificates）] このオプションを選択する場合は、適切な方法（CRL または OCSP）を選択し、[>>] をクリックして、右側のボックスに移動して、失効に使用する方法を 1 つ、または複数指定します。 （注）　いずれか一方または両方の方法を選択できます。両方の方法を選択する場合は、使用する順序で方法を追加します。 • [証明書をチェックしない（Do not check Certificates）]
証明書マップの設定	必要に応じて、次のリストからマップを選択して、証明書マップのオーバーライドオプションを指定します。各リストには、デバイスに設定されているすべての証明書マップが含まれます。 • [期限切れの証明書を許可（Allow Expired Certificates）]：期限切れの証明書を許可する証明書マップを選択します。 • [失効チェックをスキップ（Skip Revocation Check）]：失効チェックをスキップする証明書マップを選択します。

要素	説明
CRL Options	証明書失効リストを管理するためのオプションを指定します。 • [キャッシュ更新時間（Cache Refresh Time）]：CRL が古すぎて信頼できないと ASA が判断するまでの分数（1 ～ 1440）。デフォルト値は 60 分です。 • [次のCRL更新を実施（Enforce next CRL update）]：ASA が次の CRL 更新を実施する必要があるかどうかを指定します。
証明書有効期限のアラート（Certificate Expiration Alerts）	バージョン 4.9 以降、Cisco Security Manager では、24 時間ごとに、トラストポイントにおけるすべての CA および ID 証明書の有効期限のチェックが可能になっています。証明書の有効期限がまもなく切れる場合は、syslog がアラートとして発行されます。リマインダおよび繰り返しの間隔を設定できます。この機能は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスでのみサポートされています。 [開始（Begin）]：最初のアラートが送信される有効期限までの日数を入力します。範囲は 1 ～ 90 日です。デフォルトでは、リマインダは有効期限の 60 日前に開始されます。 [繰り返し（Repeat）]：証明書が更新されない場合にアラートが繰り返される頻度を日数で入力します。範囲は 1 ～ 14 日です。デフォルトでは、リマインダは 7 日ごとに送信されます。

要素	説明
自動インポート	バージョン 4.10 以降、Cisco Security Manager では Trustpool 証明書バンドルの自動インポートが有効になります。自動インポートを有効にすると、Trustpool 証明書バンドルのダウンロードとインポートに ASA が使用する URL を設定できます。この機能は、ASA ソフトウェアバージョン 9.5(2) 以降を実行しているデバイスでのみサポートされます。 バージョン 4.13 以降、Cisco Security Manager には、ASA が宛先 URL を識別するために使用できる送信元インターフェイスオプションが用意されています。この機能は、9.7.1 より前の ASA バージョンではサポートされていません。 [インターフェイス（Interface）]：[選択（Select）] ボタンをクリックして、インターフェイスを選択します。設定されたインターフェイスが管理専用の場合、宛先 URL は管理 VRF を介してルーティングされます。非管理インターフェイスの場合、URL はデータ VRF を介してルーティングされます。インターフェイスが指定されていない場合、管理 VRF とデータ VRF の両方のルーティングテーブルがポーリングされ、URL に到達するルートが識別されます。 [URLからインポート（Import from a URL）：ASA が Trustpool 証明書バンドルをダウンロードする URL を入力します。 [ダウンロード時刻（Download Time）]：ASA が証明書バンドルをダウンロードする時刻を入力します。インポートは、ここで指定した時刻に毎日実行されます。 URL のデフォルト値は http://www.cisco.com/security/pki/ios_core.p7b で、ダウンロード時刻のデフォルト値は 22:00:00 です。
Trustpool Managerの起動（Launch Trustpool Manager）	Trustpool 証明書の管理に使用される Trustpool Manager を起動します。Trustpool Manager を使用して、以下を実行できます。 詳細については、Trustpool Manager の使用 （1748 ページ）を参照してください。

Trustpool Manager の使用

Trustpool Manager を使用して、trustpool に含まれる証明書を管理します。Trustpool Manager は、次の機能を提供します。

- trustpool の更新
- 証明書のバンドルのインポート
- 証明書のバンドルのエクスポート
- trustpool からの証明書の削除

ナビゲーション パス

（デバイスビューのみ）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [Trusted Pool] を選択し、次に [Trustpool Managerの起動（Launch Trustpool Manager）] をクリックします。

trustpool の更新

次のいずれかの条件が満たされる場合は、trustpool を更新する必要があります。

- trustpool の証明書が期限切れまたは再発行されている。
- 公開された CA 証明書のバンドルに、特定のアプリケーションで必要な追加の証明書が含まれている。

trustpool の証明書を更新するには、[証明書の更新（Refresh Certificates）] をクリックします。

証明書のバンドルのインポート

次の形式のいずれかで、さまざまな場所から個々の証明書または証明書のバンドルをインポートできます。

- pkcs7 構造でラップされた DER 形式の x509 証明書
- PEM 形式（PEM ヘッダーに囲まれた）の連結した x509 証明書のファイル

証明書またはバンドルをインポートするには、次の手順を実行します。

1. [Import Bundle] をクリックします。
2. バンドルの場所を選択します。
   - [シスコの公開署名済みルートファイル配布からのインポート（Import from Cisco published signed root file distribution）]：公開配布サイトからインポートするには、このオプションを選択します。
   - [URLからインポート（Import from a URL）]：バンドルがサーバーでホストされている場合は、このオプションを選択します。リストからプロトコルを選択し、ボックスに URL を入力します。
   - [デバイスでファイルをバンドル（Bundle file on device）]：バンドルが ASA フラッシュファイルシステムに保存されている場合はこのオプションを選択し、バンドルへのパスを入力します。
   - [バンドルファイルを選択（Select bundle file）]：バンドルがマシンに保存されている場合は、[ファイルからインポート（Import from a file）]をクリックし、[ローカルファイルを参照（Browse Local Files）] をクリックして、バンドルに移動します。
3. 次のインポートオプションを指定します。
   - [インポートする前にすべての証明書をクリア（Clear all certificates before import）]：バンドルをインポートする前に trustpool をクリアするかどうか。

- [署名の検証が失敗または実行できない場合にバンドルをインポートし続ける（Continue to import the bundle if signature validation fails or can't be performed）]：署名を検証できない場合にインポートを続行するかどうか。

4. [インポート（Import）] をクリックします。

証明書のバンドルのエクスポート

trustpool を正しく設定したら、プールをエクスポートする必要があります。これにより、このポイントまで（たとえばエクスポート後に trustpool に追加された証明書を削除する場合など）trustpool を復元できます。Security Manager サーバーファイルシステムまたはローカルファイルシステムにプールをエクスポートできます。

証明書のバンドルをエクスポートするには、次の手順を実行します。

1. [バンドルのエクスポート（Export Bundle）] をクリックします。
2. [参照（Browse）] をクリックします。
3. エクスポート先のファイルシステム（ローカルマシンまたは Security Manager サーバー）に対応するタブを選択します。
4. trustpool を保存するフォルダに移動します。
5. [File name] ボックスに、trustpool の一意の覚えやすい名前を入力します。
6. [保存（Save）] をクリックします。

Trustpool からの証明書の削除

次の方法を使用して、trustpool から証明書を削除できます。

- 個別の証明書を削除するには、証明書を選択して [削除（Delete）] をクリックします。
- デフォルトのバンドルの一部ではないすべての証明書を削除するには、[Trustpoolのクリア（Clear Trustpool）] をクリックします。

（注） trustpool をクリアする前に、必要に応じて現在の設定を復元できるように、現在の trustpool をエクスポートする必要があります。

関連項目

- SSL VPN サーバー検証の設定（ASA） （1805 ページ）
- 信頼できるプール設定の設定（ASA） （1746 ページ）

[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス

[スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックスを使用して、証明書のユーザー名のマッピングに使用するスクリプトを定義します。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [証明書スクリプトのユーザー名（Username from Cert Scripts）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [証明書スクリプトのユーザー名（ASA）（Username from Cert Scripts (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *385 : [スクリプトの追加/編集（Add/Edit Scripts）] ダイアログボックス*

要素	説明
スクリプト名（Script Name）	スクリプトの名前を指定し、トンネルグループ AAA 認証および許可でスクリプトを使用します。スクリプト名は、認証と許可で異なる場合があります。ここでスクリプトを定義すると、CLI で同じスクリプトを使用してこの機能を実行できます。
スクリプトパラメータの選択（Select Script Parameters）	スクリプトの属性および内容を指定します。
ユーザー名の値（Value for Username）	ユーザー名（サブジェクト DN）として使用する標準的な DN 属性のドロップダウンリストから属性を選択します。
フィルタリングなし（No Filtering）	指定した DN 名全体を使用することを指定します。
部分文字列によるフィルタ処理（Filter by Substring）	開始インデックス（一致する最初の文字の文字列内の位置）および終了インデックス（検索する文字列数）を指定します。このオプションを選択する場合、開始インデックスは、空白にはできません。終了インデックスを空白にするとデフォルトは-1 となり、文字列全体が一致するかどうか検索されます。

要素	説明
正規表現でフィルタ処理（Filter by Regular Expression）	検索に適用する正規表現を [正規表現（Regular Expression）] フィールドに入力します。一般的な正規表現の演算子が適用されます。
カスタムスクリプトをLUA形式で使用（Use Custom Script in LUA format）	検索フィールドを解析するために、LUA プログラム言語で記述されたカスタムスクリプトを指定します。このオプションを選択すると、カスタム LUA スクリプトを入力できるフィールドが使用可能になります。 以下は、LUA 形式のカスタムスクリプトの例です。 • "return findpattern(cert.subject.cn,"%a+")" • local a,b,c; a,b,c = string.find(cert.subject.fulldn, ',cn=(.+),cn=Users'); cを返します。 （注） LUA では、大文字と小文字が区別されます。 次の表に LUA スクリプトで使用可能な属性名と属性の説明を示します。

表 *386 : LUA* スクリプトの属性

属性	説明
cert.subject.c	Country
cert.subject.cn	Common Name
cert.subject.dnq	DN 修飾子
cert.subject.ea	電子メール アドレス
cert.subject.genq	世代修飾子
cert.subject.gn	名
cert.subject.i	イニシャル
cert.subject.l	地名
cert.subject.n	名前
cert.subject.o	マニュアルの構成
cert.subject.ou	組織単位
cert.subject.ser	サブジェクト シリアル番号

属性	説明
cert.subject.sn	姓
cert.subject.sp	州/県
cert.subject.t	Title
cert.subject.uid	ユーザー ID
cert.issuer.c	Country
cert.issuer.cn	Common Name
cert.issuer.dnq	DN 修飾子
cert.issuer.ea	電子メール アドレス
cert.issuer.genq	世代修飾子
cert.issuer.gn	名
cert.issuer.i	イニシャル
cert.issuer.l	地名
cert.issuer.n	名前
cert.issuer.o	マニュアルの構成
cert.issuer.ou	組織単位
cert.issuer.ser	発行元シリアル番号
cert.issuer.sn	姓
cert.issuer.sp	州/県
cert.issuer.t	Title
cert.issuer.uid	ユーザー ID
cert.serialnumber	証明書シリアル番号
cert.subjectaltname.upn	ユーザー プリンシパル名

IPSec VPN ポリシーの使用

IPSec VPN に対しては、特定のポリシーを設定する必要があります。次のトピックでは、これらのリモート アクセス IPsec VPN ポリシーについて説明します。ただし、IKE プロポーザル ポリシーは、IKE プロポーザルの設定 （1488 ページ）で説明します。

ここでは、次の内容について説明します。

• Certificate to Connection Profile Map ポリシーの設定（ASA）　（1754 ページ）
• リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）（1759 ページ）

Certificate to Connection Profile Map ポリシーの設定（ASA）

Certificate to Connection Profile Map ポリシーは、リモート アクセス IKEv1 IPSec VPN の ASA デバイスでの拡張証明書認証に使用されます。これらは、リモート アクセス IKEv2 IPSec または SSL VPN では使用されません。

Certificate to Connection Profile Map ポリシーにより、指定したフィールドに基づいて、ユーザーの証明書を権限グループと照合するルールを定義できます。認証を確立するため、証明書の任意のフィールドを使用することも、またはすべての証明書ユーザが権限グループを共有することもできます。グループは、DN ルール、[Organization Unit (OU)] フィールド、IKE ID、またはピア IP アドレスから照合できます。これらの方式のいずれかまたはすべてを使用できます。

証明書の DN フィールドに基づいてユーザ権限グループを照合するには、照合するフィールドを指定したルールをグループに定義し、その選択グループに対して各ルールをイネーブルにします。接続プロファイルにルールを作成するには、設定に接続プロファイルが存在している必要があります。

ここでは、ASA サーバデバイスに接続を試みるリモート クライアントの Certificate to Connection Profile Map ポリシーを設定する方法について説明します。

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ポリシー（Policies）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ポリシー（Policies）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Certificate to Connection Profile Map Policies] ページが開きます。

ステップ 2　次のいずれか、またはすべてのオプションを選択して、認証を確立し、クライアントをマッピングする接続プロファイル（トンネル グループ）を決定します。

- [設定されているルールを使用して証明書をグループと照合（Use Configured Rules to Match a Certificate to a Group）]：[証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ルール（Rules）] ポリシーで定義されているルールを使用します。ルールの設定については、証明書/接続プロファイル マップ ルールの設定（ASA）　（1755 ページ）を参照してください。

- [証明書の組織ユニット（OU）フィールドを使用してグループを決定（Use Certificate Organization Unit (OU) Field to Determine the Group）]：クライアント証明書の組織ユニット（OU）フィールドを使用します。
- [IKE ID を使用してグループを決定（Use IKE Identify to Determine the Group）]：IKE ID を使用します。
- [ピアの IP アドレスを使用してグループを決定（Use Peer IP address to Determine the Group）]：ピアの IP アドレスを使用します。
- [グループ URL と証明書マップが異なる接続プロファイルと一致する場合はグループ URL を使用する（Use Group URL if Group URL and Certificate Map match different Connection profiles）] は、マルチコンテキストモードの ASA 9.5（2）リモートアクセス VPN でサポートされます。

証明書/接続プロファイル マップ ルールの設定（ASA）

証明書/接続プロファイルマップを設定して、[設定されているルールを使用して証明書をグループと照合（Use Configured Rules to Match a Certificate to a Group）]（Certificate to Connection Profile Map ポリシーの設定（ASA） （1754 ページ）を参照）オプションを選択した場合、ユーザ証明書に基づいたユーザと接続プロファイルとの照合に必要なルールを設定する必要があります。

証明書のフィールドに基づいてユーザ権限グループを照合するには、照合するフィールドを指定したルールをグループに定義し、その選択グループに対して各ルールをイネーブルにします。ルールを作成してマッピングする前に、接続プロファイル（トンネル グループ）を定義する必要があります。

ここでは、証明書/接続プロファイル マップ ルール、および ASA サーバ デバイスに接続を試みるリモート クライアントのパラメータを設定する方法について説明します。

ヒント Certificate to Connection Profile Map ポリシーは、リモート アクセス IKEv1 IPSec VPN だけに適用されます。IKEv2 または SSL VPN には適用されません。

はじめる前に

- マッピング ルールを作成する接続プロファイルがデバイスで設定されていることを確認してください。接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照してください。
- [証明書から接続プロファイルへのマップポリシー（Certificate to Connection Profile Maps Policies）] ポリシーで [設定されているルールを使用して証明書をグループと照合（Use Configured Rules to Match a Certificate to a Group）] を選択したことを確認します。Certificate to Connection Profile Map ポリシーの設定（ASA） （1754 ページ）を参照してください。

ステップ 1 （デバイス ビュー限定）ASA デバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ルール（Rules）]** を選択します。

[Certificate to Connection Profile Map Rules] ページが表示されます。ポリシーには次の 2 つのテーブルがあります。

- **マップテーブル（上半分のテーブル）**：上半分のテーブルには、証明書/接続マップルールを定義するすべての接続プロファイルのリストが示されます。各行はプロファイル マップであり、マップされる接続プロファイルの名前、マップのプライオリティ（数字が小さいほどプライオリティが高い）およびマップ名が含まれます。同じ接続プロファイルに複数のマップを設定できます。
  - このマップに規則を設定するには、規則を選択し、規則テーブルを使用して規則を作成、編集、および削除します。
  - マップを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Map Rule] ダイアログボックス（上半分のテーブル） （1757 ページ）に入力します。
  - （ルールではなく）マッププロパティを編集するには、マッププロパティを選択し、[行の編集（Edit Row）] ボタンをクリックします。
  - マップ全体を削除するには、マップを選択し、[行の削除（Delete Row）] ボタンをクリックします。
- **ルールテーブル（下半分のテーブル）**：上半分のテーブルで選択されているマップのルール。マップが上半分のテーブルで実際に選択されていることを確認する必要があります。ルールテーブルの上にあるグループタイトルに、[（接続プロファイル名）の詳細（Details for (Connection Profile Name)）] と表示されます。

マップを選択すると、そのマップに設定されているすべての規則がテーブルに表示されます。このテーブルには、フィールド（[subject] または [issuer]）、証明書コンポーネント、一致演算子、および規則によって検索される値などが表示されます。デバイスがマップされた接続プロファイルを使用するには、リモート ユーザはすべての設定済みルールをマップと照合する必要があります。

- ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Map Rule] ダイアログボックス（下半分のテーブル） （1758 ページ）に入力します。
- ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 2 ルールをマップに追加するには、次の手順を実行します。

a) 上半分のテーブルでマップを選択します。

マップが存在しない場合、上側のテーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックして作成し、マップ作成に関する情報を [マップルール（Map Rule）] ダイアログボックスに入力します。このダイアログボックスでは、マップの接続プロファイルを選択して、1 ～ 65535（数値が低いほどプライオリティが高くなります）の相対的プライオリティを割り当て、一意のマップ名を割り当てる必要があります。

b) マップが実際に選択されていることを確認してください。テーブルのマップが強調表示されているだけでは選択されていることにはなりません。下側のテーブルの上にあるヘッダーは、[（接続プロファイル名）の詳細（Details for (Connection Profile Name)）] でなければなりません。新規に作成されたマップでないかぎり、テーブルには、いくつかのルールが表示されます。

c) リモートクライアントがこのマップのプロファイルを使用するデバイスに接続するために満たす必要がある新しい証明書を、接続プロファイル照合ルールに追加するには、下側のテーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックします。これにより、さまざまなフィールドを示す [Map Rule] ダイアログボックスが開きます。

（注） 「設定が見つかりません。マッピングフィールドには値IDが必要です。マッピングを選択してください（Missing Settings, A value ID required for Mapping field, Please select a Mapping）」というエラーメッセージが表示された場合、上側のテーブルでマップが正常に選択されていません。必要なマップをもう一度クリックしてください。

d) [フィールド（Field）] リストから、ルールにより、クライアント証明書の Subject フィールドまたは Issuer フィールドが検証されるかどうかを選択します。

e) [コンポーネント（Component）] リストから、一致ルールに対して使用するクライアント証明書のコンポーネントを選択します。

f) [演算子（Operator）] フィールドから、コンポーネントと [値（Value）] フィールドの比較方法を [次と等しい（Equals）]（完全一致）、[次を含む（Contains）]（値全体が存在）、[次に等しくない（Does Not Equal）]、[次を含まない（Does Not Contain）] から選択します。

g) [値（Value）] フィールドで、照合する値を指定し、[OK] をクリックしてルールを保存します。

h) 必要に応じて、別の記録をマップに追加します。

ステップ 3 [デフォルトの接続プロファイル（Default Connection Profile）] フィールドで、いずれのマップルールにも一致しないユーザに使用する接続プロファイルを選択します。

[Map Rule] ダイアログボックス（上半分のテーブル）

[Certificate to Connection Profile Maps] > [Rules policy] の上側にマップ テーブルに対して開かれた [Map Rule] ダイアログボックスを使用して、マップを設定します。次に、このマップに対して、[Rules policy] の下半分のテーブルでルールを設定できます。これらのマップおよび関連付けられるルールの詳細については、を参照してください。 証明書/接続プロファイル マップ ルールの設定（ASA） （1755 ページ）

ナビゲーション パス

（デバイスビューだけ）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）]>[証明書/接続プロファイルマップ（Certificate to Connection Profile Maps）]>[ルール（Rules）] を選択します。上側のテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、上側のテーブルでマップを選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *387 : [Map Rule]* ダイアログボックス（上半分のテーブル）

要素	説明
マップ名（Map Name）	接続プロファイル マップの名前。
プライオリティ	一致ルールのプライオリティ番号（1～65535）。番号が小さいほどプライオリティが高くなります。たとえば、プライオリティ番号が 2 の一致ルールは、プライオリティ番号が 5 の一致ルールよりもプライオリティが高くなります。 複数のマップを作成した場合、それらのマップはプライオリティの順に処理されます。ユーザがマップされるプロファイルは最初の一致ルールによって決まります。
接続プロファイル	一致ルールを作成する IPSec 用および SSL 用の接続プロファイルを選択します。いずれかの接続プロファイルまたは両方の接続プロファイルを選択する必要があります。この接続プロファイルに接続しようとするクライアントは、デバイスに接続するための関連付けられた一致ルールの条件を満たす必要があります。 IPSec 用の接続プロファイルは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

[Map Rule] ダイアログボックス（下半分のテーブル）

[Certificate to Connection Profile Maps] > [Rules policy] の下側のルール テーブルに対して開かれた [Map Rule] ダイアログボックスを使用して、マップ テーブル（[Rules policy] の上側のテーブル）で選択されているマップのルールを設定します。これらのルールの設定の詳細については、証明書/接続プロファイル マップ ルールの設定（ASA） （1755 ページ）を参照してください。

ナビゲーション パス

（デバイス ビューのみ）ASA デバイスを選択し、ポリシー セレクタから **[リモートアクセス VPN（Remote Access VPN）] > [証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）] > [ルール（Rules）]** を選択します。下半分のテーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、下半分のテーブルでルールを選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *388 : [Map Rule]* ダイアログボックス（下半分のテーブル）

要素	説明
フィールド	クライアント証明書の [件名（Subject）] または [発行元（Issuer）] に従って、一致ルールのフィールドを選択します。
コンポーネント	一致規則に対して使用するクライアント証明書のコンポーネントを選択します。
演算子	一致ルールの演算子を次のうちから選択します。 • [Equals]：証明書コンポーネントは、入力された値と一致する必要があります。完全に一致しない場合、接続は拒否されます。 • [Contains]：証明書コンポーネントには、入力された値が含まれている必要があります。コンポーネントにその値が含まれていない場合、接続は拒否されます。 • [等しくない（Does Not Equal）]：証明書コンポーネントは、入力された値と異なっている必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値が US と等しければ、接続が拒否されます。 • [次を含まない（Does Not Contain）]：証明書コンポーネントには、入力された値が含まれていない必要があります。たとえば、選択された証明書コンポーネントが Country であり、入力された値が US である場合、クライアントの国の値に US が含まれていると、接続が拒否されます。
値	一致ルールの値。入力された値は、選択されたコンポーネントおよび演算子と関連付けられています。
Default Connection Profile	このオプションは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

リモート アクセス VPN サーバの IPsec プロポーザルの設定（ASA、PIX 7.0+ デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、サーバが ASA または PIX 7.0+ デバイスである場合のリモート アクセス VPN サーバの IPsec プロポーザルを作成または編集する方法について説明します。

（注） Cisco Security Manager バージョン 4.17 以降では、ソフトウェアバージョン 9.9(2) 以降を実行している ASA マルチコンテキストデバイスで IPSec プロポーザルポリシーを設定および展開できます。

Catalyst 6500/7600 デバイスなど、IOS または PIX 6.3 デバイスの IPsec プロポーザルを設定する場合は、リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）を参照してください。

IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプトマップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。

IPsec プロポーザルを設定する場合は、リモート アクセス クライアントがサーバに接続する外部インターフェイス、IKE ネゴシエーション中に使用する IKE バージョン、および VPN トンネル内のデータを保護する暗号化と認証のアルゴリズムを定義する必要があります。逆ルート注入および NAT 通過をイネーブルにすることもできます。

IPsec トンネルの概念の詳細については、IPsec プロポーザルについて （1499 ページ）を参照してください。

関連項目

- テーブル カラムおよびカラム見出しの機能 （66 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから、**[リモート アクセス VPN（Remote Access VPN）] > [IPSec VPN] > [IPsec プロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから、**[リモート アクセス VPN（Remote Access VPN）] > [IPSec VPN] > [IPsec プロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPsec Proposal] ページが開き、VPN エンドポイント、IPsec トランスフォーム セット、および逆ルート注入がプロポーザルで設定されているかどうかなど、設定されているプロポーザルが一覧表示されます。

ステップ 2 次のいずれかを実行します。

- 新しい IPsec プロポーザルを追加するには、[行の追加（Add Row）]（+）ボタンをクリックして、[IPsec Proposal Editor] ダイアログボックスに入力します。使用可能なオプションの詳細については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス） （1761 ページ）を参照してください。
- 既存のプロポーザルを編集するには、プロポーザルを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

- プロポーザルを削除するには、そのプロポーザルを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、拡張機能はサポートしていません。

[IPsec Proposal Editor] を使用して、ASA または PIX 7.0+ デバイスの IPsec プロポーザルを作成または編集します。

このダイアログボックスの要素は、選択したデバイスによって異なります。次の表に、ASA または PIX 7.0+ デバイスを選択したときの [IPsec Proposal Editor] ダイアログボックス内の [General] タブの要素を示します。

（注） PIX 7.0+ または ASA デバイスを選択したときのダイアログボックス内の要素の詳細については、IPsec Proposal Editor（IOS、PIX 6.3 デバイス）（1895 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）] を選択します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（ASA/PIX 7.x）（IPsec Proposal (ASA/PIX 7.x)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。

関連項目

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）
- IPsec プロポーザルについて （1499 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）
- AAA サーバ グループ オブジェクトの作成 （349 ページ）

フィールド リファレンス

表 *389 : [IPsec Proposal Editor]*（*ASA* および *PIX 7.0+* デバイス）

要素	説明
外部インターフェイス	リモート アクセス クライアントがサーバへの接続に使用する外部インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックして選択するか、または新しいオブジェクトを作成します。
Enable IKEv1 Enable IKEv2	IKE ネゴシエーション中に使用する IKE バージョン。IKEv2 は、Anyconnect 3.0+ クライアントの ASA ソフトウェア リリース 8.4(1)+ だけでサポートされます。必要に応じて、いずれかまたは両方のオプションを選択します。
クライアントサービスの有効化（Enable Client Services） Client Services Port Number	IKEv2 を有効にした場合だけ使用できます。 この接続の ASA のクライアント サービス サーバをイネーブルにするかどうかを選択します。クライアント サービス サーバーは、HTTPS（SSL）アクセスを提供します。これにより、AnyConnect ダウンロードは、ソフトウェア アップグレード、プロファイル、ローカリゼーションおよびカスタマイゼーション ファイル、CSD、SCEP、および AnyConnect クライアントが必要とするその他のファイル ダウンロードを受信できます。このオプションを選択する場合、クライアント サービス ポート番号（デフォルトは 443）を指定します。 クライアント サービス サーバーを有効にしない場合、ユーザーは、AnyConnect クライアントが必要する可能性があるこれらのファイルをダウンロードできません。 **ヒント** 同じデバイスで実行する SSL VPN に対して同じポートを使用できます。SSL VPN を設定した場合でも、IKEv2 IPsec クライアントで SSL を介してファイルをダウンロードするには、このオプションを選択する必要があります。

要素	説明
IKEv1 トランスフォーム セット IKEv2 トランスフォーム セット	トンネル ポリシーで使用するトランスフォーム セット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。トランスフォームセットは、各IKEバージョンで異なるため、サポートされているバージョンごとにオブジェクトを選択します。それぞれ最大11個のトランスフォームセットを選択できます。詳細については、トランスフォームセットの概要 （1501ページ）を参照してください。 選択したトランスフォームセットの2つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォームセットポリシーオブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォームセット ポリシー オブジェクトの設定 （1510ページ）を参照してください。
リバースルートインジェクション（Reverse Route Injection）	リバース ルート インジェクション（RRI）により、スタティックルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入について （1503ページ）を参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None]）：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]：クリプトマップのアクセス制御リスト（ACL）で定義されている宛先情報に基づいて、ルートが作成されます。これがデフォルトのオプションです。
Enable Network Address Translation Traversal	Network Address Translation Traversal（NAT-T; ネットワーク アドレス変換通過）を許可するかどうか。 NAT 通過は、VPN 接続されたハブとスポークの間に、IPsec トラフィックに対してネットワーク アドレス変換（NAT）を実行するデバイスがある場合に使用します。NAT通過については、VPN での NAT について （1530ページ）を参照してください。

要素	説明
[ESPv3設定（ESPv3 Settings）]（ASA 9.0.1+ のみ） 着信 ICMP エラーメッセージの検証先を暗号化マップとダイナミック暗号化マップのどちらにするかを指定し、セキュリティ単位のアソシエーションポリシーを設定するか、トラフィックフローパケットを有効にします。	
[着信ICMPのエラーメッセージを検証（Validate incoming ICMP error messages）]	IPsec トンネル経由で受信し、プライベートネットワーク上の内部ホストが宛先である ICMP エラーメッセージを検証するかどうかを指定します。
[フラグメント禁止（DF）ポリシーを有効にする（Enable Do Not Fragment (DF) Policy）]	IP ヘッダーに Do-Not-Fragment（DF）ビット セットを持つ大きなパケットを IPsec サブシステムがどのように処理するかを定義します。次のいずれかを実行します。 • 設定（Set）：DF ビットを設定して使用します。 • コピー（Copy）：DF ビットを保持します。 • クリア（Clear）：DF ビットを無視します。
トラフィック フロー機密保持（TFC）パケットを有効にする（Enable Traffic Flow Confidentiality (TFC) Packets）	トンネルを通過するトラフィック プロファイルをマスクするダミーの TFC パケットを有効にします。 （注） TFC を有効にする前に、[トンネルポリシー（クリプトマップ）（Tunnel Policy (Crypto Map)）] の [基本（Basic）] タブで IKE v2 IPsec プロポーザルを設定しておく必要があります。IKEv1 が有効になっている場合、トラフィックフローの機密性は利用できません。 バースト、ペイロード サイズ、およびタイムアウト パラメータを使用して、指定した SA で不定期にランダムな長さのパケットを生成します。

SSL および IKEv2 IPSec VPN ポリシーの使用

SSL VPN に対しては、特定のポリシーを設定する必要があります。これらのポリシーは、リモート アクセス IKEv2 IPSec VPN でも使用されます。次に示すトピックでは、これらのリモート アクセス VPN ポリシーについて説明します。

ここでは、次の内容について説明します。

• SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）
• 他の SSL VPN 設定の定義（ASA） （1774 ページ）
• SSL VPN 共有ライセンスの設定（ASA 8.2+） （1806 ページ）

SSL VPN アクセス ポリシーについて（ASA）

アクセス ポリシーには、リモート アクセス SSL または IKEv2 IPsec VPN 接続プロファイルをイネーブルにできるセキュリティ アプライアンスのインターフェイス、接続プロファイルで使用するポート、Datagram Transport Layer Security（DTLS）設定、SSL VPN セッション タイムアウト、および最大セッション数を指定します。AnyConnect VPN クライアントまたは AnyConnect Essentials クライアントを使用するかどうかも指定できます。

Anyconnect VPN クライアントの詳細については、SSL VPN AnyConnect クライアント設定について （1789 ページ）を参照してください。この他のトピックでは、DTLS および AnyConnect Essentials について詳しく説明します。

Datagram Transport Layer Security（DTLS）

Datagram Transport Layer Security（DTLS）をイネーブルにすると、AnyConnect クライアントは SSL トンネルおよび DTLS トンネルの 2 つのトンネルを同時に使用して、SSL VPN 接続を確立できます。DTLS を使用すると、SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。デフォルトでは、DTLS がイネーブルになるのは、インターフェイスで SSL VPN アクセスをイネーブルにした場合です。DTLS をディセーブルにすると、SSL VPN 接続は SSL VPN トンネルだけに接続します。

（注） DTLS が TLS 接続にフォールバックするためには、フォールバック トラストポイントを指定する必要があります。フォールバック トラストポイントが指定されていない場合に DTLS 接続に問題が発生すると、その接続は指定されたトラストポイントにフォールバックすることなく終了します。

AnyConnect Essentials VPN クライアント

AnyConnect Essentials は SSL または IKEv2 IPsec の独立ライセンスの VPN クライアントで、適応型セキュリティ アプライアンス全体に設定します。このクライアントは、次の例外を除き、AnyConnect のすべての機能を備えています。

- CSD を使用できない（HostScan/Vault/Cache Cleaner を含む）
- クライアントレス SSL VPN 非対応
- Windows Mobile サポートがオプション

AnyConnect Essentials クライアントにより、Microsoft Windows Vista、Windows Mobile、Windows XP、Windows 2000、Linux、または Macintosh OS X を実行しているリモート エンド ユーザは、Cisco VPN Client の利点を得ることができます。この機能がディセーブルの場合は、AnyConnect VPN クライアント一式が使用されます。この機能は、デフォルトではディセーブルになっています。

（注） このライセンスは、SSL VPN の共有ライセンスと同時には使用できません。

ここでは、次の内容について説明します。

- [SSL VPN Access Policy] ページ （1766 ページ）
- Access ポリシーの設定 （1772 ページ）

[SSL VPN Access Policy] ページ

[SSL VPN Access Policy] ページを使用して、リモート アクセス SSL または IKEv2 IPsec VPN のアクセス パラメータを設定します。Access ポリシーの設定の詳細については、Access ポリシーの設定 （1772 ページ）を参照してください。

ヒント このポリシーで指定するトラストポイントは、[公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーでも選択されている必要があります。詳細については、リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（ASA）（Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *390 : [SSL VPN Access Policy]* ページ

要素	説明
[Access Interface] テーブル	[Access Interface] テーブルには、リモート アクセス SSL または IKEv2 IPSec VPN 接続に設定されたインターフェイスのリストが表示されます。このテーブルには、インターフェイスがイネーブルで VPN アクセスが可能かどうか、DTLS がイネーブルにされているかどうか、クライアント証明書が必要かどうか、およびインターフェイスに使用されるトラストポイントなど、各インターフェイスのアクセス設定が表示されます。 • インターフェイスでアクセスを設定するには、[行の追加（Add Row）]（+）ボタンをクリックします（[Access Interface Configuration] ダイアログボックス （1770 ページ）を参照）。 • インターフェイスのアクセス設定を編集するには、インターフェイスを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします（[Access Interface Configuration] ダイアログボックス （1770 ページ）を参照）。 • インターフェイスのアクセス設定を削除するには、インターフェイスを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。
[サーバー名指定（Server Name Indication）] テーブル	[サーバー名指定（Server Name Indication）] テーブルには、定義済みのサーバー名指定マッピングが一覧表示されています。 • サーバー名指定マッピングを定義するには、[行の追加（Add Row）]（+）ボタンをクリックします（[サーバー名表示（Server Name Indication）] ダイアログボックス （1772 ページ）を参照）。 • 既存のマッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします（[サーバー名表示（Server Name Indication）] ダイアログボックス （1772 ページ）を参照）。 • サーバー名指定マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

要素	説明
ポート番号（Port Number）	VPNセッションに使用するポート。HTTPS トラフィックの場合、デフォルト ポートは 443 です。HTTP ポート リダイレクションがイネーブルになっている場合、デフォルトの HTTP ポート番号は 80 です。デフォルト以外のポートを指定するには、1024 ～ 65535 の数値を指定します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。 ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてポートリストオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） ポート番号を変更すると、現在の SSL VPN 接続がすべて（設定展開時に）終了するため、現在のユーザは再接続が必要になります。
DTLS Port Number	DTLS接続に使用する UDP ポート。デフォルトのポートは443です。DTLS の詳細については、SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）を参照してください。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。 ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてポートリストオブジェクトを選択するか、新しいオブジェクトを作成します。
Fallback Trustpoint	トラストポイントが割り当てられていないインターフェイスで使用するトラストポイント（認証局または CA サーバ）。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクト選択するか、新しいオブジェクトを作成します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

要素	説明
Default Idle Timeout	SSL または IKEv2 IPSec VPN セッションがアイドル状態になってから、セキュリティアプライアンスがセッションを終了するまでの時間を指定します（秒単位）。 この値が適用されるのは、ユーザのグループポリシー内の [Idle Timeout] 値がゼロ（0）に設定されている場合、つまり、タイムアウト値がない場合だけです。それ以外の場合、グループポリシーの [Idle Timeout] 値が、ここで設定したタイムアウトに優先されます。入力可能な最小値は、60秒（1分）です。デフォルトは 30 分（1800 秒）です。最大値は 24 時間（86400 秒）です。 この属性は短い時間に設定することを推奨します。これは、クッキーをディセーブルにするブラウザ設定（またはプロンプトでクッキーを要求してから拒否するブラウザ設定）によって、ユーザが接続していないにもかかわらずセッションデータベースに表示されることがあるためです。グループポリシーの [Simultaneous Logins] 属性が 1 に設定されている場合は、すでに最大接続数に達していることがデータベースによって示されるため、ユーザーは再びログインできません。アイドル タイムアウトを短く設定すると、このようなファントムセッションを迅速に削除し、ユーザーが再ログインできるようにすることができます。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Max Session Limit	許可される SSL または IKEv2 IPSec VPN セッションの最大数。次に示すように、ASA モデルによって、最大セッション数が異なるので注意してください。 • ASA 5505：25 • ASA 5510：250 • ASA 5520：750 • ASA 5540：2500 • ASA 5550、5585-X（SSP-10）：5000 • ASA 5580、5585-X（その他のモデル）：10,000 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

要素	説明
[証明書認証のタイムアウト（Certificate Authentication Timeout）] （ASA 8.4(5) または ASA 9.1(2)+）	証明書認証がタイムアウトするまでの待機時間（分単位）。有効な値は、1 ～ 120 分です。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
Allow Users to Select Connection Profile in Portal Page	ログイン時（たとえば、SSL VPN ポータルページ）にユーザが適切なプロファイルを選択するときに使用できる設定済み接続プロファイル（トンネル グループ）のリストを提供するかどうかを指定します。このオプションを選択しない場合、ユーザはプロファイルを選択できず、接続にはデフォルト プロファイルを使用する必要があります。 **ヒント** リモート アクセス IKEv2 IPSec VPN ではこのオプションを選択する必要があります。SSL VPN の場合、選択は任意です。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Enable AnyConnect Access	ユーザが AnyConnect VPN クライアントを使用して SSL または IKEv2 IPSec VPN 接続を確立できるようにするかどうかを指定します。このオプションは、デフォルトでオンになっています。AnyConnect VPN クライアントの詳細については、SSL VPN AnyConnect クライアント設定について （1789 ページ）を参照してください。 **ヒント** リモート アクセス IKEv2 IPSec VPN ではこのオプションを選択する必要があります。SSL VPN の場合、フル クライアント アクセスをイネーブルにする場合、このオプションを選択します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Enable AnyConnect Essentials	SSL および IKEv2 IPSec VPN の両方で使用できる、AnyConnect Essentials 機能をイネーブルにするかどうかを指定します。AnyConnect Essentials VPN クライアントの詳細については、SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）を参照してください。

[Access Interface Configuration] ダイアログボックス

[Access Interface Configuration] ダイアログボックスを使用して、リモート アクセス SSL または IKEv2 IPSec VPN 接続の ASA デバイスでインターフェイスを設定します。

ナビゲーション パス

SSL VPN アクセスポリシー（[SSL VPN Access Policy] ページ （1766 ページ）を参照）を開き、インターフェイステーブルの下にある [行の追加（Add Row）] をクリックするか、テーブルの行を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- Access ポリシーの設定 （1772 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *391 : [Access Interface Configuration]* ダイアログボックス

要素	説明
Access Interface	SSL または IKEv2 IPSec VPN アクセスを設定するインターフェイスまたはインターフェイス ロール オブジェクト。インターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックしてリストから名前を選択するか、新しいインターフェイス ロール オブジェクトを作成します。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Trustpoint Load Balancing Trustpoint	インターフェイスでのユーザの認証に使用するトラストポイント（認証局または CA サーバ）。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックして選択するか、新しいオブジェクトを作成します。 ロードバランシングが設定されている場合、ロードバランシング トラストポイントに個別の PKI 登録オブジェクトを選択することもできます。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
Allow Access	このインターフェイス経由の VPN アクセスをイネーブルにする場合は、このオプションを選択します。このオプションを選択しない場合、インターフェイスでアクセスは設定されますが、ディセーブルになります。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。
Enable DTLS	選択すると、インターフェイスで Datagram Transport Layer Security（DTLS）がイネーブルになり、AnyConnect VPN Client は 2 つの同時トンネル（SSL トンネルと DTLS トンネル）を使用して SSL VPN 接続を確立できます。 この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

[サーバー名表示（Server Name Indication）] ダイアログボックス

バージョン 4.8 以降、Cisco Security Manager では、有効な VPN インターフェイスによって認証に使用される [サーバー名表示（Server Name Indication）] マッピングを設定できます。この機能には、トラストポイントへのドメイン名のマッピングが含まれます。

[サーバー名表示（Server Name Indication）] ダイアログボックスを使用して、各インターフェイスのドメインやトラストポイントを定義または変更します。

注：

- トラストポイントには一意のドメイン名を設定できます。トラストポイントは複数のドメイン名にマッピングできます。最大で 16 個の一意のトラストポイントを設定できます。
- トラストポイントへのドメイン名の [サーバー名表示（Server Name Indication）] マッピングは、ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスでサポートされています。

ナビゲーション パス

SSL VPN アクセスポリシー（[SSL VPN Access Policy] ページ （1766 ページ）を参照）を開き、ServerNameIndication テーブルの下にある [行の追加（Add Row）] をクリックするか、テーブルの行を選択して [行の編集（Edit Row）] をクリックします。

フィールド リファレンス

表 *392 : [サーバー名表示（Server Name Indication）] ダイアログボックス*

要素	説明
ドメインマスク	トラストポイントを設定するドメイン名を入力します。このドメインは、特定のインターフェイスには関連付けられません。ドメインが関連付けられている証明書は、任意のインターフェースで使用できます。
Trustpoint	インターフェイスでのユーザの認証に使用するトラストポイント（認証局またはCA サーバ）。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）]をクリックして選択するか、または新しいオブジェクトを作成します。

Access ポリシーの設定

ここでは、ASA デバイスに Access ポリシーを設定する方法について説明します。アクセス ポリシーは、リモートアクセス SSL および IKEv2 IPSec VPN 接続に必要です。アクセスポリシーの詳細については、SSL VPN アクセス ポリシーについて（ASA） （1765 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（Access）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [アクセス（ASA）（Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Access] ページが開きます。このページの要素の詳細については、[SSL VPN Access Policy] ページ （1766 ページ）を参照してください。

ステップ 2 ポリシー上部のインターフェイス テーブルで、リモート アクセス SSL または IKEv2 IPSec VPN 接続を許可するすべてのインターフェイスを設定します。

- インターフェイスを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックして、[アクセスインターフェイス設定の追加（Add Access Interface Configuration）] ダイアログボックスに入力します。インターフェイス名（または目的のインターフェイスを識別するインターフェイス ロール オブジェクト）、およびインターフェイスでアクセスを許可するかどうかを指定する必要があります。

インターフェイスの Certificate Authority（CA; 認証局）サーバ トラストポイント（およびロード バランシングを使用する場合はロード バランシング トラストポイント）を識別する PKI 登録オブジェクト、DTLS 接続をイネーブルにするかどうか、およびクライアントが接続を確立するために有効な証明書が必要かどうかを指定できます。オプションの詳細については、[Access Interface Configuration] ダイアログボックス（1770 ページ）を参照してください。

- インターフェイスの設定を編集するには、そのインターフェイスを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）]ボタンをクリックします。インターフェイス設定を編集してアクセスをディセーブルにできます。そのため、インターフェイスを削除する場合、VPN から完全に削除する場合だけにしてください。

ステップ 3 残りの設定を行います。設定については、[SSL VPN Access Policy] ページ （1766 ページ）で詳しく説明されています。特に重要な設定を次に示します。

- [フォールバックトラストポイント（Fallback Trustpoint）]：インターフェイスにテーブルで設定されているトラストポイントがない場合に使用する Certificate Authority（CA; 認証局）サーバートラストポイント。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックして選択するか、新しいオブジェクトを作成します。
- [ユーザにポータルページでの接続プロファイルの選択を許可する（Allow Users to Select Connection Profile in Portal Page）]：複数のトンネルグループがある場合、このオプションを選択すると、ユーザは、ログイン時に正しいトンネルグループを選択できます。このオプションは、IKEv2 IPSec VPN で選択する必要があります。
- [Anyconnectアクセスを有効化（Enable AnyConnect Access）]：AnyConnect VPN クライアントは、フルクライアントです。VPN へのフルクライアントアクセスを許可する場合は、AnyConnect アクセスをイネーブルにする必要があります。このオプションは、IKEv2 IPSec VPN で選択する必要があります。

AnyConnect Essentials など、AnyConnect の詳細については、SSL VPN AnyConnect クライアント設定について （1789 ページ）を参照してください。

- [Connect Essentialsの有効化（Enable AnyConnect Essentials）]：AnyConnect Essentials クライアントを使用する場合、このオプションを選択します。これは、リモートアクセス SSL または IKEv2 IPSec VPN で使用できます。

ステップ 4 このポリシーで指定するトラストポイントは、[公開キーインフラストラクチャ（Public Key Infrastructure）] ポリシーでも選択されている必要があります。詳細については、リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定 （1552 ページ）を参照してください。

他の SSL VPN 設定の定義（ASA）

ASA デバイスの SSL VPN のその他の設定ポリシーは、キャッシング、コンテンツの書き換え、文字エンコード、プロキシおよびプロキシ バイパス定義、ブラウザ プラグイン、AnyConnect クライアント イメージおよびプロファイル、Kerberos Constrained Delegation、その他の一部の高度な設定を含む設定を定義します。

その他の設定ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

次のタブで設定を定義できます。

- [Performance] タブ：SSL VPN パフォーマンスを向上するようにキャッシングを設定します。SSL VPN パフォーマンス設定の定義（ASA） （1776 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Content Rewrite] タブ：ユーザがセキュリティ アプライアンス自体を介することなく特定のサイトおよびアプリケーションを参照できるように許可するルールを作成します。SSL VPN コンテンツ書き換えルールの定義（ASA） （1778 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Encoding] タブ：CIFS サーバから配信される Web ページのデフォルト以外のエンコーディングを設定します。エンコーディングは、通常、リモートユーザーのブラウザにより判別されます。SSL VPN エンコーディング ルールの設定（ASA） （1780 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

- [Proxy] タブ：HTTP または HTTPS プロキシ サーバ（ネットワークで必要な場合）、およびプロキシ バイパス ルールを定義します。SSL VPN プロキシおよびプロキシ バイパスの設定（ASA）（1782 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Plug In] タブ：Web ブラウザが専用の機能を実行するために起動する、個々のプログラムである、ブラウザプラグインを定義します。SSL VPN ブラウザプラグインの設定（ASA）（1787 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Client Settings] タブ：クライアントへのダウンロードのために AnyConnect クライアントイメージおよびプロファイルを設定します。次のトピックを参照してください。
  - SSL VPN AnyConnect クライアント設定について （1789 ページ）
  - SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）

この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN で部分的にサポートされています。ASA 9.5(2) マルチコンテキストモードでは、AnyConnect クライアントイメージのみがサポートされます。バージョン 4.12 以降、Security Manager は、管理コンテキストおよびユーザーコンテキストのマルチコンテキスト ASA 9.6(2) 以降のデバイスをサポートしています。サポートされている CLI は次のとおりです。

- Anyconnect image
- Anyconnect profile

検出中、ASA 9.5(2) リモートアクセス VPN マルチコンテキストモードの AnyConnect イメージは検出されません。検出後に AnyConnect イメージ設定を削除する場合は、FlexConfig を使用する必要があります。

- [Microsoft KCD Server]：クライアントレス SSL VPN 接続で使用する Kerberos Constrained Delegation（KCD）を設定します。次のトピックを参照してください。
  - SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） （1796 ページ）
  - SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA） （1799 ページ）

この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

- [AnyConnectカスタム属性（AnyConnect Custom Attributes）] タブ：AnyConnect カスタム属性を設定します。AnyConnect カスタム属性（ASA）の設定 （1801 ページ）を参照してください。[AnyConnectカスタム属性（AnyConnect Custom Attributes）] タブは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。
- [Advanced] タブ：メモリ、オンスクリーン キーボードおよび内部パスワード機能を設定します。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

（注） 4.15 以降、Cisco Security Manager は HTTP Strict Transport Security（HSTS）をサポートしています。HSTS は、プロトコルダウングレード攻撃および Cookie のハイジャックから Web サイトを保護するのに役立つ Web セキュリティ ポリシー メカニズムです。

[詳細（Advanced）] タブで、HSTS を有効または無効にしたり、タイムアウト値を指定したりすることができます。SSL VPN の高度な設定の定義（ASA） （1803 ページ）を参照してください。

- [SSLサーバー検証（SSL Server Verification）] タブ：クライアントレス SSL VPN ユーザーの HTTPS サーバー検証を有効にします。SSL VPN サーバー検証の設定（ASA） （1805 ページ）を参照してください。この機能は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ヒント デバイスで Connection Profile ポリシーを設定する必要があります。接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ） を参照してください。

SSL VPN パフォーマンス設定の定義（ASA）

キャッシングによって SSL VPN パフォーマンスが向上します。頻繁に再利用されるオブジェクトをシステム キャッシュに格納することで、書き換えの繰り返しやコンテンツの圧縮の必要性を低減します。SSL VPN と、リモート サーバとエンドユーザ ブラウザの両方との間のトラフィックが削減され、その結果、多数のアプリケーションがより効率的に実行されます。

ここでは、ASA セキュリティ アプライアンスでキャッシングをイネーブルにする方法について説明します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。まだ選択されていない場合、[パフォーマンス（Performance）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。まだ選択されていない場合、[パフォーマンス（Performance）] タブをクリックします。

ステップ 2 [有効（Enable）] を選択して、セキュリティアプライアンスでのキャッシングをイネーブルにします。

このオプションを選択しない場合、セキュリティアプライアンスで定義されているキャッシュ設定は有効になりません。

ステップ 3 次のオプションを設定します。

- [最小オブジェクトサイズ（Minimum Object Size）]：セキュリティアプライアンスでキャッシュに格納可能な HTTP オブジェクトの最小サイズ（KB 単位）。有効な範囲は 0 ～ 10,000 KB です。デフォルトは 0 KB です。
- [最大オブジェクトサイズ（Maximum Object Size）]：セキュリティアプライアンスでキャッシュに格納可能な HTTP オブジェクトの最大サイズ（KB 単位）。有効な範囲は 0 ～ 10,000 KB です。デフォルトは 1000 KB です。最大サイズは、最小サイズよりも大きくする必要があります。
- [最終変更係数（Last Modified Factor）]：最後に更新されたタイムスタンプだけを持ち、サーバーにより設定されたその他の有効期限値を持たないキャッシングオブジェクトの再検証ポリシーを設定する整数を指定します有効な範囲は 1 ～ 100 です。デフォルトは 20 です。

また、発信 Web サーバからセキュリティアプライアンス要求に対して、応答が期限切れになる時間を示す Expires 応答が送信されますが、この応答もキャッシングに影響を及ぼします。この応答ヘッダーは、応答が古くなり（条件付き GET 操作を使用して）最新のチェックなしでクライアントに送信できなくなる時刻を示します。

また、セキュリティアプライアンスでは、Web オブジェクトごとに、オブジェクトがディスクに書き込まれる前にオブジェクトの有効期限を計算できます。オブジェクトのキャッシュ有効期限データを計算するためのアルゴリズムは、次のとおりです。

有効期限 = (今日の日付 - オブジェクトの最終変更日付) X 有効期間係数

有効期限が経過するとオブジェクトが古いと見なされ、それ以降の要求に対しては、セキュリティアプライアンスによってコンテンツが新しく取得されます。最終変更係数を 0 に設定することは、即時の再検証を強制することに相当します。100 に設定すると、再検証までの時間が許容される範囲で最も長くなります。

- [有効期間（Expiration Time）]：セキュリティアプライアンスがオブジェクトを再検証せずにキャッシュに格納する時間（分単位）。範囲は 0 ～ 900 分です。デフォルトは 1 分です。

再検証では、キャッシュされたオブジェクトの経過時間が有効期間を超過している場合、要求されたコンテンツをクライアントブラウザに提供する前に、発信サーバからそのオブジェクトを拒否します。キャッシュされたオブジェクトの経過時間とは、セキュリティアプライアンスが発信サーバーに明示的に接続してオブジェクトがまだ有効期間内であるかどうかをチェックすることなく、オブジェクトがセキュリティアプライアンスのキャッシュに格納されている時間のことです。

- [スタティックコンテンツのキャッシュ（Cache Static Content）]：セキュリティアプライアンスでスタティックコンテンツをキャッシュできるかどうかを指定します。各 Web ページは、スタティックオブジェクトとダイナミックオブジェクトで構成されます。セキュリティアプライアンスでは、イメージファイル（*.gif、*.jpeg）、Java アプレット（.js）、カスケーディングスタイルシート（*.css）の個々のスタティック オブジェクトをキャッシュします。

SSL VPN コンテンツ書き換えルールの定義（ASA）

SSL VPN は、高度な要素（JavaScript、VBScript、Java、およびマルチバイト文字など）に対応したコンテンツ変換/書き込みエンジンを介してアプリケーショントラフィックを処理し、ユーザが SSL VPN デバイス内でアプリケーションを使用しているか、デバイスとは無関係に使用しているかに応じて、HTTP トラフィックをプロキシします。

一部のアプリケーションおよび Web リソース（パブリック Web サイトなど）がセキュリティアプライアンスを通過しないようにする場合は、セキュリティアプライアンス自体を経由せずに、ユーザが特定のサイトおよびアプリケーションをブラウズできるようにする書き換え規則を作成できます。これは、IPSec VPN 接続におけるスプリット トンネリングによく似ています。

[SSL VPN Other Settings] ページの [Content Rewrite] タブでは、複数のコンテンツ書き換え規則を作成できます。[Content Rewrite] タブには、コンテンツ書き換えがイネーブルまたはディセーブルな、すべてのアプリケーションが一覧表示されます。

ヒント セキュリティアプライアンスは、最も小さい番号から順番に書き換えルールを検索して、一致した最初のルールを適用します。

ここでは、コンテンツ書き換えルールを作成または編集する方法を示します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで [コンテンツ書き換え（Content Rewrite）] タブをクリックします。[Content Rewrite] タブには、コンテンツ書き換えがイネーブルまたはディセーブルな、すべてのアプリケーションが表示されます。

セキュリティアプライアンスは、最も小さい番号から順番に書き換えルールを検索して、一致した最初のルールを適用します。リソースマスクは、ルールと照合するアプリケーション ストリングを定義します。

番号がないルールは、番号付きのすべてのルールのあとに評価されます。

ステップ 3 次のいずれかを実行します。

- ルールを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[コンテンツ書き換えの追加（Add Content Rewrite）] ダイアログボックスに入力します。これらのオプションにつ

いては、[Add Content Rewrite]/[Edit Content Rewrite] ダイアログボックス （1779 ページ）で詳しく説明されています。

- ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックして、[コンテンツ書き換えの編集（Edit Content Rewrite）] ダイアログボックスで変更を加えます。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

（注） Cisco Security Manager 4.24 以降、[コンテンツ書き換え（Content Rewrite）] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

[Add Content Rewrite]/[Edit Content Rewrite] ダイアログボックス

[Add or Edit Content Rewrite] ダイアログボックスを使用して、SSL VPN 接続を介するプロキシ HTTP トラフィックに対して拡張要素（JavaScript、VBScript、Java、マルチバイト文字など）を含む書き換えエンジンを設定します。コンテンツ書き換えルールの詳細については、SSL VPN コンテンツ書き換えルールの定義（ASA） （1778 ページ）を参照してください。

ナビゲーション パス

ASA デバイスの SSL VPN のその他の設定ポリシーの [コンテンツのリライト（Content Rewrite）] タブから、[行の追加（Add Row）] ボタンをクリックするか、ルールを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN コンテンツ書き換えルールの定義（ASA） （1778 ページ）を参照してください。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

フィールド リファレンス

表 393 : [Add or Edit Content Rewrite] ダイアログボックス

要素	説明
有効化（Enable）	選択すると、セキュリティアプライアンスで、書き換えルールに対するコンテンツ書き換えがイネーブルになります。 外部のパブリック Web サイトなどの一部のアプリケーションでは、この処理が必要ないものもあります。これらのアプリケーションでは、コンテンツ リライトをオフにできます。

要素	説明
ルール番号	このルールの番号。この番号は、リスト内のルールの位置を指定します。番号がないルールはリストの最後に配置されます。範囲は1～65534です。 ルールは、低い番号から高い番号の順に処理され、最初に一致したルールがトラフィックに適用されます。
ルール名	コンテンツ書き換えルールを説明する英数字文字列。最大長は 128 文字です。
リソース マスク	ルールが適用されるアプリケーションまたはリソースの名前。最大長は300文字です。 次のワイルドカードを使用できます。 • *：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 • ?：単一文字と一致します。 • [!x-y]：シーケンスにない任意の文字と一致します。 • [x-y]：シーケンス内の任意の文字と一致します。

SSL VPN エンコーディング ルールの設定（ASA）

[SSL VPN Other Settings] ページの [Encoding] タブを使用して、リモート ユーザに配信される SSL VPN ポータル ページでエンコードする文字セットを指定します。デフォルトでは、SSL VPN ポータル ページの文字セットはリモート ブラウザで設定されているエンコーディング タイプセットによって決定されるため、ブラウザで適切なエンコーディングが行われることを確認する必要がある場合を除き、文字エンコーディングを設定する必要はありません。

文字エンコーディングは、データを表すために（0 や 1 などの）raw データと文字を組み合わせたものです。使用する文字エンコード方式は、言語によって決まります。ある言語では同じ方式を使用していても、別の言語でも同じとはかぎりません。通常、ブラウザで使用されるデフォルトのエンコード方式は地理上の地域によって決まりますが、リモートユーザはこれを変更できます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。

エンコード属性を使用すると、SSL VPNポータルページに文字エンコード方式の値を指定し、ユーザがブラウザを使用している地域、またはブラウザに対して行われた変更に関係なく、ブラウザにページが正しく表示されることを保証できます。

文字エンコード属性は、デフォルトですべての SSL VPN ポータル ページが継承するグローバル設定です。ただし、文字エンコード属性の値と異なる文字エンコードを使用する Common Internet File System（CIFS）サーバのファイル エンコード属性を上書きできます。異なる文字エンコードが必要な CIFS サーバには、異なるファイル エンコード値を使用できます。

CIFS サーバから SSL VPN ユーザにダウンロードされた SSL VPN ポータル ページのエンコードは、サーバ指定の SSL VPN ファイル エンコード属性の値となります。サーバで指定されていない場合、ポータルページは文字エンコード属性の値を継承します。リモートユーザーのブラウザでは、ブラウザの文字エンコードセットのエントリにこの値がマップされ、使用する適切な文字セットが決定されます。SSL VPN 設定に CIFS サーバのファイル エンコード エントリを指定せず、文字エンコード属性も設定されていない場合は、SSL VPN ポータル ページに値が指定されません。SSL VPN ポータル ページで文字エンコードを指定しなかった場合、またはブラウザがサポートしていない文字エンコード値を指定した場合、リモート ブラウザでは独自のデフォルト エンコードが使用されます。

[SSL VPN Global Settings] ページの [Encoding] タブでは、ポータル ページでエンコードされる、CIFS サーバに関連付けられた現在設定済みの文字セットを表示できます。このタブから、文字セットを作成または編集できます（次の手順を参照）。

関連項目

- 他の SSL VPN 設定の定義（ASA）　（1774 ページ）

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2　[その他の設定（Other Settings）] ページで [エンコーディング（Encoding）] タブをクリックします。[Encoding] タブには、デフォルトのエンコーディング、およびエンコーディング ルールが設定される CIFS サーバのリストが表示されます。

ステップ 3　[グローバルSSL VPNエンコーディングタイプ（Global SSL VPN Encoding Type）] リストから、テーブルに表示された CIFS サーバからの属性を除き、すべての SSL VPN ポータルページが継承する文字エンコードを決定する属性を選択します。

（注）　[なし（None）] を選択するか、SSL VPN クライアントのブラウザでサポートされていない値を指定した場合は、デフォルトのエンコーディングが使用されます。デフォルトのグローバル エンコーディングは [None] です。

次のエンコーディング タイプから選択できます。

- big5
- gb2312
- ibm-850
- iso-8859-1
- shift_jis

（注） 日本語の Shift_jis 文字エンコーディングを使用している場合は、関連付けられている [ページフォントの選択（Select Page Font）] ペインの [フォントファミリ（Font Family）] エリアにある [指定しない（Do Not specify）] をクリックして、このフォントファミリを削除します。

- unicode
- windows-1252
- none

ステップ 4 次のいずれかを実行します。

- ルールを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[ファイルエンコーディングの追加（Add File Encoding）] ダイアログボックスで次の設定を行います。
  - [CIFSサーバーIP、CIFSサーバーホスト（CIFS Server IP, CIFS Server Host）]：これらのオプションのいずれかを選択して、IP アドレスまたはホスト名のいずれかにより CIFS サーバを指定します。IP アドレスを選択する場合、IP アドレスまたは 1 つ以上の個々の IP アドレスを指定するネットワーク/ホスト オブジェクトの名前のいずれかを入力できます。

ホスト名を指定する場合、セキュリティ アプライアンスでは指定した大文字と小文字が保持されますが、名前をサーバと照合するときは大文字と小文字の違いが無視されます。

- [エンコーディングタイプ（Encoding Type）]：エンコーディングタイプを選択します。オプションは、前述のグローバル設定と同じです。
- ルールを編集するには、そのルールを選択し、[行の編集（Edit Row）] ボタンをクリックして、[ファイルエンコーディングの編集（Edit File Encoding）] ダイアログボックスで変更を加えます。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

SSL VPN プロキシおよびプロキシ バイパスの設定（ASA）

[SSL VPN Other Settings] ページの [Proxy] タブを使用して、HTTPS 接続を終了して HTTP/HTTPS 要求を HTTP および HTTPS プロキシ サーバに転送するようにセキュリティ アプライアンスを設定します。このタブでは、最小コンテンツ書き換えを実行するようにセキュリティ アプライアンスを設定したり、書き換えるコンテンツのタイプ（外部リンクまたは XML、あるいはどちらでもない）を指定したりすることもできます。

セキュリティ アプライアンスは、HTTPS 接続を終了し、HTTP および HTTPS プロキシ サーバに HTTP/HTTPS 要求を転送できます。これらのサーバは、ユーザとインターネット間を中継する機能を果たします。すべてのインターネット アクセスがユーザ制御のサーバを経由するように指定することで、別のフィルタリングが可能になり、セキュアなインターネット アクセスと管理制御が保証されます。

（注） HTTP/HTTPS プロキシは、Personal Digital Assistant への接続をサポートしていません。

HTTP プロキシ サーバからダウンロードする Proxy Auto-Configuration（PAC）ファイルを指定できます。ただし、PAC ファイルを指定する場合は、プロキシ認証を使用できません。

ユーザは、プロキシバイパスを使用するようにセキュリティアプライアンスを設定できます。これは、この機能が提供するコンテンツ リライトを使用した方が、アプリケーションや Web リソースをより有効活用できる場合に設定します。プロキシバイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。カスタム Web アプリケーションで役立ちます。

プロキシバイパスには複数のエントリを設定できます。エントリを設定する順序は重要ではありません。インターフェイスとパスマスク、またはインターフェイスとポートにより、プロキシ バイパス ルールが一意に指定されます。

パス マスクではなくポートを使用してプロキシ バイパスを設定した場合、ネットワーク設定によっては、これらのポートからセキュリティアプライアンスにアクセスできるようにファイアウォール設定を変更することが必要になる場合があります。この制限を回避するには、パスマスクを使用します。ただし、このパス マスクは変更される場合があるため、複数のパス マスク ステートメントを使用して、この可能性を排除する必要がある可能性があることに注意してください。

ここでは、SSL VPN のプロキシおよびプロキシ バイパス ルールを定義する方法を示します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで [プロキシ（Proxy）] タブをクリックします。[Proxy] タブには、現在定義されているプロキシおよびプロキシ ルールが表示されます。

ステップ 3 [プロキシタイプ（Proxy Type）] フィールドから、SSL VPN 接続に使用する外部プロキシサーバーのタイプを選択します。

- [HTTP/HTTPSプロキシサーバー（HTTP/HTTPS Proxy Server）]：プロキシサーバーを指定して、HTTP または HTTPS 要求を処理します。

- [PACを使用したプロキシ（Proxy Using PAC）]：プロキシ自動構成（PAC）ファイルを指定して、HTTP プロキシサーバーからユーザーのブラウザにダウンロードします。ダウンロードが完了すると、PAC ファイルは JavaScript 機能を使用して各 URL のプロキシを識別します。

このオプションを選択する場合、PAC ファイルの URL を [プロキシ自動構成ファイルのURLを指定（Specify Proxy Auto Config file URL）] フィールドに入力します。URL は、**http://** から開始する必要があります。開始しない場合、セキュリティアプライアンスは PAC ファイルを使用しません。

ステップ 4 プロキシ タイプで [HTTP/HTTPS Proxy Server] を選択した場合、HTTP および HTTPS プロキシ サーバの設定を行います。HTTP および HTTPS サーバは個別に設定できるため、異なるサーバを使用したり、いずれか 1 つのタイプだけを指定したりできます。次のオプションを設定します。

- [HTTPプロキシサーバーの有効化（Enable HTTP Proxy Server）]、[HTTPSプロキシサーバーの有効化（Enable HTTPS Proxy Server）]：これらのオプションのいずれかまたは両方を選択して、プロキシサーバーを設定します。
- [HTTPプロキシサーバー（HTTP Proxy Server）]、[HTTPSプロキシサーバー（HTTPS Proxy Server）]：IP アドレス、または単一 プロキシサーバーの IP アドレスを含むネットワーク/ホストオブジェクトの名前を、設定するプロキシサーバーのタイプごとに入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。

HTTP のデフォルト ポートは 80、HTTPS のデフォルト ポートは 443 です。

バージョン 4.12 以降、Security Manager は ASA 9.0(1) 以降のデバイスの IPv6 アドレスをサポートします。入力した IPv6 アドレスが無効な場合、Security Manager にはエラーが表示されます。リストからプロキシサーバーを選択したときにオブジェクトが使用できない場合、Security Manager は警告メッセージを表示します。

- [HTTPプロキシポート（HTTP Proxy Port）]、[HTTPSプロキシポート（HTTPS Proxy Port）]：HTTP または HTTPS 要求が転送されるプロキシサーバーのポートを入力します。また、ポートを定義するポートリストオブジェクトの名前を入力できます。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成することもできます。
- [除外アドレス一覧（Exception Address List）]：HTTP または HTTPS プロキシサーバーに送信できないようにする 1 つの URL、または複数の URL のカンマ区切りリスト。このストリングには文字数の制限はありませんが、コマンド全体で 512 文字以下となるようにする必要があります。リテラル URL を指定するか、次のワイルドカードを使用できます。
  - ***** は、スラッシュ（/）とピリオド（.）を含む任意の文字列と一致します。このワイルドカードは、英数字文字列とともに使用する必要があります。
  - **?** は、スラッシュおよびピリオドを含む、任意の 1 文字に一致します。
  - [x-y] は、x から y までの範囲の任意の 1 文字と一致します。x は ANSI 文字セット内のある 1 文字を表し、y は別の 1 文字を表します。
  - [!x-y] は、範囲外の任意の 1 文字と一致します。

- [認証ユーザー名（Authentication User Name）]、[認証パスワード（Authentication Password）]、[確認（Confirm）]：プロキシサーバーでユーザー認証が必要な場合は、有効なユーザー名およびパスワードを入力します。

ステップ 5 必要に応じて、タブの一番下にある [Proxy Bypass] テーブルでプロキシ バイパス ルールを設定します。プロキシ バイパスは、プロキシ バイパスに設定されている ASA インターフェイス、ポートおよびターゲット URL を指定します。次のいずれかを実行します。

- プロキシバイパスルールを追加するには、[行の追加（Add Row）] ボタンをクリックして、[プロキシバイパスの追加（Add Proxy Bypass）] ダイアログボックスに入力します。プロキシ バイパス ルールの属性の詳細については、[Add or Edit Proxy Bypass Dialog Box] ダイアログボックス （1785 ページ）を参照してください。
- プロキシバイパスルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

ヒント プロキシバイパス ルールを設定する場合、SSL VPN Access ポリシーも設定する必要があります。詳細については、Access ポリシーの設定 （1772 ページ）を参照してください。

[Add or Edit Proxy Bypass Dialog Box] ダイアログボックス

[Add or Edit Proxy Bypass] ダイアログボックスを使用して、セキュリティ アプライアンスがコンテンツ書き換えをほとんど、またはまったく実行しない場合のプロキシ バイパス ルールを設定します。

ナビゲーション パス

ASA デバイスの SSL VPN のその他の設定ポリシーの [プロキシ（Proxy）] タブから、[行の追加（Add Row）] ボタンをクリックするか、ルールを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN エンコーディング ルールの設定（ASA） （1780 ページ）を参照してください。

フィールド リファレンス

表 *394 : [Add or Edit Proxy Bypass Dialog Box]* ダイアログボックス

要素	説明
インターフェイス（Interface）	セキュリティ アプライアンスでプロキシ バイパスに使用されるインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか新しいオブジェクトを作成します。

要素	説明
Bypass On Port	プロキシ バイパスのポート番号を使用する場合、このオプションを選択します。有効なポート番号は、20000 ～ 21000 です。ポートリストオブジェクトのポートまたは名前を入力します。または、[選択（Select）]をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） パス マスクではなくポートを使用してプロキシ バイパスを設定した場合、ネットワーク設定によっては、これらのポートからセキュリティアプライアンスにアクセスできるようにファイアウォール設定を変更することが必要になる場合があります。この制限を回避するには、パス マスクを使用します。
Bypass Matching Specific Pattern	プロキシバイパスの照合にURLパスマスクを使用する場合、このオプションを選択します。パスは、URL 内のドメイン名に続くテキストです。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスになります。 次のワイルドカードを使用できます。 • *****：すべてに一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 • **?**：単一文字と一致します。 • **[x-y]**：シーケンス内の任意の文字と一致します。 • **[!x-y]**：シーケンスにない任意の文字と一致します。 最大値は 128 バイトです。 （注） パス マスクが変更される可能性をなくすために、複数のパス マスク ステートメントを使用することが必要になる場合があります。
URL	[http] または [https] プロトコルを選択し、プロキシバイパスを適用するURLを入力します。 プロキシバイパスに使用するURLでは、最大128バイトが許可されます。別のポートを指定しない限り、HTTP のポートは 80、HTTPS のポートは 443 です。
Rewrite XML	セキュリティアプライアンスによってバイパスされるように、XMLサイトおよびアプリケーションが書き換えられるかどうかを指定します。
Rewrite Hostname	セキュリティ アプライアンスによってバイパスされるように、外部リンクが書き換えられるかどうかを指定します。

SSL VPN ブラウザ プラグインの設定（ASA）

ブラウザ プラグインは、Web ブラウザによって呼び出される独立したプログラムで、ブラウザ ウィンドウ内でクライアントをサーバに接続するなどの専用の機能を実行します。セキュリティ アプライアンスを使用すると、クライアントレス SSL VPN セッション中に、リモート ブラウザにダウンロードするプラグインをインポートできます。

シスコでは、Java ベースのオープン ソース コンポーネントを再配布しています。これは、クライアントレス SSL VPN セッションで Web ブラウザのプラグインとしてアクセスされるコンポーネントで、次のものがあります。シスコでは再配布するプラグインのテストを行っており、再配布できないプラグインの接続性をテストする場合もあります。プラグインファイルは、Cisco Security Manager サーバーの製品インストールフォルダ（通常は C:\Program Files\CSCOpx）内の \files\vms\repository フォルダにあります。実際のファイル名には、リリース番号が含まれています。

- rdp-plugin.jar：Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行されているコンピュータに接続できます。再配布されるプラグインのソースがある Web サイトは http://properjavardp.sourceforge.net/ です。
- ssh-plugin.jar：Secure Shell-Telnet プラグインにより、リモート ユーザはリモート コンピュータとセキュア シェル接続または Telnet 接続を確立できます。この再配布プラグインのソースがある Web サイトは、http://javassh.org/ です。

（注） ssh-plugin.jar は、SSH プロトコルおよび Telnet プロトコルの両方をサポートします。SSH クライアントは SSH バージョン 1.0 をサポートします。

- vnc-plugin.jar：Virtual Network Computing プラグインにより、リモート ユーザはモニタ、キーボード、およびマウスを使用して、リモートデスクトップ共有がオンになっているコンピュータを表示および制御できます。この再配布プラグインのソースがある Web サイトは、http://www.tightvnc.com です。

（注） シスコでは、GNU 一般公的使用許諾（GPL）に従い、変更を加えることなくプラグインを再配布しています。GPL により、これらのプラグインを直接改良できません。

フラッシュ デバイスにプラグインをインストールすると、セキュリティ アプライアンスにより次のことが実行されます。

- （Cisco 配布のプラグイン限定）URL で指定された jar ファイルのアンパック
- セキュリティ アプライアンス ファイル システム上の csco-config/97/plugin ディレクトリへのファイルの書き込み
- 将来のすべてのクライアントレス SSL VPN セッションに対するプラグインのイネーブル化、およびメイン メニュー オプションの追加とポータル ページの [Address] フィールドの隣にあるドロップダウン メニューへのオプションの追加

クライアントレス SSL VPN セッションのユーザがポータル ページで関連するメニュー オプションをクリックすると、ポータルページにインターフェイスへのウィンドウが開き、ヘルプペインが表示されます。ドロップダウン メニューに表示されたプロトコルをユーザーが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注） Java プラグインの中には、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインのステータスをレポートするプラグインもあります。オープン ソースのプラグインはステータスをレポートしますが、セキュリティ アプライアンスはステータスをレポートしません。

[SSL VPN Global Settings] ページの [Plug-in] タブで、クライアントレス SSL VPN ブラウザ アクセスに現在設定されているブラウザ プラグインを表示できます。このタブから、プラグイン ファイルを作成または編集できます（次の手順を参照）。

プラグインの要件および制約事項

プラグインへのリモート アクセスを提供するには、セキュリティ アプライアンスでクライアントレス SSL VPN がイネーブルになっている必要があります。リモートで使用するために必要な最低限のアクセス権は、ゲスト特権モードに属しています。リモート コンピュータ上に必要な Java のバージョンは、プラグインによって自動的にインストールまたは更新されます。ステートフル フェールオーバーが発生すると、プラグインを使用して確立されたセッションは保持されません。ユーザーはフェールオーバー後に再接続する必要があります。

プラグインをインストールする前に、セキュリティ アプライアンスで次の準備を行います。

- セキュリティ アプライアンスのインターフェイスでクライアントレス SSL VPN がイネーブルであることを確認します。
- リモート ユーザが Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を使用して接続するセキュリティ アプライアンス インターフェイスに、SSL 証明書をインストールします。

（注） SSL 証明書の 一般名（CN）として IP アドレスを指定しないでください。リモート ユーザは、FQDN を使用してセキュリティ アプライアンスとの通信を試みます。リモート PC は、DNS または System32\drivers\etc\hosts ファイル内のエントリを使用して、FQDN を解決できる必要があります。

関連項目

- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで [プラグイン（Plug-in）] タブをクリックします。[Plug-in] タブには、プラグインのタイプおよび実際のプラグイン ファイルを定義するファイル ポリシー オブジェクトの名前など、設定されているすべてのプラグインのリストが表示されます。

ステップ 3 次のいずれかを実行します。

- プラグインを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、次のように、[プラグインエントリの追加（Add Plug-In Entry）] ダイアログボックスに入力します。
  - [プラグイン（Plug-in）]：追加するプラグインのタイプを選択します。
  - [Remote Desktop (RDP) or RDP2]：Remote Desktop Protocol サービス。
  - [Secure Shell (SSH), Telnet]：Secure Shell および Telnet サービス。
  - [VNC]：Virtual Network Computing サービス。
  - [Citrix (ICA)]：Citrix MetaFrame サービス。
  - [Post]：ポスト サービス。
  - [プラグインファイル（Plug-in File）]：プラグインファイルを定義するファイルポリシーオブジェクトの名前。ファイルオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、または新しいオブジェクトを作成します。ファイル オブジェクトの作成の詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。
- プラグインを編集するには、そのプラグインを選択し、[行の編集（Edit Row）] ボタンをクリックして、[プラグインエントリの編集（Edit Plug-In Entry）] ダイアログボックスで変更を加えます。
- プラグインを削除するには、そのプラグインを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

SSL VPN AnyConnect クライアント設定について

Cisco AnyConnect VPN クライアントは、セキュリティ アプライアンスへのセキュアな SSL および IKEv2 IPsec 接続をリモート ユーザに提供します。このクライアントにより、ネットワーク管理者がリモート コンピュータにクライアントをインストールして設定しなくても、リモート ユーザーは SSL または IKEv2 IPsec VPN クライアントを活用できます。

ヒント　IKEv2 IPsec 接続では、AnyConnect 3.0 以降のクライアントが必要です。

事前にクライアントがインストールされていない場合、リモート ユーザーは、SSL または IKEv2 IPsec VPN 接続を受け入れるように設定されているインターフェイスの IP アドレスをブラウザに入力します。セキュリティアプライアンスが http:// 要求を https:// にリダイレクトするように設定されている場合を除いて、ユーザは https://<*address*> 形式で URL を入力する必要があります。

URL を入力すると、ブラウザがそのインターフェイスに接続して、ログイン画面が表示されます。ユーザがログイン認証に成功し、セキュリティアプライアンスによってそのユーザがクライアントを要求していると識別されると、リモート コンピュータのオペレーティング システムに適合するクライアントがダウンロードされます。ダウンロード後、クライアントは自分自身でインストールと設定を行い、セキュアな接続を確立します。接続の終了時には、（セキュリティ アプライアンスの設定に応じて）そのまま残るか、または自分自身をアンインストールします。

事前にクライアントがインストールされている場合、ユーザ認証時に、セキュリティ アプライアンスはクライアントのリビジョンを検査し、必要な場合はクライアントをアップグレードします。

クライアントがセキュリティ アプライアンスとの接続をネゴシエートする場合は、Transport Layer Security（TLS）、および任意で Datagram Transport Layer Security（DTLS）を使用して接続します。DTLS により、一部の SSL 接続で発生する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

AnyConnect クライアントは、セキュリティ アプライアンスからダウンロードできます。または、システム管理者が手動でリモート ワークステーションにインストールできます。クライアントの手動インストールの詳細については、『*Cisco AnyConnect Secure Mobility Client Administrator Guide*』を参照してください。AnyConnect のマニュアルは、http://www.cisco.com/en/US/products/ps10884/tsd_products_support_series_home.html から入手できます。AnyConnect の一般情報については、http://www.cisco.com/go/anyconnect を参照してください。

セキュリティ アプライアンスは、接続を確立しているユーザのグループ ポリシーまたはユーザ名属性に基づいてクライアントをダウンロードします。自動的にクライアントをダウンロードするようにセキュリティ アプライアンスを設定できます。または、クライアントをダウンロードするかどうかをリモートユーザに確認するように設定することもできます後者でユーザが応答しなかった場合に、タイムアウト時間の経過後にクライアントをダウンロードするか、またはログイン ページを表示するように、セキュリティ アプライアンスを設定できます。

AnyConnect クライアント プロファイル

AnyConnect クライアント プロファイルは、XML ファイルに保存された一連の設定パラメータです。クライアントでは、クライアント ユーザ インターフェイスに表示される接続エントリを設定するときにこれらのパラメータを使用します。これらのパラメータ（XML タグ）には、

ホストコンピュータの名前とアドレス、および追加のクライアント機能を有効にする設定が含まれています。

AnyConnect クライアントインストールには、*AnyConnectProfile.tmpl* という名前のプロファイルテンプレートが含まれています。このテンプレートはテキストエディタを使用して編集したり、これを基にして他のプロファイルファイルを作成したりできます。ユーザインターフェイスからは使用できない高度なパラメータを設定することもできます。また、インストールには、*AnyConnectProfile.xsd* という名前の XML スキームファイル一式も含まれています。

その他の設定ポリシーの [Client Settings] タブにプロファイルを追加して、これをセキュリティアプライアンスにロードし、そのあとで、グループポリシーおよびユーザ名属性に基づいてクライアント ワークステーションにダウンロードできます。

関連項目

- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- AnyConnect プロファイルエディタ （1791 ページ）

AnyConnect プロファイルエディタ

プロファイルは、AnyConnect プロファイル エディタを使用して設定できます。このエディタは、Cisco Security Manager から起動する便利な GUI ベースの構成ツールです。Windows 用の AnyConnect ソフトウェアパッケージ。バージョン 2.5 以降にはエディタが含まれていて、このエディタは、適切な AnyConnect パッケージを AnyConnect クライアント イメージ リストに追加している場合に限り、[AnyConnectクライアントプロファイルの追加（Add AnyConnect Client Profile）][AnyConnectクライアントプロファイルの編集（Edit AnyConnect Client Profile）] ダイアログボックスからエディタを起動するとアクティベートされます。

（注） Cisco AnyConnect プロファイルエディタは独立したプログラムです。AnyConnect プロファイルの設定、および AnyConnect プロファイルエディタでできることについては、http://www.cisco.com/en/US/products/ps10884/products_installation_and_configuration_guides_list.html でオンラインで入手可能な資料を参照してください。

ナビゲーション パス

[AnyConnectクライアントプロファイルの追加（Add AnyConnect Client Profile）][AnyConnectクライアントプロファイルの編集（Edit AnyConnect Client Profile）] ダイアログボックスを開き、[エディタの起動（Launch Editor）] をクリックします（[AnyConnectクライアントプロファイルの追加（Add AnyConnect Client Profile）][AnyConnectクライアントプロファイルの編集（Edit AnyConnect Client Profile）] ダイアログボックスにアクセスする前に、まず適切な AnyConnect パッケージを AnyConnect クライアントイメージリストに追加する必要があります）。AnyConnect プロファイルエディタが表示されます。

関連項目

- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- SSL VPN サポート ファイルの概要と管理 （1660 ページ）

（注） バージョン 4.7 以降、Security Manager は AnyConnect バージョン 3.2 のサポートを提供します。

SSL VPN AnyConnect クライアント設定の定義（ASA）

ここでは、SSL および IKEv2 IPsec VPN クライアント イメージおよびプロファイルを定義する方法を示します。AnyConnect イメージおよびプロファイルの詳細については、 SSL VPN AnyConnect クライアント設定について （1789 ページ）を参照してください。

ヒント 必要なリリースの AnyConnect イメージを追加していることを確認してください。たとえば、IKEv2 IPsec VPN を設定する場合は、AnyConnect 3.0 以降のイメージを含める必要があります。通常、イメージ バージョンは、リモート アクセス VPN で展開する機能をサポートする必要があります。

関連項目

- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- AnyConnect プロファイルエディタ （1791 ページ）
- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで [クライアント設定（Client Settings）] タブをクリックします。このタブには、設定されている AnyConnect クライアントおよびプロファイルのリストを個別に表示する 2 つのテーブルがあります。

AnyConnectイメージには、順番を示す番号が含まれます。セキュリティアプライアンスは、最も大きい順番から始めて、オペレーティング システムと一致するまで、AnyConnect イメージの一部をリモート コンピュータにダウンロードします。そのため、最も一般的なオペレーティング システムで使用されるイメージに、最も大きい値を入力する必要があります。

モバイル ユーザは接続速度が遅いため、Windows Mobile 用の AnyConnect イメージをリストの最初でロードする必要があります。また、正規表現 **Windows CE** を指定し、Windows Mobile デバイスのユーザーエージェントを照合して、接続時間を短縮することもできます。モバイル デバイスのブラウザは ASA に接続するときに、HTTP ヘッダーにユーザエージェント文字列を含めます。ASA は、文字列を受信して、他の AnyConnect イメージが適切かどうかを確認せずに、すぐに Windows Mobile 用の AnyConnect をダウンロードします。

ステップ 3 AnyConnectクライアントイメージを追加する、または既存のリストを変更するには、次のいずれかを実行します。

- AnyConnect イメージを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[AnyConnectクライアントイメージの追加（Add AnyConnect Client Image）] ダイアログボックスに入力します。イメージを定義するファイル オブジェクトの名前、およびイメージのプライオリティ順を指定する必要があります。また、接続クライアントのダウンロード速度を改善するために正規表現を指定することもできます。オプションの詳細については、[Add AnyConnect Client Image][Edit AnyConnect Client Image] ダイアログボックス （1794 ページ）を参照してください。
- イメージを編集するには、イメージを選択し、[行の編集（Edit Row）] ボタンをクリックして、[AnyConnectクライアントイメージの編集（Edit AnyConnect Client Image）] ダイアログボックスで変更を行います。
- イメージを削除するには、イメージを選択し、[行の削除（Delete Row）]ボタンをクリックします。削除の確認が求められます。

ステップ 4 AnyConnectプロファイルを追加する、または既存のリストを変更するには、次のいずれかを実行します。

- AnyConnect プロファイルを追加するには、テーブルの下の [行の追加（Add Row）] ボタンをクリックして、[AnyConnectクライアントプロファイルの追加（Add AnyConnect Client Profile）] で次のオプションを設定します。
  - [AnyConnectプロファイル名（AnyConnect Profile Name）]：プロファイルの名前。

このプロファイルを使用するには、（ASA グループ ポリシーの SSL VPN フル クライアント設定 （1945 ページ）で説明されているように [Full Client] の設定ページで）セキュリティ アプライアンスに割り当てられる ASA Group Policy オブジェクトのプロファイル名を指定していることを確認します。デバイスのリモート アクセス Connection Profile ポリシーを介して ASA Group Policy オブジェクトを設定します（接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照）。

- [AnyConnectプロファイルタイプ（AnyConnect Profile Type）]：追加または編集する AnyConnect プロファイルのタイプを次から選択します。VPN、ネットワーク アクセス マネージャ、テレメトリ、Web セキュリティ、ISE ポスチャ、またはカスタマー エクスペリエンス フィードバック。
- [AnyConnectプロファイルファイル（AnyConnect Profile File）]：Anyconnect クライアントプロファイル XML ファイルを識別するファイルオブジェクトの名前。ファイル名の拡張子は、AnyConnectプロファ

イルのタイプによって異なります。VPN（.xml）、ネットワーク アクセス マネージャ（.nsp）、テレメトリ（.tsp）、、Web セキュリティ WSO（.wso）、ISE ポスチャ（. isp）、カスタマー エクスペリエンス フィードバック（.fsp）。[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。

（注） バージョン 4.7 以降、Security Manager は AnyConnect バージョン 3.2 のサポートを提供します。AnyConnect プロファイルタイプとして ISE ポスチャを選択した場合、AnyConnect プロファイル ファイルのファイル名拡張子は .isp である必要があります。

- [ストレージURLの有効化（Enable Storage URL）]：バージョン 4.12 以降、Security Manager では、ASA 9.6(2) 以降のマルチコンテキストデバイスに対して、プライベートまたは共有オプションのいずれかを選択できます。
- [エディタの起動（Launch Editor）]：[エディタの起動（Launch Editor）] をクリックし、AnyConnect プロファイルエディタを使用して、AnyConnect プロファイルファイルで指定されたプロファイルを編集するか、プロファイルファイルが指定されていない場合は新しいプロファイルを作成します。ファイル オブジェクトの詳細については、AnyConnect プロファイルエディタ （1791 ページ）を参照してください。

  （注） AnyConnect プロファイルエディタを使用して新しいプロファイルを作成する場合は、AnyConnect プロファイルファイルを指定しないでください。

- プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックして、[AnyConnectクライアントプロファイルの編集（Edit AnyConnect Client Profile）] ダイアログボックスで変更を行います。
- プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

（注） **AnyConnect イメージ/プロファイル**設定を保存するには、デバイスをマルチコンテキストデバイスとして Cisco Security Manager に追加する必要があります。Security Manager が **ストレージ URL** を取得するにはシステムコンテキストが必須であり、デフォルトの**ストレージ URL**（disk0:/csm）がデフォルトで割り当てられるため、マルチコンテキストデバイスをスタンドアロンとして追加すると、**AnyConnect イメージ/プロファイル**設定を追加するときに展開エラーが発生する可能性があります。このデフォルトの割り当ては、スタンドアロンデバイスとして追加されたマルチコンテキストデバイスのシステムコンテキストがないため、Security Manager が**ストレージ URL** を取得できなくなることで発生します。

[Add AnyConnect Client Image][Edit AnyConnect Client Image] ダイアログボックス

[Add or Edit AnyConnect Client Image] ダイアログボックスを使用して、クライアント イメージとしてパッケージ ファイルを作成または編集し、セキュリティ アプライアンスがイメージをリモート ワークステーションにダウンロードする順序を確立します。

ナビゲーション パス

ASA デバイスの [SSL VPNのその他の設定（SSL VPN Other Settings）] ポリシーの [クライアント設定（Client Settings）] タブから、[AnyConnectクライアントイメージ（AnyConnect Client Image）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、イメージを選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、SSL VPN AnyConnect クライアント設定について （1789 ページ）を参照してください。

関連項目

- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- SSL VPN サポート ファイルの概要と管理 （1660 ページ）

フィールド リファレンス

表 395 : [Add or Edit AnyConnect Client Image] ダイアログボックス

要素	説明
AnyConnect クライアントイメージ	Anyconnect クライアントを識別するファイル オブジェクトの名前。[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。
Image Order	セキュリティ アプライアンスがクライアント イメージをリモート ワークステーションにダウンロードする順序。イメージは、プライオリティ順でダウンロードされます。そのため、最も一般的なオペレーティング システムで使用されるイメージに、より小さい値を入力する必要があります。

要素	説明
正規表現	ユーザ エージェントを照合する正規表現。既存の正規表現のポリシー オブジェクトの名前を入力するか、[選択（Select）] をクリックして [正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスからエントリを選択します。新しい正規表現を追加するには、[正規表現セレクタ（Regular Expressions Selector）] ダイアログボックスの [追加]（+）（Add (+)）] ボタンをクリックします。詳細については、正規表現の追加/編集（1126 ページ）を参照してください。 Windows Mobile の AnyConnect パッケージを追加する場合、正規表現の **Windows CE** を指定して、Windows Mobile デバイスのユーザーエージェントを照合します。これにより、モバイルデバイスの接続時間を短縮できます。モバイル デバイスのブラウザは適応型セキュリティ アプライアンスに接続するときに、HTTP ヘッダーにユーザエージェント文字列を含めます。適応型セキュリティ アプライアンスは、文字列を受信して、他の AnyConnect イメージが適切かどうかを確認せずに、すぐに Windows Mobile 用の AnyConnect をダウンロードします。
ストレージ URL を有効にします。 （ASA 9.6(2) 以降のマルチコンテキストデバイスのみ）	バージョン 4.12 以降、Security Manager では、ASA 9.6(2) 以降のマルチコンテキストデバイスに対して、プライベートまたは共有オプションのいずれかを選択できます。 （注） **AnyConnect イメージ/プロファイル**設定を保存するには、デバイスをマルチコンテキストデバイスとして Cisco Security Manager に追加する必要があります。Security Manager が **ストレージ URL** を取得するにはシステムコンテキストが必須であり、デフォルトの**ストレージ URL**（disk0:/csm）がデフォルトで割り当てられるため、マルチコンテキストデバイスをスタンドアロンとして追加すると、**AnyConnect イメージ/プロファイル**設定を追加するときに展開エラーが発生する可能性があります。このデフォルトの割り当ては、スタンドアロンデバイスとして追加されたマルチコンテキストデバイスのシステムコンテキストがないため、Security Manager が**ストレージ URL** をフェッチできなくなるために発生します。

SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA）

認証によりネットワーク リソースを保護するには、多くの方法があります。多くの組織は、Kerberos を使用して特定の Web アプリケーションを保護し、ユーザ名とパスワード、デジタル証明書、RSA SecureID または SmartCards などのその他の認証技術を使用して、SSL VPN へのアクセスを制御します。ただし、Kerberos プロトコルの制限により、ユーザがすでに別の技術を使用して VPN に対する認証を行っている場合、Kerberos 認証は行われません。

Microsoft では、Windows Server 2003 より、この Kerberos における制限を解決しています。プロトコル移行および制約委任を使用することで、ASA は、Windows ドメイン コントローラでの Kerberos Key Distribution Center（KCD）に対する認証を行い、Kerberos 以外のプロトコルを

使用して ASA に対する認証を行っているユーザの代替チケットを取得できます。ASA は、代替チケットを使用して、リモート ユーザの他の Kerberos サービス チケットを取得できます。

Kerberos Constrained Delegation が機能するようにドメイン コントローラを設定するには、次のようにする必要があります。

- Kerberos 認証を使用するサービスの各インスタンスでは、クライアントがネットワーク上で識別できるように、Service Principle Name（SPN）が定義されている必要があります。SPN は、サービスのインスタンスが実行している Windows アカウントの Active Directory [Service-Principal-Name] 属性に登録します。特定のコンピュータで実行している別のサービスに対してあるサービスを認証する必要がある場合、そのサービスの SPN により、該当するコンピュータで実行中の他のサービスと区別します。

SPN のシンタックスは、*service_class/host_name:port* です。

- *service_class* は、サービスを識別します。これは、http などの組み込みサービス、またはユーザ定義サービスです。
- *host_name* は、サービスをホストするサーバーの完全修飾ドメイン名または NetBIOS 名を識別します。IP アドレスにすることはできません。
- *port* は、サービスが実行するポートを識別します。デフォルト サービス ポートを使用する場合は、port を省略できます。
- ASA が使用できるサービス アカウント ユーザ名およびパスワードを作成します。任意の認証プロトコルに対して Kerberos Constrained Delegation を許可するアカウントを設定します。また、ユーザ アカウントには、委任できない機密アカウントを使用しないでください。

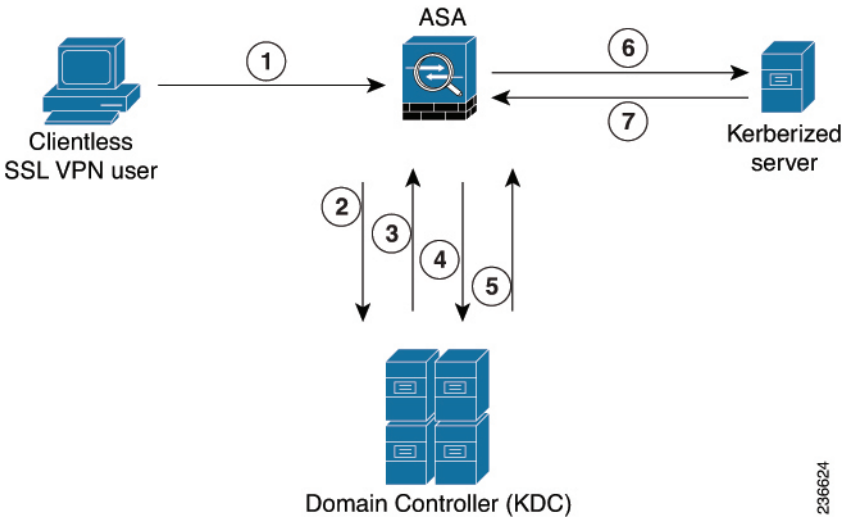
KCD を許可するように ASA を設定するには、ASA がドメインに参加したら、ASA のドメイン コントローラの [Users and Computers] リスト下にエントリが表示される必要があります。[委任（Delegation）] タブの [プロパティ（Properties）] ダイアログボックスで、[指定されたサービスの委任にのみこのコンピュータを信頼する（Trust this computer for delegation to specified services only）] を選択してから、[任意の認証プロトコルを使用する（Use any authentication protocol）] を選択します。認可サービスのテーブルで、ユーザに代わり ASA が認証を委任されるすべてのサービスを追加します。

ヒント Windows ドメイン コントローラでこの機能を設定する方法の詳細については、Microsoft のマニュアルを参照してください。

ASA が Kerberos Constrained Delegation を使用できるようにするには、SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA）（1799 ページ）で説明されているように ASA を設定する必要があります。この機能を使用できるのは、ASA Software リリース 8.4 以降のみです。

次の例では、Kerberos Constrained Delegation が ASA でホストされるクライアントレス SSL VPN でどのように機能するかについて説明しています。

図 *41 : Kerberos Constrained Delegation* の例



設定されている認証メカニズムで SSL VPN ユーザーのアイデンティティを確認した後、ASA は、プロトコル移行を使用して、ユーザーの代わりに認証を行うために Kerberos プロトコルに切り替えます。次に、ユーザーのログイン情報ではなく Kerberos サービスチケットを、認証のために Kerberos を受け入れる公開済み Web サーバーに送信します。これらのステップを次に示します。

1. SSL VPN ユーザ セッションが、ユーザに設定されている認証メカニズムを使用して ASA により認証されます。たとえば、Smartcard クレデンシャルの場合、ASA は、デジタル証明書から必要な情報（ユーザーのプリンシパル名）を抽出して、Windows Active Directory に対して LDAP 認可を実行します。
2. 認証が成功すると、ユーザは、ASA SSL VPN ポータル ページにログインします。VPN ユーザは、URL をポータルページに入力するか、ブックマークをクリックして、Web サービスにアクセスします。このアクセスで認証が必要な場合、サーバは、ASA クレデンシャルの認証確認を行い、同時に、サーバでサポートされている認証メカニズムのリストを送信します。認証確認時の HTTP ヘッダーに基づいて、ASA は、サーバで Kerberos 認証が必要かどうかを決定します。バックエンドサーバとの接続で、Kerberos 認証が必要な場合、ASA は、ユーザの代わりにそれ自体のために、代替チケットを KDC から要求します。
3. KDC は、要求されたチケットを ASA に返します。これらのチケットは ASA に渡されますが、ユーザーの許可データが含まれています。

（注） これらの最初のステップでは、プロトコル移行が行われます。これらのステップの後、Kerberos 以外の認証プロトコルを使用して ASA に対して認証を行ったユーザは、透過的に、Kerberos を使用して KDC に対して認証されます。

1. ここで、ASA は、ユーザがアクセスする特定のサービス用の KDC からのサービス チケットを要求します。サービス チケット要求には、サービスの SPN（一意な ID）が含まれます。
2. KDC は、特定のサービスのサービス チケットを ASA に返します。
3. ASA は、このサービス チケットを使用して、Web サービスへのアクセスを要求します。前述の例の場合、これは、HTTP GET 要求で Web サーバに送信されます。
4. Web サーバは、Kerberos サービス チケットを認証して、サービスへのアクセスを付与します。認証に失敗すると、表示されるポータルを確認したあとで、該当するエラー メッセージが表示されます。

SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA）

[SSL VPN Other Settings] ページの [Microsoft KCD Server] タブを使用して、ASA でホストされるクライアントレス SSL VPN の Kerberos Constrained Delegation（KCD）を設定します。

KCD は、Kerberos における制限に対処します。Kerberos 以外の方法を使用して SSL VPN に対する認証を行うユーザは、Kerberos で保護されたリソースにアクセスできません。この場合、ASA などのリモート アクセス デバイスは、Kerberos 以外の方法を使用するユーザを認証できません。ただし、企業内で Kerberos を使用して認証された Web アプリケーションへのシングル サインオン アクセスは提供されます。

この制限がネットワークに適用される場合、KCD を設定してこの制限を回避できます。KCD は、ASA に対する Kerberos 認証をオフロードします。ユーザは、SSL VPN ポータルを使用して企業ネットワークにログインすると、これ以降、Kerberos 保護サービスに透過的にアクセスします。

ヒント

- KCD では、ASA リリース 8.4+ が必要です。これ以外のリリースで KCD を設定しても、設定は無視されます。
- この機能は、クライアントレス SSL VPN アクセスだけで使用されます。
- KCD では、ドメイン コントローラとして設定された、Microsoft Windows Server（2003 または 2008）が必要です。
- SSL VPN Bookmark ポリシー オブジェクトを使用して、SSL VPN ポータル ページに含めるブックマークを定義した場合、サービスがデフォルト以外のポートを使用していると、場合によっては、明示的な Service Principle Name（SPN）パラメータをブックマークに追加する必要があります。Kerberos 認証を使用するサービスでは、SPN は、サービスが実行するアカウントの Service-Principle-Name 属性で定義される必要があります。

ブックマークは、この設定を反映する必要があります。SPN は、URL: http://<url>?SPN=<spn> or http://<url>?SPN=<spn> でのパラメータです。たとえば、**http://owa.example.com?SPN=http/owa:444** など。SPN 構文の詳細については、SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） （1796 ページ）を参照してください。

- この機能を設定するには、ホスト名、DNS および NTP ポリシーも設定する必要があります。ホスト名ポリシーでは、ホスト名およびドメイン名の両方を設定します。
- Kerberos 認証では、ホスト間のクロックは、5 分（デフォルト設定）以下で同期化される必要があります。この制限は、ASA、ドメイン コントローラおよびアプリケーション サーバのクロックに適用されます。すべてのサーバで同じ NTP サーバを設定すると、この要件に対処できます。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで、[Microsoft KCDサーバー（Microsoft KCD Server）] タブをクリックします。

ステップ 3 [KCDの設定（Configure KCD）] を選択して、次のオプションを設定します。

- [KCDサーバー（KCD Server）]：Kerberos Constrained Delegation で使用する Microsoft KCD サーバー（ドメインコントローラ）を識別する AAA サーバー グループ オブジェクト。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。オブジェクトは、Kerberos AAA サーバ ポリシー オブジェクトを使用して、ドメイン コントローラを識別する必要があります。
- [ユーザー名、パスワード、確認（Username, Password, Confirm）]：ASA が Active Directory ドメインに参加するために使用できるユーザーアカウント。

ASA が Kerberos プロトコル移行および Kerberos Constrained Delegation を使用し、リモート アクセス ユーザの代わりにサービス チケットを取得するには、ドメイン コントローラ認証のために ASA により使用されるアカウントは、Active Directory に含まれている必要があり、任意のプロトコルで Kerberos Constrained Delegation を許可できるように設定される必要があります。また、ユーザ アカウントには、委任できない機密アカウントを使用しないでください。Active Directory の設定要件の詳細については、SSL VPN の Kerberos Constrained Delegation（KCD）について（ASA） （1796 ページ）を参照してください。

AnyConnect カスタム属性（ASA）の設定

AnyConnect カスタム属性が、ASA ソフトウェアをアップグレードすることなく、新しいクライアントコントロールの追加を総合的にサポートする機能を ASA に提供することで、新しいエンドポイント機能のより迅速な配信と展開が可能になります。

[SSL VPNのその他の設定（ SSL VPN Other Settings）] ページの [AnyConnectカスタム属性（AnyConnect Custom Attribute）] タブでは、設定済みの AnyConnect カスタム属性を表示したり、新しい属性を追加したり、既存の属性を変更または削除したりできます。

関連項目

- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで、[AnyConnectカスタム属性（AnyConnect Custom Attribute）] タブをクリックします。[AnyConnectカスタム属性（AnyConnect Custom Attribute）] タブには、定義済みのすべてのカスタム属性が一覧表示されます。

ステップ 3 次のいずれかを実行します。

- カスタム属性を追加するには、テーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[AnyConnectカスタム属性の追加（Add AnyConnect Custom Attribute）] ダイアログボックスに入力します。これらのオプションについては、[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1801 ページ）で詳しく説明されています。
- カスタム属性を編集するには、そのカスタム属性を選択し、[行の編集（Edit Row）] ボタンをクリックして、[プラグインエントリの編集（Edit Plug-In Entry）] ダイアログボックスで変更します。
- カスタム属性を削除するには、カスタム属性を選択して [行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。

[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス

[AnyConnectカスタム属性の追加または編集（Add or Edit AnyConnect Custom Attribute）] ダイアログボックスを使用して、AnyConnect カスタム属性を追加または変更します。AnyConnect カスタム属性により、ASA ソフトウェアをアップグレードすることなく、新しいクライアントコ

ントロールの追加を総合的にサポートする機能を ASA に提供することで、新しいエンドポイント機能のより迅速な配信と展開が可能になります。

バージョン 4.7 以降、Security Manager では、ソフトウェアバージョン 9.3(1) 以降を実行している ASA デバイスの既存のカスタム属性タイプにカスタム属性データを追加できます。[AnyConnectカスタム属性の追加または編集（Add or Edit AnyConnect Custom Attribute）] ダイアログボックスを使用して、既存の AnyConnect カスタム属性タイプの属性名と属性値を追加または変更します。詳細については、[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1802 ページ）を参照してください。

ナビゲーション パス

ASA デバイスの SSL VPN の [その他の設定（Other Settings）] ポリシーに含まれる [AnyConnectカスタム属性（AnyConnect Custom Attribute）] タブから、[AnyConnectカスタム属性（AnyConnect Custom Attribute）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、属性を選択して [行の編集（Edit Row）] ボタンをクリックします。タブを開く方法の詳細については、AnyConnect カスタム属性（ASA）の設定 （1801 ページ）を参照してください。

関連項目

- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- SSL VPN サポート ファイルの概要と管理 （1660 ページ）

フィールド リファレンス

表 *396 : [AnyConnectカスタム属性の追加または編集（Add or Edit AnyConnect Custom Attribute）] ダイアログボックス*

要素	説明
タイプ	AnyConnect カスタム属性のタイプ。Security Manager で属性を参照する場合、および AnyConnect クライアントに送信される集約認証プロトコルメッセージで使用されます。最大長は 32 文字です。
説明	属性の使用方法の自由形式の説明。このテキストは、カスタム属性がグループポリシー属性コンフィギュレーションモードから参照された場合に、コマンドヘルプで表示されます。最大長は 128 文字です。

[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス

Security Manager version 4.7 以降、[AnyConnectカスタム属性の追加または編集（Add or Edit AnyConnect Custom Attribute）] ダイアログボックスを使用して、既存の AnyConnect カスタム属性タイプの属性名と属性値を追加または変更できます。

ナビゲーション パス

ASA デバイスの SSL VPN のその他の設定ポリシーの [AnyConnectカスタム属性（AnyConnect Custom Attribute）] タブをクリックします。[カスタム属性（Custom Attribute）] テーブルで属性タイプを選択し、[カスタム属性データ（Custom Attribute Data）] テーブルの [行の追加（Add Row）] ボタンをクリックします。または、[カスタム属性データ（Custom Attribute Data）] テーブルで既存のカスタム属性データを選択し、[行の編集（Edit Row）] ボタンをクリックします。

属性タイプごとに、対応する値を持つ複数の属性名を定義できます。

属性タイプの追加または変更については、 SSL VPN AnyConnect クライアント設定について（1789 ページ）を参照してください。

関連項目

- SSL VPN AnyConnect クライアント設定について （1789 ページ）
- [AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1801 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- SSL VPN サポート ファイルの概要と管理 （1660 ページ）

フィールド リファレンス

表 *397 : [AnyConnect*カスタム属性の追加または編集（*Add or Edit AnyConnect Custom Attribute*）*]* ダイアログボックス**

要素	説明
Attribute Name	AnyConnect カスタム属性のタイプ。この名前は、group-policy および dynamic-access-policy-record 設定モードで属性を参照するときに使用します。最大長は 32 文字です。
属性値（Attribute Value）	属性値を含む自由形式の文字列。この属性値は、属性名に関連付けられ、接続の設定中にクライアントに渡されます。文字列の最大長は 420 文字です。 属性値には、複数のテキスト行を含めることができます。

SSL VPN の高度な設定の定義（ASA）

[SSL VPN Other Settings] ページの [Advanced] タブを使用して、メモリ、オンスクリーン キーボードおよび内部パスワード機能を ASA デバイスで設定します。Cisco Security Manager 4.15 以降では、HSTS サポートを有効にして、タイムアウト値を指定することもできます。これらの設定はすべて任意です。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [その他の設定（Other Settings）] ページで [詳細（Advanced）] タブをクリックします。

ステップ 3 [メモリサイズ（Memory Size）] フィールドで、SSL VPN セッションに割り当てるメモリ容量を指定します。デフォルトは 50% です。

設定を変更するには、次のいずれかのオプションを選択して、目的の数値を入力します。

- [物理メモリ合計の割合（% of Total Physical Memory）]：全体のメモリに対するパーセンテージで指定します。デフォルトは 50% です。
- [キロバイト（Kilobytes）]：KB 単位で指定します。許可される最小設定値は、20 KB です。次の例に示すように、ASA モデルのタイプによって合計のメモリ量が異なるため、KB 単位では指定することは推奨されません。

（注） メモリ サイズを変更した場合、新しい設定は、システムをリブートしないと有効になりません。

ステップ 4 [オンスクリーンキーボードの有効化（Enable On-Screen Keyboard）] フィールドで、次のいずれかのオプションを選択します。

- [無効（Disabled）]：オンスクリーンキーボードは表示されません。ユーザは、標準のキーボードを使用してクレデンシャルを入力する必要があります。これがデフォルトです。
- [すべてのページ（On All Pages）]：ユーザーは、ログインクレデンシャルが必要になると表示されるオンスクリーンキーボードを使用してクレデンシャルを入力できます。
- [ログインページのみ（On Logon Page Only）]：ユーザーは、ログインページに表示される（クレデンシャルを必要としないページでは表示されません）オンスクリーンキーボードを使用してクレデンシャルを入力できます。

（注） Cisco Security Manager 4.24 以降、オンスクリーンキーボードの有効化機能は、ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

ステップ 5 内部サイトにアクセスするときに追加パスワードを要求する場合は、[内部パスワードの入力を許可（Allow Users to Enter Internal Password）] を選択します。この機能は、内部パスワードを SSL VPN パスワードとは別のパスワードにする必要がある場合に役立ちます。たとえば、ASA への認証にはあるワンタイム パスワードを使用して、内部サイトには別のパスワードを使用できます。

（注） HSTS オプションは、ASA 9.8.2 以降のデバイスでのみ使用できます。

ステップ 6 [HTTP厳重トランスポートセキュリティ（HSTS）（HTTP Strict Transport Security (HSTS)）] 領域で、次の手順を実行します。

- HSTS サポートを有効にするには、[HSTSヘッダーの有効化（Enable HSTS Header）] チェックボックスをオンにします。HSTS 機能は、ヘッダーをクライアントに送信することで有効にできます。サポートを無効にするには、このチェックボックスをオフにします。
- [HSTSヘッダーの有効化（Enable HSTS Header）] チェックボックスを選択した場合は、[HSTSヘッダーのタイムアウト（HSTS Header Timeout）] にタイムアウト値を入力します。このフィールドを空白のままにすると、Cisco Security Manager はデフォルトのタイムアウト値である 10886400 を使用します。
- ヘッダーにサブドメイディレクティブを含める場合は、[サブドメインを含める（Include Sub Domains）] チェックボックスをオンにします。
- ヘッダーにペイロードディレクティブを含める場合は、[ペイロード（Payload）] チェックボックスをオンにします。
- [HSTSクライアントの有効化（Enable HSTS-Client）] チェックボックスをオンにすると、HSTS ホストの HSTS ポリシーの適用が制御されます。
- [X-Content-Type-Optionsの有効化（Enable X-Content-Type-Options）] チェックボックスをオンにすると、X-Content-Type-Options 応答ヘッダーをクライアントに送信できます。
- [X-XSS-Protectionの有効化（Enable X-XSS-Protection）] チェックボックスをオンにすると、X-XSS-Protection 応答ヘッダーをクライアントに送信できます。

（注） [ペイロード（Payload）] チェックボックスを選択すると、[サブメインを含める（Sub Domains）] もデフォルトで選択されます。

- ペイロードを選択する場合は、HSTS ヘッダーのタイムアウト値が 31536000 以上であることを確認してください。

（注） バージョン 4.21 以降、Cisco Security Manager は HSTS サーバーコマンドで [HSTSクライアントの有効化（Enable HSTS-Client）]、[X-Content-Type-Optionsの有効化（Enable X-Content-Type-Options）]、および [X-XSS-Protectionの有効化（Enable X-XSS-Protection）] CLI オプションのサポートを開始します。ただし、[コンテンツセキュリティポリシー（Content-Security-Policy）] はサポートされていません。これは Flex Config を介してのみ設定できます。

SSL VPN サーバー検証の設定（ASA）

クライアントレス SSL VPN 経由でリモート SSL 対応サーバに接続する場合は、リモート サーバを信頼できること、また、接続先が実際にサーバであることを認識することが重要です。ASA 9.0 には、クライアントレス SSL VPN の信頼できる認証局（CA）証明書のリストに対する SSL サーバ証明書の検証のためのサポートが追加されています。

HTTPS プロトコルを使用して Web ブラウザ経由でリモート サーバに接続する場合、サーバはサーバ自体を識別するために CA が署名したデジタル証明書を提供します。Web ブラウザには、サーバ証明書の有効性を検証するために使用される一連の CA 証明書が付属しています。これは、公開キー インフラストラクチャ（PKI）の 1 つの形式です。

ブラウザが証明書管理の機能を提供するのと同様に、ASA も信頼できる証明書のプール管理機能の形式を提供します（trustpools）。これは、複数の既知の CA 証明書を表すトラストポイントの特殊なケースと見なすことができます。ASA には、Web ブラウザで提供されるのと同様のデフォルトの証明書のバンドルが含まれますが、管理者がアクティブにするまで非アクティブとなります。

（注） すでに Cisco IOS の trustpools に精通している場合、ASA バージョンが、似ているが同じではないことがわかります。

ここでは、クライアントレス SSL VPN ユーザーの HTTPS サーバー検証を有効にする方法について説明します。

関連項目

- 他の SSL VPN 設定の定義（ASA） （1774 ページ）
- 信頼できるプール設定の設定（ASA） （1746 ページ）
- Trustpool Manager の使用 （1748 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** を選択します。[SSL サーバー検証（SSL Server Verification）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（ASA）（Other Settings (ASA)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[SSL サーバー検証（SSL Server Verification）] タブをクリックします。

ステップ 2 クライアントレス SSL VPN ユーザーの HTTPS サーバー検証を有効にするには、[有効（Enable）] を選択します。

ステップ 3 サーバー証明書の検証に失敗した場合に実行するアクションを指定します。

- [ユーザーを HTTPS から切断（Disconnect user from Https）] ページ：サーバーを検証できなかった場合は切断します。
- [ユーザーに HTTPS への接続を許可（Allow user to continue to Https）] ページ：チェックが失敗した場合でも、ユーザーが接続を継続できるようにします。

SSL VPN 共有ライセンスの設定（ASA 8.2+）

[SSL VPN Shared License] ページを使用して、SSL VPN 共有ライセンスを設定します。

多数の SSL またはリモート アクセス IKEv2 IPsec VPN セッションに対応した共有ライセンスを購入し、ASA デバイスの 1 つを共有ライセンス サーバ、残りのデバイスをクライアントとして設定すると、必要に応じて ASA デバイスのグループ全体でセッションを共有できます。サーバ ライセンスの場合、500 単位で 500 ～ 50,000 ライセンス、1000 単位で 50,000 ～ 1,040,000 ライセンスを共有できます。

ライセンスは、SSL または IKEv2 IPsec 接続を確立する各リモート アクセス ユーザにより使用されます。

（注） 共有ライセンスは、AnyConnect Essentials ライセンスと同時には使用できません。

ここでは、共有ライセンスの設定手順について説明します。

- 共有ライセンス クライアントとしての ASA デバイスの設定 （1809 ページ）
- 共有ライセンス サーバとしての ASA デバイスの設定 （1810 ページ）

ナビゲーション パス

- （デバイス ビュー）バージョン 8.2 以降を使用する ASA デバイスを選択し、ポリシー セレクタから [リモート アクセス VPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（Shared License）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから、[リモート アクセス VPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（ASA 8.2+）（Shared License (ASA 8.2+)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 398 : [SSL VPN Shared License] ページ

要素	説明
Select Role	設定するロール（[Shared License Client] または [Shared License Server]）。選択した項目によって、表示されるフィールドが異なります。
Shared License Client	
共有秘密鍵（Shared Secret）	共有ライセンス サーバとの通信に使用される、大文字と小文字が区別される文字列（4 ～ 128 文字）。
ライセンス サーバ	ライセンス サーバとして設定されている ASA デバイスを識別するネットワーク/ホスト オブジェクトの IP アドレスまたは名前。[選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
License Server Port	ライセンス サーバが通信する TCP ポートの番号。ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。
Select Backup Role of Client	クライアントのバックアップ ロール。 • [Client Only]：選択すると、クライアントはクライアントとしてだけ機能します。この場合は、別のデバイスをバックアップ サーバとして指定できます。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。 • [Backup Server]：選択すると、クライアントはバックアップ サーバとしても機能します。この場合は、この目的に使用されるインターフェイスも指定する必要があります。インターフェイス名またはインターフェイス ロール オブジェクトのカンマ区切りリストを入力します。あるいは、[選択（Select）]をクリックして、インターフェイスまたはオブジェクトを選択するか、新しいオブジェクトを作成します。
Shared License Server	
共有秘密鍵（Shared Secret）	共有ライセンス サーバとの通信に使用される、大文字と小文字が区別される文字列（4 ～ 128 文字）。
License Server Port	ライセンス サーバが通信する TCP ポートの番号。ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。
更新間隔（Refresh Interval）	10 ～ 300 秒のリフレッシュ間隔。デフォルトは 30 秒です。
インターフェイス	クライアントとの共有ライセンスの通信に使用されるインターフェイスのカンマ区切りリスト。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックしてインターフェイスまたはオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Configure Backup shared SSL VPN License Server	共有ライセンス サーバのバックアップ サーバを設定するかどうかを指定します。このオプションを選択した場合は、次の項目を設定します。 • [バックアップライセンスサーバー（Backup License Server）]：現在のサーバーが使用できなくなった場合のバックアップ ライセンス サーバーとして機能するサーバーの IP アドレス、またはアドレスを含むネットワーク/ホストオブジェクト。[選択（Select）] をクリックしてオブジェクトを選択するか、新しいオブジェクトを作成します。 • [バックアップサーバーのシリアル番号（Backup Server Serial Number）]：バックアップ ライセンス サーバーのシリアル番号。 • [HAペアのシリアル番号（HA Peer Serial Number）]：（任意）フェールオーバーペアのバックアップサーバーのシリアル番号。

ここでは、次の内容について説明します。

- 共有ライセンス クライアントとしての ASA デバイスの設定 （1809 ページ）
- 共有ライセンス サーバとしての ASA デバイスの設定 （1810 ページ）

共有ライセンス クライアントとしての ASA デバイスの設定

ここでは、ASA デバイスを共有ライセンス クライアントとして設定する方法について説明します。

ヒント SSL VPN Shared License Client アクティベーション キーがデバイスに存在することを確認する必要があります。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASAデバイスを選択して、ポリシーセレクタから[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（Shared License）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（ASA 8.2+）（Shared License (ASA 8.2+)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SSL VPN Shared License] ページが表示されます（SSL VPN 共有ライセンスの設定（ASA 8.2+） （1806 ページ）を参照）。

ステップ 2 デバイスのロールとして [共有ライセンスクライアント（Shared License Client）] を選択します。

ステップ 3 [Shared Secret] フィールドに、共有ライセンス サーバとの通信に使用されるストリング（4 ～ 128 文字で、大文字と小文字が区別される）を入力して、確認します。

ステップ 4 [License Server] フィールドで、ライセンス サーバとして設定されている ASA デバイスを識別するネットワーク/ホスト オブジェクトの IP アドレスまたは名前を入力します。

ステップ 5 [License Server Port] フィールドに、ライセンス サーバが通信する TCP ポートの番号を入力します。

ステップ 6 クライアントのロールを選択します。

- [クライアントのみ（Client Only）]：選択すると、クライアントはクライアントとしてのみ機能します。この場合は、別のデバイスをバックアップ サーバとして指定できます。
- [バックアップサーバー（Backup Server）]：選択すると、クライアントはバックアップサーバーとしても機能します。この場合は、この目的に使用されるインターフェイスも指定する必要があります。

共有ライセンス サーバとしての ASA デバイスの設定

ここでは、ASA デバイスを共有ライセンス サーバとして設定する方法について説明します。

ヒント SSL VPN Shared License Server アクティベーション キーがデバイスに存在することを確認する必要があります。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（Shared License）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [共有ライセンス（ASA 8.2+）（Shared License (ASA 8.2+)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SSL VPN Shared License] ページが表示されます（SSL VPN 共有ライセンスの設定（ASA 8.2+） （1806 ページ）を参照）。

ステップ 2 デバイスのロールとして [共有ライセンスサーバー（Shared License Server）] を選択します。

ステップ 3 [Shared Secret] フィールドに、共有ライセンス サーバとの通信に使用されるストリング（4 ～ 128 文字で、大文字と小文字が区別される）を入力して、確認します。

ステップ 4 [License Server Port] フィールドに、ライセンス サーバが通信する TCP ポートの番号を入力します。

ステップ 5 [Refresh Interval] フィールドに、リフレッシュ間隔として使用される 10 ～ 300 秒の間の値を入力します。デフォルトは 30 秒です。

ステップ 6 [Interfaces] フィールドに、クライアントとの通信に使用されるインターフェイスを入力または選択します。

ステップ 7 （オプション）（任意）[共有SSL VPNライセンスサーバーのバックアップを設定（Configure Backup shared SSL VPN License Server）] を選択して、共有ライセンスサーバーのバックアップサーバーを設定します。設定項目は次のとおりです。

- [バックアップライセンスサーバー（Backup License Server）]：現在のサーバーが使用できなくなった場合のバックアップ ライセンス サーバーとして機能するサーバーの IP アドレス、またはアドレスを含むネットワーク/ホストオブジェクト。
- [バックアップサーバーのシリアル番号（Backup Server Serial Number）]：バックアップ ライセンス サーバーのシリアル番号。
- [HAペアシリアル番号（HA Peer Serial Number）]：（任意）フェールオーバーペアのバックアップサーバーのシリアル番号。

クライアントレス SSL VPN ポータルのカスタマイズ

ブラウザベースのクライアントレス SSL VPN のポータル ページに使用する Web サイトとそのコンテンツは、カスタマイズできます。ASA デバイスでは、IOS デバイスよりもさまざまなカスタマイゼーションが可能です。ユーザが VPN にログインしたとき、または VPN からログアウトしたときに表示される Web ページの外観、ポータルのホームページ、およびユーザが使用可能なブックマークとスマート トンネルを定義する、さまざまなポリシー オブジェクトを作成できます。

ここでは、次の内容について説明します。

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）
- ASA デバイスの独自 SSL VPN ログイン ページの作成 （1817 ページ）
- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （1820 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化 （1825 ページ）

SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定

SSL VPN カスタマイゼーション オブジェクトは、ユーザに表示される、ブラウザベースのクライアントレス SSL VPN Web ページの外観を記述します。これには、ユーザが ASA セキュリ

ティ アプライアンスに接続したときに表示されるログイン ページ、認証後に表示されるホームページ、およびユーザが SSL VPN サービスからログアウトしたときに表示されるログアウト ページが含まれます。

SSL VPN カスタマイゼーション オブジェクトは、ASA デバイスに ASA グループ オブジェクトまたは Remote Access VPN Connection ポリシーを定義する場合に使用します。それぞれのユーザ グループに対して、そのグループ専用に設計された Web ページが表示されるように、いくつかのカスタマイゼーション オブジェクトを作成し、複数の ASA グループまたは接続プロファイルを定義できます。カスタマイゼーションには、各グループに適した言語で Web ページをローカライズすることも含まれています。ローカリゼーションの詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。

まず、ユーザが初めて接続するとき、接続プロファイルで識別されたデフォルトのカスタマイゼーション オブジェクトによって、ログイン画面の表示方法が決定されます。ユーザがログイン ページの接続プロファイル リストとは異なるグループを選択した場合、そのグループに独自のカスタマイゼーションが設定されていれば、選択したグループのカスタマイゼーション オブジェクトを反映するように画面が変更されます。リモート ユーザが認証されると、グループ ポリシーに割り当てられているカスタマイゼーション オブジェクトによって、画面の外観が決定されます。

この手順で説明した SSL VPN カスタマイゼーション オブジェクトを作成したあとは、このオブジェクトを使用して、次のポリシーのポータル特性を指定できます。

- ASA グループ ポリシー オブジェクトの [SSL VPN] > [設定（Settings）] ページで（ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照）、次のポリシーのいずれかを選択します。
  - **[Remote Access VPN] > [Group Policies]**
  - [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]
- [リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）] ポリシーで、[SSL] タブの SSL VPN カスタマイゼーション オブジェクトを指定することもできます（[SSL] タブ（[Connection Profiles]） （1734 ページ）を参照）。

関連項目

- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス （2011 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ヒント　SSL VPN カスタマイゼーション オブジェクトは、このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに作成することもできます。詳細については、ポリシーのオブジェクトの選択　（288 ページ）を参照してください。

ステップ 2　オブジェクト タイプ セレクタから [SSL VPNのカスタマイズ（SSL VPN Customization）] を選択します。[SSL VPN Customization] ページが開き、既存の SSL VPN カスタマイゼーション オブジェクトのリストが表示されます。

ステップ 3　作業領域を右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add SSL VPN Customization] ダイアログボックスが表示されます（[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス　（1992 ページ）を参照）。

ステップ 4　オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5　さまざまなページの設定を行う前に、[Preview] ボタンを使用してデフォルト設定を表示します。[レビュー（Preview）] をクリックすると [参照（browser）] ウィンドウが開き、[ログイン（Logon）] ページ、[ポータル（Portal）] ページ、または [ログアウト（Logout）] ページのうち、コンテンツ テーブルで選択されたいずれかのページの現在の設定が表示されます（これらのフォルダのいずれかのページを選択することは、親フォルダを選択することと同じです）。

ヒント　設定を変更したあと、希望したとおりに変更されているかを確認するには[プレビュー（Preview）] をクリックします。

ステップ 6　ログイン ページの設定を行います。この Web ページは、ユーザが SSL VPN ポータルに接続したときに最初に表示されるページです。VPN へのログインに使用されます。ダイアログボックスの左側のコンテンツ テーブルで、[Logon Page] フォルダから次の項目を選択し、設定を表示および変更します。

- [ログインページ（Logon Page）]：ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。
- [タイトルパネル（Title Panel）]：[ログイン（Logon）] ページで、Web ページ内にタイトルを表示するかどうかを定義します。タイトル パネルをイネーブルにすると、使用するタイトル、フォント、フォント サイズとフォントの太さ、スタイル、および色を指定できます。ロゴのグラフィックを識別するファイル オブジェクトを選択することもできます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel]　（1996 ページ）を参照してください。
- [言語（Language）]：ASA デバイスで他言語への変換テーブルを設定し、そのテーブルを使用する場合は、サポートされる言語を設定して、ユーザが自分の言語を選択するようにできます。変換テーブルおよびローカリゼーション サポートの詳細については、ASA デバイスの SSL VPN Web ページのローカライズ　（1815 ページ）を参照してください。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Language]　（1997 ページ）を参照してください。
- [ログインフォーム（Logon Form）]：ユーザのログイン情報を入力するフォームで使用されるラベルおよび色を設定します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logon Form]　（2000 ページ）を参照してください。
- [情報パネル（Informational Panel）]：ユーザに追加情報を表示する場合は、情報パネルを有効にして、テキストおよびロゴのグラフィックを追加できます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Informational Panel]　（2001 ページ）を参照してください。

- [著作権パネル（Copyright Panel）]：[ログイン（Logon）]ページに著作権情報を表示する場合は、著作権パネルを有効にして、著作権ステートメントを入力できます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Copyright Panel] （2002 ページ）を参照してください。
- [フルカスタマイズ（Full Customization）]：セキュリティアプライアンスの組み込みログインページを使用しない（カスタマイズもしない）場合は、代わりにフルカスタマイズを有効にして独自の Web ページを指定できます。必要なファイルの作成の詳細については、ASA デバイスの独自 SSL VPN ログイン ページの作成 （1817 ページ）を参照してください。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Full Customization] （2003 ページ）を参照してください。

ステップ 7 ポータルページの設定を行います。これは SSL VPN ポータルのホームページで、ユーザがログインしたあとに表示されます。ダイアログボックスの左側のコンテンツテーブルで、ポータルページフォルダから次の項目を選択し、設定を表示および変更します。

- [ポータルページ（Portal Page）]：ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。
- [タイトルパネル（Title Panel）]：ポータルページで、Web ページ内にタイトルを表示するかどうかを定義します。タイトルパネルをイネーブルにすると、使用するタイトル、フォント、フォントサイズとフォントの太さ、スタイル、および色を指定できます。ロゴのグラフィックを識別するファイル オブジェクトを選択することもできます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel] （1996 ページ）を参照してください。
- [ツールバー（Toolbar）]：ポータルページに、参照する URL を入力するフィールドを含むツールバーを表示するかどうかを定義します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Toolbar] （2004 ページ）を参照してください。
- [アプリケーション（Applications）]：ページ上に表示されるアプリケーションボタンを定義します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Applications] （2005 ページ）を参照してください。
- [カスタムペイン（Custom Panes）]：ポータルページの本文を整理する方法を定義します。デフォルトは、内部ペインのない 1 カラム型のページです。複数カラム レイアウトの作成、テキストまたは URL への参照を表示する内部ペインの作成、およびペインを配置するカラムと行の指定ができます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Custom Panes] （2006 ページ）を参照してください。
- [ホームページ（Home Page）]：ホームページに URL リストを表示するかどうか、その表示方法、およびポータルページの本文に独自の Web ページを使用するかどうかを定義します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Home Page] （2009 ページ）を参照してください。

ステップ 8 [ログアウトページ（Logout Page）] を選択して、ユーザが SSL VPN からログアウトするときに表示されるページの設定を行います。タイトル、メッセージ テキスト、フォント、および色を設定できます。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logout Page] （2010 ページ）を参照してください。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 10 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。ポリシーオブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 11 [OK] をクリックしてオブジェクトを保存します。

ASA デバイスの SSL VPN Web ページのローカライズ

ローカリゼーションとは、ターゲット ユーザに適した言語のテキストを指定するプロセスです。ASA デバイスでホストされる、ブラウザベースのクライアントレス SSL VPN Web ページの外観を定義するための SSL VPN カスタマイゼーション オブジェクトを作成するときに、目的の言語を使用するページを設定できます。

ローカライズされた Web ページを正しく表示するには、ユーザは UTF-8 エンコードを使用するようにブラウザを設定する必要があります（たとえば、Internet Explorer では [表示（View）] > [エンコーディング（Encoding）] > [ユニコード（UTF-8）（Unicode (UTF-8)）] を選択します）。また、[Regional and Language Options] コントロール パネルを使用して、言語に必要なフォントまたは言語サポート ファイルをインストールする必要もあります。[Languages] タブで、[Details] をクリックして必要な言語をインストールし、東アジア言語、文字体系の複雑な言語、および右から左に記述する言語の適切な補助言語設定を選択します。[Advanced] タブで、適切なコードページ変換テーブルを選択します。ユーザがブラウザを正しく設定しなかった場合は、文字ではなく四角形が表示されることがあります。

ASA デバイスでホストされる SSL VPN Web ページは、2 つの方法でのローカライズできます。これらの方法は互いに排他的ではなく、両方を使用できます。その方法は次のとおりです。

- **必要な言語を使用して SSL VPN カスタマイゼーション オブジェクトを設定**：SSL VPN カスタマイゼーション オブジェクトを作成すると、UTF-8 エンコードで英語以外、ASCII 文字以外の言語のラベルおよびメッセージのテキストを入力できます。ASCII 文字以外の言語を UTF-8 エンコードで入力するには、適切なロケール設定で Windows を設定し、必要なフォントをインストールしておく必要があります。システムを設定して、文字体系の複雑な言語または東アジア言語に必要なファイルをインストールするには、[Regional and Language Options] コントロール パネルを使用します。テキストを直接入力する場合は、適切なキーボードもインストールする必要があります。キーボードをインストールしない場合は、その言語の文字をサポートするテキストエディタを使用して、使用するテキストが含まれるドキュメントからそのテキストをコピーアンドペーストできます。

SSL VPN ブックマーク オブジェクトに、ASCII 文字以外の言語を入力することもできます。

- **使用可能にする言語をサポートする ASA デバイスで変換テーブルを設定**：ユーザに表示されるポータルおよび画面の言語変換をセキュリティアプライアンスが提供できるようにするには、必要な言語を変換テーブルに定義して、セキュリティアプライアンスにそのテーブルをインポートする必要があります。セキュリティアプライアンスのソフトウェア イメージ パッケージには、変換テーブルのテンプレートが含まれています。SSL VPN カスタマイゼーション オブジェクトに表示されるすべての言語では、対応する変換テーブルがデバイスに設定されている必要があります。逆に、SSL VPN カスタマイゼーション オブジェクトに表示されていない言語の変換テーブルは無視されます。

この方法を使用する場合は、ASA CLI または ASDM を使用して、変換テーブルを設定およびアップロードする必要があります。Security Manager では変換テーブルを管理できません。ただし、SSL VPN カスタマイゼーション オブジェクトの設定を使用すると、ブラウザ言語を自動的に設定し、ユーザによる適切な言語の選択をイネーブルにできます。したがって、10 言語の変換テーブルをインストールした場合は、そのすべての言語のユーザが、SSL VPN カスタマイゼーション オブジェクトに定義されたページを使用できます。これらの設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Language] （1997 ページ）を参照してください。

次のどちらの機能にも変換テーブルが必要ですが、これらは独立した相補的な機能です。

- **ブラウザ言語の自動選択**：ブラウザ言語の自動選択は、ユーザのブラウザ設定に基づき、適切な言語の選択を試行します。この方法ではユーザ入力が要求されません。SSL VPN カスタマイゼーション オブジェクトでは、ブラウザとのネゴシエーションに使用される言語のリストを作成します。接続時には、セキュリティ アプライアンスがブラウザから言語のリスト（およびそのプライオリティ）を受信し、一致する言語が検出されるまで言語のリストを上から下までもれなく調べます。一致する言語がなかった場合は、リストに定義された言語がデフォルト言語として使用されます。デフォルト言語が指定されていない場合は英語が使用されます。

セキュリティ アプライアンス上の言語は、変換テーブルのラベルとなります。この言語はブラウザの言語を反映する必要があり、（アルファベット文字で始まる）最大 8 文字の英数字をハイフンで区切ったグループで構成されます。たとえば、fr-FR-paris-univ8 などとなります。ただし、Security Manager のリストに言語を追加するときに使用できるのは、先頭の 2 文字だけです。

一致を検索するとき、セキュリティ アプライアンスは最も長い言語名から開始し、一致しない場合は名前の右端のグループを廃棄します。たとえば、ブラウザの優先言語が fr-FR-paris-univ8 で、セキュリティ アプライアンスが fr-FR-paris-univ8、fr-FR-paris、fr-FR、および fr をサポートする場合は、fr-FR-paris-univ8 が一致するので、この変換テーブルの変換ストリングが使用されます。セキュリティ アプライアンス上の言語が fr だけの場合、セキュリティ アプライアンスはこの言語も一致する言語と見なし、その変換テーブルを使用します。

変換テーブルの設定の詳細については、ASA デバイスおよびオペレーティング システムのユーザ マニュアル、または ASDM オンライン ヘルプを参照してください。

- **言語セレクタ**：言語セレクタを有効にすると、サポートする言語のリストから必要な言語をアクティブに選択する機能をユーザに提供します。この方法は、正しく設定されているブラウザ言語設定に依存しません。言語セレクタはログインページに表示されます。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）

ASA デバイスの独自 SSL VPN ログイン ページの作成

ブラウザベースのクライアントレス SSL VPN には、セキュリティ アプライアンスから提供されるページを使用するのではなく、独自のカスタム SSL VPN ログイン ページを作成できます。これはフル カスタマイゼーションと呼ばれ、SSL VPN カスタマイゼーション ポリシー オブジェクトでの設定を置き換えます。

独自のログイン ページを表示するには、ページを作成し、作成したページを Security Manager サーバにコピーして、[SSL VPN Customization object] ダイアログボックスの [Full Customization] ページでこのページを指定する必要があります。SSL VPN カスタマイゼーション オブジェクトの作成の詳細については、 SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）を参照してください。

フル カスタマイゼーションをイネーブルにすると、ポリシー オブジェクトに設定された、ログイン ページの他のすべての設定が無視されます。ASA デバイスに設定を展開すると、Security Manager によってカスタム ページがデバイスにコピーされます。

作成するログイン ページには、ページを正しく表示するために必要なすべての HTML コード、およびログイン フォームと [Language Selector] ドロップダウン リストの機能を提供するシスコ独自の HTML コードが含まれている必要があります。HTML ファイルを作成する場合は、次の点を考慮してください。

- ファイル拡張子は **.inc** とする。
- カスタム ログイン ページのすべてのイメージを、セキュリティ アプライアンスに配置する必要がある。ファイルパスをキーワード **/+CSCOU+/** で置き換える。これは、ASA デバイスの内部ディレクトリです。イメージをデバイスにアップロードすると、そのイメージはこのディレクトリに保存されます。
- **csco_ShowLoginForm('lform')** JavaScript 関数を使用して、ログインフォームをページに追加する。このフォームによって、ユーザ名、パスワード、およびグループ情報の入力が要求されます。この関数をページのいずれかの場所に記述しておく必要があります。
- JavaScript 関数 **csco_ShowLanguageSelector('selector')** を使用して、[言語セレクタ（Language Selector）] ドロップダウンリストをページに追加する。複数言語の使用をサポートしない場合、この関数を使用する必要はありません。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）
- [SSL VPN Customization] ダイアログボックス - [Full Customization] （2003 ページ）

ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定

ブラウザベースのクライアントレス SSL VPN を設定する場合は、SSL VPN ポータル ページに追加するブックマークまたは URL のリストを定義できます。ブックマーク リストを定義するには、SSL VPN ブックマーク ポリシー オブジェクトを使用します。

IOS デバイスまたは ASA デバイスでホストされる SSL VPN に対する SSL VPN ブックマーク オブジェクトを作成できます。ただし、作成できるブックマーク設定はデバイス タイプによって異なり、ASA デバイスの方が IOS デバイスより多くの設定オプションを設定できます。設定できるオプションが多いほか、ASA デバイスには英語以外、ASCII 文字以外の言語のブックマークも作成できます。ASA デバイスのブックマークおよびポータルのローカライズの詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。

この手順に従って SSL VPN ブックマークオブジェクトを作成したあと、このオブジェクトを使用して、次のポリシーの [ポータルWebページ（Portal Web Pages）] フィールドまたは [ブックマーク（Bookmarks）] フィールドでブックマークオブジェクトを指定できます。

- ASA デバイス：ASA グループ ポリシー オブジェクトの [SSL VPN] > [クライアントレス（Clientless）] ページで（ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）を参照）、次のポリシーのいずれかを選択します。
  - **[Remote Access VPN] > [Group Policies]**
  - [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]
- ASA デバイス：[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] ポリシーの [メイン（Main）] > [ブックマーク（Bookmarks）] タブで、SSL VPN ブックマークオブジェクトを指定できます（[Main] タブ （1844 ページ）を参照）。
- IOS デバイス：SSL VPN 用に設定されるユーザー グループ ポリシー オブジェクトの [クライアントレス（Clientless）] ページ（[User Group] ダイアログボックス - クライアントレス設定 （2036 ページ）を参照）。このページの [全般（General）] タブの [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] ポリシーで選択します。

関連項目

- グループ ポリシーの作成（ASA、PIX 7.0+） （1743 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）
- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）
- SSL VPN ポリシーの設定（IOS） （1908 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

- Policy Object Manager （290 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（ Policy Object Manager （290 ページ）を参照）。

ヒント SSL VPN ブックマーク オブジェクトは、このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

ステップ 2 オブジェクトタイプセレクタから [SSL VPNブックマーク（SSL VPN Bookmarks）] を選択します。[SSL VPN Bookmarks] ページが開き、既存の SSL VPN ブックマーク オブジェクトのリストが表示されます。

ステップ 3 作業領域内で右クリックし、[新規オブジェクト（New Object）] を選択します。

[Add SSL VPN Bookmark] ダイアログボックスが表示されます（ [Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （1982 ページ）を参照）。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 IOS デバイスでホストされる SSL VPN のオブジェクトを作成する場合は、ブックマークリストの上に表示される見出しの名前を [ブックマークの見出し（IOS）（Bookmarks Heading (IOS))] フィールドで入力できます。

ステップ 6 Bookmarks テーブルに、オブジェクトに定義されたすべての URL が表示されます。ブックマークを追加するには、テーブルの下にある [行の追加（Add Row）] ボタンをクリックします。既存のブックマークを編集するには、ブックマークを選択して [行の編集（Edit Row）] ボタンをクリックします。

[Add/Edit SSL VPN Bookmark Entry] ダイアログボックスが開きます。このダイアログボックスのフィールドの詳細については、[ブックマークエントリの追加（Add Bookmark Entry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス （1984 ページ）を参照してください。

- [ブックマークオプション（Bookmark Option）] フィールドで、ブックマークを定義するか（[ブックマークの入力（Enter Bookmark）]）、別の SSL VPN ブックマークオブジェクトからブックマークを追加するか（[既存のブックマークを含める(Include Existing Bookmarks）]）を選択します。既存のオブジェクトを追加する場合は、オブジェクトの名前を入力するか、または [選択（Select）] をクリックして既存のオブジェクトのリストからオブジェクトを選択します。
- IOS デバイスで使用するオブジェクトを作成する場合は、ユーザに表示されるブックマークのタイトルと、URL を入力します。URL には正しいプロトコルを選択するように注意してください。[OK] をクリックして、ブックマークをブックマークテーブルに追加します。
- ASA デバイスで使用するオブジェクトを作成する場合は、さらに多くのオプションがあります。タイトルと URL のほか、ブックマークのサブタイトルとイメージ アイコンおよびその他のオプションを定義できます。

ヒント プロトコル RDP、SSH、Telnet、VNC、または ICA を選択する場合は、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシーで、プロトコルのプラグインを設定する必要があります（ SSL VPN ブラウザ プラグインの設定（ASA） （1787 ページ）を参照）。

Get 方式ではなく Post 方式を使用するブックマークを設定することもできます。Post を使用する場合は、[Postパラメータ（Post Parameters）] テーブルの下の [行の追加（Add Row）] をクリックして Post パラメータを設定する必要があります。Post パラメータの詳細については、次の項を参照してください。

- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （1820 ページ）
- [Add Post Parameter]/[Edit Post Parameter] ダイアログボックス （1988 ページ）

[OK] をクリックして、ブックマークをブックマークテーブルに追加します。

ステップ 7 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 8 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。 ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 9 [OK] をクリックしてオブジェクトを保存します。

SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用

ASA デバイスでホストされる SSL VPN のブックマークを設定する場合には、URL で使用される方式として Get または Post を選択するというオプションがあります。標準の方式は Get 方式であり、この場合、ユーザが URL をクリックすると Web ページに移動します。Post 方式は、データの格納や更新、製品の注文、または電子メールの送信など、データの処理にそのデータの変更が含まれる場合に有効です。

Post URL 方式を選択する場合は、ブックマーク エントリに Post パラメータを設定する必要があります。これらは、ユーザ ID とパスワード、または他の入力パラメータを含む個人別のリソースであることが多く、クライアントレス SSL VPN マクロ置換を定義する必要がある場合があります。

クライアントレス SSL VPN マクロ置換を使用すると、ユーザ ID とパスワード、または他の入力パラメータを含む個人別のリソースにユーザがアクセスできるように設定できます。このようなリソースの例には、ブックマーク エントリ、URL リスト、およびファイル共有などがあります。

（注） セキュリティ上の理由から、パスワード置換はファイルアクセス URL（cifs://）に対してはディセーブルにされています。同様に、セキュリティ上の理由から、Web リンク（特に非 SSL インスタンス）にパスワード置換を導入する場合は注意が必要です。

次のマクロ置換を使用できます。

- ログイン情報置換：セキュリティアプライアンスは、SSL VPN ログインページからこれらの置換のための値を取得します。ユーザ要求内のこれらのストリングを認識し、このストリングをユーザ固有の値で置き換えてから、リモート サーバに要求を渡します。

使用可能なマクロ置換は、次のとおりです。

- CSCO_WEBVPN_USERNAME

SSL VPN へのログインに使用するユーザ名

- CSCO_WEBVPN_PASSWORD

SSL VPN へのログインに使用するパスワード

- CSCO_WEBVPN_INTERNAL_PASSWORD

SSL VPN へのログイン時に入力する内部リソース パスワード

- CSCO_WEBVPN_CONNECTION_PROFILE

SSL VPN へのログイン時に選択されるユーザ グループに関連付けられた接続プロファイル

たとえば、URL リストにリンク http://someserver/homepage/CSCO_WEBVPN_USERNAME.html が含まれている場合、このリンクはセキュリティ アプライアンスによって次の一意なリンクに変換されます。

- USER1 の場合、リンクは http://someserver/homepage/USER1.html になります。
- USER2 の場合、リンクは http://someserver/homepage/USER2.html になります。

次の例では、cifs://server/users/CSCO_WEBVPN_USERNAME により、セキュリティ アプライアンスでファイル ドライブが特定のユーザにマップされます。

- USER1 の場合、リンクは cifs://server/users/USER1 になります。
- USER2 の場合、リンクは cifs://server/users/USER2 になります。

- RADIUS/LDAP ベンダー固有属性（VSA）：これらの置換を使用すると、RADIUS サーバーまたはLDAP サーバーのいずれかに設定された置換を設定できます。使用可能なマクロ置換は、次のとおりです。
  - CSCO_WEBVPN_MACRO1
  - CSCO_WEBVPN_MACRO2

ブックマークの設定については、ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）を参照してください。

ASA デバイスの SSL VPN スマート トンネルの設定

スマートトンネルは、ユーザーのワークステーションで動作するアプリケーションとプライベートサイト間の接続です。この接続は、セキュリティ アプライアンスをパスおよびプロキシサーバとして使用するクライアントレス（ブラウザベース）SSL VPN セッションを使用します。スマート トンネルではユーザのアプリケーションがローカル ポートに接続する必要がないため、ユーザに管理権限を指定することなく、フル トンネル サポートが必要な場合と同様にアプリケーションがネットワークにアクセスできます。ただし、アプリケーションへのアク

セスを許可するようにネットワークを設定していない場合は、サポートするアプリケーションのスマート トンネルを作成できます。

アプリケーションへのスマート トンネル アクセスは、次の条件下で設定できます。

- アプリケーションが Winsock 2 の TCP ベースのアプリケーションであり、アプリケーションにブラウザ プラグインが存在する。シスコでは、SSH（SSH セッションおよび Telnet セッション）、RDP、および VNC を含め、クライアントレス SSL VPN で使用するため、一部のアプリケーション向けにプラグインを配布しています。他のアプリケーションについては、プラグインを提供または入手する必要があります。プラグインは、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシーの [プラグイン（Plug-Ins）] タブで設定します。
- ユーザーのワークステーションは、サポートされているプラットフォームです。サポートされているプラットフォームについては、使用している ASA バージョンに対応する Cisco ASA 5500 シリーズ適応型セキュリティアプライアンスのマニュアル（http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html [英語]）を参照してください。

スマート トンネル（またはポート転送）を使用する Microsoft Windows Vista のユーザは、ASA デバイスの URL を信頼済みサイト ゾーンに追加する必要があります。信頼済みサイトゾーンは、Internet Explorer（[ツール（Tools）] > [インターネットオプション（Internet Options）] の [セキュリティ（Security）] タブ）で設定します。

- ユーザーのブラウザで Java、Microsoft ActiveX、またはその両方をイネーブルにする必要があります。
- ユーザーのワークステーションがセキュリティアプライアンスに接続するためにプロキシサーバーを必要とする場合は、接続の終端側の URL が、プロキシサービスから除外される URL のリストに含まれている必要があります。この設定では、スマート トンネルは基本認証だけをサポートします。

ヒント ステートフル フェールオーバーが発生したとき、スマート トンネル接続は保持されません。ユーザーはフェールオーバー後に再接続する必要があります。

アプリケーションにスマート トンネル アクセスを設定する場合は、SSL VPN スマート トンネル リスト ポリシー オブジェクトを作成し、このオブジェクトを ASA グループ ポリシー オブジェクトに追加します。次に、[リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] ポリシーで、ASA グループ ポリシー オブジェクトをデバイスに割り当てます。

関連項目

- グループ ポリシーについて（ASA） （1741 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- Policy Object Manager （290 ページ）

ステップ 1 SSL VPN スマート トンネル リスト ポリシー オブジェクトを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開き（ Policy Object Manager （290 ページ）を参照）、コンテンツテーブルから [SSL VPNスマートトンネルリスト（SSL VPN Smart Tunnel Lists）] を選択します。

ヒント ASA グループ ポリシー オブジェクトを作成または編集するときに、SSL VPN スマート トンネル リスト オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

b) [オブジェクトの追加（Add Object）] ボタンをクリックして、 [Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （2013 ページ）を開きます。

c) オブジェクトの名前を、最大 64 文字で入力します。

d) アプリケーションのテーブルに、スマートトンネルアクセスを付与するアプリケーションを追加します（[行の追加（Add Row）] ボタンをクリックして [Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス （2015 ページ）を開きます）。以下の点に注意してください。

- わかりやすいアプリケーション名を入力し、複数のバージョンをサポートする場合はバージョン番号を含めます。たとえば、Microsoft Outlook などと入力します。
- アプリケーション パスの場合、たとえば、outlook.exe などのファイル名だけを入力すると、わかりやすく、メンテナンスも簡単です。このようにすると、ユーザは任意のフォルダにアプリケーションをインストールできます。特定のインストール構造を強制する場合は、フル パスを入力します。
- ハッシュ値はオプションですが、スプーフィングの防止に使用できます。ハッシュ値が設定されていない場合、ユーザはアプリケーションの名前をサポートされているファイル名に変更できます。この場合、セキュリティ アプライアンスはファイル名とパスだけをチェックします（指定された場合）。ただし、ハッシュ値を入力すると、ユーザがパッチを適用するとき、またはアプリケーションをアップグレードするときにそのハッシュ値を保守する必要があります。ハッシュ値の決定の詳細については、 [Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス （2015 ページ）を参照してください。

[OK] をクリックしてエントリを保存します。

e) 他の SSL VPN スマート リスト オブジェクトをこのオブジェクトに組み込むこともできます。このようにすると、核となるスマートリストオブジェクトセットを作成し、他のオブジェクトで繰り返し使用できます。

f) [OK] をクリックしてオブジェクトを保存します。

ステップ 2 （任意）SSL VPN スマート トンネル自動サインオン リスト ポリシー オブジェクトを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開き（ Policy Object Manager （290 ページ）を参照）、コンテンツテーブルから [SSL VPNスマートトンネル自動サインオンリスト（SSL VPN Smart Tunnel Auto Signon Lists）] を選択します。

ヒント ASA グループ ポリシー オブジェクトを作成または編集するときに、SSL VPN スマート トンネル自動サインオン リスト オブジェクトを作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

b) [オブジェクトの追加（Add Object）] ボタンをクリックして、[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス （2020 ページ）を開きます。
c) オブジェクトの名前を、最大 64 文字で入力します。
d) スマートトンネル自動サインオンエントリのテーブルに、スマートトンネル設定中のログイン情報の発行を自動化するサーバーを追加します（[行の追加（Add Row）] ボタンをクリックして [Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス （2022 ページ）を開きます）。
e) 他の SSL VPN スマート トンネル自動サインオン リスト オブジェクトをこのオブジェクトに組み込むこともできます。このようにすると、核となるスマートトンネル自動サインオン リストオブジェクトセットを作成し、他のオブジェクトで繰り返し使用できます。
f) [OK] をクリックしてオブジェクトを保存します。

ステップ 3 SSL VPN スマート トンネル リスト オブジェクトを使用するための ASA グループ ポリシー オブジェクトを設定します。

a) Policy Object Manager （290 ページ）または [リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）] ポリシーから、ASA グループ ポリシー オブジェクトを編集（または作成）します。このオブジェクトは、SSL VPN をサポートするように設定する必要があります（これらのオブジェクトは、[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）] ポリシーの個々のプロファイルから編集することもできます）。
b) コンテンツテーブルから [SSL VPN] > [クライアントレス（Clientless）] フォルダを選択して ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）を開きます。
c) [スマートトンネル（Smart Tunnel）] フィールドに SSL VPN スマート トンネル リスト オブジェクトの名前を入力します。
d) [スマートトンネルの自動開始（Auto Start Smart Tunnel）] を選択して、ユーザーが SSL VPN ポータルに接続したときに、アプリケーションのスマートトンネルが自動的に開始されるようにします。

   このオプションを選択しない場合、ユーザーはクライアントレス SSL VPN ポータルページで [アプリケーションアクセス（Application Access）] > [スマートトンネルの開始（Start Smart Tunnels）] ボタンを使用して、スマートトンネルアクセスを開始する必要があります。

e) [スマートトンネル自動サインオンサーバーリスト（Smart Tunnel Auto Signon Server List）] フィールドに SSL VPN スマートトンネル自動サインオン リスト オブジェクトの名前を入力します。
f) 汎用命名規則（ドメイン\ユーザー名）が認証に必要な場合、Windows ドメインを指定して、[ドメイン名（Domain Name）] フィールドの自動サインオン中のユーザー名に追加します。たとえば、ユーザ名 qa_team の認証を行う場合、CISCO と入力して CISCO\qa_team を指定します。自動サインオン サーバリストで関連エントリを設定する場合は、[Use Domain] オプションも選択する必要があります。

WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

クライアントレス SSL VPN では、WINS および Common Internet File System（CIFS）プロトコルを使用して、リモート システム上のファイル、プリンタ、および他のマシン リソースにアクセス、またはこれらを共有します。ASA デバイスまたは IOS デバイスは、プロキシ CIFS クライアントを使用して、このアクセスを透過的に提供します。このため、ユーザには（個々のファイルおよびユーザの権限に従って）ファイル システムに直接アクセスしているように見えます。

ユーザがコンピュータ名を使用して Windows コンピュータへのファイル共有接続を試みる場合、ユーザが指定するファイル サーバは、ネットワーク上のリソースを識別する特定の WINS 名に対応します。セキュリティ アプライアンスは WINS サーバまたは NetBIOS ネーム サーバにクエリーを行い、WINS 名を IP アドレスにマップします。SSL VPN は NetBIOS に再クエリーを行い、リモート システム上のファイルにアクセス、またはファイルを共有します。

これらの Microsoft のファイルおよびディレクトリ共有名の解決に使用される WINS サーバのリストを設定するには、WINS サーバ リスト ポリシー オブジェクトを使用します。WINS サーバーリストオブジェクトでは、Common Internet File System（CIFS）の名前解決に、（**nbns-list** コマンドおよび **nbns-server** コマンドを使用して）デバイスの NetBIOS Name Service（NBNS）サーバーを定義します。

WINS サーバ リスト ポリシー オブジェクトを作成したあと、次のポリシーおよびポリシー オブジェクト内で、このポリシー オブジェクトを設定できます。また、許可するファイル アクセス サービスを選択することもできます。

- ASA デバイス：**[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]** ポリシーで、[SSL] タブの WINS サーバーリストオブジェクトを指定します（[SSL] タブ（[Connection Profiles]） （1734 ページ）を参照）。

ASA グループ ポリシー オブジェクトの **[SSL VPN] > [クライアントレス（Clientless）]** ページでファイルアクセスオプションを選択し（ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）を参照）、次のポリシーのいずれかを選択します。

- **[リモートアクセスVPN（Remote Access VPN）] > [グループポリシー（Group Policies）]**
- [全般（General）] タブの **[リモートアクセスVPN（Remote Access VPN）] > [接続プロファイル（Connection Profiles）]**
- IOS デバイス：SSL VPN 用に設定されるユーザ グループ ポリシー オブジェクトの [クライアントレス（Clientless）] ページ（[User Group] ダイアログボックス - クライアントレス設定 （2036 ページ）を参照）。ここで、[全般（General）] タブの **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN]** ポリシー内で選択します。

関連項目

- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して、 Policy Object Manager （290 ページ）を開きます。

ヒント WINS サーバ リスト オブジェクトは、このオブジェクト タイプを使用するポリシーまたはオブジェクトを定義するときに作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

ステップ 2 オブジェクトタイプセレクタから [WINSサーバーリスト（WINS Server Lists）] を選択します。

[WINS Server List] ページが開き、現在定義されている WINS サーバ リスト オブジェクトが表示されます。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [Add WINS Server List]/[Edit WINS Server List] ダイアログボックス （2045 ページ）を開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 テーブルの下にある [行を追加（Add Row）] ボタンをクリックするか、またはテーブル内のサーバーを選択して [行を編集（Edit Row）] をクリックし、オブジェクトに定義された WINS サーバーを設定します。設定する項目は次のとおりです。

- [サーバー（Server）]：WINS サーバーの IP アドレス。ネットワーク/ホスト オブジェクトを選択するか、またはアドレスを直接入力できます。
- [プライマリブラウザとして設定（Set as Primary Browser）]：サーバーがプライマリブラウザの場合にこのオプションを選択します。プライマリブラウザは、コンピュータおよび共有リソースのリストを保持します。

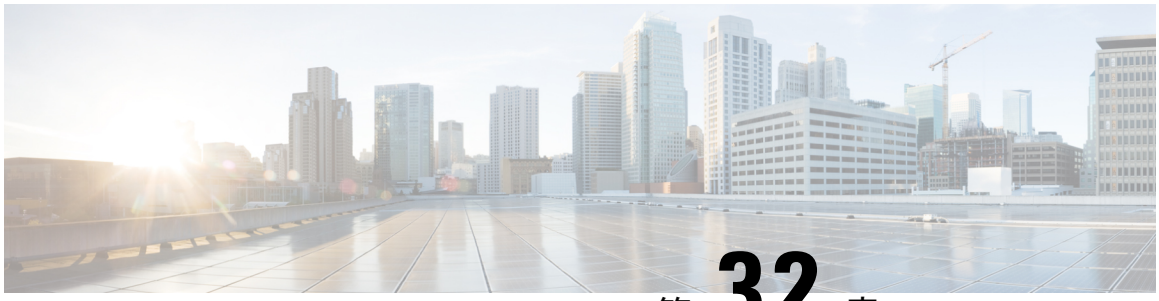
他のフィールドはオプションです。デフォルト値以外の値が必要な場合は、これらのフィールドを変更してください。詳細については、 [Add WINS Server]/[Edit WINS Server] ダイアログボックス （2047 ページ）を参照してください。

[OK] をクリックして変更を保存します。

ステップ 6 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 7 （任意）[デバイスごとに値のオーバーライドを許可（Allow Value Override per Device）] を選択して、このオブジェクトのプロパティを個々のデバイスで再定義できるようにします。 ポリシー オブジェクトの上書きの許可 （311 ページ）を参照してください。

ステップ 8 [OK] をクリックしてオブジェクトを保存します。



第 32 章

リモート アクセス VPN のダイナミック アクセス ポリシーの管理（ASA 8.0+ デバイス）

この章では、リモート アクセス ユーザを接続プロファイル（トンネル グループ）に割り当てる Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）について説明します。これらのポリシーを、ASA 8.0+ デバイスのリモート アクセス IKEv1 IPsec、ASA 8.4(x) デバイスの IKEv2 IPsec および ASA 8.0+（8.5 を除く）デバイスの SSL VPN に設定できます。

ASA および PIX 7.0+ デバイスの他のリモート アクセス ポリシーの設定については、ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理 （1705 ページ）を参照してください。

この章は次のトピックで構成されています。

- ダイナミック アクセス ポリシーについて （1827 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）
- [Dynamic Access] ページ（ASA） （1840 ページ）

ダイナミック アクセス ポリシーについて

個々の VPN 接続には、頻繁に変更されるイントラネット設定、組織内の各ユーザーが持つさまざまなロール、および設定とセキュリティ レベルが異なるリモート アクセス サイトからのログインなど、複数の変数が影響する可能性があります。VPN 環境でのユーザー認可のタスクは、スタティックな設定のネットワークでの認可タスクよりもかなり複雑です。

セキュリティ アプライアンスで Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）を使用すると、これらの多くの変数に対処する認可を設定できます。ダイナミック アクセス ポリシーは、特定のユーザー トンネルまたはユーザー セッションに関連付ける一連のアクセス コントロール属性を設定して作成します。これらの属性により、複数のグループ メンバーシップやエンドポイント セキュリティの問題に対処します。つまり、セキュリティ アプライアンスは、定義されるポリシーに基づいて、特定のセッションの特定のユーザにアクセス権を付与します。セキュリティ アプライアンスは、ユーザーが接続するときに、1 つまたは複数の DAP レコードから属性を選択または集約して、DAP を生成します。DAP レコードは、リモー

トデバイスのエンドポイントセキュリティ情報および認証されたユーザーの AAA 認可情報に基づいて選択されます。選択された DAP レコードは、ユーザー トンネルまたはセッションに適用されます。DAP システムには、注意を必要とする次のコンポーネントがあります。

- DAP 選択設定ファイル：セッション確立時に DAP レコードを選択および適用するためにセキュリティ アプライアンスが使用する、基準が記述されたテキスト ファイル。セキュリティ アプライアンス上に格納されています。Security Manager を使用すると、このファイルを変更したり、XML データ形式でセキュリティ アプライアンスにアップロードしたりできます。DAP選択設定ファイルには、ユーザーが設定するすべての属性が記載されています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。
- DfltAccess ポリシー：常に DAP サマリー テーブルの最後のエントリで、プライオリティは必ず0。デフォルトアクセスポリシーのアクセスポリシー属性を設定できますが、AAA 属性またはエンドポイント属性は含まれておらず、これらの属性は設定できません。DfltAccessPolicy は削除できません。また、サマリー テーブルの最後のエントリになっている必要があります。

ヒント　ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

Cisco Secure Desktop と DAP の統合

Cisco Secure Desktop（CSD）機能は、セキュリティ アプライアンスによってダイナミック アクセス ポリシー（DAP）に統合されます。設定に応じて、セキュリティアプライアンスでは、DAP を割り当てる条件として、1 つ以上のエンドポイント属性値を、オプションの AAA 属性値と組み合わせて使用します。DAP のエンドポイント属性でサポートされる Cisco Secure Desktop 機能には、OS 検出、プリログイン ポリシー、基本ホスト スキャン結果、およびエンドポイント評価があります。

管理者は、セッションに DAP を割り当てるために必要な条件を構成する属性を、単独で、または組み合わせて指定できます。DAP により、エンドポイント AAA 属性値に適したレベルでネットワーク アクセスが提供されます。設定したエンドポイント基準がすべて満たされたときに、セキュリティ アプライアンスによって DAP が適用されます。

関連項目

- ダイナミック アクセス ポリシーの設定　（1829 ページ）
- DAP 属性の設定　（1836 ページ）

ダイナミック アクセス ポリシーの設定

ここでは、ダイナミック アクセス ポリシーを作成または編集する方法について説明します。

関連項目

- ダイナミック アクセス ポリシーについて （1827 ページ）
- DAP 属性について （1831 ページ）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dynamic Access] ページが開きます。このページの要素の詳細については、[Dynamic Access] ページ（ASA）（1840 ページ）を参照してください。

ステップ 2 [作成（Create）] をクリックするか、またはテーブル内のポリシーを選択して [編集（Edit）] をクリックします。

[Add/Edit Dynamic Access Policy] ダイアログボックスが開き、デフォルトで [Main] タブが表示されます。このダイアログボックスの要素の詳細については、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を参照してください。

ステップ 3 DAP レコードの名前を入力します（最大 128 文字）。

ステップ 4 DAP レコードのプライオリティを指定します。セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。

ステップ 5 DAP レコードの説明を入力します。

ステップ 6 [メイン（Main）] タブで、DAP 属性、およびセキュリティアプライアンスの DAP システムでサポートされるリモートアクセス方式のタイプを設定します。このタブの要素の詳細については、[Main] タブ （1844 ページ）を参照してください。

a) テーブルの下の [作成（Create）] をクリックするか、またはテーブル内の DAP エントリを選択して [編集（Edit）] をクリックします。[Add/Edit DAP Entry] ダイアログボックスが開きます。このダイアログボックスの要素の詳細については、[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （1853 ページ）を参照してください。

DAP 属性を定義する手順の詳細については、DAP 属性の設定 （1836 ページ）を参照してください。

b) DAP システムで許可されるリモート アクセスのタイプを選択します。

c) [ネットワーク ACL（Network ACL）] タブを選択し、この DAP レコードに適用するネットワーク ACL を選択および設定します。Security Manager バージョン 4.10 以降では、拡張 ACL エントリに加えて統合 ACL エントリを選択できます。

このタブは、[Web Portal] 以外のアクセス方式を選択した場合にかぎり、使用可能です。

d) [WebType ACL] タブを選択し、この DAP レコードに適用する Web タイプ ACL を選択および設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

e) [Functions] タブを選択し、ファイル サーバー エントリとブラウジング、HTTP プロキシ、および DAP レコードの URL エントリを設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

f) [ポートフォワーディング（Port Forwarding）] タブを選択し、ユーザー セッションのポート転送リストを選択および設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

Cisco Security Manager 4.24 以降、[ポートフォワーディング（Port Forwarding）] ポリシーオブジェクトは ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

（注） ASA デバイスを 9.17(1) 以降のバージョンにアップグレードする場合は、展開の失敗を避けるために、ポート設定 CLI を削除する必要があります。

g) [ブックマーク（Bookmark）] タブを選択し、ユーザー セッションの URL リストを選択および設定します。

このタブは、AnyConnect Client 以外のアクセス方式を選択した場合にかぎり、使用可能です。

h) [アクション（Action）] タブを選択し、許可されるリモート アクセスのタイプを設定します。

このタブは、どのタイプのアクセス方式でも使用できます。

i) [AnyConnect] タブを選択し、AnyConnect サービス プロファイルの Always-On VPN の設定を未変更のままにするか、無効にするか、AnyConnect プロファイル設定を使用する必要があるかを選択します。Always-On VPN を使用すると、システムにログオンした後、AnyConnnect で VPN セッションを自動的に確立できます。

j) [カスタム属性（Custom Attributes）] タブを選択し、AnyConnect カスタム属性を追加します。

このタブは、アクセス方式として [変更なし（Unchanged）]、[AnyConnect クライアント（AnyConnect Client）]、[両方、デフォルトは Web ポータル（Both Default Web Portal）]、または [両方、デフォルトは Anyconnect クライアント（Both Default Anyconnect Client）] を選択した場合にのみ使用できます。AnyConnect カスタム属性を追加する方法については、[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1801 ページ）を参照してください。

ステップ 7 [論理的な操作（Logical Operations）] タブを選択し、エンドポイント属性のタイプごとに複数のインスタンスを作成します。このタブの要素の詳細については、[論理的な操作（Logical Operators）] タブ （1884 ページ）を参照してください。

ステップ 8 [拡張表現（Advanced Expressions）] タブを選択し、自由形式の LUA を使用して DAP の追加属性を設定します。このタブの要素の詳細については、[Advanced Expressions] タブ （1887 ページ）を参照してください。

ステップ 9 [OK] をクリックします。

DAP 属性について

DAP レコードには、ユーザが設定するすべての属性が含まれています。これには、AAA 属性、エンドポイント属性、およびネットワーク ACL と Web タイプ ACL のフィルタ、ポート転送、URL のリストとして設定されたアクセス ポリシーなどがあります。

DAP と AAA 属性

DAP は AAA サービスを補完します。用意されている許可属性のセットはかぎられていますが、それらの属性によって AAA で提供される許可属性を無効にできます。セキュリティ アプライアンスは、ユーザの AAA 認可情報およびセッションのポスチャ評価情報に基づいて、DAP レコードを選択します。セキュリティ アプライアンスは、この情報に基づいて複数の DAP レコードを選択でき、それらのレコードを集約して DAP 認可属性を作成します。

AAA 属性は、Cisco AAA 属性階層から、またはセキュリティ アプライアンスが RADIUS サーバまたは LDAP サーバから受信するフル セットの応答属性から指定できます。

AAA 属性の定義

次の表に、DAP で使用できる AAA 選択属性名の定義を示します。属性名欄は、LUA 論理式での各属性名の入力方法を示しており、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスの [Advanced] タブでこのように入力する場合があります。

表 *399 : AAA* 属性の定義

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
シスコ	aaa.cisco.memberof	AAA	string	128	memberof の値
	aaa.cisco.username	AAA	string	64	ユーザ名の値
	aaa.cisco.class	AAA	string	64	クラス属性値
	aaa.cisco.ipaddress	AAA	number	–	framed-ip アドレスの値
	aaa.cisco.tunnelgroup	AAA	string	64	トンネル グループ名
LDAP	aaa.ldap.<label>	LDAP	string	128	LDAP 属性値ペア
RADIUS	aaa.radius.<number>	RADIUS	string	128	RADIUS 属性値ペア

DAP とエンドポイント セキュリティ

セキュリティ アプライアンスは、設定されたポスチャ評価方式を使用して、エンドポイント セキュリティ属性を取得します。これには、Cisco Secure Desktop および NAC が含まれます。プリログイン ポリシーの一致、基本ホスト スキャン エントリ、ホスト スキャン拡張機能、またはこれらの属性と他のポリシー属性の任意の組み合わせを使用して、アクセス権および制約を適用できます。最低でも、プリログイン ポリシーごと、および基本ホスト スキャン エントリごとに割り当てられるように DAP を設定します。

ホスト スキャン拡張機能であるエンドポイント評価では、アンチウイルスとアンチスパイウェアのアプリケーション、関連する定義の更新、およびファイアウォールの大規模なコレクションについて、リモート コンピュータを検査します。この機能を使用すると、セキュリティ アプライアンスによって特定の DAP がセッションに割り当てられる前に、要件を満たすようにエンドポイント基準を組み合わせることができます。

DAP とアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォール プログラム

セキュリティ アプライアンスは、ユーザー属性が、設定済みの AAA 属性およびエンドポイント属性に一致する場合に DAP ポリシーを使用します。Cisco Secure Desktop のプリログイン評価モジュールおよびホスト スキャン モジュールは、設定済みエンドポイント属性の情報をセキュリティ アプライアンスに返し、DAP サブシステムでは、その情報に基づいてそれらの属性値に一致する DAP レコードを選択します。すべてではありませんが、ほとんどのアンチウイルス、アンチスパイウェア、およびパーソナル ファイアウォールのプログラムは、アクティブ スキャンをサポートしています。つまり、それらのプログラムはメモリ常駐型であり、常に動作しています。ホスト スキャンは、エンドポイントにプログラムがインストールされているかどうか、およびそのプログラムがメモリ常駐型かどうかを、次のようにしてチェックします。

- インストールされているプログラムがアクティブ スキャンをサポートしない場合、ホスト スキャンはそのソフトウェアの存在をレポートします。DAP システムは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがイネーブルになっている場合、ホスト スキャンはそのソフトウェアの存在をレポートします。この場合も、セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択します。
- インストールされているプログラムがアクティブ スキャンをサポートしており、そのプログラムでアクティブ スキャンがディセーブルになっている場合、ホスト スキャンはそのソフトウェアの存在を無視します。セキュリティ アプライアンスは、そのプログラムを指定する DAP レコードを選択しません。さらに、そのプログラムがインストールされているとしても、DAP についての情報が多く含まれる **debug trace** コマンドの出力にはプログラムの存在が示されません。

エンドポイント属性の定義

次の表に、DAP で使用できるエンドポイント選択属性名の定義を示します。属性名欄は、LUA 論理式での各属性名の入力方法を示しており、[Add Dynamic Access Policy]/[Edit Dynamic Access

Policy] ダイアログボックスの [Advanced] タブでこのように入力する場合があります。*label* 変数は、アプリケーション、ファイル名、プロセス、またはレジストリ エントリを示します。

表 *400*：エンドポイント属性の定義

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
アンチスパイウェア（Cisco Secure Desktop が必要）	endpoint.as.label.exists	ホストスキャン	true	–	アンチスパイウェアプログラムが存在する
	endpoint.as.label.version		string	32	アンチスパイウェアの説明
	endpoint.as.label.description		string	128	クラス属性値
	endpoint.as.label.lastupdate		整数	–	アンチスパイウェア定義を更新してからの経過時間（秒）
アンチウイルス（Cisco Secure Desktop が必要）	endpoint.av.label.exists	ホストスキャン	true	–	アンチウイルスプログラムが存在する
	endpoint.av.label.version		string	32	アンチウイルスの説明
	endpoint.av.label.description		string	128	クラス属性値
	endpoint.av.label.lastupdate		整数	–	アンチウイルス定義を更新してからの経過時間（秒）
アプリケーション	endpoint.application.clienttype	アプリケーション	string	–	クライアント タイプ： CLIENTLESS ANYCONNECT IPSEC L2TP
ファイル（File）	endpoint.file.label.exists	Secure Desktop	true	–	ファイルが存在する
	endpoint.file.label.lastmodified		整数	–	ファイルが最後に変更されてからの経過時間（秒）
	endpoint.file.label.crc.32		整数	–	ファイルの CRC32 ハッシュ

属性タイプ	属性名	送信元	値	ストリングの最大長	説明
NAC	endpoint.nac.status	NAC	string	-	ユーザー定義ステータス ストリング
オペレーティング システム	endpoint.os.version	Secure Desktop	string	32	Windows のサービス パック
	endpoint.os.servicepack		整数	–	オペレーティング システム
パーソナル ファイア ウォール（Secure Desktop が必要）	endpoint.fw.label.exists	ホスト スキャン	true	–	パーソナル ファイア ウォールが存在する
	endpoint.fw.label.version		string	32	Version
	endpoint.fw.label.description		string	128	パーソナル ファイア ウォールの説明
ポリシー（Policy）	endpoint.policy.location	Secure Desktop	string	64	Cisco Secure Desktop からのロケーション値
プロセス	endpoint.process.label.exists	Secure Desktop	true	–	プロセスが存在する
	endpoint.process.label.path		string	255	プロセスのフル パス
Registry	endpoint.registry.label.type	セキュアなデスクトップ	dword ストリング	–	dword
	endpoint.registry.label.value		string	255	レジストリ エントリの値
VLAN	endpoint.vlan.type	CNA	sting	–	VLAN タイプ： ACCESS AUTH ERROR GUEST QUARANTINE ERROR STATIC TIMEOUT

AAA 属性またはエンドポイント属性の高度な式について

テキスト ボックスに、AAA またはエンドポイント、あるいはその両方の選択論理演算を表す自由形式の LUA テキストを入力します。ASDM は、ここで入力されたテキストを検証せず、このテキストを単に DAP ポリシー ファイルにコピーします。セキュリティ アプライアンスがそれを処理し、解析できない式があるとその式は廃棄されます。

このオプションは、上の説明にある AAA およびエンドポイントの属性領域で指定可能な基準以外の選択基準を追加する場合に有効です。たとえば、指定された基準のいずれかまたはすべてを満たす、あるいはいずれも満たさない AAA 属性を使用するようにセキュリティ アプライ

アンスを設定できます。エンドポイント属性は累積的で、すべてを満たす必要があります。セキュリティ アプライアンスが任意のエンドポイント属性を使用できるようにするには、LUA で適切な論理式を作成し、ここでその式を入力する必要があります。

DAP 論理式の例

LUA で論理式を作成する場合は、次の例を参考にしてください。

- この AAA LUA 式は、「b」で始まるユーザ名に一致するかどうかをテストします。この式では、ストリング ライブラリおよび正規表現を使用しています。

```
not(string.find(aaa.cisco.username, "^b") == nil)
```

- このエンドポイント式は、CLIENTLESS または CVC クライアント タイプに一致するかどうかをテストします。

```
endpoint.application.clienttype=="CLIENTLESS" or endpoint.application.clienttype=="CVC"
```

- このエンドポイント式は、Norton Antivirus バージョン 10.x かどうかをテストしますが、10.5.x は除外します。

```
(endpoint.av.NortonAV.version > "10" and endpoint.av.NortonAV.version < "10.5") or
endpoint.av.NortonAV.version > "10.6"
```

DAP 接続シーケンス

次のシーケンスに、標準的なリモート アクセス接続を確立する場合の概要を示します。

1. リモート クライアントが VPN 接続を試みます。
2. セキュリティ アプライアンスが、設定された NAC 値と Cisco Secure Desktop のホスト スキャン値を使用してポスチャ評価を実行します。
3. セキュリティ アプライアンスが、AAA を介してユーザを認証します。AAA サーバーは、ユーザーの認可属性も返します。
4. セキュリティ アプライアンスが、セッションに AAA 認可属性を適用し、VPN トンネルを確立します。
5. セキュリティ アプライアンスが、ユーザの AAA 認可情報とセッションのポスチャ評価情報に基づいて DAP レコードを選択します。
6. セキュリティ アプライアンスが、選択した DAP レコードから DAP 属性を集約します。集約された属性が DAP ポリシーを構成します。
7. セキュリティ アプライアンスが、その DAP ポリシーをセッションに適用します。

関連項目

- ダイナミック アクセス ポリシーの設定 （1829 ページ）
- ダイナミック アクセス ポリシーについて （1827 ページ）

• DAP 属性の設定 （1836 ページ）

DAP 属性の設定

DAP ポリシーに定義する属性には、認可属性とエンドポイント属性を指定する必要があります。ネットワーク ACL と Web タイプ ACL、ファイル ブラウジング、ファイル サーバ エントリ、HTTP プロキシ、URL エントリ、ポート転送リスト、および URL リストを設定することもできます。

ここでは、DAP ポリシーに必要な AAA 属性およびエンドポイント属性を作成または編集する方法について説明します。

関連項目

- DAP 属性について （1831 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）
- ダイナミック アクセス ポリシーについて （1827 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dynamic Access] ページが開きます。このページの要素の詳細については、[Dynamic Access] ページ（ASA）（1840 ページ）を参照してください。

ステップ 2 [ダイナミックアクセス（Dynamic Access）] ポリシーページで [作成（Create）] をクリックするか、またはこのページのテーブル内のポリシー行を選択して [編集（Edit）] をクリックします。

[Add/Edit Dynamic Access Policy] ダイアログボックスが開き、[Main] タブが表示されます。[Main] タブの要素の詳細については、[Main] タブ （1844 ページ）を参照してください。

ステップ 3 テーブルの下の [作成（Create）] をクリックするか、またはテーブル内の DAP エントリを選択して [編集（Edit）] をクリックします。[Add/Edit DAP Entry] ダイアログボックスが開きます。このダイアログボックスの要素の詳細については、[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （1853 ページ）を参照してください。

ステップ 4 [Criterion] リストから属性タイプを選択し、適切な値を入力します。ダイアログボックスの値は、選択に応じて変わります。次のオプションがあります。

- AAA 属性 Cisco（表 404 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）] （1857 ページ）を参照）。

- AAA 属性 LDAP（表 405 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP （1859 ページ）を参照）
- AAA 属性 RADIUS（表 406 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [AAA属性RADIUS（AAA Attributes RADIUS）] （1861 ページ）を参照）。
- アンチスパイウェア（表 407 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [スパイウェア対策（Anti-Spyware）] （1862 ページ）を参照）。
- アンチウイルス（表 408 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）] （1863 ページ）を参照）。
- AnyConnect アイデンティティ（表 409 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの AnyConnect ID （1865 ページ）を参照）。
- アプリケーション（表 410 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのアプリケーション （1866 ページ）を参照）。
- デバイス（表 411 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [デバイス（Device）] （1867 ページ）を参照）。
- ファイル（表 412 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル （1869 ページ） を参照）。
- NAC（表 413 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [NAC] （1871 ページ） を参照）。
- オペレーティングシステム（表 414 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）] （1872 ページ）を参照）。
- パーソナルファイアウォール（表 415 : [DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）] （1874 ページ）を参照）。
- ポリシー（表 416 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスポリシー （1875 ページ） を参照）。
- プロセス（表 417 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）] （1876 ページ）を参照）。
- レジストリ（表 418 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのレジストリ （1878 ページ）を参照）。
- マルチ証明書認証（表 420 : [DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）] （1881 ページ）を参照）。

ステップ 5 [OK] をクリックします。

ASA デバイスでの Cisco Secure Desktop ポリシーの設定

Cisco Secure Desktop（CSD）は、クライアント システム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供することによって、機密データのすべてのトレースを確実に除去する方法を提供します。CSD では、機密データが SSL VPN セッションの間だけ共有されるセッションベースのインターフェイスを使用できます。すべてのセッション情報が暗号化され、セッションが終了したときに（たとえ接続が突然終了した場合でも）、セッションデータのすべてのトレースがリモート クライアントから削除されます。このため、クッキー、ブラウザ履歴、一時ファイル、およびダウンロードしたコンテンツがシステムに残ることはありません。

セッションを閉じた場合、CSD は Department of Defense（DoD; 米国国防総省）消去アルゴリズムを使用して、すべてのデータを上書きして削除し、エンドポイントの機密保持を行います。

（注） Cisco Secure Desktop プログラムの詳細な機能および設定については、このマニュアルでは説明しません。CSD の設定および CSD の機能については、http://www.cisco.com/en/US/products/ps6742/tsd_products_support_configure.html のオンラインで入手できる資料を参照してください。設定する CSD バージョンのコンフィギュレーション ガイドを選択してください。

ここでは、ASA デバイスで Cisco Secure Desktop 機能を設定する方法について説明します。

はじめる前に

- 接続プロファイルポリシーがデバイスに設定済みであることを確認します。接続プロファイルの設定（ASA、PIX 7.0+）（1713 ページ）を参照してください。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+）（1713 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ASA デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dynamic Access] ページが開きます。このページの要素の詳細については、[Dynamic Access] ページ（ASA）（1840 ページ）を参照してください。

ステップ 2 [Cisco Secure Desktop] セクションで [CSDを有効化（Enable CSD）] を選択し、ASA デバイスで CSD を有効にします。

（注） [CSDを有効化（Enable CSD）] オプションは、ASA 9.5(2) 以前のバージョンの ASA を実行しているデバイスで使用できます。Security Manager 4.10 以降では、ASA バージョン 9.5(2) 以降を実行しているデバイスでのみ、Hostscan を設定する（CSD を無効にする）ための新しいチェックボックスを使用できます。

ステップ 3 [CSDパッケージ（CSD Package）] フィールドで、デバイスにアップロードする Cisco Secure Desktop パッケージを示すファイルオブジェクトの名前を指定します。[選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。

（注） パッケージ バージョンは、ASA オペレーティング システムのバージョンと互換性がある必要があります。デバイスビューでローカルポリシーを作成する場合、[バージョン（Version）] フィールドは選択すべき CSD パッケージのバージョンを示します。（バージョンはパッケージ ファイル名に含まれています。たとえば、securedesktop-asa_k9-3.3.0.118.pkg は CSD バージョン 3.3.0.118 です。) ポリシービューで共有ポリシーを作成する場合、[バージョン（Version）] フィールドは選択した CSD ファイルのバージョンを示します。バージョン互換性の詳細については、SSL VPN サポート ファイルの概要と管理 （1660 ページ）を参照してください。

ステップ 4 （任意）[Hostscanパッケージ（Hostscan Package）] フィールドで、デバイスにアップロードする Host Scan パッケージを示すファイルオブジェクトの名前を指定します。[選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。

ステップ 5 [設定（Configure）] をクリックして、セキュリティアプライアンスで CSD を設定できる Cisco Secure Desktop Manager（CSDM）ポリシーエディタを開きます。これは、Security Manager とは別のアプリケーションです。ポリシー エディタの使用方法については、上記の CSD のマニュアルを参照してください。

エディタに含まれる主な項目は、次のとおりです（コンテンツ テーブルで選択します）。

- [Prelogin Policies]：これは決定ツリーです。ユーザが接続を試みると、そのユーザのシステムがルールに照らして評価され、最初に一致したルールが適用されます。通常は、セキュアなロケーション、ホーム ロケーション、およびセキュアでないパブリック ロケーションのポリシーを作成します。レジストリ情報、特定のファイルまたは証明書があるかどうか、ワークステーションのオペレーティング システム、または IP アドレスに基づいてチェックを行うことができます。

編集を行う場合は、必ず右クリック メニューを使用します。ボックスまたは [+] 記号を右クリックして、関連する設定をアクティブにします（ある場合）。

エンド ノードの場合は、次のオプションを選択できます。

- [Access Denied]：基準に一致するワークステーションがネットワークにアクセスできなくなります。
- [Policy]：この時点での固有の許可ポリシーを定義します。ポリシーは、名前を付けた後にコンテンツ テーブルに追加されます。ポリシーの各項目を選択して、その設定を行います。
- [Subsequence]：追加チェックを実行します。このワークステーションを評価する次の決定ツリーの名前を入力します。
- [Host Scan]：基本ホスト スキャンの一部を構成する一連のレジストリ エントリ、ファイル名、およびプロセス名を指定できます。ホスト スキャンは、プリログイン評価が行われた後、ダイナミック アク

セス ポリシーが割り当てられる前に実行されます。セキュリティ アプライアンスは、基本ホスト スキャンの後、ログイン クレデンシャル、ホスト スキャン結果、プリログイン ポリシー、および設定された他の基準に基づいて、ダイナミック アクセス ポリシーを割り当てます。次のアセスメントをイネーブルにできます。

- [Endpoint Assessment]：リモート ワークステーションは、アンチウイルス、アンチスパイウェア、パーソナル ファイアウォールの各アプリケーション、および関連する更新の大規模なコレクションをスキャンします。
- [Advanced Endpoint Assessment]：すべてのエンドポイント評価機能を含みます。また、指定されたバージョン要件を満たすように、準拠していないワークステーションの更新を試みるよう設定できます。この機能を設定するには、ライセンスを購入してインストールする必要があります。

[Dynamic Access] ページ（ASA）

[Dynamic Access] ページを使用して、セキュリティ アプライアンスで定義されている Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）を参照します。このページから、DAP を作成、編集、または削除できます。

[Cisco Secure Desktop] セクションを使用して、選択した ASA デバイスで Cisco Secure Desktop（CSD）ソフトウェアをイネーブルにし、ダウンロードします。Cisco Secure Desktop は、クライアント システム上にセッション アクティビティおよび削除のためのセキュアなロケーションを 1 つだけ提供することで、機密性が高いデータを SSL VPN セッションの間だけ共有できるようにしています。

（注） SSL VPN ポリシーが適切に機能するためには、CSD クライアント ソフトウェアがデバイスにインストールされてアクティブになっている必要があります。

ヒント ダイナミック アクセス ポリシーは、グループ ポリシーに優先します。ダイナミック アクセス ポリシーで設定を指定していない場合、ASA デバイスは設定を指定しているグループ ポリシーがないかどうかを確認します。

ナビゲーション パス

- （デバイスビュー）ASA デバイスを選択し、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（ASA）（Dynamic Access (ASA)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ダイナミック アクセス ポリシーについて （1827 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）
- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）

フィールド リファレンス

表 *401 : [Dynamic Access Policy]* ページ（*ASA*）

要素	説明
プライオリティ	設定済みのダイナミック アクセス ポリシー レコードのプライオリティ。
名前	設定済みのダイナミック アクセス ポリシー レコードの名前。
Network ACL	セッションに適用されるファイアウォール ACL の名前。
WebType ACL	セッションに適用される Web タイプ VPN ACL。
ポート転送	セッションに適用されるポート転送リストの名前。
[Bookmarks（ブックマーク）]	セッションに適用される SSL VPN ブックマーク オブジェクトの名前。
終了（Terminate）	セッションが終了しているかどうかを示します。
説明	設定済みのダイナミック アクセス ポリシーに関する追加情報。
[Create] ボタン	このボタンをクリックして、ダイナミック アクセス ポリシーを作成します。 [Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を参照してください。
[編集（Edit）] ボタン	このボタンをクリックして、選択したダイナミックアクセスポリシーを編集します。 [Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を参照してください。
[削除（Delete）] ボタン	このボタンをクリックして、選択したダイナミックアクセスポリシーを削除します。
Cisco Secure Desktop ASA デバイスで CSD を設定する手順については、 ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）を参照してください。	

要素	説明
Enable CSD	選択すると、デバイスで CSD がイネーブルになります。CSD をイネーブルにすると、指定した Cisco Secure Desktop パッケージがロードされます。CSDパッケージファイルを転送または置換する場合は、CSD をいったんディセーブルにしてから、CSD をイネーブルにしてファイルをロードします。
CSD Package	デバイスにアップロードする Cisco Secure Desktop パッケージを識別するファイル オブジェクトの名前を指定します。 [選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。
Hostscan Package	デバイスにアップロードする Hostscan パッケージを識別するファイル オブジェクトの名前を指定します。 [選択（Select）] をクリックして既存のファイルオブジェクトを選択するか、新しいファイルオブジェクトを作成します。詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。
バージョン	パッケージ バージョンは、ASA オペレーティング システムのバージョンと互換性がある必要があります。デバイス ビューでローカル ポリシーを作成する場合、[Version] フィールドは選択する必要がある CSD パッケージ バージョンを示します（バージョンはパッケージ ファイル名に含まれています。たとえば、securedesktop-asa_k9-3.3.0.118.pkg は CSD バージョン 3.3.0.118 です）。ポリシービューで共有ポリシーを作成する場合、[バージョン（Version）] フィールドは選択した CSD ファイルのバージョンを示します。バージョン互換性の詳細については、SSL VPN サポート ファイルの概要と管理 （1660 ページ）を参照してください。
設定（Configure）	[設定（Configure）] をクリックして、セキュリティアプライアンスで CSD を設定できる Cisco Secure Desktop Manager（CSDM）ポリシーエディタを開きます。このダイアログボックスの要素の詳細については、[Cisco Secure Desktop Manager Policy Editor] ダイアログボックス（1888 ページ）を参照してください。

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスを使用して、セキュリティ アプライアンスで Dynamic Access Policy（DAP; ダイナミック アクセス ポリシー）

を設定します。追加するダイナミック アクセス ポリシーに名前を指定し、プライオリティを選択し、LUA 表現で属性を指定できます。また、ネットワークおよび Web タイプ ACL フィルタ、ファイルアクセス、HTTP プロキシ、URL エントリおよびリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式に対して属性を設定できます。

（注） ダイナミック アクセス ポリシー属性の詳細については、DAP 属性について （1831 ページ）を参照してください。

これらのタブは、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスで使用可能です。

- [Main] タブ （1844 ページ）
- [論理的な操作（Logical Operators）] タブ （1884 ページ）
- [Advanced Expressions] タブ （1887 ページ）

ナビゲーション パス

[Dynamic Access] ページ（ASA） （1840 ページ）を開き、[作成（Create）] をクリックするか、テーブルのダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスが表示されます。

関連項目

- ダイナミック アクセス ポリシーについて （1827 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 402 : [Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス

要素	説明
名前	ダイナミック アクセス ポリシー レコードの名前（最大 128 文字）。
プライオリティ	ダイナミック アクセス ポリシー レコードのプライオリティ。セキュリティ アプライアンスは、ここで設定した順序でアクセス ポリシーを適用します。数が大きいほどプライオリティは高くなります。プライオリティ設定が同じで、ACL ルールが競合するダイナミック アクセス ポリシー レコードがある場合は、最も厳しいルールが適用されます。 プライオリティは、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。

要素	説明
説明	ダイナミック アクセス ポリシー レコードに関する追加情報（最大 1024 文字）。 説明は、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。
[メイン（Main）] タブ	ダイナミック アクセス ポリシー エントリを追加し、設定するリモート アクセスのタイプに応じてアクセス ポリシーの属性を設定できます。 このタブの要素の詳細については、[Main] タブ （1844 ページ）を参照してください。
[論理的な操作（Logical Operators）] タブ	各タイプのエンドポイント属性の複数のインスタンスを作成できます。 このタブの要素の詳細については、[論理的な操作（Logical Operators）] タブ （1884 ページ）を参照してください。
[Advanced Expressions] タブ	1 つ以上の論理式を設定して、[AAA] および [Endpoint] 領域で設定できない AAA 属性またはエンドポイント属性を設定できます。 このタブの要素の詳細については、[Advanced Expressions] タブ （1887 ページ）を参照してください。

[Main] タブ

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスの [Main] タブを使用して、セキュリティ アプライアンスでサポートされるダイナミック アクセス ポリシー属性およびリモート アクセス方式のタイプを設定します。ネットワークおよび Web タイプ ACL フィルタ、ファイル アクセス、HTTP プロキシ、URL エントリおよびリスト、ポート転送、およびクライアントレス SSL VPN アクセス方式に対して属性を設定できます。

ナビゲーション パス

[Main] タブは、[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス（1842 ページ）を開くと表示されます。

関連項目

- ダイナミック アクセス ポリシーの設定 （1829 ページ）
- DAP 属性の設定 （1836 ページ）

フィールド リファレンス

表 *403 : [ダイナミックアクセスポリシーの追加/編集（Add/Edit Dynamic Access Policy）] ダイアログボックス > [Main] タブ*

要素	説明
Criteria ID	ダイナミック アクセス ポリシーに使用可能な AAA およびエンドポイントの選択属性名。
Content	セキュリティ アプライアンスがセッションの確立中にダイナミック アクセス ポリシー レコードを選択および適用するために使用する、AAA 属性およびエンドポイント属性の値。ここで設定した属性値は、AAA システム内の認可の値（既存のグループ ポリシー、トンネル グループ、およびデフォルト グループ レコード内の値を含む）を上書きします。
[Create] ボタン	このボタンをクリックして、AAA 属性およびエンドポイント属性を DAP レコードの選択基準として設定します。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （1853 ページ）を参照してください。
[編集（Edit）] ボタン	このボタンをクリックして、選択したダイナミック アクセス ポリシーを編集します。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス （1853 ページ）を参照してください。
[削除（Delete）] ボタン	このボタンをクリックして、選択したダイナミック アクセス ポリシーを削除します。
アクセス方式	許可されるリモート アクセスのタイプを指定します。 • [Unchanged]：現在のリモート アクセス方式を引き続き使用します。 • [AnyConnect Client]：Cisco AnyConnect VPN クライアントを使用して接続します。 • [Webポータル（Web Portal）]：クライアントレス VPN を使用して接続します。 • [両方、デフォルトはWebポータル（Both default Web Portal）]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトはクライアントレスです。 • [両方、デフォルトはAnyConnect（Both default AnyConnect Client）]：クライアントレスまたは AnyConnect クライアントを介して接続します。デフォルトは AnyConnect です。

要素	説明
[Network ACL] タブ：このダイナミック アクセス ポリシーに適用するネットワーク ACL を選択および設定できます。ダイナミック アクセス ポリシーの ACL には、許可ルールと拒否ルールのいずれかを含めることができますが、両方を含めることはできません。ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキュリティ アプライアンスで拒否されます。	
Network ACL	SSL†VPN へのユーザ アクセスを制限するために使用されるアクセス コントロール リスト（ACL）が一覧表示されます。 Security Manager バージョン 4.10 以降、ネットワーク ACL は IPv6 エントリをサポートします。また、IPv6は、ソフトウェアバージョン ASA 9.0 以降を実行しているデバイスでサポートされています。これは、ネットワーク ACL と Web タイプ ACL の両方に適用されます。 [選択（Select）] ボタンをクリックして、Access Control Lists Selector を開きます。ここから選択できます。ACL には、パケットのトラフィック ストリームが記述された条件と、それらの条件に基づいて実行する処理が記述されたアクションが含まれます。許可ルールだけ、または拒否ルールだけが含まれている ACL だけが適格となります。 ネットワーク ACL は、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。
[AnyConnect] タブ：AnyConnect サービスプロファイルの Always-on VPN の設定を未変更にするか、ディセーブルにするか、AnyConnect プロファイル設定を使用するかを選択できます。Always-On VPN を使用すると、システムにログオンした後、AnyConnnect で VPN セッションを自動的に確立できます。	
[カスタム属性] タブ：AnyConnect カスタム属性タイプとカスタム属性名を一覧表示します。AnyConnect カスタム属性により、ASA ソフトウェアをアップグレードすることなく、新しいクライアントコントロールの追加を総合的にサポートする機能を ASA に提供することで、新しいエンドポイント機能のより迅速な配信と展開が可能になります。バージョン 4.7 以降、Security Manager では、カスタム属性データを既存のカスタム属性タイプに追加できます。この機能は、ASA ソフトウェアバージョン 9.3(1) 以降を実行しているデバイスでサポートされています。	
属性タイプ	[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1801 ページ）ページで設定した属性タイプを選択します。
属性名	[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1801 ページ）ページで設定した属性名を選択します。

要素	説明
[WebType ACL] タブ：このダイナミック アクセス ポリシーに適用する Web タイプ ACL を選択および設定できます。ダイナミック アクセス ポリシーの ACL には、許可ルールまたは拒否ルールを含めることができます。ACL に許可ルールと拒否ルールの両方が含まれる場合は、セキュリティ アプライアンスで拒否されます。	
Web Type ACL	SSL†VPN へのユーザ アクセスを制限するために使用される Web タイプ アクセス コントロール リストを指定します。 [選択（Select）] ボタンをクリックして、Access Control Lists Selector を開きます。ここから選択できます。許可ルールだけ、または拒否ルールだけが含まれている ACL だけが適格となります。バージョン 4.10 以降では、Web タイプ ACL に IPv6 値を入力できます。
[Functions] タブ：ファイル サーバのエントリとブラウズ、HTTP プロキシ、およびダイナミック アクセス ポリシーの URL エントリを設定できます。	
[ファイルサーバーブラウズ（File Server Browsing）]	ポータル ページで設定するファイル サーバ ブラウズ設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：ファイルサーバーまたは共有機能に対する CIFS ブラウズをイネーブルにします。 • [無効（Disable）]：ファイルサーバーまたは共有機能に対する CIFS ブラウズをディセーブルにします。 （注） ブラウズには、NBNS（プライマリブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。CIFS ブラウズ機能では、国際化がサポートされていません。

要素	説明
File Server Entry	ポータル ページで設定するファイル サーバ エントリ設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：ユーザはポータルページでファイルサーバーのパスおよび名前を入力できます。 イネーブルになっている場合、ポータルページにファイルサーバーエントリのドロワが配置されます。ユーザーは、Windowsファイルへのパス名を直接入力できます。ユーザーは、ファイルをダウンロード、編集、削除、名前変更、および移動できます。また、ファイルおよびフォルダを追加することもできます。適用可能なWindowsサーバーでユーザーアクセスに対して共有を設定する必要もあります。ネットワークの要件によっては、ユーザーがファイルへのアクセス前に認証を受ける必要があることもあります。 • [無効（Disable）]：ユーザはポータルページでファイルサーバーのパスおよび名前を入力できません。

要素	説明
HTTP プロキシ	HTTPS 接続を終了して HTTP/HTTPS 要求を HTTP および HTTPS プロキシ サーバに転送するための、セキュリティ アプライアンスの設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：HTTP アプレットプロキシのクライアントへの転送を許可します。 このプロキシは、適切なコンテンツ変換に干渉するテクノロジー（Java、ActiveX、Flash など）に対して有用です。このプロキシによって、セキュリティアプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、ブラウザの古いプロキシ設定を変更し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。 • [無効（Disable）]：HTTP アプレットプロキシのクライアントへの転送をディセーブルにします。 • [自動開始（Auto-start）]：HTTP プロキシをイネーブルにし、DAP レコードによりこれらの機能に関連付けられたアプレットが自動的に開始されるように設定します。

要素	説明
URL Entry	SSL VPN を使用しても、すべてのサイトとの通信が必ずしもセキュアになるとはかぎりません。SSL VPN は、リモートユーザの PC またはワークステーションと、企業ネットワークのセキュリティアプライアンスの間のデータ送信のセキュリティを確保します。ユーザが（インターネットまたは内部ネットワークに存在する）HTTPS 以外の Web リソースにアクセスする場合、企業セキュリティ アプライアンスから宛先 Web サーバへの通信は保護されません。 クライアントレス VPN 接続では、セキュリティ アプライアンスがエンド ユーザ Web ブラウザとターゲット Web サーバの間のプロキシとして機能します。ユーザが SSL 対応の Web サーバに接続すると、セキュリティ アプライアンスによりセキュアな接続が確立され、サーバ SSL 証明書が検証されます。エンド ユーザー ブラウザでは提示された証明書を受信しないため、証明書を調査して検証することはできません。SSL VPN の現在の実装では、期限切れになった証明書を提示するサイトとの通信は許可されません。また、セキュリティ アプライアンスが信頼できる CA 証明書検証を実行することも許可されません。このため、ユーザーは、SSL 対応の Web サーバーと通信する前に、そのサーバーにより提示された証明書を分析することはできません。 ポータル ページでの URL エントリの設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：ユーザはポータルページで HTTP または HTTPS の URL を入力できます。この機能がイネーブルになっている場合、ユーザーは URL エントリ ボックスに Web アドレスを入力できます。また、クライアントレス SSL VPN を使用して、これらの Web サイトにアクセスできます。 • [無効（Disable）]：ユーザはポータルページで HTTP または HTTPS の URL を入力できません。 （注） ユーザのインターネットアクセスを制限するには、[URL エントリ（URL Entry）] フィールドで [無効（Disable）] を選択します。これにより、SSL VPN ユーザはクライアントレス VPN 接続中に Web をサーフィンできなくなります。

要素	説明
[Port Forwarding] タブ：ユーザ セッションのポート転送リストを選択および設定できます。 （注） ポート転送は、一部の SSL/TLS バージョンでは使用できません。 注意 ポート転送（アプリケーション アクセス）およびデジタル証明書をサポートする Sun Microsystems Java Runtime Environment（JRE）1.4+ がリモート コンピュータにインストールされていることを確認します。	
ポート転送	この DAP レコードに適用されるポート転送リストのオプションを選択します。 • [変更なし（Unchanged）]：実行コンフィギュレーションから属性を削除します。 • [有効（Enable）]：デバイスでポート転送をイネーブルにします。 • [無効（Disable）]：デバイスでポート転送をディセーブルにします。 • [自動開始（Auto-start）]：ポート転送をイネーブルにし、DAP レコードによりそのポート転送リストに関連付けられたポート転送アプレットが自動的に開始されるように設定します。
Port Forwarding List	クライアントマシン上のポート番号から SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートへのマッピングを定義する、ポート転送リスト。 [選択（Select）] をクリックすると [ポート転送リストセレクタ（Port Forwarding List Selector）] が開き、そこで、ポート転送リストオブジェクトのリストから必要なポート転送リストを選択できます。ポート転送リストオブジェクトは、リモートクライアント上のポート番号から SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートへのマッピングを定義します。
[Bookmark] タブ：SSL VPN ブックマークをイネーブルにし、設定できます。イネーブルになっている場合、SSL VPN に正常にログインしたユーザに、定義済みのブックマークのリストを含むポータルページが表示されます。これらのブックマークにより、ユーザは [Clientless] アクセス モードで SSL VPN Web サイト上で使用可能なリソースにアクセスできます。	

要素	説明
Enable Bookmarks	ポータル ページで設定するファイル サーバ ブラウズ設定を指定します。 • [変更なし（Unchanged）]：このセッションに適用するグループ ポリシーの値を使用します。 • [有効（Enable）]：SSL VPN ポータルページのブックマークをイネーブルにします。 • [無効（Disable）]：SSL VPN ポータルページのブックマークをディセーブルにします。
ブックマーク	ユーザが SSL VPN Web サイトで使用可能なリソースにアクセスできるように、ポータルページにブックマークとして表示される Web サイトのリスト。 [選択（Select）] をクリックすると、[ブックマークセレクタ（Bookmarks Selector）] が開きます。このセレクタで適宜、リストから目的のブックマークを選択するか、新しいブックマークを作成できます。
[Action] タブ：特定の接続またはセッションに適用される特別な処理を指定します。 [アクション（Action）] タブは、マルチコンテキスト ASA バージョン 9.6(2) 以降のデバイスの Security Manager バージョン 4.12 以降でサポートされています。 ドロップダウン リストから、次のいずれかのオプションを選択します。	
続行（Continue）	（デフォルト）選択すると、セッションが続行されます。デフォルトでは、アクセス ポリシー属性がセッションに適用され、セッションは実行されます。
検疫（Quarantine）	選択すると、セッションが隔離されます。 検疫を使用すると、VPN経由ですでにトンネルを確立した特定のクライアントを制限できます。制限付き ACL がセッションに適用され、制限付きグループが形成されます。この基になるのは、選択された DAP レコードです。管理目的で定義されたポリシーにエンドポイントが準拠していないときも、ユーザは修復のためのサービス（たとえばアンチウイルスアプリケーションのアップデート）にアクセスできますが、そのユーザには制限が適用されます。修復後、ユーザーは再接続できます。この再接続により、新しいポスチャ アセスメントが起動されます。このアセスメントに合格すると、接続されます。 （注） このパラメータを使用するには、AnyConnect セキュア モビリティ機能をサポートしている AnyConnect リリースが必要です。

要素	説明
終了（Terminate）	選択した場合、セッションが終了します。デフォルトでは、アクセスポリシー属性がセッションに適用され、セッションは実行されます。
ユーザ メッセージ	この DAP レコードが選択されたときにポータル ページに表示されるテキスト メッセージを入力します。最大 128 文字を入力できます。ユーザ メッセージは、黄色のオーブとして表示されます。ユーザがログインすると、メッセージは 3 回点滅してから静止します。複数の DAP レコードが選択されており、かつ、それぞれにユーザ メッセージが設定されている場合は、すべてのユーザ メッセージが表示されます。 （注） このようなメッセージには、URL やその他の埋め込みテキストを含めることができます。この場合は、正しい HTML タグを使用する必要があります。例：すべてのコントラクタは、ご使用のアンチウイルスソフトウェアのアップグレード手順について、手順 を参照してください。 （注） ユーザメッセージは、マルチコンテキストモードでバージョン 9.6(2) 以降を実行している ASA デバイスの Security Manager バージョン 4.12 以降でサポートされています。

マルチコンテキスト ASA 9.6(2) デバイスの Security Manager バージョン 4.12 以降でサポートされるダイナミック アクセス ポリシー CLI は次のとおりです。

- Dynamic-access-policy-record アクション
- description
- exit
- help
- network-acl
- ×
- プライオリティ
- quit
- user-message

[Add DAP Entry]/[Edit DAP Entry] ダイアログボックス

[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスを使用して、ダイナミック アクセス ポリシーの認可属性とエンドポイント属性を指定します。セキュリティ アプライアンスは、リモート デバイスのエンドポイント セキュリティ情報と認証済みユーザの AAA 認可情報に基づい

て、ダイナミック アクセス ポリシーを選択します。次に、そのダイナミック アクセス ポリシーをユーザ トンネルまたはセッションに適用します。

ダイナミック アクセス ポリシー属性の詳細については、DAP 属性について （1831 ページ）を参照してください。

このダイアログボックスの内容は、選択した基準によって変わります。この基準は、セキュリティ アプライアンスがセッション確立中にダイナミック アクセス ポリシーを選択および適用するときに使用する選択基準として機能する認可またはエンドポイント属性です。次の基準から選択できます。

- [AAA Attributes Cisco]：AAA 階層モデルに格納されているユーザ認可属性を参照します。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）] （1856 ページ）を参照してください
- [AAA Attributes LDAP]：LDAP クライアントにおいて、ユーザの AAA セッションに関連付けられたデータベースに、すべてのネイティブ LDAP 応答属性のペアが格納されるように設定します。 [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP （1858 ページ）を参照してください。
- [AAA Attributes RADIUS]：RADIUS クライアントがユーザの AAA セッションに関連付けられたデータベースにすべてのネイティブ RADIUS 応答属性のペアを格納するように設定します。 [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [AAA属性RADIUS（AAA Attributes RADIUS）] （1860 ページ）を参照してください。
- [Anti-Spyware]：[Anti-Spyware] タイプのエンドポイント属性を作成します。Cisco Secure Desktop のホスト スキャン モジュールを使用して、リモート コンピュータで実行されているアンチスパイウェア アプリケーションおよび更新をスキャンできます。 [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [スパイウェア対策（Anti-Spyware）] （1861 ページ）を参照してください。
- [Anti-Virus]：[Anti-Virus] タイプのエンドポイント属性を作成します。Cisco Secure Desktop のホスト スキャン モジュールを使用して、リモート コンピュータで実行されているアンチウイルス アプリケーションおよび更新をスキャンできます。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）] （1863 ページ）を参照してください。
- [AnyConnect アイデンティティ（AnyConnect Identity）]：[AnyConnect アイデンティティ（AnyConnect Identity）] タイプのエンドポイント属性を作成します。 [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの AnyConnect ID （1864 ページ）を参照してください。
- [Application]：リモート アクセス接続のタイプを示します。 [DAPエントリの追加（Add DAP Entry）、]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのアプリケーション （1866 ページ）を参照してください。
- [デバイス（Device）]：[デバイス（Device）] タイプのエンドポイント属性を作成します。[デバイス基準（Device Criterion）] では、関連付けられたプリログイン ポリシー チェック中に使用できる特定のデバイス情報を提供できます。 [DAPエントリの追加（Add DAP

Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス>[デバイス（Device）]（1867 ページ）を参照してください。

- [File]：[File] タイプのエンドポイント属性を作成します。Cisco Secure Desktop Manager を使用して、基本ホスト スキャンによって実行されるファイル名チェックを明示的に設定する必要があります。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル （1868 ページ）を参照してください。
- [NAC]：[NAC] タイプのエンドポイント属性を作成します。NAC は、エンドポイント準拠を実行することにより、ワーム、ウイルス、および不正なアプリケーションの侵入や感染からエンタープライズ ネットワークを保護します。これらのチェックをポスチャ検証と呼びます。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [NAC] （1870 ページ）を参照してください。
- [Operating System]：[Operating System] タイプのエンドポイント属性を作成します。CSD のプリログイン評価モジュールは、リモート デバイスの OS バージョン、IP アドレス、および Microsoft Windows レジストリ キーをチェックできます。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）] （1871 ページ）を参照してください。
- [Personal Firewall]：[Personal Firewall] タイプのエンドポイント属性を作成します。Cisco Secure Desktop のホスト スキャン モジュールを使用して、リモート コンピュータで実行されているパーソナル ファイアウォール アプリケーションおよび更新をスキャンできます。このダイアログボックスの要素の詳細については、[DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）] （1873 ページ）を参照してください。
- [Policy]：[Policy] タイプのエンドポイント属性を作成します。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスポリシー （1874 ページ）を参照してください。
- [Process]：Cisco Secure Desktop Manager を使用して、基本ホスト スキャンによって実行されるプロセス名チェックを明示的に設定する必要があります。[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）] （1875 ページ）を参照してください。
- [Registry]：[Registry] タイプのエンドポイント属性を作成します。レジストリ キー スキャンは、Microsoft Windows オペレーティング システムを実行しているコンピュータにだけ適用されます。[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスのレジストリ （1877 ページ）を参照してください。
- [複数証明書認証（Multiple Certificate Authentication）]：[複数証明書認証（Multiple Certificate Authentication）] タイプのエンドポイント属性を作成します。リモート VPN ユーザーの複数証明書認証の属性を指定できます。[DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）] （1881 ページ）を参照してください。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）]

ダイナミック アクセス ポリシーの選択基準として AAA 属性を設定するには、[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスで、セッションの確立中にダイナミック アクセス ポリシーを選択および適用するときに使用する選択基準として [AAA Attributes Cisco] を設定します。これらの属性を、入力した値と一致するように、または一致しないように設定できます。各ダイナミック アクセス ポリシーの AAA 属性の数に制限はありません。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性Cisco（AAA Attributes Cisco）] を選択します。

関連項目

- DAP 属性について （1831 ページ）

- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *404 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）]ダイアログボックス、[AAA属性Cisco（AAA Attributes Cisco）]*

要素	説明
基準	選択基準として [AAA Attributes Cisco] が表示されます。
[グループ ポリシー（Group Policy）]	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、ユーザーに関連付けられた AAA サーバーグループの名前を入力します。64 文字まで指定できます。 AAA サーバ グループは、ネットワーク セキュリティ ポリシー全体の特定の側面を実施することに焦点を当てた、認証サーバの集合を表します。
IPv4 アドレス	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、割り当てられた IP アドレスを入力します。 アドレスは、定義済みのネットワーク オブジェクトです。また、[選択（Select）] をクリックすると、使用可能なすべてのネットワークホストが一覧表示されたダイアログボックスが開きます。このダイアログボックスで、ネットワーク ホスト オブジェクトを作成または編集できます。 **ヒント** このオプションを選択して、あとでルールを ASDM で参照すると、IP アドレス属性は [Assigned IP Address] になります。
IPv6 アドレス （Security Manager バージョン 4.12 以降および ASA バージョン 9.0 以降）	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、割り当てられた IP アドレスを入力します。 アドレスは、定義済みのネットワーク オブジェクトです。また、[選択（Select）] をクリックすると、使用可能なすべてのネットワークホストが一覧表示されたダイアログボックスが開きます。このダイアログボックスで、ネットワーク ホスト オブジェクトを作成または編集できます。 **ヒント** このオプションを選択して、あとでルールを ASDM で参照すると、IP アドレス属性は [Assigned IP Address] になります。

要素	説明
Member-of	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、ユーザーに適用されるグループポリシー名をカンマ区切りの文字列として入力します。この属性により、複数のグループ メンバーシップを指定できます。最大長は 128 文字です。 **ヒント** このオプションを選択して、あとでルールを ASDM で参照すると、このオプションは表示されません。このオプションは [memberof LDAP] 属性と間違いやすいため、通常はこのオプションは使用されません。このルールはローカル認証にも適用されるため、[Member-of] 属性の代わりに [Username] 属性を使用できます。
ユーザー名	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、認証済みユーザーのユーザー名を入力します。最大 64 文字を使用できます。
[ユーザー名2（Username 2）]	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] または [次に一致しない（isn't）] など）を選択して、認証済みユーザーのセカンダリユーザー名を入力します。
接続プロファイル	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、セキュリティアプライアンスで定義されているすべての SSL VPN Connection Profile ポリシーのリストから接続プロファイルを選択します。 SSL VPN 接続プロファイルは、VPN トンネル接続プロファイル ポリシーを含む一連のレコードで構成されます。このレコードには、トンネルそのものの作成に関連する属性も含まれます。 （注） SSL VPN Connection Profiles ポリシーの設定手順については、接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照してください。
必要な SCEP	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] または [次に一致しない（isn't）]）を選択して、[True] または [False] を選択します。この属性により、接続が証明書認証に失敗したかどうかを照合できます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP

LDAP クライアントでは、ユーザの AAA セッションに関連付けられたデータベースに、すべての LDAP 応答属性値のペアが格納されます。LDAP クライアントでは、受信した順に応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードとグループ レコードの両方が LDAP サーバーから読み込まれると、このシナリオが発生する場合があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

Active Directory グループ メンバーシップをサポートするために、AAA LDAP クライアントでは、LDAP memberOf 応答属性に対する特別な処理が行われます。AD memberOf 属性は、AD 内のグループ レコードの DN 文字列を指定します。グループの名前は、DN 文字列内の最初の CN 値です。LDAP クライアントでは、DN 文字列からグループ名を抽出して、AAA memberOf 属性として格納し、応答属性データベースに LDAP memberOf 属性として格納します。LDAP 応答メッセージ内に追加の memberOf 属性が存在する場合、それらの属性からグループ名が抽出され、前の AAA memberOf 属性と結合されて、グループ名がカンマで区切られた文字列が生成されます。この文字列は応答属性データベース内で更新されます。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性LDAP（AAA Attributes LDAP）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *405 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス の AAA 属性 LDAP*

要素	説明
基準	選択基準として [AAA Attributes LDAP] が表示されます。
属性 ID	ダイナミック アクセス ポリシー内の LDAP 属性マップの名前を指定します。LDAP 属性マップは、ユーザが定義した属性名をシスコ定義の属性にマッピングします。最大 64 文字を使用できます。

要素	説明
値	ドロップダウンリストから一致基準（*is* など）を選択して、Cisco マップ値にマップされるカスタムマップ値を入力するか、カスタムマップ値にマップされる Cisco マップ値を入力します。複数の値を入力するには、各値を区切り文字の**;** で区切ります。 属性マップには、カスタマーのユーザ定義属性値をカスタマー属性名および一致する Cisco 属性の名前と値に適用する値マッピングが読み込まれます。 または、[ADグループのフェッチ（Fetch AD Groups）] ボタンをクリックして、[ADグループのフェッチ（Fetch AD Groups）] ダイアログボックスを開きます。ダイアログボックスの表には、選択できる使用可能な LDAP サーバーのユーザグループ ID とユーザグループ名がリストされます。1 つ以上の行を選択し、[選択（Select）] ボタンをクリックします。 リスト内の特定のユーザグループを検索するには、[フィルター（Filter）] テキストボックスにテキストを入力して、[検索（Search）] をクリックします。条件を満たすユーザグループ名がリストに表示されます。 （注） 使用可能な LDAP サーバーのリストを表示できるようにするには、最初にドメインから AD サーバーグループへのマッピングを設定する必要があります。このタスクを実行するには、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] に移動し、コンテンツテーブルから [設定の確認（Identity Settings）] を選択します。詳細については、[Identity Settings] ページ （693 ページ）を参照してください。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [AAA属性RADIUS（AAA Attributes RADIUS）]

RADIUS クライアントは、ユーザの AAA セッションに関連付けられたデータベースにすべての RADIUS 応答属性値のペアを格納します。RADIUS クライアントは、受け取った順序で応答属性をデータベースに書き込みます。その名前の後続の属性はすべて廃棄されます。ユーザー レコードおよびグループ レコードの両方が RADIUS サーバーから読み込まれた場合、このシナリオが発生する可能性があります。ユーザー レコード属性が最初に読み込まれ、グループ レコード属性よりも常に優先されます。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性RADIUS（AAA Attributes RADIUS）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *406*：*[DAP*エントリの追加/編集（*Add/Edit DAP Entry*）*]*ダイアログボックスの *[AAA*属性 *RADIUS*（*AAA Attributes RADIUS*）*]*

要素	説明
基準	選択基準として [AAA Attributes RADIUS] が表示されます。
属性 ID	ダイナミック アクセス ポリシー内の RADIUS 属性の名前または番号を指定します。最大 64 文字を使用できます。 3 つのセキュリティ アプライアンスすべて（VPN 3000、PIX、および ASA）に対するサポートをより反映するために、RADIUS 属性名に cVPN3000 プレフィックスは含まれていません。アプライアンスは、属性名ではなく数値の属性 ID に基づいて、RADIUS 属性を使用します。LDAP 属性は、ID ではなく属性名で使用します。
値	ドロップダウンリストから一致基準（[は（is）] など）を選択して、属性値を入力します。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [スパイウェア対策（Anti-Spyware）]

Cisco Secure Desktop 機能のホスト スキャン機能を使用して、リモート コンピュータで実行されているアンチウイルス、パーソナルファイアウォール、およびアンチスパイウェアのアプリケーションと更新をスキャンできます。プリログイン ポリシーおよびホスト スキャンのオプションの設定に続いて、ホスト スキャン結果の 1 つまたは任意の組み合わせの一致を設定して、ユーザ ログイン後のダイナミック アクセス ポリシーに割り当てることができます。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [スパイウェア対策（Anti-Spyware）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *407 : [DAP*エントリの追加/編集（*Add/Edit DAP Entry*）*]* ダイアログボックスの *[*スパイウェア対策（*Anti-Spyware*）*]*

要素	説明
基準	選択基準として [Anti-Spyware] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたマルウェア対策がリモートPC上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：指定されたマルウェア対策がリモートPC上に存在して有効になっていることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたマルウェア対策がリモートPC上に単に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	[一致（Matches）] を [タイプ（Type）] として選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	[一致（Matches）] を [タイプ（Type）] として選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、エンドポイント属性をそのバージョンと等しくするかどうかを指定します。

要素	説明
Last Update	[一致（Matches）] を [タイプ（Type）] として選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く実行するか、遅く実行するかを指定できます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）]

アンチウイルス アプリケーションおよび更新のスキャンを、Cisco AnyConnect またはクライアントレス SSL VPN 接続の完了の条件として設定できます。プリログイン評価に続いて、Cisco Secure Desktop ではエンドポイント評価チェックをロードし、ダイナミック アクセス ポリシーの割り当てに使用できるように、セキュリティ アプライアンスに結果を返します。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [アンチウイルス（Anti-Virus）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *408 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [アンチウイルス（Anti-Virus）]*

要素	説明
基準	選択基準として [Anti-Virus] が表示されます。

要素	説明
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたアンチウイルスがリモート PC 上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：指定されたアンチウイルスがリモート PC 上に存在して有効になっていることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたアンチウイルスがリモート PC 上に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、エンドポイント属性をそのバージョンと等しくするかどうかを指定します。
Last Update	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く実行するか、遅く実行するかを指定できます。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの AnyConnect ID

ダイナミック アクセス ポリシーの選択基準として AnyConnect ID 属性を設定するには、[DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスで AnyConnect ID を選択基準として設定します。ASA は、AnyConnect モバイル クライアントから受信した AnyConnect 識別属性に基づいて DAP エンドポイント属性を生成します。Security Manager を使用して Cisco Secure Desktop がこれらの特定の属性を設定できるようにする必要はありません。

ダイナミック アクセス ポリシーを割り当てる目的で、特定の DAP エントリに複数の AnyConnect アイデンティティ属性を設定した場合、いずれかの属性値が true の場合、エントリは一致と見

なされます。各ダイナミック アクセス ポリシーの AnyConnect アイデンティティ属性の数に制限はありません。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [AnyConnectアイデンティティ（AnyConnect Identity）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *409 : [DAP*エントリの追加/編集（*Add/Edit DAP Entry*）*]* ダイアログボックスの *AnyConnect ID*

要素	説明
基準	選択基準として [AnyConnectアイデンティティ（AnyConnect Identity）] を表示します。
クライアント バージョン（Client Version）	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* など）を選択して、AnyConnect クライアントのバージョン番号を入力します。
プラットフォーム	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is*など）を選択して、ドロップダウンリストから適切なプラットフォームを選択します。
プラットフォーム バージョン（Platform Version）	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is*など）を選択して、プラットフォームの適切なバージョン番号を入力します。

要素	説明
デバイスタイプ	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* など）を選択して、ドロップダウンリストから適切なデバイスタイプを選択します。
デバイス固有 ID	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* など）を選択して、固有のデバイス ID を入力します。この ID はデバイスを識別し、そのデバイス専用のポリシーを設定できるようにします。

[DAPエントリの追加（Add DAP Entry）、]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスのアプリケーション

このダイアログボックスを使用して、ダイナミック アクセス ポリシーのエンドポイント属性としてリモート アクセス接続のタイプを指定します。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [アプリケーション（Application）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *410 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスのアプリケーション

要素	説明
基準	選択基準として [Application] が表示されます。

要素	説明
Client Type	チェックボックスをオンにし、ドロップダウンリストから一致基準（*is* または *isn't* など）を選択して、リストからリモートアクセス接続のタイプ（[AnyConnect]、[Clientless]、[Cut-through Proxy]、[IPsec]、[Generic IKEv2 Client]、または [L2TP]）を指定します。 （注） クライアント タイプとして [AnyConnect] を選択した場合は、必ず Cisco Secure Desktop をイネーブルにしてください。Cisco Secure Desktop がイネーブルになっていないと、Security Manager でエラーが生成されます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [デバイス（Device）]

[DAP Device Criterion] では、関連付けられたプリログイン ポリシー チェック中に使用できる特定のデバイス情報を提供できます。[ホスト名（host name）]、[MACアドレス（MAC address）]、[ポート番号（port number）]、[プライバシー保護の選択（Privacy Protection selection）] のうち、1 つ以上のデバイス属性を指定し、属性ごとに照合対象（[is] または [isn't]）を指定できます。

[isn't] は排他的であることに注意してください。たとえば、Host Name isn't zulu_2 という基準を指定した場合、zulu_2 以外の名前のデバイスがすべて一致します。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [デバイス（Device）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *411 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [デバイス（Device）]*

要素	説明
基準	選択された [Criterion] として [Device] が表示されます。

要素	説明
ホスト名	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するデバイスホスト名を入力します。
MAC アドレス	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するデバイスの MAC アドレスを入力します。
BIOS シリアル番号	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するデバイスの BIOS シリアル番号値を入力します。数値フォーマットは、製造業者固有です。フォーマット要件はありません。
ポート番号（Port Number）	このオプションを選択し、一致基準（[is] または [isn't]）を選択して、照合するデバイスポートを入力するか、または選択します。
TCP/UDPポート番号（TCP/UDP Port Number）	このオプションを選択し、一致基準（[is] または [isn't]）を選択して、照合するリスニング状態の TCP/UDP ポートを入力するか、または選択します。 TCP/UDP コンボボックスでは、照合対象のポートの種類（TCP（IPv4）、UDP（IPv4）、TCP（IPv6）、または UDP（IPv6））を選択します。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。複数のポートを照合する場合は、DAP の個々のエンドポイント属性ルールを複数作成し、各ルールにポートを 1 つ指定します。
Privacy Protection	このオプションを選択し、一致基準（[is] または [isn't]）を選択し、デバイスで定義されている [プライバシー保護（Privacy Protection）] オプション（[none]、[cache cleaner]、または [secure desktop]）を選択します。
CSDバージョン（CSD Version）	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、エンドポイントで実行中の Host Scan イメージのバージョンを入力します。
エンドポイント評価バージョン（Endpoint Assessment Version）	このオプションを選択し、関連するドロップダウンリストから一致基準（[is] または [isn't]）を選択して、照合するエンドポイント評価（OPSWAT）のバージョンを入力します。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル

ファイル基準プリログイン チェックにより、関連付けられたプリログイン ポリシーに対して適格となる条件として、特定のファイルが存在すること、または存在しないことを指定できます。たとえば、ファイル プリログイン チェックを使用して、プリログイン ポリシーの割り当

て前に、企業ファイルが必ず存在すること、あるいは悪意のあるソフトウェアを含む1つ以上のピアツーピア ファイル共有プログラムが存在してはならないことを指定できます。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [ファイル（File）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *412 : [DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスファイル*

要素	説明
基準	選択基準として [File] が表示されます。
タイプ（Type）	このエンドポイント属性が、セッションの確立中にダイナミック アクセス ポリシーを選択および適用するために設定した基準と一致する必要があるか、または一致しない必要があるかを指定します。
エンドポイント ID（Endpoint ID）	ファイルのエンドポイントを識別する文字列を選択します。ダイナミック アクセス ポリシーでは、この ID を使用して、ダイナミック アクセス ポリシー選択の Cisco Secure Desktop ホスト スキャン属性を照合します。この属性を設定する前に、[Host Scan] を設定する必要があります。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。
ファイル名	ファイル名を指定します。

要素	説明
Last Update	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く（[<]）実行するか、遅く（[>]）実行するかを指定できます。
チェックサム（Checksum）	DAP レコードのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 このチェックボックスをオンにして、ファイルを認証するようにチェックサムを指定し、次に、0x で始まる 16 進形式でチェックサムを入力します。 バージョン 4.7 以降、Security Manager には、ファイルの CRC32 チェックサムを計算するユーティリティが用意されています。[CRC32チェックサムの計算（Compute CRC32 Checksum）] ボタンをクリックして、[チェックサムの計算（Compute Checksum）] ダイアログ ボックスを開きます。[参照（Browse）] をクリックしてファイルブラウザを開き、必要なファイルを選択して [計算（Compute）] ボタンをクリックします。ファイルの CRC32 チェックサムが計算され、[チェックサム（Checksum）] フィールドに入力されます。 （注） Compute CRC32 チェックサムユーティリティでは、クライアント側の参照のみがサポートされています。デフォルトでは、クライアント側の参照が有効になっています。これを無効にすると、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [デスクトップのカスタマイズ（Customize Desktop）] を選択します。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [NAC]

NAC は、エンドポイント準拠および脆弱性チェックをネットワークへの実稼働アクセスの条件として実行することにより、ワーム、ウイルス、および不正なアプリケーションの侵入や感染からエンタープライズ ネットワークを保護します。これらのチェックをポスチャ検証と呼びます。イントラネット上の脆弱なホストにアクセスする前に、ポスチャ検証を設定して、AnyConnect またはクライアントレス SSL VPN セッションを使用するホスト上のアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防御ソフトウェアが最新の状態であることを確認できます。ポスチャ検証の一部として、リモート ホストで実行されているアプリケーションが最新のパッチで更新されているか検証することもできます。NAC は、ユーザ認証およびトンネルの設定の完了後に行われます。自動ネットワーク ポリシー実施が適用されないホスト（ホーム PC など）からエンタープライズ ネットワークを保護する場合は、NAC が特に有用です。セキュリティ アプライアンスは、Extensible Authentication Protocol（EAP）over UDP（EAPoUDP）メッセージングを使用して、リモート ホストのポスチャを検証します。

エンドポイントとセキュリティアプライアンスの間にトンネルが確立されると、ポスチャ検証がトリガーされます。クライアントがポスチャ検証要求に応答しない場合に、クライアントの IP アドレスを任意指定の監査サーバに渡すように、セキュリティ アプライアンスを設定できます。監査サーバ（Trend サーバなど）では、ホスト IP アドレスを使用して、ホストに対して直接チャレンジを行い、ホストのヘルスを評価します。たとえば、ホストに対してチャレンジを行い、そのウイルス チェック ソフトウェアがアクティブで最新の状態かどうかを判断します。監査サーバは、リモート ホストとの対話を完了すると、リモート ホストのヘルスを示すトークンをポスチャ検証サーバに渡します。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [NAC] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *413 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスの *[NAC]*

要素	説明
基準	選択基準として [NAC] が表示されます。
ポスチャ ステータス	ドロップダウンリストから一致基準（[は（is）] など）を選択して、ACS から受け取ったポスチャ トークン文字列を入力します。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）]

プリログイン評価には、VPN 接続の確立を試行する OS のチェックが含まれます。ただし、ユーザが接続を試行すると、OS プリログインチェックを挿入したかどうかに関係なく、Cisco Secure Desktop によって OS がチェックされます。

接続に割り当てられているプリログイン ポリシーの Secure Desktop（Secure Session）がイネーブルになっており、かつ、リモート PC で Microsoft Windows XP または Windows 2000 が実行されている場合は、OS プリログイン チェックを挿入したかどうかに関係なく、Secure Session がインストールされます。プリログイン ポリシーの Secure Desktop がイネーブルになっており、かつ、オペレーティング システムが Microsoft Windows Vista、Mac OS X 10.4、または Linux の場合は、代わりにキャッシュ クリーナが実行されます。このため、キャッシュ クリーナの設定が、Secure Desktop またはキャッシュ クリーナをインストールするように設定したプリログイン ポリシーに対して適切であることを確認する必要があります。Cisco Secure Desktop により OS がチェックされますが、プリログイン ポリシーを適用して OS ごとに後続のチェックを分離するための条件として OS プリログイン チェックを挿入することもできます。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [オペレーティング システム（Operating System）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *414 : [DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [オペレーティングシステム（Operating System）]*

要素	説明
基準	選択基準として [Operating System] が表示されます。
OS Version	チェックボックスをオンにし、ドロップダウンリストから一致基準（[is] など）を選択して、リストから OS バージョンを選択します。iPhone および同様のデバイスには、[Apple Plugin] を選択します。

要素	説明
サービス パック	チェックボックスをオンにし、ドロップダウンリストから一致基準（[is] など）を選択して、オペレーティングシステムのサービスパックを選択します。

[DAP エントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスの [パーソナルファイアウォール（Personal Firewall）]

Cisco Secure Desktop インターフェイスで [Host Scan] をクリックして、エンドポイント評価をイネーブルにします。エンドポイント評価は、リモート コンピュータで実行されているパーソナル ファイアウォールのスキャンです。一部を除くほとんどのパーソナル ファイアウォール プログラムでは、アクティブなスキャンがサポートされています。つまり、このようなスキャンでは、プログラムがメモリに常駐するため、常に動作中になります。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

重要 パーソナルファイアウォールの基準は、Host Scan バージョン 4.6 より前の場合は **FW**、バージョン 4.6 以降の場合は **PFW** として示されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [AAA属性Cisco（AAA Attributes Cisco）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *415: [DAP* エントリの追加/編集（*Add/Edit DAP Entry*）*]* ダイアログボックスの *[*パーソナルファイアウォール（*Personal Firewall*）*]*

要素	説明
基準	選択基準として [Personal Firewall] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたパーソナルファイアウォールがリモート PC 上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：設定するプリログインポリシーに適合させるために、指定されたパーソナルファイアウォールがリモート PC 上に存在し、有効になっているかどうかを選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたパーソナルファイアウォールがリモート PC 上に単に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	このエンドポイント属性とそのすべての設定がリモート PC で使用可能である必要があることを選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	このエンドポイント属性とそのすべての設定がリモート PC で使用可能である必要があることを選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、エンドポイント属性をそのバージョンと等しくするかどうかを指定します。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスポリシー

Windows ロケーションを使用すると、クライアントとバーチャル プライベート ネットワークとの接続方法を判断して適宜に保護できます。たとえば、NAT デバイスの背後にある 10.x.x.x ネットワークの職場 LAN 内から接続しているクライアントが、機密情報を公開するリスクはほとんどないと考えられます。これらのクライアントに対しては、10.x.x.x ネットワーク上の IP アドレスで指定された Work という名前の Cisco Secure Desktop Windows ロケーションを設定し、このロケーションに対してキャッシュ クリーナと Secure Desktop 機能の両方をディセー

ブルにします。Cisco Secure Desktop は、[Windows Location Settings] ウィンドウのリスト内の順序でロケーションをチェックし、最初に一致したロケーション定義に基づいてクライアント PC に権限を付与します。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。基準として [ポリシー（Policy）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *416 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスポリシー

要素	説明
基準	選択基準として [Policy] が表示されます。
参照先	ドロップダウンリストから一致基準（[is] など）を選択して、リストから Cisco Secure Desktop Microsoft Windows ロケーションプロファイルを選択します。Cisco Secure Desktop Manager で設定されたすべてのロケーションは、このリストに表示されます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックスの [プロセス（Process）]

基本ホスト スキャンの一部となる一連のプロセス名を指定できます。ホスト スキャンは、基本ホスト スキャンとエンドポイント評価または拡張エンドポイント評価で構成され、プリログイン評価の終了後、ダイナミック アクセス ポリシーの割り当ての前に行われます。基本ホスト スキャンに続いて、セキュリティ アプライアンスはログイン クレデンシャル、ホスト スキャン結果、プリログイン ポリシー、および DAP の割り当て用に設定したその他の基準を使用します。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [プロセス（Process）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *417 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスの *[*プロセス（*Process*）*]*

要素	説明
基準	選択基準として [Process] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [一致する（Matches）]：指定されたプロセスがリモート PC 上に存在することだけを、設定するプリログインポリシーと一致していることの十分条件とする場合は、これを選択します。 • [一致しない（Doesn't Match）]：指定されたプロセスがリモート PC 上に存在しないことを、設定するプリログインポリシーに一致していることの十分条件とする場合は、これを選択します。
エンドポイント ID（Endpoint ID）	ファイル、プロセス、またはレジストリ エントリのエンドポイントを示す文字列。ダイナミック アクセス ポリシーでは、この ID を使用して、ダイナミック アクセス ポリシー選択の Cisco Secure Desktop ホスト スキャン属性を照合します。この属性を設定する前に、[Host Scan] を設定する必要があります。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。

要素	説明
パス（Path）	チェックボックスをオンにし、ドロップダウンリストから一致基準（[次に一致する（is）] など）を選択して、プロセスの名前を入力します。これを Microsoft Windows で表示するには、[Windows Task Manager] ウィンドウを開いて [Processes] タブをクリックします。 この属性を設定する前に、[Host Scan] を設定します。[Host Scan] を設定すると、設定がこのペインに表示されるため、DAP を設定する場合にこのエントリをエンドポイント属性として割り当てるとき、この設定を選択して同じインデックスを指定できます。これにより、入力や構文のエラーを減少させることができます。

[DAPエントリの追加/編集（Add/Edit DAP Entry）] ダイアログボックスのレジストリ

レジストリ キー スキャンは、Microsoft Windows オペレーティング システムを実行しているコンピュータにだけ適用されます。基本ホスト スキャンでは、コンピュータで Mac OS または Linux が実行されている場合にレジストリ キー スキャンを無視します。

（注） 重複するエントリは許可されません。AAA またはエンドポイント属性のないダイナミック アクセス ポリシーを設定する場合は、すべての選択基準が満たされるため、セキュリティ アプライアンスでは常にそのポリシーが選択されます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [レジストリ（Registry）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *418 : [DAP*エントリの追加（*Add DAP Entry*）*]/[DAP*エントリの編集（*Edit DAP Entry*）*]* ダイアログボックスのレジストリ

要素	説明
基準	選択基準として [Registry] が表示されます。
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [一致する（Matches）]：指定されたレジストリキーがリモート PC 上に存在することだけを、設定するプリログインポリシーと一致していることの十分条件とする場合は、これを選択します。たとえば、プリログインポリシーを割り当てるための基準と一致する条件として、HKEY_LOCAL_MACHINE\SOFTWARE\<Protective_Software> というレジストリ キーが存在することを要求する場合は、このオプションを選択します。 • [一致しない（Doesn't Match）]：指定されたレジストリキーがリモート PC 上に存在しないことを、設定するプリログインポリシーに一致していることの十分条件とする場合は、これを選択します。たとえば、プリログインポリシーを割り当てるための基準と一致する条件として、HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\<Evil_SpyWare> というレジストリ キーが存在しないことを要求する場合は、このオプションを選択します。
エンドポイント ID（Endpoint ID）	ファイル、プロセス、またはレジストリエントリのエンドポイントを示す文字列。ダイナミック アクセス ポリシーでは、この ID を使用して、ダイナミック アクセス ポリシー選択の Cisco Secure Desktop ホスト スキャン属性を照合します。この属性を設定する前に、[Host Scan] を設定する必要があります。[Host Scan] を設定した場合は設定がこのペインに表示されるため、設定を選択して、入力エラーまたは構文エラーの可能性を低減できます。
Registry Name	レジストリ名を説明するテキストをリストから選択します。
値	リストから [dword] または [string] の値を選択し、一致基準（等しいか等しくないか）を選択します。次に、リモート PC 上のレジストリキーの dword または文字列の値と比較する 10 進数または文字列を入力します。 （注） 「DWORD」は、[レジストリ基準の追加（Add Registry Criterion）]/[レジストリ基準の編集（Edit Registry Criterion）] ダイアログボックス内の属性を参照します。「Dword」は、レジストリキーに表示される属性を参照します。Windows コマンドラインからアクセスできる regedit アプリケーションを使用して、レジストリ キーの Dword 値を確認します。または、このアプリケーションを使用して、Dword 値をレジストリ キーに追加して、設定する要件を満たします。
Ignore Case	選択すると、レジストリエントリ内に文字列が含まれている場合に、大文字と小文字の違いが無視されます。

[DAPエントリの追加（Add DAP Entry）]/[DAPエントリの編集（Edit DAP Entry）] ダイアログボックス > [マルウェア対策（Anti-Malware）]

Host Scan バージョン 4.6 以降では、ウイルス対策（AV）、スパイウェア対策（AS）、およびファイアウォール（FW）基準がサポートされなくなりました。ただし、代わりに 2 つの新しい基準であるマルウェア対策（AM）とパーソナルファイアウォール（PFW）が追加されており、Host Scan の設定時に使用できます。

Cisco Secure Desktop インターフェイスで [Host Scan] をクリックして、リモートコンピュータで実行されているパーソナルファイアウォールのスキャンであるエンドポイント評価を有効にします。プリログインポリシーおよび Host Scan のオプションの設定に続いて、Host Scan 結果の 1 つまたは任意の組み合わせに関する一致を設定して、ユーザーログイン後のダイナミックアクセス ポリシーに割り当てることができます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [マルウェア対策（Anti-Malware）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *419 : [DAP*エントリの追加（*Add DAP Entry***）*]/[DAP*エントリの編集（***Edit DAP Entry***）*]* ダイアログボックス > *[*マルウェア対策（***Anti-Malware***）*]***

要素	説明
基準	選択基準として [スパイウェア対策（Anti-Spyware）] が表示されます。

要素	説明
タイプ（Type）	次のいずれかのオプションを選択し、関連する値を割り当てます。 • [未インストール（Not Installed）]：指定されたマルウェア対策がリモート PC 上にないことを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。 • [インストール済みで有効（Installed and enabled）]：設定するプリログインポリシーと一致させるために、名前付きマルウェア対策がリモート PC 上に存在し、有効になっている必要があるかどうかを選択します。 • [インストール済みで無効（Installed and disabled）]：指定されたマルウェア対策がリモート PC 上に存在していることを、設定するプリログインポリシーに一致するための十分条件とする場合に選択します。
ベンダー名（Vendor Name）	アプリケーションベンダーを説明するテキストをリストから選択します。
製品 ID	リストから選択したベンダーによってサポートされる製品の固有識別情報を選択します。
製品の説明	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 チェックボックスをオンにし、リストから製品の説明を選択します。
バージョン	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 アプリケーションのバージョンを識別し、エンドポイント属性をそのバージョンに対して次のいずれかにするかどうかを指定します。 • **等しくない** • **等しい** • **より少ない** • **より大きい** • **以下** • **以上**
Last Update	ダイナミック アクセス ポリシーのエンドポイント属性と一致する基準を選択した場合にだけ使用可能です。 最後の更新からの日数を指定します。更新を、ここで入力した日数よりも早く実行するか、遅く実行するかを指定できます。

[DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）]

DAP マルチ証明書認証基準により、関連付けられたプリログイン ポリシー チェック中に使用できる特定のデバイス情報を提供できます。Cisco Security Manager は、リモート VPN ユーザーを認証するための 2 つの証明書をサポートしています。証明書には、サブジェクト、発行者、サブジェクト代替名、シリアル番号、および証明書ストアの 1 つ以上の属性を指定できます。

（注） 証明書オプション以外の DAP エントリを変更できます。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開いて [メイン（Main）] タブを選択し、[作成（Create）] をクリックするか、テーブルでダイナミック アクセス ポリシーを選択して [編集（Edit）] をクリックします。[Add DAP Entry]/[Edit DAP Entry] ダイアログボックスが表示されます。[基準（Criterion）] として [マルチ証明書認証（Multiple Certificate Authentication）] を選択します。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *420 : [DAP エントリの追加（Add DAP Entry）]/[DAP エントリの編集（Edit DAP Entry）] ダイアログボックスの [マルチ証明書認証（Multiple Certificate Authentication）]*

要素	説明
基準	選択基準として [マルチ証明書認証（Multiple Certificate Authentication）] が表示されます。
証明書	4.13 ではマルチ証明書は 2 つの証明書による認証を指します。次のいずれかのオプションを選択し、関連する属性を割り当てます。 • [証明書 1（Cert1）]：設定しているプリログインポリシーに一致する証明書 1 の詳細を提供する場合に選択します。 • [証明書 2（Cert2）]：設定しているプリログインポリシーに一致する証明書 2 の詳細を提供する場合に選択します。 （注） 証明書オプションを編集/変更することはできません。

要素	説明
Subject	ドロップダウンリストから、証明書のサブジェクト名からドメイン名（DN）属性フィールドを選択します。 • dnq：ドメイン名修飾子 • fulldn：完全なサブジェクト名 • ser：シリアル番号 • cn：一般名 • i：イニシャル • ou：組織ユニット • sp：州/都道府県 • o：組織 • n：名前 • sn：姓 • t：役職 • uid：ユーザー識別子 • genq：世代識別子 • c：国 • l：市町村名 • gn：名 • ea：電子メールアドレス 隣のテキストボックスに、選択したサブジェクトの DAP エントリ値を入力します。 （注） テキストボックスを空白のままにすると、保存時にエラーメッセージが表示されます。

要素	説明
発行元（Issuer）	ドロップダウンリストから、証明書の発行元名からドメイン名（DN）属性フィールドを選択します。 • dnq：ドメイン名修飾子 • fulldn：完全な発行元名 • ser：シリアル番号 • cn：一般名 • i：イニシャル • ou：組織ユニット • sp：都道府県 • o：組織 • n：名前 • sn：姓 • t：役職 • uid：ユーザー識別子 • genq：世代識別子 • c：国 • l：局所性 • gn：名 • ea：電子メールアドレス 隣のテキストボックスに、選択した発行元の DAP エントリ値を入力します。 （注） テキストボックスを空白のままにすると、保存時にエラーメッセージが表示されます。
Subject Alternate Name	シリアル番号を設定するには、このドロップダウンリストから [upn] を選択します。隣のテキストボックスに、証明書の [サブジェクト代替名（Subject Alt Name）] フィールドからのユーザープリンシパル名を入力します。
シリアル番号	照合する証明書のシリアル番号を入力します。この値は 16 進数（0 ～ 9 および A ～ F の組み合わせ）である必要があります。 （注） 16 進数以外を入力すると、保存時にエラーメッセージが表示されます。

要素	説明
証明書のストア	認証用の証明書がある関連ストアを選択します。 • [なし（None）]：証明書のタイプが分からない場合に選択します。 • [マシン（Machine）]：証明書がマシンに関連する（特権プロセスでのみアクセス可能）場合に選択します。証明書 1 と証明書 2 の両方にこのオプションを選択することはできません。 • [ユーザー（User）]：証明書がユーザーログインに関連する（ログインしたユーザーが所有するプロセスでのみアクセス可能）場合に選択します。 （注） Windows の場合、ストアは a）1 つのマシンと 1 人のユーザーまたは b）2 人のユーザーです。Windows 以外のプラットフォームの場合、常に 2 つのユーザー証明書が表示されます。

[論理的な操作（Logical Operators）] タブ

[ダイナミックアクセスポリシーの追加（Add Dynamic Access Policy）]/[ダイナミックアクセスポリシーの編集（Edit Dynamic Access Policy）] ダイアログボックスの [論理的な操作（Logical Operators）] タブを使用して、AAA の複数のインスタンスと、[DAPエントリ（DAP Entry）] ダイアログボックスで定義したエンドポイント属性の各タイプを設定します。このタブで、エンドポイント属性または AAA 属性の各タイプについて、タイプのインスタンスの 1 つのみを必要とするか（[Match Any] = OR）か、またはタイプのすべてのインスタンス（[Match All] = AND）を必要とするかを設定します。

- エンドポイント カテゴリの 1 つのインスタンスだけを設定する場合、値を設定する必要はありません。
- エンドポイント属性によっては、複数のインスタンスを設定しても有用でない場合があります。たとえば、複数の OS を実行するユーザがいない場合などです。
- 各エンドポイント タイプ内に [Match Any]/[Match All] 操作を設定するとします。この場合、セキュリティ アプライアンスは、エンドポイント属性の各タイプを評価したあと、設定されたすべてのエンドポイントで論理 AND 演算を実行します。つまり、各ユーザは、AAA 属性だけでなく、設定したエンドポイントのすべての条件を満たす必要があります。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開き、[論理的な操作（Logical Operators）] タブをクリックします。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）

- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *421 : [ダイナミックアクセスポリシーの追加（Add Dynamic Access Policy）]/[ダイナミックアクセスポリシーの編集（Edit Dynamic Access Policy）] ダイアログボックスの [論理的な操作（Logical Operators）] タブ*

要素	説明
AAA	ダイナミック アクセス ポリシー内に AAA 属性を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：属性間に OR 関係を作成します。基準のいずれかに一致する属性が、フィルタに追加されます。セキュリティ アプライアンスは、属性のいずれか1つがすべての基準に一致していても、特定のユーザに対して、特定のセッションへのアクセスを許可します。 • [Match All]：属性間に AND 関係を作成します。セキュリティ アプライアンスは、属性がすべての基準に一致している場合にだけ、特定のユーザに対して、特定のセッションへのアクセスを許可します。 • [Match None]：属性間に NOT 関係を作成します。ダイナミック アクセス ポリシーは、セッションへのアクセスを許可するために、ユーザの属性のいずれも一致する必要がないことを指定します。
Anti-Spyware	エンドポイント属性として [Anti-Spyware] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：属性間に OR 関係を作成します。基準のいずれかのインスタンスに一致するポリシーが、ユーザの認可に使用されます。 • [Match All]：属性間に AND 関係を作成します。すべての基準に一致する属性だけが、ユーザの認可に使用されます。
ウイルス対策	エンドポイント属性として [Anti-Virus] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルス エンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。

要素	説明
Application	エンドポイント属性として [Application] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。
ファイル（File）	エンドポイント属性として [File] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。
Personal Firewall	パーソナルファイアウォールルールを使用すると、ファイアウォールが許可またはブロックするアプリケーションおよびポートを指定できます。エンドポイント属性として [Personal Firewall] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。
プロセス	エンドポイント属性として [Process] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルスエンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。

要素	説明
レジストリ	レジストリ キー スキャンは、Microsoft Windows オペレーティング システムを実行しているコンピュータにだけ適用されます。基本ホスト スキャンでは、コンピュータで Mac OS または Linux が実行されている場合にレジストリ キー スキャンを無視します。 エンドポイント属性として [Registry] を定義した場合は、次のいずれかのオプションを選択します。 • [Match Any]：ユーザ認可属性が、設定しているアンチウイルス エンドポイント属性のいずれかの値と一致する必要があることを設定します。 • [Match All]：ユーザ認可属性が、設定しているエンドポイント属性のすべての値と一致し、AAA 属性も満たす必要があることを設定します。

[Advanced Expressions] タブ

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックスの [Advanced Expressions] タブを使用して、ダイナミック アクセス ポリシーの追加属性を設定します。各タイプのエンドポイント属性の複数のインスタンスを設定できます。これは、LUA（www.lua.org）の知識を必要とする高度な機能であることに注意してください。

ナビゲーション パス

[Add Dynamic Access Policy]/[Edit Dynamic Access Policy] ダイアログボックス （1842 ページ）を開き、[拡張表現（Advanced Expressions）] タブをクリックします。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）

フィールド リファレンス

表 *422 : [ダイナミックアクセスポリシーの追加/編集（Add/Edit Dynamic Access Policy）] ダイアログボックス > [拡張表現（Advanced Expressions）] タブ*

要素	説明
Basic Expressions	このテキスト ボックスには、ダイナミック アクセス ポリシー内に設定したエンドポイント属性および AAA 属性に基づいて基本表現が入力されます。

要素	説明
[Relationship] ドロップダウン リスト	基本選択ルールと、このタブに入力した論理式の間の関係を指定します。つまり、新しい属性を、すでに設定されている AAA 属性およびエンドポイント属性に追加するか、それとも置き換えるかを指定します。次のオプションのいずれかを選択します。 • [基本AND拡張（Basic AND Advanced）]：基本表現と拡張表現の間に AND 関係を作成します。ダイナミック アクセス ポリシー内で定義されている基本表現と拡張表現の両方が、ユーザの認証中に考慮されます。 デフォルトでは、このオプションが選択されています。 • [基本OR拡張（Basic OR Advanced）]：基本表現と拡張表現の間に OR 関係を作成します。ダイナミック アクセス ポリシー内の基本表現または拡張表現のいずれかがユーザ ポリシーに一致すると、ユーザはセッションへのアクセスを許可されます。 • [基本のみ（Basic Only）]：DAP エントリ内に定義されている基本表現だけを使用して、セキュリティアプライアンスが特定のセッションに対するアクセスをユーザーに許可するかどうかが決定されます。 • [拡張のみ（Advanced Only）]：DAP エントリ内に定義されている拡張表現だけを使用して、SSL VPN セッションに対してユーザーが認可されます。
Advanced Expressions	1 つ以上の論理式を入力して、上記の [AAA] および [Endpoint] 領域で設定できない AAA 属性またはエンドポイント属性を設定します。 新しい AAA 選択属性またはエンドポイント選択属性（あるいはその両方）を定義するフリー形式の LUA テキストを入力します。ここで入力したテキストは、Security Manager によって検証されず、ダイナミック アクセス ポリシーの XML ファイルにコピーされるだけです。このテキストはセキュリティアプライアンスによって処理され、解析できない表現はすべて廃棄されます。

[Cisco Secure Desktop Manager Policy Editor] ダイアログボックス

[Cisco Secure Desktop Manager (CSDM) Policy Editor] ダイアログボックスを使用して、プリログイン ポリシーの設定、ユーザがセキュリティ アプライアンスとの接続を確立してからログイン クレデンシャルを入力するまでの間に実行されるチェックの指定、およびホスト スキャンの設定を実行できます。ASA デバイスでの CSD の設定の詳細については、ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）を参照してください。

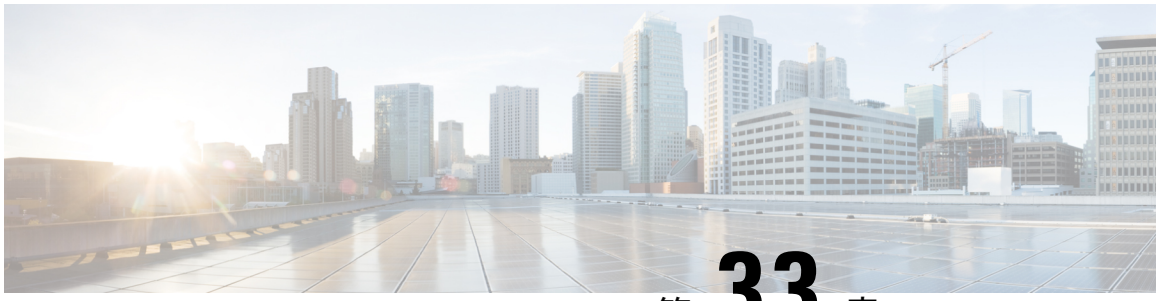
（注） Cisco Secure Desktop Manager Policy Editor は、独立したプログラムです。CSD の設定および CSD の機能については、https://www.cisco.com/c/ja_jp/products/index.html で入手できる資料を参照してください。具体的には、プリログイン ポリシーおよびホスト スキャンの設定に関する情報を参照してください。設定する CSD バージョンのコンフィギュレーション ガイドを選択してください。

ナビゲーション パス

[Dynamic Access] ページ（ASA） （1840 ページ）を開き、[Cisco Secure Desktop] セクションから [設定（Configure）] をクリックします（最初に CSD パッケージを指定する必要があります）。[CSDM Policy Editor] ダイアログボックスが表示されます。

関連項目

- DAP 属性について （1831 ページ）
- DAP 属性の設定 （1836 ページ）
- ダイナミック アクセス ポリシーの設定 （1829 ページ）



第 33 章

IOS および PIX 6.3 デバイスでのリモートアクセス VPN の管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

Cisco IOS ソフトウェアまたは PIX 6.3 を実行するデバイスのリモートアクセス IPsec、および IOS 12.4(6)T 以上のデバイス（PIX デバイスではありません）の SSL VPN を設定および管理できます。サポート対象の特定のデバイスモデルの詳細については、各リモート アクセス VPN テクノロジーでサポートされるデバイスについて （1665 ページ）を参照してください。

これらのリモートアクセス VPN の設定は、これらのデバイスタイプで同じです。ASA および PIX 7.0 以降のデバイスは、リモートアクセス VPN に異なる設定を使用します（ASA および PIX 7.0+ デバイスでのリモートアクセス VPN の管理 （1705 ページ）を参照）。

この章のトピックでは、IOS および PIX 6.3 デバイスに固有のポリシーを設定する方法を説明します。リモート アクセス VPN の詳細については、次のトピックを参照してください。

- リモート アクセス VPN について （1655 ページ）
- 各リモートアクセスVPNテクノロジーでサポートされるデバイスについて （1665ページ）
- リモート アクセス VPN ポリシーの検出 （1669 ページ）
- Remote Access VPN Configuration ウィザードの使用 （1671 ページ）
  - Remote Access VPN Configuration ウィザードを使用した IPSec VPN の作成（IOS および PIX 6.3 デバイス） （1703 ページ）
  - Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス） （1697 ページ）

この章は次のトピックで構成されています。

- IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要 （1892 ページ）

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）
- リモートアクセス VPN での高可用性の設定（IOS）（1904 ページ）
- ユーザ グループ ポリシーの設定（1906 ページ）
- SSL VPN ポリシーの設定（IOS）（1908 ページ）

IOS および PIX 6.3 デバイスのリモート アクセス VPN ポリシーの概要

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

IOS または PIX 6.3 デバイスでリモート アクセス VPN を設定する場合、設定する VPN のタイプに基づいて、次のポリシーを使用します。PIX 6.3 デバイスでは SSL VPN を設定できないことに注意してください。

- **IPsec および SSL リモート アクセス VPN の両方で使用されるポリシー**：
  - **グローバル設定**：リモートアクセス VPN のすべてのデバイスに適用されるグローバル設定を定義できます。グローバル設定には、Internet Key Exchange（IKE; インターネット キー交換）、IPsec、NAT、フラグメンテーションの定義などがあります。グローバル設定には、通常、ほとんどの状況に適用できるデフォルトが設定されています。そのため、グローバル設定ポリシーの設定はオプションです。デフォルト以外の動作が必要な場合だけ設定してください。詳細については、VPN グローバル設定（1517 ページ）を参照してください。
  - **Public Key Infrastructure**：Public Key Infrastructure（PKI）ポリシーを作成して、CA 証明書およびRSA キーの登録要求を生成し、キーや証明書を管理できます。Certification Authority（CA; 認証局）サーバは、これらの証明書要求を管理し、IPsec または SSL リモート アクセス VPN に接続するユーザに対して証明書を発行するために使用されます。詳細については、Public Key Infrastructure ポリシーについて （1544 ページ）および リモート アクセス VPN での公開キー インフラストラクチャ ポリシーの設定（1552 ページ）を参照してください。
- **リモート アクセス IPsec VPN だけで使用されるポリシー**：
  - **IKE プロポーザル**：インターネット キー エクスチェンジ（IKE）は、ISAKMP とも呼ばれ、2 台のホストで IPsec セキュリティ アソシエーションの構築方法を一致させるためのネゴシエーションプロトコルです。IKE は、IPsec ピアの認証、IPsec 暗号キーのネゴシエーションと配布、および IPsec Security Association（SA; セキュリティ アソシエーション）の自動確立に使用されます。IKE プロポーザル ポリシーは、IKE ネゴシエーションのフェーズ 1 の要件を定義するときに使用します。詳細については、IKE プロポーザルの設定 （1488 ページ）を参照してください。

- **IPsec プロポーザル（IOS/PIX 6.x）**：IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプト マップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。このポリシーは、IKE フェーズ 2 ネゴシエーションに使用されます。詳細については、リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）を参照してください。
- **高可用性**：Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブデバイスで構成された HA グループを作成することで、高可用性（HA）がサポートされます。詳細については、リモートアクセス VPN での高可用性の設定（IOS）（1904 ページ）を参照してください。
- **ユーザーグループ（IOS/PIX 6.x）**：ユーザーグループポリシーには、VPN へのユーザーアクセスおよびVPNの使用を決定する属性を指定します。詳細については、ユーザ グループ ポリシーの設定（1906 ページ）を参照してください。

- **リモート アクセス SSL VPN だけで使用されるポリシー**：
  - **SSL VPN**：SSL VPN ポリシーテーブルには、SSL VPN の仮想設定を定義するすべてのコンテキストが一覧表示されます。各コンテキストには、ゲートウェイ、ドメインまたは仮想ホスト名、およびユーザ グループ ポリシーが含まれます。詳細については、SSL VPN ポリシーの設定（IOS）（1908 ページ）を参照してください。

リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

ここでは、サーバーが Cisco IOS Software または PIX リリース 6.3 を使用している場合の、リモートアクセス VPN サーバーの IPsec プロポーザルを作成または編集する方法について説明します。

IPsec プロポーザルは、1 つ以上のクリプトマップのコレクションです。クリプトマップには、IPsec ルール、トランスフォーム セット、リモート ピア、および IPsec SA の定義に必要となる可能性のあるその他のパラメータを含め、IPsec Security Association（SA; セキュリティ アソシエーション）の設定に必要なすべてのコンポーネントが組み合わされています。

IPsec プロポーザルを設定する場合は、リモート アクセス クライアントがサーバに接続する外部インターフェイス、および VPN トンネル内のデータを保護する暗号化と認証のアルゴリズムを定義する必要があります。また、（ローカル サーバまたは外部 AAA サーバで）グループ

ポリシーの検索順序を定義するグループ認可（グループ ポリシー ルックアップ）方式、およびユーザ アカウントの検索順序を定義するユーザ認証（Xauth）方式も選択できます。

IPsec トンネルの概念の詳細については、IPsec プロポーザルについて （1499 ページ）を参照してください。

IPsec プロポーザルを作成または編集する場合は、次を設定することもできます。

- Catalyst 6500/7600 デバイス上の VPN Services Module（VPNSM; VPN サービス モジュール）インターフェイス IPsec VPN Shared Port Adapter（VPN SPA; VPN 共有ポート アダプタ）（[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス（1898 ページ）を参照）
- 7600 デバイスを除く、Cisco IOS ソフトウェアバージョン 12.4(2)T 以降を実行している IOS ルータ上の動的仮想インターフェイス。詳細については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （1900 ページ）を参照してください。
- ルータまたは Catalyst 6500/7600 デバイスの VRF 対応 IPsec（リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （1900 ページ）を参照）。

関連項目

- VRF 対応 IPsec について （1398 ページ）
- [VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス（1898 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPsec Proposal] ページが開き、VPN エンドポイント、IPsec トランスフォーム セット、および逆ルート注入がプロポーザルで設定されているかどうかなど、設定されているプロポーザルが一覧表示されます。デフォルトの表示に他の列を追加して、AAA、VRF、および dVTI の設定を表示できます。

ステップ 2 次のいずれかを実行します。

- 新しい IPsec プロポーザルを追加するには、[行の追加（Add Row）]（+）ボタンをクリックして、[IPsec Proposal Editor] ダイアログボックスに入力します。使用可能なオプションの詳細については、IPsec Proposal Editor（IOS、PIX 6.3 デバイス） （1895 ページ）を参照してください。

- 既存のプロポーザルを編集するには、プロポーザルを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- プロポーザルを削除するには、そのプロポーザルを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

IPsec Proposal Editor（IOS、PIX 6.3 デバイス）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および PIX の機能をサポートしていますが、拡張機能はサポートしていません。

[IPsec Proposal Editor] を使用して、Catalyst 6500/7600 など、リモート アクセス VPN の IOS または PIX 6.3 デバイスの IPsec プロポーザルを作成または編集します。エディタには、[全般（General）] と [動的VTI/VRF対応IPsec（Dynamic VTI/VRF Aware IPsec）] の 2 つのタブがあります。このトピックでは、[全般（General）] タブの基本設定について説明します。[Dynamic VTI/VRF Aware IPsec] 設定の説明については、リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス） （1900 ページ）を参照してください。

このダイアログボックスの要素は、選択したデバイスによって異なります。次の表に、Cisco IOS ルータ、Catalyst 6500/7600、または PIX 6.3 デバイスを選択したときの [IPsec Proposal Editor] ダイアログボックス内の [General] タブの要素を示します。

（注） PIX 7.0+ または ASA デバイスを選択したときのダイアログボックス内の要素の詳細については、[IPsec Proposal Editor]（ASA、PIX 7.0+ デバイス） （1761 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。
- （ポリシービュー）ポリシータイプセレクタから、**[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [IPsecプロポーザル（IOS/PIX 6.x）（IPsec Proposal (IOS/PIX 6.x)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。[Add Row]（+）または [Edit Row]（鉛筆）ボタンをクリックします。

関連項目

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）

- IPsec プロポーザルについて （1499 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）
- AAA サーバ グループ オブジェクトの作成 （349 ページ）

フィールド リファレンス

表 *423 : [IPsec Proposal Editor]* の *[General]* タブ（*IOS* および *PIX 6.3* デバイス）

要素	説明
外部インターフェイス	（注） 選択したデバイスが IOS ルータの場合にかぎり使用できます。 リモート アクセス クライアントがサーバへの接続に使用する外部インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックして選択するか、または新しいオブジェクトを作成します。
Inside VLAN	（注） 選択したデバイスが Catalyst 6500/7600 ルータの場合にだけ使用可能です。 VPN Services Module（VPNSM; VPN サービス モジュール）または VPN SPA または VSPA への Inside インターフェイスとして機能する内部 VLAN。[選択（Select）] をクリックし、[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス （1898 ページ）の説明に従って内部 VLAN を設定します。
IKEv1 トランスフォームセット	トンネル ポリシーで使用するトランスフォーム セット。トランスフォーム セットは、トンネル内のトラフィックの確立に使用される認証アルゴリズムおよび暗号化アルゴリズムを指定します。最大 9 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要（1501 ページ）を参照してください。 選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォーム セットが使用されます。 [選択（Select）] をクリックして、トポロジで使用する IPsec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクト リストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。

要素	説明
リバース ルート インジェクション（Reverse Route Injection）	リバース ルート インジェクション（RRI）により、スタティック ルートは、リモート トンネル エンドポイントで保護されているネットワークとホストのルーティング プロセスに自動的に挿入されます。詳細については、逆ルート注入について （1503 ページ）を参照してください。 次のいずれかのオプションを選択して、クリプト マップで RRI を設定します。 • [なし（None]）：クリプトマップで RRI の設定を無効にします。 • [標準（Standard）]：クリプトマップのアクセス制御リスト（ACL）で定義されている宛先情報に基づいて、ルートが作成されます。これがデフォルトのオプションです。 • [リモートピア（Remote Peer）]：リモートエンドポイント用に1つ、クリプトマップが適用されるインターフェイス経由でのリモートエンドポイントへのルート再帰用に 1 つ、合計 2 つのルートを作成します。 • [リモートピアIP（Remote Peer IP）]：アドレスをリモート VPN デバイスへの明示的なネクストホップとして指定します。IP アドレス、またはアドレスを指定するネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）]をクリックして、リストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） ネットワークまたはホストオブジェクトを使用する場合は、オブジェクトで [デバイスごとの値のオーバーライドを許可（Allow Value Override per Device）] オプションを選択し、必要に応じて、このオブジェクトを使用する特定のデバイスの IP アドレスをオーバーライドできます。
Group Policy Lookup/AAA Authorization Method	グループ ポリシーを検索する順序を定義するために使用される AAA 認可方式リスト。グループ ポリシーは、ローカル サーバまたは外部 AAA サーバ上に設定できます。リモート ユーザはグループ化され、リモート クライアントから VPN サーバに接続が正常に確立されたときに、その特定のユーザ グループのグループ ポリシーがユーザ グループに属するすべてのクライアントにプッシュされます。 [選択（Select）]をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。

要素	説明
User Authentication (Xauth)/AAA Authentication Method	ユーザ アカウントの検索順序を定義する AAA または Xauth ユーザ認証方式。 Xauth では、すべての Cisco IOS ソフトウェア AAA 認証方式で、IKE 認証フェーズ 1 の交換後に別のフェーズでユーザ認証を実行できます。 [選択（Select）] をクリックすると、使用可能なすべての AAA グループサーバーを表示したダイアログボックスが開き、そこで、AAA グループ サーバー オブジェクトを作成できます。該当する項目をすべて選択し、上矢印ボタンと下矢印ボタンを使用してプライオリティ順に並べ替えます。

[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックス

（注） このダイアログボックスは、選択したデバイスが Catalyst 6500/7600 の場合にだけ使用可能です。

[VPNSM/VPN SPA/VSPA設定（VPNSM/VPN SPA/VSPA Settings）] ダイアログボックスを使用して、Catalyst 6500/7600 デバイスで VPN Services Module（VPNSM; VPN サービスモジュール）、VPN Shared Port Adapter（VPN; 共有ポートアダプタ）、または Cisco VPN Service Port Adapter（VSPA; VPN サービスポートアダプタ）を構成するための設定を指定します。

注記

- 設定を定義する前に、Catalyst 6500/7600 デバイスを Cisco Security Manager インベントリにインポートし、そのインターフェイスを検出する必要があります。詳細については、VPNSM または VPN SPA/VSPA エンドポイントの設定 （1436 ページ）を参照してください。
- デバイスで VRF 対応 IPsec を使用して VPNSM または VPN SPA を設定する前に、VRF 対応 IPsec を使用する IPsec プロポーザルと、VRF 対応 IPsec を使用しない IPsec プロポーザルがデバイスで設定されていないことを確認してください。

ナビゲーション パス

[IPsecプロポーザルエディタ（IPsec Proposal Editor）] ダイアログボックス（Catalyst 6500/7600 デバイスの場合）の [全般（General）] タブで、[内部VLAN（Inside VLAN）] フィールドの横にある [選択（Select）] をクリックします。IPsec プロポーザルエディタを開く方法の詳細については、IPsec Proposal Editor（IOS、PIX 6.3 デバイス） （1895 ページ）を参照してください。

関連項目

- インターフェイス ロール オブジェクトの作成 （383 ページ）

フィールド リファレンス

表 *424 : [VPNSM/VPN SPA/VSPA*設定（*VPNSM/VPN SPA/VSPA Settings*）] ダイアログボックス

要素	説明
Inside VLAN	必要なクリプト マップが適用される、VPNSM、VPN SPA または VSPA への Inside インターフェイスとして機能する内部 VLAN。[VLAN ID] を入力します。あるいは、[選択（Select）] をクリックして VLAN を選択するか、または新しいインターフェイス ロール オブジェクトを作成して VLAN を識別します。
スロット サブスロット	VPNSM または VPNSPA/VSPA のスロット位置を指定する番号です。VPNSPA/VSPA を設定する場合は、サブスロット番号も必要です。 （注） VPNSM を設定している場合は、0 を選択します。
External Port	内部 VLAN に接続する外部ポートまたは VLAN。VLAN またはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択します。内部 VLAN に選択したものとは異なるインターフェイスまたはインターフェイス ロールを選択する必要があります。 （注） VRF 対応 IPsec がデバイスに設定されている場合は、外部ポートまたは VLAN に IP アドレスが必要です。VRF 対応 IPsec が設定されていない場合は、外部ポートまたは VLAN に IP アドレスを含めないでください。
Enable Failover Blade	シャーシ内のハイ アベイラビリティを確保するために、フェールオーバー VPNSM または VPNSPA/VSPA ブレードを設定するかどうかを指定します。 （注） 同じデバイスで VPNSM ブレードと VPNSPA/VSPA ブレードをプライマリ ブレードおよびフェールオーバー ブレードとして使用することはできません。 次のように、フェールオーバー ブレードを指定します。 • [スロット（Slot）] : VPNSM ブレードまたは VPNSPA/VSPA ブレードの位置を特定するスロット番号です。 • [サブスロット（Subslot）] : VPNSPA/VSPA を設定している場合は、フェールオーバー VPN SPA ブレードがインストールされているサブスロットの番号を選択します。 （注） VPNSM を設定している場合は、0 を選択します。

リモートアクセス VPN での Dynamic VTI/VRF Aware IPsec の設定（IOS デバイス）

（注） [Dynamic VTI/VRF Aware IPsec] タブは、選択したデバイスが Cisco IOS ルータまたは Catalyst 6500/7600 の場合にかぎり使用可能です。

[IPsec Proposal Editor] の [Dynamic VTI/VRF Aware IPsec] タブを使用して、（Cisco IOS ルータまたは Catalyst 6500/7600 デバイスで）リモート アクセス VPN の [VRF Aware IPsec]、または（Cisco IOS ルータで）ダイナミック仮想インターフェイス、あるいはその両方を設定します。

IOS デバイスでは、ダイナミック Virtual Template Interface（VTI; 仮想テンプレート インターフェイス）を使用できます。このインターフェイスは、リモート アクセス VPN に非常に安全でスケーラブルな接続を提供し、ダイナミック クリプト マップおよびダイナミック ハブアンドスポーク方式に代わってトンネルを確立します。ダイナミック VTI は、サーバ設定とリモート設定の両方に使用できます。トンネルにより、各 VPN セッションに対して、仮想アクセス インターフェイスがオンデマンドで個別に提供されます。仮想アクセスインターフェイスの設定は、仮想テンプレート設定から複製されます。仮想テンプレート設定には、IPsec 設定および仮想テンプレート インターフェイスに設定されたすべての機能が含まれています。ダイナミック VTI によって IP アドレスの使用が効率的になり、セキュアな接続が提供されます。それらによって、動的にダウンロード可能な、グループごとおよびユーザーごとのポリシーを RADIUS サーバー上で設定できます。VRF がインターフェイスに設定されるため、VRF 対応 IPsec の展開はダイナミック VTI によって簡素化されます。

この機能をイネーブルにすると、リモート アクセス VPN 内の選択デバイスの仮想テンプレート インターフェイスが Security Manager によって暗黙的に作成されます。必要となる作業は、仮想テンプレート インターフェイスとして使用されるサーバの IP アドレスの指定、または既存のループバック インターフェイスの使用だけです。仮想テンプレートインターフェイスは、リモートクライアントで IP アドレスなしで作成されます。

注記

- ダイナミック VTI を設定できるのは、Cisco IOS Release 12.4(2)T 以降が稼働しているルータだけです（7600 デバイスを除く）。
- ダイナミック VTI は、VRF 対応 IPsec が設定されているかどうかにかかわらず設定できます。VRF 対応 IPsec の詳細については、VRF 対応 IPsec について （1398 ページ）を参照してください。
- また、ダイナミック VTI は、サイト間 Easy VPN トポロジでも設定できます。詳細については、Easy VPN とダイナミック仮想トンネル インターフェイス （1601 ページ）を参照してください。

ナビゲーション パス

[IPsecプロポーザルエディタ（IPsec Proposal Editor）] ダイアログボックス（IOS ルータおよび Catalyst 6500/7600 デバイス）で、[ダイナミック VTI/VRF 対応 IPsec（Dynamic VTI/VRF Aware IPsec）] タブをクリックします。詳細については、IPsec Proposal Editor（IOS、PIX 6.3 デバイス）（1895 ページ）を参照してください。

関連項目

- リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）

フィールド リファレンス

表 *425 : IPsec* プロポーザルエディタの *[ダイナミック VTI/VRF* 対応 *IPsec*（*Dynamic VTI/VRF Aware IPsec*）*]* タブ

要素	説明
Enable Dynamic VTI	選択すると、Security Manager は IOS ルータ上にダイナミック仮想テンプレート インターフェイスを暗黙的に作成できます。 （注） ダイナミック VTI は、Cisco IOS Release 12.4(2)T 以降を実行している IOS ルータ（7600 デバイスを除く）でだけ設定できます。デバイスがダイナミック VTI をサポートしていない場合、オプションはグレー表示されます。
Enable VRF Settings	選択すると、選択済みのハブアンドスポーク トポロジに対してデバイスで VRF を設定できます。 （注） VPN トポロジにすでに定義されている VRF 設定を削除するには、このチェックボックスをオフにします。
ユーザー グループ	リモート アクセス VPN サーバを設定する場合、リモート クライアントがデバイスに接続できるように、リモートクライアントのグループ名を、VPN サーバで設定されているユーザ グループ オブジェクトと同じにする必要があります。 デバイスに関連付けられているユーザー グループ ポリシー オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからユーザー グループ ポリシー オブジェクトを選択します。また、新しいオブジェクトを作成したり、選択リストから既存のオブジェクトを編集したりすることもできます。

要素	説明
CA Server	デバイスの証明書要求の管理に使用する Certification Authority（CA; 証明局）サーバを選択します。[選択（Select）] をクリックして CA サーバーを定義する PKI 登録ポリシーオブジェクトを選択するか、または新規オブジェクトを作成します。詳細については、 [PKI Enrollment] ダイアログボックス（1554 ページ）を参照してください。 CA サーバを使用する IPsec 設定の詳細については、 Public Key Infrastructure ポリシーについて （1544 ページ）を参照してください。
Virtual Template IP Type	[ダイナミック VTI の有効化（Enable Dynamic VTI）] を選択した場合に使用可能になります。 使用する仮想テンプレート インターフェイスを指定します。 • [IP]：仮想テンプレート インターフェイスとして IP アドレスを使用します。プライベート IP アドレスを指定します。 • [ループバック インターフェイスを使用（Use Loopback Interface）]：仮想テンプレート インターフェイスとして既存のループバック インターフェイスから取得した IP アドレスを使用します。[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロール オブジェクトを選択するか、あるいはループバック インターフェイスを識別する新規オブジェクトを作成します。
VRF Solution	[VRF 設定の有効化（Enable VRF Settings）] を選択した場合に使用可能になります。 VRF ソリューションを選択します。 • [1 ボックス（1-Box）]（IPsec Aggregator + MPLS PE）：1 つのデバイスが、カスタマーエッジ（CE）デバイスから IPsec 暗号化および復号化を実行する以外に、パケットの MPLS タギングも実行するプロバイダーエッジ（PE）ルータとして機能します。詳細については、 VRF 対応 IPsec 1 ボックス ソリューション （1399 ページ）を参照してください。 • [2 ボックス（2-Box）]（IPsec Aggregator だけ）：PE デバイスは MPLS タギングだけを実行し、IPsec Aggregator デバイスが CE から IPsec 暗号化および復号化を実行します。詳細については、 VRF 対応 IPsec 2 ボックス ソリューション （1400 ページ）を参照してください。
[VRF名（VRF Name）]	IPsec Aggregator の VRF ルーティング テーブルの名前。VRF 名では、大文字と小文字が区別されます。

要素	説明
ルート識別子	IPsec Aggregator の VRF ルーティング テーブルの固有識別情報。この一意のルート識別子によって、他の PE ルータへの MPLS コアにわたって各 VPN のルーティング分離を保持します。識別情報は次のいずれかの形式です。 • *IP address:X*（*X* は 0 ～ 999999999） • *N:X*（*N* は 0 ～ 65535、X は 0 ～ 999999999） （注） VRF 設定をデバイスに展開したあとは RD 識別子を上書きできません。展開後に RD 識別子を変更するには、デバイス CLI を介してその RD 識別子を手動で削除してから、再び展開する必要があります。
Interface Towards Provider Edge	2 ボックス VRF でのみ使用可能。 IPsec Aggregator 上の、PE デバイスに向けた VRF 転送インターフェイス。[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロール オブジェクトを選択するか、あるいはインターフェイスを識別する新規オブジェクトを作成します。 （注） IPsec Aggregator（ハブ）が Catalyst VPN サービス モジュールの場合は、VLAN を指定する必要があります。
ルーティング プロトコル（Routing Protocol）	2 ボックス VRF でのみ使用可能。 IPsec Aggregator と PE の間に使用するルーティング プロトコルを選択します。オプションは、[BGP]、[EIGRP]、[OSPF]、[RIPv2]、または [Static route] です。 保護された IGP 用のルーティング プロトコルが、IPsec Aggregator と PE の間のルーティング プロトコルとは異なる場合、ルーティングを保護された IGP に再配布するためのルーティング プロトコルを選択します。
AS 番号（AS Number）	BGP または EIGRP ルーティングによる 2 ボックス VRF でのみ使用可能。 IPsec Aggregator と PE の間の自律システム（AS）を識別するために使用する番号。AS 番号は 1 ～ 65535 の範囲にしてください。 保護された IGP 用のルーティング プロトコルが、IPsec Aggregator と PE の間のルーティング プロトコルと異なる場合、IPsec Aggregator と PE からルーティングを再配布する宛先の保護された IGP を識別する AS 番号を入力します。これは、GRE または DMVPN が適用される場合だけに関連します。
Process Number	OSPF ルーティングによる 2 ボックス VRF でのみ使用可能。 IPsec Aggregator と PE の間のルーティングを設定するために使用するルーティング プロセス ID 番号。プロセス番号は、1 ～ 65535 の範囲にしてください。

要素	説明
OSPF Area ID	OSPF ルーティングによる 2 ボックス VRF でのみ使用可能。 パケットが属する領域の ID 番号。0 ～ 4294967295 の範囲で任意の番号を入力できます。 （注） すべての OSPF パケットは単一の領域に関連付けられるため、すべてのデバイスに同じ領域 ID 番号が必要です。
Redistribute Static Route	スタティック ルート以外の任意のルーティング プロトコルによる 2 ボックス VRF でのみ使用可能。 選択すると、スタティック ルートを、PE デバイス方向の IPsec Aggregator で設定されているルーティング プロトコルでアドバタイズできます。 （注） このチェックボックスがオフになっており、かつ、IPsec プロポーザルに対して [Enable Reverse Route Injection] がイネーブルになっている場合（デフォルト）も、スタティック ルートは IPsec Aggregator のルーティング プロトコルでアドバタイズされます。
Next Hop IP Address	スタティック ルーティングによる 2 ボックス VRF でのみ使用可能。 プロバイダー エッジ デバイス（または IPsec Aggregator に接続されているインターフェイス）の IP アドレス。

リモートアクセス VPN での高可用性の設定（IOS）

[High Availability] ページを使用して、リモート アクセス VPN の Cisco IOS ルータまたは Cisco Catalyst スイッチに対して High Availability（HA）ポリシーを設定します。

Security Manager では、Hot Standby Routing Protocol（HSRP）を使用して透過的な自動デバイス フェールオーバーを提供する 2 つ以上のハブデバイスで構成された HA グループを作成することで、高可用性（HA）がサポートされます。仮想 IP アドレスを共有することによって、HA グループのデバイスは、外観上は、リモートアクセスユーザーに対して単一の仮想デバイスまたはデフォルトゲートウェイになります。HA グループの 1 つのデバイスが常にアクティブになって仮想 IP アドレスを独占的に使用し、同時に他のデバイスはスタンバイデバイスになります。グループ内のデバイスは、アクティブデバイスおよびスタンバイデバイスから hello パケットが着信するのを待ちます。アクティブデバイスが何らかの理由で使用できなくなると、スタンバイ デバイスが仮想 IP アドレスの所有権を取得して、リモート アクセス VPN を引き継ぎます。この転送は、リモートアクセスユーザーに対してシームレスかつ透過的に実行されます。

HA グループ内の HSRP デバイス間で状態情報が確実に共有するために、ステートフル スイッチオーバー（SSO）が使用されます。デバイスで障害が発生した場合、共有されている状態情報により、スタンバイ デバイスは、トンネルの再確立またはセキュリティ アソシエーションの再ネゴシエートを行わずに、IPsec セッションを維持できます。

ヒント

- HA グループを設定している場合は、デバイスのインターフェイスのいずれか 1 つのサブネットと一致し、IPsec プロポーザルで設定される VPN 仮想 IP に加えて、デバイス上のインターフェイスのいずれか 1 つのサブネットと一致する内部仮想 IP を指定する必要があります。リモート アクセス VPN サーバの IPsec プロポーザルの設定（IOS、PIX 6.3 デバイス）（1893 ページ）を参照してください。
- HA が設定されたリモート アクセス VPN サーバ デバイスは、リモート アクセス VPN サーバに使用されたインターフェイスと同じ外部インターフェイスを使用して HA が設定されたサイト間 VPN トポロジのハブとしては設定できません。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）IOS デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [高可用性（High Availability）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [IPSec VPN] > [高可用性（High Availability）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[高可用性（High Availability）] ページが表示されます。

ステップ 2 次の表で説明されているオプションを設定します。

表 426 : [High Availability] ページ、[Remote Access VPN]

要素	説明
Inside Virtual IP	HA グループ内のデバイスによって共有され、HA グループの Inside インターフェイスを表す IP アドレス。仮想 IP アドレスは、HA グループ内のデバイスの内部インターフェイスと同じサブネットにする必要がありますが、これらのインターフェイスのいずれかと同じ IP アドレスにすることはできません。 デバイスのインターフェイスのいずれか 1 つのサブネットと一致し、IPsec プロポーザルで設定される VPN 仮想 IP に加えて、デバイス上のインターフェイスのいずれか 1 つのサブネットと一致する内部仮想 IP を指定する必要があります。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。
Inside Mask	内部仮想 IP アドレスのサブネット マスク。
VPN Virtual IP	HA グループ内のデバイスによって共有され、HA グループの VPN インターフェイスを表す IP アドレス。この IP アドレスは、VPN トンネルのエンドポイントとして機能します。 （注） デバイスに既存のスタンバイ グループがある場合は、提供する IP アドレスがデバイスにすでに設定されている仮想 IP アドレスと異なることを確認します。

要素	説明
VPN Mask	VPN 仮想 IP アドレスのサブネット マスク。
Hello 間隔（Hello Interval）	ステータスと優先度を示すためにデバイスがグループ内の別のデバイスにエコー hello メッセージを送信する秒単位の間隔（1 ～ 254）。デフォルトは 5 秒です。
保留時間（Hold Time）	デバイスがダウンしていると結論付ける前に、スタンバイ デバイスがアクティブなデバイスから hello メッセージの受信を待機する秒単位の期間（2 ～ 255）。デフォルトは 15 秒です。
Standby Group Number (Inside)	HA グループ内のデバイスの内部仮想 IP サブネットと一致する内部デバイス インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 1 です。
Standby Group Number (Outside)	HA グループ内のデバイスの外部仮想 IP サブネットと一致する外部デバイス インターフェイスのスタンバイ番号。番号は 0 ～ 255 の範囲である必要があります。デフォルトは 2 です。 （注） 外部スタンバイ グループ番号は、内部スタンバイ グループ番号と異なっている必要があります。
Failover Server	リモート ピア フェールオーバー サーバの内部インターフェイスを識別する IP アドレスまたはネットワーク/ホスト ポリシー オブジェクト。IP アドレスまたはネットワーク/ホストオブジェクト名を入力するか、[選択（Select）] をクリックして、オブジェクトを選択するか、新しいオブジェクトを作成します。
Enable Stateful Failover	ステートフル フェールオーバーに対して SSO をイネーブルにします。このオプションは常に選択されるため、リモート アクセス VPN に対して選択解除することはできません。

ユーザ グループ ポリシーの設定

ユーザーグループ（IOS/PIX 6.x）ポリシーを使用して、リモートアクセス IPSec VPN サーバーのユーザーグループを指定します。ユーザーグループは、Cisco IOS ルータ、PIX 6.3 ファイアウォール、または Catalyst 6500/7600 デバイスに設定できます。

リモートアクセス VPN サーバーを設定する場合は、リモートクライアントが属するユーザーグループを作成する必要があります。ユーザ グループ ポリシーには、VPN へのユーザ アクセスおよび VPN の使用を決定する属性を指定します。ユーザ グループによってシステム管理が簡素化され、多数のユーザの VPN アクセスを迅速に設定できます。

たとえば、一般的なリモート アクセス VPN では、財務グループにアクセスを許可するプライベート ネットワーク、カスタマー サポート グループに許可するネットワーク、および MIS グループに許可するネットワークがそれぞれ異なる場合があります。また、MIS に所属する特定のユーザには、他の MIS ユーザにはアクセスできないシステムにアクセスを許可する場合が

あります。ユーザ グループ ポリシーにより、このようなアクセスを安全に行うための柔軟性が提供されます。

リモート クライアントのグループ名は、VPN サーバに設定されたユーザ グループの名前と同じである必要があります。この場合、リモート クライアントがデバイスに接続できます。名前が異なる場合は接続を確立できません。リモート クライアントが VPN サーバへの接続を確立すると、そのユーザ グループのグループ ポリシーが同じユーザ グループに属するすべてのクライアントにプッシュされます。ローカル リモート アクセス VPN サーバーまたは外部 AAA サーバー上でユーザーグループを設定できます。

注記

- Remote Access VPN Configuration ウィザードを使用してユーザ グループを指定することもできます。詳細については、Remote Access VPN Configuration ウィザードの使用 （1671 ページ）を参照してください。
- IOS デバイスで SSL VPN のグループ ポリシーを指定するには、SSL VPN ポリシーの設定（IOS） （1908 ページ）で説明されているように、SSL VPN ポリシーを使用します。

関連項目

- リモート アクセス IPSec VPN について （1656 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）IOS ルータ、Catalyst 6500/7600、または PIX 6.3 デバイスを選択して、ポリシー セレクタから **[リモート アクセス VPN（Remote Access VPN）] > [IPSec VPN] > [ユーザー グループ（IOS/PIX 6.x）（User Groups (IOS/PIX 6.x)）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[リモート アクセス VPN（Remote Access VPN）] > [IPSec VPN] > [ユーザー グループ（IOS/PIX6.x）（User Groups (IOS/PIX6.x)）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[User Groups] ページが開きます。

このページには、リモート アクセス IPsec VPNS に設定されているすべての既存ユーザ グループ ポリシー オブジェクトのリストである [Available User Groups] と、デバイス上に設定されるすべてのユーザ グループ ポリシー オブジェクトのリストである [Selected User Groups] という、2 つのリストが含まれています。

ステップ 2 選択したユーザ グループのリストに、適切なユーザ グループ ポリシー オブジェクトが含まれていることを確認してください。

- 新しいユーザ グループ ポリシー オブジェクトを作成するには、使用可能なユーザ グループ リストの下にある [Create]（+）ボタンをクリックして、[Add User Group] ダイアログボックスを開きます。オブジェクトの作成方法については、[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）を参照してください。

グループを作成すると、そのグループは使用可能なリストに追加されます。そのグループを使用する場合は、選択したリストに追加する必要があります。

- 選択したリストにユーザーグループを追加するには、利用可能なリストでユーザーグループを選択し、[>>] をクリックします。
- ユーザーグループを削除するには、選択したリストでそのユーザーグループを選択して [<<] をクリックします。グループがデバイスにすでに設定されている場合、次の展開時に削除されます。
- いずれかのリストでユーザー グループ オブジェクトを選択し、[編集（Edit）] ボタンをクリックすることで、ユーザー グループ オブジェクトのプロパティを編集できます。

SSL VPN ポリシーの設定（IOS）

SSL VPN ポリシーを使用して、IOS ルータの SSL VPN 接続ポリシーを設定します。このページから、SSL VPN ポリシーを作成、編集、または削除できます。

関連項目

- リモート アクセス SSL VPN について （1657 ページ）
- Remote Access VPN Configuration ウィザードを使用した SSL VPN の作成（IOS デバイス）（1697 ページ）
- テーブルのフィルタリング （64 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）IOS デバイスを選択して、ポリシーセレクタから [リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[リモートアクセス VPN（Remote Access VPN）] > [SSL VPN] > [SSL VPN ポリシー（IOS）（SSL VPN Policy (IOS)）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SSL VPN] ページが表示されます。

テーブルに、SSL VPN の仮想設定を定義するすべてのコンテキストが一覧表示されます。各コンテキストには、ゲートウェイ、ドメインまたは仮想ホスト名、およびユーザ グループ ポリシーが含まれます。また、コンテキストのステータス（[In Service] または [Out of Service]）も表示されます。

ステップ 2 次のいずれかを実行します。

- コンテキストを追加するには、[行の追加（Add Row）] ボタンをクリックして、[SSL VPN Context Editor] ダイアログボックス（IOS） （1910 ページ）を開きます。
- コンテキストを編集するには、コンテキストを選択し、[行の編集（Edit Row）] ボタンをクリックします。

（注） コンテキストを削除するには、コンテキストを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 3 ポリシーについて、少なくとも次の一般的な設定を行います。その他のフィールドの詳細については、[General] タブ （1911 ページ）を参照してください。

- [名前、ドメイン（Name, Domain）]：新しいポリシーの場合は、SSL VPN の仮想設定を定義するコンテキストの名前。多数のコンテキスト設定の管理を簡素化するには、コンテキスト名をドメインまたは仮想ホスト名と同じ名前にします。
- [ゲートウェイ（Gateway）]：インターフェイスおよびポート設定を含む、ユーザーが接続するゲートウェイデバイスを識別する SSL VPN ゲートウェイ ポリシー オブジェクト。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

オブジェクトを選択すると、[Portal Page URL] フィールドに、ユーザが接続する URL が表示されます。

- [認証サーバーグループ（Authentication Server Group）]：ユーザーの認証に使用する AAA サーバーを識別する AAA サーバー グループ オブジェクトのプライオリティ付きリスト。
- [ユーザーグループ（User Groups）]：SSL VPN ポリシーで使用されるユーザーグループ。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。

ユーザーグループを追加するには、[行の追加（Add Row）] をクリックすると、既存のユーザー グループ ポリシー オブジェクトのリストが開き、グループを選択できます。目的のグループがまだ存在しない場合は、使用可能なグループリストの下にある [作成（Create）] ボタンをクリックして作成します。ユーザ グループ オブジェクトの詳細については、[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）を参照してください。

ステップ 4 [ポータルページ（Portal Page）] タブをクリックして、ログインページのデザインをカスタマイズします。タイトル、ロゴのグラフィック、ログイン プロンプトの上に表示されるメッセージ、およびバックグラウンドとテキストの色をカスタマイズできます。

別のグラフィックを選択する場合は、最初に Security Manager サーバにそのグラフィックをコピーする必要があります。ワークステーションのハードドライブからはグラフィックを選択できません。

ステップ 5 [Secure Desktop] タブをクリックして、Cisco Secure Desktop（CSD）ソフトウェアを設定します。CSD ポリシーは、クライアント システムのエントリ要件を定義し、クライアント システム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供します。これにより、機密データは SSL VPN セッションの間だけ共有されるようになります。

CSD を使用する場合は、[Cisco Secure Desktopの有効化（Enable Cisco Secure Desktop）] を選択し、[選択（Select）] をクリックして、VPN アクセスおよびホストスキャンの制御に使用するルールが定義される Cisco Secure Desktop 設定ポリシーオブジェクトを選択します。選択リストから新しいオブジェクトを作成できます。これらのオブジェクトの設定の詳細については、Cisco Secure Desktop 設定オブジェクトの作成（1913 ページ）を参照してください。

（注） 設定を機能させるには、デバイスに Secure Desktop Client ソフトウェアをインストールしてアクティブ化する必要があります。

ステップ 6 [詳細設定（Advanced）] タブをクリックし、コンテキストの最大同時ユーザー数を設定するか、VRF を使用している場合は、SSL VPN コンテキストに関連付けられた VRF インスタンスの名前を設定します。

ステップ 7 [OK] をクリックして変更を保存します。

[SSL VPN Context Editor] ダイアログボックス（IOS）

このダイアログボックスを使用して、SSL VPN の仮想設定を定義するコンテキストを作成または変更します。詳細については、SSL VPN ポリシーの設定（IOS） （1908 ページ）を参照してください。

ナビゲーション パス

SSL VPN（IOS）ポリシーを開き、[行の追加（Add Row）]（+）をクリックするか、テーブル内のコンテキストを選択して [行の編集（Edit Row）] をクリックします。SSL VPN ポリシーを開く方法については、SSL VPN ポリシーの設定（IOS） （1908 ページ）を参照してください。

フィールド リファレンス

表 *427 : [SSL VPN Context Editor]* ダイアログボックス

要素	説明
[一般（General）] タブ	SSL VPN ポリシーに必要な一般設定を定義します。一般設定には、ゲートウェイ、ドメイン、アカウンティングと認証用の AAA サーバ、およびユーザグループの指定が含まれます。このタブの各フィールドの説明については、[General] タブ （1911 ページ）を参照してください。
[Portal Page] タブ	SSL VPN ポリシーのログイン ページの設計を定義します。タブの一番下にある表示ボックスが変わり、選択内容がどのように表示されるかが示されます。次のことを設定できます。 • [Title]：ページの一番上に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Primary] 設定を使用して色を制御します。 • [Logo]：タイトルの隣に表示されるグラフィック。[None]、[Default]、または [Custom] を選択します。カスタムグラフィックを設定するには、目的のグラフィックを Cisco Security Manager サーバーにコピーし、[参照（Browse）] をクリックしてファイルを選択する必要があります。サポートされるグラフィック タイプは、GIF、JPG、および PNG で、最大サイズは 100 KB です。 • [Login Message]：ログイン プロンプトのすぐ上に表示されるテキスト。[Title Color] フィールドと [Text Color] フィールド内の [Secondary] 設定を使用して色を制御します。

要素	説明
[Secure Desktop] タブ	ルータで Cisco Secure Desktop（CSD）ソフトウェアを設定します。CSD ポリシーは、クライアントシステムのエントリ要件を定義し、クライアントシステム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供します。これにより、機密データは SSL VPN セッションの間だけ共有されるようになります。 （注） 設定を機能させるには、デバイスに Secure Desktop Client ソフトウェアをインストールしてアクティブ化する必要があります。 CSD を使用する場合は、[Cisco Secure Desktopの有効化（Enable Cisco Secure Desktop）] を選択し、[選択（Select）] をクリックして、VPN アクセスおよびホストスキャンの制御に使用するルールが定義される Cisco Secure Desktop 設定ポリシーオブジェクトを選択します。選択リストから新しいオブジェクトを作成できます。これらのオブジェクトの設定の詳細については、Cisco Secure Desktop 設定オブジェクトの作成 （1913 ページ）を参照してください。
[詳細設定（Advanced）] タブ	次の追加設定を行います。 • [Maximum Number of Users]：一度に許可される SSL VPN ユーザ セッションの最大数（1 ～ 1000）。 • [VRF Name]：デバイスで Virtual Routing Forwarding（VRF）が設定されている場合、SSL VPN コンテキストに関連付けられている VRF インスタンスの名前。VRF の詳細については、VRF 対応 IPsec について （1398 ページ）を参照してください。

[General] タブ

[SSL VPN Context Editor] ダイアログボックスの [General] タブを使用して、SSL VPN ポリシーに必要な一般設定を定義または編集します。一般設定には、ゲートウェイ、ドメイン、アカウンティングと認証用の AAA サーバ、およびユーザ グループの指定が含まれます。

ナビゲーション パス

[SSL VPN Context Editor] ダイアログボックス（IOS） （1910 ページ）を開き、[全般（General）] タブをクリックします。

関連項目

- SSL VPN ポリシーの設定（IOS） （1908 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス （2011 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

フィールド リファレンス

表 *428 : [SSL VPN Context Editor]* の *[General]* タブ（*IOS*）

要素	説明
Enable SSL VPN	SSL VPN 接続をアクティブにして、「In Service」にするかどうかを指定します。
名前	SSL VPN の仮想設定を定義するコンテキストの名前。 （注） 多数のコンテキスト設定の管理を簡素化するには、コンテキスト名をドメインまたは仮想ホスト名と同じ名前にします。
ゲートウェイ	ユーザが VPN に入るときに接続するゲートウェイの特性を定義する SSL VPN ゲートウェイ ポリシー オブジェクトの名前。SSL VPN 接続のインターフェイスおよびポート設定を提供するゲートウェイ オブジェクト。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
ドメイン	SSL VPN 接続のドメインまたは仮想ホスト名。
Portal Page URL	SSL VPN の URL。ゲートウェイ オブジェクトを選択すると、自動的に入力されます。ユーザは、この URL に接続して VPN に入ります。
Authentication Server Group	認証サーバ グループ。リストは、プライオリティ順に表示されます。認証は最初のグループを使用して試行され、ユーザが認証または拒否されるまで、リスト内のグループが順に使用されます。ゲートウェイ自体でユーザが定義されている場合は、LOCAL グループを使用します。 AAA サーバ グループの名前を入力します。複数のエントリはカンマで区切ります。[選択（Select）] をクリックして、グループを選択するか、または新しいグループを作成します。
認証ドメイン（Authentication Domain）	SSL VPN リモート ユーザ認証のリストまたは方式。リストも方式も指定しない場合、ゲートウェイではリモートユーザ認証にグローバル AAA パラメータが使用されます。
Accounting Server Group	アカウンティング サーバ グループ。AAA サーバー グループ ポリシー オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。

要素	説明
ユーザー グループ	SSL VPN ポリシー内で使用されるユーザ グループ。ユーザ グループでは、SSL VPN ゲートウェイへの接続時にユーザが使用できるリソースを定義します。テーブルに、グループに対してフル クライアント、CIFS ファイル アクセス、シン クライアントのいずれがイネーブルになっているかが示されます。 • ユーザーグループを追加する場合は、[行の追加（Add Row）] をクリックして、既存のユーザー グループ ポリシー オブジェクトのリストを開き、グループを選択できます。目的のグループがまだ存在しない場合は、使用可能なグループリストの下にある [作成（Create）] ボタンをクリックして作成します。ユーザ グループ オブジェクトの詳細については、[Add User Group]/[Edit User Group] ダイアログボックス（2024 ページ）を参照してください。 • ユーザーグループを編集するには、ユーザーグループを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ユーザーグループを削除するには、ユーザーグループを選択し、[行の削除（Delete Row）] ボタンをクリックします。この操作ではポリシーからグループが削除されるだけで、ユーザ グループ ポリシー オブジェクトが削除されることはありません。

Cisco Secure Desktop 設定オブジェクトの作成

Cisco Secure Desktop (CSD) 設定オブジェクトでは、IOS デバイスの SSL VPN ポリシーで Secure Desktop をイネーブルにする場合に使用する設定を定義します（SSL VPN ポリシーの設定（IOS）（1908 ページ）を参照）。ASA デバイスの場合、この機能は Dynamic Access ポリシーの一部として設定されます（ダイナミック アクセス ポリシーについて（1827 ページ）および ASA デバイスでの Cisco Secure Desktop ポリシーの設定（1838 ページ）を参照）。

Cisco Secure Desktop（CSD）は、クライアント システム上のセッション アクティビティおよび削除に、単一のセキュアなロケーションを提供することによって、機密データのすべてのトレースを確実に除去する方法を提供します。CSD では、機密データが SSL VPN セッションの間だけ共有されるセッションベースのインターフェイスを使用できます。すべてのセッション情報が暗号化され、セッションが終了したときに（たとえ接続が突然終了した場合でも）、セッション データのすべてのトレースがリモート クライアントから削除されます。

Windows ロケーションについて

Windows ロケーションを使用すると、クライアントとバーチャル プライベート ネットワークとの接続方法を判断して適宜に保護できます。たとえば、NAT デバイスの背後にある 10.x.x.x ネットワークの職場 LAN 内から接続しているクライアントが、機密情報を公開するリスクはほとんどないと考えられます。これらのクライアントについては、10.x.x.x ネットワークの IP アドレスで指定される Work という名前の CSD Windows ロケーションを設定して、このロケーションの Cache Cleaner および Secure Desktop 機能を両方ともディセーブルにします。

一方、ユーザーのホーム PC は多目的で使用されるため、ウイルスに対するリスクが高いと見なされます。これらのクライアントについては、会社から提供される証明書で指定された Home という名前のロケーションを設定し、従業員はホーム PC にこの証明書をインストールします。このロケーションでネットワークにフル アクセスするには、アンチウイルス ソフトウェア、およびサポートされている特定のオペレーティング システムがインストールされている必要がある場合があります。

または、インターネットカフェなどの信頼できないロケーションの場合は、一致基準を持たない「Insecure」という名前のロケーションを設定します（これが他のロケーションに一致しないクライアントのデフォルトになります）。このロケーションではすべての Secure Desktop 機能が必要で、不正なユーザによるアクセスを防止するためにタイムアウト期間が短く設定される場合があります。ロケーションを作成して基準を指定しない場合は、そのロケーションが [Locations] リストの最後のエントリであることを確認してください。

関連項目

- SDM を使用した IOS 上の Cisco Secure Desktop 設定例：http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml [英語]
- Microsoft Windows クライアント用の CSD の設定：http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html [英語]
- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます（Policy Object Manager （290 ページ）を参照）。

ステップ 2 オブジェクトタイプセレクタから [Cisco Secure Desktopの設定（Cisco Secure Desktop Configuration）] を選択します。

ステップ 3 作業領域を右クリックし、[新規オブジェクト（New Object）] を選択して [Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス （1969 ページ）を開きます。

ステップ 4 オブジェクトの名前を入力し、任意でオブジェクトの説明を入力します。

ステップ 5 [Windowsロケーションの設定（Windows Location Settings）] を選択して、（Work、Home、または Insecure などの）ロケーションを作成し、CSD のロケーションベース設定（適応型ポリシーとも呼ばれる）を定義します。

a) 設定するロケーションごとに [追加するロケーション（Location to Add）] フィールドに名前を入力し、[追加（Add）] をクリックして [ロケーション（Locations）] フィールドにその名前を移動します。[Move Up] ボタンおよび [Move Down] ボタンを使用すると、ロケーションの順序を並べ替えることができます。ユーザが接続すると、これらのロケーションが順番に評価され、最初に一致したロケーションがそのユーザのポリシー定義に使用されます。

ロケーションを追加すると、そのロケーション用のフォルダがコンテンツテーブルに追加されます。フォルダおよびそのサブフォルダでは、ロケーションのポリシーを定義します。

b) Secure Desktop のインストール後に、開いているブラウザ ウィンドウをすべて閉じる場合は、該当するチェックボックスがオンになっていることを確認します。

c) インストールまたはロケーション照合が失敗した場合に Web ブラウジング、ファイル アクセス、ポート転送、およびフル トンネリングをイネーブルにする VPN Feature ポリシーを設定するには、必要なチェックボックスをオンにします。

ステップ 6 追加した Windows ロケーションのフォルダおよびサブフォルダを選択し、その設定を行います。これらの設定の詳細については、『*Setting Up CSD for Microsoft Windows Clients*』（http://www.cisco.com/en/US/docs/security/csd/csd311/csd_for_vpn3k_cat6k/configuration/guide/CSDwin.html [英語]）を参照してください。

ステップ 7 [Windows CE] を選択して、Microsoft Windows CE が動作しているリモートクライアントの Web ブラウジングおよびリモート サーバー ファイル アクセスをイネーブル化または制限するように、VPN 機能ポリシーを設定します。

ステップ 8 [MacおよびLinuxキャッシュクリーナ（Mac and Linux Cache Cleaner）] を選択して、該当するクライアントのキャッシュクリーナと、Web ブラウジング、リモート サーバー ファイル アクセス、およびポート転送のイネーブル化または制限などの VPN 機能ポリシーを設定します。

ステップ 9 （任意）[Category] の下で、[Objects] テーブルでこのオブジェクトを識別するために使用するカテゴリを選択します。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

ステップ 10 [OK] をクリックしてオブジェクトを保存します。

第 34 章

リモート アクセス VPN 用のポリシー オブジェクトの設定

主にリモート アクセス VPN で使用するポリシー オブジェクトや、リモート アクセス VPN のみで使用するポリシー オブジェクトがいくつかあります。これらのオブジェクトの一部である ASA グループ ポリシーおよびユーザ グループ オブジェクトも、Easy VPN サイト間トポロジで使用されます。このリファレンスでは、これらのポリシー オブジェクトの設定について説明します。

この章は次のトピックで構成されています。

- [ASA Group Policies] ダイアログボックス （1918 ページ）
- [Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス （1969 ページ）
- [Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）
- [Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス （1977 ページ）
- [Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス （1980 ページ）
- [Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （1982 ページ）
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）
- [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス （2011 ページ）
- [Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （2013 ページ）
- [スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス （2017 ページ）
- [Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス （2020 ページ）
- [Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）
- [Add WINS Server List]/[Edit WINS Server List] ダイアログボックス （2045 ページ）

[ASA Group Policies] ダイアログボックス

[Add ASA Group Policies]/[Edit ASA Group Policies] ダイアログボックスを使用して、ASA ユーザ グループ ポリシー オブジェクトを作成、コピー、および編集します。

ASA グループ ポリシーは、Easy VPN トポロジ、リモート アクセス IPSec VPN、およびリモート アクセス SSL VPN の ASA セキュリティ アプライアンスで設定されます。Easy VPN またはリモート アクセス VPN 接続を設定する場合は、リモート クライアントが属するグループ ポリシーを作成する必要があります。グループ ポリシーは、VPN 接続用のユーザ関連の属性と値のペアがセットになったもので、デバイスに内部的（ローカル）に保存されるか、外部の AAA サーバに保存されます。トンネル グループは、トンネルの確立後にユーザ接続の期間を設定するグループ ポリシーを使用します。グループ ポリシーを使用すると、各ユーザに対して個別に各属性を指定するのではなく、属性セット全体をユーザまたはユーザ グループに適用できます。

（注） オブジェクトを作成するテクノロジーを選択する必要があります。選択したテクノロジーに応じて、構成に適切な設定を使用できます。IKEv1 または IKEv2 オプションを選択した場合、選択した IKE バージョンをサポートするには、IKE Proposal ポリシーおよび IPSec Proposal ポリシーも設定する必要があります。

バージョン 4.18 から、Cisco Security Manager ではグループポリシーをオーバーライドするオプションが導入されました。[ASA グループポリシー（ASA Group Policy）] ページでは、デバイスオーバーライドを有イネーブルにして、右クリックメニューからデバイスオーバーライドを編集できます。オーバーライドを有効にすると、

ナビゲーション パス

Policy Object Manager （290 ページ）で、[ASA グループポリシー（ASA Group Policies）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

ヒント このタイプのオブジェクトを使用するポリシーの設定時には、リモート アクセスおよび Easy VPN 用の Connection Profile ポリシー、またはリモート アクセス VPN 用の Group Policies ポリシーを含むオブジェクトを作成することもできます。

関連項目

- 接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）
- グループ ポリシーの作成（ASA、PIX 7.0+） （1743 ページ）

フィールド リファレンス

表 *429* : テクノロジー設定が含まれた、*[Add ASA Group Policies]/[Edit ASA Group Policies]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成（299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
[Settings] ペイン ダイアログボックスの本体は左右に分割されたペインであり、左側にはコンテンツ テーブル、右側にはコンテンツ テーブルで選択された項目に関連する設定が表示されます。 まずテクノロジー設定を指定する必要があります。次に、左側のコンテンツ テーブルから項目を選択し、必要なオプションを設定できます。[Technology] ページの選択内容によって、これらのページとコンテンツ テーブルで使用できるオプションが制御されます。 コンテンツ テーブルの上部にあるフォルダは、次に説明する設定可能な VPN テクノロジーまたはその他の設定を表します。	

要素	説明
Technology settings	

要素	説明
	これらの設定によって、グループ ポリシーで定義できる内容が制御されます。 • [グループポリシータイプ（Group Policy Type）]：グループポリシーを ASA デバイス自体（[内部（Internal）]）または AAA サーバー（[外部（External）]）のどちらに格納するかを指定します。このオプションは、オブジェクトを編集するときに変更できません。 [外部（External）] を選択すると、設定できる属性は、AAA サーバーを識別する AAA サーバーグループオブジェクトの名前およびそのパスワードだけになります。 • [テクノロジー（Technology）]：このオブジェクトでグループポリシーを定義する VPN のタイプ。該当するタイプをすべて選択します。 • [Easy VPN/IPSec IKEv1]：IKEv1 ネゴシエーションを許可する Easy VPN トポロジまたはリモート アクセス IPsec VPN 用。 • [Easy VPN/IPSec IKEv2]：IKEv2 ネゴシエーションを許可するリモート アクセス IPsec VPN 用。IKEv2 は、Easy VPN トポロジではサポートされていません。 • [SSL Clientless]：クライアントレス以外のタイプも含む、すべてのタイプのリモート アクセス SSL VPN 用。 （注） group-policy 属性で Web ベース VPN（webvpn）オプションをイネーブルにするには、「ssl-client」または「ssl-clientless」トンネリングプロトコルを有効にする必要があります。つまり、Security Manager でのデバイス検出時に、group-policy 属性「vpn-tunnel-protocol」の設定に「ssl-client」または「ssl-clientless」のいずれも含まれていない場合、デバイスの次回の展開中に、Security Manager は group-policy 属性下の「webvpn」オプションを削除します。 （注） Cisco Security Manager 4.24 以降、[SSLクライアントレス（SSL Clientless）] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。 • [外部サーバーグループ（External Server Group）]：グループ ポリシー属性を外部 AAA サーバーに格納する場合は、認証に使用する AAA サーバーグループを指定します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 外部サーバーグループを選択すると、[パスワード（Password）] フィー

要素	説明
	ルドと [確認（Confirm）] フィールドがアクティブになります。サーバでの認証に使用する英数字のパスワードを両方のフィールドに入力します。パスワードには最大 128 文字を使用できます。スペースは使用できません。
DNS/WINS	グループに関連付けられているクライアントにプッシュされる、DNS サーバと WINS サーバおよびドメイン名。 ASA グループ ポリシーの DNS/WINS 設定 （1963 ページ）を参照してください。
スプリット トンネリング（Split Tunneling）	この設定によって、リモート クライアントでは、暗号化されたパケットを条件に応じてセキュアなトンネルを介して中央サイトに送信でき、同時に、ネットワーク インターフェイスを介してインターネットにクリア テキスト トンネルを確立できます。 ASA グループ ポリシーのスプリット トンネリング設定 （1965 ページ）を参照してください。
Easy VPN/IPSec VPN	Easy VPN およびリモート アクセス IPSec VPN の設定： • [Client Configuration]：グループの Cisco クライアント パラメータ。ASA グループ ポリシーのクライアント設定 （1925 ページ）を参照してください。 • [Client Firewall Attributes]：グループの VPN クライアントのファイアウォール設定。 ASA グループ ポリシーのクライアント ファイアウォール属性 （1926 ページ）を参照してください。 • [Hardware Client Attributes]：グループの VPN 3002 ハードウェア クライアント設定。 ASA グループ ポリシーのハードウェア クライアント属性 （1928 ページ）を参照してください。 • [IPSec]：グループのトンネリング プロトコル、フィルタ、接続設定、およびサーバ。 ASA グループ ポリシーの IPSec 設定 （1930 ページ）を参照してください。
SSL VPN	SSL VPN の設定： • [Clientless]：SSL VPN における企業ネットワークへのクライアントレス アクセス モードの設定。 ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）を参照してください。 • [Full Client]：SSL VPN における企業ネットワークへのフル クライアント アクセス モードの設定。 ASA グループ ポリシーの SSL VPN フル クライアント設定 （1945 ページ）を参照してください。 • [Settings]：SSL VPN におけるクライアントレス/ポート転送に必要な一般設定。 ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照してください。

要素	説明
接続設定	バナー テキストを含む、グループの接続設定（セッション タイムアウトやアイドル タイムアウトなど）。ASA グループ ポリシーの接続設定（1967 ページ） を参照してください。
全般設定	• [グループポリシーのオーバーライド（Override Group Policy）]：バージョン 4.18 以降、Cisco Security Manager はグループポリシーのオーバーライドを許可します。ASA ポリシーグループのオーバーライド （1923 ページ） を参照してください。

ASA ポリシーグループのオーバーライド

Cisco Security Manager では、デバイスのグループポリシーが作成され、Cisco Security Manager レベルで維持されます。アップグレードがある場合、再検出時に、Cisco Security Manager はこれらのポリシーを新しいものとして再作成します（ポリシー名にサフィックスを付けます）。この重複に対応するために、バージョン 4.18 から、[デバイスごとに値のオーバーライドを許可（Allow Value Override per device）] チェックボックスを使用して、特定のデバイスにグループポリシーのオーバーライドを設定します。詳細については、 オブジェクト オーバーライドの管理 （309 ページ）を参照してください。

グループポリシーのオーバーライドをデバイスレベルで編集できます。 [Policy Object Overrides] ウィンドウ （314 ページ） を参照してください。

リモートアクセス VPN マルチコンテキスト モードでサポートされる CLI - グループポリシー

次の CLI は、マルチコンテキストモードのリモートアクセス VPN で、ASA バージョン9.5(2) のグループポリシーでサポートされています。これらの CLI は、管理およびユーザコンテキストでサポートされています。

（注） サポートされていない設定の場合、Security Manager は無視できる警告メッセージを表示します。デルタは生成されません。

- address-pools
- バナー
- Client-bypass-protocol
- default-domain
- Dhcp-network-scope
- Dns-server

- 終了（Exit）
- Gateway-fqdn
- Gateway-fqdn
- Ipv6-address-pools
- Ipv6-address-pools
- Msie-proxy
- なし
- Security-group-tag
- Smartcard-removal-disconnect
- Periodic-authentication
- Split-dns
- split-tunnel-all-dns
- Split-tunnel-network-list
- Split-tunnel-policy
- Vpn-access-hours
- Vpn-filter（S2S のマルチモードで既にサポートされています）
- Vpn-simultaneous-logins
- Vpn-idle-timeout（S2S のマルチモードで既にサポートされています）
- Vpn-session-timeout（S2S のマルチモードで既にサポートされています）
- Vpn-tunnel-protocol ssl-client
- Wins-server
- webvpn
    - Anyconnect-custom
    - anyconnect Dpd-interval
    - anyconnect dtls
    - anyconnect firewall-rule
    - anyconnect keep-installer
    - anyconnect modules
    - anyconnect Mtu
    - anyconnect routing-filtering-ignore
    - anyconnect Ssl

- exit
- homepage value | none
- ×

ASA グループ ポリシーのクライアント設定

[Client Configuration] 設定ページを使用して、Easy VPN またはリモート アクセス VPN 用の、ASA グループ ポリシーの Cisco クライアント パラメータを設定します。

クライアント設定は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）の目次で [Easy VPN/IPSec VPN] > [クライアント設定（Client Configuration）] を選択します。

フィールド リファレンス

表 *430 : ASA* グループ ポリシーのクライアント設定

要素	説明
Store Password on Client System	ローカル システムにパスワードを格納することをユーザに許可するかどうかを指定します。この機能は、ローカル システムがセキュアなサイトに存在する場合にだけイネーブルにしてください。
Enable IPsec over UDP UDP ポート（UDP Port）	NAT を実行しているセキュリティ アプライアンスへの UDP を使用した接続を Cisco VPN Client またはハードウェア クライアントに許可するかどうかを指定します。 このオプションを選択した場合は、4001 ～ 49151 の範囲の UDP ポート番号を指定します。IPsec ネゴシエーションでは、セキュリティ アプライアンスは、設定されたポートでリッスンし、他のフィルタ ルールによって UDP トラフィックがドロップされた場合でもこのポートの UDP トラフィックを転送します。 （注） Cisco VPN Client は、特定のデバイス上でデフォルトで設定されている IPsec over UDP を使用するように設定する必要もあります。

要素	説明
IPsec Backup Servers Servers List	バックアップ サーバの設定を指定します。 • [クライアント設定を保持（Keep Client Configuration）]：セキュリティ アプライアンスは、クライアントにバックアップサーバー情報を送信しません。クライアントは、独自のバックアップ サーバー リストを使用します（設定されている場合）。これはデフォルトです。 • [クライアント設定をクリア（Clear Client Configuration）]：クライアントは、バックアップサーバーを使用しません。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。 • [指定されたバックアップサーバーを使用（Use Specified Backup Servers）]：サーバーリストで指定したバックアップサーバーが使用されます。サーバの IP アドレス、またはネットワーク/ホスト オブジェクトの名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 バックアップサーバは、クライアント上またはプライマリ セキュリティ アプライアンス上で設定できます。セキュリティ アプライアンス上でバックアップ サーバを設定すると、セキュリティ アプライアンスは、バックアップ サーバ ポリシーをグループ内のクライアントにプッシュし、クライアント上でバックアップ サーバ リストが設定されている場合はそのリストを置き換えます。

ASA グループ ポリシーのクライアント ファイアウォール属性

クライアント ファイアウォール属性の設定を使用して、Easy VPN またはリモート アクセス IPSec VPN 用の、ASA グループ ポリシーの VPN クライアントのファイアウォール設定値を設定します。Microsoft Windows を実行している VPN クライアントだけが、これらのファイアウォール設定を使用できます。

クライアント ファイアウォール属性は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）の目次で [Easy VPN/IPSec VPN] > [クライアント ファイアウォール属性（Client Firewall Attributes）] を選択します。

フィールド リファレンス

表 *431 : ASA* グループ ポリシーのクライアント ファイアウォール属性

要素	説明
ファイアウォール モード	グループのクライアント システムのファイアウォール要件： • [ファイアウォールなし（No Firewall）]：ファイアウォールを使用しません。このページ上の他のオプションは設定できません。 • [ファイアウォールは必要（Firewall Required）]：グループ内のすべてのユーザーが、指定されたファイアウォールを使用する必要があります。セキュリティ アプライアンスは、指定されたファイアウォールがインストールされ、稼働していないと、接続を試行するセッションをすべてドロップします。この場合、セキュリティ アプライアンスは、ファイアウォール設定が一致していないことを VPN クライアントに通知します。 （注） Windows VPN クライアント以外のクライアントがグループに存在していないことを確認してください。クライアント ファイアウォールを必須としている場合、グループ内の Windows VPN 以外のクライアント（VPN 3002 ハードウェア クライアントなど）は接続できません。 • [ファイアウォールは任意（Firewall Optional）]：ユーザーはファイアウォールを使用できますが、必須ではありません。このオプションによって、グループ内のすべてのユーザが接続できます。ファイアウォールに対応しているユーザーは、ファイアウォールを使用できます。ファイアウォールなしで接続するユーザーには、警告メッセージが表示されます。この設定は、一部のユーザだけがファイアウォールに対応しているグループを作成するときに役立ちます。たとえば、Microsoft Windows が実行されないシステムを持つクライアントが存在する場合や、一部のクライアントにファイアウォール ソフトウェアがインストールされていない場合などが当てはまります。
Firewall Type	必須または任意にするファイアウォールのタイプ。このリストには、Cisco、Network ICE、Sygate、および Zone Labs など、サポートされているすべてのファイアウォール ソフトウェアが示されます。 • [Custom Firewall] を選択した場合は、[Custom Firewall] グループのフィールドに入力する必要があります。ポリシー ソースを設定する必要もあります。ベンダーによってサポートされているオプションだけを選択します。 • 一部のファイアウォール タイプでは、ファイアウォールによって実装されているポリシー ソースを指定する必要があります。

要素	説明
Policy Source	一部のタイプのファイアウォールでは、クライアント ファイアウォールがポリシーを取得する場所を設定できます。 • [Get Policy From Remote Firewall]：ポリシーは、クライアント ファイアウォール アプリケーションで設定されます。大半のクライアント ファイアウォールがこの方法で動作します。 • [Use Specified Policy]：指定したポリシーが、クライアント ファイアウォールにプッシュされます。独自のポリシーを使用する必要があります。 [着信トラフィックポリシー（Inbound Traffic Policy）] フィールドと [発信トラフィックポリシー（Outbound Traffic Policy）] フィールドの両方で、拡張アクセス コントロール リスト ポリシー オブジェクトまたは統合 ACL の名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成する必要があります。統合 ACL は、ASA バージョン 9.0 以降でサポートされています。
カスタム ファイアウォール	カスタム ファイアウォールをファイアウォール タイプとして選択した場合に、必須または任意のファイアウォールを定義する属性： • [Vendor ID]：カスタム ファイアウォールのベンダーを指定する番号。値は 1 ～ 255 です。 • [Product ID]：カスタム ファイアウォールの製品またはモデルを指定する番号。値は 1 ～ 32 または 255 です。複数の範囲を指定できます（4-12, 24-32 など）。サポートされているすべての製品を指定する場合は255を使用します。 • [Description]：ベンダーや製品の名前など、カスタム ファイアウォールに関する任意の説明。

ASA グループ ポリシーのハードウェア クライアント属性

ハードウェア クライアント属性設定を使用して、Easy VPN またはリモート アクセス IPSec VPN 用の、ASA グループ ポリシーの VPN 3002 ハードウェア クライアント設定値を設定します。

ハードウェアクライアント属性は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）のコンテンツテーブルで [Easy VPN/IPSec VPN] > [ハードウェアクライアント属性（Hardware Client Attributes）] を選択します。

フィールド リファレンス

表 *432 : ASA* グループ ポリシーのハードウェア クライアント属性

要素	説明
Require Interactive Client Authentication	セキュア ユニット認証をイネーブルにするかどうかを指定します。セキュア ユニット認証では、クライアントがトンネルを開始するたびに、ユーザ名とパスワードを使用した認証を実行するようにVPNハードウェア クライアントに求めることによって、セキュリティを高めます。ハードウェア クライアントには、ユーザ名およびパスワードは保存されません。 （注） セキュアユニット認証では、ハードウェア クライアントが使用するトンネル グループ用の認証サーバ グループを設定している必要があります。プライマリ セキュリティ アプライアンスでセキュア ユニット認証が必要な場合は、すべてのバックアップ サーバでもセキュア ユニット認証を必ず設定してください。
Require Individual User Authentication	ハードウェア クライアントの背後の個々のユーザが、このトンネル経由でネットワークにアクセスする場合に認証される必要があるかどうかを指定します。個々のユーザーは、設定した認証サーバーの順序に従って認証されます。 このオプションを選択しない場合、セキュリティ アプライアンスでは、別のグループ ポリシーからユーザ認証の値を継承できます。
Enable Cisco IP Phone Bypass	ハードウェア クライアントの背後のIP電話が、ユーザ認証プロセスなしで接続できるかどうかを指定します。セキュア ユニット認証は、他のユーザに関しては引き続き有効です。
Enable LEAP Bypass	VPN ハードウェア クライアントの背後のワイヤレス デバイスからのLightweight Extensible Authentication Protocol（LEAP）パケットが、ユーザ認証の前に、VPNトンネルを通過できるかどうかを指定します。このアクションによって、Cisco ワイヤレス アクセス ポイント デバイスを使用するワークステーションは、LEAP認証を確立し、その後ユーザ認証ごとに認証を再度実行できます。 （注） LEAP は、接続の一方の側のワイヤレス クライアントと、もう一方の側の RADIUS サーバとの間の相互認証を実行する 802.1X ワイヤレス認証方式です。パスワードなど、認証に使用されるクレデンシャルは、ワイヤレス媒体を経由して送信される前に必ず暗号化されます。

要素	説明
Allow Network Extension Mode	ハードウェア クライアントのネットワーク拡張モードをイネーブルにするかどうかを指定します。 ネットワーク拡張モードを使用すると、ハードウェア クライアントは、単一のルーティング可能なネットワークを VPN トンネルを介してリモート プライベート ネットワークに提供できます。IPsec によって、ハードウェア クライアントの背後のプライベート ネットワークからセキュリティ アプライアンスの背後のネットワークまでのすべてのトラフィックがカプセル化されます。PAT は適用されません。セキュリティ アプライアンスの背後のデバイスは、ハードウェア クライアントの背後のプライベート ネットワーク上のデバイスには、トンネルを介してだけ直接アクセスできます。またその逆も可能です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。
Idle Timeout Mode	個々のクライアントの非アクティブ期間を処理する方法： • [期間指定によるタイムアウト（Specified Timeout）]：指定した期間、ハードウェアクライアントの背後のユーザーによる通信アクティビティがない場合、セキュリティアプライアンスはそのクライアントのアクセスを終了します。値は 1 ～ 35791394 分です。 • [Unlimited Timeout]：ユーザ セッションは、非アクティブが原因で終了されることはありません。

ASA グループ ポリシーの IPSec 設定

IPsec 設定を使用して、Easy VPN またはリモート アクセス IPSec VPN 用の、ASA グループ ポリシーのトンネリング プロトコル、フィルタ、接続設定、およびサーバを指定します。これにより、認証、暗号化、カプセル化、およびキー管理を制御するセキュリティ アソシエーションが作成されます。

IPSec は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）の目次から **[Easy VPN/IPSec VPN]** > **[IPsec]** を選択します。

フィールド リファレンス

表 *433 : ASA* グループ ポリシーの *IPSec* 設定

要素	説明
Enable Re-Authentication on IKE Re-Key	セキュリティ アプライアンスが、最初のフェーズ 1 IKE ネゴシエーション中にユーザに対してユーザ名とパスワードの入力を求めるかどうか、およびセキュリティを高めるために、IKE キーの再生成が発生するたびにユーザ認証を求めるかどうかを指定します。接続の反対側にユーザがいない場合、再認証は失敗します。
Enable IPsec Compression	モデムで接続しているリモート ダイヤルイン ユーザの伝送レートを上げるデータ圧縮をイネーブルにするかどうかを指定します。 **注意** データ圧縮を使用すると、各ユーザ セッションのメモリ要件と CPU 使用率が高くなり、その結果セキュリティ アプライアンスの全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。
Enable Perfect Forward Secrecy (PFS)	暗号化された各交換で一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS; 完全転送秘密）の使用をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、PFS によって、新しい各暗号キーが以前のいずれのキーとも関連しないことが保証されます。
Tunnel Group Lock	トンネル グループのロックでは、VPN クライアントで設定されているグループが、ユーザが割り当てられているトンネル グループと同じであるかどうかを確認することによって、ユーザを制限します。同じでない場合、セキュリティ アプライアンスによって、そのユーザの接続が防止されます。 トンネル名を指定しない場合、セキュリティ アプライアンスは、割り当てられているグループに関係なくユーザを認証します。グループのロックは、デフォルトではディセーブルになっています。

要素	説明
[Client Access Rules] テーブル	クライアントのアクセス ルール。これらのルールによって、アクセスを拒否されるクライアントのタイプが制御されます（ある場合）。最大で 25 のルールを定義し、結合できます。ルールは 255 文字に制限されます。 **ヒント** ルールを定義すると、暗黙的な deny all ルールが追加されます。このため、クライアントがいずれの許可ルールにも一致しなかった場合、そのクライアントはアクセスを拒否されます。ルールを作成する場合は、許可されているすべてのクライアント用の許可ルールを必ず定義してください。*をワイルドカードとして使用して、文字部分を照合できます。 最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアント タイプまたはバージョンと一致する最小の整数値を持つルールが適用されます。プライオリティの低いルールが矛盾する場合、セキュリティ アプライアンスはそのルールを無視します。 • ルールを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Client Access Rules]/[Edit Client Access Rules] ダイアログボックス （1932 ページ）を開きます。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[削除（Delete）] ボタンをクリックします。

[Add Client Access Rules]/[Edit Client Access Rules] ダイアログボックス

[Client Access Rules] ダイアログボックスを使用して、クライアント アクセス ルールのプライオリティ、アクション、VPN クライアント タイプおよび VPN クライアント バージョンを作成または編集します。

ナビゲーション パス

ASA グループ ポリシーの IPSec 設定 （1930 ページ）で、[クライアントアクセスルール（Client Access Rules）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはルールを選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *434 : [Add Client Access Rules]/[Edit Client Access Rules]* ダイアログボックス

要素	説明
プライオリティ	ルールの相対的プライオリティ。 最小の整数値を持つルールは、プライオリティが最も高くなります。したがって、クライアント タイプまたはバージョンと一致する最小の整数値を持つルールが適用されます。プライオリティの低いルールが矛盾する場合、セキュリティ アプライアンスはそのルールを無視します。値は 1 ～ 65535 です。
操作	このルールで、クライアントへのトラフィック アクセスを許可するか拒否するかを指定します。
VPN Client Type VPN Client Version	ルールが適用される VPN クライアントのタイプまたはバージョン。スペースを使用できます。 * をワイルドカードとして使用して、ゼロ以上の文字を照合できます。クライアントのタイプまたはバージョンを送信しないクライアントには n/a を使用できます。これらのフィールドに入力した文字列は、ASA デバイスで **show vpn-sessiondb remote** コマンドを使用して表示された文字列と一致する必要があります。 次に、プライオリティ、許可/拒否、タイプ、およびバージョンの例を順に示します。 • **3 Deny * version 3.*** は、プライオリティ 3 のルールで、ソフトウェアバージョンが 3.x のすべてのクライアントタイプを拒否します。 • **5 Permit VPN3002 *** は、プライオリティ 5 のルールで、すべてのソフトウェアバージョンの VPN3002 クライアントを許可します。 • **255 Permit * *** は、プライオリティ 255 のルールで、すべてのタイプおよびバージョンのクライアントを許可します。このルールは、特定のタイプのクライアントだけを拒否し、その他のすべてのタイプに関しては許可ルールを作成しない場合に役立ちます。

ASA グループ ポリシーの SSL VPN クライアントレス設定

クライアントレス設定を使用して、リモート アクセス SSL VPN における企業ネットワークへのクライアントレス アクセス モードを ASA グループ ポリシー オブジェクトに設定します。

ユーザがクライアントレス モードで SSL VPN に接続する場合、そのユーザは SSL VPN ポータル ページにログインします。このポータル ページでは、ポータルの設定方法に応じて、ユーザは使用可能なすべての HTTP サイトにアクセスしたり、Web 電子メールにアクセスしたり、Common Internet File System（CIFS）ファイル サーバを参照したりできます。

クライアントレスは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN ではサポートされていません。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）のコンテンツテーブルから [SSL VPN] > [クライアントレス（Clientless）] を選択します。

フィールド リファレンス

表 *435 : ASA* グループ ポリシーの *SSL VPN* クライアントレス設定

要素	説明
Portal Page Websites	ポータル ページ上に表示する Web サイト URL が含まれる SSL VPN ブックマーク ポリシー オブジェクトの名前。これらの Web サイトを使用すると、ユーザは目的のリソースにアクセスできます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Allow Users to Enter Websites	ブラウザへの Web サイト URL の直接入力をリモート ユーザに許可するかどうかを指定します。このオプションを選択しない場合、ユーザはポータルに表示されている URL だけにアクセスできます。
Enable File Server Browsing	CIFS ファイル サーバ上のファイル共有の参照をリモート ユーザに許可するかどうかを指定します。
Enable File Server Entry	ファイル共有名の入力による CIFS ファイル サーバ上のファイル共有の検索をリモート ユーザに許可するかどうかを指定します。
Enable Hidden Shares	非表示の CIFS 共有を表示することでユーザがアクセスできるようにするかどうかを指定します。
HTTP プロキシ	セキュリティ アプライアンスが HTTP 接続を転送する外部 HTTP プロキシ サーバに許可するアクセスのタイプ。アクセスをイネーブルにするか、アクセスをディセーブルにするか、またはユーザのログイン時にプロキシを自動的に起動する [Auto Start] を選択できます。
Filter ACL	ユーザによる SSL VPN へのアクセスを制限するために使用する、Web タイプのアクセス コントロール リスト ポリシー オブジェクトの名前。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。バージョン 4.10 以降では、Web タイプ ACL に IPv6 値を入力できます。

要素	説明
Enable ActiveX Relay	ActiveX リレーをイネーブルにするかどうかを指定します。ActiveX リレーによって、ユーザはポータル ページから ActiveX プログラムを起動できます。これにより、ユーザは Web ブラウザから Microsoft Office アプリケーションを起動し、Office 文書をアップロードおよびダウンロードできます。
UNIX Authentication Group ID	UNIX 認証グループ ID。
UNIX Authentication User ID	UNIX 認証ユーザ ID。
Smart Tunnel	このグループに割り当てるスマート トンネル リスト ポリシー オブジェクトの名前。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 スマート トンネルとは、Winsock 2 の TCP ベース アプリケーションとプライベート サイトとの間の接続です。この接続では、セキュリティ アプライアンスをパスウェイおよびプロキシ サーバとして使用して、クライアントレス（ブラウザベース）SSL VPN セッションを使用します。このため、スマート トンネルでは、ユーザは管理者権限を持つ必要はありません。詳細については、ASA デバイスの SSL VPN スマート トンネルの設定（1821 ページ）を参照してください。 （注） Cisco Security Manager 4.24 以降、[スマートトンネル（Smart Tunnel）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
Auto Start Smart Tunnel	ユーザのログイン時に、スマート トンネル アクセスを自動的に開始するかどうかを指定します。このオプションを選択しない場合、ユーザは、ポータル ページ上のアプリケーション アクセス ツールを使用して手動でトンネルを開始する必要があります。 自動サインオンでは、Microsoft Windows オペレーティング システム上の Microsoft WININET ライブラリを使用する HTTP および HTTPS を使用するアプリケーションだけがサポートされています。たとえば、Microsoft Internet Explorer では、WININET ダイナミック リンク ライブラリを使用して、Web サーバーと通信します。 （注） Cisco Security Manager 4.24 以降、[スマートトンネルの自動開始（Auto Start Smart Tunnel）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

要素	説明
[スマート トンネル ネットワーク リスト（Smart Tunnel Network List）]	次のオプションから選択して、スマートトンネルを使用するホストまたはネットワークのリストを選択します。選択を有効にするには、最初にスマート トンネル ネットワーク リストのエントリを作成する必要があります。詳細については、[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （2019 ページ）を参照してください。この機能は ASA ソフトウェアバージョン 8.3(1) 以降を実行しているデバイスでサポートされていることに注意してください。 • [なし（None）]：このオプションを選択すると、グループポリシーはデフォルトのグループ ポリシーから値を継承します。このオプションは、デフォルトで有効です。 • [すべてをトンネル（Tunnel All）]：すべてのネットワークトラフィックにスマートトンネルを使用する場合は、このオプションを選択します。 • [含める（Include）]：特定のネットワークにスマートトンネルを使用する場合は、このオプションを選択します。次に、[選択（Select）] をクリックして、[スマート トンネル ネットワーク リスト セレクタ（Smart Tunnel Network List Selector）] ダイアログボックスを開きます。利用可能なエントリから選択するか、エントリを追加することができます。スマート トンネル ネットワーク リスト エントリを追加するには、[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （2019 ページ）を参照してください。 • [Exclude（除く）]：特定のネットワークにスマートトンネルを使用しない場合は、このオプションを選択します。次に、[選択（Select）] をクリックして、[スマート トンネル ネットワーク リスト セレクタ（Smart Tunnel Network List Selector）] ダイアログボックスを開きます。利用可能なエントリから選択するか、エントリを追加することができます。スマート トンネル ネットワーク リスト エントリを追加するには、[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （2019 ページ）を参照してください。 （注） Cisco Security Manager 4.24 以降、[スマート トンネル ネットワーク リスト（Smart Tunnel Network List）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

要素	説明
Smart Tunnel Auto Signon Server List	このグループに割り当てるスマート トンネル自動サインオン リスト ポリシー オブジェクトの名前。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） Cisco Security Manager 4.24 以降、[スマートトンネル自動サインオンサーバーリスト（Smart Tunnel Auto Signon Server List）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
[ドメイン名（Domain Name）]（任意）	一般的な命名ルール（ドメイン\ユーザ名）が認証に必要な場合に、自動サインオン時にユーザ名に追加する Windows ドメイン。たとえば、ユーザ名 qa_team の認証を行う場合、CISCO と入力して CISCO\qa_team を指定します。自動サインオンサーバリストで関連エントリを設定する場合は、[Use Domain] オプションも選択する必要があります。
Port Forwarding List	このグループに割り当てるポート転送リスト ポリシー オブジェクトの名前。ポート転送リストには、クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートを介してアクセスできるアプリケーションのセットが含まれます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 （注） Cisco Security Manager 4.24 以降、[ポート フォワーディング リスト（Port Forwarding List）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
Auto Start Port Forwarding	ユーザのログイン時に、ポート転送を自動的に開始するかどうかを指定します。 （注） Cisco Security Manager 4.24 以降、[ポートフォワーディングの自動開始（Auto Start Port Forwarding）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。
Port Forwarding Applet Name	ポータル上の [Port Forwarding Java] アプレット画面に表示されるアプリケーション名または短い説明。最大 64 文字です。これは、ユーザがダウンロードするアプレットの名前です。このアプレットは、SSL VPN ゲートウェイで設定したサービス用の TCP プロキシとしてクライアント マシン上で動作します。 （注） Cisco Security Manager 4.24 以降、[ポート フォワーディング アプレット名（Port Forwarding Applet Name）][1] 機能は ASA 9.17(1) 以降のバージョンのデバイスに対しては廃止されています。

要素	説明
[VDI サーバーリスト（VDI Servers List）] テーブル	仮想デスクトップ インフラストラクチャを構成する Citrix XenApp または XenDesktop サーバー。 • VDI サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックして、[VDIサーバーの追加または編集（Add or Edit VDI Server）] ダイアログボックス （1938 ページ）を開きます。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[削除（Delete）] ボタンをクリックします。

[VDIサーバーの追加または編集（Add or Edit VDI Server）] ダイアログボックス

[VDI サーバー（VDI Server）] ダイアログボックスを使用して、Citrix XenApp または XenDesktop サーバーエントリを作成または編集します。

仮想デスクトップインフラストラクチャ（VDI）モデルでは、管理者は、企業アプリケーションまたは企業アプリケーションに事前にロードされているデスクトップをパブリッシュし、エンドユーザーは、これらのアプリケーションにリモートアクセスします。これらの仮想リソースは、ユーザーが Citrix Access Gateway を移動してアクセスする必要がないように、電子メールなどのその他のリソースと同様に表示されます。ユーザーは Citrix Receiver モバイル クライアントを使用して ASA にログオンし、ASA は事前定義された Citrix XenApp または XenDesktop サーバーに接続されます。ユーザーが Citrix の仮想化されたリソースに接続する場合に、Citrix サーバーのアドレスおよびクレデンシャルをポイントするのではなく、ASA の SSL VPN IP アドレスおよびクレデンシャルを入力するように、管理者は [Group Policy] で Citrix サーバーのアドレスおよびログオン クレデンシャルを設定する必要があります。ASA がクレデンシャルを確認したら、受信側クライアントは ASA 経由で許可されているアプリケーションの取得を開始します。

サポートされているモバイル デバイス

- iPad：Citrix Receiver バージョン 4.x 以降
- iPhone/iTouch：Citrix Receiver バージョン 4.x 以降
- Android 2.x/3.x/4.0/4.1 電話機：Citrix Receiver バージョン 2.x 以降
- Android 4.0 電話機：Citrix Receiver バージョン 2.x 以降

ナビゲーション パス

ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）で、[VDI サーバーリスト（VDI Servers List）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはルールを選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *436 : [VDI*サーバーの追加または編集（*Add or Edit VDI Server*）*]* ダイアログボックス

要素	説明
[ホスト名/IP アドレス（IPv4/IPv6）（Hostname/IP Address (IPv4/IPv6)）]	XenApp または XenDesktop サーバーのアドレス。この値は、クライアントレス マクロにすることができます。バージョン 4.12 以降、Cisco Security Manager では、バージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスがサポートされています。無効な IPv6 アドレスの場合、Security Manager はエラーをスローします。
[ポート番号（Port Number）]（任意）	Citrix サーバーに接続するためのポート番号。この値は、クライアントレスマクロにすることができます。
ドメイン	仮想化インフラストラクチャ サーバーにログインするためのドメイン。この値は、クライアントレス マクロにすることができます。
Secure HTTP; セキュア HTTP	サーバーに SSL を使用して接続する場合は、チェックボックスをオンにします。

要素	説明
ユーザー名	

要素	説明
	仮想化インフラストラクチャ サーバーにログインするためのユーザー名。この値は、クライアントレス マクロにすることができます。 ユーザー名に使用できるマクロは次のとおりです。 • CSCO_WEBVPN_USERNAME：SSL VPN ユーザーのログイン ID。 • CSCO_WEBVPN_CONNECTION_PROFILE：SSL VPN ユーザー ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス • CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。RADIUS 経由での変数置換は、VSA#223 によって行われます。 • CSCO_WEBVPN_MACRO2：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。RADIUS 経由での変数置換は、VSA#224 によって行われます。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンド サーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。 • base64：解析された各値は Base 64 で符号化されます。

要素	説明
	• CSCO_WEBVPN_PRIMARY_USERNAME：二重認証が有効で、ログイン ID にプライマリログインユーザー名がある場合のプライマリユーザーログイン ID。 • CSCO_WEBVPN_SECONDARY_USERNAME：二重認証が有効になっている場合のセカンダリユーザーのログイン ID。

要素	説明
パスワード	

要素	説明
	仮想化インフラストラクチャ サーバーにログインするためのパスワード。この値は、クライアントレス マクロにすることができます。 パスワードに使用できるマクロは次のとおりです。 • CSCO_WEBVPN_PASSWORD：SSL VPNユーザーのログインパスワード。 • CSCO_WEBVPN_INTERNAL_PASSWORD：SSL VPN ユーザーの内部リソースパスワード。キャッシュされた認定証であり、AAAサーバーによって認証されていません。ユーザーがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。 • CSCO_WEBVPN_MACRO1：MACRO1 ユーザー名のパスワード。 • CSCO_WEBVPN_MACRO2：MACRO2 ユーザー名のパスワード。 • CSCO_WEBVPN_MACROLIST1 およびCSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに1つのデリミタが使用されます。 • インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンド サーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされたURLになります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。 • base64：解析された各値は Base 64 で符号化されます。 • CSCO_WEBVPN_PRIMARY_PASSWORD：二重認証用のプライマリユーザーのログインパスワード。 • CSCO_WEBVPN_SECONDARY_PASSWORD：二重認証用のセカンダリ

要素	説明
	ユーザーのログインパスワード。

ASA グループ ポリシーの SSL VPN フル クライアント設定

フル クライアント設定を使用して、リモート アクセス SSL VPN における企業ネットワークへのフル クライアント アクセス モードを ASA グループ ポリシー オブジェクトに設定します。

フル クライアント モードによって、SSL VPN トンネルを介して企業ネットワークに完全にアクセスできるようになります。フルクライアントアクセスモードでは、トンネル接続はグループ ポリシー設定によって決まります。フル クライアント ソフトウェアである SSL VPN Client（SVC）または AnyConnect がリモート クライアントにダウンロードされるため、トンネル接続はリモート ユーザが SSL VPN ゲートウェイにログインしたときに確立されます。

ヒント　フルクライアントアクセスを有効にするには、デバイス上で **[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）]** ポリシーを設定して、そのデバイスにインストールする AnyConnect イメージパッケージを識別する必要があります。これらのイメージは、ユーザがダウンロードできるようにデバイス上に存在している必要があります。詳細については、SSL VPN AnyConnect クライアント設定について （1789 ページ）および[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。

次のポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

- セキュリティ グループ タグ（Security Group Tag）
- 定期的な証明書の検証（Periodic Certificate Verification）
- Client Dead Peer Detection Timeout
- Gateway Dead Peer Detection Timeout
- Datalayerトランスポート層セキュリティ圧縮（Datalayer Transport layer Security Compression）
- Keep AnyConnect Client on Client System
- ルーティングとフィルタルールを無視（Ignore Routing and Filter Rules）
- AnyConnectモジュール（AnyConnect Modules）
- AnyConnect MTU
- AnyConnectファイアウォールクライアントパブリックACL（AnyConnect Firewall-Client Public ACL）
- AnyConnectファイアウォールクライアントプライベートACL（AnyConnect Firewall-Client Private ACL）

- Enable Datagram Transport Layer Security

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）の目次から **[SSL VPN] > [フルクライアント（Full Client）]** を選択します。

フィールド リファレンス

表 *437 : ASA* グループ ポリシーの *SSL VPN* フル クライアント設定

要素	説明
Enable Full Client	フル クライアント モードをイネーブルにするかどうかを指定します。
[モード（Mode）]	SSL VPN が動作するモード： • [AnyConnectクライアントのダウンロードに失敗した場合に他のアクセスモードを使用する（Use Other Access Modes if AnyConnect Client Download Fails）]：フルクライアントをリモートユーザーにダウンロードできなかった場合、ユーザーに VPN へのクライアントレスまたはシンクライアントアクセスを許可します。 • [フルクライアントのみ（Full Client Only）]：クライアントレスまたはシンクライアントアクセスを禁止します。ユーザは、フル クライアントをインストールし、VPN への接続に使用できるようにしておく必要があります。
Keep AnyConnect Client on Client System	クライアントの切断後も、AnyConnect クライアントをクライアントシステムにインストールしておくかどうかを指定します。クライアントをインストールしたままにしておかない場合、ユーザは、ゲートウェイに接続するたびにクライアントをダウンロードする必要があります。
Enable Keepalive Messages	トンネルでのデータ送受信にピアを使用できることを示すために、ピア間でキープアライブ メッセージを交換するかどうかを指定します。キープアライブ メッセージは、設定された間隔で送信され、その間隔で切断が発生すると、バックアップ デバイスを使用して新しいトンネルが作成されます。 このオプションを選択した場合は、リモートクライアントが IKE キープアライブパケットの送信を待機する時間間隔（秒単位）を [間隔（Interval）] フィールドに入力します。

要素	説明
SSL圧縮（SSL Compression）	データ圧縮を有効にするかどうかを指定します。有効にする場合は、使用するデータ圧縮の方法（[なし（None）]、[デフレート（Deflate）]または[LZS]）を選択します。データ圧縮を使用すると、モデムで接続するリモート ダイヤルイン ユーザーの転送速度が向上します。 **注意** データ圧縮を使用すると、各ユーザセッションのメモリ要件とCPU使用率が高くなり、その結果セキュリティアプライアンスの全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモートユーザに対してだけイネーブルにすることを推奨します。モデム ユーザに固有のグループ ポリシーを設計し、それらのユーザに対してだけ圧縮をイネーブルにします。
Client Dead Peer Detection Timeout (sec)	パケットがSSL VPNトンネルを介してリモートユーザから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔（秒数）。 DPDは、着信トラフィックが受信されなくても発信トラフィックを送信する必要がある場合にだけピア デバイス間でキープアライブ メッセージを送信するために使用されます。
Gateway Dead Peer Detection Timeout (sec)	パケットがSSL VPNトンネルを介してゲートウェイから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔（秒数）。
Key Renegotiation Method	リモート ユーザ グループ クライアントのトンネル キーをリフレッシュする方法は、次のとおりです。 • [無効（Disabled）]：トンネルキーの更新を無効にします。 • [既存のトンネルを使用（Use Existing Tunnel）]：SSL トンネル接続を再ネゴシエートします。 • [新規トンネルの作成（Create New Tunnel）]：新しいトンネル接続を開始します。 トンネルの更新サイクルの時間間隔（分単位）を[間隔（Interval）]フィールドに入力します。
Enable Datagram Transport Layer Security	グループのDatagram Transport Layer Security（DTLS）接続をイネーブルにするかどうかを指定します。 DTLSをイネーブルにすると、AnyConnectクライアントは、SSL VPN接続を確立して2つのトンネル（SSL トンネルとDTLS トンネル）を同時に使用できます。DTLSによって、一部のSSL接続に関連する遅延および帯域幅の問題が回避され、パケット遅延の影響を受けやすいリアルタイム アプリケーションのパフォーマンスが向上します。

要素	説明
Datagram Transport Layer Security圧縮（Datagram Transport Layer Security Compression）	グループの Datagram Transport Layer Security（DTLS）接続を圧縮するかどうかを指定します。圧縮する場合は、使用するデータ圧縮の方法（[なし（None）]、[デフォルト（Default）]、または [LZS]）を選択します。
Don't Fragment（DF）ビットを無視（Ignore Don’t Fragment (DF) bit）	フラグメント化が必要なパケットの DF ビットを無視するかどうかを指定します。この機能では、DF ビットが設定されているパケットを強制的にフラグメント化して、トンネルを通過させることができます。使用例として、TCP MSS ネゴシエーションに適切に応答しないネットワークのサーバーに対する使用などがあります。

要素	説明
AnyConnect Module	

要素	説明
	AnyConnect クライアントがオプションの機能を有効にするために必要なモジュール。[選択（Select）] をクリックして、[AnyConnectモジュールの追加（Add AnyConnect Module）] ダイアログボックスから該当するモジュールを選択します。 • [AnyConnect DART]：AnyConnect Diagnostics and Reporting Tool（DART）を有効にするには、このモジュールを選択します。DART を使用すると、指定したログファイルとクライアント接続の分析とデバッグに使用できる診断情報が結び付けられます。 • [AnyConnect Network Access Manager]：Network Access Manager を有効にするには、このモジュールを選択します。Network Access Manager を使用すると、管理上定義されたエンドユーザーポリシーおよび認証ポリシーを適用して、エンドユーザーが事前設定されたネットワークプロファイルを利用できるようになります。 • [AnyConnect SBL]：Start Before Logon（SBL）を有効にするには、このモジュールを選択します。SBL を使用すると、Windows のログインダイアログボックスが表示される前に AnyConnect を開始することで、ユーザーは Windows にログインする前に VPN 接続を介して企業インフラストラクチャに強制的に接続されます。ASA に認証されると、Windows ログインダイアログが表示されるので、ユーザーは通常どおりにログインします。SBL は Windows でのみ使用可能で、ログイン スクリプト、パスワードのキャッシュ、ネットワーク ドライブからローカル ドライブへのマッピングなどの使用を制御できます。 • [AnyConnect Webセキュリティモジュール（AnyConnect Web Security Module）]：AnyConnect Web セキュリティモジュールを有効にするには、このモジュールを選択します。AnyConnect Web セキュリティモジュールは、HTTP トラフィックを ScanSafe スキャニングプロキシにルーティングするエンドポイントコンポーネントです。トラフィックは、プロキシ上で ScanSafe Web スキャニングサービスによって評価されます。 • [AnyConnectテレメトリモジュール（AnyConnect Telemetry Module）]：AnyConnect セキュア モビリティ クライアント用の AnyConnect テレメトリモジュールを有効にするには、このモジュールを選択します。このモジュールは、悪意のあるコンテンツの発信元に関する情報を Cisco IronPort Web セキュリティアプライアンス（WSA）の Web フィルタリング インフラストラクチャに送信します。この Web フィルタリング インフラストラクチャでは、Web セキュリティ スキャニング アルゴリズムの強化、URL カテゴリと Web レピュテーション データベースの精度の向上、最終的な URL フィルタリング ルールの改良のために、このデータを使用します。

要素	説明
	• [AnyConnect ISE Network Setup Assistant]：AnyConnect ISE Network Setup Assistant モジュールを有効にするには、このモジュールを選択します。 • [AnyConnect ISEポスチャ（AnyConnect ISE Posture）]：AnyConnect ISE ポスチャモジュールを有効にするには、このモジュールを選択します。 • [AnyConnectポスチャモジュール（AnyConnect Posture Module）]：AnyConnect ポスチャモジュールを有効にするには、このモジュールを選択します。このモジュールを使用すると、AnyConnect セキュアモビリティクライアントがホストにインストールされているオペレーティングシステム、およびウイルス対策、スパイウェア対策、ファイアウォールの各ソフトウェアを識別できます。ホストスキャンアプリケーションはポスチャモジュールのコンポーネントに含まれる、こうした情報を収集するアプリケーションです。 （注） 他のオプションが表示されている場合は、この機能の説明について、Cisco AnyConnect VPN クライアントのリリース ノートを参照してください。
AnyConnect MTU	Cisco AnyConnect VPN クライアントによって確立された SSL VPN 接続の最大伝送単位（MTU）サイズ。
AnyConnect Always-On VPN（AnyConnect Always-On VPN）	Always-On VPN を使用すると、システムにログオンした後、AnyConnnect で VPN セッションを自動的に確立できます。VPN セッションは、システムからログオフするまで開いたままになります。 次のオプションのいずれか 1 つを選択します。 • [なし（None）]：AnyConnect サービスプロファイルは変更されません。デフォルトグループポリシーの値を継承します。 • [AnyConnectプロファイル設定（AnyConnect Profile Setting）]：AnyConnect VPN プロファイルで設定されている [Always-On VPN] オプションは、AnyConnect クライアントによって使用されます。 • [無効（Disable）]：[Always-On VPN] オプションを無効にします。

要素	説明
AnyConnect Profile Name	グループに使用するAnyConnectプロファイルの名前。カンマで区切ることで複数のプロファイル名を入力できます。この名前を設定して、[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] ポリシー内のプロファイルに関連付ける必要があります。 （注） AnyConnect プロファイル名は、マルチコンテキストモードでバージョン 9.6(2) を実行している ASA デバイスの Cisco Security Manager バージョン 4.12 以降でサポートされています。サポートされている CLI は次のとおりです。 • Webvpn：Anyconnect プロファイル
Prompt User to Choose Client Time User Has to Choose Default Location	クライアントのダウンロードをユーザに確認するかどうかを指定します。ユーザーが選択を完了する必要がある秒数を [ユーザーの選択完了時間（Time User Has to Choose）] フィールドに入力します。デフォルトは 120 秒です。 このオプションを選択しない場合、ユーザには即座にデフォルトの場所が示されます。また、選択する時間が期限切れになった場合も、デフォルトの場所がユーザに示されます。 • [Webポータル（Web Portal）]：ポータルページが Web ブラウザにロードされます。 • [AnyConnectクライアント（AnyConnect Client）]：AnyConnect クライアントがダウンロードされます。
セキュリティ グループ タグ（Security Group Tag）	VPN セッションのセキュリティ グループ タギングは、ASA バージョン 9.3(1)以降でサポートされています。セキュリティ グループ タグ（SGT）は、外部 AAA サーバを利用して VPN セッションに割り当てることができます。また、ローカルユーザデータベースの設定によって割り当てることも可能です。さらに、レイヤ 2 イーサネット経由で、Cisco TrustSec システムを介してこのタグを伝搬することができます。AAA サーバーが SGT を提供できない場合には、セキュリティ グループ タグをグループ ポリシーで利用したり、ローカル ユーザーが利用したりすることができます。 [デフォルト（Default）]チェックボックスをオンにすると、セキュリティグループタグは割り当てられません。 セキュリティグループタグを指定するには、[デフォルト（Default）] チェックボックスをオフにし、このグループポリシーで接続する VPN ユーザーに割り当てられる SGT タグの数値を [セキュリティグループタグ（Security Group Tag）] フィールドに入力します。有効値は 2 ～ 65519 です。

要素	説明
定期的な証明書の検証（Periodic Certificate Verification）	VPN セッションでクライアント証明書の定期的な検証と失効チェックを有効にするかどうかを指定します。このオプションを選択する場合は、1～168 の時間間隔を時間単位で入力します。この機能は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスでのみサポートされています。 デフォルトでは、定期的な証明書の検証は無効になっています。
AnyConnectファイアウォールクライアントパブリック ACL（AnyConnect Firewall-Client Public ACL）	SSL VPN へのユーザーアクセスを制限するために使用する拡張または統合アクセス制御リスト、あるいはポリシーオブジェクトの名前。パブリック ルールは、クライアント上のすべてのインターフェイスに適用されます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 統合 ACL は、ASA バージョン 9.0 からサポートされています。デフォルトは拡張 ACL です。デバイスのバージョンが ASA 9.0 より後の場合、すべての Anyconnect 値は統合 ACL として検出され、展開中に展開されます。
AnyConnectファイアウォールクライアントプライベートACL（AnyConnect Firewall-Client Private ACL）	SSL VPN へのユーザーアクセスを制限するために使用する拡張または統合アクセス制御リストポリシーオブジェクトの名前。プライベート ルールは、仮想アダプタに適用されます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 統合 ACL は、ASA バージョン 9.0 からサポートされています。デフォルトは拡張 ACL です。デバイスのバージョンが ASA 9.0 より後の場合、すべての Anyconnect 値は統合 ACL として検出され、展開中に展開されます。

要素	説明
[AnyConnectカスタム属性（AnyConnect Custom Attributes）] テーブル	[AnyConnectカスタム属性（AnyConnect Custom Attributes）] テーブルには、このグループポリシーに割り当てられているカスタム属性、名前、および対応する値が一覧表示されます。[SSL VPNのその他の設定（SSL VPN Other Settings）] ページの [AnyConnectカスタム属性（AnyConnect Custom Attributes）] タブで定義されている AnyConnect カスタム属性がここに一覧表示されます（AnyConnect カスタム属性（ASA）の設定 （1801 ページ）を参照）。バージョン 4.7 以降、Cisco Security Manager では、カスタム属性データを既存のカスタム属性タイプに追加できます。 カスタム属性をグループポリシーに追加するか、グループポリシーから削除し、各属性の値を設定できます。 • カスタム属性と属性の値を追加するには、テーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[AnyConnectカスタム属性の追加（Add AnyConnect Custom Attribute）] ダイアログボックスに入力します。 • カスタム属性と属性の値を編集するには、カスタム属性を選択し、[行の編集（Edit Row）] ボタンをクリックして、[AnyConnectカスタム属性の編集（Edit AnyConnect Custom Attribute）] ダイアログボックスで変更を加えます。 • カスタム属性を削除するには、カスタム属性を選択して [行の削除（Delete Row）] ボタンをクリックします。削除の確認が求められます。 詳細については、[AnyConnectカスタム属性の追加/編集（Add/Edit AnyConnect Custom Attribute）] ダイアログボックス （1801 ページ）を参照してください。

ASA グループ ポリシーの SSL VPN 設定

SSL VPN設定を使用して、ユーザがサーバにアクセスするための自動サインオンルールなど、クライアントレスおよびポート転送（シン クライアント）アクセス モードが機能するために必要な属性を設定します。自動サインオンでは、SSL VPN ユーザ ログイン クレデンシャル（ユーザ名とパスワード）を中間サーバに自動的に渡すように、セキュリティアプライアンスが設定されます。複数の自動サインオン ルールを設定できます。

ホームページ URL ポリシーは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN の [SSL] タブでサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）のコンテンツテーブルから [SSL VPN] > [設定（Settings）] を選択します。

フィールド リファレンス

表 *438 : ASA* グループ ポリシーの *SSL VPN* 設定

要素	説明
ホーム ページ	SSL VPN ホーム ページの URL。この URL は自由形式のテキストです。このページは、ユーザが VPN にログインするときに表示されます。URL を入力しないと、ホーム ページは表示されません。 バージョン 4.12 以降、Security Manager は、ソフトウェアバージョン 9.0 以降を実行している ASA デバイスのホームページ URL で IPv6 アドレスをサポートします。IPv6 アドレスのホームページ URL の形式は、http://[IPv6 アドレス]/appname です。ホームページ URL の先頭には http://（または）https:// を付ける必要があります。
Authentication Failure Message	VPN へのログインには成功したが、VPN 権限を持っていないために何も実行できないリモートユーザに表示するメッセージ。デフォルトのメッセージを次に示します。 「Login was successful, but because certain criteria have not been met or due to some specific group policy, you do not have permission to use any of the VPN features. Contact your IT administrator for more information.」
Minimum Keepalive Object Size (kilobytes)	セキュリティ アプライアンスのキャッシュに格納できる IKE キープアライブ パケットの最小サイズ（KB 単位）。
Single Sign On Server	このグループに使用するサーバを指定する、Single Sign-On（SSO; シングル サインオン）サーバ ポリシー オブジェクトの名前（ある場合）。SSO サーバによって、ユーザは、ユーザ名とパスワードを 1 回入力するだけで、ネットワーク内の他のサーバにアクセスできます。アクセスするたびにログインする必要はありません。SSO サーバを設定する場合は、自動サインオン ルール テーブルも設定します。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、[Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス （1980 ページ）を参照してください。
Enable HTTP Compression	HTTP 圧縮オブジェクトをセキュリティ アプライアンスにキャッシュできるかどうかを指定します。

要素	説明
[Auto Signon Rules] テーブル	シングルサインオンサーバーを設定する場合、自動サインオンルールテーブルには、ユーザーのログイン情報が提供される中間サーバーを決定するルールが含まれています。したがって、ネットワーク内の一部のサーバにはシングルサインオンを提供し、他のサーバには提供しないようにできます。 各ルールは許可ルールであり、サーバを識別する IP アドレス、サブネット、または Uniform Resource Identifier（URI; ユニフォーム リソース識別子）、およびユーザがサーバへのアクセスを試行したときにサーバに送信される認証のタイプ（基本 HTML、NTLM、FTP、またはこれらすべて）を示します。これらのルールは上から下の順に処理され、最初に一致したルールが適用されます。したがって、上下の矢印ボタンを使用してルールを必ず適切な順番に並べてください。 ユーザは、これらのいずれのルールでも識別されなかったサーバにアクセスする場合、そのサーバにログインしてアクセスする必要があります。 • ルールを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックス （1957 ページ）を開きます。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。
Portal Page Customization	ポータル Web ページの外観を定義する SSL VPN カスタマイゼーション ポリシーオブジェクトの名前。このポータルページによって、リモートユーザは、SSL VPN ネットワークで使用可能すべてのリソースにアクセスできます。オブジェクトを選択しない場合は、デフォルトのページ外観が使用されます。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、 SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）を参照してください。

要素	説明
User Storage Location	クライアントレス SSL VPN のセッション間に、ユーザの個人情報が格納される場所。場所を指定しなかった場合、情報はセッション間で格納されません。格納される情報は暗号化されます。 ファイル システムの指定を次の形式で入力します。 **protocol://username:password@host:port/path** ここで、**protocol** はサーバーのプロトコル、**username** と **password** はサーバー上の有効なユーザーアカウント、および **host** はサーバーの名前を示します。また、**port** はプロトコルのデフォルトを使用しない場合のポート番号、および **path** は使用するサーバー上の場所のディレクトリパスを示します。次に例を示します。 **cifs://newuser:12345678@anyfiler02a/new_share**
Storage Key 確認（Confirm）	セッション間で格納されるデータを保護するために使用されるストレージキー。スペースはサポートされていません。
Post Max Size	ポストするオブジェクトに許可される最大サイズ。指定できる値の範囲は 0 ～ 2147483647（デフォルト）です。[0] を設定すると、ポスティングが防止されます。
Upload Max Size	アップロードするオブジェクトに許可される最大サイズ。指定できる値の範囲は 0 ～ 2147483647（デフォルト）です。[0] を設定すると、アップロードが防止されます。
Download Max Size	ダウンロードするオブジェクトに許可される最大サイズ。指定できる値の範囲は 0 ～ 2147483647（デフォルト）です。[0] を設定すると、ダウンロードが防止されます。

[Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックス

[Add Auto Signon Rules]/[Edit Auto Signon Rules] ダイアログボックスを使用して、セキュリティアプライアンスが内部サーバに SSL VPN ユーザ ログイン クレデンシャルを渡すために使用する自動サインオン ルールを設定します。

ナビゲーション パス

ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を開いてから、[作成（Create）] をクリックするか、またはテーブル内の項目を選択して [編集（Edit）] をクリックします。

フィールド リファレンス

表 *439 : [Add Auto Signon Rules]/[Edit Auto Signon Rules]* ダイアログボックス

要素	説明
Allow IP	ルールの IPv4 または IPv6 アドレスまたはサブネットを設定するには、このオプションを選択します。このサブネット内のすべてのサーバに、指定したログイン クレデンシャルが提供されます。バージョン 4.12 以降、Security Manager は、ASA 9.0 以降を実行しているデバイスの IPv6 アドレスをサポートします。 • 単一サーバの IP アドレスを入力するには、完全な IP アドレスを入力し、サブネット マスクとして 255.255.255.255 を使用します。 • サブネットを指定するには、ネットワーク アドレスおよびサブネット マスクを入力します。たとえば、IP アドレス 10.100.10.0、マスク 255.255.255.0 を入力します。 ユーザがアクセスしようとする内部サーバに対してアプライアンスがクレデンシャルを送信する必要がある場合は、すべての内部ネットワーク用のルールを作成します。このことは、単一のルールを使用して実現できる場合があります。
Allow URI	このオプションを選択して、ルールの Universal Resource Identifier（URI; ユニバーサル リソース識別子）を設定します。これにより、IP アドレスではなく URI に基づいて内部サーバが識別されます。たとえば、**https://*.example.com/*** では、example.com ドメイン内のあらゆるサーバー上の全 Web ページ用のルールが作成されます。0 以上の文字に適用するワイルドカードとしてアスタリスクを使用します。

要素	説明
ログイン クレデンシャル	

要素	説明
	Security Manager バージョン 4.7 以降、使用可能な変数またはマクロからログインユーザー名とパスワードを選択できます。 （注） これらのマクロは、ASA ソフトウェア リリース バージョン 8.2(1) 以降を実行しているデバイスでサポートされています。 ユーザー名に使用できるマクロは次のとおりです。 • CSCO_WEBVPN_USERNAME：SSL VPN ユーザーのログイン ID。 • CSCO_WEBVPN_CONNECTION_PROFILE：SSL VPN ユーザー ログイン グループ ドロップダウン、接続プロファイル内のグループエイリアス。 • CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。RADIUS 経由での変数置換は、VSA#223 によって行われます。 • CSCO_WEBVPN_MACRO2：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。RADIUS 経由での変数置換は、VSA#224 によって行われます。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンドサーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。

要素	説明
	• base64：解析された各値は Base 64 で符号化されます。 • CSCO_WEBVPN_PRIMARY_USERNAME：二重認証が有効で、ログイン ID にプライマリログインユーザー名がある場合のプライマリユーザーログイン ID。 • CSCO_WEBVPN_SECONDARY_USERNAME：二重認証が有効になっている場合のセカンダリユーザーのログイン ID。 パスワードに使用できるマクロは次のとおりです。 • CSCO_WEBVPN_PASSWORD：SSL VPN ユーザーのログインパスワード。 • CSCO_WEBVPN_INTERNAL_PASSWORD：SSL VPN ユーザーの内部リソースパスワード。キャッシュされた認定証であり、AAA サーバーによって認証されていません。ユーザーがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。 • CSCO_WEBVPN_PRIMARY_PASSWORD：二重認証用のプライマリユーザーのログインパスワード。 • CSCO_WEBVPN_SECONDARY_PASSWORD：二重認証用のセカンダリユーザーのログインパスワード。
認証タイプ（Authentication Type）	このルールが該当するサーバにセキュリティ アプライアンスが渡すクレデンシャルのタイプ（基本 HTML、NT LAN Manager（NTLM）認証、FTP、またはこれらの方式すべて）。 デフォルトのオプションは[すべて（All）]です。特定のタイプにログインを制限する必要がある場合を除き、デフォルトを使用してください。

ASA グループポリシーのブラウザ プロキシ設定

ブラウザプロキシの設定を使用して、ブラウザの属性を構成します。

ブラウザプロキシは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）のコンテンツテーブルから [ブラウザプロキシ（ Browser Proxy）] を選択します。

フィールド リファレンス

表 *440 : ASA* グループポリシーのブラウザ プロキシ設定

要素	説明
プロキシサーバーポリシー（Proxy Server Policy）	次のいずれかを選択します。 • [プロキシなし（No proxy）]：このオプションを選択すると、プロキシ設定は使用されません。 • [クライアントプロキシを変更しない（Do not modify client proxy）]：このオプションを選択すると、ASA はエンドポイントデバイスのプロキシ設定を変更しません。 • [プロキシを使用（Use proxy）]：このオプションを選択した場合は、[プロキシ方式の選択（Select Proxy Method）] で使用可能な 1 つ以上の方式を選択します。
プロキシ方式の選択（Select Proxy Method）	次の項目の 1 つ以上を選択します。 • [自動検出（Auto Detect）]：クライアントデバイスのブラウザでの自動プロキシサーバー検出の使用をイネーブルにするにはこのオプションを選択します。 • 以下で構成したプロキシサーバーの設定を使用（Use Proxy Server Setting Configured Below）：このオプションを選択して、プロキシサーバー設定を指定します。 • [以下で構成されたユーザプロキシ自動構成（PAC）（User Proxy Auto Configuration (PAC) configured below）]：プロキシ自動構成ファイルの URL から HTTP プロキシサーバー設定を取得するようにブラウザに指示するには、このオプションを選択します。

要素	説明
プロキシサーバーの設定（Proxy Server Setting）	次を入力します。 • [サーバーアドレス（Server Address）]：クライアントデバイスに適用されるブラウザサーバーの IP アドレスまたは名前とポートを「サーバーアドレス:ポート番号」の形式で指定します。複数のプロキシサーバーを設定するには、スペースを使用してサーバーアドレスを区切ります。 • [例外リスト（Exception List）]：プロキシサーバーアクセスから除外するサーバーの名前と IP アドレスを一覧表示します。プロキシサーバー経由のアクセスを行わないアドレスのリストを入力します。このリストは、ブラウザの [プロキシ設定（Proxy Settings ）] ダイアログボックスにある [例外（Exceptions）] ボックスに相当します。複数の例外リストを設定するには、スペース、コンマ、またはセミコロンを使用してリストを区切ります。 • [ローカルアドレスのプロキシサーバーをバイパス（Bypass Proxy Server for Local Addresses）]：クライアント PC での Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定します。[はい（Yes）] を選択するとローカルバイパスがイネーブルになり、[いいえ（No）] を選択するとローカルバイパスがディセーブルになります。このオプションを使用しない場合は、[なし（None）] を選択します。デフォルトで選択されているオプションは [なし（None）] です。
プロキシ自動構成（PAC）URL（Proxy Auto Configuration (PAC) URL）	自動構成ファイルの URL を指定します。このファイルには、ブラウザがプロキシ情報を探せる場所が記述されています。
ポリシーロックダウン（Policy Lockdown）	[有効（Enable）] を選択すると、AnyConnect VPN セッション時にブラウザの接続タブが非表示になります。[無効（Disable）] を選択すると、接続タブの表示はそのまま変わりません。このオプションを使用しない場合は、[なし（None）] を選択します。デフォルトで選択されているオプションは [なし（None）] です。

ASA グループ ポリシーの DNS/WINS 設定

DNS/WINS 設定を使用して、この ASA グループ ポリシーに関連付けられているクライアントにプッシュする DNS サーバと WINS サーバおよびドメイン名を定義します。これらの設定は、Easy VPN、リモート アクセス IPSec および SSL VPN の設定に適用されます。

DNS/WINS は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）のコンテンツ テーブルから [DNS/WINS] を選択します。

フィールド リファレンス

表 *441 : ASA* グループ ポリシーの *DNS/WINS* 設定

要素	説明
プライマリ IPv4 DNS サーバー	グループのプライマリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。セカンダリ IPv4 DNS サーバーを設定するには、プライマリ IPv4 DNS サーバーアドレスが必須です。
セカンダリ IPv4 DNS サーバー	グループのセカンダリ DNS サーバーの IPv4 アドレス。ネットワーク/ホストオブジェクトの IPv4 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
プライマリ IPv6 DNS サーバー	グループのプライマリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。バージョン 4.12 以降、Security Manager は ASA デバイス 9.0 以降の IPv6 アドレスをサポートします。プライマリ IPv6 DNS サーバーアドレスは、セカンダリ IPv6 DNS サーバーを設定するために必須です。
セカンダリ IPv6 DNS サーバー	グループのセカンダリ DNS サーバーの IPv6 アドレス。ネットワーク/ホストオブジェクトの IPv6 アドレスまたは名前を入力します、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。バージョン 4.12 以降、Security Manager は ASA デバイス 9.0 以降の IPv6 アドレスをサポートします。
プライマリ WINS サーバ（Primary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。
セカンダリ WINS サーバ（Secondary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。

要素	説明
DHCP Network Scope	グループの DHCP ネットワークのスコープ。ネットワーク/ホスト オブジェクトの IP ネットワークアドレスまたは名前を入力します。または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
デフォルト ドメイン	グループのデフォルト ドメイン名。デフォルトは空白、つまりなしです。

ASA グループ ポリシーのスプリット トンネリング設定

スプリット トンネリング設定を使用して、中央サイトへのセキュアなトンネルを設定すると同時にインターネットへのクリアテキストトンネルを設定します。これらの設定は、Easy VPN、リモート アクセス IPSec および SSL VPN の設定に適用されます。

スプリット トンネリングを使用すると、リモート クライアントは、条件に応じて、パケットを IPsec または SSL VPN トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。スプリット トンネリング ポリシーは、特定のネットワークに適用されます。

スプリットトンネリングは、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ヒント　最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）のコンテンツテーブルから [スプリットトンネリング（Split Tunneling）] を選択します。

フィールド リファレンス

表 *442 : ASA* グループ ポリシーのスプリット トンネリング設定

要素	説明
DNS Names	スプリット トンネルを介して解決されるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを使用して解決されます。リストを入力しない場合は、デフォルトのポリシー グループからリストが継承されます。 複数のエントリは、スペースまたはカンマで区切ります。文字列全体で最大 255 文字を使用できます。

要素	説明
トンネルを介してすべてのDNS トラフィックを送信する	AnyConnect クライアントが、VPN トンネル（SSL または IPsec/IKEv2）を経由するすべての DNS アドレスを解決するかどうかを指定します。トンネルを介した DNS 解決に失敗すると、アドレスは未解決のまま残り、AnyConnect クライアントは、パブリック DNS サーバを介したアドレスの解決を試行しません。 このオプションを選択しない場合、クライアントは、トンネルオプションの設定で指定されたスプリットトンネルポリシーに従って、トンネルを介して DNS クエリを送信します。
Tunnel Option	イネーブルにする、スプリット トンネリングのポリシー： • [Disabled]（デフォルト）：トラフィックは、暗号化されずに送信されることがないか、またはセキュリティ アプライアンス以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [Tunnel Specified Traffic]：ネットワーク ACL で許可されているネットワークとの間のすべてのトラフィックをトンネルします。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザのインターネット サービス プロバイダーによってルーティングされます。 • [Exclude Specified Traffic]：ネットワーク ACL で許可されたネットワークとの間でトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。このオプションは、Cisco VPN Client だけに適用されます。

要素	説明
IPv6 トンネル オプション	バージョン 4.10 以降、Security Manager は、ASA バージョン 9.0 からのスプリットトンネリングに対して IPv6 トラフィックのサポートを提供します。 イネーブルにする、スプリット トンネリングのポリシー： • [Disabled]（デフォルト）：トラフィックは、暗号化されずに送信されることがないか、またはセキュリティ アプライアンス以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [Tunnel Specified Traffic]：ネットワーク ACL で許可されているネットワークとの間のすべてのトラフィックをトンネルします。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザのインターネット サービス プロバイダーによってルーティングされます。 • [Exclude Specified Traffic]：ネットワーク ACL で許可されたネットワークとの間でトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。このオプションは、Cisco VPN Client だけに適用されます。
ネットワーク	トラフィックがトンネルを通過する必要があるネットワーク、およびトンネリングを必要としないネットワークを識別する、標準、拡張、または統合アクセス制御リストのポリシーオブジェクトの名前。統合 ACL は、ASA バージョン 9.0 からサポートされています。許可および拒否する方法は、[トンネルオプション（Tunnel Option）] での選択に応じて解釈されます。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。ACL を指定しない場合、ネットワーク リストは、デフォルト グループ ポリシーから継承されます。

ASA グループ ポリシーの接続設定

接続設定を使用して、アクセス コントロールおよびセッション タイムアウトを含む、ASA グループ ポリシーの接続特性を設定します。これらの設定は、Easy VPN およびリモート アクセス IPsec または SSL VPN の各セッションに適用されます。

接続設定は、マルチコンテキストモードの ASA 9.5(2) リモートアクセス VPN でサポートされています。

ナビゲーション パス

[ASA Group Policies] ダイアログボックス （1918 ページ）の目次から [接続設定（Connection Settings）] を選択します。

フィールド リファレンス

表 *443 : ASA* グループ ポリシーの接続設定

要素	説明
Filter ACL	VPN 接続でトラフィックをフィルタリングするために使用する拡張アクセスコントロールリスト（ACL）ポリシーオブジェクトの名前。ACLは、許可または拒否するトラフィックを決定します。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。バージョン4.10およびASAバージョン 9.0 以降では、標準、拡張、または統合 ACL オブジェクトのリストから選択できます。 この ACL は、クライアントレス SSL VPN 接続には適用されません。
バナー テキスト（Banner Text）	リモート クライアントが VPN に接続したときに、リモート クライアント上に表示されるバナー、つまり初期テキスト。 • バージョン 4.9 以降、Security Manager は、バージョン 9.5(1) 以降の ASA デバイスのバナーテキストで、最大 4000 文字をサポートします。 • 9.5(1) より前の ASA バージョンの場合、Security Manager では、バナーテキストに最大 500 文字を入力できます。
IPv4アドレスプール（IPv4 Address Pools）	このグループポリシーで使用する 1 つ以上の IPv4 アドレスプールの名前を指定します。IPv4アドレスプールオブジェクトの名前をカンマで区切って入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。
IPv6 アドレス プール（IPv6 Address Pools）	このグループポリシーで使用する 1 つ以上の IPv6 アドレスプールの名前を指定します。IPv6アドレスプールオブジェクトの名前をカンマで区切って入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。バージョン 4.12 以降、Security Manager は ASA デバイス 9.0 以降の IPv6 アドレスプールをサポートします。
Access hours	VPNへのアクセスをユーザに許可する時間を指定する、時間範囲ポリシーオブジェクトの名前。時間範囲を指定しない場合、ユーザはいつでもVPNにアクセスできます。ネットワークへのアクセスを特定の時間（通常の就業時間や自分の組織での就業時間など）に制限する場合は、時間範囲を指定します。 オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。詳細については、時間範囲オブジェクトの設定 （379 ページ）を参照してください。

要素	説明
Max Simultaneous Logins	1 人のユーザに許可する同時ログイン数。値は、0 ～ 2147483647 です。デフォルトは 3 です。[0] を指定すると、ログインがディセーブルになり、ユーザはアクセスできなくなります。
Max Connection Time	ユーザが VPN への接続を継続できる最大時間。次のいずれかを選択します。 • [Specified Connection time]：入力した最大時間値が使用されます。値は 1 ～ 4473924 分です。この時間を超えると、セキュリティ アプライアンスによって接続が閉じられます。 • [Unlimited Connection time]：セキュリティ アプライアンスは、接続時間に基づいて接続を閉じることはありません。
アイドル タイムアウト	接続がアイドル状態である、つまり通信アクティビティがない場合に、ユーザが VPN への接続を継続できる合計時間。次のいずれかを選択します。 • [Specified Timeout]：入力したタイムアウト値が使用されます。値は 1 ～ 35791394 分です。このアイドル時間を超えると、セキュリティ アプライアンスによって接続が閉じられます。デフォルトは 30 分です。 • [Unlimited Timeout]：セキュリティ アプライアンスによってアイドル接続が閉じられることはありません。
VLAN マッピング VLAN ID（Admin. VLAN ID）	VLAN ID の値は 1 ～ 4094 で、ASA の VLAN インターフェイスに対応している必要があります。 ASA の VLAN マッピング機能により、VPN 接続からのトラフィックを指定された VLAN インターフェイスに送信できます。 Cisco Security Manager バージョン 4.10 および ASA バージョン 9.5(1) 以降では、IPv6 アドレスをリモートユーザに割り当てることができます。 Cisco Security Manager バージョン 4.17 以降、ASA 9.9(2) 以降のマルチコンテキストデバイスで VLAN を設定できます。

[Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス

[Add Cisco Secure Desktop Configuration]/[Edit Cisco Secure Desktop Configuration] ダイアログボックスを使用して、IOS ルータの Cisco Secure Desktop 設定オブジェクトを編集します。異なるロケーション タイプから接続している Windows クライアントに必要な設定値を設定したり、Windows CE クライアントの Web ブラウズやファイル アクセスをイネーブルまたは制限した

り、Macintosh クライアントと Linux クライアントのキャッシュ クリーナを設定したりできます。

Cisco Secure Desktop（CSD）は、クライアント システム上のセッションのアクティビティおよび削除用に単一のセキュアなロケーションを提供することで、機密データのすべてのトレースを確実に除去する方法を提供して、ネットワーク エンドポイントを保護します。

このポリシー オブジェクトでは、Secure Desktop Manager アプリケーションを使用して、設定値を設定します。設定値の設定の例については、「SDM を使用した IOS 上の Cisco Secure Desktop 設定例（http://www.cisco.com/en/US/products/ps6496/products_configuration_example09186a008072aa7b.shtml）[英語] を参照してください。この設定例の最初の部分では、SDM のセットアップについて説明しますが、これは無視してください。代わりに、例全体の中央付近にある、Windows ロケーションのセットアップの説明を検索してください。ここに示されている画面ショットは、CSD 設定を調べる場合の識別に役立ちます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプ セレクタから [Cisco Secure Desktop（ルータ）（Cisco Secure Desktop (Router)）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- Cisco Secure Desktop 設定オブジェクトの作成 （1913 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 444 : [Add Secure Desktop Configuration]/[Edit Secure Desktop Configuration] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成（299 ページ）を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。
Windows Location Settings	

要素	説明
Windows Locations	Windows クライアントが特定のロケーションから接続するために設定するロケーションの名前（Work、Home、Insecure など）。 ロケーションを作成すると、そのロケーション項目がコンテンツ テーブルに追加されます。そのコンテンツ テーブルで、ロケーションに関連する設定フォルダを選択し、プロパティを設定できます。これらの設定には、クライアントが特定のロケーションから接続しているかどうかを識別する方法の定義が含まれています。 設定するロケーションごとに[追加するロケーション（Location to Add）]フィールドに名前を入力し、[追加（Add）]をクリックして[ロケーション（Locations）]リストにその名前を移動します。 [Move up] ボタンと [Move down] ボタンを使用して、ロケーションを並べ替えることができます。CSD では、このダイアログボックスにリストされている順番でロケーションをチェックし、一致した最初のロケーション定義に基づいて、クライアント PC に権限を付与します。最後のロケーションとして Insecure などのデフォルト ロケーションを作成し、そのロケーションに対して最も厳しいセキュリティを設定できます。詳細については、Cisco Secure Desktop 設定オブジェクトの作成 （1913 ページ）を参照してください。
Close all open browser windows after installation	Secure Desktop アプリケーションのインストール後に、開いているすべてのブラウザ ウィンドウを閉じるかどうかを指定します。
VPN Feature Policy	インストールまたはロケーション照合が失敗した場合に該当する機能をイネーブルにするには、次のチェックボックスをオンにします。 • Web ブラウジング • File Access • ポート転送 • Full Tunneling
Windows CE	
VPN Feature Policy	Windows CE オプションを使用すると、Microsoft Windows CE を実行しているリモート クライアントによる Web ブラウズおよびリモート サーバ ファイル アクセスをイネーブルまたは制限するように、VPN 機能を設定できます。これらのクライアントのロケーションは設定できません。
Mac and Linux Cache Cleaner	

要素	説明
Launch Cleanup Upon Global Timeout	CSD がキャッシュ クリーナを起動したあとにグローバル タイムアウトを設定するかどうかを指定します。タイムアウト（デフォルトは 30 分）を選択し、ユーザがこのタイムアウト値をリセットできるかどうかを選択します。
Launch Cleanup Upon Exiting of Browser	ユーザがすべての Web ブラウザ ウィンドウを閉じたときに、キャッシュ クリーナを起動するかどうかを指定します。
Enable Canceling of Cleaning	キャッシュの消去のキャンセルをユーザに許可するかどうかを指定します。
Secure Delete	CSD がセキュアなクリーンアップを実行するためのパスの数。デフォルトは 1 パスです。 CSD は、キャッシュを暗号化し、リモート クライアントのディスクに書き込みます。Secure Desktop の終了時に、CSD はキャッシュを占有しているすべてのビットをすべて 0 に変換してから 1 に変換し、次に 0 と 1 にランダムに変換します。
Enable Web Browsing if Mac or Linux Installation Fails	キャッシュ クリーナのインストールに失敗した場合に、Web ブラウズを許可する（ただし、その他のリモート アクセス機能は許可しない）かどうかを指定します。
VPN Feature Policy	Web ブラウズ、リモート サーバ ファイル アクセス、およびポート転送を Macintosh クライアントと Linux クライアントに許可するかどうかを指定します。ポート転送では、ローカル PC にインストールされているクライアント アプリケーションをリモート サーバ上のピア アプリケーションの TCP/IP ポートに接続するために、Secure Desktop の使用を許可します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

[Add File Object]/[Edit File Object] ダイアログボックス

[Add File Object]/[Edit File Object] ダイアログボックスを使用して、ファイル オブジェクトを作成、コピー、および編集します。ファイル オブジェクトは、デバイス設定で使用されるファイル（通常は、リモート アクセス VPN ポリシーおよびポリシー オブジェクト用）を表します。これらのファイルには、Anyconnect クライアント プロファイルおよびイメージ（グラフィック）ファイル、プラグイン jar ファイル、および Cisco Secure Desktop パッケージ ファイルがあります。

ファイル オブジェクトを作成すると、Security Manager によってそのファイルのコピーが Security Manager のストレージ システムに作成されます。これらのファイルは、Security Manager デー

タベースのバックアップを作成するたびにバックアップされ、Security Manager データベースを復元すると復元されます。ファイルオブジェクトを指定する設定を展開すると、関連付けられているファイルが、該当するディレクトリのデバイスにダウンロードされます。

ファイル オブジェクトの作成後、通常はそのオブジェクトを編集することはありません。ファイルを置き換える必要がある場合は、そのファイル オブジェクトを編集して新しいファイルを選択するか、または新しいファイル オブジェクトを作成します。ファイルを編集できる場合は、ファイルオブジェクトを編集してファイルリポジトリにおけるファイルのロケーションを特定し、任意のエディタを使用して Security Manager の外部にあるファイルを開いて編集できます。ファイルリポジトリは、インストールディレクトリ（通常は C:\Program Files）内の **CSCOpx\MDC\FileRepository** フォルダです。これらのファイルは、ファイル タイプに応じた名前が付けられたサブフォルダに整理されています。

イメージファイルを除くすべてのファイルタイプの場合、[ファイルの選択（Choose a file）] ダイアログボックスで適切なタブを選択して、Security Manager サーバーまたはローカルの Security Manager クライアントからファイルを追加できます。ネットワークサーバーからファイルを選択することはできません。Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。

ヒント ファイルオブジェクトで使用するためにファイルを Security Manager サーバーにコピーするときは、ファイルをファイルリポジトリに直接コピーしないでください。

ファイル オブジェクトを削除しても、関連付けられているファイルはファイル リポジトリから削除されません。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [ファイルオブジェクト（File Objects）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- SSL VPN ブラウザ プラグインの設定（ASA） （1787 ページ）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）
- [SSL VPN Customization] ダイアログボックス - [Informational Panel] （2001 ページ）
- [SSL VPN Customization] ダイアログボックス - [Title Panel] （1996 ページ）

フィールド リファレンス

表 *445 : [Add File Object]/[Edit File Object]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299ページ）を参照してください。 名前を入力しない場合は、ファイルの名前がオブジェクト名に使用されます。
説明	（任意）オブジェクトの説明。
ファイル タイプ	ファイルのタイプ。ポリシーの設定時にオブジェクトを作成する場合は、適切なファイル タイプが事前に選択されています。次のオプションがあります。 • Image：グラフィック ファイル用。 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • AnyConnect Profile • AnyConnect Image • Hostscan Image

要素	説明
ファイル（File）	ファイルの名前およびフル パス。[参照（Browse）] をクリックしてファイルを選択します。 次のファイルタイプは、Image Manager を使用して管理されます。詳細については、Image Manager でサポートされるイメージタイプ （3754 ページ）を参照してください。 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • AnyConnect Image • Hostscan Image AnyConnect プロファイルファイルとイメージファイルの場合、Security Manager サーバーからファイルを追加できます。ネットワークサーバーからファイルを選択することはできません。 ヒント Security Manager クライアントにエクスポートまたはインポートする機能は、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デスクトップのカスタマイズ（Customize Desktop）] から制御できます。詳細については、[Customize Desktop] ページ （654 ページ）を参照してください。 編集しているファイル オブジェクトの場合、パスは Security Manager ファイル リポジトリにおけるロケーションを示します。
File Name on Device	ポリシーの展開時にファイルがデバイスにダウンロードされるときに使用するファイルの名前。デフォルトは、元のファイルと同じファイル名の使用です。 デバイスからのポリシーの検出によってオブジェクトが作成された場合、このフィールドでは、そのデバイス上に存在していたファイルの元の名前が使用されます。この名前は、元の名前が Security Manager サーバ上の既存のファイル名と重複していた場合、Security Manager サーバに存在する名前とは同じでない可能性があります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

[ファイルオブジェクト—ファイルを選択（File Object—Choose a file）] ダイアログボックス

[ファイルオブジェクト—ファイルを選択（File Object — Choose a file）] ダイアログボックスを使用して、追加または編集しているファイルオブジェクトに使用するファイルを選択します。

使用可能なファイルは、Image Manager を使用して管理されます。詳細については、Image Manager でサポートされるイメージタイプ （3754 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [ファイルオブジェクト（File Objects）] を選択します。ファイルオブジェクトを追加または編集し、[ファイルオブジェクトの追加または編集（Add or Edit File Object）] ダイアログボックスで [参照（Browse）] をクリックして、[ファイルオブジェクト—ファイルを選択（File Object — Choose a file）] ダイアログボックスを開きます。

関連項目

- SSL VPN サポート ファイルの概要と管理 （1660 ページ）
- [Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）
- SSL VPN AnyConnect クライアント設定の定義（ASA） （1792 ページ）
- SSL VPN ブラウザ プラグインの設定（ASA） （1787 ページ）
- ASA デバイスでの Cisco Secure Desktop ポリシーの設定 （1838 ページ）
- [SSL VPN Customization] ダイアログボックス - [Informational Panel] （2001 ページ）
- [SSL VPN Customization] ダイアログボックス - [Title Panel] （1996 ページ）

フィールド リファレンス

表 *446 :* ファイル オブジェクト — ファイルを選択ダイアログボックス

要素	説明
イメージリポジトリ	ファイルオブジェクトの定義に使用できる利用可能なファイルを一覧表示します。使用可能なファイルは、Image Manager を使用して管理されます。詳細については、Image Manager でサポートされるイメージタイプ （3754 ページ）を参照してください。
[選択されているファイル（File selected）]	現在選択されているファイルオブジェクトを表示します。

要素	説明
[以下のタイプのファイル（Files of Type）]	ファイルのリストをフィルタリングします。次のオプションがあります。 （注） すべてのファイルオブジェクトを表示するか、追加または編集しているファイルオブジェクトのタイプによってフィルタリングされたオブジェクトのみを表示できます。 • Cisco Secure Desktop Package • Plug-In：ブラウザ プラグイン ファイル用。 • AnyConnect Image • Hostscan Image • すべて

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス

[Port Forwarding List] ダイアログボックスを使用して、ポート転送リスト ポリシー オブジェクトを作成、コピー、および編集します。ポート転送リストオブジェクトを作成して、SSL VPN 用のシン クライアント アクセス モードの設定時に使用できます。

ポート転送により、ユーザは SSL VPN セッション経由で企業内のアプリケーション（Telnet、電子メール、VNC、SSH、Terminal Services など）にアクセスできます。ポート転送がイネーブルな場合、SSL VPN クライアント上の hosts ファイルは、転送リストで設定されているポート番号にアプリケーションをマッピングするために変更されます。ポート フォワーディング リスト オブジェクトは、リモートクライアント上のポート番号を SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートにマッピングします。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [ポートフォワーディングリスト（Port Forwarding List）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

• SSL VPN アクセスのモード （1659 ページ）
• ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）
• [User Group] ダイアログボックス - シン クライアント設定 （2038 ページ）

- Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ （1686 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *447 : [Port Forwarding List]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成（299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
[Port Forwarding List] テーブル	このオブジェクトで定義されているポート転送エントリ。このエントリは、ローカル ポートからリモート サーバおよびポートへのマッピングを示します。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックス （1979 ページ）を開きます。 • マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）] ボタンをクリックします。
Include Port Forwarding Lists	オブジェクトに含める、他のポート転送リスト オブジェクトの名前。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。 その他のポート転送リストを追加する場合、それらのリストのエントリは、このオブジェクトに直接入力されたように扱われ、含めたオブジェクトの名前は、展開中はデバイス コンフィギュレーション コマンドに反映されません。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックス

[Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry] ダイアログボックスを使用して、新しいポート転送リスト エントリを作成するか、または既存のエントリを編集します。

ナビゲーション パス

[Add Port Forwarding List]/[Edit Port Forwarding List] ダイアログボックス （1977 ページ）に移動し、[行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [ポート転送リスト（Port Forwarding List）] テーブルの下にある [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *448 : [Add A Port Forwarding Entry]/[Edit A Port Forwarding Entry]* ダイアログボックス

要素	説明
Local TCP Port	ローカル アプリケーションがマッピングされるポート番号（1 ～ 65535）。
リモート サーバ（Remote Server） IPv4/IPv6アドレス（IPv4/IPv6 Address） 名前	リモートサーバーの IPv4 または IPv6 アドレス、または完全修飾ドメイン名。エントリのタイプを選択し、IP アドレスまたは名前を入力します。 バージョン 4.12 以降、Security Manager は、ソフトウェアバージョン 9.0 以降を実行している ASA デバイスの IPv6 アドレスをサポートします。 IP アドレスの場合は、リモートサーバーの IP アドレスを指定するネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成できます。

要素	説明
Remote TCP Port	ポート転送が設定されるアプリケーションのポート番号（1 ～ 65535）。
説明	ポート転送エントリの説明。この情報は、Cisco IOS デバイスの場合は必須です。

[Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックス

[Add Single Sign On Server]/[Edit Single Sign On Server] ダイアログボックスを使用して、（ASA グループ ポリシー オブジェクトで設定されている）SSL VPN で使用する Single Sign-On（SSO; シングル サインオン）サーバ オブジェクトを作成、コピー、および編集します。ASA グループ ポリシーで SSO サーバを設定する方法については、ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照してください。

シングル サインオンを使用すると、ユーザは、ユーザ名とパスワードを複数回入力することなく、異なるサーバ上のさまざまなセキュア サービスにアクセスできます。認証では、セキュリティ アプライアンスは、SSO サーバに対する SSL VPN ユーザのプロキシとして機能します。Computer Associates SiteMinder SSO サーバまたは Security Assertion Markup Language（SAML）Browser Post Profile バージョン 1.1 サーバを識別するように、このオブジェクトを設定できます。

SSO メカニズムは、AAA プロセスの一環として、つまり AAA サーバに対するユーザ認証が成功したあとに開始されます。セキュリティ アプライアンスで稼働している SSL VPN サーバは、認証サーバに対するユーザのプロキシとして機能します。ユーザがログインすると、SSL VPN サーバは、ユーザ名とパスワードを含む SSO 認証要求を認証サーバに送信します。サーバは、この認証要求を承認すると、SSO 認証クッキーを SSL VPN サーバに返します。セキュリティ アプライアンスは、このクッキーをユーザのために保持し、ユーザの認証に使用して、SSO サーバによって保護されているドメイン内の Web サイトを保護します。

SSL VPN グループの SSO を設定する場合、RADIUS や LDAP サーバなどの AAA サーバを設定する必要もあります。

（注） SAML Browser Artifact プロファイル方式のアサーション交換は、サポートされていません。

ナビゲーション パス

Policy Object Manager （290 ページ）で [シングルサインオンサーバー（Single Sign On Servers）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

SSL VPN 用の ASA ユーザ グループ オブジェクトを設定するときに、オブジェクトを作成することもできます（ASA グループ ポリシーの SSL VPN 設定 （1954 ページ）を参照）。

フィールド リファレンス

表 449 : [Add Single Sign-On Server]/[Edit Single Sign-On Server] ダイアログボックス

要素	説明
名前	オブジェクト名。4～31 文字である必要があります。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
認証タイプ（Authentication Type）	クライアントレス SSL VPN 接続で使用する SSO サーバのタイプ。このページのその他の属性は、選択内容によって変わります。 • [SiteMinder]：Computer Associates SiteMinder SSO サーバー。 • [SAML POST]：セキュリティ アサーション マークアップ言語（SAML）Browser Post Profile サーバー。
URL （SiteMinder のみ）	セキュリティアプライアンスが認証要求を行う SiteMinder SSO サーバの URL。HTTP と HTTPS のいずれを使用するかを選択し、URL を入力します。 ヒント HTTPS 通信の場合は、SSL 暗号化設定が、セキュリティアプライアンスと SiteMinder サーバの両方で一致していることを確認してください。セキュリティアプライアンスで、**ssl encryption** コマンドを使用して一致を確認できます。
秘密キー（Secret Key） 確認（Confirm） （SiteMinder のみ）	SiteMinder サーバとの認証通信を暗号化するために使用するキー（ある場合）。キーには、任意の英数字を使用できます。文字の最小数や最大数の制限はありません。両方のフィールドに同じキーを入力します。 ヒント 秘密キーを入力した場合は、Cisco Java プラグイン認証スキームを使用して、同じキーを SiteMinder で設定する必要があります。
Assertion URL （SAML POST のみ）	SAML タイプの SSO アサーション コンシューマ サービスの URL。HTTP と HTTPS のいずれを使用するかを選択し、URL を入力します。URL は 255 文字未満である必要があります。

要素	説明
Assertion Issuer （SAML POST のみ）	SAML タイプの SSO サーバにアサーションを送信するセキュリティ デバイスの名前。これは、通常、セキュリティ アプライアンスの名前（asa.example.com など）です。この名前は、65 文字未満である必要があります。
Trustpoint （SAML POST のみ）	SAML タイプのブラウザ アサーションの署名に使用する証明書が含まれたトラストポイントとして機能する Certificate Authority（CA; 認証局）サーバを識別する、PKI 登録ポリシー オブジェクトの名前。名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
最大再試行回数（Max Retries）	認証がタイムアウトするまでに、セキュリティ アプライアンスが、失敗した SSO 認証を再試行する回数。範囲は 1 ～ 5 再試行です。デフォルトは 3 再試行です。
要求のタイムアウト（Request Timeout）	失敗した SSO 認証の試行がタイムアウトするまでの秒数。範囲は 1 ～ 30 秒です。デフォルトは 5 秒です。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add Bookmarks]/[Edit Bookmarks] ダイアログボックス

[ブックマークの追加（Add Bookmarks）]/[ブックマークの編集（Edit Bookmarks）] ダイアログボックスを使用して、SSL VPN ブックマーク オブジェクト用のブラウザベースのクライアントレス SSL VPN ブックマーク（URL リスト）を設定します。このダイアログボックスで、テーブル内のブックマーク エントリの順序を変更し、SSL VPN ブックマーク オブジェクトを作成、コピー、編集、および削除できます。

SSL VPN ブックマーク オブジェクトによって、ログインの成功後にポータル ページに表示される URL が定義されます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [SSL VPNブックマーク（SSL VPN Bookmarks）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （1820 ページ）
- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）

フィールド リファレンス

表 *450 : [Add Bookmarks]/[Edit Bookmarks]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成（299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
Bookmarks Heading (IOS) （IOS デバイスのみ）	IOS デバイスでホスティングされている SSL VPN のポータル ページにリストされている URL の上に表示される見出し。
ブックマーク	オブジェクトのブックマーク エントリのリスト。 • エントリの並び順を変更するには、エントリを選択し、[Move Up]/[Move Down] 矢印ボタンをクリックします。テーブル内のエントリ順によって、ユーザに表示されるブックマークの順序が定義されます。 • エントリを追加するには、[Add] ボタンをクリックし、[Add Bookmark Entry] ダイアログボックスに入力します（[ブックマークエントリの追加（Add Bookmark Entry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス （1984 ページ）を参照）。 • エントリを編集するには、エントリを選択し、[Edit] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[Delete] ボタンをクリックします。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[ブックマークエントリの追加（AddBookmarkEntry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス

[ブックマークエントリの追加（Add Bookmark Entry）] または [ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックスを使用して、SSL VPN ブックマークオブジェクトに含めるブックマークを作成または編集します。

ASA デバイスで使用するようにオブジェクトを設定している場合は、英語以外の非 ASCII 言語をブックマークに表示するテキストとして使用できます。SSL VPN ポータルをローカル言語で設定する方法の詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。

ナビゲーション パス

Policy Object Manager で、[Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （1982 ページ）から、[ブックマーク（Bookmarks）] テーブル内を右クリックし、次に [行の追加（Add Row）] を選択するか、行を右クリックして [行の編集（Edit Row）] を選択します。

関連項目

- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （1820 ページ）

フィールド リファレンス

表 *451 : [ブックマークエントリの追加（Add Bookmark Entry）]/[ブックマークエントリの追加（Edit Bookmark Entry）] ダイアログボックス*

要素	説明
Bookmark Option	新しい SSL VPN ブックマーク エントリを定義するか、または既存のオブジェクトのエントリを使用するかを選択します。 • [ブックマークの入力（Enter Bookmark）]：ブックマークエントリを定義します。 • [既存のブックマークを含める（Include Existing Bookmarks）]：既存の SSL VPN ブックマークオブジェクトで定義されているブックマークエントリを含めます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。 • [事前定義されたアプリケーションテンプレート（Predefined Application Templates）]：適切に定義された特定のアプリケーションに必要な値が事前に入力されている、事前定義されたテンプレートを使用します。
[自動サインオンアプリケーションを選択（Select Auto sign-on Application）]	[ブックマークオプション（Bookmark Option）] として [定義済みのアプリケーションテンプレート（Predefined Application Templates）] を選択した場合は、使用するテンプレートを含む自動サインオンアプリケーションを選択します。 • Citrix XenApp • Citrix XenDesktop • Domino Web Access • Microsoft Outlook Web Access 2010 • Microsoft Outlook Web Access 2013（ASA 9.4(1)+ のみ） • Microsoft SharePoint 2007 • Microsoft SharePoint 2010 • Microsoft SharePoint 2013（ASA 9.5(1)+ のみ） • Citrix StoreFront 2.1（ASA 9.3(1)+ のみ） • Citrix StoreFront 2.5（ASA 9.4(1)+ のみ） 自動サインオンアプリケーションを選択すると、選択したアプリケーションに基づいて [詳細なフォームとURLの設定（Advanced Form and URL Settings）] が入力されます。

要素	説明
タイトル	ユーザに表示される、ブックマークのテキスト ラベル。
URL	ブックマークの Universal Resource Locator アドレス。ブックマークのプロトコルを選択し、編集ボックスに URL の残りの部分を入力します。 **ヒント** ASA デバイスで使用するブックマークを作成し、デバイスに Kerberos の制約付き委任も設定する場合は、Service Principle Name（SPN）を URL に追加することが必要になる場合があります。詳細については、SSL VPN の Kerberos Constrained Delegation（KCD）の設定（ASA）（1799 ページ）を参照してください。
設定 これらの設定は、ソフトウェアバージョン 8.x を実行している ASA デバイスでホスティングされている SSL VPN ポータルに対してのみ適用可能です。これらの設定値は、他のデバイスで使用する SSL VPN ブックマーク オブジェクトには設定しないでください。	
Subtitle	ブックマーク エントリを説明する、ユーザに表示される追加のタイトル。
Thumbnail	ポータル上のブックマークに関連付けるアイコンを表すファイル オブジェクト。ファイルオブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
Authentication Access	[Portal] ページ上だけにサムネールを表示するかどうかを指定します。このオプションの選択を解除すると、このサムネールはログイン ページ上にも表示されます。
Enable Favorite URL Option	ポータル ホーム ページ上にブックマーク エントリを表示するかどうかを指定します。アプリケーション ページ上だけにブックマーク エントリを表示する場合は、このチェックボックスをオフにします。
[詳細なフォームとURLの設定（Advanced Form and URL Settings）] これらの設定は、ソフトウェアバージョン 8.x を実行している ASA デバイスでホスティングされている SSL VPN ポータルに対してのみ適用可能です。これらの設定値は、他のデバイスで使用する SSL VPN ブックマーク オブジェクトには設定しないでください。	

要素	説明
URL Method	リストから必要な URL メソッドを選択します。 • [Get]：このオプションは、単純なデータ取得を行う場合に選択します。 • [Post]：このオプションは、データを処理するときにデータ変更を伴う可能性がある場合（データの保存や更新、製品の購入、電子メールの送信など）に選択します。このオプションを選択した場合は、[Post Parameters] テーブルで Post パラメータを設定する必要があります。 • [自動サインオンフォーム（Auto Sign-on Form）]：自動サインオンを使用する場合は、このオプションを選択します。
Enable Smart Tunnel Option （Get および Post URL メソッドのみ）	セキュリティ アプライアンスとの間でデータを受け渡すスマートトンネル機能を使用する新しいウィンドウでブックマークを開くかどうかを指定します。
ページのプリロードオプション （Get および Post URL メソッドのみ）	必要に応じて、次のプリロードオプションを設定します。 [プリロードURL（Preload URL）]：ブックマークリンクがロードされる前にロードするページの URL。 [待機時間（Wait Time）]：実際の POST URL に転送される前に、ページのロードに費やすことのできる時間。
[自動サインオン（Auto Sign-on）]（ASA 9.0.1+ のみ） （自動サインオンフォーム URL メソッドのみ）	自動サインオンフォームが URL メソッドとして選択されている場合は、次のオプションを設定します。 （注） 次のフィールドに入力する URL では、ワイルドカードを使用できます。たとえば、http*://www.example.com/myurl* と入力します。 [ログインページのURL（Login Page URL）]：自動サインオンするログインページの URL。 [ランディングページのURL（Landing Page URL）]：ログインに成功した後に読み込まれるページの URL。ASA では、アプリケーションへの正常なログインを検出するために、ランディング ページを設定する必要があります。 [ログイン前のページのURL（Pre-Login Page URL）]：ログインページの前にロードされるページの URL。このページには、ログイン画面に進むためのユーザー インタラクションが必要になります。 [制御ID（Control ID）]：ログインページに進む前にログイン前のページの URL でクリックイベントを取得する制御/タグの ID です。

要素	説明
Post Parameters	ブックマーク エントリの Post パラメータの名前と値のリスト。 • パラメータを追加するには、[Add] ボタンをクリックし、[Add Post Parameter] ダイアログボックスに入力します（[Add Post Parameter]/[Edit Post Parameter] ダイアログボックス （1988 ページ）を参照）。 • パラメータを編集するには、パラメータを選択し、[Edit] ボタンをクリックします。 • パラメータを削除するには、パラメータを選択し、[Delete] ボタンをクリックします。
[ポストスクリプト（Post Script）]	一部のアプリケーションで必要な javascript を入力するためのオプションのフィールド。Microsoft Outlook Web Access などの一部の Web アプリケーションは、JavaScript を実行して、ログイン フォームを送信する前に、要求パラメータを変更する場合があります。

[Add Post Parameter]/[Edit Post Parameter] ダイアログボックス

[Add Post Parameter]/[Edit Post Parameter] ダイアログボックスを使用して、新しい Post パラメータ エントリを作成するか、またはテーブル内の既存のエントリを編集します。Post パラメータの詳細については、SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （1820 ページ）を参照してください。

ナビゲーション パス

Policy Object Manager で、[Add Bookmarks]/[Edit Bookmarks] ダイアログボックス （1982 ページ）から、[ポストパラメータ（Post Parameters）] テーブル内を右クリックし、[行の追加（Add Row）] を選択するか、または行を右クリックしてから [行の編集（Edit Row）] を選択します。

関連項目

- ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）
- SSL VPN ブックマークでの Post URL 方式およびマクロ置換の使用 （1820 ページ）

フィールド リファレンス

表 *452 : [Add Post Parameter]/[Edit Post Parameter]* ダイアログボックス

要素	説明
名前	対応する HTML 形式で定義されているのと厳密に同じ post パラメータの名前。たとえば、 **param_name** in <input name="*param_name* " value="*param_value* ">。

要素	説明
値	

要素	説明
	対応する HTML 形式で定義されているのと厳密に同じ post パラメータの値。たとえば、**param_value** in <input name="*param_name* " value="*param_value* ">。 次のいずれかを選択します。 • CSCO_WEBVPN_USERNAME：SSL VPN ユーザのログイン ID。 • CSCO_WEBVPN_PASSWORD：SSL VPN ユーザのログインパスワード。 • CSCO_WEBVPN_INTERNAL_PASSWORD：SSL VPN ユーザの内部リソースパスワード。キャッシュされた認定証であり、AAA サーバーによって認証されていません。ユーザーがこの値を入力すると、パスワード値の代わりに、これが自動サインオンのパスワードとして使用されます。 • CSCO_WEBVPN_CONNECTION_PROFILE：SSL VPN ユーザー ログイン グループ ドロップダウン、接続プロファイル内のグループ エイリアス • CSCO_WEBVPN_DYNAMIC_URL1：ユーザのポータルで複数のブックマークリンクを生成できる単一のブックマーク。このマクロはデリミタをオプションで使用します。デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • CSCO_WEBVPN_DYNAMIC_URL2：ユーザのポータルで複数のブックマークリンクを生成できる単一のブックマーク。このマクロはデリミタをオプションで使用します。デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。 • CSCO_WEBVPN_MACRO1：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value1 になります。RADIUS 経由での変数置換は、VSA#223 によって行われます。 • CSCO_WEBVPN_MACRO2：RADIUS-LDAP ベンダー固有属性によって設定。ldap-attribute-map を経由して LDAP からこれをマッピングする場合は、この変数を使用するシスコの属性は WEBVPN-Macro-Substitution-Value2 になります。RADIUS 経由での変数置換は、VSA#224 によって行われます。 • CSCO_WEBVPN_MACROLIST1 および CSCO_WEBVPN_MACROLIST2：静的に設定されたブックマーク。LDAP 属性マップによって提供される任意のサイズのリストを使用できます。 これらのマクロは、次の 3 つのパラメータを使用します。 • デリミタ：デリミタは管理者によって提供される文字列です。この文字列の文字を使用して LDAP にマッピングされた文字列を区切り、値のリストにします。マクロの使用ごとに 1 つのデリミタが使用されます。

要素	説明
	• インデックス：インデックスは管理者によって提供される整数で、選択する要素の番号を指定します。値の範囲は 1 ～ 128 です。 • URL エンコーディング：URL エンコーディングは、ASA デバイスの要求に置き換える前に LDAP 文字列に適用する条件選択肢です。次のいずれかの値を選択できます。 • None：バックエンドサーバーへの送信前に、文字列値に対して変換を行いません。 • url-encode：解析された各値はエンコードされた URL になります。ただし、URL で特殊文字列を構成する一連の予約済み文字は除外されます。 • url-encode-data：解析された各値は、URL エンコードで完全に変換されます。 • base64：解析された各値は Base 64 で符号化されます。 • CSCO_WEBVPN_PRIMARY_USERNAME：二重認証が有効で、ログイン ID にプライマリログインユーザー名がある場合のプライマリユーザーログイン ID。 • CSCO_WEBVPN_SECONDARY_USERNAME：二重認証が有効になっている場合のセカンダリユーザのログイン ID。 • CSCO_WEBVPN_PRIMARY_PASSWORD：二重認証用のプライマリユーザのログインパスワード。 • CSCO_WEBVPN_SECONDARY_PASSWORD：二重認証用のセカンダリユーザのログイン ID。

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックスを使用して、SSL VPN カスタマイゼーション オブジェクトを作成、コピー、および編集します。SSL VPN カスタマイゼーション ポリシー オブジェクトでは、ASA 8.x デバイス上でホスティングされているブラウザベースのクライアントレス SSL VPN の Web ページをカスタマイズする方法について説明します。詳細については、次を参照してください。

ASA デバイスおよび IOS デバイスの SSL VPN ブックマーク リストの設定 （1818 ページ）

英語以外の非 ASCII 言語を、これらのページ上に表示するテキストに使用できます。SSL VPN ポータルをローカル言語で設定する方法の詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクトタイプセレクタから [SSL VPN カスタマイゼーション（SSL VPN Customization）] を選択します。作業領域内を右クリックしてから [新規オブジェクト(New Object] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）
- ASA デバイスの独自 SSL VPN ログイン ページの作成 （1817 ページ）

フィールド リファレンス

表 *453 : [Add SSL VPN Customization]/[Edit SSL VPN Customization]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ） を参照してください。
説明	（任意）オブジェクトの説明。
[Settings] ペイン ダイアログボックスの本体は左右に分割されたペインであり、左側にはコンテンツ テーブル、右側にはコンテンツ テーブルで選択された項目に関連する設定が表示されます。設定値を設定する前に、[Preview] ボタンをクリックしてデフォルト設定を表示すると、何を変更する必要があるかを（変更する必要がある場合）判断するのに役立ちます。 コンテンツ テーブルの上部にあるフォルダは、次に説明するカスタマイズ可能な SSL VPN Web ページを表します。	

要素	説明
ログイン ページ	[Logon] Web ページは、ユーザが SSL VPN ポータルに接続するときに最初に表示されるページです。VPN へのログインに使用されます。コンテンツ テーブル内の [Logon Page] フォルダの次の項目を選択して、設定を表示および変更します。 • [ログオンページ（Logon Page）]：[ブラウザウィンドウのタイトル（Browser Window Title）] フィールドで、ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。 • [タイトルパネル（Title Panel）]：Web ページ自体に表示されるタイトル。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel] （1996 ページ）を参照してください。 • [言語（Language）]：[ログオン（Logon）]、[ポータル（Portal）]、および [ログアウト（Logout）] の各ページでサポートされる言語。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Language] （1997 ページ）を参照してください。 • [ログオンフォーム（Logon Form）]：ユーザーのログイン情報を受け取る形式で使用されるラベルと色。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logon Form] （2000 ページ）を参照してください。 • [情報パネル（Informational Panel）]：ユーザーに情報を伝えるための追加情報パネル。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Informational Panel] （2001 ページ）を参照してください。 • [著作権パネル（Copyright Panel）]：ログインページ上の著作権情報。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Copyright Panel] （2002 ページ）を参照してください。 • [フルカスタマイズ（Full Customization）]：セキュリティアプライアンスの組み込みログインページを使用しない（カスタマイズもしない）場合は、代わりにフルカスタマイズをイネーブルにして独自の Web ページを指定できます。カスタムの [Logon] ページの作成および設定の詳細については、ASA デバイスの独自 SSL VPN ログイン ページの作成 （1817 ページ）および [SSL VPN Customization] ダイアログボックス - [Full Customization] （2003 ページ）を参照してください。

要素	説明
ポータル ページ	[Portal] Web ページは、ユーザが SSL VPN にログインしたあとに表示されるページ、つまり、ホーム ページです。コンテンツ テーブル内の [Portal Page] フォルダの次の項目を選択して、設定を表示および変更します。 • [ポータルページ（Portal Page）]：[ブラウザウィンドウのタイトル（Browser Window Title）] フィールドで、ブラウザのタイトルバーに表示される、Web ページのタイトルを定義します。 • [タイトルパネル（Title Panel）]：Web ページ自体に表示されるタイトル。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Title Panel] （1996 ページ）を参照してください。 • [ツールバー（Toolbar）]：[ポータル（Portal）] ページの主要部分の上に表示されるツールバー。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Toolbar] （2004 ページ）を参照してください。 • [アプリケーション（Applications）]：ページ上に表示されるアプリケーションボタン。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Applications] （2005 ページ）を参照してください。 • [カスタムペイン（Custom Panes）]：[ポータル（Portal）] ページの主要部分のレイアウト。デフォルトは、内部ペインのない 1 カラム型のページです。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Custom Panes] （2006 ページ）を参照してください。 • [ホームページ（Home Page）]：URL リストをホームページ上に表示する方法および表示するかどうかを指定します。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Home Page] （2009 ページ）を参照してください。
\[Logout\] ページ	[Logout] Web ページは、SSL VPN をログアウトしたあとに表示されるページです。設定の詳細については、[SSL VPN Customization] ダイアログボックス - [Logout Page] （2010 ページ）を参照してください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイスレベルでのオブジェクト定義の変更を許可するかどうか。ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[Overrides] フィールドは、このオブジェクトに対するオーバーライドを持つデバイスの数を示します。

[SSL VPN Customization] ダイアログボックス - [Title Panel]

[SSL VPN Customization] ダイアログボックスの [Title Panel] ページを使用して、[Logon] ページまたは [Portal] ページで、Web ページ自体にタイトルを表示するかどうかを決定します。タイトル パネルをイネーブルにすると、使用するタイトル、フォント、フォント サイズとフォントの太さ、スタイル、および色を指定できます。ロゴのグラフィックを識別するファイル オブジェクトを選択することもできます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）のコンテンツテーブルで、[ログオンページ（Logon Page）] > [タイトルパネル（Title Panel）] を選択して [ログオン（Logon）] ページのタイトルを設定するか、または [ポータルページ（Portal Page）] > [タイトルパネル（Title Panel）] を選択して [ポータル（Portal）] ページのタイトルを設定します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）

フィールド リファレンス

表 454 : [SSL VPN Customization] ダイアログボックス - [Title Panel]

要素	説明
Display Title Panel	タイトル パネルを Web ページ内に表示するかどうかを指定します。デフォルトでは、タイトルは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してタイトルを設定できます。
Gradient	背景色が徐々に変化するかどうかを指定します。

要素	説明
Title Text	タイトル パネルに表示するテキスト。
Font Weight フォントサイズ Font Color	タイトル テキストに使用するフォントの特性。太さ、フォント サイズ、および色を選択できます。[選択（Select）] をクリックしてフォントの色を選択します。
背景色（Background Color）	タイトル パネルの背景色。[選択（Select）] をクリックして色を選択します。
Style (CSS)	タイトル パネルのスタイル特性を定義する Cascading Style Sheet（CSS）パラメータ。最大 256 文字を使用できます。 **ヒント** CSS の詳細については、World Wide Web Consortium（W3C）の Web サイト（www.w3.org）を参照してください。
Logo Image	タイトル パネルに含めるロゴ イメージ（ある場合）を識別するファイル ポリシー オブジェクト。ファイル オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** イメージ ファイルとして、GIF、JPG、または PNG ファイルを使用できます。ファイルのサイズは最大 100 KB です。 ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。

[SSL VPN Customization] ダイアログボックス - [Language]

[SSL VPN Customization] ダイアログボックスの [Language] ページを使用して、ブラウザベースのクライアントレス SSL VPN ポータルでサポートする言語を指定します。ASA デバイスで他の言語の変換テーブルを設定して使用するには、サポートされる言語を設定し、ユーザが自分の言語を選択できるようにします。これらの設定を設定する前に、次を参照してください。

ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）の目次で **[ログオン（Logon）] ページ > [言語（Language）]** を選択します。

関連項目

- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）
- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 *455 : [SSL VPN Customization] ダイアログボックス - [Language]*

要素	説明
Automatic Browser Language Selection	このテーブルには、ブラウザ言語自動選択用に Web ページでサポートする言語が示されます。ブラウザ言語自動選択を使用すると、ASA デバイスは、ユーザーの Web ブラウザとネゴシエートして、Web ページで表示する言語を決定できます。ここで指定するすべての言語について、ASA デバイス上で変換テーブルを設定する必要があります。ブラウザ言語自動選択の詳細については、ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。 言語は、短縮形でテーブル内に示されます。言語は、一致が検出されるまで、上から下に評価されます。デフォルト言語として示されている言語（テーブルで True として示されている）は、デバイスがブラウザとは異なる言語でネゴシエートできなかった場合に使用されます。デフォルトを指定しない場合、英語がデフォルトになります。 • 言語を追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • 言語を編集するには、言語を選択し、[Edit Row] ボタンをクリックします。 • 言語を削除するには、言語を選択し、[Delete Row] ボタンをクリックします。
Enable Language Selector	[Logon] ページで [Language Selector] を表示するかどうかを指定します。[Language Selector] によって、ユーザは優先する言語を選択できます。[Language Selector] は、ブラウザ言語自動選択機能を補完します。
Language Selector Prompt	[Language Selector] プロンプトのテキスト ラベル。

要素	説明
Language Table	[Language Selector] ドロップダウン リストに含める言語のリスト。ここで指定するすべての言語について、ASA デバイス上で変換テーブルを設定する必要があります。詳細については、 ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）を参照してください。 このテーブルには、短縮形による言語および言語タイトル、または言語の共通名が示されます。タイトルは、ドロップダウン リストに表示されるテキストです。言語タイトルは変更できますが、短縮形は変更できません。 • 言語を追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • 言語を編集するには、言語を選択し、[Edit Row] ボタンをクリックします。 • 言語を削除するには、言語を選択し、[Delete Row] ボタンをクリックします。

[Add Language]/[Edit Language] ダイアログボックス

[Add Language]/[Edit Language] ダイアログボックスを使用して、ブラウザ言語自動選択または [Language Selector] ドロップダウン リストでサポートする言語のエントリを追加または編集します。

ナビゲーション パス

[SSL VPN Customization] ダイアログボックス - [Language] （1997 ページ）ページで、[ブラウザ言語自動選択（Automatic Browser Language Selection）] テーブルと [言語セレクタ（Language Selector）] テーブルのいずれかの [行の追加（Add Row）] ボタンをクリックするか、または行を選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）
- ASA デバイスの SSL VPN Web ページのローカライズ （1815 ページ）

フィールド リファレンス

表 *456 : [Add Language]/[Edit Language]* ダイアログボックス

要素	説明
Language	ブラウザベースのクライアントレス SSL VPN Web ページでサポートされる言語のリスト。短縮形で示されます。

要素	説明
デフォルト （[Automatic Browser Language Selection] のみ）	ポータルのデフォルト言語として言語を定義するかどうかを指定します。デフォルト言語は、ASA デバイスが、クライアントのブラウザの言語とネゴシエートできない場合に使用されます。
タイトル （[Language Selector] のみ）	[Logon] ページ上の [Language Selector] に表示される言語の名前。

[SSL VPN Customization] ダイアログボックス - [Logon Form]

[SSL VPN Customization] ダイアログボックスの [Logon Form] 設定を使用して、ログイン ボックスのタイトル、[SSL VPN]ページのログインプロンプト（ユーザ名、パスワード、グループの各プロンプトなど）、ログインボタン、およびブラウザベースのクライアントレス SSL VPN ユーザが最初にセキュリティ アプライアンスに接続したときに表示されるログイン ボックスのスタイル要素をカスタマイズします。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）の目次で [ログオン（Logon）] ページ > [ログオンフォーム（Logon Form）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 457 : [SSL VPN Customization] ダイアログボックス - [Logon] ページ

要素	説明
Title	ログイン ボックスのタイトルとして表示されるテキスト。
メッセージ	ユーザ名フィールドとパスワードフィールドの上のログインボックスに表示されるメッセージ。最大 256 文字を入力できます。
Username Prompt	ユーザ名エントリ フィールドのプロンプトのテキスト。
パスワード プロンプト	パスワード エントリ フィールドのプロンプトのテキスト。

要素	説明
Secondary Username Prompt Secondary Password Prompt	2 つのログイン クレデンシャルが必要な場合の、2 番めのユーザ名とパスワードのプロンプト。接続プロファイル ポリシーがセカンダリ認証を必要とするように設定されている場合にだけ、セカンダリ認証をイネーブルにできます。 ユーザ名とパスワードのセカンダリ プロンプトは、これらを設定している場合にだけ表示されます。ユーザ名プロンプトを空白のままにすると、プライマリ ユーザ名が使用され、セカンダリ パスワードはプライマリ ユーザ名と関連付けられている必要があります。
Internal Password Prompt	内部パスワード エントリ フィールドのプロンプトのテキスト。
Show Internal Password First	内部パスワードのプロンプトをパスワードプロンプトの上に配置するかどうかを指定します。内部パスワードは、保護されている内部 Web サイトへのアクセスにクライアントレス SSL VPN を使用する場合に必要です。
Group Selector Prompt	[Group Selector] ドロップダウン リストのプロンプトのテキスト。
Button Text	ユーザが SSL VPN にログインするためにクリックするボタンの名前。
Border Color	ログイン ボックスの枠の色。[選択（Select）] をクリックして色を選択します。
Title Font Color	ログイン ボックス タイトルのフォントの色。[選択（Select）] をクリックして色を選択します。
Title Background Color	ログイン ボックスのタイトル部分の背景色。[選択（Select）] をクリックして色を選択します。
Font Color	ログイン フォームのフォントの色。[選択（Select）] をクリックして色を選択します。
背景色（Background Color）	ログイン フォームの背景色。[選択（Select）] をクリックして色を選択します。

[SSL VPN Customization] ダイアログボックス - [Informational Panel]

[SSL VPN Customization] ダイアログボックスの [Informational Panel] ページを使用して、[Logon] ページの情報パネルの外観をカスタマイズします。情報パネルは、ユーザに追加情報を提供できる領域であり、オプションです。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）の目次で **[ログオン（Logon）] ページ > [情報パネル（Informational Panel）]** を選択します。

関連項目

- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 458 : [SSL VPN Customization] ダイアログボックス - [Informational Panel]

要素	説明
Display Informational Panel	情報パネルを表示するかどうかを指定します。デフォルトでは、情報パネルは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してパネルを設定できます。
Panel Position	情報パネルの位置。[Logon] ボックスの左または右のいずれかです。
テキスト（Text）	情報パネルに表示されるテキスト。最大 256 文字を入力できます。
Logo Image	情報パネルに含めるロゴイメージ（ある場合）を識別するファイル ポリシー オブジェクト。ファイルオブジェクトの名前を入力するか、または[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 **ヒント** イメージ ファイルとして、GIF、JPG、または PNG ファイルを使用できます。ファイルのサイズは最大 100 KB です。 ファイル オブジェクトの詳細については、[Add File Object]/[Edit File Object] ダイアログボックス （1972 ページ）を参照してください。
Image Position	パネルでのロゴ イメージの位置。テキストの上または下のいずれかです。

[SSL VPN Customization] ダイアログボックス - [Copyright Panel]

[SSL VPN Customization] ダイアログボックスの [Copyright Panel] ページを使用して、[Logon] ページの [Copyright] パネルの外観をカスタマイズします。[Copyright] パネルは、著作権情報を提供し、ページの下に表示されるオプションのパネルです。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）のコンテンツテーブルで **[ログインページ（Logon Page）] > [著作権パネル（Copyright Panel）]** を選択します。

関連項目

- [Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）
- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 *459 : [SSL VPN Customization] ダイアログボックス - [Copyright Panel]*

要素	説明
Display Copyright Panel	[Copyright] パネルを表示するかどうかを指定します。デフォルトでは、情報パネルは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してパネルを設定できます。
テキスト（Text）	著作権パネルに表示されるテキスト。最大 256 文字を入力できます。

[SSL VPN Customization] ダイアログボックス - [Full Customization]

[SSL VPN Customization] ダイアログボックスの [Full Customization] ページを使用して、独自のカスタム [Logon] ページを指定します。このダイアログボックスで使用可能な [Logon] ページ設定が、カスタム ページに置き換えられます。カスタム [Logon] ページの作成の詳細については、 ASA デバイスの独自 SSL VPN ログイン ページの作成 （1817 ページ）を参照してください。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）のコンテンツテーブルで、[ログイン（Logon）] ページ > [フルカスタマイズ（Full Customization）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 460 : [SSL VPN Customization] ダイアログボックス - [Full Customization]

要素	説明
Enable Full Customization	独自のカスタム [Logon] ページを使用するかどうかを指定します。フルカスタマイズをイネーブルにすると、[Logon] ページのその他のすべての設定が無視されます。
Custom Page	カスタム [Logon] ページ。ファイルをここで指定する前に、Security Manager サーバにファイルをコピーする必要があります。[参照（Browse）] をクリックしてファイルを選択します。ファイルの選択の詳細については、Cisco Security Manager でのファイルまたはディレクトリの選択または指定 （67 ページ）を参照してください。

[SSL VPN Customization] ダイアログボックス - [Toolbar]

[SSL VPN Customization] ダイアログボックスの [Toolbar] ページを使用して、[Portal] ページのツールバーの外観をカスタマイズします。ツールバーは、[Portal] ページの本体の上に表示され、ユーザがブラウズする URL を入力できるフィールドがあります。このツールバーはオプションです。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）のコンテンツテーブルで **[ポータルページ（Portal Page）] > [ツールバー（Toolbar）]** を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 461 : [SSL VPN Customization] ダイアログボックス - [Toolbar]

要素	説明
Display Toolbar	ツールバーを表示するかどうかを指定します。デフォルトでは、ツールバーは表示されません。このオプションを選択した場合、このページの他のフィールドを使用してツールバーを設定できます。
Prompt Box Title	ユーザがターゲット Web ページのプロトコルを選択し、URL を入力するフィールド用のプロンプトのテキスト。

要素	説明
Browse Button Text	ターゲット URL に移動するためにユーザがクリックするボタンの名前。
Logout Prompt	SSL VPN からのログアウト用のプロンプトのテキスト。
ユーザープロンプト（User Prompt）（ASA 9.7.1+ のみ）	現在リモートアクセス VPN にログインしているユーザーに対するプロンプトのテキスト。

[SSL VPN Customization] ダイアログボックス - [Applications]

[SSL VPN Customization] ダイアログボックスの [Applications] ページを使用して、[Portal] ページに表示されるアプリケーション リンクをカスタマイズします。このページには、SSL VPN ポータル ページの左側のナビゲーション パネルに表示できるすべてのアプリケーション リンクが示されます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）から、コンテンツテーブルで [ポータルページ（Portal Page）] > [アプリケーション（Applications）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 462 : [SSL VPN Customization] ダイアログボックス - [Applications]

要素	説明
番号 [Move Up]/[Move Down] ボタン（テーブルの下）	テーブル内のアプリケーションの連続番号。アプリケーションの並び順を変更するには、アプリケーションを選択し、[Move Up]/[Move down] ボタンをクリックして、目的の位置に移動します。アプリケーションは、ここで示されている順序で [Portal] ページに表示されます。
Application	アプリケーションに関連付けられているグラフィック。

要素	説明
タイトル	アプリケーションの名前。標準のアプリケーションには、[Home]、[Web Applications]、[Browse Networks]、[Application Access]、および [AnyConnect Client] が含まれています。また、SSL VPN グローバル設定値の設定時に作成するブラウザプラグインもリストされており、このページでの選択に使用することもできます。 タイトルをダブルクリックして編集可能な状態にして、この名前を変更できます。
有効	アプリケーションを [Portal] ページに含めるかどうかを指定します。
ナビゲーションパネルの表示	ポータルページにナビゲーションパネルを表示するかどうか。このオプションの選択を解除すると、アプリケーションのリストはポータルに表示されません。

[SSL VPN Customization] ダイアログボックス - [Custom Panes]

[SSL VPN Customization] ダイアログボックスの [Custom Panes] ページを使用して、[Portal] ページ本体の外観をカスタマイズします。カスタム ペインを作成し、カラム レイアウトを指定して、エンド ユーザへのポータル情報の効率的な表示に役立つ情報グリッドを作成できます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）のコンテンツテーブルで [ポータルページ（Portal Page）] > [カスタムペイン（Custom Panes）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 463 : [SSL VPN Customization] ダイアログボックス - [Custom Panes]

要素	説明
[Columns] テーブル	[Portal] ページの本体が分割されるカラムのリスト。ページ幅のパーセンテージに基づいてカラムを定義します。パーセンテージは、100 まで追加できます。100 まで追加しない場合、デバイスによってカラム幅が調整されます。 [Portal] ページに表示する、左から右のカラムを作成します。 • カラムを追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • カラムを編集するには、カラムを選択して [Edit Row] ボタンをクリックします。 • カラムを削除するには、カラムを選択して [Delete Row] ボタンをクリックします。
[Custom Panes] テーブル	[Portal] ページの本体に表示されるカスタム ペイン。このテーブルには、ペインの表示がイネーブルであるかどうか、ペインのタイプ、その特性、およびページ上でペインが表示されるカラムおよび行が示されます。これらのペインには、プレーンテキストを表示するか、またはHTML の URL、イメージ、または RSS リンクを含めることができます。 設定の詳細については、[Add Custom Pane]/[Edit Custom Pane] ダイアログボックス （2008 ページ）を参照してください。 • カスタム ペインを追加するには、テーブルの下にある [Add Row] ボタンをクリックします。 • カスタム ペインを編集するには、カスタム ペインを選択して [Edit Row] ボタンをクリックします。 • カスタムペインを削除するには、カスタム ペインを選択して [Delete Row] ボタンをクリックします。

[Add Column]/[Edit Column] ダイアログボックス

[Add Column]/[Edit Column] ダイアログボックスを使用して、ブラウザベースのクライアントレス SSL VPN の [Portal] ページ本体のカラムを作成または編集します。合計領域のパーセンテージとして、目的のカラム幅を [Percentage] フィールドに入力します。

ナビゲーション パス

[SSL VPN Customization] ダイアログボックス - [Custom Panes] （2006 ページ）ページで、[カラム（Column）] テーブルの 行の追加（Add Row）] ボタンをクリックするか、カラムを選択して [行の編集（Edit Row）] ボタンをクリックします。

[Add Custom Pane]/[Edit Custom Pane] ダイアログボックス

[Add Custom Pane]/[Edit Custom Pane] ダイアログボックスを使用して、ブラウザベースのクライアントレス SSL VPN の本体または [Portal] ページに表示されるペインを作成または編集します。

ナビゲーション パス

[SSL VPN Customization] ダイアログボックス - [Custom Panes] （2006 ページ）ページで、[カスタムペイン（Custom Pane）] テーブルの [行の追加（Add Row）] ボタンをクリックするか、またはペインを選択してから [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *464 : [Add Custom Pane]/[Edit Custom Pane]* ダイアログボックス

要素	説明
有効化（Enable）	[Portal] ページ上にカスタム ペインを表示するかどうかを指定します。
タイプ（Type）	ペインに表示するコンテンツのタイプ。次のいずれかになります。 • [Text]：プレーン テキスト。HTML マーク アップを含めることができます。 • [HTML]：URL で提供される HTML コンテンツ。 • [Image]：URL で提供されるイメージ。 • [RSS]：URL で提供される RSS フィード。
タイトル表示 タイトル	タイトルをペインに表示するかどうかを指定します。このオプションを選択した場合は、タイトルを [Title] フィールドに入力します。
Show Border	ペインを囲む枠を表示するかどうかを指定します。
列 行	ペインで表示するカラムおよび行の番号。それぞれの番号を選択または入力して、目的のグリッド位置を指定します。
高さ	ペインの高さ（ピクセル単位）。
URL （HTML、イメージ、および RSS コンテンツのみ）	ペインに表示するコンテンツをホスティングする URL。

要素	説明
テキスト（Text） （テキストコンテンツのみ）	ペインに表示するテキスト。HTML マーク アップをテキストに含めることができます。

[SSL VPN Customization] ダイアログボックス - [Home Page]

[SSL VPN Customization] ダイアログボックスの [Home Page] ページを使用して、[Portal] ページ上の URL とファイル リストの外観、および [Portal] ページ本体のコンテンツをカスタマイズします。URL リストは、明示的にディセーブルにしている場合を除き、ポータル ホーム ページのデフォルト要素と見なされます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）の目次で **[ポータルページ（Portal Page）] > [ホームページ（Home Page）]** を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 465 : [SSL VPN Customization] ダイアログボックス - [Home Page]

要素	説明
Enable Custom Intranet Web Page	カスタム イントラネット Web ページを表示するかどうか（表示すると、URL ブックマークも [Portal] ページに表示されます）を指定します。このオプションを選択した場合、このページの他のフィールドを使用してパネルを設定できます。
URL List Mode	URL リストをホーム ページに表示する方法。URL リストを表示する場合、カスタム ペイン（[Portal Page] > [Custom Panes] で設定）が使用していないカラム セルに表示されます。次のオプションがあります。 • [アプリケーション別グループ（Group By Application）]：ブックマークはアプリケーションタイプ別にグループ化されます。たとえば、Web ブックマーク、ファイル ブックマークです。 • [グループなし（No Group）]：URL リストが別々のペインに表示されます。 • [表示しない（Do Not Display）]：URL リストは表示されません。

要素	説明
Custom Intranet Web Page URL	ホーム ページとしてロードするカスタム Web ページの URL。このページは、[Portal] ページ本体に表示されます。 カスタム ページを指定すると、[Custom Panes] ページの設定は無視され、ブックマーク リストが、[Portal] ページの左側のナビゲーション パネルからアクセスするアプリケーション ページ上に表示されます。

[SSL VPN Customization] ダイアログボックス - [Logout Page]

[SSL VPN Customization] ダイアログボックスの [Logout Page] ページを使用して、ブラウザベースのクライアントレス SSL VPN の [Logout] ページの外観をカスタマイズします。この [Logout] ページは、ユーザが VPN からログアウトしたあとに表示されます。

ナビゲーション パス

[Add SSL VPN Customization]/[Edit SSL VPN Customization] ダイアログボックス （1992 ページ）から、コンテンツテーブルの [ログアウトページ（Logout Page）] を選択します。

関連項目

- SSL VPN カスタマイゼーション オブジェクトを使用した ASA ポータル表示の設定 （1811 ページ）

フィールド リファレンス

表 466 : [SSL VPN Customization] ダイアログボックス - [Logout Page]

要素	説明
Title	タイトル パネルに表示するテキスト。
テキスト（Text）	[Logout] ページに表示するメッセージ。[Preview] をクリックして、デフォルトのログアウト メッセージを確認します。最大 256 文字を入力できます。
Show Login Button Login Button Text	[Login] ボタンをページに表示するかどうかを指定します。このボタンを表示すると、ユーザは簡単にポータルにログインし直すことができます。 このボタンをイネーブルにすると、[Login Button Text] フィールドでボタンの名前を指定できます。
Border Color	ログアウト ボックスを囲む枠の色。[選択（Select）] をクリックして色を選択します。

要素	説明
Title Font Color Title Background Color	ページのタイトル領域のフォントおよび背景の色。[選択（Select）] をクリックして色を選択します。
Font Color 背景色（Background Color）	ログアウト ボックスに表示されるメッセージのフォントおよび背景の色。[選択（Select）] をクリックして色を選択します。

[Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス

[Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックスを使用して、SSL VPN ゲートウェイ オブジェクトを作成、コピー、および編集します。これらのオブジェクトは、IOS デバイスで SSL VPN 接続を設定するときに使用します。詳細については、SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） （1699 ページ）を参照してください。

SSL VPN ゲートウェイは、リモート デバイス上の Web 対応ブラウザとの間の SSL 暗号化接続を介してアクセスされる、保護されたリソースへの接続のプロキシとして機能します。SSL VPN ごとに 1 つのゲートウェイだけを設定できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [SSL VPNゲートウェイ（SSL VPN Gateway）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- SSL VPN Configuration ウィザード：[Gateway and Context] ページ（IOS） （1699 ページ）
- [General] タブ （1911 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 467 : [Add SSL VPN Gateway]/[Edit SSL VPN Gateway] ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）最大 1024 文字のオブジェクトの説明。

要素	説明
IPアドレス	ゲートウェイの IP アドレス。リモート ユーザが接続するアドレスです。 • [静的IPアドレスを使用（Use Static IP Address）]：使用するアドレスを指定します。このアドレスは、ルータのインターフェイスでも設定する必要があります。 • [インターフェイスから取得（Obtained from Interface）]：デバイス上の単一インターフェイスに解決されるインターフェイスロールを指定します。インターフェイスに設定されている IP アドレスが使用されます。このオプションを使用すると、明示的に IP アドレスを入力しなくても、接続に使用する外部インターフェイスを指定できます。インターフェイス上のアドレスを変更する必要がある場合でも、このオブジェクトを再設定する必要はありません。
[ポート（Port）]	HTTPS トラフィックを伝送するポートの番号。単一のポート番号を指定するポートリストオブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択することもできます。デフォルトは HTTPS オブジェクトであり、ポート 443 が指定されます。ポート 443 を使用しない場合、1025 ～ 65535 の範囲の別のポート番号を入力できます。
Trustpoint	セキュアな接続を確立するために必要なデジタル証明書。SSL VPN ゲートウェイがアクティブな場合は、自己署名証明書が生成されます。
Enable Gateway	SSL VPN ゲートウェイをアクティブにするかどうかを指定します。
Specify SSL Encryption Algorithms	接続に使用する暗号化アルゴリズムを制限するかどうか、または別の使用順を指定するかどうかを指定します。デフォルトでは、すべてのアルゴリズムを、3DES と SHA1、AES と SHA1、RC4 と MD5 の順で使用可能にします。 アルゴリズム優先順位を選択します。1 つまたは 2 つのアルゴリズムを削除するには、[None] を選択します。
Redirect HTTP Traffic HTTP ポート（HTTP Port）	ゲートウェイが、セキュア HTTP（HTTPS）経由で HTTP トラフィックをリダイレクトするかどうかを指定します。このポートに着信するトラフィックは、[Port] フィールドで指定したポートにリダイレクトされます。 HTTP トラフィックのポート番号を [HTTPポート（HTTP Port）] フィールドに入力します。ポートリストオブジェクトの番号または名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。 通常、HTTP ポートは 80 です。ただし、ネットワークで使用されているその他の任意の番号（1025 ～ 65535）を入力できます。

要素	説明
ホストネーム	ゲートウェイのホスト名。 • [Do Not Specify]：ホスト名は割り当てられません。ゲートウェイの IP アドレスが使用されます。 • [デバイスのホストとドメインの名前を使用（Use the host and domain names of the device）]：これらの名前は、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）] ポリシーで定義されています。 • [Use the Object]：ホスト名は、テキスト ポリシー オブジェクトで定義されている値です。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス

[Add Smart Tunnel Lists]/[Edit Smart Tunnel Lists] ダイアログボックスを使用して、SSL VPN スマート トンネル オブジェクトを作成、コピー、および編集します。

SSL VPN スマート トンネル リストには、プライベート サイトへのスマート トンネル アクセスに適格なアプリケーションが示されます。スマート トンネル リストを使用して、ユーザが SSL VPN ポータル経由で指定のアプリケーションにアクセスできるように、ASA グループ ポリシーのクライアントレス設定値を設定できます。スマート トンネル アクセスをサポートするアプリケーションのタイプについては、 ASA デバイスの SSL VPN スマート トンネルの設定（1821 ページ）を参照してください。

その他の SSL VPN スマート トンネル リスト オブジェクトをオブジェクトに含めることができます。このため、アプリケーションの基本的なリストを指定する小さなオブジェクト セットを

作成してから、必要なアプリケーションの組み合わせを作成するその他のオブジェクトを作成できます。たとえば、アプリケーション A と B へのスマート トンネル アクセスを 3 つの ASA グループ ポリシーすべてに対して許可し、その他のアプリケーションはグループごとに一意にする場合があります。A と B を指定する単一オブジェクトを作成して、そのオブジェクトをグループ ポリシーの各 SSL VPN スマート トンネル リスト オブジェクトに含めることができます。これらのオブジェクトで必要となるのは、それぞれの一意のアプリケーションをアプリケーション テーブルで指定することだけです。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SSL VPN スマートトンネルリスト（SSL VPN Smart Tunnel Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 468 : [Add Smart Tunnel Lists]/[Edit Smart Tunnel Lists] ダイアログボックス

要素	説明
名前	最大 64 文字のオブジェクト名。スペースは使用できません。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
[Smart Tunnel Entries] テーブル	アプリケーションの名前、クライアント ワークステーションでのアプリケーションの位置など、ユーザが SSL VPN 経由でスマート トンネル アクセスを実行できるアプリケーション。 • アプリケーションを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス （2015 ページ）を開きます。 • アプリケーションを編集するには、アプリケーションを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • アプリケーションを削除するには、アプリケーションを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
Include Smart Tunnel Lists	このオブジェクトに含めるその他の SSL VPN スマート トンネル リスト オブジェクト（ある場合）。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックス

[Add A Smart Tunnel Entry]/[Edit A Smart Tunnel Entry] ダイアログボックスを使用して、新しいスマート トンネル エントリを作成するか、または [SSL VPN Smart Tunnel Lists] ダイアログボックスにあるテーブルの既存のエントリを編集します。

ナビゲーション パス

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （2013 ページ）で、[スマートトンネルエントリ（Smart Tunnel Entries）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *469 : [Add Smart Tunnel Entry]/[Edit Smart Tunnel Entry]* ダイアログボックス

要素	説明
アプリ名	スマート トンネル アクセスを許可するアプリケーションの名前。名前には最大 64 文字を使用できます。スマート トンネル アクセスを複数のバージョンに許可する場合は、アプリケーションのバージョン番号を含めることを検討します。
App Path	アプリケーションのファイル名、およびオプションのパス。このエントリには最大 128 文字を使用できます。次のいずれかを使用します。 • [ファイル名（Filename）] : たとえば、**outlook.exe**。指定するのはファイル名だけです。ユーザがアプリケーションをインストールしたワークステーション上の場所を指定する必要はありません。ただし、このファイル名は完全に一致する必要があります。 • [フルパスとファイル名（Full path and filename）] : たとえば、**C:\Program Files\Microsoft Office\OFFICE11\OUTLOOK.EXE**。これにより、アプリケーションが指定のディレクトリにインストールされている場合にかぎり、アプリケーションのスマート トンネル アクセスが許可されます。これを、組織標準を適用するために使用できます。 ヒント • フル パスを指定しており、一定期間動作していたスマート トンネル アプリケーションが動作しなくなった場合は、製品アップグレードによってインストール パスが変更された可能性があります。新しいパスで構成された新しいエントリを追加します。 • コマンドラインから起動されるアプリケーションへのスマートトンネルアクセスを許可する場合は、**cmd.exe**（Windows コマンドライン）用に 1 つのエントリを作成し、アプリケーション用に別のエントリを作成します。
プラットフォーム	アプリケーションのホスト オペレーティング システムを指定します。 • Windows • Mac

要素	説明
Hash Value	（任意）アプリケーションのハッシュ値。ハッシュ値を指定することによって、ユーザが、サポートされているファイル名を使用するために別のアプリケーション名を変更し、サポートされていない、望ましくないアプリケーションをスマートトンネル経由で起動することを確実に阻止できます。 ハッシュ値を取得するには、アプリケーションのチェックサム（実行可能ファイルのチェックサム）を、SHA-1 アルゴリズムを使用してハッシュを計算するユーティリティに入力します。このようなユーティリティの例として、Microsoft ファイルチェックサム整合性検証（FCIV）を挙げることができます。このユーティリティは、http://support.microsoft.com/kb/841290/ で入手できます。ハッシュ対象のアプリケーションの一時コピーを、スペースを含まないパス（c:\temp など）に配置し、**fciv.exe -sha1** アプリケーションをコマンドラインに入力して（**fciv.exe -sha1 c:\msimn.exe** など）、SHA-1 ハッシュを表示します。値をコピーしてこのフィールドに貼り付けます。 SHA-1 ハッシュは、常に 16 進数 40 文字です。アプリケーションのスマート トンネル アクセスを認可する前に、クライアントレス SSL VPN は、[App Name] に一致するアプリケーションのハッシュを計算します。結果がハッシュ値と一致すると、アプリケーションのスマート トンネル アクセスが認定されます。 チェックサムはアプリケーションのバージョンやパッチごとに異なるため、入力したハッシュは、リモート ホスト上の 1 つのバージョンまたはパッチとだけ一致します。アプリケーションの複数のバージョンのハッシュを指定する場合は、各ハッシュ値に一意のスマート トンネル エントリを作成します。 **ヒント** ハッシュ値はメンテナンスする必要があります。ハッシュ値を指定しているアプリケーションの今後のバージョンまたはパッチをサポートする場合は、スマートトンネルリストを更新する必要があります。スマートトンネル アクセスで突然問題が発生した場合は、ハッシュ値が含まれたアプリケーション リストが、アプリケーションのアップグレードに関して最新でない可能性があります。ハッシュを入力しないことで、この問題を回避できます。

[スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス

Security Manager バージョン 4.7 以降、[スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]および[スマートトンネルネットワークリストの編集（Edit Smart Tunnel

Network Lists）] ダイアログ ボックスを使用して、スマートトンネルポリシーの設定に使用できるホストのリストを作成および編集できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SSL VPN スマートネットワークリスト（SSL VPN Smart Network Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。または、[追加（+）（Add (+)）] ボタンをクリックして新しいオブジェクトを追加するか、[編集（Edit）]（鉛筆）ボタンをクリックしてオブジェクトを編集できます。

関連項目

- ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- Policy Object Manager （290 ページ）
- [スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス （2019 ページ）

フィールド リファレンス

表 *470 : [*スマートトンネルネットワークリストの追加（*Add Smart Tunnel Network Lists***）*]/[*スマートトンネルネットワークリストの編集（***Edit Smart Tunnel Network Lists***）*] ダイアログボックス**

要素	説明
名前	トンネルポリシーに適用するために使用するスマート トンネル ネットワーク リスト オブジェクト名。名前には最大 64 文字を使用できます。スペースは使用できません。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）ネットワーク リスト オブジェクトの説明。
スマート トンネル ネットワーク リスト エントリ テーブル	アプリケーションが SSL VPN を介したスマートトンネルアクセスを許可されるネットワークのホストマスクまたは IP アドレス。 • エントリを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログ ボックス （2013 ページ）を開きます。 • エントリを編集するには、エントリを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
Include Other Lists	このオブジェクトに含めるその他の SSL VPN スマート トンネル ネットワーク リスト オブジェクト（ある場合）。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイスレベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[スマートトンネルネットワークリストエントリの追加および編集（Add and Edit A Smart Tunnel Network List Entry] ダイアログボックス

[スマートトンネルネットワークリストエントリの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストエントリの編集（Edit Smart Tunnel Network Lists）] ダイアログボックスを使用して、新しいスマートトンネルエントリを作成するか、または [SSL VPN Smart Tunnel Lists] ダイアログボックスにあるテーブルの既存のエントリを編集します。

ナビゲーション パス

[Add Smart Tunnel List]/[Edit Smart Tunnel List] ダイアログボックス （2013 ページ）で、[スマートトンネルネットワークリストエントリ（Smart Tunnel Network List Entries）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- [スマートトンネルネットワークリストの追加（Add Smart Tunnel Network Lists）]/[スマートトンネルネットワークリストの編集（Edit Smart Tunnel Network Lists）] ダイアログボックス （2017 ページ）
- ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）

- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *471 : [*スマートトンネルネットワークリストエントリの追加（***Add Smart Tunnel Network Lists***）*]/[*スマートトンネルネットワークリストエントリの編集（***Edit Smart Tunnel Network Lists***）*]* ダイアログボックス

要素	説明
ホスト（Host）	スマート トンネル ネットワーク リスト エントリの一部となるホストマスク。
IPアドレス	スマート トンネル ネットワーク リスト エントリの一部となるホストの IP アドレス。バージョン 4.12 以降、Security Manager は IPv6 アドレスをサポートします。
サブネットマスク	指定された IP アドレスのサブネットマスク。

[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス

[Add Smart Tunnel Auto Signon Lists]/[Edit Smart Tunnel Auto Signon Lists] ダイアログボックスを使用して、SSL VPN スマート トンネル自動サインオン オブジェクトを作成、コピー、および編集します。

スマート トンネル自動サインオンは、クライアントレス SSL VPN ユーザに対するシングル サインオン方式です。この方式では、ログイン クレデンシャル（ユーザー名とパスワード）を NTLM 認証と HTTP 基本認証のいずれか一方または両方を使用する認証用の内部サーバーに渡します。スマート トンネル自動サインオンは、ソフトウェア バージョン 7.1(1) 以降を実行している ASA 5500 デバイスでサポートされています。

SSL VPN スマート トンネル自動サインオン リスト オブジェクトでは、スマート トンネルの設定時にログイン クレデンシャルの送信を自動化するサーバを指定します。ユーザがサーバにスマート トンネル接続を確立する際にユーザ クレデンシャルを再発行する場合は、ASA グループ ポリシーのクライアントレス設定値にスマート トンネル自動サインオン リストを設定できます。スマート トンネル アクセスをサポートするアプリケーションのタイプについては、ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）を参照してください。

その他の SSL VPN スマート トンネル自動サインオン リスト オブジェクトをオブジェクトに含めることができます。このため、サーバの基本的なリストを指定するオブジェクト セットを作成し、これらのオブジェクトをサーバのリスト上に展開する別のオブジェクトに含めることができます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SSL VPNスマートトンネル自動サインオンリスト（SSL VPN Smart Tunnel Auto Signon Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ASA グループ ポリシーの SSL VPN クライアントレス設定 （1933 ページ）
- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *472 : [Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List]* ダイアログボックス

要素	説明
名前	最大64文字のオブジェクト名。スペースは使用できません。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
[Smart Tunnel Auto Signon Entries] テーブル	スマートトンネルの設定時にログインクレデンシャルの送信を自動化するサーバ。 • サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックして、 [Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス （2022 ページ）を開きます。 • エントリを編集するには、エントリを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • エントリを削除するには、エントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。
Include Other Lists	このオブジェクトに含めるその他のスマート トンネル自動サインオン リスト オブジェクト（ある場合）。オブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストから選択するか、または新しいオブジェクトを作成します。複数のエントリを指定する場合は、カンマで区切ります。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）]ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックス

[Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry] ダイアログボックスを使用して、新しいスマート トンネル エントリを作成するか、または [SSL VPN Smart Tunnel Auto Signon List] ダイアログボックスにあるテーブルの既存のエントリを編集します。

ナビゲーション パス

[Add Smart Tunnel Auto Signon List]/[Edit Smart Tunnel Auto Signon List] ダイアログボックス （2020 ページ）で、[スマートトンネル自動サインインエントリ（Smart Tunnel Auto Signon Entries）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、またはエントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- ASA デバイスの SSL VPN スマート トンネルの設定 （1821 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *473 : [Add Smart Tunnel Auto Signon Entry]/[Edit Smart Tunnel Auto Signon Entry]* ダイアログボックス

要素	説明
Matching Mode： • ホスト（Host） • IPv4/IPv6 アドレス	スマートトンネルの設定時にログインクレデンシャルの送信を自動化するサーバを指定します。[Host] を使用して、サーバをホスト名またはワイルドカードマスクで指定します。また、[IP Address] を使用して、サーバを IP アドレスおよびネットマスクで指定します。 • [ホスト（Host）] : [ホスト（Host）] を選択して、ホスト名またはワイルドカードマスクを [ホスト名マスク（Hostname Mask] フィールドに入力します。これにより、スマートトンネルの設定時にログインクレデンシャルの送信を自動化するホストが識別されます。 （注） このオプションを使用すると、IP アドレスのダイナミックな変更からコンフィギュレーションを保護します。 • [IPv4/IPv6アドレス（IPv4/IPv6 Address）] : [IPアドレス（IP Address）] を選択して、スマートトンネルの設定時にログインクレデンシャルの送信を自動化するホストの IP アドレスおよびネットマスク、またはサブネットワークを入力します。 （注） バージョン 4.12 以降、Security Manager は IPv6 アドレスをサポートします。デフォルトでは、IPv4/IPv6 アドレスを選択すると、Security Manager は IPv4/IPv6 アドレスを検索します。必要に応じてサブネットマスクまたはプレフィックス長を入力します。 （注） Firefox では、管理者が正確なホスト名または IP アドレスを使用してホストを指定する必要があります（ワイルドカードを使用したホストマスク、IP アドレスを使用したサブネット、およびネットマスクは使用できません）。たとえば、Firefox では、*.cisco.com を入力したり、email.cisco.com をホストする自動サインオンを期待したりすることはできません。
ポート番号（Port Number）	自動サインオンを実行するポート。Firefox では、ポート番号が指定されていない場合、自動サインオンはデフォルトのポート番号 80 および 443 でそれぞれアクセスされた HTTP および HTTPS に対して実行されます。
認証レルム（Authentication Realm）	認証のレルム。[Authentication Realm] は Web サイトの保護領域に関連付けられ、認証時に認証プロンプトまたは HTTP ヘッダーのいずれかでブラウザに再度渡されます。自動サインオンが設定され、レルムの文字列が指定されたら、ユーザはレルムの文字列を Web アプリケーション（Outlook Web Access など）で設定し、Web アプリケーションにサインオンすることなくアクセスできます。

要素	説明
Use Domain	このオプションを選択して、認証で Windows ドメインが必要な場合に、ユーザ名に Windows ドメインを追加します。このオプションを使用する場合は、スマート トンネル リストを 1 つ以上のグループ ポリシーに割り当てるときにドメイン名を指定してください。

[Add User Group]/[Edit User Group] ダイアログボックス

[Add User Group]/[Edit User Group] ダイアログボックスを使用して、ユーザ グループ オブジェクトを作成または編集します。ユーザ グループ オブジェクトは、IOS デバイスの Easy VPN トポロジ、リモート アクセス VPN、および SSL VPN で使用されます。

リモート アクセス VPN、SSL VPN、または Easy VPN サーバを設定する場合、リモート クライアントが属するユーザ グループを作成できます。リモート クライアントは、サーバに接続するために、VPN サーバ上のユーザ グループと同じグループ名を使用して設定されている必要があります。そうでない場合、接続は確立されません。リモート クライアントが VPN サーバに正常に接続されると、特定のユーザ グループのグループ ポリシーが、そのユーザ グループに属しているすべてのリモート クライアントにプッシュされます。

ユーザ グループの詳細については、次を参照してください。

- ユーザ グループ ポリシーの設定 （1906 ページ）
- Easy VPN における User Group ポリシーの設定 （1617 ページ）
- SSL VPN ポリシーの設定（IOS） （1908 ページ）

（注） ユーザ グループ オブジェクトを作成するテクノロジー（Easy VPN/リモート アクセス VPN、または SSL VPN）を選択する必要があります。既存のユーザ グループ オブジェクトを編集する場合、テクノロジーはすでに選択されており、変更できません。選択したテクノロジーに応じて、構成に適切な設定を使用できます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [ユーザーグループ（User Groups）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

ヒント このダイアログボックスには、[リモートアクセスVPN（Remote Access VPN）] > [IPSec VPN] > [ユーザーグループ（User Groups）] または [リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] ポリシーからアクセスすることもできます。

関連項目

- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *474 : [User Group]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
[Settings] ペイン ダイアログボックスの本体は左右に分割されたペインであり、左側にはコンテンツ テーブル、右側にはコンテンツ テーブルで選択された項目に関連する設定が表示されます。 まずテクノロジー設定を指定する必要があります。次に、左側のコンテンツ テーブルから項目を選択し、必要なオプションを設定できます。[Technology] ページの選択内容によって、これらのページとコンテンツ テーブルで使用できるオプションが制御されます。 コンテンツ テーブルの上部にあるフォルダは、次に説明する設定可能な VPN テクノロジーまたはその他の設定を表します。	
Technology settings	これらの設定によって、グループ ポリシーで定義できる内容が制御されます。 • [グループ名（Group Name）]：ユーザーグループの名前（最大 128 文字）。適切なグループ属性が確実にダウンロードされるように、リモート クライアントまたはデバイス内で同じユーザ グループ名を設定します。 • [テクノロジー（Technology）]：このオブジェクトでグループ ポリシーを定義する VPN のタイプ。このオプションは、オブジェクトを編集しているとき、または VPN ポリシーの編集中にユーザ グループ オブジェクトを作成するとき、変更できません。Easy VPN/リモート アクセス IPSec VPN と SSL VPN のいずれかの設定値を設定できますが、両方は設定できません。

要素	説明
[Easy VPN/Remote Access IPSec VPN] ページ	[Easy VPN/Remote Access IPSec VPN] をテクノロジーとして選択した場合、次のページで設定値を設定できます。 • [User Group] ダイアログボックス - 一般設定 （2027 ページ） • [User Group] ダイアログボックス - DNS/WINS 設定 （2028 ページ） • [User Group] ダイアログボックス - スプリット トンネリング （2029 ページ） • [User Group] ダイアログボックス - IOS クライアント設定 （2030 ページ） • [User Group] ダイアログボックス - IOS Xauth オプション （2032 ページ） • [User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新 （2034 ページ） • [User Group] ダイアログボックス - PIX の詳細オプション （2035 ページ）
[SSL VPN] ページ	[SSL VPN] をテクノロジーとして選択した場合、次のページで設定値を設定できます。 • [User Group] ダイアログボックス - クライアントレス設定 （2036 ページ） • [User Group] ダイアログボックス - シン クライアント設定 （2038 ページ） • [User Group] ダイアログボックス - SSL VPN フル トンネル設定 （2039 ページ） • [User Group] ダイアログボックス - DNS/WINS 設定 （2028 ページ） • [User Group] ダイアログボックス - SSL VPN スプリット トンネリング （2042 ページ） • [User Group] ダイアログボックス - ブラウザ プロキシ設定 （2043 ページ） • [User Group] ダイアログボックス - SSL VPN 接続設定 （2045 ページ）

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

[User Group] ダイアログボックス - 一般設定

ユーザ グループに設定する一般設定には、認証方式、IP アドレス プール情報、および PIX 6.3 ファイアウォールの接続属性があります。

（注） これらの設定は、Easy VPN およびリモート アクセス IPSec VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）のコンテンツテーブルから [全般（General）] を選択します。

フィールド リファレンス

表 *475 : [User Group]* ダイアログボックス - 一般設定

要素	説明
事前共有キー（Preshared Key）	このユーザ グループに関連付けられているクライアントの認証に使用される事前共有キー。 （注） グループ認証にデジタル証明書を使用している場合は、事前共有キーを入力する必要はありません。 通常の IPsec VPN では、事前共有キーによって、1 つ以上のピアが個別の共有秘密キーを使用して、暗号化されたトンネルを認証できます。事前共有キーは、各参加ピア上で設定する必要があります。参加ピアの 1 つに同じ事前共有キーが設定されていない場合は、IKE SA を確立できません。 Easy VPN 認証では、サーバ/クライアント キーを確実に一致させるために、同じ Easy VPN サーバ キーがスポーク設定に使用されます。 リモート アクセス IPSec VPN 認証では、リモート アクセス VPN サーバとリモート クライアントとの間で VPN 接続をネゴシエートするために、同じキーが使用されます。
IP Address Pool Subnet/Ranges	内部 IP アドレスをクライアントに割り当てるために使用される、ローカル プールの IP アドレス範囲。リモート クライアントは、このプールから割り当てられた IP アドレスです。複数のエントリを指定する場合は、カンマで区切ります。デフォルトは、172.16.0.1 ～ 172.16.4.254 です。

要素	説明
Backup Servers IP Address	Easy VPN またはリモート アクセス IPSec VPN サーバのバックアップとして使用されるサーバの IP アドレス。ルータは、Easy VPN またはリモート アクセス VPN サーバへのプライマリ接続が失敗した場合に、これらのサーバへの接続を試行します。複数のエントリを指定する場合は、カンマで区切ります。
PIX Only Attributes	次の属性は、PIX 6.3 デバイスだけに適用されます。 • [アイドル時間（Idletime）]：VPN接続のタイムアウト時間（秒単位）。通信がこの接続でこの時間中に発生しなかった場合、デバイスはこの接続を終了します。最小は 60 秒で、最大時間は 35791394 分です。デフォルトは 30 分です。 • [最大時間（Max Time）]：VPN 接続の最大時間（秒単位）。この時間が終了すると、デバイスによって接続が終了されます。最小は 60 秒で、最大は 35791394 分です。デフォルトはありません。

[User Group] ダイアログボックス - DNS/WINS 設定

このユーザ グループに関連付けられているクライアントにプッシュする DNS サーバと WINS サーバおよびドメイン名を定義するように、ユーザ グループの DNS/WINS 設定値を設定します。

（注） ユーザ グループに設定した DNS/WINS 設定値は、Easy VPN、リモート アクセス VPN、および SSL VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）のコンテンツ テーブルから [DNS/WINS] を選択します。

フィールド リファレンス

表 *476 : [User Group] ダイアログボックス - DNS/WINS 設定*

要素	説明
プライマリ DNS サーバ（Primary DNS Server）	グループのプライマリ DNS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
セカンダリ DNS サーバ（Secondary DNS Server）	グループのセカンダリ DNS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
ドメイン名	ユーザ グループで設定する DNS サーバのドメイン名。
プライマリ WINS サーバ（Primary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
セカンダリ WINS サーバ（Secondary WINS Server）	グループのプライマリ WINS サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

[User Group] ダイアログボックス - スプリット トンネリング

スプリット トンネリングを使用すると、リモート クライアントは、条件に応じて、パケットを IPsec または SSL VPN トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。

スプリット トンネリング ポリシーは、特定のネットワークに適用されます。スプリット トンネリングを設定する場合、保護されたトラフィックと保護されていないトラフィックの両方を同じインターフェイスで送信できます。中央サイトへの安全なトンネルが確立されるように、保護されたトラフィックおよびそのトラフィックの宛先を指定する必要がある一方で、クリア（保護されていない）トラフィックはパブリック ネットワーク経由で送信されます。

ヒント　最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

（注）　スプリット トンネリングは、Easy VPN、リモートアクセス VPN、および SSL VPN の設定で適用できます。SSL VPN のスプリット トンネリングの設定については、[User Group] ダイアログボックス - SSL VPN スプリット トンネリング （2042 ページ）を参照してください。

ナビゲーション パス

Easy VPN/リモートアクセス IPSec VPN を設定する場合は、[Add User Group]/[Edit User Group] ダイアログボックス（2024ページ）のコンテンツテーブルから [スプリットトンネリング（Split Tunneling）] を選択します。

フィールド リファレンス

表 *477 : [User Group]* ダイアログボックス - スプリット トンネリング

要素	説明
スプリット トンネリング（Split Tunneling）	トラフィックをトンネル化するネットワーク。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネットサービスプロバイダーによってルーティングされます。次のいずれかのオプションを使用して、ネットワークを指定できます。 • [保護対象ネットワーク（Protected Networks）]：ネットワークアドレスでネットワークを指定します。アドレスまたはネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。アドレスの指定については、ポリシー定義中の IP アドレスの指定（401 ページ）を参照してください。 • [ACL]：拡張アクセス制御リストポリシーオブジェクトを使用して、ネットワークを指定します。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
スプリット DNS	トンネル化される、つまりプライベートネットワークに解決される必要があるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを介して解決されます。 複数のドメイン名をカンマで区切って入力できます。

[User Group] ダイアログボックス - IOS クライアント設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

VPN クライアントのファイアウォール設定など、Cisco IOS 固有のユーザ グループ オプションを定義するように、IOS クライアント設定値を設定します。

（注） これらの設定は、Easy VPN およびリモート アクセス IPSec VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）の目次で [クライアント設定（Client Settings (IOS)）] を選択します。

フィールド リファレンス

表 *478 : [User Group] ダイアログボックス - [Client Settings (IOS)]*

要素	説明
Enable Firewall Are-You-There （7600 シリーズまたは ASR ルータでは使用できません）	この機能は、VPN クライアントが Black Ice または Zone Alarm パーソナル ファイアウォールを実行している場合に使用できます。 選択した場合、パーソナル ファイアウォールが、接続時および接続中、確実に実行されるようになります。サーバによって要求された場合、Firewall-Are-U-There 属性が Black Ice および Zone Alarm パーソナル ファイアウォールによって送信されます。パーソナル ファイアウォールが動作を停止した場合、接続は終了されます。この機能がイネーブルになっており、かつサーバ上でパーソナル ファイアウォールが稼働していない場合、接続は確立されません。
[モード（Mode）]	サーバ上の Central Policy Push（CPP）ファイアウォール ポリシーに従い、ローカル AAA サーバで必須のファイアウォールがリモート デバイスに備えられているかどうかに基づき、トンネルを許可または拒否します。 [Mode] オプションを使用して、Central Policy Push（CPP）ポリシーが任意であるか必須であるかを次のように指定します。 • [任意（Optional）]：CPP ポリシーが任意であるとして定義され、Easy VPN サーバー設定に含まれている場合、トンネルのセットアップは、定義されたポリシーをクライアントが確認しなくても続行されます。 • [必須（Required）]：CPP ポリシーが必須であるとして定義され、Easy VPN サーバー設定に含まれている場合、トンネルのセットアップは、クライアントがこのポリシーを確認した場合にだけ許可されます。それ以外の場合、トンネルは終了されます。
Firewall Type	必須または任意にするファイアウォールのタイプ。このリストには、Cisco および Zone Labs のソフトウェアなど、サポートされているすべてのファイアウォール ソフトウェアが示されます。

要素	説明
ポリシー タイプ	CPP ファイアウォール ポリシー タイプを指定します。 • [プレゼンスのチェック（Check Presence）]：指定したファイアウォールタイプの存在をチェックするようサーバーに指示します。 • [中央ポリシープッシュ（Central Policy Push）]：指定したクライアント ファイアウォール タイプによって適用される必要がある、入力アクセスリストおよび出力アクセスリストなどの実際のポリシー。次を指定します。 • 使用するアクセス コントロール リスト。拡張 ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 • アクセス コントロール リストの方向：着信および発信
Include Local LAN	非スプリット トンネリング接続が、クライアントと同時にローカル LAN にアクセスすることを許可するかどうかを指定します。
Perfect Forward Secrecy	Perfect Forward Secrecy（PFS; 完全転送秘密）をイネーブルにするかどうかを指定します。PFS がイネーブルな場合、サーバは、PFS が IPsec SA に必要であるかどうかを中央サイト ポリシーのクライアントに通知するように設定されています。PFS に提示された Diffie-Hellman（D-H; デフィーヘルマン）グループは、IKE ネゴシエーションのフェーズ 1 でネゴシエートされたグループと同じです。

[User Group] ダイアログボックス - IOS Xauth オプション

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

IOS Xauth オプションでは、バナー テキストなど、ユーザ グループの IKE Extended Authentication（Xauth; 拡張認証）ユーザ認証および接続パラメータを設定します。

（注） これらの設定は、Easy VPN およびリモート アクセス VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）の目次から [Xauthオプション（IOS）（Xauth Options (IOS)）] を選択します。

フィールド リファレンス

表 *479 : [User Group]* ダイアログボックス - *IOS Xauth* オプション

要素	説明
バナー	Easy VPN トンネルが最初に起動したときの Xauth および Web ベースのアクティベーション中に、Easy VPN リモート クライアントに表示されるバナー テキスト。最大 1024 文字を使用できます。
Maximum Logins Per User	ユーザが同時に確立できる最大接続数。最大値は 10 です。
最大接続数	このグループから Easy VPN サーバへの最大クライアント接続数。グループごとの最大値は 5000 です。
Enable Group-Lock	グループ ロックをイネーブルにするかどうかを指定します。グループ ロックは、ユーザが拡張 Xauth ユーザ名を次のいずれかの形式で入力する場合に必要となります。 • username/groupname • username\groupname • username@groupname • username%groupname 区切り文字のあとに指定されたグループは、次に、IKE アグレッシブ モードで送信されたグループ ID と比較されます。これらのグループは一致する必要があります。一致しない場合、接続が拒否されます。 （注） 証明書など、RSA シグニチャ認証メカニズムを使用している場合は、このオプションを選択しないでください。
Enable Save Password	ユーザがユーザの Xauth パスワードをクライアント上でローカルに保存することを許可するかどうかを指定します。以降の認証で、ユーザは、ソフトウェア クライアント上のチェックボックスを使用するか、またはユーザ名とパスワードを Cisco IOS ハードウェア クライアント プロファイルに追加して、パスワードをアクティブ化できます。ユーザがパスワードをアクティブ化すると、ユーザ名とパスワードは Xauth 時にサーバに自動的に送信されます。 このオプションは、ユーザがスタティック パスワード、つまりトークンによって生成されるようなワンタイム パスワードではないパスワードを持っている場合にだけ役立ちます。

[User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、拡張機能はサポートしていません。

クライアント VPN ソフトウェア更新（IOS）設定を使用して、ユーザ グループの IOS VPN クライアントに関して、インストールされている各クライアント VPN ソフトウェア パッケージのプラットフォーム タイプ、VPN クライアント リビジョン、およびイメージ URL を設定します。

クライアント更新機能は、IOS ルータ バージョン 12.4(2)T 以降、および Catalyst 6500/7600 デバイス バージョン 12.2(33)SRA 以降でサポートされています。

- クライアントを追加するには、[行の追加（Add Row）] ボタンをクリックして、[Add Client Update]/[Edit Client Update] ダイアログボックス （2034 ページ）を開きます。
- クライアントを編集するには、クライアントを選択して [行の編集（Edit Row）] ボタンをクリックします。
- クライアントを削除するには、クライアントを選択して [行の削除（Delete Row）] ボタンをクリックします。

（注） これらの設定は、Easy VPN およびリモート アクセス VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）の目次で [クライアント VPN ソフトウェア更新（IOS）（Client VPN Software Update (IOS)）] を選択します。

[Add Client Update]/[Edit Client Update] ダイアログボックス

[Add Client Update]/[Edit Client Update] ダイアログボックスを使用して、クライアント VPN ソフトウェア パッケージのプラットフォームタイプ、イメージ URL、および VPN クライアント リビジョンを設定します。

ナビゲーション パス

[User Group] ダイアログボックス - IOS クライアント VPN ソフトウェア更新 （2034 ページ）を開き、[行の追加（Add Row）] をクリックするか、テーブル内の項目を選択して [行の編集（Edit Row）] をクリックします。

関連項目

- [Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）

フィールド リファレンス

表 *480 : [Add Client Update]/[Edit Client Update]* ダイアログボックス

要素	説明
[システム タイプ（System Type）]	IOS VPN クライアントが動作するプラットフォーム。 • [All Windows]（デフォルト）：このオプションには、VPN クライアントを使用できる Windows プラットフォームがすべて含まれています。 • Macintosh OS X
IOS Image URL	クライアントをダウンロードできる URL を入力します。URL は、http:// または https:// で始まる必要があります。
IOS VPN Client Revisions	VPN クライアントのリビジョン レベルを入力します。複数のクライアント リビジョンをカンマで区切って指定できます。

[User Group] ダイアログボックス - PIX の詳細オプション

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、拡張機能はサポートしていません。

PIX の詳細オプションは、ユーザ グループの PIX 6.3 ファイアウォール専用のオプションです。

（注） これらの設定は、Easy VPN およびリモート アクセス VPN の設定に適用されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）の目次から [詳細オプション（PIX）（Advanced Options (PIX)）] を選択します。

フィールド リファレンス

表 *481 : [User Group]* ダイアログボックス - *PIX* の詳細オプション

要素	説明
User Idle Timeout (sec)	ユーザのアクティビティがなくても VPN トンネルを開いたままにしておける時間（秒数）。値の範囲は 60 ～ 86400 秒です。
User Authentication Server	リモートデバイスがユーザ認証要求を送信する AAA サーバ。サーバーグループの名前を入力するか、[選択（Select）] をクリックしてリストからサーバーグループを選択するか、または新しいグループを作成します。AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）を参照してください。
Enable Device Pass-Through	Media Access Control（MAC; メディア アクセス コントロール）アドレスを使用して、AAA 認証をサポートしていない Cisco IP Phone などのデバイスの認証をバイパスするかどうかを指定します。 MAC ベースの AAA 免除がイネーブルである場合、デバイスは、デバイスの MAC アドレスと（DHCP サーバによって動的に割り当てられた）IP アドレスの両方に一致するトラフィックの AAA サーバをバイパスします。認証をバイパスすると、認可サービスは自動的にディセーブルになります。アカウンティング レコードは引き続き生成されますが（イネーブルになっている場合）、ユーザ名は表示されません。
Enable Secure Unit Authentication	リモート クライアントからデバイスへのアクセスを許可する場合に、セキュリティを強化するかどうかを指定します。 Secure Unit Authentication（SUA）では、ワンタイム パスワード、2 要素認証、および類似の認証スキームを使用して、Extended Authentication（Xauth; 拡張認証）中にリモート デバイスを認証できます。 SUA は、デバイス上の VPN ポリシーで指定され、リモート クライアントにダウンロードされます。これにより、SUA がイネーブルになり、リモート クライアントの接続動作が決まります。
Enable User Authentication	Individual User Authentication（IUA; 個別ユーザ認証）をイネーブルにするかどうかを指定します。IUA を使用すると、各内部クライアントの IP アドレスに基づいて、リモート アクセス VPN の内部ネットワークでクライアントを個別に認証できます。IUA では、スタティックと OTP の両方の認証メカニズムをサポートしています。

[User Group] ダイアログボックス - クライアントレス設定

クライアントレス設定を使用して、SSL VPN における企業ネットワークへのクライアントレス アクセス モードを設定します。

クライアントレス アクセス モードでは、ユーザーが認証され、セッションが確立されると、SSL VPN ポータルページおよびツールバーがユーザーの Web ブラウザに表示されます。このポータル ページから、ユーザは使用可能なすべての HTTP サイトにアクセスしたり、Web 電子メールにアクセスしたり、Common Internet File System（CIFS）ファイル サーバを参照したりできます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）のコンテンツテーブルから [クライアントレス（Clientless）] を選択します。

関連項目

- Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ （1686 ページ）

フィールド リファレンス

表 *482 : [User Group]* ダイアログボックス - クライアントレス設定

要素	説明
Portal Page Websites	ポータル ページ上に表示する Web サイト URL が含まれる SSL VPN ブックマーク ポリシー オブジェクトの名前。これらの Web サイトを使用すると、ユーザは目的のリソースにアクセスできます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Allow Users to Enter Websites	ブラウザへの Web サイト URL の直接入力をリモート ユーザに許可するかどうかを指定します。このオプションを選択しない場合、ユーザはポータルに表示されている URL だけにアクセスできます。

要素	説明
Enable Common Internet File System (CIFS)	クライアントレス モードでは、リモート クライアントが、Microsoft Windows サーバで作成されたファイルとディレクトリに Web ブラウザ経由でアクセスできます。Common Internet File System（CIFS）をイネーブルにすると、ファイル サーバのリストおよびディレクトリ リンクが、ログイン後にポータル ページに表示されます。 CIFS プロトコルを使用すると、SSL VPN ゲートウェイでの権限をカスタマイズして、次のように、リモート クライアントに対して、共有ファイルへのアクセスまたは変更を許可できます。 • [ファイル参照を有効化（Enable File Browsing）]：CIFS ファイル サーバー上のファイル共有を参照することをリモートユーザーに許可するかどうかを指定します。 • [ファイルエントリの有効化（Enable File Entry）]：ファイル共有の名前を入力して、CIFS ファイル サーバー上のファイル共有を検索することをリモートユーザーに許可するかどうかを指定します。
WINS Server List	WINS サーバ リスト ポリシー オブジェクトの名前。この名前によって、ファイル サーバ名の解決に使用する WINS/NetBIOS サーバが指定されます。CIFS をイネーブルにした場合は、オブジェクトを指定する必要があります。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Enable Citrix	リモート クライアントが、クライアント ソフトウェアがなくても、アプリケーションがローカルにインストールされているかのように、SSL VPN を介して Citrix 対応アプリケーション（Microsoft Word や Excel など）を実行できるようにするかどうかを指定します。Citrix ソフトウェアは、ルータが到達可能な 1 台以上のサーバにインストールされている必要があります。

[User Group] ダイアログボックス - シン クライアント設定

シン クライアント設定を使用して、SSL VPN における企業ネットワークへのシン クライアント（またはポート転送）アクセス モードをイネーブルにします。ポート転送により、ユーザは SSL VPN セッション経由で企業内のアプリケーション（Telnet、電子メール、VNC、SSH、Terminal Services など）にアクセスできます。ポート フォワーディング リスト オブジェクトは、リモート クライアント上のポート番号を SSL VPN ゲートウェイの背後にあるアプリケーションの IP アドレスとポートにマッピングします。

シン クライアント アクセス モードでは、リモート ユーザは、SSL VPN ゲートウェイで設定されているサービス用の TCP プロキシとしてクライアント マシン上で機能する Java アプレットをダウンロードします。このプロキシによって、ポート転送サービスが提供されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）のコンテンツテーブルから [シンクライアント（Thin Client）] を選択します。

関連項目

- Create Group Policy ウィザード：[Clientless and Thin Client Access Modes] ページ （1686 ページ）

フィールド リファレンス

表 *483 : [User Group]* ダイアログボックス - シン クライアント設定

要素	説明
Enable Thin Client	SSL VPN へのシン クライアント アクセスを許可するかどうかを指定します。
Port Forward List	このグループに割り当てるポート転送リスト ポリシー オブジェクトの名前。ポート転送リストには、クライアントレス SSL VPN セッションのユーザが転送先 TCP ポートを介してアクセスできるアプリケーションのセットが含まれます。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Download Port Forwarding Applet on Client Login	ユーザが SSL VPN にログインしたときに、ポート転送 Java アプレットがクライアントに自動的にダウンロードされるかどうかを指定します。アプレットを自動的にダウンロードしない場合、ユーザがログイン後に手動でダウンロードする必要があります。

[User Group] ダイアログボックス - SSL VPN フル トンネル設定

SSL VPN フル トンネル設定を使用して、SSL VPN におけるフル トンネル クライアント アクセス モードをイネーブルにします。フル トンネル アクセスをイネーブルにした場合は、ユーザ グループの DNS/WINS サーバ設定、ブラウザ プロキシ設定、およびスプリット トンネリングも定義する必要があります。

フル トンネル クライアント アクセス モードでは、トンネル接続はグループ ポリシー設定によって決まります。フル トンネル クライアント ソフトウェアである SSL VPN Client（SVC）がリモート クライアントにダウンロードされるため、トンネル接続はリモート ユーザが SSL VPN ゲートウェイにログインしたときに確立されます。

ヒント　フル トンネル クライアント アクセスが機能するには、クライアント ソフトウェアをゲートウェイにインストールする必要があります。ユーザは、ゲートウェイに接続したときにクライアントをダウンロードします。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）のコンテンツテーブルから **[フルトンネル（Full Tunnel）] > [設定（Settings）]** を選択します。

関連項目

- Create Group Policy ウィザード：[Full Tunnel] ページ （1682 ページ）

フィールド リファレンス

表 *484 : [User Group]* ダイアログボックス - フル トンネル設定

要素	説明
Enable Full Tunnel	SSL VPN へのフル トンネル クライアント アクセスをイネーブルにするかどうかを指定します。
Use Other Access Modes if SSL VPN Client Download Fails Full Tunnel Only	問題が発生してユーザのシステム上でクライアントを正常にダウンロード、インストール、および起動できない場合でも、SSL VPN への接続をユーザに許可するかどうかを指定します。 [フルトンネルのみ（Full Tunnel Only）] を選択すると、ダウンロードが失敗し、そのことによってユーザがネットワークからロックアウトされた場合、ユーザは SSL VPN に接続できません。ダウンロードの問題が発生した場合にクライアントレスまたはシンクライアントアクセスを許可するには、[他のアクセスモードを使用（Use Other Access Modes）] を選択します。

要素	説明
Client IP Address Pool	フル トンネル クライアントがログインしたときに取得するアドレス プールの IP アドレス範囲。このアドレスプールは、デバイスのインターフェイス IP アドレスのいずれかと同じサブネットに存在する必要があります。 アドレス範囲を指定する場合は、最初と最後の IP アドレスをハイフンで区切って入力します。たとえば、**10.100.10.2-10.100.10.255** です。1 つのアドレスを入力した場合、プールには 1 つのアドレスだけが含まれます。サブネット指定は入力しないでください。 範囲を定義するネットワーク/ホストポリシーオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成することもできます。複数の範囲を指定する場合は、カンマで区切ります。
Filter ACL	SSL VPN へのアクセスを制限する、拡張アクセス コントロール リスト（ACL）オブジェクトの名前。オブジェクトの名前を入力するか、[選択（Select）] をクリックしてリストから選択するか、または新しいオブジェクトを作成します。
Keep SSL VPN Client on Client Computer	ユーザが接続を切断したあとも、フルクライアントをユーザのワークステーションにインストールしたままにするかどうかを指定します。クライアントをユーザのシステムに残さないようにすると、ユーザは、SSL VPN ゲートウェイへの接続を確立するたびにクライアントをダウンロードする必要があります。
ホーム ページ URL（Home Page URL）	フル クライアントのログイン ホーム ページの Web アドレス。
Client Dead Peer Detection Timeout	パケットが SSL VPN トンネルを介してリモート ユーザから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔。1 ～ 3600 秒の範囲の値を入力します。
Gateway Dead Peer Detection Timeout	パケットが SSL VPN トンネルを介してゲートウェイから受信されるたびに、Dead-Peer Detection（DPD）タイマーがリセットされる時間間隔。1 ～ 3600 秒の範囲の値を入力します。
Key Renegotiation Method	リモート ユーザ グループ クライアントのトンネル キーをリフレッシュする方法は、次のとおりです。 • [無効（Disabled）]：トンネルキーの更新を無効にします。 • [新規トンネルの作成（Create New Tunnel）]：新しいトンネル接続を開始します。トンネルのリフレッシュサイクルの時間間隔（秒数）を [間隔（Interval）] フィールドに入力します。

[User Group] ダイアログボックス - SSL VPN スプリット トンネリング

スプリット トンネリング設定を使用して、中央サイトへのセキュアなトンネル、およびそれと同時にインターネットへの SSL VPN 用クリア テキスト トンネルを設定します。

スプリット トンネリングを使用すると、リモート クライアントは、条件に応じて、パケットを IPsec または SSL VPN トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。スプリット トンネリングがイネーブルになっている場合、宛先がトンネルの反対側でないパケットは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが必要ありません。スプリット トンネリング ポリシーは、特定のネットワークに適用されます。

ヒント　最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことを推奨します。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）の目次から **[フルトンネル（Full Tunnel）] > [スプリットトンネリング（Split Tunneling）]** を選択します。

フィールド リファレンス

表 485 : [User Group] ダイアログボックス - スプリット トンネリング設定

要素	説明
Tunnel Option	スプリット トンネリングを許可するかどうかを指定し、許可する場合は、保護するトラフィック、または暗号化されずにパブリック ネットワークを介して送信するトラフィックを指定します。 • [Disabled]（デフォルト）：トラフィックは、暗号化されずに送信されることがないか、またはゲートウェイ以外の宛先には送信されません。リモート ユーザは企業ネットワーク経由でネットワークに接続し、ローカル ネットワークにはアクセスできません。 • [指定されたトラフィックをトンネル化（Tunnel Specified Traffic）]：[宛先（Destinations）] フィールドに示されているアドレスとの間のすべてのトラフィックをトンネル化します。その他すべてのアドレスへのトラフィックは、暗号化されずに送信され、リモートユーザーのインターネット サービス プロバイダーによってルーティングされます。 • [指定されたトラフィックを除外（Exclude Specified Traffic）]：[宛先（Destinations）] フィールドに示されているアドレスとの間をトラフィックが暗号化されずに送信されます。これは、トンネル経由で企業ネットワークに接続しているリモート ユーザがプリンタなどのローカル ネットワーク上のデバイスにアクセスする場合に役立ちます。

要素	説明
宛先	トラフィックがトンネルを介して通過する必要があるネットワーク、およびトンネリングが不要なネットワークを示す、ホストまたはネットワークの IP アドレス。これらのアドレスへのトラフィックが、暗号化されてゲートウェイにトンネリングされるか、または暗号化されずに送信されるかは、[トンネルオプション（Tunnel Option）] での選択によって決まります。 10.100.10.0/24 などのネットワーク アドレスまたは 10.100.10.12 などのホスト アドレスを入力します。ネットワーク/ホストポリシーオブジェクトの名前を入力するか、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成することもできます。カンマで複数のアドレスを区切ります。
Exclude Local LANs	ローカル LAN を暗号化されたトンネルから除外するかどうかを指定します。このオプションは、[指定されたトラフィックを除外（Exclude Specified Traffic）] トンネルオプションを選択している場合にのみ選択できます。このオプションを選択すると、LAN に接続しているシステム（プリンタなど）との通信をユーザに許可するために、ローカル LAN アドレスを宛先フィールドに入力する必要がなくなります。 選択した場合、この属性によって、クライアントと同時にローカル サブネットワークにアクセスする非スプリット トンネリング接続が許可されなくなります。
Split DNS Names	スプリット トンネルを介してプライベート ネットワークに解決されるドメイン名のリスト。他のすべての名前は、パブリック DNS サーバを使用して解決されます。 ドメインのリストに最大 10 のエントリをカンマで区切って入力します。文字列全体は、255 文字以下である必要があります。

[User Group] ダイアログボックス - ブラウザ プロキシ設定

ブラウザ プロキシ設定を使用して、SSL VPN におけるフル トンネル アクセスのプロキシ バイパスを設定します。

セキュリティ アプライアンスは、HTTPS 接続を終了し、ユーザとインターネット間の中間サーバとして機能する HTTP プロキシ サーバと HTTPS プロキシ サーバに HTTP/HTTPS 要求を転送できます。プロキシバイパスはコンテンツの書き換えに代わる手法であり、元のコンテンツの変更を最小限に抑えます。カスタム Web アプリケーションで役立ちます。

ヒント このブラウザ プロキシ設定は、Microsoft Internet Explorer の場合にだけ機能します。つまり、他のタイプのブラウザでは機能しません。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）のコンテンツテーブルから [フルトンネル（Full Tunnel）] > [ブラウザプロキシ設定（Browser Proxy Settings）] を選択します。

関連項目

- SSL VPN プロキシおよびプロキシ バイパスの設定（ASA） （1782 ページ）

フィールド リファレンス

表 *486 : [User Group]* ダイアログボックス - ブラウザ プロキシ設定

要素	説明
Browser Proxy Option	リモートクライアントのブラウザ上でプロキシ設定値を設定するかどうか、および設定する方法を指定します。 • [Blank]：プロキシ設定値は設定されません。 • [Do Not Use Proxy Server]：プロキシを使用しないようにブラウザを設定します。 • [Automatically Detect Settings]：プロキシ設定を自動的に検出するようにブラウザを設定します。 • [Bypass Proxy Server for Local Addresses]：ユーザによって設定されたプロキシ設定をバイパスするようにブラウザを設定します。
プロキシ サーバ（Proxy Server）	プロキシ サーバのアドレス。 • [IP address]：アドレスを指定するネットワーク/ホスト オブジェクトの IP アドレスまたは名前。[選択（Select）] をクリックして、リストからオブジェクトを選択します。 • [Name]：完全修飾ドメイン名。proxy.example.com などです。
プロキシ サーバのポート（Proxy Server Port）	プロキシ トラフィックに使用される、サーバ上のポート番号。80 などです。1 ～ 65535 の範囲の値を入力します。
Do Not Use Proxy Server for Addresses Beginning With	プロキシを設定した場合、プロキシがバイパスされる特定のホストを指定できます。ユーザがこれらのホストをブラウザで開くと、プロキシは接続で使用されません。 完全な IP アドレスまたは完全修飾ドメイン名を入力します。10.100.10.14、www.cisco.com などです。

[User Group] ダイアログボックス - SSL VPN 接続設定

SSL VPN 接続設定ページを使用して、バナー テキストなど、ユーザ グループの SSL VPN セッション接続の設定値を設定します。SSL VPN セッションは、クライアントがセッション タイムアウトよりも長い時間接続されている場合、またはアイドル タイムアウトよりも長い時間アイドル状態である場合、切断されます。

ナビゲーション パス

[Add User Group]/[Edit User Group] ダイアログボックス （2024 ページ）の目次から [接続設定（Connection Settings）] を選択します。

フィールド リファレンス

表 487 : [User Group] ダイアログボックス - [Connection Settings]

要素	説明
アイドル タイムアウト	SSL VPN セッションのアイドル タイムアウト時間。セッションは、指定されたアイドル タイムアウトよりも長い時間クライアントがアイドル状態である場合に切断されます。値の範囲は 0 ～ 3600 秒です。
セッションのタイムアウト（Session Timeout）	SSL VPN セッションのタイムアウト時間。セッションは、ユーザがまだアクティブである場合でもこのタイムアウトに到達すると切断されます。値の範囲は 1 ～ 1209600 秒です。
バナー テキスト（Banner Text）	リモート ユーザが SSL VPN に接続したときに表示される、初期メッセージなどのバナー。 二重引用符または新しい行（Carriage Return（CR; 復帰））をバナーテキストに使用することはできません。ただし、HTML タグを挿入することで、目的のレイアウトを作成できます。

[Add WINS Server List]/[Edit WINS Server List] ダイアログボックス

[WINS Server Lists] ダイアログボックスを使用して、WINS サーバ リスト オブジェクトを作成、コピー、および編集します。WINS サーバ リスト オブジェクトによって、Windows ファイル サーバ名を IP アドレスに変換するために使用する、Windows Internet Naming Server（WINS; インターネット ネーム サービス）サーバのリストを定義します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [WINSサーバーリスト（WINS Server Lists）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化 （1825 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *488 : [WINS Server Lists]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成（299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
WINS Server List	オブジェクトに定義されている WINS サーバ。 • サーバを追加するには、[Add] ボタンをクリックし、[Add WINS Server] ダイアログボックスに入力します（[Add WINS Server]/[Edit WINS Server] ダイアログボックス （2047 ページ）を参照）。 • サーバを編集するには、サーバを選択し、[Edit] ボタンをクリックします。 • サーバを削除するには、サーバを選択し、[Delete] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）]ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）]ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[Add WINS Server]/[Edit WINS Server] ダイアログボックス

[Add WINS Server]/[Edit WINS Server] ダイアログボックスを使用して、新しい WINS サーバ エントリを作成するか、または [WINS Server Lists] ダイアログボックスのテーブル内の既存のエントリを編集します。

ナビゲーション パス

[Add WINS Server List]/[Edit WINS Server List] ダイアログボックス （2045 ページ）で、[WINS サーバーリスト（WINS Server List）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

関連項目

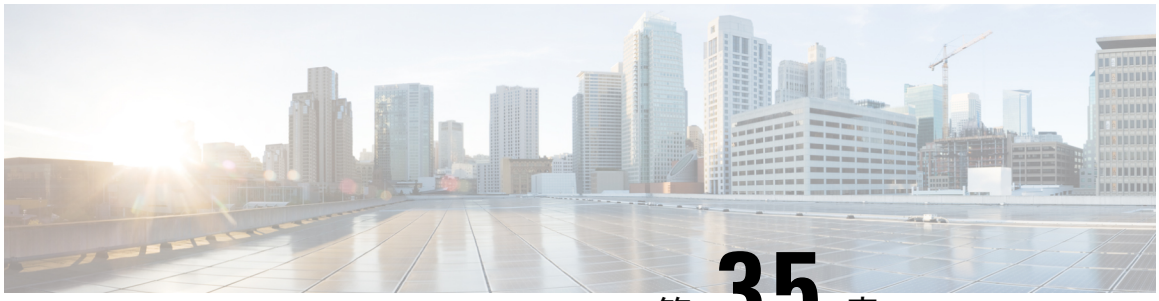
- WINS/NetBIOS Name Service（NBNS）サーバの設定による SSL VPN でのファイル システム アクセスのイネーブル化 （1825 ページ）

フィールド リファレンス

表 *489 : [Add WINS Server]/[Edit WINS Server]* ダイアログボックス

要素	説明
サーバ	Windows ファイル サーバ名を IP アドレスに変換するために使用される WINS サーバの IP アドレス。サーバを指定するネットワーク/ホスト ポリシー オブジェクトの名前を入力することもできます。[選択（Select）]をクリックしてネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。
プライマリブラウザとして設定（Set as Primary Browser）	サーバーをプライマリブラウザとして設定するかどうか。プライマリブラウザは、コンピュータおよび共有リソースのリストを維持します。

要素	説明
タイムアウト（Timeout）	セキュリティ アプライアンスが、WINS クエリーへの応答を待機する時間。この時間を超えると、セキュリティアプライアンスは、サーバが 1 台だけの場合は同じサーバに再度 WINS クエリーを送信し、サーバが複数存在する場合は次のサーバに送信します。 デフォルトのタイムアウトは 2 秒です。値の範囲は 1 ～ 30 秒です。
Retries	設定されているサーバへの WINS クエリーの送信を再試行する回数。セキュリティアプライアンスは、エラー メッセージを送信する前に、この回数に達するまでサーバのリストを順に試行します。 デフォルトは 2 です。範囲は 0 ～ 10 です。



第 35 章

マップ ビューの使用

ここでは、マップ ビューの使用方法について説明します。

- マップとマップ ビューについて （2049 ページ）
- マップの操作 [英語] （2058 ページ）
- マップでのネットワークの表示 （2065 ページ）
- マップ ビューにおける VPN の管理 （2074 ページ）
- マップ ビューにおけるデバイス ポリシーの管理 （2076 ページ）

マップとマップ ビューについて

Security Manager のマップ ビューでは、VPN およびレイヤ 3 ネットワーク トポロジのグラフィカル ビューが提供されます。

マップ ビューを使用すると、VPN 設定をグラフィカルに表示して詳細を調査できます。トンネルがトポロジで表示されることにより、複数の VPN 設定における関係（階層型 VPN など）を把握しやすくなります。また、デバイスのグループ化により、VPN 設定の全体像がわかりやすくなります。これは、ハブのフェールオーバーペアが、ピアと数百のスポークのような場合に役立ちます。

レイヤ 3 ネットワーク トポロジをグラフィカルに表し、それに管理対象デバイス（デバイス ノードと呼ばれる）を読み込むことができます。デバイス、クラウド、ネットワークなどの管理対象外のオブジェクト（マップ オブジェクトと呼ばれる）を追加することによって、トポロジの全体像がさらにわかりやすくなります。大規模なネットワークの場合は、全体のトポロジの一部だけを取り込むことによってトポロジ図を簡素化できます。トポロジマップは、今後使用する場合に備えて保存できます。

ネットワークの地理的組織や機能的組織が反映された、複数のトポロジマップを保存できます。保存したマップを親マップ上のノードにリンクすると、親マップから、より詳細な情報を含むリンクされたマップまでドリルダウンできます（詳細については、リンクされたマップの使用方法 （2064 ページ）を参照してください）。保存したマップは、必要なアクセス権を持つすべてのユーザ間で共有されます。

その他の Security Manager 機能をマップ ビューから起動できます。場合によっては、マップからノードを選択することによって機能の使用を簡素化してから、別の機能を起動できます。た

とえば、複数のノードを選択してから、それらのノードをメンバーとして含む VPN を作成できます。

ヒント　マップに表示されるネットワーク データは、通常、このようなデータの変更時に更新されます。ただし、確実に現在のネットワークデータがマップに表示されるようにするには、[マップ（Map）] > [マップの更新（Refresh Map）] を選択して手動で更新できます。

ここでは、次の内容について説明します。

- マップ ビューのメイン ページについて （2050 ページ）
- マップ ツールバー （2052 ページ）
- ナビゲーション ウィンドウの使用方法 （2053 ページ）
- マップのコンテキスト メニュー （2053 ページ）
- マップのアクセス権 （2057 ページ）

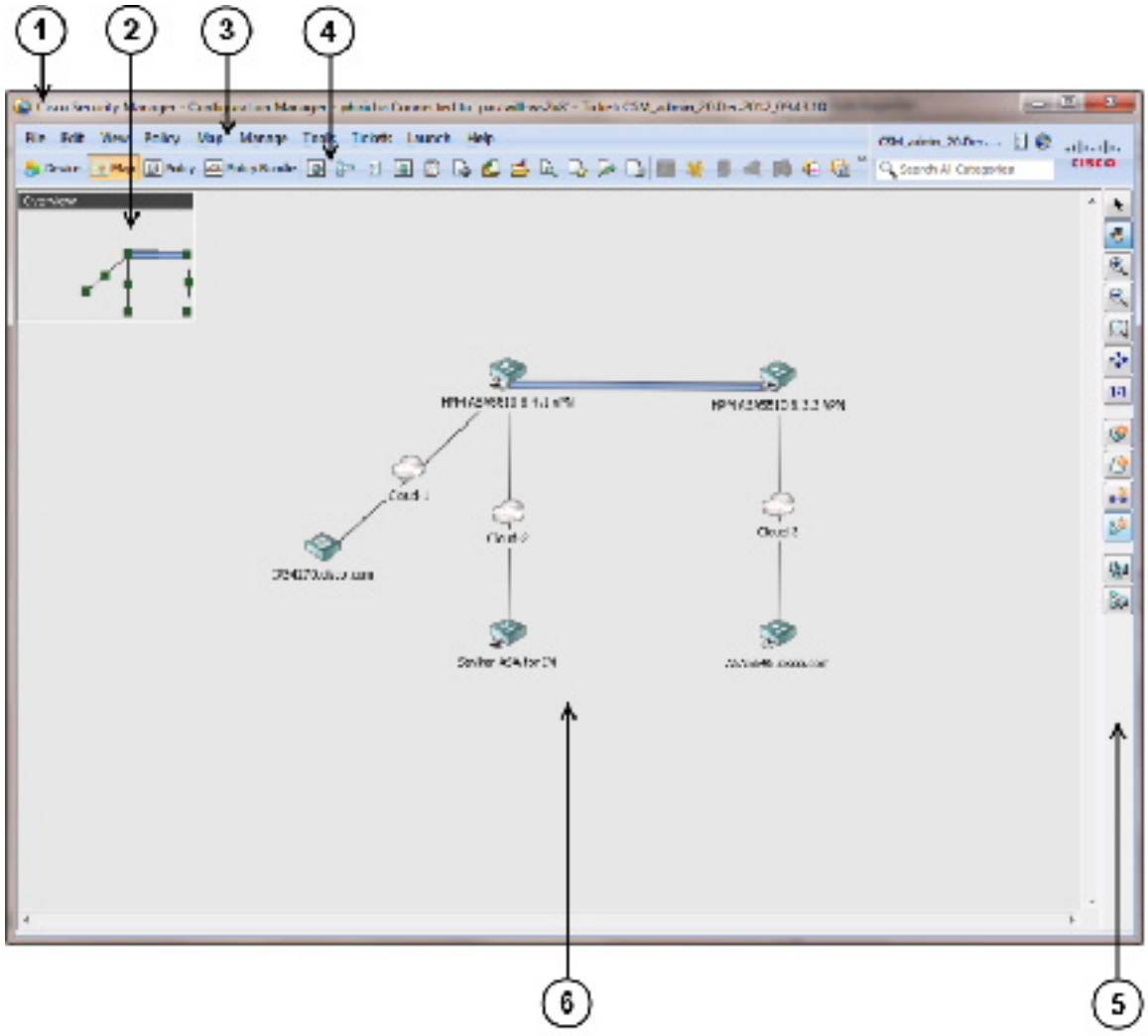
マップ ビューのメイン ページについて

マップ ビューを使用すると、カスタマイズされた視覚的なトポロジ マップでネットワークを表示できます。このトポロジ マップで、デバイス間の接続を参照したり、VPN およびアクセス コントロール設定を簡単に行ったりできます。次の図は、マップ ビューの機能領域を示しています。

マップビューのメインページを開くには、ツールバーの [マップビュー（Map View）] ボタンをクリックします。

マップ ウィンドウを切り離すと、マップを開いたままで他の製品機能を使用できるようになります。マップを切り離すには、[マップ（Map）] > [マップビューの切り離し（Undock Map View）] を選択します。マップウィンドウをドッキングするには、[マップ（Map）] > [マップビューのドッキング（Dock Map View）] を選択します。

図 *42* : マップ ビューのメイン ページ



1	タイトル バー	2	ナビゲーション ウィンドウ（ナビゲーション ウィンドウの使用方法 （2053 ページ）を参照）
3	メニュー バー（[Map] メニュー （Configuration Manager） （43 ページ）を参照）	4	ツールバー（ツールバー リファレンス （Configuration Manager） （51 ページ）を参照）
5	マップ ツールバー（マップ ツールバー （2052 ページ）を参照）	6	マップ（マップ要素について （2065 ページ）を参照）

関連項目

- マップとマップ ビューについて （2049 ページ）

- マップの操作 [英語] （2058 ページ）
- マップでのネットワークの表示 （2065 ページ）
- マップ ビューにおける VPN の管理 （2074 ページ）
- マップ ビューにおけるデバイス ポリシーの管理 （2076 ページ）

マップ ツールバー

次の表に、マップ ツールバーのボタンを示します。

表 *490* : マップ ツールバー

ツールバーボタン	説明
	マップ上のオブジェクトを選択します。ボタンをクリックし、マップ上の項目をクリックします。
	マップをパンします。ボタンをクリックし、マップ上でクリックしたままカーソルをドラッグします。
	マップをズームインします。
	マップをズームアウトします。
	描いた長方形が埋まるようにマップをズームします。
	マップ全体が表示されるようにマップをズームします。
	マップを実際のサイズまでズームします。
	Security Manager の管理対象ノードを新規作成します。インベントリに作成した新しいデバイスは、アクティブなマップにデバイス ノードとして追加されます。
	マップに新しいマップ オブジェクトを追加します。
	マップに新しいリンクを追加します。
	マップ上のノード間に新しい VPN 接続を作成します。

ツールバーボタン	説明
	マップ上にデバイス ノードとして表示するデバイスを選択します。
	マップ上に表示する VPN を選択します。

ナビゲーション ウィンドウの使用方法

ナビゲーション ウィンドウには、アクティブなマップ全体の縮小版が表示されます。影付きの長方形で、現在表示されているマップの領域を定義します。

ナビゲーション ウィンドウを使用して、表示するマップの部分を選択したり、マップ ズーム レベルを変更したりします。

- ナビゲーションウィンドウの表示を切り替えるには、**[マップ（Map）]>[ナビゲーション ウィンドウの表示/非表示（Show/Hide Navigation Window）]** を選択します。
- ナビゲーションコントロールをパンして表示するマップの一部を選択するには、影付きの長方形をクリックし、新しい場所にドラッグします。
- ズーム レベルを変更するには、影付きの長方形の隅にあるいずれかのサイズ変更ハンドルをクリックし、ドラッグして表示するマップの領域を拡大または縮小します。マップがズームされ、マップ インジケータで示されている領域が表示されます。

ナビゲーション ウィンドウのタイトル バーには、マップの名前が表示されます。マップに保存されていない変更がある場合は、マップ名の横にアスタリスク（*）が表示されます。

マップをパンおよびズームする他の方法については、マップのパン、中央への配置、およびズーム （2062 ページ）を参照してください。

マップのコンテキスト メニュー

ここでは、マップ コマンドを含むメニューについて説明します。コンテキスト メニューを開くには、マップ要素を右クリックします。

- [Managed Device Node] コンテキスト メニュー （2054 ページ）
- [Multiple Selected Nodes] コンテキスト メニュー （2055 ページ）
- [VPN Connection] コンテキスト メニュー （2056 ページ）
- [Layer 3 Link] コンテキスト メニュー （2056 ページ）
- [Map Object] コンテキスト メニュー （2056 ページ）
- [Map Background] コンテキスト メニュー （2057 ページ）

[Managed Device Node] コンテキスト メニュー

[Managed Device Node] コンテキスト メニューは、管理対象デバイスを表すマップ ノードを右クリックすると開きます。表示されるコマンドは、選択したデバイスのタイプによって異なります。次の表に、表示される可能性があるすべてのコマンドを示します。

表 *491 : [Managed Device Node]* コンテキスト メニュー

メニュー コマンド	説明
Edit Firewall Policies	デバイスのファイアウォール ポリシーを編集します。 サブメニューからファイアウォール ポリシー タイプを選択して編集します。
Edit Firewall Settings	デバイスのファイアウォール設定を編集します。 サブメニューから設定を選択して編集します。
Edit VPN Peers	デバイスが参加している VPN 内のピアを編集します。
Edit VPN Policies	デバイスの VPN ポリシーを編集します。
デバイス プロパティ	デバイス プロパティを表示します。
Clone Device	デバイスのコピーを作成します。 デバイスの複製 （160 ページ）を参照してください。
Copy Policies Between Devices	デバイスおよびその他のデバイス間でポリシーをコピーします。 デバイス間でのポリシーのコピー （251 ページ）を参照してください。
Share Device Policies	デバイスのローカル ポリシーを共有します。
Catalyst Summary Info	Security Manager によって検出されたサービス モジュール、ポート、VLAN などのシステム情報の概要を表示できます。 Catalyst サマリー情報の表示 （3403 ページ）を参照してください。
Show in Device View	選択したデバイスのデバイス ビューを開きます。
Device Manager	Device Manager を起動します。 デバイス マネージャの起動 （3697 ページ）を参照してください。
インベントリ ステータス	デバイスの [Inventory Status] ウィンドウを表示します。 [Inventory Status] ウィンドウ （3695 ページ）を参照してください。
Show VPN Peers	デバイスが参加している VPN 内のピアを表示します。
Preview Configuration	コミット済みのすべての変更を含め、デバイス設定をプレビューします。

メニュー コマンド	説明
Show Containment	デバイス内のセキュリティ コンテキストとサービス モジュールを表示します。
ノードのプロパティ	ノード プロパティを表示します。
Set Linked Map	このノードから別のマップへのリンクを作成します。
Open Linked Map	ノードにリンクされたマップを開きます。
Discover Policies on Device	デバイス上のポリシーを検出します。
Move To Center	マップをパンしてノードを中央に表示します。
デバイスの削除	デバイスをデバイス インベントリから削除します。
Remove from Map	ノードをマップから削除します。

[Multiple Selected Nodes] コンテキスト メニュー

[Multiple Selected Device Node] コンテキスト メニューは、複数のマップ ノードを選択し、選択したノードを右クリックすると開きます。

選択したノードの一部が VPN に対応していない場合は、VPN を設定するためのコマンドが表示されません。

表 *492 : [Multiple Selected Nodes]* コンテキスト メニュー

メニュー コマンド	説明
Create Point to Point VPN	選択した 2 つのデバイス間にポイントツーポイント VPN を作成します。 選択したすべてのノードが管理対象の VPN 対応ノードである必要があります。
Create Hub and Spoke VPN	選択したノードを含むハブアンドスポーク VPN を作成します。 右クリックしたノードが VPN ハブになります。選択したすべてのノードが管理対象の VPN 対応ノードである必要があります。
Create Meshed VPN	選択したノードを含む完全メッシュ VPN を作成します。 選択したすべてのノードが管理対象の VPN 対応ノードである必要があります。
Remove Selected Nodes	選択したすべてのデバイス ノードを削除します。選択したデバイス ノードを右クリックした場合にだけ表示されます。

メニュー コマンド	説明
Delete Map Objects	選択したすべてのマップ オブジェクトを削除します。選択したマップ オブジェクトを右クリックした場合にだけ表示されます。

[VPN Connection] コンテキスト メニュー

[VPN Connection] コンテキスト メニューは、マップ上の VPN 接続を右クリックすると開きます。詳細については、マップからの VPN ポリシーまたはピアの編集 （2076 ページ）を参照してください。

表 *493 : [VPN Connection]* コンテキスト メニュー

メニューコマンド	説明
Edit VPN Peers	VPN 内のピアを編集します。
Edit VPN Policies	VPN ポリシーを編集します。

[Layer 3 Link] コンテキスト メニュー

[Layer 3 Link] コンテキスト メニューは、マップ上のレイヤ 3 リンクを右クリックすると開きます。

表 *494 : [Layer 3 Link]* コンテキスト メニュー

メニューコマンド	説明
Link Properties	リンク プロパティを表示します。
Delete Link	リンクをマップから削除します。

[Map Object] コンテキスト メニュー

[Map Object] コンテキスト メニューは、管理対象デバイス以外を表すマップ オブジェクトを右クリックすると開きます。

表 *495 : [Map Object]* コンテキスト メニュー

メニュー コマンド	説明
ノードのプロパティ	ノード プロパティを表示します。
Move To Center	マップをパンしてノードを中央に表示します。
Set Linked Map	ノードをマップにリンクします。
Open Linked Map	ノードのリンク先のマップを開きます。

メニュー コマンド	説明
Delete Map Object	マップ オブジェクトを削除します。

[Map Background] コンテキスト メニュー

[Map Background] コンテキスト メニューは、マップの背景領域（つまり、オブジェクトやリンク以外）を右クリックすると開きます。

表 *496 : [Map Background]* コンテキスト メニュー

メニュー コマンド	説明
Show Devices on Map	マップ上に表示する管理対象デバイスを選択します。
Show VPNs on Map	マップ上に表示する VPN を選択します。
Add Map Object	マップ オブジェクトをマップに追加します。
Add Link	レイヤ 3 リンクをマップに追加します。
新規デバイス（New Device）	新しい管理対象デバイスを作成し、デバイス ノードとしてマップに追加します。
New VPN	新しい VPN を作成し、マップに追加します。
Find Map Node	マップ上のノードを検索します。
Open Map	保存済みのマップを開きます。
Save Map	開いたマップを保存します。
Show/Hide Navigation Window	マップのナビゲーション ウィンドウの表示を切り替えます。
マップのプロパティ	マップのプロパティを表示します。
Hierarchical layout	ネットワーク ノードを階層レイアウトで配置します。
Radial layout	ネットワーク ノードを放射レイアウトで配置します。
Circular layout	ネットワーク ノードを円形レイアウトで配置します。
Dock/Undock Map	マップ ビューを切り離します。

マップのアクセス権

マップへのアクセスは、次の 2 つのユーザ権限体系に基づいて制御されます。

- デバイス権限：マップを開くには、少なくともマップ内のすべてのデバイスに対する読み取り権限が必要です。

- マップ権限：マップへのアクセスは、Security Manager のユーザ ロールに基づきます。マップ アクセスには次の 2 つのレベルがあります。
  - 読み取り専用：マップを開くことができますが、編集はできません。このマップ権限レベルでは、マップを変更する機能は使用できません。
  - 読み取りと書き込み：マップを変更できます。すべてのマップ変更機能を使用できます。

マップの操作 [英語]

マップは、ネットワークの一部を表現したものです。ネットワークの管理ニーズに対応するために、複数のマップを作成して保存できます。マップを使用するには、マップビューを表示する必要があります（[表示（View]）> [マップビュー（Map View）] を選択）。

マップを作成して保存すると、マップ上のすべてのデバイスに対する読み取り以上のアクセス権を持っているシステム上のすべてのユーザはマップを使用できるようになります。マップ上のデバイスに対する読み取り権限を持っていないユーザがマップを開こうとしても、既存のマップのリストにそのマップは表示されません。詳細については、マップのアクセス権 （2057 ページ）を参照してください。

一度に開くことができるマップは1つだけです。マップが開いている状態で新しいマップを作成するか、または既存のマップを開くと、現在開いているマップに加えた保存されていない変更を保存するか廃棄するように要求されます。

複数のユーザが同時に同じマップを開いたり変更したりできます。あるユーザがマップに変更を保存すると、そのマップを使用している他のユーザは通知を受け取り、次のいずれかを実行できます。

- マップを他のユーザが保存したバージョンに更新します。この場合、自分で加えた変更は失われます。
- 自分のマップを新しいマップとして保存し、自分で加えた変更を保持します。

ここでは、次の内容について説明します。

- 新しいマップまたはデフォルト マップの作成 （2059 ページ）
- マップを開く （2060 ページ）
- マップの保存 （2060 ページ）
- マップの削除 （2061 ページ）
- マップのエクスポート （2061 ページ）
- マップ要素の配置 （2061 ページ）
- マップのパン、中央への配置、およびズーム （2062 ページ）
- マップ要素の選択 （2063 ページ）

- マップ ノードの検索 （2063 ページ）
- リンクされたマップの使用方法 （2064 ページ）
- マップの背景プロパティの設定 （2064 ページ）

新しいマップまたはデフォルト マップの作成

新しいマップを作成する方法は 2 つあります。

- 空のマップを作成します。新しい空のマップを作成するには、[マップ（Map）] > [新規マップ（New Map）] を選択します。マップビューをすでに表示している必要があります（[表示（View）] > [マップビュー（Map View）] を選択）。現在マップを開いており、保存されていない変更がある場合は、保存するかどうか尋ねられます。マップに要素を追加する方法については、マップでのネットワークの表示 （2065 ページ）を参照してください。
- インベントリ内のすべての管理対象デバイスと VPN を含む新しいマップを作成します。このマップはデフォルトマップと呼ばれます。マップを作成する場合は、デフォルトマップを生成することを推奨します。生成したマップを一意の名前で保存して標準マップにし、必要に応じて変更します。

デフォルト マップは必要なときにいつでも生成できます。デフォルト マップには、その生成時のインベントリが含まれます。デフォルトマップは、明示的にデフォルトマップとして保存することはできません。選択するたびにデフォルトマップが再生成されます。

次の手順では、デフォルト マップを使用して新しいマップを作成する方法について説明します。

ヒント

- マップをリフレッシュしても **[マップ（Map）] > [マップの更新（Refresh Map）]** を選択）、デフォルトマップの生成後にインベントリに追加された項目はマップに追加されません。新しいデバイスを表示するには、デフォルト マップを再び開く必要があります。

ステップ 1 マップビューで、**[マップ（Map）] > [マップを開く（Open Map）]** を選択します。

ステップ 2 [使用可能なマップ（Available Maps）] リストから [デフォルトマップ（Default Map）] を選択し、[OK] をクリックします。

（注） インベントリ内のすべてのデバイスに対する十分なアクセス権がない場合、開いたデフォルトマップには、アクセス権を持っているデバイスのサブセットだけが表示されます。詳細については、マップのアクセス権 （2057 ページ）を参照してください。

ステップ 3 デフォルトマップを標準マップとして保存するには、**[マップ（Map）] > [マップの保存（Save Map）]** または **[マップ（Map）] > [マップを次の名前で保存（Save Map As）]** を選択し、マップの名前をクリックして [OK] をクリックします。

マップを開く

既存のマップを開くには、[マップ（Map）] > [マップを開く（Open Map）] を選択し、使用可能なマップのリストから目的のマップを選択して [OK] をクリックします。マップビューをすでに表示している必要があります（表示（[View）] > [マップビュー（Map View）]）。現在マップを開いており、保存されていない変更がある場合は、保存するかどうか尋ねられます。

使用可能なマップのリストには、[デフォルトマップ（Default Map）] という特殊なマップがあります。このマップには、インベントリ内のすべての管理対象デバイスおよび VPN が含まれています。基本的には、デフォルトマップを開くたびに新しいマップを作成することになります。デフォルトマップの詳細については、新しいマップまたはデフォルトマップの作成 （2059 ページ）を参照してください。

ヒント　自分で作成したすべてのマップと、デフォルト マップを開くことができます。別のユーザーが作成したマップを開くこともできますが、そのマップに表示されるデバイスに関する必要な権限設定を持っている場合にかぎります（マップのアクセス権 （2057ページ）を参照）。

関連項目

- マップの操作 [英語] （2058 ページ）
- マップ要素について （2065 ページ）

マップの保存

アクティブなマップを保存するには、[マップ（Map）] > [マップの保存（Save Map）] を選択します。最後の保存後に加えた変更が保存されます。そのマップを保存したことがない場合は、[Save Map As] ダイアログボックスが開き、マップに名前を割り当てて保存できます。

マップを新しい名前で保存するには、[マップ（Map）] > [マップを次の名前で保存（Save Map As）] を選択します。最大 256 文字のマップ名を指定できますが、予約名「Default Map」または「New Map」は使用できません。

保存されていない変更を含むマップを閉じる場合、変更を保存するように要求されます。

保存されていない変更を含むマップが開いているときに、Security Manager セッションが非活動状態のため閉じた場合は、マップの現在のバージョンが保存されます（マップに名前がある場合）。そのマップを保存したことがない場合、マップは廃棄されます。たとえば、デフォルト マップを生成するか、または新しいマップを作成し、セッションがタイムアウトする前にマップを保存しなかった場合、そのマップは取得できなくなります。

マップの削除

不要になったマップは削除できます（編集権限がある場合）。マップを削除しても、マップに表示されるデバイスまたは VPN は削除されず、設定も削除または変更されません。マップだけが削除されます。

マップを削除すると、マップはサーバから永久に削除されます。他のユーザは、削除されたマップを使用できません。

マップを削除するには、[マップ（Map）]>[マップの削除（Delete Map）] を選択し、使用可能なマップのリストから削除するマップを選択し、[OK] をクリックします。削除の確認が求められます。

マップを削除するには、マップビューをすでに表示している必要があります（[表示（View）] > [マップビュー（Map View）] を選択）。

マップのエクスポート

マップの表示中、Security Manager の外部で使用できるように、マップを Scalable Vector Graphics（SVG）イメージ ファイルにエクスポートできます。

関連項目

- マップの操作 [英語] （2058 ページ）
- マップ要素について （2065 ページ）

ステップ 1 [マップ（Map）] > [マップのエクスポート（Export Map）] を選択します。[Export Topology Map to SVG] ダイアログボックスが開きます。

ステップ 2 ファイルの保存場所を参照します。

ステップ 3 [File name] フィールドにファイル名を入力します。正しいファイル拡張子が自動的に追加されます。

ステップ 4 [保存（Save）] をクリックします。

マップ要素の配置

マップ要素を移動するには、要素をクリックしたまま目的の位置にドラッグします。関連付けられているリンクは自動的に移動しますが、リンクのもう一方の端は移動しません。

マップ上のネットワーク ノードを定義済みのいくつかのレイアウトで自動的に配置することもできます。マップにすでに表示されているノードだけが配置されます。あとで追加したノードはレイアウトに従いません。

マップ レイアウトを選択するには、マップの背景を右クリックし、マップ コンテキスト メニューから次のいずれかのレイアウトを選択します。

- [Hierarchical Layout]：ノードを階層レイアウトで配置します。

- [Radial Layout]：ノードを放射レイアウトで配置します。
- [Circular Layout]：ノードを円形レイアウトで配置します。

マップのパン、中央への配置、およびズーム

マップをナビゲートするには多くの方法があります。マップをパン（ズーム レベルを変えずにマップ内を移動）したり、特定のマップ要素がビューの中心になるようにマップをパンしたり、ズームインまたはズームアウトして別のマップ範囲を表示したりできます。

ズーム レベルを変えずにマップをパンするには、次の手順を実行します。

- [Pan Map] ツールバー ボタンをクリックし、マップの任意の場所をクリックしたままカーソルをドラッグします。
- 表示されているページにマップ全体が収まらない場合に使用可能な、垂直および水平スクロール バーを使用します。
- ナビゲーション ウィンドウで影付きの長方形をクリックし、ドラッグします。
- 特定のマップ要素が中心になるようにマップを表示するには、要素を右クリックして、[中心に移動（Move to Center）] を選択します。

マップをズームインまたはズームアウトするには、次の手順を実行します。

マップのズーム レベルを定義済みの増分で変更するには、次の手順を実行します。

- マップをズームインするには、[マップ（Map）] > [ズームイン（Zoom In）] を選択するか、または [ズームイン（Zoom In）] ツールバーボタンをクリックします。
- マップをズームアウトするには、[マップ（Map）] > [ズームアウト（Zoom Out）] を選択するか、または [ズームアウト（Zoom Out）] ツールバーボタンをクリックします。
- マップの特定の領域をズームインするには、マップツールバーの [長方形をズーム（Zoom Rectangle）] をクリックし、マップをクリックして領域を囲むように長方形をドラッグします。マウス ボタンを離すと、長方形で定義した領域が表示されるようにマップがズームされます。
- マップの特定の領域をズームインまたはズームアウトするには、ナビゲーション ウィンドウの影付きの長方形の隅をクリックしてドラッグします。
- マップ全体を表示するには、[マップ（Map）] > [ウィンドウに合わせる（Fit to Window）] を選択します。
- マップを実際のサイズで表示するには、[マップ（Map）] > [実際のサイズで表示（Display Actual Size）] を選択します。

関連項目

- ナビゲーション ウィンドウの使用方法 （2053 ページ）

マップ要素の選択

次の表に、マップ要素の選択方法を示します。選択した要素に他の要素が含まれている（たとえば、FWSM が含まれている Catalyst スイッチなど）場合は、その包含関係が表示されます。詳細については、Catalyst スイッチ、ファイアウォール、および適応型セキュリティ アプライアンスの包含関係の表示 （2068 ページ）を参照してください。

表 *497* : ネットワーク要素の選択

選択対象	選択方法
単一のマップ要素	要素をクリックします。
複数の連続しないマップ要素	Ctrl を押しながら各要素をクリックします。
複数の連続したマップ要素	マップをクリックし、要素が含まれるように長方形をドラッグします。

マップ ノードの検索

アクティブなマップで見つられるようマップノードを検索するには、[マップ（Map）]>[マップノードの検索（Find Map Node）] を選択します。このコマンドによって、[Find Node] ダイアログボックスが開きます。

[Find Node] ダイアログボックスには、最初はマップ上のすべてのオブジェクトが表示されます。リストをフィルタリングするには、リストの上にあるフィールドを使用します（リストには、すべてのフィルタ基準を満たすオブジェクトだけが表示されます）。目的のノードが見つかったら、リスト内のそのノードを選択し、[OK] をクリックします。ノードがマップの中央に表示され、選択されます。

リストをフィルタリングするには、次の方法があります。

- [タイプ（Type）] リストからノードタイプを選択して、そのタイプのオブジェクトだけを表示します。
- [名前（Name）] フィールドに、名前を入力するか、または少なくとも名前の最初の文字を入力します。入力するとリストがフィルタリングされます。検索語句は、オブジェクト名の先頭の文字から入力する必要があります。ワイルドカード文字は使用できません。
- IP アドレスやサブネット マスクの全体または一部を入力します。情報を入力するとリストがフィルタリングされます。

リンクされたマップの使用方法

リンクされたマップは、別のマップ上のマップ要素に関連付けるマップです。大規模なネットワーク上のすべてのノードを 1 つのマップに含めるのは実用的ではないため、リンクされたマップを使用して、ネットワークの階層トポロジを作成できます。

ノードを同じマップ内の別のノードにリンクすることはできません。

はじめる前に

マップにリンクする前に、リンク先のマップを作成する必要があります。

ステップ 1 マップのリンク先となるマップ要素を右クリックし、[リンクされたマップの設定（Set Linked Map）] を選択します。[Set Linked Map] ダイアログボックスが開きます。

ステップ 2 選択したマップ要素に関連付けるマップを選択し、[OK] をクリックします。

ステップ 3 リンクされたマップを開くには、リンクされたノードを右クリックし、[リンクされたマップを開く（Open Linked Map）] を選択します。現在のマップが閉じ、リンクされたマップが開きます。

マップの背景プロパティの設定

マップの背景は、色を変更するか、またはイメージを設定することによって変更できます。推奨される背景イメージの使用方法としては、地理的領域を表すイメージの使用があります。その後、地理的な場所に従ってマップ要素を配置できます。

Security Manager には、いくつかの背景イメージが付属しています。また、イメージをサーバに転送し、背景イメージとして使用することもできます。背景イメージには、JPEG、GIF、PNG、IVL、およびSVGのファイル形式を使用できます。新しいイメージを使用する場合は、サーバに直接接続して、イメージ ファイルを Security Manager サーバ ファイル システムにコピーします。セキュリティ上の理由から、Security Manager には、ファイルをサーバに転送する手段は用意されていません。

マップの背景を設定するには、マップビューで [マップ（Map）]>[マップのプロパティ（Map Properties）] を選択して [マップの設定（Map Settings）] ダイアログボックスを開きます。

- 背景イメージを設定するには、ファイルリストでイメージを選択します（マップの背景イメージを削除するには、[なし（none）] を選択します）。

イメージがリストに表示されない場合は、[追加（Add）] をクリックし、[背景イメージのインポート（Import Background Image）] ダイアログボックスを使用して、サーバーに配置したファイルを参照します。[OK] をクリックすると、使用可能な背景イメージのリストにイメージが追加されます。

リストに表示されているイメージが不要になった場合は、イメージを選択し、[削除（Delete）] をクリックします。

ヒント　X 座標と Y 座標およびスケール設定を使用して、イメージの場所とスケールを制御できます。XY 原点は、イメージの左上隅です。正の数または負の数を使用できます。目的の結果を得るためには、設定を試してみる必要があります。スケール設定は、パーセンテージで指定します。

- 背景色を変更するには、背景色フィールドの横にある [選択（Select）] をクリックし、目的の色を選択します。

マップでのネットワークの表示

マップ ビューを使用し、マップを作成してネットワーク トポロジを表示します。マップは、ネットワークを視覚的に表現したもの、または、ネットワークが大きすぎて 1 つのマップに収まらない場合は、ネットワークの一部を表現したものです。マップは、ネットワーク内のデバイス、リンク、およびその他のオブジェクトを表すマップ要素で構成されます。マップの詳細については、マップの操作 [英語] （2058 ページ）を参照してください。

次の項では、マップの作成方法について説明します。

- マップ要素について （2065 ページ）
- マップでの管理対象デバイスの表示 （2067 ページ）
- Catalyst スイッチ、ファイアウォール、および適応型セキュリティ アプライアンスの包含関係の表示 （2068 ページ）
- ネットワーク トポロジを表すマップ オブジェクトの使用方法 （2069 ページ）
- マップにおけるレイヤ 3 リンクの追加と管理 （2072 ページ）

マップ要素について

マップに表示できるすべてのオブジェクトが、マップ要素になります。マップ要素をマップに表示して、ネットワークの一部を表現します。マップの詳細については、マップの操作 [英語] （2058 ページ）を参照してください。マップを開くには、マップを開く （2060 ページ）を参照してください。

次の表に、マップに表示できる要素を示します。

- 表 498 : デバイス ノード タイプ （2066 ページ）では、マップに表示できるデバイス ノードを示します。これらの要素は、Security Manager によって管理されます。
- 表 499 : マップ オブジェクト タイプ （2067 ページ）では、マップに表示できるマップ オブジェクトを示します。これらの要素は、Security Manager によって管理されません。
- 表 500 : マップ要素インジケータ （2067 ページ）では、デバイス ノードとともに表示できるマップ要素インジケータを示します。

表 *498 :* デバイス ノード タイプ

ノード タイプ	アイコン	説明
ファイアウォール セキュリティ コンテキスト		セキュリティ コンテキストを選択すると、親デバイスが強調表示されます。輪郭が点線で表示されている場合、そのアイコンはセキュリティ コンテキストであることを示します。
Adaptive Security Appliance		デバイスを選択すると、セキュリティ コンテキストが強調表示されます。
Firewall		デバイスを選択すると、セキュリティ コンテキストが強調表示されます。
適応型セキュリティ アプライアンスのセキュリティ コンテキスト		セキュリティ コンテキストを選択すると、親デバイスが強調表示されます。輪郭が点線で表示されている場合、そのアイコンはセキュリティ コンテキストであることを示します。
ルータ（Router）		ルータまたは VPN コンセントレータ。
Catalyst 6500/7600 または Catalyst スイッチ		Catalyst デバイス ノードを選択すると、そのノードに含まれているファイアウォール サービス モジュールが強調表示されます。
Firewall Services Module（FWSM）		ファイアウォール サービス モジュールを選択すると、そのモジュールに含まれているセキュリティ コンテキストがマップ上で強調表示されます。
FWSM セキュリティ コンテキスト		セキュリティ コンテキストを選択すると、親デバイスが強調表示されます。輪郭が点線で表示されている場合、そのアイコンはセキュリティ コンテキストであることを示します。
IPS センサーまたはセキュリティ サービス モジュール		IPS センサー。
VPN 接続		任意のタイプの VPN 接続。 GET VPN の場合、破線はグループ メンバーおよびキー サーバ間の接続を示します。

表 *499* : マップ オブジェクト タイプ

ノード タイプ	アイコン	説明
管理対象外のファイアウォール		管理対象外のファイアウォール デバイス。
管理対象外のルータ		管理対象外のルータ。
ネットワーク（Network）		指定されたアドレス空間を持つネットワーク。
ホスト（Host）		ネットワーク ホスト。 例：CSA、syslog サーバ、CA サーバ、AAA ホスト
クラウド		指定されたノード間の接続を提供する、マップ オブジェクトの不特定のグループ。
レイヤ 3 リンク	—	レイヤ 3 ネットワーク接続。

表 *500* : マップ要素インジケータ

Indicator	アイコン	説明
リンクされたマップ		ノードは別のマップにリンクされています。

関連項目

- ネットワーク トポロジを表すマップ オブジェクトの使用方法 （2069 ページ）
- マップにおけるレイヤ 3 リンクの追加と管理 （2072 ページ）

マップでの管理対象デバイスの表示

デバイス ノードは、Security Manager によって管理されているデバイスを表します。デバイス ノードをマップに追加するには、Security Manager インベントリからデバイスを選択します。

デバイス ノードをマップに追加すると、マップ上の他のノードとのレイヤ 3 接続が自動的に作成されます。詳細については、マップにおけるレイヤ 3 リンクの追加と管理 （2072 ページ）を参照してください。

管理対象ノードは、次の方法で追加、削除、または表示できます。

- **すでに Security Manager インベントリにあるデバイスを追加する場合**：[マップ（Map）] > [マップ上にデバイスを表示（Show Devices on Map）] を選択して、デバイスセレクタを開きます。使用可能なデバイスのリストから目的のデバイスを選択し、[>>] をクリックして選択したデバイスのリストに移動します。デバイス グループを選択すると、そのグループ内のすべてのデバイスを移動できます。選択したデバイスのリストに目的のノードがあ

る場合は、[OK] をクリックします。選択済みリスト内のデバイスだけがマップに表示されます。

デバイスを削除するには、選択済みデバイスのリストでデバイス選択して [<<] をクリックします。

- **新しいデバイスをマップとデバイスインベントリに追加する場合**：マップツールバーの [新規デバイス（New Device）] ボタンをクリックするか、またはマップの背景を右クリックして [新規デバイス（New Device）] を選択します。[New Device] ダイアログボックスが開きます。デバイス インベントリへのデバイスの追加 （94 ページ）の手順に従って新しいデバイスを追加します。
- **管理対象ノードを削除する場合**：ノードを右クリックし、[マップから削除（Remove from Map）] を選択します。
- **デバイスビューで開いているマップにデバイスを配置する場合**：デバイスセレクタでデバイスを右クリックし、[マップビューに表示（Show in Map view）] を選択します。デバイスはアクティブなマップに表示される場合、切り離されたマップの中心に配置され、強調表示されます。デバイスがアクティブなマップに表示されない場合は、デバイスが見つからないことが通知されます。
- **マップからデバイスビューにデバイスを配置する場合**：デバイスを右クリックし、[デバイスビューに表示（Show in Device View）] を選択します。デバイスが選択された状態のデバイス ビューが開き、そのデバイスのポリシーを編集できます。

関連項目

- マップ要素について （2065 ページ）
- Catalyst スイッチ、ファイアウォール、および適応型セキュリティ アプライアンスの包含関係の表示 （2068 ページ）

Catalyst スイッチ、ファイアウォール、および適応型セキュリティ アプライアンスの包含関係の表示

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、拡張機能はサポートしていません。

Catalyst や Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）デバイスとそのサービス モジュールやセキュリティ コンテキスト間の包含関係、PIX 7.x+ デバイスや FWSM とそのセキュリティ コンテキスト間の包含関係、または IPS デバイスとその仮想センサー間の包含関係は、次のようにマップに表示されます。

- Catalyst デバイスを選択すると、その Firewall Services Module（FWSM; ファイアウォール サービス モジュール）を表すノードが強調表示されます。

- ASA を選択すると、そのセキュリティ サービス モジュールを表すノードが強調表示されます。
- サービス モジュールを選択すると、そのモジュールを含むデバイスが強調表示されます。
- IPS デバイスを選択すると、そのデバイスに定義されている仮想センサーを表すノードが強調表示されます。
- ノードを右クリックして [包含を表示（**Show Containment**）] を選択すると、ASA、ファイアウォール、または FWSM デバイスに含まれているセキュリティコンテキストのリスト、または IPS デバイスに含まれている仮想センサーのリストを表示できます。このコマンドを選択すると、デバイス内のサービス モジュールも表示されます。
- セキュリティ コンテキスト ノードを選択すると、そのすべての祖先デバイス ノードが強調表示されます。
- 仮想センサーを選択すると、そのセンサーが定義されているデバイスが強調表示されます。

ネットワーク トポロジを表すマップ オブジェクトの使用方法

Security Manager によって管理されないオブジェクト（デバイス、リンクなど）を表すマップ要素をマップに追加できます。これらのノードはマップ オブジェクトと呼ばれます。マップ オブジェクトを使用すると、より有用なネットワーク トポロジ表現を作成できます（管理対象デバイスを追加する場合は、マップでの管理対象デバイスの表示 （2067 ページ）を参照してください）。

マップ要素がデバイス ノード、マップ ノード、または両方のタイプの組み合わせであるかどうかにかかわらず、マップ要素間にレイヤ 3 リンクを追加できます。

ヒント マップオブジェクトを削除するには、オブジェクトを右クリックし、[マップオブジェクトの削除（Delete Map Object）] を選択します。

ステップ 1 [マップ（Map）] > [マップオブジェクトの追加（Add Map Object）] を選択します。[Add Map Object] ダイアログボックスが表示されます（[Add Map Object] および [Node Properties] ダイアログボックス （2070 ページ）を参照）。

ステップ 2 次のいずれかを実行します。

- Security Manager ポリシーオブジェクトの定義に基づくマップオブジェクトを追加する場合は、[ポリシーオブジェクトのコピー（Copy Policy Object）] をクリックして [Select Policy Object] ダイアログボックス （2071 ページ）を開きます。次に、オブジェクトのタイプ（AAA サーバー、ネットワーク/ホスト、PKI 登録）を選択し、[選択（Select）] をクリックしてオブジェクトを選択します。[ポリシーオブジェクトの選択（Select Policy Object）] ダイアログボックスで [OK] をクリックします。ポリシー オブジェクト内の情報が [Add Map Object] ダイアログボックスに入力されます。

オブジェクトの名前がマップ オブジェクト名として使用されますが、この名前は必要に応じて変更できます。

- ポリシーオブジェクトに基づかないマップオブジェクトを追加する場合は、[名前（Name）] フィールドにマップオブジェクトの名前を入力します。

ステップ 3 [タイプ（Type）] リストから、ノードが表すオブジェクトのタイプを選択します。ポリシー オブジェクトを選択した場合は、そのタイプが事前に選択されますが、選択を変更できます。

ステップ 4 （任意）各インターフェイスに対して次の操作を実行して、ノードにインターフェイスを追加します。

a) [追加（Add）] をクリックして [Interface Properties] ダイアログボックス （2072 ページ）を開きます。項目がすでにリストに表示されている場合は、その項目を選択し、[編集（Edit）] をクリックして変更します。

b) インターフェイス名、IP アドレス、およびネットワークマスクを入力し、[OK] をクリックします。

ステップ 5 [OK] をクリックマップ オブジェクトがマップの中央に追加されます。オブジェクトを目的の場所に移動します。

[Add Map Object] および [Node Properties] ダイアログボックス

管理対象外のマップ オブジェクトの場合、[Add Map Object] ダイアログボックスと [Node Properties] ダイアログボックスは同じです。[Add Map Object] ダイアログボックスでは、オブジェクトをマップに追加します。[Node Properties] ダイアログボックスでは、マップ オブジェクトのプロパティを表示または編集します。詳細については、ネットワーク トポロジを表すマップ オブジェクトの使用方法 （2069 ページ）を参照してください。

管理対象マップ オブジェクト（管理対象デバイスなど）の場合、[Node Properties] ダイアログボックスは読み取り専用です。このダイアログボックスには、オブジェクト名、タイプ、およびインターフェイス名と IP アドレスのリスト（Security Manager でデバイスに対して定義されている場合）が表示されます。下の参照情報は、このバージョンの [Node Properties] ダイアログボックスには適用されません。

ナビゲーション パス

- [マップオブジェクトの追加（Add Map Object）] ダイアログボックスを開くには、[マップ（Map）] > [マップオブジェクトの追加（Add Map Object）] を選択します。
- [ノードのプロパティ（Node Properties）] ダイアログボックスを開くには、マップオブジェクトまたは管理対象デバイスを右クリックし、[ノードのプロパティ（Node Properties）] を選択します。

フィールド リファレンス

表 *501* : 管理対象外のノードの *[Add Map Object]* および *[Node Properties]* ダイアログボックス

要素	説明
名前	マップ オブジェクトの名前。ポリシー オブジェクトを選択した場合は、オブジェクトの名前が自動的に使用されますが、この名前は変更できます。
[Copy Policy Object] ボタン	クリックして、[Select Policy Object] ダイアログボックス （2071 ページ）でマップ オブジェクトの基本として使用するポリシー オブジェクトを参照します。
[Type] リスト	作成するオブジェクトのタイプ。ポリシー オブジェクトを選択した場合は、タイプが自動的に選択されますが、必要に応じてタイプを変更できます。
インターフェイス テーブル	ノードのインターフェイス。ポリシー オブジェクトを選択した場合は、情報がこのテーブルに追加されていることがあります。 • インターフェイスを追加するには、[追加（Add）]（+）ボタンをクリックし、[Interface Properties] ダイアログボックス （2072 ページ）に値を入力します。 • インターフェイスを編集するには、インターフェイスを選択し、[編集（Edit）]（鉛筆）ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[削除（Delete）]（ゴミ箱）ボタンをクリックします。

[Select Policy Object] ダイアログボックス

[Select Policy Object] ダイアログボックスを使用して、ポリシー オブジェクトで定義されているオブジェクトをマップに追加します。

マップに追加するノードが定義されているオブジェクトのタイプを [ポリシーオブジェクトの選択（Select a Policy Object）] リストから選択し、[選択（Select）] をクリックして特定のポリシーオブジェクトを選択します。オブジェクトの名前がわかっている場合は、[選択（Select）] をクリックする代わりに、テキストボックスに名前を入力できます。

詳細については、ネットワーク トポロジを表すマップ オブジェクトの使用方法 （2069 ページ）を参照してください。

ナビゲーション パス

このダイアログボックスを開くには、[マップオブジェクトの追加（Add Map Object）] ダイアログボックスで [ポリシーオブジェクトのコピー（Copy Policy Object）] をクリックします（[Add Map Object] および [Node Properties] ダイアログボックス （2070 ページ）を参照）。

[Interface Properties] ダイアログボックス

[Interface Properties] ダイアログボックスを使用して、マップ オブジェクトのインターフェイスを追加および編集します。詳細については、ネットワーク トポロジを表すマップ オブジェクトの使用方法 （2069 ページ）を参照してください。

ナビゲーション パス

このダイアログボックスを開くには、[Add Map Object] および [Node Properties] ダイアログボックス （2070 ページ）で [追加（Add）] または [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *502 : [Interface Properties]* ダイアログボックス

要素	説明
Interface Name	インターフェイス名。
Interface IP Addr/Mask	インターフェイスの IP アドレスとネットワーク マスク。たとえば、10.100.10.0/24、10.100.10.0/255.255.255.0 など。

マップにおけるレイヤ 3 リンクの追加と管理

レイヤ 3 リンクは、2 つのデバイス インターフェイス間のネットワーク接続を表すマップ上の線です。

インターフェイス情報を含むマップ要素を追加すると、レイヤ 3 接続情報が自動的にマップに追加されます。インターフェイス情報を含むマップ要素を追加すると、次のいずれかの処理が実行されます。

- マップ上でネットワーク マップ オブジェクトとして表されていないネットワークにインターフェイスがある場合は、ネットワーク マップ オブジェクトが新しいマップ要素へのレイヤ 3 リンクとともにマップに追加されます。
- マップ上でネットワーク マップ オブジェクトとして表されているネットワークにインターフェイスがある場合は、新しいマップ要素とネットワーク マップ オブジェクト間にレイヤ 3 リンクが追加されます。

レイヤ 3 リンクのエンドポイントであるノードインターフェイスを削除すると、リンクも削除されます。

デバイスノードとマップオブジェクト間に他のレイヤ 3 リンクを追加して、ネットワークの接続を示すことができます。マップにレイヤ 3 リンクを追加しても、ネットワーク デバイスは設定されません。レイヤ 3 リンクは、マップ上の視覚要素にすぎません。

レイヤ 3 リンクを作成して、マップ上の 2 つのインターフェイスを接続します。選択したインターフェイスによっては、レイヤ 3 リンクに中間ネットワークまたはネットワーク クラウドが

含まれる場合があります。接続されたインターフェイス間に挿入する中間ネットワークおよびネットワーク クラウドを選択できる場合もあります。

次の手順では、新しいレイヤ 3 リンクを手動で作成する方法について説明します。

ヒント

- ネットワーク オブジェクトとリンクの自動追加は、自動リンクと呼ばれます。プライベート ネットワーク アドレスまたは特定の予約済みネットワーク アドレスを自動的に追加しないように自動リンクを設定できます。設定するには、[ツール（Tools）]>[Security Manager 管理（Security Manager Administration）] を選択してから、[自動リンク（Autolink）] をクリックします。
- リンクのプロパティを表示するには、レイヤ3リンクを右クリックし、[リンクプロパティ（Link Properties）] を選択します。
- レイヤ 3 リンクを削除するには、削除するレイヤ 3 リンクを右クリックし、[リンクの削除（Delete Link）] を選択します。レイヤ3リンクを削除しても、マップ要素間の中間ネットワークまたはネットワーク クラウドは削除されません。

ステップ 1 マップビューで、[マップ（Map）]>[リンクの追加（Add Link）] またはツールバーの [リンクの追加（Add Link）] ボタンをクリックします。

ステップ 2 接続するマップ要素の一方をクリックしてから、接続するもう一方のマップ要素をクリックします。

ステップ 3 マップ要素にインターフェイスが含まれている場合は、 [Select Interfaces] および [Link Properties] ダイアログボックス （2073 ページ）でリンクの送信元インターフェイスと宛先インターフェイスを選択し、[OK] をクリックします。

選択したインターフェイスによっては、[Add Link] ダイアログボックスが開く場合があります。

ステップ 4 [Add Link] ダイアログボックス （2074 ページ）が開いた場合は、挿入する中間オブジェクトおよびネットワーククラウドを選択し、[OK] をクリックします。

[Select Interfaces] および [Link Properties] ダイアログボックス

[Select Interfaces] および [Link Properties] ダイアログボックスは、マップ上のレイヤ 3 リンクで使用されます。これらのダイアログボックスには、リンクの送信元と宛先のデバイスに関する情報が表示されます（送信元は、リンクの作成時に最初にクリックしたデバイスです）。

リンクを作成する場合は、[Select Interfaces] ダイアログボックスを使用します。Security Manager でデバイスにインターフェイスが定義されている場合は、作成するリンクの目的の送信元インターフェイスと宛先インターフェイスを [送信元/宛先インターフェイス（Source/Destination Interface）] リストから選択します。

ヒント　リンクの作成時にどちらのデバイスにもインターフェイスが定義されていない場合は、インターフェイス リストがグレーになります。一方のデバイスにインターフェイスが定義されている場合は、両方のフィールドがアクティブですが、インターフェイスが定義されていないデバイスのフィールドは空です。リンク プロパティを表示する場合は、インターフェイスを変更できません。

ナビゲーション パス

レイヤ3リンクの作成方法またはリンクのプロパティの表示方法については、マップにおけるレイヤ 3 リンクの追加と管理　（2072 ページ）を参照してください。

[Add Link] ダイアログボックス

[Add Link] ダイアログボックスを使用して、マップに追加するレイヤ 3 リンクの表し方を選択します。

[Add Link] ダイアログボックスの内容は、接続するノードとインターフェイスによって異なります。接続するノード間に挿入する各中間マップ オブジェクト（ネットワークまたはクラウド）のチェックボックスをオンにします。必要に応じて、マップ オブジェクトの名前を変更できます。

ナビゲーション パス

接続対象として選択したインターフェイスによっては、ノード間にリンクを追加するときに、このダイアログボックスが開く場合があります。手順については、マップにおけるレイヤ3リンクの追加と管理　（2072 ページ）を参照してください。

マップ ビューにおける VPN の管理

ここでは、マップ ビューで VPN を管理する方法について説明します。

- マップにおける既存 VPN の表示　（2074 ページ）
- マップ ビューにおける VPN トポロジの作成　（2075 ページ）
- マップからの VPN ポリシーまたはピアの編集　（2076 ページ）

マップにおける既存 VPN の表示

マップで既存の VPN を表示するには、[マップ（Map）] > [マップでVPNを表示（Show VPNs on Map）] を選択します。既存の VPN を含むリストが表示されます。使用可能な VPN のリストから目的の VPN を選択し、[>>] をクリックして選択済みリストに移動します。

ヒント　このコマンドを使用して VPN を削除することもできます。選択済み VPN リストから削除する VPN を選択し、[<<] をクリックします。VPN を削除すると、VPN トンネルだけが削除されます。デバイス ノードはマップ上に残ります。

VPN を表示すると、そのすべてのメンバー デバイスがデバイス ノードとしてマップに追加され、そのすべてのトンネルが強調表示されます。ただし、以前にマップから削除したデバイスは、表示する VPN のメンバーであっても追加されません。このようなデバイスは手動でマップに追加できます。追加すると、その VPN 接続が表示されます。

VPN トンネルは、2 つのデバイス間の VPN 接続を表すマップ上の線です。VPN トンネルは、VPN のメンバーであるデバイス ノードを追加しても自動的にはマップに追加されません。ただし、VPN がマップに表示するものとしてすでに選択されている場合は、VPN 内のデバイスをマップに追加すると、トンネルも表示されます。

マップで使用されるアイコンの説明については、マップ要素について （2065ページ）を参照してください。

マップ ビューにおける VPN トポロジの作成

マップに表示されている VPN 対応管理対象デバイス ノード間に VPN 接続を作成できます。ただし、エクストラネット VPN は作成できません。

VPN を作成するには、次のいずれかを実行します。

- ツールバーの [新規VPN（New VPN）] ボタンをクリックし、設定する VPN のタイプ（ポイントツーポイント、ハブアンドスポーク、または完全メッシュ）を選択します。
- VPN に参加させるデバイスを選択し（複数のデバイスを選択する場合は Ctrl を押しながらクリック）、右クリックして目的の VPN タイプのコマンドを選択するか、または [新規VPN（New VPN）] ボタンをクリックして VPN タイプを選択します。

次のヒントを考慮してください。

- ポイントツーポイント VPN を作成する場合は、2 つのデバイスだけを選択します。
- ハブアンドスポーク VPN を作成する場合は、右クリックしたデバイスが最初にハブとして定義されますが、ウィザードで変更できます。
- ウィザードで、デバイスを追加または削除できます。マップで選択したデバイスに制限されません。

どちらの方法を使用しても、Create VPN ウィザードが開き、VPN を作成できます。詳細については、VPN トポロジの作成または編集 （1416ページ）を参照するか、またはウィザードの [Help] ボタンをクリックしてください。

ウィザードを完了すると、マップに VPN が表示されます。

関連項目

- マップ要素の選択 （2063 ページ）

マップからの VPN ポリシーまたはピアの編集

マップ ビューから、VPN ポリシー、または VPN に参加しているピアを編集できます。ポリシーまたはピアを編集するには、VPN トンネルまたはデバイス ノードを右クリックし、次のいずれかのコマンドを選択します。

- [VPN ポリシーの編集（Edit VPN Policies）]：VPN を定義するポリシーを編集できる Site-to-Site VPN Manager を開きます。詳細については、 [Site-to-Site VPN Manager] ウィンドウ （1404 ページ）を参照してください。
- [VPN ピアの編集（Edit VPN Peers）]：VPN に参加しているピアを設定できるダイアログボックスを開きます。詳細については、ダイアログボックスの[ヘルプ（Help）]ボタンをクリックしてください。
- [VPN ピアの表示（Show VPN Peers）]：リストを編集しないで VPN に参加しているデバイスを表示します（[VPN ピア（VPN Peers）] ダイアログボックス）。

デバイスが複数の VPN に参加している場合は、まず、適切なダイアログボックスが開く前に [Select VPN to Configure] ダイアログボックスで目的の VPN を選択するように要求されます。

マップ ビューにおけるデバイス ポリシーの管理

マップ ビューでは、基本的なポリシー管理だけを実行したり、ファイアウォール サービス ポリシーを設定したりできます。その他のタイプのポリシーは設定できません。ここでは、マップ ビューからポリシーを管理する方法について説明します。

- マップ ビューにおける基本的なポリシー管理の実行 （2076 ページ）
- マップ ビューにおけるファイアウォール ポリシーの管理 （2077 ページ）
- マップ ビューにおけるファイアウォール設定の管理 （2078 ページ）

マップ ビューにおける基本的なポリシー管理の実行

マップ ビューでは、一部の基本的なポリシー管理タスクを実行できます。デバイスを右クリックし、次のいずれかのコマンドを選択します。

- **Copy Policies Between Devices**：ローカルデバイスポリシーをあるデバイスから別のデバイスにコピーします。ポリシーのコピーの詳細については、 デバイス間でのポリシーのコピー （251 ページ）を参照してください。

- **Share Device Policies**：ローカルデバイスポリシーから共有ポリシーを作成します。ポリシーの共有の詳細については、選択したデバイスの複数のポリシーの共有 （263 ページ）を参照してください。
- **Clone Device**：デバイス（ポリシーを含む）のコピーを作成します。デバイスの複製の詳細については、デバイスの複製 （160 ページ）を参照してください。
- **Preview Configuration**：デバイスに対して生成される設定ファイル（前回の展開からの変更を含む）を表示します。設定のプレビューの詳細については、設定のプレビュー （535 ページ）を参照してください。
- **Discover Policies on Device**：デバイスで定義されているポリシーを検出し、それらのポリシーを Security Manager で設定します。その際、デバイスに対して Security Manager で定義されているポリシーをすべて消去します。デバイス検出の詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

関連項目

- 展開の管理 （481 ページ）
- デバイス インベントリの管理 （87 ページ）
- ポリシーの管理 （209 ページ）

マップ ビューにおけるファイアウォール ポリシーの管理

マップ ビューでは、デバイスのファイアウォール ポリシーを設定できます。これらのポリシーは、共有ポリシーになるのではなく、デバイスに対してローカルになります（共有ポリシーを設定するにはポリシー ビューを使用する必要があります）。

ヒント 共有ポリシーをデバイスに割り当てる場合は、マップ ビューにおける基本的なポリシー管理の実行 （2076 ページ）を参照してください。

マップ ビューでデバイスのローカル ファイアウォール ポリシーを設定するには、デバイスを右クリックし、次のいずれかのコマンドを選択します。

- [ファイアウォールポリシーの編集（Edit Firewall Policies）]>[AAA ルール（AAA Rules）]：AAA ポリシーを設定します。このポリシーでは、デバイスへのアクセスが許可されるユーザーおよびアクセス権を持つユーザーが使用できるサービスを制御します。AAA ルールの設定の詳細については、[AAA Rules] ページ （880 ページ）を参照してください。
- [ファイアウォールポリシーの編集（Edit Firewall Policies）]>[アクセスルール（Access Rules）]：デバイスを通過するトラフィックを制御するアクセスルールポリシーを設定します。アクセス ルールの設定の詳細については、[Access Rules] ページ （924 ページ）を参照してください。

- [ファイアウォールポリシーの編集（Edit Firewall Policies）] > [インスペクションルール（Inspection Rules）]：インスペクション ルール ポリシーを設定します。このポリシーでは、アプリケーションレイヤのトラフィックを分析し、TCP および UDP セッションを追跡して詳細なアクセスコントロールを実行します。インスペクション ルールの設定の詳細については、[Inspection Rules] ページ （986 ページ）を参照してください。
- [ファイアウォールポリシーの編集（Edit Firewall Policies）] > [ボットネット トラフィック フィルタ ルール（Botnet Traffic Filter Rules）]：（ASA 8.2 以降だけ）Web トラフィックをモニターするボットネット トラフィック フィルタ ルール ポリシーを設定します。ボットネット トラフィック フィルタ ルールの設定の詳細については、[Botnet Traffic Filter Rules] ページ （1174 ページ）を参照してください。
- [ファイアウォールポリシーの編集（Edit Firewall Policies）] > [トランスペアレント ルール（Transparent Rules）]：トランスペアレント ファイアウォールの EtherType ルールを定義するトランスペアレント ルール ポリシーを設定します。インスペクション ルールの設定の詳細については、[Transparent Rules] ページ （1300 ページ）を参照してください。
- [ファイアウォールポリシーの編集（Edit Firewall Policies）] > [Web フィルタルール（Web Filter Rules）]：Web アクセスのルールを定義する Web フィルタルールポリシーを設定します。Web フィルタ ルールの設定の詳細については、[Webフィルタルール（Web Filter Rules）] ページ（ASA/PIX/FWSM） （1138 ページ）または [Web Filter Rules] ページ（IOS） （1150 ページ）を参照してください。
- [ファイアウォールポリシーの編集（Edit Firewall Policies）] > [ゾーンベースのファイアウォールルール（Zone Based Firewall Rules）]：（IOS 12.4(6)T 以降のみ）セキュリティ ゾーンを使用してインスペクションと Web フィルタリングを設定するゾーンベースのファイアウォール ルール ポリシーを設定します。ゾーン ベースのファイアウォール ルールの設定については、[Zone-based Firewall Rules] ページ （1272 ページ）を参照してください。

関連項目

- ファイアウォール サービスの概要 （755 ページ）
- ポリシーの管理 （209 ページ）

マップ ビューにおけるファイアウォール設定の管理

マップ ビューでは、デバイスのファイアウォール設定ポリシーを設定できます。これらのポリシーは、共有ポリシーになるのではなく、デバイスに対してローカルになります（共有ポリシーを設定するにはポリシー ビューを使用する必要があります）。

ヒント　共有ポリシーをデバイスに割り当てる場合は、マップ ビューにおける基本的なポリシー管理の実行 （2076 ページ）を参照してください。

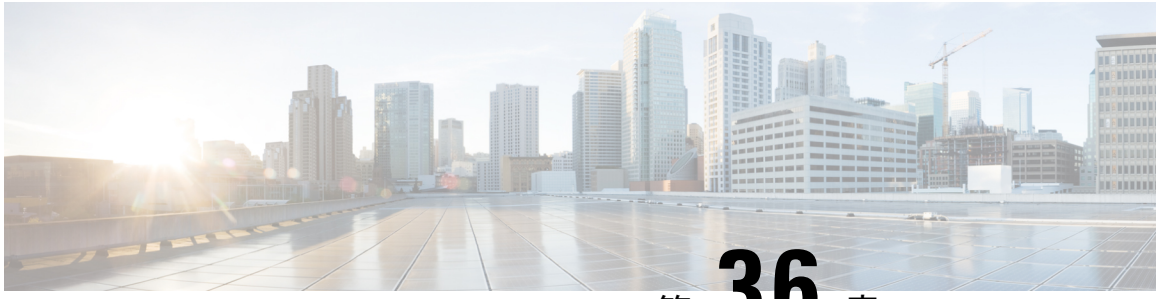
マップ ビューでデバイスのローカル ファイアウォール設定ポリシーを設定するには、デバイスを右クリックし、次のいずれかのコマンドを選択します。

- **[ファイアウォール設定の編集（Edit Firewall Settings）] > [AAAファイアウォール（AAA Firewall）]**：（ASA/PIX/FWSM のみ）プロキシ、認証チャレンジ、MAC 免除リスト、およびその他の一般的な AAA 設定を定義する AAA ファイアウォール設定ポリシーを設定します。AAA ファイアウォール設定の詳細については、[AAA Firewall] 設定ページの [Advanced Setting] タブ （895 ページ）および [AAA Firewall] ページの [MAC-Exempt List] タブ （902 ページ）を参照してください。
- **[ファイアウォール設定の編集（Edit Firewall Settings）] > [アクセス制御（Access Control）]**：最適化およびその他の一般的なアクセス制御の設定を定義するアクセス制御設定ポリシーを設定します。アクセス コントロール設定の詳細については、[Access Control Settings] ページ （944 ページ）を参照してください。
- **[ファイアウォール設定の編集（Edit Firewall Settings）] > [AuthProxy]**：（IOS デバイスのみ）認可プロキシの一般的な設定を行う AuthProxy 設定ポリシーを設定します。認可プロキシの設定の詳細については、[AAA] ページ （905 ページ）を参照してください。
- **[ファイアウォール設定の編集（Edit Firewall Settings）] > [インスペクション（Inspection）]**：（IOS デバイスのみ）インスペクション ルールのタイムアウトおよびセッション設定を定義するインスペクション設定ポリシーを設定します。インスペクション設定の詳細については、IOS デバイスのインスペクション ルールの設定 （1129 ページ）を参照してください。
- **[ファイアウォール設定の編集（Edit Firewall Settings）] > [Webフィルタ（Web Filter）]**：Web フィルタリングに使用するサーバーを設定する Web フィルタ設定ポリシーを設定します。Web フィルタ設定の詳細については、Web Filter 設定ページ （1156 ページ）を参照してください。
- **[ファイアウォール設定の編集（Edit Firewall Settings）] > [ゾーンベースのファイアウォール（Zone Based Firewall）]**：（IOS 12.4(6)T 以降のデバイス）ゾーンおよび Trend Web フィルタサーバー設定を定義するゾーンベースのファイアウォール設定を設定します。

第 IV 部

IPS の設定

- IPS 設定を開始する前に （2083 ページ）
- IPS デバイスインターフェイスの管理 （2127 ページ）
- 仮想センサーの設定 （2151 ページ）
- IPS シグニチャの定義 （2165 ページ）
- イベント アクション ルールの設定 （2211 ページ）
- IPS 異常検出の管理 （2247 ページ）
- グローバル相関の設定 （2265 ページ）
- Attack Response Controller でのブロッキングとレート制限の設定 （2275 ページ）
- IPS センサーの管理 （2299 ページ）
- IOS IPS ルータの設定 （2315 ページ）



第 36 章

IPS 設定を開始する前に

Cisco Intrusion Prevention System（IPS; 侵入防御システム）センサーは、ネットワーク トラフィックの疑わしいアクティビティやアクティブなネットワーク攻撃のリアルタイム モニタリングを実行するネットワーク デバイスです。IPS センサーは、ネットワーク パケットとフローを分析して、その内容がネットワークに対する攻撃を示しているように見えるかどうかを判断します。

Cisco Security Manager を使用して、センサーを設定および管理できます。センサーには、専用のスタンドアロン ネットワーク アプライアンス、Catalyst 6500 スイッチ モジュール、サポートされる ASA デバイスまたはルータで実行されているサービス モジュール、およびサービス統合型ルータで実行されている IPS 対応 Cisco IOS ソフトウェア イメージがあります。サポートされる IPS デバイスおよびソフトウェア バージョンの完全なリストについては、このバージョンの製品の『Supported Devices and Software Versions for Cisco Security Manager』を参照してください。

この章は次のトピックで構成されています。

- IPS ネットワーク検知について （2084 ページ）
- IPS 設定の概要 （2088 ページ）
- 許可ホストの識別 （2091 ページ）
- SNMP の設定 （2092 ページ）
- ユーザ アカウントとパスワードの要件の管理 （2101 ページ）
- NTP サーバの識別 （2112 ページ）
- DNS サーバの識別 （2113 ページ）
- HTTP プロキシ サーバの識別 （2114 ページ）
- IPS SSHv2 の既知のホストキー （2115 ページ）
- IPS SSHv1 フォールバック設定の指定 （2116 ページ）
- 外部製品インターフェイスの設定 （2117 ページ）
- IPS ロギング ポリシーの設定 （2121 ページ）
- IPS ヘルスモニター （2122 ページ）
- IPS セキュリティ設定の指定 （2125 ページ）

IPS ネットワーク検知について

ネットワーク検知は、Cisco IPS センサー（アプライアンス、スイッチモジュール、ネットワーク モジュール、および SSM）と Cisco IOS IPS デバイス（IPS 対応のイメージがある Cisco IOS ルータと Cisco ISR）で実行できます。これらの検知プラットフォームは、Cisco Intrusion Prevention System のコンポーネントであり、Cisco Security Manager を通じて管理および設定できます。これらの検知プラットフォームは、ネットワーク トラフィックをリアルタイムでモニタおよび分析します。これは、ネットワーク フロー検証、広範囲に渡る埋め込み型シグニチャ ライブラリ、および異常検出エンジンに基づいて異常や悪用を探すことで行います。ただし、これらのプラットフォームは検出した侵入への対応方法が異なります。

ヒント Cisco IPS センサーと Cisco IOS IPS デバイスは、IPS デバイスまたは単純にセンサーと総称されることがあります。ただし、Cisco IOS IPS は、完全に専用の IPS ソフトウェアを実行せず、その設定に IPS デバイス固有のポリシーは含まれません。また、Cisco IOS IPS の方が、実行できる検知の量が限られています。次のセクションでは、Cisco IOS IPS ではなく、IOS ルータにインストールされているサービスモジュールを含め、専用の IPS デバイスの使用に焦点を当てます。Cisco IOS IPS に焦点を当てた説明については、Cisco.com の『Intrusion Prevention System (IPS) Cisco IOS Intrusion Prevention System Deployment Guide』およびIOS IPS ルータの設定 （2315 ページ）http://www.cisco.com/go/iosips を参照してください。

IPS デバイスが不正なネットワーク アクティビティを検出した場合、接続の終了、関連するホストの永続的なブロックなどのアクションを実行できます。

（注） 使用可能なアプライアンスとサービスモジュールの比較、デバイスインターフェイスの詳細など、IPS センサーの概要については、『*Installing Cisco Intrusion Prevention System Appliances and Modules*』の「Introduction the Sensor」を参照してください。各 IPS リリースのこれらのドキュメントのリストは、http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/prod_installation_guides_list.html で入手できます。

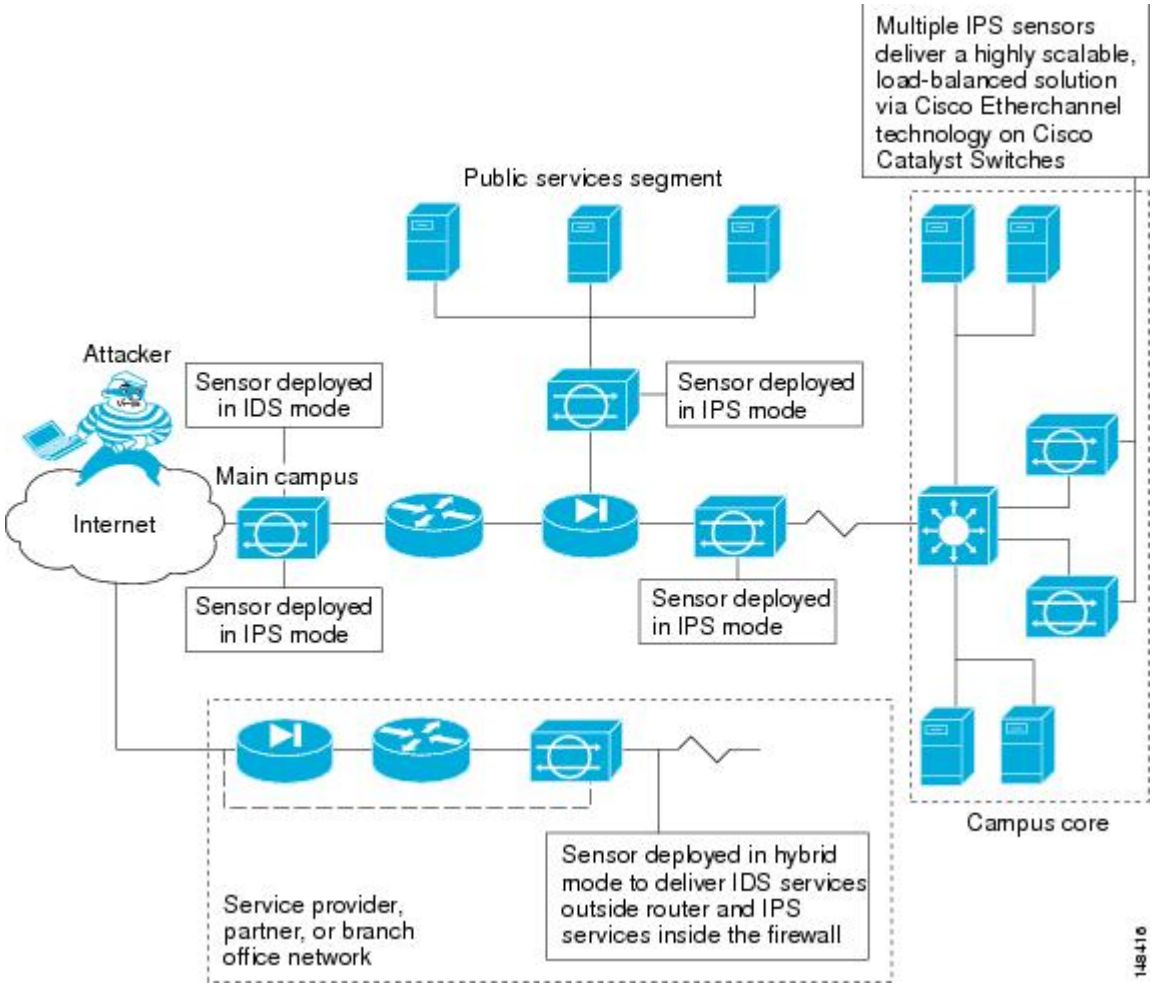
ここでは、次の内容について説明します。

- ネットワーク トラフィックのキャプチャ （2085 ページ）
- センサーの適切な展開 （2086 ページ）
- IPS の調整 （2087 ページ）

ネットワーク トラフィックのキャプチャ

センサーは、無差別モードまたはインライン モードで動作できます。次の図に、インライン（IPS）モードと無差別モード（IDS）モードの両方で動作するセンサーの組み合わせを展開してネットワークを保護する方法を示します。

図 *43 :* 包括的な *IPS* 展開ソリューション



コマンドおよび制御インターフェイスは常に Ethernet です。このインターフェイスには IP アドレスが割り当てられており、この IP アドレスによってマネージャ ワークステーションまたはネットワーク デバイス（シスコのスイッチ、ルータ、およびファイアウォール）と通信できます。このインターフェイスはネットワーク上で参照できるため、暗号化を使用してデータのプライバシーを維持する必要があります。CLI を保護するには SSH を使用し、マネージャ ワークステーションを保護するには TLS/SSL を使用します。SSH および TLS/SSL は、マネージャ ワークステーションでデフォルトでイネーブルになります。

攻撃に対応する場合、センサーは次の処理を行うことができます。

- 検知インターフェイスを介して TCP リセットを挿入する。

（注） TCP リセット アクションは、TCP ベースのサービスに関連付けられているシグニチャでだけ選択する必要があります。TCP ベース以外のサービスでアクションとして選択した場合、アクションは実行されません。また、TCP プロトコルの制限により、TCP リセットでは攻撃セッションのティアダウンが保証されません。

- センサーが管理するスイッチ、ルータ、およびファイアウォールの ACL を変更する。

（注） ACL は、現在のトラフィックではなく今後のトラフィックだけをブロックできます。

- IP セッション ログ、セッション リプレイ、およびトリガー パケット表示を生成する。

IP セッション ログを使用して、不正な使用に関する情報を収集します。IP ログ ファイルは、アプライアンスで検索するように設定されているイベントが発生した場合に書き込まれます。

- 複数のパケット ドロップ アクションを実装して、ワームやウイルスを停止する。

センサーの適切な展開

センサーを展開および設定する前に、ネットワークについて次のことを理解する必要があります。

- ネットワークの規模と複雑さ。
- ネットワークと、インターネットなどの他のネットワークとの間の接続。
- ネットワーク上のトラフィックの量とタイプ。

この知識は、必要なセンサーの数、各センサーのハードウェア設定（たとえば、ネットワーク インターフェイス カードのサイズとタイプ）、および必要なマネージャの数を判断するのに役立ちます。

IPS センサーは、常にファイアウォールや適応型セキュリティ アプライアンスなどの境界フィルタリング デバイスの背後に配置する必要があります。境界デバイスは、セキュリティ ポリシーに一致するようにトラフィックをフィルタリングして、許容されるトラフィックだけがネットワークに入れるようにします。適切な配置によって、アラートの数が大幅に削減され、セキュリティ違反の調査に使用できる対処可能データ量が増えます。IPS センサーをファイアウォールの前面のネットワークのエッジに配置した場合、センサーは、ネットワークの実装にとって重要な意味がない場合でも、すべての単一スキャンおよび攻撃の試行に対してアラートを生成します。（大規模なエンタープライズ環境では）実際にはクリティカルまたは対処可能でない数百、数千、または数百万のアラートが環境に生成されます。このタイプのデータの分析には、時間とコストがかかります。

IPS の調整

IPS を調整すると、表示されるアラートに、実際に対処可能な情報が反映されます。IPS を調整しないと、偽陽性とも呼ばれる良性のイベントが大量に表示され、ネットワークでのセキュリティ調査が困難になります。false positive はすべての IPS デバイスで副次的に発生しますが、Cisco IPS デバイスはステートフルで標準化されており、攻撃評価に脆弱性シグニチャを使用するため、Cisco IPS デバイスでは発生頻度がはるかに低くなります。Cisco IPS デバイスは、ハイリスクのイベントを識別するリスク レーティングと、リスク レーティングに基づいて IPS シグニチャ アクションを実施するためのルールを展開できるポリシーベースの管理も提供します。

IPS センサーを調整するときは、次のヒントに従います。

- センサーは、ネットワーク上の境界フィルタリング デバイスの背後に配置する。

センサーを適切に配置すると、検査する必要のあるアラートの数を 1 日に数千単位で削減できます。

- デフォルトのシグニチャを設定したままセンサーを展開する。

デフォルトのシグニチャ セットでは、非常に高いセキュリティ保護ポスチャが提供されます。シスコのシグニチャ チームは、センサーに非常に高い保護を与えるデフォルトのテストに多くの時間を費やしました。これらのデフォルトが失われたと思われる場合は、復元できます。

- リスク レーティングが 90 を超えるパケットをドロップするようにイベント アクションのオーバーライドが設定されていることを確認する。

これはデフォルトであり、ハイリスク アラートが即時に停止されるようにします。

- 次のいずれかの方法で、脆弱性スキャナやロードバランサなどの特殊なソフトウェアが原因の false positive をフィルタで除外する。
  - スキャナおよびロード バランサの IP アドレスからのアラートを無視するようにセンサーを設定できる。
  - これらのアラートを許可するようにセンサーを設定し、イベント ビューアを使用して false positive をフィルタで除外できる。
- Informational アラートをフィルタリングする。

このような低い優先度のイベント通知は、別のデバイスが IPS で保護されているデバイスを探査しているときに発生することがあります。これらの Informational アラートから送信元 IP アドレスを調べ、送信元を判断します。

- 残りの対処可能なアラートを分析する。
  - アラートを調べる。
  - 攻撃元を突き止める。
  - 宛先ホストを突き止める。

- より多くの情報を提供するように IPS ポリシーを修正する。

IPS 設定の概要

さまざまなデバイスに侵入防御システムを設定できます。設定の視点から、デバイスは2つのグループに分けられます。1 つは、完全な IPS ソフトウェアを実行する専用アプライアンスおよびサービス モジュール（ルータ、スイッチ、および ASA デバイスの場合）です。もう 1 つは、Cisco IOS ソフトウェア 12.4(11)T 以降（Cisco IOS IPS）を実行する IPS 対応ルータです。

次の手順は、専用アプライアンスおよびサービスモジュールでの IPS 設定の概要です。Cisco IOS IPS デバイス（ルータに設置されている IPS サービス モジュールを含みません）の場合は、Cisco IOS IPS 設定の概要 （2318 ページ）を参照してください。

ステップ 1 デバイスを設置し、ネットワークに接続します。デバイス ソフトウェアをインストールし、基本的なデバイス構成を実行します。デバイス上で実行するすべてのサービスに必要なライセンスをインストールします。最初に実行する設定量は、Security Manager で設定する必要がある内容に影響します。

使用している IPS バージョンの『Installing Cisco Intrusion Prevention System Appliances and Modules』マニュアルの指示に従います。

ステップ 2 デバイスを Security Manager のデバイス インベントリに追加します（デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください）。

ヒント モジュールが設置されているデバイスを追加するときに、ルータおよび Catalyst スイッチ モジュールを検出できます。ASA デバイスの場合は、サービス モジュールを別途追加する必要があります。

ステップ 3 インターフェイスの設定 （2133 ページ）の説明に従って、インターフェイスを設定します。デバイスが機能するには、ネットワークに接続されているインターフェイスをイネーブルにする必要があります。

特定のタイプのサービス モジュールの場合は、追加のポリシーを設定します。

- ルータにホスティングしているサービスモジュール：ルータに [IPS モジュール（IPS Module）] インターフェイス設定ポリシーを設定します。詳細については、Cisco IOS ルータでの IPS モジュール インターフェイス設定 （3032 ページ）を参照してください。
- IDSM：[IDSM 設定（IDSM Settings）] Catalyst プラットフォームポリシーを設定します。詳細については、IDSM 設定 （3459 ページ）を参照してください。
- ASA デバイスの IPS モジュール：ホスト ASA の [プラットフォーム（Platform）] > [サービスポリシールール（Service Policy Rules）] > [IPS、QoS、および接続ルール（IPS, QoS, and Connection Rules）] ポリシーを設定して、検査するトラフィックを指定します。詳細については、ASA デバイスでの IPS モジュールについて （2961 ページ）および[サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）を参照してください。

ステップ 4 [仮想センサー（Virtual Sensors）ポリシー] を使用して、インターフェイスを仮想センサーに割り当てます。これには、すべての IPS デバイスに存在する基本 vs0 仮想センサーが含まれます。仮想センサーの設定と仮想センサーへのインターフェイスの割り当てについては、仮想センサーの定義 （2157 ページ）を参照してください。

必要な場合、デバイスがサポートしていれば、ユーザー定義の仮想センサーを作成して、1 つのデバイスに複数のセンサーのように機能させることもできます。ほとんどの IPS 設定は親デバイスで行われますが、シグニチャ、異常検出、イベント アクション用に独自の設定を仮想センサーごとに設定できます。詳細については、仮想センサーの設定 （2151 ページ）を参照してください。

ステップ 5 基本的なデバイス アクセス プラットフォーム ポリシーを設定します。これらのポリシーによって、だれがデバイスにログインできるかが決定されます。

- [AAA]：このポリシーは、RADIUS サーバーを使用してデバイスへのアクセスを制御する場合に設定します。[ユーザーアカウント（User Accounts）] ポリシーで定義されたローカルユーザーアカウントと組み合わせて AAA 制御を使用できます。IPS デバイスの AAA アクセス コントロールの設定（2109 ページ）を参照してください。
- [許可ホスト（Allowed Hosts）]：アクセスを許可されているホストのアドレス。許可されたホストとして Security Manager サーバーが含まれていることを確認してください。含まれていないと、Security Manager を使用してデバイスを設定できません。許可ホストの識別 （2091 ページ）を参照してください。
- [SNMP]：SNMP アプリケーションを使用してデバイスを管理する場合は、このポリシーを設定します。SNMP の設定 （2092 ページ）を参照してください。
- [パスワード要件（Password Requirements）]：ユーザーパスワードの許容される特性を定義できます。ユーザ パスワード要件の設定 （2108 ページ）を参照してください。
- [ユーザーアカウント（User Accounts）]：デバイスで定義されているユーザーアカウント。IPS ユーザ アカウントの設定 （2105 ページ）を参照してください。

ステップ 6 基本的なサーバ アクセス プラットフォーム ポリシーを設定します。次のポリシーにより、デバイスが接続できるサーバーが識別されます。

- [外部製品インターフェイス（External Product Interface）]：Management Center for Cisco Security Agents を使用する場合は、このポリシーを設定して、センサーがアプリケーションからホストポスチャをダウンロードできるようにします。外部製品インターフェイスの設定 （2117 ページ）を参照してください。
- [NTP]：このポリシーは、ネットワーク タイム プロトコル サーバーを使用してデバイス時間を制御する場合に設定します。NTP サーバの識別 （2112 ページ）を参照してください。
- [DNS]、[HTTP プロキシ（HTTP Proxy）]：[DNS] ポリシーおよび [HTTP プロキシ（HTTP Proxy）] ポリシーは、グローバル相関を設定する場合にのみ必要です。これらは、DNS 名を IP アドレスに解決できるサーバを特定します。ネットワークでプロキシを使用してインターネットに接続する必要がある場合は、[HTTP プロキシ（HTTP Proxy）] ポリシーを使用します。それ以外の場合は、[DNS] ポリシーを使用します。DNS サーバの識別 （2113 ページ）またはHTTP プロキシ サーバの識別（2114 ページ）を参照してください。

ステップ 7 デフォルト以外のロギングが必要な場合は、[Logging] ポリシーを設定します。IPS ロギング ポリシーの設定 （2121 ページ）を参照してください。

ステップ 8 IPS シグニチャおよびイベント アクションを設定します。イベント アクション ポリシーの設定は、カスタムのシグニチャの作成よりも簡単であるため、特定のシグニチャを編集する前に、イベント アクション フィルタを使用して、シグニチャの動作を変更するように上書きしてみてください。詳細は、次のトピックを参照してください。

- イベント アクション ルールの設定 （2211 ページ）
- シグニチャの設定 （2169 ページ）

ステップ 9 [Request Block] または [Request Rate Limit] イベント アクションのいずれかを使用する場合は、ブロッキングまたはレート制限ホストを設定します。IPS のブロッキングおよびレート制限の設定 （2282 ページ）を参照してください。

ステップ 10 その他の必要な、高度な IPS サービスを設定します。次のトピックを参照してください。

- グローバル相関の設定 （2265 ページ）
- 異常検出の設定 （2253 ページ）

ステップ 11 デバイスを次のように保守します。

- 必要に応じて、設定を更新および再配布します。
- 更新したシグニチャおよびエンジン パッケージを適用します。更新の確認、更新の適用、および定期的な自動更新の設定については、IPS 更新の管理 （2302 ページ）を参照してください。
- デバイス ライセンスを管理します。ライセンスを更新して再配布することも、ライセンスの更新を自動化することもできます。詳細は、次のトピックを参照してください。
  - IPS ライセンス ファイルの更新 （2299 ページ）
  - IPS ライセンス ファイルの再展開 （2301 ページ）
  - IPS ライセンス ファイル更新の自動化 （2301 ページ）
- SSL（HTTPS）通信に必要な証明書を管理します。これらの証明書は有効期限があるため、約 2 年ごとに再生成する必要があります。証明書の再生成方法、およびデバイスで定義されている証明書を Security Manager の証明書ストアに保存されている証明書と同期させる方法については、IPS 証明書の管理 （2310 ページ）を参照してください。

ステップ 12 デバイスを監視します。

- デバイスから生成されたアラートを表示するには、イベント ビューア アプリケーションを使用します。イベントビューアーは、Configuration Manager または Report Manager の [起動（Launch）] メニューか、Windows の [スタート（Start）] メニューから開くことができます。
  - Event Viewer の使用については、イベントの表示 （3473 ページ）を参照してください。
  - IPS アラートをフィルタ処理する方法の例については、イベント テーブルからの false positive IPS イベントの削除 （3557 ページ）を参照してください。

- Report Manager アプリケーションを使用して、IPS の使用に関するレポートを生成します。このレポートには、インラインモードと無差別モード、およびグローバル相関と従来のインスペクションが含まれます。上位攻撃者、攻撃対象、署名、ブロックされた署名を分析し、ターゲット分析を実行することもできます。次のトピックで、Report Manager および IPS レポートの詳細について説明します。
  - レポートの管理 （3561 ページ）
  - 全般 IPS レポートについて （3585 ページ）
  - IPS 上位レポートについて （3583 ページ）
  - レポートの起動と生成 （3586 ページ）

許可ホストの識別

[Allowed Hosts] ポリシーを使用して、IPS センサーにアクセスできるホストまたはネットワークを識別します。デフォルトでは、どのホストもセンサーへのアクセスを許可されないため、このポリシーにホストまたはネットワークを追加する必要があります。

具体的には、Security Manager サーバの IP アドレスまたはそのネットワーク アドレスを追加します。そうしないと、Security Manager はデバイスを設定できません。また、CS-MARS など、使用するその他すべての管理ホストのアドレスを追加します。

ヒント ホスト アドレスだけを追加した場合、デバイスへのアクセスにはそれらのワークステーションだけを使用できます。あるいは、ネットワークアドレスを指定して、特定の「安全な」ネットワークアクセスに接続されているすべてのホストを許可することもできます。

ステップ 1 次のいずれかを実行して、[許可されたホスト（Allowed Hosts）] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [許可されたホスト（Allowed Hosts）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [許可されたホスト（Allowed Hosts）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次のいずれかを実行します。

- エントリを追加するには、[行の追加（Add Row] ボタンをクリックし、[アクセスリスト（Access List）] ダイアログボックスに入力します。

最大 512 のエントリを追加できます。

- エントリを編集するには、エントリを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- エントリを削除するには、エントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 3 エントリを追加または編集する場合は、[アクセスリストの追加または変更（Add or Modify Access List）] ダイアログボックスでホストまたはネットワークアドレスを指定してから、[OK] をクリックします。次の形式を使用して、アドレスを入力できます。

- ホストアドレス：10.100.10.10 などの単純な IP アドレス。
- ネットワーク アドレス：10.100.10.0/24 や 10.100.10.0/255.255.255.0 などのネットワーク アドレスおよびマスク。
- ネットワーク/ホストポリシーオブジェクト：[選択（Select）] をクリックして既存のオブジェクトを選択するか、新しいオブジェクトを作成します。このポリシーでオブジェクトを使用するには、値が単一の値（単一のネットワークまたは単一のホスト）になっている必要があります。

SNMP の設定

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

SNMP は、単純な要求/応答プロトコルです。ネットワーク管理システムが要求を発行し、管理対象デバイスが応答を返します。この動作は、Get、GetNext、Set、および Trap の 4 つのプロトコル操作のいずれかを使用することによって実装されます。

SNMP によるモニタリングのためにセンサーを設定することができます。SNMP は、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。

SNMP トラップを送信するようにセンサーを設定できます。SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

トラップで指示される通知には次の利点があります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。イベントのトラップと呼ばれるメッセージを送信することで、この処理を行います。

イベントの受信後、マネージャはイベントを表示し、イベントに基づいてアクションを実行できます。たとえば、マネージャは、エージェントを直接ポーリングするか、他の関連デバイス エージェントをポーリングしてイベントの詳細情報を取得できます。

ヒント　トラップで指示された通知は、重要でない SNMP 要求を排除することによって、ネットワークおよびエージェントのリソースを実質的に節約できます。ただし、SNMP ポーリングを完全には排除できません。SNMP 要求は、検出とトポロジ変更に必要です。また、管理対象デバイス エージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

この手順では、トラップの設定など、SNMP 管理ステーションでセンサーを管理できるように IPS センサーで SNMP を設定する方法を説明します。

ステップ 1　次のいずれかを実行して、[SNMP] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2　[一般設定（General Configuration）] タブで、少なくとも次のオプションを設定します。使用可能なすべてのオプションの詳細な説明については、汎用 SNMP 設定オプション （2095 ページ）を参照してください。

- [SNMP Gets/Setsの有効化（Enable SNMP Gets/Sets）]：このオプションを選択して、SNMP 管理ワークステーションが情報を取得（get）したり、IPS センサーの値を修正（set）したりできるようにします。このオプションをイネーブルにしない場合、管理ワークステーションはこのセンサーを管理できません。
- [読み取り専用コミュニティストリング（Read-Only Community String）]：センサーへの読み取り専用アクセスに必要なコミュニティストリング。管理ステーションからの SNMP get 要求は、センサーからの get 応答に対してこのストリングを提供する必要があります。このストリングによって、すべての SNMP get 要求にアクセスできます。
- [読み取り/書き込みコミュニティストリング（Read-Write Community String）]：センサーへの読み取り/書き込みアクセスに必要なコミュニティストリング。管理ステーションからの SNMP set 要求は、センサーからの get 応答に対してこのストリングを提供する必要があります。また、get 要求で使用されることもあります。このストリングによって、すべての SNMP get 要求と set 要求にアクセスできます。

ステップ 3　[SNMPv3 ユーザー（SNMPv3 Users）] タブで、1 人以上の SNMPv3 ユーザを追加して、管理対象 IPS デバイスで SNMPv3 設定を構成します。バージョン 4.6 以降、Security Manager では、管理する IPS デバイスで SNMPv3 設定を構成できます。詳細については、SNMPv3 ユーザータブ （2096 ページ）を参照してください。

（注） SNMPv3 は IPS バージョン 7.2.2 以降でサポートされていますが、IPS バージョン 7.3.1 ではサポートされていません。ただし、Security Manager は IPS 7.3.1 デバイスを管理できます。Cisco Security Manager を使用して、SNMP ポリシーが設定されているバージョン 7.2.2 からバージョン 7.3.1 に IPS デバイスをアップグレードしようとすると、マウスオーバーのツールチップに「選択されたアップグレードは推奨されません。デバイスの SNMP ポリシーの割り当てを解除して展開し、7.3.1 へのアップグレードを続行します」と表示されます。バージョン 7.2.2 以降の IPS デバイスでの SNMPv3 ポリシーの管理については、Cisco Intrusion Prevention System 7.2(2) のリリースノートを参照してください。

ステップ 4 SNMP トラップを設定する場合は、[SNMPトラップ設定（SNMP Trap Configuration）] タブをクリックして、少なくとも次のオプションを設定します。使用可能なすべてのオプションの詳細な説明については、[SNMP Trap Configuration] タブ （2098 ページ）を参照してください。

- [通知の有効化（Enable Notifications）]：センサーが SNMP トラップを送信できるようにするには、このオプションを選択します。
- [トラップ宛先（Trap Destinations）]：トラップの宛先となる SNMP 管理ステーションを追加します。[行の追加（+）（Add Row（+））]ボタンをクリックして新しい宛先を追加するか、宛先を選択して、[行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックして設定を変更します。

トラップ宛先を追加または編集する場合、入力したトラップ コミュニティ ストリングは、[SNMPトラップ設定（SNMP Trap Configuration）] タブで入力したデフォルトのコミュニティ ストリングよりも優先されます。コミュニティストリングがこの宛先に送信されたトラップに表示されます。これは、複数のエージェントから複数のタイプのトラップを受信する場合に役立ちます。たとえば、ルータまたはセンサーがトラップを送信する場合に、具体的にルータまたはセンサーを識別する何かをコミュニティ ストリングに入力すると、コミュニティ ストリングに基づいてトラップをフィルタリングすることができます。

宛先を削除するには、宛先を選択し、[行の削除（ゴミ箱）（Delete Row (trash can)）] ボタンをクリックします。

ステップ 5 トラップの宛先を設定する場合は、[SNMPトラップの要求（Request SNMP Trap）] アクションに必要なアラートを含める必要もあります。このアクションの追加には、次のオプションがあります。

- （(簡単な方法。）イベント アクション オーバーライドを作成して、指定したリスクレーティングのすべてのアラートに [SNMPトラップの要求（Request SNMP Trap）] アクションを追加します（[IPS] > [イベントアクション（Event Actions）]>[イベントアクションオーバーライド（Event Action Overrides）] ポリシー）。たとえば、リスクレーティングが 85 ～ 100 のすべてのアラートに対してトラップを生成できます。イベントアクション オーバーライドを使用すると、各シグニチャを個別に編集することなくアクションを追加できます。詳細については、イベント アクション オーバーライドの設定 （2227 ページ）を参照してください。
- （正確な方法。）シグニチャポリシーを編集して（[IPS] > [シグニチャ（Signatures）> [シグニチャ（Signatures）]）、トラップ通知を送信するシグニチャに [SNMPトラップの要求（Request SNMP Trap）] アクションを追加します。トラップは、トラップを送信するように設定したシグニチャだけに送信されます。

（注） シグニチャの送信元がデフォルトの場合は、アクションを変更する前に送信元をローカル送信元に変更する必要があります。ただし、シグニチャテーブルの [アクション（Action）] セルを右クリックして [アクションの編集（Edit Actions）] を選択し、[SNMP トラップの要求（Request SNMP Trap）]（およびその他の必要なアクション）を選択して [OK] をクリックすると、ソースは自動的にローカルに変更されます。

ステップ 6 SNMP 管理ステーションを [Allowed Hosts] ポリシーに追加します。管理ステーションは、センサーへのアクセスを許可されているホストである必要があります。許可ホストの識別 （2091 ページ） を参照してください。

汎用 SNMP 設定オプション

[SNMP] ページの [一般設定（General Configuration）] タブを使用して、一般的な SNMP パラメータを設定して、IPS センサーに適用します。手順については、SNMP の設定 （2092 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[General Configuration] タブを選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。[General Configuration] タブを選択します。

フィールド リファレンス

表 503 : [General Configuration] タブ、IPS センサーの [SNMP] ポリシー

要素	説明
Enable SNMP Gets/Sets	SNMP 管理ワークステーションで、IPS センサー上の情報の取得および値の修正（設定）をイネーブルにするかどうか。このオプションをイネーブルにしていない場合、管理ワークステーションはこのセンサーを管理できません。センサーは SNMP 要求に応答しません。
Read-Only Community String	センサーへの読み取り専用アクセスに必要なコミュニティ ストリング。管理ステーションからの SNMP get 要求は、センサーからの get 応答に対してこのストリングを提供する必要があります。このストリングによって、すべての SNMP get 要求にアクセスできます。このストリングを使用すると、センサーの識別に役立ちます。

要素	説明
Read-Write Community String	センサーへの読み取り/書き込みアクセスに必要なコミュニティストリング。管理ステーションからの SNMP set 要求は、センサーからの get応答に対してこのストリングを提供する必要があります。また、get要求で使用されることもあります。このストリングによって、すべての SNMP get 要求と set 要求にアクセスできます。このストリングを使用すると、センサーの識別に役立ちます。
Sensor Contact	このセンサーに責任を持つネットワーク管理者または担当者。
センサーの位置（Sensor Location）	建物の住所、名前、部屋番号など、センサーの物理的な場所。
Sensor Agent Port	センサーとの SNMP get/set 通信に使用するポート。デフォルトは 161 です。有効な範囲は 1 ～ 65535 です。 ポートリストオブジェクトのポート番号または名前を入力します。または、[選択（Select）] をクリックしてリストからポートリストオブジェクトを選択するか、または新しいオブジェクトを作成します。ポート リスト オブジェクトでは、単一ポートが識別されます。
SNMPエージェントプロトコル（SNMP Agent Protocol）	SNMP に使用しているプロトコル（UDP（デフォルト）または TCP）。SNMP 管理ステーションで使用されるプロトコルを選択します。

SNMPv3 ユーザータブ

バージョン 4.6 以降、Security Manager では、管理する IPS デバイスで SNMPv3 設定を構成できます。SNMPv3 ユーザーを追加して、管理対象 IPS デバイスで SNMPv3 設定を指定する必要があります。

[SNMP] ページの [SNMPv3 ユーザー（SNMPv3 Users）] タブを使用して、SNMPv3 ユーザーを表示、追加、編集、または削除できます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMPv3 ユーザー（SNMPv3 Users）] タブを選択します。
- （ポリシービュー）**[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [SNMP]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[SNMPv3 ユーザー（SNMPv3 Users）] タブを選択します。

次のいずれかを実行します。

- SNMPv3 ユーザーを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [SNMPv3 ユーザーの追加（Add SNMPv3 User）] ダイアログボックスが開きます。ユーザーを作成するために必要な情報を入力します。設定の詳細については、[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス （2097 ページ）を参照してください。
- SNMPv3 ユーザーを編集するには、そのユーザーを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、[SNMPv3 ユーザーの編集（Edit SNMPv3 User）] ダイアログボックスに必要な変更を加えます。
- 既存の SNMPv3 ユーザーを削除するには、ユーザーを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

フィールド リファレンス

表 *504 : SNMPv3* ユーザー

要素	説明
User Name	SNMP エージェントに属するホスト上のユーザーの名前。
アクセス制御	SNMPv3 ユーザーのアクセス権限。
セキュリティ レベル（Security Level）	SNMPv3 ユーザーのセキュリティレベル。
認証プロトコル（Authentication Protocol）	認証プロトコルキーワードは、SNMPv3ユーザーの設定に使用される認証レベルです。
プライバシー プロトコル（Privacy Protocol）	プライバシー プロトコル キーワードは、SNMPv3 ユーザーの設定に使用されるプライバシーまたは暗号化アルゴリズムです。

[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス

[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックスを使用して、管理対象 IPS デバイスの新しい SNMPv3 ユーザーを設定します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMPv3ユーザー（SNMPv3 Users ）] タブを選択し、[行の追加（Add Row ）]（+）ボタンをクリックします。
- （ポリシービュー）**[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [SNMP]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作

成します。[SNMPv3ユーザー（SNMPv3 Users）] タブを選択し、[行の追加（Add Row）]（+）ボタンをクリックします。

フィールド リファレンス

表 *505 : [SNMPv3*ユーザーの追加（*Add SNMPv3 Users*）*]* ダイアログボックス

要素	説明
User Name	新しい SNMPv3 ユーザーの名前を入力します。
アクセス制御	新しい SNMPv3 ユーザーのアクセス権限を選択します。
セキュリティ レベル（Security Level）	SNMPv3 ユーザーに対して、次のいずれかのセキュリティレベルを選択します。 • **NoAuthNoPriv**：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。 • **AuthNoPriv**：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。 • **AuthPriv**：認証とプライバシーが設定されます。メッセージが認証および暗号化されることを意味します。
認証プロトコル（Authentication Protocol）	使用される認証レベルを指定する認証プロトコルキーワードを選択します。デフォルト値はありません。
プライバシー プロトコル（Privacy Protocol）	使用するプライバシーまたは暗号化アルゴリズムを指定するプライバシー プロトコル キーワードを選択します。暗号化アルゴリズムには、AES キーワードを指定できます。デフォルト値はありません。
認証パスフレーズ（Authentication Passphrase）	認証ユーザーパスワードを指定する認証パスフレーズ引数を入力します。このパスワードは 8 文字以上にする必要があります。デフォルト値はありません。
プライバシーパスフレーズ（Privacy Passphrase）	暗号化ユーザーパスワードを指定するプライバシーパスフレーズ引数を入力します。このパスワードは 8 文字以上にする必要があります。デフォルト値はありません。

[SNMP Trap Configuration] タブ

[SNMP] ページの [SNMPトラップ通信（SNMP Trap Communication）] タブを使用して、トラップを設定してセンサーに適用し、トラップの送信先の受信者を指定します。手順については、SNMP の設定 （2092 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMP Trap Configuration] タブを選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。[SNMP Trap Configuration] タブを選択します。

フィールド リファレンス

表 *506 : [SNMP* トラップ設定（*SNMP Trap Configuration***）*]* タブ、*IPS* センサーの *[SNMP]* ポリシー**

要素	説明
通知の有効化（Enable Notifications）	センサーで特定のタイプのイベントが発生したときに、センサーがトラップ通知をトラップの宛先に送信することをイネーブルにするかどうか。このオプションを選択しない場合、センサーはトラップを送信しません。 **ヒント** センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベントアクションとして [SNMPトラップを要求（Request SNMP Trap）] も選択する必要があります。トラップは、トラップを送信するように設定したシグニチャだけに送信されます。
Error Filter	イベントの重大度（重大、エラー、または警告）に基づいてSNMP トラップを生成するイベントのタイプ。必要な重大度をすべて選択します。複数の値を選択するには、Ctrl キーを押しながらクリックします。 センサーは、選択された重大度のイベント通知だけを送信します。
Enable Detail Traps	トラップにアラートのテキスト全体を含めるかどうか。このオプションを選択しない場合、スパースモードが使用されます。スパース モードでは、484 バイト未満のアラートのテキストが含まれます。
Default Trap Community String	[トラップ宛先（Trap Destinations）] テーブルでトラップの宛先に特定の文字列が設定されていない場合に、トラップに使用されるコミュニティ文字列。 **ヒント** すべてのトラップがコミュニティ ストリングを伝送します。デフォルトでは、宛先と同じコミュニティ ストリングを持つすべてのトラップが宛先で取得されます。その他すべてのトラップは、宛先によって廃棄されます。ただし、受け入れるトラップ文字列を判断するように宛先を設定できます。

要素	説明
[Trap Destinations] テーブル	トラップ通知を送信する SNMP 管理ステーション。テーブルには、管理ステーションの IP アドレス、このセンサーからトラップに追加されるコミュニティ ストリング、およびトラップの送信先のポートが表示されます。 • 宛先を追加するには、[行の追加（Add Row）] ボタンをクリックし、[SNMP トラップ通信の追加（Add SNMP Trap Communication）] ダイアログボックスに入力します（ [Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス （2100 ページ）を参照）。 • 宛先を編集するには、その宛先を選択して [行の編集（Edit Row）] ボタンをクリックし、変更を行います。 • 宛先を削除するには、その宛先を選択して [行の削除（Delete Row）] ボタンをクリックします。

[Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス

[SNMP トラップ通信の追加または変更（Add or Modify SNMP Trap Communication）] ダイアログボックスを使用して、SNMP トラップの宛先を設定します。宛先は、IPS センサーからトラップを受信する必要がある SNMP 管理ステーションです。

ナビゲーション パス

IPS の [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] ポリシーに移動し、[SNMP トラップ設定（SNMP Trap Configuration）] タブを選択して [トラップの宛先（Trap Destinations）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、テーブルで宛先を選択して [行の編集（Edit Row）] ボタンをクリックします。詳細については、 [SNMP Trap Configuration] タブ （2098 ページ）を参照してください。

フィールド リファレンス

表 507 : [Add SNMP Trap Communication]/[Modify SNMP Trap Communication] ダイアログボックス

要素	説明
IP アドレス	トラップ通知を受信する SNMP 管理ステーションの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力するか [選択（Select）] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。ネットワーク/ホスト オブジェクトでは、単一のホスト IP アドレスを指定する必要があります。
Trap Community String	トラップのコミュニティ ストリング。トラップ文字列を入力しない場合は、[SNMP Trap Communication] タブで定義されたデフォルトのトラップ文字列が、この宛先に送信されるトラップに使用されます。

要素	説明
トラップ ポート（Trap Port）	SNMP管理ステーションがトラップの受信に使用するポート。ポート リスト オブジェクトのポート番号または名前を入力するか、[Select] をクリックしてリストからオブジェクトを選択します。または、新しいオブジェクトを作成します。ポート リスト オブジェクトでは、単一ポートが識別されます。
SNMPv3ユーザー（SNMPv3 User）	[SNMPv3ユーザーの追加（Add SNMPv3 User）] ダイアログボックス（2097ページ）を使用して設定したSNMPv3ユーザーのユーザー名を入力します。SNMPv3 ユーザーを関連付けない場合は、このフィールドを空白のままにします。 （注） 設定済みの SNMPv3 ユーザーではないユーザー名を入力すると、SNMP トラップ通信の設定の保存中にエラーメッセージが表示されます。また、最大 23 人の SNMPv3 ユーザーを追加できます。

ユーザ アカウントとパスワードの要件の管理

IPSデバイスに対して、ユーザ アカウントとパスワード、および一般的なパスワード要件を設定できます。ローカル ユーザ（デバイスで直接定義）を設定するか、RADIUS AAA サーバを使用するか、この両方を組み合わせることができます。使用されるポリシーは、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）] フォルダにある [AAA] ポリシー、[ユーザーアカウント（User Accounts）] ポリシー、および [パスワード要件（Password Requirements）] ポリシーです。

Security Manager でローカル ユーザ アカウントを作成または編集する場合は、入力するパスワードが、[Password Requirements] ポリシーで定義した要件を満たしている必要があります。これにより、新しいパスワードがセキュリティ要件を満たすことが保証されます。

ヒント パスワード要件を変更し、いずれかのローカル ユーザ アカウントに変更を加えた場合は、Security Manager によって管理されているパスワードを持つすべてのユーザ アカウントで新しい要件が満たされる必要があります。その理由は、いずれか 1 つのアカウントを再設定する必要がある場合に、Security Manager によってすべての管理対象アカウントのパスワードが再設定されるためです。

[User Accounts] ポリシーを使用して、IPS デバイスのローカル ユーザ アカウントを集中管理できます。共有ポリシーを使用すると、すべてのIPSデバイスに同じパスワードを持つ同じアカウントが含まれる状態を確保するために役立ちます。ただし、パスワードは暗号化されているため、Security Manager はデバイスに定義されている実際のパスワードを検出できません。Security Manager でパスワードを定義する場合にだけ、Security Manager によってアカウントのパスワードが管理されます。Security Manager では、RADIUS AAA サーバで定義されたユーザ アカウントは管理しません。

ここでは、IPS ユーザ アカウント、および Security Manager の検出と展開の考慮事項について詳細に説明します。

- IPS ユーザーロールについて （2102 ページ）
- 管理対象と管理対象外の IPS パスワードについて （2103 ページ）
- IPS パスワードの検出および展開方法について （2104 ページ）
- IPS ユーザ アカウントの設定 （2105 ページ）
- ユーザ パスワード要件の設定 （2108 ページ）
- IPS デバイスの AAA アクセス コントロールの設定 （2109 ページ）

IPS ユーザーロールについて

IPS ユーザ アカウントには 4 つのユーザ ロールがあります。

- **ビューア（Viewer）**：ユーザは、デバイス設定とイベントを表示できますが、自身のユーザパスワード以外の設定データは修正できません。
- **オペレータ（Operator）**：ユーザはすべてのデータを表示できるほか、次のオプションを修正できます。
  - シグニチャチューニング（優先順位、無効/有効）
  - 仮想センサーの定義
  - 管理対象ルータ。
  - ユーザ パスワード。
- **管理者（Administrator）**：ユーザはすべてのデータを表示できるほか、オペレータが修正できるすべてのオプションに加えて、次のオプションを修正できます。
  - センサー アドレッシング設定。
  - 設定エージェントまたはビュー エージェントとして接続が許可されたホストのリスト。
  - 物理的な検知インターフェイスの割り当て。
  - 物理インターフェイスの制御のイネーブル化またはディセーブル化。
  - ユーザとパスワードの追加および削除。
  - 新しい SSH ホスト キーおよびサーバ証明書の生成。
- **サービス（Service）**：サービス権限を持つユーザはセンサーに 1 人だけ存在できます。サービス ユーザは、IDM または IME にログインできません。サービス ユーザは、CLI ではなく bash シェルにログインします。サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。

（注） Service アカウントの目的は、通常は発生しない問題を Cisco テクニカル サポートがトラブルシューティングできるようにすることにあります。通常のシステム設定およびトラブルシューティングには必要ありません。サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

管理対象と管理対象外の IPS パスワードについて

各 IPS ローカル ユーザ アカウントには、デバイスへのセキュアなユーザ ログインを可能にするパスワードがあります。これらのユーザ パスワードは、IPS デバイスで暗号化されます。このため、IPS デバイスを Security Manager インベントリに追加すると、Security Manager は実際のユーザ パスワードを読み取れません。

Security Manager はパスワードを読み取れないため、新規に検出されたユーザ アカウントのパスワードをデバイスに展開できません。ユーザアカウントのパスワードが不明で使用不可の状態にならないように、Security Manager は検出されたユーザアカウントのパスワードに**管理対象外**というマークを付けます。パスワードのステータスは、[プラットフォーム（Platform）]> [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ユーザアカウント（User Accounts）] ポリシーの [管理対象のパスワード？（Is Password Managed?）] カラムに表示されます。

- [いいえ（No）] と表示されている場合、このアカウントのパスワードは Security Manager で設定されません。このポリシーを展開する場合、Security Manager はこのユーザ アカウントのパスワードの設定を試みません。
- [はい（Yes）] と表示されている場合、このアカウントのパスワードは Security Manager で設定または更新されています。このポリシーを展開する場合、Security Manager は、最後の展開後に変更されたパスワードだけでなく、すべての管理対象アカウントのパスワードを再設定します。

Security Manager は変更されていないパスワードも設定するため、すべての管理対象パスワードは [Password Requirements] ポリシーで定義されているパスワード要件を満たす必要があります。

このため、管理対象と管理対象外のアカウント パスワードを混在させることができます。たとえば、集中管理されている共有ユーザ アカウントのセットを使用し、これらのアカウントのパスワードを Security Manager で管理できます。他のアカウントは、個人ごとに固有にすることができます。これらのアカウントのパスワードを Security Manager で編集しない場合は、ユーザがデバイス上でパスワードを個別に管理できます。

ヒント　ユーザアカウントを Security Manager で管理しない場合は、[ユーザアカウントポリシー（User Accounts policy）] が空であることを確認するか、ポリシーの割り当てを解除します（ポリシーを右クリックし、[ポリシーの割り当て解除（Unassign Policy）] を選択します）。Security Manager は、ユーザアカウント設定を変更しません。

IPS パスワードの検出および展開方法について

ユーザ パスワードは IPS デバイスで暗号化されるため、Security Manager は、デバイスでポリシーを検出または設定を展開するときに、特に注意してこれらのパスワードを処理する必要があります。IPS デバイスでユーザ アカウントを検出または展開する場合、Security Manager は次の処理を行います。

- [検出（Discovery）] : IPS デバイスをインベントリに追加するとき、またはポリシーを再検出するとき、Security Manager は各ユーザーアカウントの現在のステータスを判断し、検出されたユーザー名とそれに関連付けられているロールでユーザーアカウントポリシーを更新し、ユーザーパスワードを管理対象外としてマークします（管理対象と管理対象外の IPS パスワードについて （2103 ページ）を参照）。

アカウントステータスは動的で変化する可能性があるため、Security Manager を介して表示することはできません。ただし、[Discovery Status] ウィンドウに、検出時のステータスが表示されます。アカウントには次のステータスがあります。

- [アクティブ（Active）] : この状態は、アカウントが使用可能なことを示します。アクティブアカウントには、そのアカウントに割り当てられているユーザが認証トークンを使用してアクセスできます。
- [期限切れ（Expired）] : この状態は、アカウントの認証トークンが期限切れになっており、トークンが更新されるまで、トークンを使用してアカウントにアクセスできないことを示します。
- [ロック（Locked）] : この状態は、認証試行の失敗回数が多過ぎたために、このアカウントへのログインが無効になったことを示します。これらのアカウントのパスワードを更新する必要があります。

[展開（Deployment）] : ユーザーアカウントが [期限切れ（Expired）] または [ロック（Locked）] 状態にある場合に警告が表示されます。管理対象外のパスワードは、デバイスに展開されません。また、次の点に注意してください。

- デバイス上のいずれかのユーザアカウントに変更を加える場合は、管理対象パスワードを持つすべてのユーザ アカウントが再設定されます。[Password Requirements] ポリシーも変更した場合は、すべてのパスワードが新しいポリシーと比較され、新しい要件を満たす必要があります。
- デバイスの設定時に Security Manager が使用するようにデバイスのプロパティで定義されているユーザーアカウントのパスワードを変更した場合は、正常な展開後に、Security Manager がデバイスのプロパティのパスワードを新しいパスワードに更新します。パス

ワードを手動で更新する必要はありません。デバイスのプロパティを表示するには、[ツール（Tools）] > [デバイスプロパティ（Device Properties）] を選択します。

この動作は、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] >[デバイス通信（Device Communication）] ページの [デバイスへの接続方法（Connect to Device Using）] オプションに対して [Security Managerデバイスのクレデンシャル（Security Manager Device Credentials）] を選択したことを想定しています。ログインしているユーザのクレデンシャルを展開に使用している場合は、正常な展開後に、展開全体が失敗としてマークされ、接続の再確立方法がメッセージで説明されます。 [Device Communication] ページ （668 ページ）を参照してください。

- アウトオブバンド変更検出を使用する場合は、パスワードに対する変更が検出されません。ただし、ユーザ名とロールに対する変更は検出されます。アウトオブバンド変更検出の詳細については、アウトオブバンド変更の検出および分析 （537 ページ）を参照してください。
- 設定をプレビューする場合、IPS（[Delta] > [User Passwords]）を選択してユーザ アカウントに対する変更を表示できます。ただし、パスワードはマスクされています。詳細については、 設定のプレビュー （535 ページ）を参照してください。
- 設定をロールバックする場合、ユーザ アカウントはロールバックされません。ユーザ アカウントの現在のステータスと設定は変更されません。

ヒント IPS センサーは、SSH クライアントを介してデバイスにログインするときに、RSA 認証の公開キーを受け入れることができます。各ユーザには、認可されたキーのリストが関連付けられています。ユーザは、パスワードの代わりにこれらのキーを使用できます。Security Manager は、検出および展開時にこれらのキーを無視します。このため、キーが設定されている場合、Security Manager は設定を削除しません。

関連項目

- ポリシーの検出 （223 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）
- 設定のロールバックについて （560 ページ）
- IPS および IOS IPS のロールバックについて （564 ページ）

IPS ユーザ アカウントの設定

[User Accounts] ポリシーを使用して、IPS デバイスのローカル ユーザ アカウントを設定します。ユーザは、これらのアカウントを使用してデバイスにログインできます。新規ユーザの作成、ユーザ権限とパスワードの修正、およびユーザの削除を行うことができます。

ユーザ アカウント ポリシーには少なくとも次のアカウントが必要です。

- cisco：「cisco」という名前のアカウントがデバイスに存在する必要があり、削除できません。
- Security Manager が使用できる管理者アカウント：Security Manager が、設定するデバイスにログインできる必要があります。通常は、この目的のアカウントを作成します。ただし、Security Manager がデバイスにログインするために、設定を展開するユーザのユーザ アカウントを使用することもできます。この設定は、[ツール（Tools）]>[Security Manager の管理（Security Manager Administration）]>[デバイス通信（Device Communication）]ページの [デバイスの接続に使用（Connect to Device Using）] オプションを使用して行うことができます。 [Device Communication] ページ （668 ページ）を参照してください。

IPS ユーザ アカウントの設定は、見た目よりも複雑です。IPS ユーザ アカウントを設定する前に、次の項を参照してください。

- ユーザ アカウントとパスワードの要件の管理 （2101 ページ）
- IPS ユーザーロールについて （2102 ページ）
- 管理対象と管理対象外の IPS パスワードについて （2103 ページ）
- IPS パスワードの検出および展開方法について （2104 ページ）
- ユーザ パスワード要件の設定 （2108 ページ）
- IPS デバイスの AAA アクセス コントロールの設定 （2109 ページ）

ヒント

- Cisco IOS IPS デバイスでは、ルータに定義されているのと同じユーザ アカウントを使用します。この手順は、Cisco IOS IPS 設定には適用されません。
- デバイス プロパティで定義されたユーザのパスワード（Security Manager でデバイスに設定を展開するために使用）を変更する場合、Security Manager は、デバイス プロパティに定義された既存のクレデンシャルを使用してデバイスにログインし、変更を展開します。展開に成功したら、デバイスプロパティは、新しい設定を使用するように変更されます。デバイスプロパティのクレデンシャルの詳細については、 [Device Credentials] ページ （143 ページ）を参照してください。

関連項目

- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

ステップ 1 次のいずれかを実行して、[User Accounts] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）]>[ユーザーアカウント（User Accounts）] を選択します。

- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ユーザーアカウント（User Accounts）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ポリシーには、ユーザ名、ロール、（管理対象と管理対象外の IPS パスワードについて （2103 ページ）で説明したように）パスワードが Security Manager で管理されるかどうかなど、既存のユーザ アカウントが表示されます。

ステップ 2 次のいずれかを実行します。

- ユーザーアカウントを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [Add User] ダイアログボックスが開きます。アカウントの定義に必要な情報を入力します。設定の詳細については、ユーザの追加またはユーザログイン情報の編集ダイアログボックス （2107 ページ）を参照してください。
- ユーザーアカウントを編集するには、そのアカウントを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、[ユーザーの編集（Edit User）] ダイアログボックスに必要な変更を加えます。

ユーザ ロールをサービス ロールに、またはサービス ロールをユーザ ロールには変更できません。

- ユーザーアカウントを削除するには、そのアカウントを選択して [行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。cisco という名前のアカウントは削除できません。

ヒント すべてのパスワード変更は、[Password Requirements] ポリシーの要件を満たしている必要があります。要件ポリシーを変更した場合、すべての新規ユーザ アカウント、または編集したアカウントが、新規要件に対してテストされます。既存の編集していないユーザ アカウントのパスワードはテストされませんが、Security Manager は次の設定展開時にすべてのアカウントを展開するため、このポリシーで定義したユーザ アカウントを変更する場合は、既存のユーザ アカウントのパスワードもパスワード要件を満たしている必要があります。ポリシーを検証する場合は、パスワードの適合性がチェックされます。これは通常、データベースに変更を送信するときに行われます。詳細については、IPS パスワードの検出および展開方法について （2104 ページ）を参照してください。

ユーザの追加またはユーザログイン情報の編集ダイアログボックス

[ユーザの追加（Add User）] または [ユーザログイン情報の編集（Edit User Credentials）] ダイアログボックスを使用して、IPS デバイスのユーザーアカウントを追加または編集します。

ナビゲーション パス

IPS プラットフォームの [ユーザーアカウント（User Accounts）] ポリシーで、[行の追加（+）（Add Row (+)）] ボタンをクリックして新しいアカウントを作成するか、既存のアカウントを選択して [行の編集（鉛筆）（Edit Row (pencil)）] ボタンをクリックします。[User Accounts] ポリシーへのアクセス方法については、IPS ユーザアカウントの設定 （2105 ページ）を参照してください。

フィールド リファレンス

表 *508 : [Add User]/[Edit User]* ダイアログボックス

要素	説明
User Name	アカウントのユーザ名。名前は 1 ～ 64 文字で、大文字と小文字、数字、および ( ) + : , _ / -] + $ の特殊文字から構成できます。 アカウントを編集する場合、ユーザ名は変更できません。
パスワード 確認（Confirm）	このユーザ アカウントのパスワード。両方のフィールドにパスワードを入力します。 パスワードは、IPS デバイスの [Password Requirements] ポリシーに準拠する必要があります。ユーザ パスワード要件の設定 （2108 ページ）を参照してください。
ロール	このユーザのロール。これらのロールの説明については、IPS ユーザーロールについて （2102 ページ）を参照してください。 **ヒント** ユーザアカウントを編集する場合、サービス ロールは選択できません。サービス ロールに割り当てられているアカウントを編集する場合、ロールは変更できません。

ユーザ パスワード要件の設定

IPS プラットフォームの [Password Requirements] ポリシーを使用して、ローカル IPS デバイス ユーザ アカウントのパスワードのルールを設定します。ユーザが作成するすべてのセンサー パスワードは、このポリシーに定義されている要件に準拠する必要があります。IPS ソフトウェア バージョン 6.0 以降を実行しているセンサーのパスワード要件を設定できます。

ヒント ここで定義する要件は、[User Accounts] ポリシーで受け入れることができるパスワードかどうかを決める条件になります（IPS ユーザ アカウントの設定 （2105 ページ）を参照）。このポリシーを変更した場合は、変更されていないユーザアカウントにも適用できます。このポリシーに対する変更の展開の暗黙的な意味については、IPS パスワードの検出および展開方法について （2104 ページ）を参照してください。

IPS パスワード要件を設定するには、次のいずれかのポリシーを選択します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [パスワード要件（Password Requirements）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [パスワード要件（Password Requirements）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

次の表で、設定できるパスワード要件オプションについて説明します。

表 *509 : [Password Requirements]* ポリシー

要素	説明
Attempt Limit	過剰な失敗試行によりユーザアカウントをロックする前にユーザがデバイスへのログイン試行を許可される回数。 デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。
Size Range	ユーザパスワードに対して許可される最小と最大のサイズ。最小と最大をハイフンで区切ります。範囲は 6 ～ 64 文字です。デフォルトは 8-64 です。 **ヒント** いずれかの最小文字数オプションにゼロ以外の値を設定した場合、[Size Range] フィールドに入力する最小サイズは、それらの値の合計以上である必要があります。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。
Minimum Digit Characters	パスワードに含まれる必要のある数字の最小数。
Minimum Uppercase Characters	パスワードに含まれる必要のある大文字の英字の最小数。
Minimum Lowercase Characters	パスワードに含まれる必要のある小文字の英字の最小数。
Minimum Other Characters	パスワードに含まれる必要のある英数字以外の印刷可能文字の最小数。
Number of Historical Passwords	各アカウントについてセンサーで記憶する過去のパスワードの数。新しいパスワードが記憶されているいずれかのパスワードと一致した場合は、アカウントのパスワードの変更試行に失敗します。0 を指定した場合、以前のパスワードは記憶されません。

IPS デバイスの AAA アクセス コントロールの設定

AAA ポリシーを使用して、IPS デバイスの AAA アクセス コントロールを設定します。AAA を設定するには、デバイスで IPS ソフトウェアリリース 7.0(4) 以降または 7.1.3 以降を使用する必要があります。たとえば、7.1.1 や 7.1.2 は AAA をサポートしていません。

デバイスへのユーザ アクセスの認証に RADIUS AAA サーバを使用するように、IPS デバイスを設定できます。AAA を設定することにより、デバイスで定義するローカル ユーザの数を減らし、既存の RADIUS 設定を活用できます。AAA サーバを設定する場合は、RADIUS サーバ

が使用できない場合のフォールバック メカニズムとしてローカル ユーザ アカウントを許可するように、デバイスを設定できます。

AAA の設定時に、AAA サーバ ポリシー オブジェクトを使用して RADIUS サーバを識別できます。ポリシーの作成時にオブジェクトを作成できます。そうしなかった場合は、Policy Object Manager で作成できます。AAA サーバ オブジェクトを設定する場合は、次の制限事項に従う必要があります。

- [ホスト（Host）]：IP アドレスを指定する必要があります。DNS 名は使用できません。
- [タイムアウト（Timeout）]：タイムアウト値を入力する場合は、1 ～ 512 秒の範囲で指定する必要があります。汎用 AAA サーバ オブジェクトではさらに大きい数字を使用できますが、IPS のタイムアウトの範囲はそれよりも制限されています。デフォルトは 3 です。
- [プロトコル（Protocol）]：サポートされるプロトコルは RADIUS のみです。
- [キー（Key）]：RADIUS サーバーで定義された共有秘密キーを指定する必要があります。このフィールドは、汎用 AAA サーバ オブジェクトの場合は任意ですが、IPS の場合、キーは必要です。
- [ポート（Port）]：RADIUS 認証/許可ポートが正しいことを確認します。AAA サーバ オブジェクトのデフォルト ポートが IPS のデフォルト（1812）と異なることに注意してください。IPS のデフォルトを使用する場合は、ポートを変更する必要があります。

AAA サーバ オブジェクトを設定する方法については、AAA サーバ オブジェクトの作成 （330 ページ）を参照してください。

ヒント 使用する認可方式に応じて、デバイス プロパティに設定されたユーザ アカウントが RADIUS サーバに存在するか、またはローカル ユーザ アカウントとして存在するか確認する必要があります。ローカル モードと AAA モードを切り替える場合、または AAA サーバを変更する場合は、使用しているユーザ アカウント データベースのいずれにもアカウントが定義されていることを確認する必要があります。ローカル フォールバックが設定された AAA を使用している場合、アカウントはすべてのデータベースで定義されている必要があります。このアカウントは、デバイスの Security Manager デバイス プロパティで定義されているパスワードと同じパスワードで存在している必要があります。そうでない場合、デバイスの展開が失敗します。検出および展開に使用するユーザ アカウントには管理者権限が必要です。

関連項目

- ユーザ アカウントとパスワードの要件の管理 （2101 ページ）
- IPS ユーザ アカウントの設定 （2105 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [AAA] を選択します。
- （ポリシービュー）[IPS]>[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[AAA] を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次の基本的なプロパティを設定します。

- [認証モード（Authentication Mode）]：ローカルモードと AAA モードのどちらを使用するか。Local モードでは、IPS デバイスで定義されたユーザ アカウントだけを使用します。AAA モードでは、RADIUS サーバがユーザ認証の基本手段です。ローカル ユーザ アカウントをフォールバック メカニズムとして設定できます。デフォルトは Local です。このポリシーのその他のオプションを設定するには、AAA を選択する必要があります。
- [プライマリRADIUSサーバー、セカンダリRADIUSサーバー（Primary RADIUS Server, Secondary RADIUS Server）]：メイン（プライマリ）AAA サーバーおよびバックアップ サーバー（使用する場合）。RADIUS サーバーを識別する AAA サーバー ポリシー オブジェクトの名前を入力します。または、[選択（Select）] をクリックして、オブジェクトのリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

ユーザの認証時に、IPS デバイスは、プライマリ サーバにユーザ認証の試行を送信します。セカンダリ サーバには、プライマリ サーバへの要求がタイムアウトになった場合にアクセスが行われます。

ステップ 3 デフォルト以外の値を設定する場合は、次の任意のプロパティを設定します。

- [コンソール認証（Console Authentication）]：コンソールを介して IPS デバイスにアクセスするユーザーを認証する方法。
  - [Local]：コンソール ポートを介して接続するユーザは、ローカル ユーザ アカウントを使用して認証されます。
  - [Local and RADIUS]：コンソール ポートを介して接続するユーザは、最初に RADIUS を使用して認証されます。RADIUS が失敗した場合は、ローカル認証が試行されます。
  - [RADIUS]：コンソール ポートを介して接続するユーザは、RADIUS によって認証されます。[Enable Local Fallback] も選択する場合は、ローカル ユーザ アカウントを使用してユーザを認証することもできます。
- [RADIUS NAS ID]：認証を要求するサービスを識別するネットワークアクセス ID。値には、すでに RADIUS サーバで設定されている NAS-ID、cisco-ips、NAS-ID 以外を指定できます。デフォルトは cisco-ips です。
- [ローカルへのフォールバックを有効化（Enable Local Fallback）]：すべての RADIUS サーバーが使用できない場合に、ローカルユーザーアカウント認証にフォールバックするかどうか。このオプションは、デフォルトで選択されます。RADIUS サーバがログインの試行に対して否定的な応答を示した場合、ローカル認証は試行されないことに注意してください。RADIUS サーバから応答を受信しなかった場合だけ、ローカル認証が試行されます。
- [デフォルトユーザーロール（Default User Role）]：RADIUS サーバーでロールを割り当てられていないユーザに割り当てるロール。Service 以外の Viewer、Operator、または Administrator をデフォルトの

ロールにできます。デフォルトのロールを割り当てない場合は、[Unspecified] を選択します（これがデフォルトです）。ユーザ ロールの説明については、IPS ユーザーロールについて （2102 ページ）を参照してください。

（注） ユーザ ロール設定はとても重要です。デフォルトのユーザ ロールを使用せず、RADIUS サーバでもユーザに対してロールを割り当てない場合、センサーは、RADIUS サーバがユーザ名およびパスワードを受け入れたとしてもユーザのログインを阻止します。

RADIUS サーバでユーザに対して明示的にロールを割り当てるには、そのアカウントの Accept Message を、ips-role=administrator、ips-role=operator、ips-role=viewer、または ips-role=service として設定します。ユーザ アカウントごとにそれぞれ Accept Message を設定します。例として、特定のユーザーの Reply 属性は、「Hello <user> your ips-role=operator」を返すように設定できます。

RADIUS サーバでサービス アカウントを設定する場合は、デバイス上でローカルに同じサービス アカウントを設定する必要もあります。サービス アカウントの場合は、ログイン時に RADIUS アカウントとローカル アカウントがチェックされます。

NTP サーバの識別

[NTP] ポリシーを使用して、ネットワーク タイム プロトコル（NTP）サーバを IPS デバイスのタイム ソースとして設定します。NTP を使用すると、ネットワーク デバイス間で時間が同期され、イベント分析に役立ちます。NTP は、IPS デバイスで時間を設定するための推奨される方法です。

Cisco IOS ルータを NTP サーバーとして設定する方法など、センサーに時間を設定する方法の詳細については、コマンド ライン インターフェイス バージョン 7.0 を使用した Cisco Intrusion Prevention System センサーの設定 [英語] の「Configuring Time」を参照してください。

ヒント IPS ソフトウェアの更新に問題がある場合は、IPS センサーで時刻をチェックします。センサーの時刻が、関連付けられている証明書の時刻よりも進んでいる場合、証明書は拒否され、センサー ソフトウェアの更新が失敗します。

ステップ 1 次のいずれかを実行して、[NTP] ポリシーを開きます。

- （デバイス ビュー）ポリシー セレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバー アクセス（Server Access）] > [NTP] を選択します。
- （ポリシー ビュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバー アクセス（Server Access）] > [NTP] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [NTPサーバーIPアドレス（NTP Server IP Address）] フィールドに、NTP サーバーの IP アドレスを入力します。サーバーの単一のホストアドレスを識別するネットワーク/ホストオブジェクトの名前も入力できま

す。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。

（注） Cisco Security Manager 4.19 以降、ASA 9.12(1) 以降のすべてのデバイスに対して、IPV6 アドレスを使用して NTP サーバーを設定できます。

ステップ 3 NTP サーバーに認証が不要な場合は、[認証済みNTP（Authenticated NTP）] チェックボックスをオフにします。

NTP サーバに認証が必要な場合は、次のオプションを設定します。

- [認証済みNTP（Authenticated NTP）]：認証された接続を有効にするには、このオプションを選択します。
- [キー、確認（Key, Confirm）]：NTP サーバーのキー値。キーは、MD5 タイプのキー（数値または文字）です。これは、NTP サーバの設定に使用されたキーです。
- [キーID（Key ID）]：NTP サーバーのキー ID 値（1 ～ 65535 の数値）。

ヒント キーとキー ID は NTP サーバで設定します。これらを NTP サーバ設定から取得する必要があります。

DNS サーバの識別

IPS 7.0+ センサーでグローバル相関を設定する場合、センサーはグローバル相関の更新をダウンロードするときに更新サーバに正常に接続するために、ドメイン名を解決できる必要があります。[DNS] ポリシーを使用して、センサーがドメイン名から IP アドレスへの解決に使用できるドメイン ネーム システム（DNS）サーバを識別します。

ヒント インターネット接続の確立時にネットワークにHTTPプロキシが必要な場合は、[DNS] ポリシーの代わりに [HTTP Proxy] ポリシーを設定します。HTTP プロキシ サーバの識別（2114 ページ）を参照してください。

（注） AIP-SSC-5 サービス モジュールでは、DNS サーバはサポートされません。

ステップ 1 次のいずれかを実行して、HTTP プロキシ ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS] を選択します。

- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [プライマリ（Primary）]、[セカンダリ（Secondary）]、および [ターシャリ（Tertiary）] アドレスフィールドで、最大 3 つの DNS サーバーの IP アドレスを指定します。センサーでは、リストの順序でサーバが使用されます。1 つのサーバが応答しない場合は、次のサーバがアクセスされます。

サーバアドレスを含むネットワーク/ホスト オブジェクトの IP アドレスまたは名前を入力できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。ネットワーク/ホスト オブジェクトでは、単一のホスト アドレスを指定する必要があります。

HTTP プロキシ サーバの識別

IPS 7.0+ センサーにグローバル相関を設定し、ネットワークでインターネットへの接続に HTTP プロキシを使用する必要がある場合は、[HTTP Proxy] ポリシーを設定して、IPS センサーで使用できるプロキシを識別する必要があります。グローバル相関の更新をダウンロードする場合、IPS センサーはこのプロキシを使用して更新サーバに接続します。プロキシは、DNS 名を解決できる必要があります。

ヒント HTTP プロキシを使用しない場合は、IPS センサーが更新サーバのアドレスを解決できるように DNS サーバを設定します。DNS サーバの識別 （2113 ページ）を参照してください。

（注） AIP-SSC-5 サービス モジュールでは、HTTP プロキシ サーバはサポートされません。

ステップ 1 次のいずれかを実行して、HTTP プロキシ ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [HTTPプロキシ（HTTP Proxy）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [HTTPプロキシ（HTTP Proxy）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次のオプションを設定します。

- [プロキシの有効化（Enable Proxy）]：設定したプロキシサーバーを介して接続するようにデバイスに通知するには、このオプションを選択します。

- [IPアドレス（IP Address）]：プロキシサーバーの IP アドレス、またはサーバーの IP アドレスを含むネットワーク/ホストオブジェクトの名前を入力します。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。ネットワーク/ホスト オブジェクトには、単一のホスト IP アドレスが含まれている必要があります。
- [ポート（Port）]：プロキシサーバーへの HTTP 接続に使用するポート番号を入力します。デフォルトは 80 です。

IPS SSHv2 の既知のホストキー

IPS SSHv2 の既知のホストキーポリシーを使用すると、SSHv2 サーバーホストキー（IPS センサーから SSH サーバーへの発信 SSHv2 接続）を設定できます。この機能は、Cisco IPS の 7.1(8) 以降のバージョンを実行している IPS センサーで使用できます。

ホストキーは、有効な IP アドレスを使用して IPS センサーから取得できます。把握している場合は手動で入力することもできます。ホストキーの取得には数秒かかる場合があります。

ステップ 1 次のいずれかを実行して、IPS SSHv2 の既知のホストキーポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [SSHv2の既知のホストキー（SSHv2 Known Host Keys）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [SSHv2の既知のホストキー（SSHv2 Known Host Keys）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

ステップ 2 [追加（Add）] ボタンをクリックして、[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス （2115 ページ）を開きます。

ステップ 3 行を選択してから [編集（Edit）] ボタンをクリックし、[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス （2115 ページ）を開きます。

[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックス

[既知のホストRSAキーの追加または編集（Add or Edit Known Host RSA Key）] ダイアログボックスを使用して、IPS センサーから SSHv2 キーを取得するか、キーがわかっている場合は手動でキーを入力します。

ナビゲーション パス

[SSHv2既知ホストキー（SSHv2 Known Host Keys）] ポリシーから、[IPアドレス/公開キー（IP Address/Public Key）] テーブルにある [追加（Add）] ボタンをクリックするか、テーブルの行を選択して [編集（Edit）] ボタンをクリックします。[SSHv2既知ホストキー（SSHv2 Known Host Keys）] ポリシーについては、IPS SSHv2 の既知のホストキー （2115 ページ）を参照してください。

フィールド リファレンス

表 *510 : [*既知のホスト*RSA*キーの追加または編集（*Add or Edit Known Host RSA Key*）*]* ダイアログボックス

要素	説明
IPアドレス	公開キーを取得する IPS センサーの IP アドレス。
公開キーの取得	[IPアドレス（IP Address）] フィールドで識別されたデバイスから公開キーの取得を開始します。 [公開キーの取得（Retrieve Public Key）] オプションは、デバイスビューで使用できます（共有ポリシービューには表示されません）。ただし、共有ポリシーに公開キーのインライン値を入力するか、デバイスビューで公開キーを取得し、[ポリシーの共有（Share Policy）] オプションを使用して共有することができます。
公開キー（3Public Key）	お客様が知っていて手動で入力できる公開キー。 共有ポリシーの場合、ホストキーのインライン値を入力できます。

IPS SSHv1 フォールバック設定の指定

IPS SSHv1 フォールバックポリシーは、Cisco IPS の 7.1(8) 以降のバージョンを実行している IPS センサーで使用できます。

ステップ 1 次のいずれかを実行して、SSHv1 フォールバックを有効または無効にします。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [設定（Settings）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [設定（Settings）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

ステップ 2 SSHv1 フォールバックを有効にするには、チェックボックスをクリックします。

ステップ 3 SSHv1 フォールバックを無効にするには、チェックボックスをオフにします。

外部製品インターフェイスの設定

[External Product Interface] ポリシーを使用して、Security Manager が Management Center for Cisco Security Agents（CSA MC）と連携する方法を設定します。

一般に、外部製品インターフェイスは、外部セキュリティおよび管理製品から情報を受信して処理するように設計されています。これらの外部セキュリティおよび管理製品は、センサー設定情報を自動的に拡張するために使用できる情報を収集します。Management Center for Cisco Security Agents は、IPS と通信するように設定できる唯一の外部製品です。IPS デバイスごとに最大 2 つの Management Center for Cisco Security Agents サーバを設定できます。

ヒント Management Center for Cisco Security Agents は、アクティブな製品ではなくなりました。このポリシーは、このアプリケーションをまだ使用している場合にだけ設定します。詳細については、『Installing and Using Cisco Intrusion Prevention System Device Manager 6.0』の「About CSA MC」および http://www.cisco.com/en/US/products/sw/cscowork/ps5212/index.html を参照してください。

Management Center for Cisco Security Agents は、ネットワーク ホストでセキュリティ ポリシーを強制します。これには 2 つのコンポーネントがあります。

- ネットワーク ホスト上に存在し、そのホストを保護するエージェント。
- エージェントを管理するアプリケーションである管理コンソール。セキュリティ ポリシーの更新をエージェントにダウンロードし、エージェントから操作情報をアップロードします。

はじめる前に

Security Manager がセンサーに外部製品との通信を許可するように、外部製品を許可ホストとして追加します。詳細については、許可ホストの識別 （2091 ページ）を参照してください。

ステップ 1 次のいずれかを実行して、[External Product Interface] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [外部製品インターフェイス（External Product Interface）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [外部製品インターフェイスExternal Product Interface）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Management Center for Cisco Security Agents] タブには、外部アプリケーションの IP アドレス（またはネットワーク/ホストオブジェクト）、URL、およびポート、ログインに使用されるユーザ名とパスワード、接続がイネーブルになっているかどうかなどの既存の定義が表示されます。インターフェイス タイプは常に [Extended SDEE] です。

ステップ 2 次のいずれかを実行します。

- サーバーを追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [External Product Interface] ダイアログボックスが開きます。サーバの識別に必要な情報を入力し、ポスチャ ACL を設定します。設定の詳細については、[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス （2118 ページ）を参照してください。

最大 2 台のサーバを追加できます。

- サーバーを編集するには、そのサーバーを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックして、[外部製品インターフェイス（External Product Interface）] ダイアログボックスに必要な変更を加えます。
- サーバーを削除するには、そのサーバーを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス

[Add External Product Interface]/[Edit External Product Interface] ダイアログボックスを使用して、Management Center for Cisco Security Agents（CSA MC）と IPS デバイスおよび関連ポスチャ ACL との間のインターフェイスを追加または修正します。

ナビゲーション パス

[外部製品インターフェイス（External Product Interface）] IPS プラットフォームポリシーで、[行の追加（Add Row）] をクリックするか、エントリを選択して [行の編集（Edit Row）] をクリックします。[External Product Interface] ポリシーを開く方法については、外部製品インターフェイスの設定 （2117 ページ）を参照してください。

フィールド リファレンス

表 511 : [Add External Product Interface]/[Edit External Product Interface] ダイアログボックス

要素	説明
[外部製品のIPアドレス（External Product's IP Address）]	外部製品の IP アドレス、またはアドレスを含むネットワーク/ホスト ポリシー オブジェクト。IP アドレスまたはオブジェクト名を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
インターフェイス タイプ	物理インターフェイス タイプを識別します。これは常に [Extended SDEE] です。
Enable receipt of information	外部製品からセンサーに情報を渡せるかどうか。

要素	説明
SDEE URL	IPS が SDEE 通信を使用して情報を取得するために使用する CSA MC 上の URL。IPS が通信している CSA MC のソフトウェア バージョンに基づいて、URL を次のように設定する必要があります。 • CSA MC バージョン 5.0 の場合：/csamc50/sdee-server。 • CSA MC バージョン 5.1 の場合：/csamc51/sdee-server。 • CSA MC バージョン 5.2 以降の場合：/csamc/sdee-server（デフォルト値）。
[ポート（Port）]	通信に使用するポートまたはポートを識別するポート リスト オブジェクト。ポートまたはポートリスト名を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
ユーザー名 [パスワード（Password）]	外部製品にログインできるユーザ名とパスワード。
Enable receipt of host postures	CSA MC からのホスト ポスチャ情報の受信を許可するかどうか。このオプションをディセーブルにした場合、CSA MC から受信したホスト ポスチャ情報は削除されます。
[到達不能ホストのポスチャを許可（Allow unreachable hosts' postures）]	CSA MC が到達できないホストのホスト ポスチャ情報の受信を許可するかどうか。 CSA MC がホストポスチャに含まれるどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IP アドレスが IPS センサーから参照可能でないポスチャ、またはネットワーク上で重複している可能性のあるポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC が到達できないホストには IPS でも到達できないようなネットワーク トポロジ（IPS と CSA MC が同じネットワーク セグメントにあるなど）に最適です。

要素	説明
[Posture ACL] テーブル	ポスチャ ACL とは、ネットワーク アドレス範囲です。その範囲に対してホスト ポスチャが許可または拒否されます。ポスチャ ACL を使用して、IPS で認識できない、またはネットワーク全体で重複している可能性がある IP アドレスを持つポスチャをフィルタリングします。 • ポスチャ ACL を追加するには、[行の追加（Add Row）]（+）ボタンをクリックします。この操作によって [Add Posture ACL] ダイアログボックスが開きます。ポスチャ ACL の設定の詳細については、[Add Posture ACL]/[Modify Posture ACL] ダイアログボックス （2120 ページ）を参照してください。 • ポスチャ ACL を編集するには、ポスチャ ACL を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • ポスチャ ACL を削除するには、ポスチャ ACL を選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。 • ACL のプライオリティを変更するには、その ACL を選択し、[Up] または [Down] ボタンをクリックします。ACL は順番に処理され、最初の一致に関連付けられているアクションが適用されます。
Enable receipt of watch listed addresses	CSA MC からのウォッチ リスト情報の受信を許可するかどうか。このオプションをディセーブルにした場合、CSA MC から受信したウォッチ リスト情報は削除されます。
Manual Watch List RR increase	手動ウォッチ リスト Risk Rating（RR; リスク レーティング）のパーセンテージ。デフォルトは 25 で、有効な範囲は 0 ～ 35 です。
Session-based Watch List RR Increase	セッション ベースのウォッチ リスト リスク レーティングのパーセンテージ。デフォルトは 25 で、有効な範囲は 0 ～ 35 です。
Packed-based Watch List RR Increase	パケット ベースのウォッチ リスト リスク レーティングのパーセンテージ。デフォルトは 10 で、有効な範囲は 0 ～ 35 です。

[Add Posture ACL]/[Modify Posture ACL] ダイアログボックス

[Add Posture ACL]/[Modify Posture ACL] ダイアログボックスを使用して、Management Center for Security Agents のポスチャ ACL を設定します。ポスチャ ACL とは、ネットワーク アドレス範囲です。その範囲に対してホスト ポスチャが許可または拒否されます。ポスチャ ACL を使用して、IPS で認識できない、またはネットワーク全体で重複している可能性がある IP アドレスを持つポスチャをフィルタリングします。

次のフィールドを設定して、ポスチャ ACL を定義します。

- [ネットワークアドレス（Network Address）]：ホストまたはネットワークの IP アドレスまたはホスト、または IP アドレスを指定するネットワーク/ホストオブジェクトの名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成できます。
- [アクション（Action）]：ホストポスチャがネットワークアドレス上のホストで許可されるか拒否されるか。

ナビゲーション パス

[外部製品インターフェイス（External Product Interface）] ダイアログボックス（[Add External Product Interface]/[Edit External Product Interface] ダイアログボックス （2118 ページ）を参照）で、[ポスチャACL（Posture ACL）] テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックするか、ポスチャ ACL を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

IPS ロギング ポリシーの設定

IPS プラットフォームの [Logging] ポリシーを使用して、トラフィック フロー通知と分析エンジンのグローバル変数を設定します。これらの設定は、IPS センサーの一般操作に適用されます。

トラフィック フロー通知では、センサーのインターフェイス上のトラフィック フローを扱う必要があります。インターフェイス上のパケットのフローをモニタし、そのフローが指定した間隔中に変更（開始および停止）された場合に通知を送信するようにセンサーを設定できます。特定の通知間隔内に欠落パケットのしきい値を設定でき、ステータスイベントがレポートされる前のインターフェイス アイドル遅延も設定できます。

分析エンジンは、パケット分析とアラート検出を実行します。指定したインターフェイスを流れるトラフィックをモニタします。分析エンジンには、[Maximum Open IP Log Files] という 1 つのグローバル変数だけがあります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] を選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [ロギング（Logging）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 512 : [IPS Logging] ページ

要素	説明
[Interface Notifications] タブ	

要素	説明
Missed Packets Threshold	通知を受信する前に発生する必要のある欠落パケットの割合。デフォルトは 0 で、範囲は 0 ～ 100 です。
通知間隔（Notification Interval）	欠落パケットのパーセンテージをチェックする時間の長さ（秒単位）。デフォルトは 30 で、有効な範囲は 5 ～ 3600 です。
Interface Idle Threshold	この時間が経過すると通知が生成される、インターフェイスがアイドルになってパケットを受信しない時間の長さ（秒単位）。デフォルトは 30 で、有効な範囲は 5 ～ 3600 です。
[Analysis Engine] タブ	
フロー深度の指定（Specify-Flow-Depth）	フローの検査深度を指定できます。フロー深度は、フローで検査されるバイト数です。新しい値は、新しいフローにのみ適用されます。有効な範囲は 0 ～ 4294967296 です。デフォルトは 0 です。
サービスアクティビティの有効化（Enable Service Activity）	サービスアクティビティを使用して、診断目的でサービスアクティビティに関する情報を収集できます。詳細はよりきめ細かく、ポートレベルの詳細があります。サービスアクティビティを有効にすると、システムのパフォーマンスに影響します。診断目的でのみ、サービスアクティビティの収集を一時的に有効にします。変更を有効にするには、サービスアクティビティを有効にした後、センサーをリブートする必要があります。
サービスアクティビティの制限（Service Activity Limit）	有効にするサービスの数の制限を設定します。有効範囲は 10 ～ 65536 です。デフォルトは 15 です。
（注） [フロー深度の指定（Specify-Flow-Depth）]、[サービスアクティビティの有効化（Enable Service Activity）]、および[サービスアクティビティの制限（Service Activity Limit）] フィールドは、バージョン 7.2(2) 以降の IPS デバイスに適用されます。	
Maximum Open IP Log Files	センサーで開くことのできる IP ログ ファイルの最大数。デフォルトは 20 で、範囲は 20 ～ 100 です。

IPS ヘルスモニター

[IPS ヘルスモニター（IPS Health Monitor）] ページで、IPS デバイスの正常性およびネットワーク セキュリティ ステータスを判断するために使用されるメトリック（パラメータ）を設定できます。IPS デバイスは、これらのメトリックを使用して、IPS イベントを送信するときに適切なシビラティ（重大度）を割り当てます。結果は、Security Manager の Health and Performance Monitor（[起動（Launch）] > [Health and Performance Monitor]）に表示されます。

IPS Health Monitor は、IPS バージョン 6.1 以降の IPS デバイスとバージョン 4.4 以降の Security Manager でサポートされています。次の特殊なケースに注意してください。

1. 7.x を実行している IPS デバイスの場合、IPS セキュリティ設定ポリシーの 11 の設定項目はすべて、Security Manager GUI で適切に表示および監視されます。
2. 6.1 より前のバージョンを実行している IPS デバイスの場合、ネットワーク参加とグローバル相関のエントリは、Security Manager のデバイスビューに表示されません。
3. IPS ヘルスモニターの一部の設定項目は、デバイス側自体で保護されているエントリであり、編集できません。そのような場合は、Security Manager によって通知されます。

チェックボックスをオンにしてメトリックを選択しないと、Health and Performance Monitor に表示されません。デフォルト設定を受け入れるか、値を編集できます。メトリックを選択しないと、項目は無効になり、編集できません。

すべてのメトリックの中で最も重要な設定が、全体的な正常性になります。たとえば、選択されたメトリックが、1 つのクリティカルを除いてすべて正常であっても、全体的な正常性はクリティカルになります。IPS センサーの全体的な正常性ステータスが変化すると、IPS センサーは正常性およびセキュリティ ステータス イベントを送信します。

IPS センサーのセキュリティステータスは、仮想センサーによって検出されたイベントの脅威レーティングを使用して、仮想センサーごとに決定されます。仮想センサーが、その仮想センサーのしきい値を超える脅威レーティングを持つイベントを検出すると、その仮想センサーのセキュリティステータスが上昇します。しきい値を超えると、そのセキュリティステータスは、イベントがより高いレベルで検出されずに、設定された時間が経過するまで、クリティカルレベルで維持されます。

[IPS ヘルスモニター（IPS Health Monitor）] ページでメトリックを設定するには、次のいずれかのポリシーを選択します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ヘルスモニター（Health Monitor）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS] > [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ヘルスモニター（Health Monitor）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

（注） ポリシービューでは、共有 IPS ヘルスモニターポリシーが、6.1 より前のバージョンを実行している IPS デバイスに適用されている場合、検証が実行されません。Security Manager は、デバイスへの展開時にそのようなポリシーを無視し、展開ログにもそれらをキャプチャします。

次の表で、設定できる IPS ヘルスモニターメトリックについて説明します。

表 *513 : IPS* セキュリティ設定ポリシー

要素	説明
[検査負荷（Inspection Load）]	検査負荷のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。
[受信できなかったパケット（Missed Packet）]	受診できなかったパケットのしきい値のパーセントと、このメトリックがセンサーの全体的なヘルスレーティングに適用されるかどうかを設定できます。
メモリ使用率	メモリ使用量のしきい値のパーセントと、このメトリックがセンサーの全体的なヘルスレーティングに適用されるかどうかを設定できます。
シグニチャ アップデート	最後のシグニチャのアップデートが適用された時間のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。
ライセンスの期限切れ	ライセンスの有効期限のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。
[イベント取得（Event Retrieval）]	最後にイベントが取得された時間のしきい値と、このメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを設定できます。 （注） イベント取得メトリックでは、IME などの外部モニタリングアプリケーションによって最後のイベントが取得された時間が記録されます。外部のイベントモニタリングを実行しない場合は、[イベント取得（Event Retrieval）] を無効にします。
ネットワーク参加	ネットワーク参加ヘルスメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。
グローバル相関	グローバル相関ヘルスメトリックをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。
アプリケーションの障害	センサーの全体的なヘルスレーティングにアプリケーションの障害を適用することを選択できます。
[バイパスモードの IPS（IPS in Bypass Mode）]	バイパスモードがアクティブであるかどうかを認識し、それをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。

要素	説明
[1 つ以上のアクティブインターフェイスがダウン（One or More Active Interfaces Down）]	1 つ以上のインターフェイスがダウンしているかどうかを認識し、それをセンサーの全体的なヘルスレーティングに適用するかどうかを選択できます。
警告	警告しきい値の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。
重大	重大しきい値の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。

IPS セキュリティ設定の指定

IPS セキュリティ設定ポリシーを使用すると、IPS デバイスのセキュリティにとって重要な次の 2 つの項目を設定できます。

- パケットキャプチャロギングの許可（Permit packet capture logging）：この機能を使用すると、IPS デバイスは、ユーザーによる packet capture/display/iplog コマンドの任意の実行を防ぐことができます。以前のバージョンの Cisco Security Manager では、そのようなアクションにおいて、コマンドを実行したユーザーの痕跡が残りませんでした。
- 設定可能なアイドルタイムアウト（Configurable idle timeout）：この機能を設定している場合、指定した時間が経過すると IPS デバイスへの接続が終了します。その目的は、CLI セッションのセキュリティを強化することです。

（注） これらの設定は、IPS 7.1.3 以降で動作するデバイスで使用できます。

IPS セキュリティ設定を指定するには、次のいずれかのポリシーを選択します。

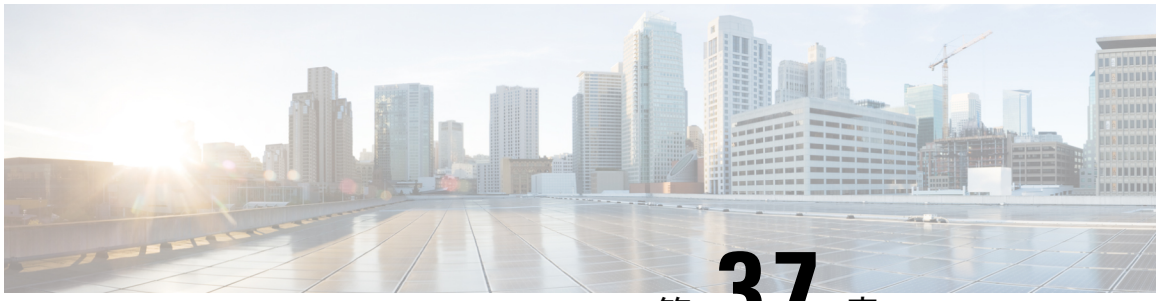
- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [設定（Settings）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [設定（Settings）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

次の表で、定義できる IPS セキュリティ設定について説明します。

表 *514 : IPS* セキュリティ設定ポリシー

要素	説明
[パケットロギングの許可（Permit packet logging）]	パケットロギングを有効にするかどうか。packet capture/display/iplog コマンドに適用されます。

要素	説明
[CLI の非アクティブタイムアウト（分単位）（CLI Inactivity Timeout (In Minutes)）]	指定した時間が経過すると、IPSデバイスへの接続が終了します。



第 37 章

IPS デバイスインターフェイスの管理

Cisco IOS IPS デバイスは通常のルータ インターフェイス ポリシーを使用して設定しますが、専用IPSアプライアンスおよびサービスモジュールには、独自のインターフェイス設定があります。この章では、専用IPSアプライアンスおよびサービスモジュール独自のインターフェイスを設定する方法について説明します。

この章は次のトピックで構成されています。

- インターフェイスについて （2127 ページ）
- インターフェイス モードについて （2129 ページ）
- インターフェイスの設定 （2133 ページ）

インターフェイスについて

ヒント この項では、IPS インターフェイスの概要について説明します。アプライアンスおよびサービスモジュールの各タイプに関する特定のインターフェイスの名前と位置、サポートされているロール、設定上の制限、ハードウェアに関する考慮事項など、詳細な説明については、Cisco.com で、ご使用の IPS ソフトウェアバージョンの『Installing and Using Cisco Intrusion Prevention System Device Manager』の「Configuring Interfaces」の章を参照してください。この情報は、IME ガイドおよび CLI ガイドでも提供されています。全般情報については、http://www.cisco.com/go/ips を参照してください。

センサーのインターフェイスは、インターフェイスの最大速度および物理的な場所に従って名前が付けられています。たとえば、GigabitEthernet2/1 は、1 ギガビットの最大速度をサポートし、下から 2 番めの拡張スロットの右から 2 番めのインターフェイスです。

インターフェイスには、次の 3 つの役割があります。

- **コマンド/コントロール**：コマンド/コントロール インターフェイスは、IP アドレスを持ち、センサーの設定に使用されます。このインターフェイスは、センサーからセキュリティ イベントとステータス イベントを受信し、センサーに統計情報を問い合わせます。

コマンド/制御インターフェイスは、常にイネーブルです。このインターフェイスは特定の物理インターフェイス（センサーのモデルによって異なる）に常時マッピングされています。コマンド/制御インターフェイスを検知インターフェイスや代替 TCP リセット インターフェイスとして使用することはできません。デバイス タイプ別のコマンド/コントロール インターフェイスのリストについては、上記の IPS マニュアルを参照してください。

- **検知**：検知インターフェイスは、セキュリティ違反に関してトラフィックを分析するために、センサーによって使用されます。センサーには、1 つ以上の検知インターフェイスがあり、その数はセンサーによって異なります。検知インターフェイスは、無差別モードで個別に動作させるか、またはペアにしてインライン インターフェイスを作成できます。無差別モードでは、パケットはセンサーを通過しません。センサーは、モニタ対象トラフィックのコピーを分析します。インライン モードでは、IPS はトラフィック フローに挿入され、トラフィックに直接影響を与えます。検知モードの詳細については、インターフェイス モードについて （2129 ページ）を参照してください。

（注） アプライアンスでは、すべての検知インターフェイスがデフォルトでディセーブルになっています。これらのインターフェイスを使用するには、イネーブルにする必要があります。モジュールでは、検知インターフェイスは常にイネーブルです。デバイス タイプ別の検知インターフェイスのリストについては、上記の IPS マニュアルを参照してください。

- **代替 TCP リセット**：攻撃者のホストと攻撃のターゲットホストとの間のネットワーク接続をリセットするために、TCP リセットパケットを送信するようにセンサーを設定できます。一部のインストールでは、インターフェイスが無差別モードで動作している場合、攻撃が検出された検知インターフェイスと同じインターフェイスでセンサーが TCP リセットパケットを送信できないことがあります。このような場合は、検知インターフェイスを代替 TCP リセット インターフェイスに関連付けることができます。これにより、無差別モードで動作している場合に通常は検知インターフェイスで送信されるすべての TCP リセットを、関連付けた代替 TCP リセット インターフェイスで送信できます。

検知インターフェイスが代替 TCP リセット インターフェイスに関連付けられている場合、その関連付けは、センサーが無差別モードに設定されている場合は適用されますが、検知インターフェイスがインライン モード（インターフェイスまたは VLAN ペア）に設定されている場合は無視されます。TCP リセットは、これらのモードの検知インターフェイスで常に送信されるためです。

（注） IDSM-2 を除いて、すべての検知インターフェイスは、別の検知インターフェイスの代替 TCP リセット インターフェイスとなることができます。IDSM-2 の代替 TCP リセット インターフェイスは、ハードウェアの制限があるために固定されています。ただし、（ルータまたは ASA デバイス上の）IPS モジュールに存在する検知インターフェイスは 1 つだけであるため、IPS モジュールでは代替 TCP リセット インターフェイスを指定できません。デバイス タイプ別の適格な代替 TCP リセット インターフェイスのリスト、および代替 TCP リセット インターフェイスを使用する状況の詳細については、上記の IPS マニュアルを参照してください。

インターフェイス モードについて

検知インターフェイスは、さまざまなモードで動作できます。インターフェイスに設定されたモードによって、検査できるトラフィックおよびイベントへの応答方法が決まります。

ここでは、次の内容について説明します。

- 無差別モード （2129 ページ）
- インライン インターフェイス モード （2130 ページ）
- インライン VLAN ペア モード （2130 ページ）
- VLAN グループ モード （2131 ページ）

無差別モード

無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されるパケットではなく、モニタ対象のトラフィックのコピーを分析します。無差別モードで運用する利点は、転送されるトラフィックでパケットのフローにセンサーが影響を与えないことです。ただし、無差別モードで運用するときは、アトミック アタック（シングル パケット攻撃）などの特定のタイプの攻撃の場合に、悪意のあるトラフィックがターゲットに到達することをセンサーで阻止できないという短所があります。無差別モードのセンサーデバイスによって実行される応答アクションはイベント後の応答であるため、多くの場合、攻撃に対応するために、ルータやファイアウォールなど、他のネットワーキング デバイスによるサポートが必要となります。このような応答アクションは一部の攻撃を防ぐことはできますが、アトミック アタックでは、無差別モードベースのセンサーが管理対象デバイス（ファイアウォール、スイッチ、ルータなど）に ACL 修正を適用する前に、シングル パケットがターゲット システムに到達する可能性があります。

デフォルトでは、すべての検知インターフェイスは無差別モードです。インターフェイスをインライン インターフェイス モードから無差別モードに変更するには、変更対象のインターフェイスを含むすべてのインライン インターフェイスを削除し、インターフェイス設定からそのインターフェイスのすべてのインライン VLAN ペアのサブインターフェイスを削除します。

関連項目

- インターフェイスについて （2127 ページ）
- 物理インターフェイスの設定 （2139 ページ）

インライン インターフェイス モード

インライン インターフェイス ペア モードで運用する場合は、IPS が直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。遅延が加わるため、パケット転送速度は遅くなります。その結果、センサーは、悪意のあるトラフィックがターゲットに到達する前にそのトラフィックをドロップして攻撃を阻止できるため、保護サービスが提供されます。インラインデバイスは、レイヤ3および4で情報を処理するだけでなく、より高度な埋め込み型攻撃のパケットの内容およびペイロードも分析します（レイヤ 3 ～ 7）。この詳細な分析では、通常は従来のファイアウォールデバイスを通過する攻撃をシステムが識別し、停止またはブロックすることができます。

インラインインターフェイスペア モードでは、パケットはセンサーのペアの1つめのインターフェイスを経由して入り、ペアの2つめのインターフェイスを経由して出ます。パケットは、シグニチャによって拒否または変更されないかぎり、ペアの2つめのインターフェイスに送信されます。

（注）

- ペアになっているインターフェイスが同じスイッチに接続されている場合は、それらのインターフェイスをスイッチ上で 2 つのアクセス ポートとして設定し、それぞれが異なるVLANアクセスを持つようにする必要があります。このようにしないと、トラフィックはインライン インターフェイスを通過しません。
- ルータおよび ASA デバイスの IPS モジュールは、検知インターフェイスが 1 つしかない場合でも、インラインで動作するように設定できます。

関連項目

- インターフェイスについて （2127 ページ）
- インライン インターフェイス ペアの設定 （2144 ページ）

インライン VLAN ペア モード

物理インターフェイス上で、VLANをペアで関連付けることができます。これは、インライン VLAN ペア モードと呼ばれます。ペアの一方の VLAN で受信されたパケットは、分析後にペアのもう一方の VLAN に転送されます。

インラインVLANペア モードは、アクティブ検知モードです。このモードでは、検知インターフェイスが 802.1q トランク ポートとして動作し、センサーがトランク上の VLAN のペア間のVLANブリッジングを実行します。センサーは、ペアごとに各VLAN上で受信するトラフィッ

クを検査し、そのパケットをペアのもう一方の VLAN に転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。IPS センサーは、各検知インターフェイス上で最大 255 個の VLAN ペアを同時にブリッジするように設定できます。センサーは、受信した各パケットの 802.1q ヘッダー内の VLAN ID フィールドを、センサーがパケットを転送する出力 VLAN の ID に置き換えます。センサーは、インライン VLAN ペアに割り当てられていないすべての VLAN で受信したすべてのパケットをドロップします。

（注）

- インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。
- インライン VLAN ペアは、ルータまたは ASA デバイスの IPS モジュールではサポートされていません。

関連項目

- インターフェイスについて （2127 ページ）
- インライン VLAN ペアの設定 （2145 ページ）

VLAN グループ モード

各物理インターフェイスまたはインラインインターフェイスは、VLAN グループサブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスのVLANのグループで構成されます。複数の仮想センサーを設定している場合、各仮想センサーは、これらのインターフェイスの1つまたは複数をモニタできます。これにより、複数のポリシーを同じセンサーに適用できます。この利点は、わずかなインターフェイスしかないセンサーを多くのインターフェイスがあるかのように使用できる点にあります。

（注） インライン VLAN ペアに含まれている物理インターフェイスは、VLAN グループに分けることはできません。

VLAN グループ サブインターフェイスによって、物理インターフェイスまたはインライン インターフェイスと VLAN セットが関連付けられます。VLAN を複数の VLAN グループ サブインターフェイスのメンバにすることはできません。各 VLAN グループ サブインターフェイスは、1 ～ 255 の数値で識別されます。サブインターフェイス 0 は、仮想化されていない物理インターフェイスまたは論理インターフェイス全体を表すために使用される予約済みのサブインターフェイス番号ですサブインターフェイス0を作成、削除、または変更することはできません。また、サブインターフェイス 0 に関する統計情報は報告されません。

VLAN グループを作成すると、次のように無差別またはインラインに設定されます。

- 無差別 VLAN グループ：物理インターフェイスで VLAN グループを設定する場合、その VLAN グループは、無差別モード （2129 ページ）で説明しているように無差別になります。
- インライン VLAN グループ：インライン インターフェイス ペア（論理インターフェイス）で VLAN グループを設定する場合、VLAN グループは、インライン インターフェイス モード （2130 ページ）で説明しているようにインラインになります。

したがって、VLAN グループは、選択した VLAN にインターフェイスの動作を制限することにより、無差別モード インターフェイスまたはインライン インターフェイスの動作を強化します。VLAN グループを物理インターフェイスまたはインライン インターフェイスに割り当てると、そのインターフェイスは単なる無差別またはインライン インターフェイス ペアではなくなり、インライン VLAN グループに対してだけ使用できるようになります。

未割り当て VLAN グループは、別の VLAN グループに明示的に割り当てられていないすべての VLAN を含んでいる状態で維持されます。未割り当て VLAN グループ内の VLAN を直接指定することはできません。別の VLAN グループ サブインターフェイスに VLAN が追加されたり、または別の VLAN グループ サブインターフェイスから VLAN が削除されたりすると、未割り当て VLAN グループは更新されます。

通常、802.1q トランクのネイティブ VLAN 内のパケットには、そのパケットが属する VLAN 番号を示す 802.1q カプセル化ヘッダーがありません。各物理インターフェイスには、デフォルトの VLAN 変数が関連付けられており、この変数をネイティブ VLAN の VLAN 番号または 0 に設定する必要があります。値 0 は、ネイティブ VLAN が不明であるか、またはネイティブ VLAN の指定の有無は関係ないことを示しています。デフォルトの VLAN 設定が 0 の場合は、次の処理が行われます。

- 802.1q カプセル化のないパケットによってトリガーされたアラートには、VLAN 値 0 が報告されます。
- 802.1q カプセル化のないトラフィックは未割り当て VLAN グループに関連付けられ、ネイティブ VLAN として他の VLAN グループに割り当てることができません。

（注） スイッチのポートは、アクセス ポートまたはトランク ポートとして設定できます。アクセス ポートでは、すべてのトラフィックは、アクセス VLAN と呼ばれる 1 つの VLAN 内にあります。トランク ポートでは、ポートで複数の VLAN を伝送することができ、各パケットには VLAN ID を含む 802.1q ヘッダーと呼ばれる特別なヘッダーが付加されます。このヘッダーは、一般に VLAN タグと呼ばれます。ただし、トランク ポートには、ネイティブ VLAN と呼ばれる特別な VLAN があります。ネイティブ VLAN 内のパケットには、802.1q ヘッダーは付加されていません。IDSM-2 は、ネイティブでないすべてのトラフィックの 802.1q ヘッダーを読み取り、そのパケットの VLAN ID を判断することができます。ただし、IDSM-2 は、スイッチ設定内のポートのネイティブ VLAN としてどの VLAN が設定されているかは把握していないため、ネイティブパケットを受信する VLAN も認識できません。したがって、どの VLAN が該当のポートのネイティブ VLAN であるかを IDSM-2 に通知する必要があります。IDSM-2 は、タグが付いていないパケットを、ネイティブ VLAN ID のタグが付いたパケットとして処理します。

関連項目

- VLAN グループの展開　（2133 ページ）
- インターフェイスについて　（2127 ページ）
- VLAN グループの設定　（2147 ページ）

VLAN グループの展開

インライン ペアの VLAN グループは、VLAN ID を変換しません。したがって、論理インターフェイスで VLAN グループを使用するには、2 つのスイッチ間にインライン ペア インターフェイスが存在する必要があります。アプライアンスの場合、2 つのペアを同じスイッチに接続し、それらをアクセス ポートにして、2 つのポートに対して別々にアクセス VLAN を設定できます。この設定では、センサーは 2 つの VLAN 間を接続します。これは、2 つのポートはそれぞれアクセス モードであり、1 つの VLAN だけを伝送するためです。この場合、2 つのポートは異なる VLAN に存在する必要があります。センサーはこれら 2 つの VLAN をブリッジし、2 つの VLAN 間を流れるすべてのトラフィックをモニタします。IDSM-2 の 2 つのデータ ポートは常に同じスイッチに接続されているため、IDSM-2 はこの方法でも動作します。

2 つのスイッチ間にアプライアンスを接続することもできます。2 つの方法があります。第 1 の方法では、2 つのポートがアクセス ポートとして設定されるため、1 つの VLAN を伝送できます。この方法では、センサーは 2 つのスイッチ間で 1 つの VLAN をブリッジします。

第 2 の方法では、2 つのポートはトランク ポートとして設定されるため、複数の VLAN を伝送できます。この設定では、センサーは2つのスイッチ間で複数の VLAN をブリッジします。複数の VLAN がインライン インターフェイス ペアで伝送されるため、VLAN をグループに分けることができ、各グループを仮想センサーに割り当てることができます。第 2 の方法は、IDSM-2 には適用されません。IDSM-2 はこの方法では接続できないためです。

関連項目

- インターフェイスについて　（2127 ページ）
- VLAN グループ モード　（2131 ページ）
- VLAN グループの設定　（2147 ページ）

インターフェイスの設定

IPS アプライアンスおよびサービス モジュールのインターフェイス ポリシーを使用して、デバイスのインターフェイス設定値を設定します。ここでは、さまざまなタイプの設定値を設定する方法について説明します。これらの項は、標準のルータ インターフェイス ポリシーを使用する Cisco IOS IPS デバイスには該当しません。

- IPS インターフェイス ポリシーについて　（2134 ページ）
- 物理インターフェイスの設定　（2139 ページ）

- バイパス モードの設定 （2142 ページ）
- CDP モードの設定 （2143 ページ）
- インライン インターフェイス ペアの設定 （2144 ページ）
- インライン VLAN ペアの設定 （2145 ページ）
- VLAN グループの設定 （2147 ページ）
- IPS インターフェイス設定のサマリーの表示 （2137 ページ）

IPS インターフェイス ポリシーについて

IPS インターフェイス ポリシーを使用して、IPS アプライアンスおよびサービス モジュールで、物理インターフェイス、インライン ペア、VLAN ペア、および VLAN グループを設定できます。このポリシーは、Cisco IOS IPS デバイスには適用されません。

無差別モード、インライン ペア モード、インライン VLAN ペア モード、無差別 VLAN グループ、またはインライン VLAN グループで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせてインターフェイスを設定することはできません。

ヒント ポリシーの内容は、デバイス タイプおよび IPS ソフトウェア バージョンによって異なります。たとえば、一部のデバイスには、物理インターフェイスのタブだけが表示されるため、別のタイプの設定を作成することはできません。次に説明するタブまたはオプションが、設定するポリシーで表示されない場合、そのデバイスには適用されません。

ナビゲーション パス

（デバイスビューのみ）ポリシーセレクタから [IPS] > [インターフェイス（Interfaces）] を選択します。

関連項目

- インターフェイスについて （2127 ページ）
- インターフェイス モードについて （2129 ページ）
- Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）

フィールド リファレンス

表 *515 : IPS* インターフェイス ポリシー

要素	説明
[Physical Interfaces] タブ	デバイスで使用可能な物理インターフェイス。デバイスで使用可能なインターフェイスのみ編集できます（デバイスを選択し、[行の編集（Edit Row）] ボタンをクリックします）。デバイス上でインベントリ検出を実行して、物理インターフェイスの正しいリストを取得する必要があります（インターフェイス カードをデバイスに追加する場合など）。 このタブに表示されるカラムは、各インターフェイスの設定を示し、[Modify Physical Interface Map] ダイアログボックス （2140 ページ）で説明されています。[Administrative State] カラムは、インターフェイスがイネーブルであるかどうか（[Yes] または [No]）を示していることに注意してください。インターフェイスを動作させるには、インターフェイスをイネーブルにする必要があります。 詳細については、物理インターフェイスの設定 （2139 ページ）を参照してください。
[Inline Pairs] タブ	インライン インターフェイス モード （2130 ページ）で説明しているように、インライン モード処理を可能にするインライン インターフェイス ペア。この表には、ペアの名前、それぞれのインターフェイス、および説明（ある場合）が示されます。詳細については、 インライン インターフェイス ペアの設定 （2144 ページ）を参照してください。 • ペアを追加するには、[行の追加（Add Row）] ボタンをクリックし、[インターフェイスペアの追加（Add Interface Pair）] ダイアログボックスに入力します。 • ペアを編集するには、ペアを選択して [行の編集（Edit Row）] ボタンをクリックします。 • ペアを削除するには、そのペアを選択して [行の削除（Delete Row）] ボタンをクリックします。

要素	説明
[VLAN Pairs] タブ	インライン VLAN ペア モード （2130 ページ）で説明しているように、各物理インターフェイスの VLAN ペア。この表には、インターフェイスおよびサブインターフェイス、ペアになっている 2 つの VLAN、および説明（ある場合）を示します。詳細については、インライン VLAN ペアの設定 （2145 ページ）を参照してください。 • ペアを追加するには、[行の追加（Add Row）] ボタンをクリックし、[VLAN ペアの追加（Add VLAN Pair）] ダイアログボックスに入力します。 • ペアを編集するには、ペアを選択して [行の編集（Edit Row）] ボタンをクリックします。 • ペアを削除するには、そのペアを選択して [行の削除（Delete Row）] ボタンをクリックします。
[VLAN Groups] タブ	VLAN グループ モード （2131 ページ）で説明しているように、物理インターフェイスまたはインライン ペアに定義されている VLAN グループ。この表には、インターフェイスまたはペアの名前、VLAN グループ（空白の場合は、未割り当てのすべての VLAN を意味します）、および説明（ある場合）を示します。詳細については、VLAN グループの設定 （2147 ページ）を参照してください。 • グループを追加するには、[行の追加（Add Row）] ボタンをクリックし、[VLAN グループの追加（Add VLAN Group）] ダイアログボックスに入力します。 • グループを編集するには、グループを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • グループを削除するには、グループを選択し、[行の削除（Delete Row）] ボタンをクリックします。
[サマリー（Summary）] タブ	検知インターフェイスをどのように設定したか（無差別モードに設定したインターフェイス、インライン ペアとして設定したインターフェイス、およびインライン VLAN ペアとして設定したインターフェイス）のサマリー。 詳細については、IPS インターフェイス設定のサマリーの表示 （2137 ページ）を参照してください。

要素	説明
[バイパスモード（Bypass Mode）]	デバイスのバイパス モード。このモードによって、センサー プロセスがアップグレードのために一時的に停止した場合や、センサー モニタリング プロセスが失敗した場合に、センサーがインライン モード トラフィックを処理する方法が決定されます。これは、デバイス上のすべてのインライン モードに適用されるグローバル設定です。必要なオプションを選択します。各オプションがインライン トラフィックに与える影響の詳細については、バイパス モードの設定 （2142 ページ）を参照してください。 • [オフ（インライントラフィックを常に検査する）（Off (Always inspect inline traffic)）]：バイパスモードを無効にします。トラフィックは常に検査され、センサーのモニタリング プロセスがダウンした場合は、トラフィックが通過しなくなります。 • [オン（インライントラフィックを検査しない）（On (Never inspect inline traffic)）]：トラフィックは、分析エンジンをバイパスし、検査されません。 • [自動（分析エンジンが停止している場合は検査をバイパスする）（Auto (Bypass inspection when analysis engine is stopped)）]：センサーのモニタリング プロセスがダウンしている場合を除き、トラフィックは検査されます。モニタリング プロセスがダウンした場合、トラフィックは検査されずにセンサーを通過し続けます。これがデフォルトです。Auto モードは、センサーのアップグレード時に役立ちます。センサーのアップグレード中でもトラフィック フローが確保されるからです。
CDP Mode	Cisco Discovery Protocol（CDP）パケットの処理方法。CDP 設定は、デバイス上のすべてのインターフェイスにグローバルに適用されます。ただし、効果があるのはインライン インターフェイス（インライン インターフェイスとインライン VLAN ペア）だけです。詳細については、CDP モードの設定 （2143 ページ）を参照してください。次のうち、適切なオプションを選択します。 • [CDPパケットの転送（Forward CDP packets）]：CDP パケットがセンサーを通過できるようにします。 • [CDPパケットをドロップ（Drop CDP packets）]：センサーにすべての CDP パケットをドロップさせ、センサーを通過できないようにします。これがデフォルト設定です。

IPS インターフェイス設定のサマリーの表示

インターフェイス ポリシーの [Summary] タブには、検知インターフェイスを設定した方法（無差別モードに設定したインターフェイス、インライン ペアとして設定したインターフェイス、インライン VLAN ペアとして設定したインターフェイス、インライン VLAN グループ、およ

び無差別 VLAN グループ）のサマリーが含まれています。この表の内容は、インターフェイス設定を変更すると、変わります。

無差別モード、インライン ペア モード、またはインライン VLAN ペア モードで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせてインターフェイスを設定することはできません。

ヒント　すべてのサービス モジュールにサマリーのタブがあるわけではありません。

ナビゲーション パス

（デバイスビュー）ポリシーセレクタから [インターフェイス（Interface）] を選択します。[サマリー（Summary）] タブをクリックします。

関連項目

- インターフェイスについて （2127 ページ）
- IPS インターフェイス ポリシーについて （2134 ページ）
- 物理インターフェイスの設定 （2139 ページ）
- バイパス モードの設定 （2142 ページ）
- CDP モードの設定 （2143 ページ）
- インライン インターフェイス ペアの設定 （2144 ページ）
- インライン VLAN ペアの設定 （2145 ページ）
- VLAN グループの設定 （2147 ページ）

フィールド リファレンス

表 *516 : [IPS Interface Summary]* タブ

要素	説明
名前	インターフェイスの名前。 この名前は、無差別インターフェイスの FastEthernet または GigabitEthernet です。インラインインターフェイスの場合、この名前はペアに割り当てた名前になります。
Subinterface Number	インライン VLAN ペアまたは VLAN グループのサブインターフェイス番号です。1 ～ 255 のサブインターフェイス番号を指定できます。
Inline Interface Name	インライン インターフェイス ペアの名前。

要素	説明
[モード（Mode）]	インターフェイスのモード：無差別、インライン、無差別 VLAN グループ、またはインライン VLAN グループおよび VLAN ペアが存在するかどうか。インターフェイス モードの詳細については、インターフェイス モードについて （2129 ページ）を参照してください。
VLAN A VLAN B	VLAN ペアの 1 番めの VLAN および 2 番めの VLAN の VLAN ID。1 ～ 4095 の VLAN 番号を指定できます。
VLAN の範囲	VLAN グループに属している VLAN ID の範囲（100 ～ 200 など）。 未割り当てのすべての VLAN に適用するように VLAN グループが設定されている場合、このフィールドは空になります。

物理インターフェイスの設定

IPS インターフェイス ポリシーの [Physical Interfaces] タブには、使用しているセンサー上の既存の物理インターフェイスおよび関連付けられている設定が表示されます。このポリシーの物理インターフェイスは追加または削除できません。代わりに、ポリシー検出を使用して、デバイスからインターフェイスの最新リストを取得する必要があります。したがって、（一部のアプライアンスで使用可能な）インターフェイス カードを追加または削除した場合、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）で説明しているように、デバイスを再検出する必要があります。

トラフィックをモニタするようにセンサーを設定するには、この手順を使用してインターフェイスをイネーブルにする必要があります。**setup** コマンドを使用して（IPS でコマンド ライン インターフェイスを使用して）センサーを初期化したときに、インターフェイスまたはインラインペアを仮想センサーに割り当て、インターフェイスまたはインラインペアをイネーブルにしています。インターフェイス設定を変更する必要がある場合は、[Physical Interfaces] タブで変更できます。インターフェイスを仮想センサーに割り当てるには、[Virtual Sensors] ポリシーを選択し、必要に応じて仮想センサーを追加または編集します。

ヒント　各物理インターフェイスは、VLAN グループ サブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。詳細については、VLAN グループの設定 （2147 ページ）を参照してください。

関連項目

- インターフェイスについて （2127 ページ）
- 仮想センサーの定義 （2157 ページ）
- 仮想センサーのポリシーの編集 （2162 ページ）
- 仮想センサーへのインターフェイスの割り当て （2155 ページ）

- バイパス モードの設定 （2142 ページ）
- CDP モードの設定 （2143 ページ）
- インライン インターフェイス ペアの設定 （2144 ページ）

ステップ 1 （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] を選択し、[物理インターフェイス（Physical Interfaces）] タブをクリックします（必要な場合）。

ステップ 2 設定を変更するインターフェイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。[Modify Physical Interface Map] ダイアログボックスが表示されます。

ステップ 3 必要な設定変更を行い、[OK] をクリックします。よく変更される設定を次に示します。すべてのオプションについては、[Modify Physical Interface Map] ダイアログボックス （2140 ページ）を参照してください。

- [イネーブル（Enabled）] : インターフェイスがイネーブルであるかどうか（[はい（Yes）] または [いいえ（No）]）。インターフェイスを動作させるには、[Yes] を選択します。このオプションの値は、[Physical Interfaces] タブの [Administrative State] カラムに表示されます。
- [デフォルト VLAN（Default VLAN）] : インターフェイスが割り当てられている VLAN。
- [TCP リセットインターフェイスを指定（Specify Interface for TCP Reset）] : インターフェイスについて （2127 ページ）で説明しているように、代替 TCP リセットインターフェイスを割り当てるには、このオプションを選択してから、[インターフェイス名（interface-name）] リストから代替インターフェイスを選択します。

[Modify Physical Interface Map] ダイアログボックス

[Modify Physical Interface Map] ダイアログボックスを使用して、IPS センサーの物理インターフェイスの設定を変更します。手順については、物理インターフェイスの設定 （2139 ページ）を参照してください。

ナビゲーション パス

（デバイスビュー）ポリシーセレクタから [インターフェイス（Interface）] を選択します。[物理インターフェイス（Physical Interfaces）] タブで、インターフェイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。

関連項目

- インターフェイスについて （2127 ページ）
- IPS インターフェイス ポリシーについて （2134 ページ）

フィールド リファレンス

表 *517 : [Modify Physical Interface Map]* ダイアログボックス

要素	説明
名前	物理インターフェイスの名前。
メディア タイプ（Media Type）	物理インターフェイスのメディア タイプ。メディア タイプは、次のとおりです。 • [TX]：銅線メディア。 • [SX]：ファイバ メディア。 • [XL]：ネットワーク アクセラレータ カード。 • [Backplane interface]：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
Description	インターフェイスの説明。
[有効（Enabled）]	インターフェイスがイネーブルであるかどうか（[Yes] または [No]）。 インターフェイスを動作させるには、[はい（Yes）] を選択する必要があります。インターフェイスの仮想センサーにインターフェイスを割り当てる必要もあります。[Virtual Sensors] ポリシーを使用します。
デュプレックス	インターフェイスのデュプレックス設定。デュプレックス設定は、次のとおりです。 • [Auto]：インターフェイスを自動ネゴシエーション デュプレックスに設定します。 • [Full]：インターフェイスを全二重に設定します。 • [Half]：インターフェイスを半二重に設定します。

要素	説明
速度	インターフェイスの速度設定。速度のオプションは、次のとおりです。 • [Auto]：インターフェイスを自動ネゴシエーション速度に設定します。 • [10 MB]：インターフェイスを 10 MB に設定します（TX インターフェイスの場合だけ）。 • [100 MB]：インターフェイスを 100 MB に設定します（TX インターフェイスの場合だけ）。 • [1 GB]：インターフェイスを 1 GB に設定します（ギガビット インターフェイスの場合だけ）。 • [10 GB]：インターフェイスを 10 GB に設定します（10 ギガビット インターフェイスの場合だけ）。
Default VLAN	ネイティブ トラフィックに関連付けられている VLAN ID、または 0（不明な場合や、どの VLAN であるかは関係ない場合）。
Specify Interface for TCP Reset interface-name	代替インターフェイスが無差別モニタリングに使用され、シグニチャの起動によってリセット アクションがトリガーされた場合に、代替インターフェイスで TCP リセットを送信するかどうか。 このオプションを選択した場合は、[interface-name] リストから代替 TCP リセット インターフェイスを選択します。 代替 TCP リセットの詳細については、インターフェイスについて （2127 ページ）を参照してください。

バイパス モードの設定

インラインバイパスは、分析ツールとして、およびフェールオーバー保護メカニズムとして使用できます。通常は、センサーの分析エンジンがパケット分析を実行します。インラインバイパスがアクティブである場合、分析エンジンはバイパスされ、トラフィックは検査されることなく、インライン インターフェイスおよびインライン VLAN ペアを通過できます。インラインバイパスによって、センサープロセスがアップグレードのために一時的に停止した場合や、センサー モニタリング プロセスが失敗した場合でも、パケットは引き続きセンサーを通過できます。オン、オフ、および自動という 3 つのモードがあります。デフォルトでは、バイパス モードは自動に設定されています。

使用するバイパス モードを決定する前に、次のことを考慮してください。

- センサーをバイパス モードにすると、セキュリティ上の影響があります。バイパス モードをオンにすると、トラフィックはセンサーをバイパスし、検査されません。そのため、センサーは悪意のある攻撃を阻止できません。

- インライン バイパス機能は、ソフトウェアで実行されるため、オペレーティング システムが稼働している場合にだけ動作します。センサーの電源がオフになっている場合、またはシャットダウンされている場合、インライン バイパスは動作しません。つまり、トラフィックはセンサーを通過しません。
- センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関更新のサイズによって決まります。バイパス モードをオフにすると、インラインセンサーはアップデートの適用中にトラフィックの送信を停止します。

バイパス モードの設定を変更するには、次の手順を実行します。

ステップ 1 （デバイスビュー）ポリシーセレクタから [インターフェイス（Interface）] ポリシーを選択します。

ステップ 2 ポリシーの一番下にある [バイパスモード（Bypass Mode）] フィールドで、目的のオプションを選択します。

- [オフ（インライントラフィックを常に検査する）（Off (Always inspect inline traffic)）]：バイパスモードを無効にします。

トラフィックは、検査のために、センサーを介して送信されます。センサーのモニタリング プロセスがダウンすると、トラフィックは通過しなくなります。これは、インライン トラフィックが常に検査されることを意味します。

- [オン（インライントラフィックを検査しない）（On (Never inspect inline traffic)）]：トラフィックは、分析エンジンをバイパスし、検査されません。これは、インライン トラフィックが常に検査されないことを意味します。
- [自動（分析エンジンが停止している場合は検査をバイパスする）（Auto (Bypass inspection when analysis engine is stopped)）]：センサーのモニタリングプロセスがダウンしている場合を除き、センサー経由のトラフィックフローは検査されます。これがデフォルトです。

センサーのモニタリング プロセスがダウンすると、センサーが再び動作するまで、トラフィックはセンサーをバイパスします。センサーは、動作を再開すると、トラフィックを検査します。Auto モードは、センサーのアップグレード時に役立ちます。センサーのアップグレード中でもトラフィック フローが確保されるからです。また、Auto モードによって、モニタリング プロセスが失敗した場合でも、トラフィックは引き続きセンサーを通過します。

CDP モードの設定

Cisco Discovery Protocol（CDP）パケットの転送をイネーブルまたはディセーブルするように、IPS センサーを設定できます。CDP 設定は、デバイス上のすべてのインターフェイスにグローバルに適用されます。ただし、効果があるのはインライン インターフェイス（インライン インターフェイスとインライン VLAN ペア）だけです。

Cisco Discovery Protocol は、メディアおよびプロトコルに依存しないデバイス検出プロトコルであり、すべてのシスコ製装置（ルータ、アクセス サーバ、ブリッジ、スイッチなど）上で動作します。CDP を使用することにより、デバイスはその存在を他のデバイスにアドバタイズし、同じ LAN 上または WAN のリモート サイト上の他のデバイスに関する情報を受信できます。CDP は、SNAP をサポートするすべてのメディア（LAN、フレーム リレー、ATM メディアなど）で稼働します。

ヒント　CDP モード設定は、一部の IPS アプライアンスおよびサービス モジュールでは使用できません。[CDP Mode] フィールドがインターフェイス ポリシーに表示されない場合、それらの設定は、設定中のデバイスには適用されません。

デバイスで CDP モード設定を変更するには、次の手順を実行します。

ステップ 1　（デバイスビュー）ポリシーセレクタから [インターフェイス（Interface）] ポリシーを選択します。

ステップ 2　ポリシーの一番下にある [CDPモード（CDP Mode）] フィールドで、必要なオプションを選択します。

- [CDPパケットを転送（Forward CDP packets）]：CDP パケットがセンサーを通過できるようにします。
- [CDPパケットをドロップ（Drop CDP packets）]：センサーにすべての CDP パケットをドロップさせ、センサーを通過できないようにします。これがデフォルト設定です。

インライン インターフェイス ペアの設定

センサーでインラインモニタリングを実行できる場合は、センサーでインターフェイスのペアを設定できます。インライン ペアの詳細については、インライン VLAN ペア モード （2130 ページ）を参照してください。

ヒント　ルータおよび ASA デバイスの IPS モジュールでは、モニタリング用のインライン ペアは必要ありません。必要となるのは、物理インターフェイスを仮想センサーに追加することだけです。

関連項目

- インターフェイスについて （2127 ページ）
- バイパス モードの設定 （2142 ページ）
- CDP モードの設定 （2143 ページ）
- 物理インターフェイスの設定 （2139 ページ）
- VLAN グループの設定 （2147 ページ）

- 仮想センサーの定義 （2157 ページ）
- 仮想センサーのポリシーの編集 （2162 ページ）
- 仮想センサーへのインターフェイスの割り当て （2155 ページ）

ステップ 1 （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] を選択し、次に [インラインペア（Inline Pairs）] タブをクリックします。

ステップ 2 次のいずれかを実行します。

- ペアを追加するには、[行の追加（Add Row）] ボタンをクリックします。[Add Interface Pair] ダイアログボックスが開きます。
- ペアを編集するには、ペアを選択して [行の編集（Edit Row）] ボタンをクリックします。[Edit Interface Pair] ダイアログボックスが開きます。

ヒント ペアを選択し、[行の削除（Delete Row）] ボタンをクリックして削除することもできます。インライン VLAN グループが存在する場合は、インライン ペアを削除できません。最初にインライン VLAN グループを [VLAN Groups] タブから削除し、次にインライン ペアを削除します。

ステップ 3 [Add or Edit Inline Pairs] ダイアログボックスで、次のオプションを設定します。

- [インラインインターフェイス名（Inline Interface Name）]：インラインペアに付ける名前。この名前は、32 文字以下とする必要があります。使用できる文字は、英数字とアンダースコアです。この名前は、ペアを作成したあとには編集できません。
- [インターフェイス1および2（Interface 1 and 2）]：ペアの形成に使用する 2 つの物理インターフェイスを選択します。このリストには、[Physical Interfaces] タブで定義されたインターフェイスで、かつインライン ペア、VLAN ペア、または VLAN グループの一部になっていないインターフェイスだけが表示されます。
- [説明（Description）]：ペアの説明（任意）。

ステップ 4 [OK] をクリックして変更を保存します。

インライン VLAN ペアの設定

IPS インターフェイス ポリシーの [VLAN Pairs] タブを使用して、物理インターフェイス用の VLAN ペアを設定します。このサマリー テーブルには、各物理インターフェイスの既存の VLAN ペアが表示されます。単一の物理インターフェイスに複数の VLAN ペアを作成できます。インライン VLAN ペア モードの詳細については、インライン VLAN ペア モード （2130 ページ）を参照してください。

ヒント

- インターフェイスが、すでにインライン インターフェイス ペアの一部である場合は、そのインターフェイスの VLAN ペアは作成できません。インライン インターフェイス ペアの VLAN グループを作成します。
- 無差別モードで動作し、仮想センサーに割り当てられているインターフェイス用のインライン VLAN ペアを作成するには、最初にそのインターフェイスを仮想センサーから削除し（[Virtual Sensors] ポリシーを使用）、次にインライン VLAN ペアを作成する必要があります。
- インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。
- 使用しているセンサーが、インライン VLAN ペアをサポートしていない場合、[VLAN Pairs] ペインは表示されません。ルータおよび ASA デバイスの IPS モジュールは、インライン VLAN ペアをサポートしていません。
- インライン VLAN ペアを使用する場合は、VLAN をホストしている、接続されているスイッチで単方向リンク検出（UDLD）を設定する必要があります。UDLD を使用すると、スイッチがスパニングツリー転送ループおよび単一方向リンクを回避するのに役立ちます。詳細については、https://www.cisco.com/c/en/us/td/docs/security/ips/7-0/configuration/guide/idm/idmguide7/idm_interfaces.html#wp1169508を参照してください。

関連項目

- インターフェイスについて （2127 ページ）
- バイパス モードの設定 （2142 ページ）
- CDP モードの設定 （2143 ページ）
- 物理インターフェイスの設定 （2139 ページ）
- VLAN グループの設定 （2147 ページ）

ステップ 1 （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] を選択し、次に [VLANペア（VLAN Pairs）] タブをクリックします。

ステップ 2 次のいずれかを実行します。

- ペアを追加するには、[行の追加（Add Row）] ボタンをクリックします。[Add VLAN Pair] ダイアログボックスが開きます。
- ペアを編集するには、ペアを選択して [行の編集（Edit Row）] ボタンをクリックします。[Edit VLAN Pair] ダイアログボックスが開きます。

ヒント ペアを選択し、[行の削除（Delete Row）] ボタンをクリックして削除することもできます。インライン VLAN ペアは、仮想センサーに割り当てられている場合は削除できません。[Virtual Sensors] ポリシーを使用して最初に仮想センサーへの割り当てを削除してから、インライン VLAN ペアを削除します。

ステップ 3 [Add VLAN Pairs]/[Edit VLAN Pairs] ダイアログボックスで、次のオプションを設定します。

- [物理インターフェイス（Physical Interfaces）]：VLAN ペアを作成する物理インターフェイスを選択します。このリストには、[Physical Interfaces] タブで定義され、かつインライン インターフェイス ペアまたは VLAN グループの一部となっていないインターフェイスだけが含まれています。ただし、単一のインターフェイス上で複数の VLAN ペアを作成できます。
- [サブインターフェイス番号（Subinterface Number）]：サブインターフェイスとして割り当てる番号を入力します。この番号は、インターフェイスで一意である必要があります。つまり、選択した物理インターフェイス上の別の VLAN ペアにまだ割り当てられていない必要があります。1 ～ 255 のサブインターフェイス番号を指定できます。
- [説明（Description）]：ペアの説明（任意）。
- [VLAN A、B（VLAN A, B）]：ペアとして結合する 2 つの VLAN の番号。VLAN 番号は、1 ～ 4095 の値です。異なる番号を入力する必要があります。また、選択した物理インターフェイス上の別の VLAN ペアの番号と同じ番号は使用できません。

ステップ 4 [OK] をクリックして変更を保存します。

VLAN グループの設定

IPS インターフェイス ポリシーの [VLAN Groups] タブを使用して、物理インターフェイスおよびインライン インターフェイス ペア（論理インターフェイス）の VLAN グループを設定します。サマリーテーブルには、既存の VLAN グループが表示されます。単一の物理インターフェイスまたはインライン インターフェイス ペア上に複数の VLAN グループを作成できます。VLAN グループ モードの詳細については、VLAN グループ モード （2131 ページ）を参照してください。

VLAN グループは、インターフェイスに存在する VLAN ID のグループで構成されています。各 VLAN グループは、少なくとも 1 つの VLAN ID で構成されています。インターフェイス（論理または物理）ごとに最大 255 の VLAN グループを設定できます。各グループには、任意の数の VLAN ID を含めることができます。

VLAN ID を VLAN グループに割り当てたあとに、その VLAN グループを仮想センサーに割り当てて、動作できるようにする必要があります。単一グループは、1 つの仮想センサーだけに割り当てることができます。[Virtual Sensors] ポリシーを使用して、割り当てを行います。

（注） VLAN グループは、IPS 6.0 以降でだけサポートされています。すべての IPS アプライアンスまたはサービス モジュールで VLAN グループがサポートされているわけではありません。[VLAN Groups] タブが [Interfaces] ポリシーに表示されない場合、設定しているそのデバイスではこの機能がサポートされていません。

関連項目

- インターフェイスについて （2127 ページ）
- バイパス モードの設定 （2142 ページ）
- CDP モードの設定 （2143 ページ）
- 物理インターフェイスの設定 （2139 ページ）
- 仮想センサーの定義 （2157 ページ）
- 仮想センサーのポリシーの編集 （2162 ページ）
- 仮想センサーへのインターフェイスの割り当て （2155 ページ）

ステップ 1 （デバイスビュー）ポリシーセレクタから[インターフェイス（Interfaces）]を選択し、次に[VLANグループ（VLAN Groups）]タブをクリックします。

この表には、グループが定義されているインターフェイス、サブインターフェイス番号、説明（ある場合）、グループに割り当てられている VLAN を含む、既存の VLAN グループが示されます。VLAN のセルが空白の場合、そのグループはインターフェイス上のすべての未割り当て VLAN 用に定義されています。

ステップ 2 次のいずれかを実行します。

- ペアを追加するには、[行の追加（Add Row）]ボタンをクリックします。[Add VLAN Group] ダイアログボックスが開きます。
- ペアを編集するには、ペアを選択して [行の編集（Edit Row）] ボタンをクリックします。[Edit VLAN Group] ダイアログボックスが開きます。

ヒント グループを選択し、[行の削除（Delete Row）]ボタンをクリックしてグループを削除することもできます。VLAN グループは、仮想センサーに割り当てられている場合は削除できません。[Virtual Sensors] ポリシーを使用して最初に仮想センサーへの割り当てを削除してから、VLAN グループを削除します。

ステップ 3 [Add VLAN Group] または [Edit VLAN Group] ダイアログボックスで、次のオプションを設定します。

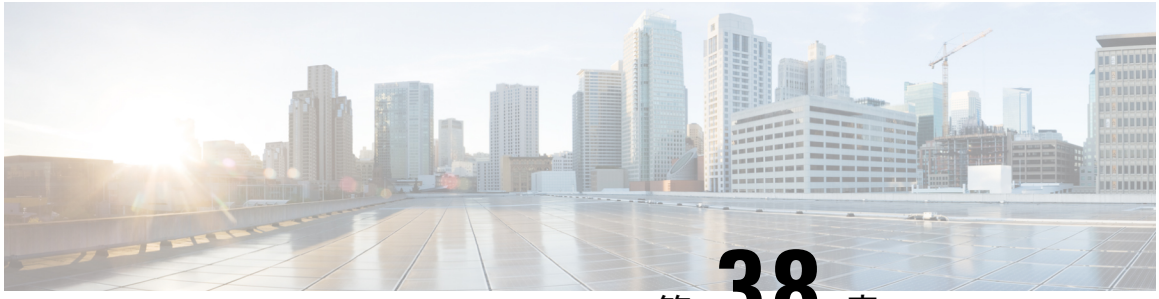
- [物理および論理インターフェイス（Physical and Logical Interfaces）]：この VLAN グループを作成している物理インターフェイスまたはインラインインターフェイスペアを選択します。このリストには、インライン VLAN ペアがまだ定義されておらず、ペアになっていない物理インターフェイス（[Physical Interfaces] タブで定義）や、[Inline Pairs] タブで定義されているインライン インターフェイス ペアだけが表示されます。単一のインターフェイス上で複数の VLAN グループを作成できます。次の点を考慮してください。
  - 物理インターフェイスを選択した場合は、無差別 VLAN グループを作成します。
  - 論理インターフェイスを選択した場合は、インライン VLAN グループを作成します。
- [サブインターフェイス番号（Subinterface Number）]：サブインターフェイスとして割り当てる番号を入力します。この番号は、インターフェイスで一意である必要があります。つまり、選択したインター

フェイス上の別の VLAN グループにまだ割り当てられていない必要があります。1 ～ 255 のサブインターフェイス番号を指定できます。

- [説明（Description）]：グループの説明（任意）。
- [VLAN assignment]：次のいずれかのオプションを選択します。
  - [すべての割り当てられていない VLAN ID（All Unassigned VLAN IDs）]：このグループには、他の VLAN グループに割り当てられていないすべての VLAN が含まれます。これはデフォルトのオプションです。
  - [無料VLAN IDの範囲（Range of free VLAN IDs）]：このグループには、特定の VLAN が含まれます。[範囲（Range）] ボックスに、1 つの VLAN ID または範囲の任意の組み合わせを入力し（ID の先頭と末尾をハイフンで区切る）、複数のエントリをカンマで区切ります。たとえば、10,12-25,33-49 のように入力します。VLAN 番号は、1 ～ 4095 の値です。

この VLAN ID には、選択したインターフェイスの別の VLAN グループの VLAN ID は使用できません。また、VLAN は、接続されているスイッチで設定する必要があります。そうしないと、検査するトラフィックが存在しないことになります。

ステップ 4 [OK] をクリックして変更を保存します。



第 38 章

仮想センサーの設定

すべての IPS デバイスおよびサービス モジュールに、vs0 という名前の基本仮想センサーがあります。IPS アプライアンスまたはサービス モジュールの設定時に、基本の vs0 センサーを設定してインターフェイスを割り当てる必要があります。この割り当てによって、検査するインターフェイスがデバイスに示されます。また、仮想センターには指定できるその他の設定があります。

基本の vs0 仮想センサー以外に、数多くの IPS アプライアンスおよびサービス モジュールで、ユーザ定義の仮想センサーを作成できます。これらの仮想センサーを使用すると、単一の物理センサーが複数のセンサーのように機能できるように、トラフィックごとに別々のポリシーを作成できます。仮想センサーは、シグニチャ エンジンおよびイベント アクション フィルタを適用するための検知インターフェイスと設定ポリシーの論理グループです。

この章は次のトピックで構成されています。

- 仮想センサーについて （2151 ページ）
- 仮想センサーの定義 （2157 ページ）
- 仮想センサーのポリシーの編集 （2162 ページ）
- 仮想センサーの削除 （2162 ページ）

仮想センサーについて

センサーは1つまたは多数のモニタ対象データ ストリームからのデータ入力を受信できます。これらのモニタ対象データ ストリームは、物理インターフェイス ポートまたは仮想インターフェイス ポートのどちらでも構いません。たとえば、単一のセンサーでファイアウォールの前からのトラフィック、ファイアウォールの後ろからのトラフィック、またはファイアウォールの前後からのトラフィックを同時にモニタできます。単一のセンサーで1つ以上のデータ ストリームをモニタできます。この場合、単一のセンサー ポリシーまたは設定がすべてのモニタ対象データストリームに適用されます。

仮想センサーでは、特定のトラフィック フィードに適用するための、別々のポリシーを作成できます。たとえば、データセンターのポリシーを作成し、キャンパス ネットワークに別のまったく異なるポリシーを作成して、両方のポリシーを同じハードウェア デバイスで実行する場合は、別々の仮想センサーを設定してこれらのポリシーを実装できます。

仮想センサーに対して次のポリシーおよび設定を別々に設定します。

- シグニチャおよびシグニチャ設定（[IPS] のポリシー > [Signatures] フォルダ）
- イベント アクション ポリシー（[IPS] のポリシー > [Event Actions] フォルダ）
- 異常検出ポリシー（[IPS] > [Anomaly Detection] ポリシー）および異常検出モード（[Virtual Sensors] ポリシー）
- 仮想センサーでモニタする無差別インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、インライン VLAN グループ、または無差別 VLAN グループ

（注） パケットが複数の仮想センサーで処理されることはありません。つまり、同じ物理または論理インターフェイスを複数のセンサーに割り当てることはできません。どの仮想センサーにも割り当てられていないインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループからのパケットは、[インターフェイス（Interfaces）] ポリシーで定義したインラインバイパス設定に従って破棄されます。

- インライン TCP セッション トラッキングおよびノーマライザ モード（[Virtual Sensors] ポリシー）

（注） シグネチャ、イベントアクション、または異常検出のために IPS デバイスでポリシーインスタンスを作成し、そのデバイスのどの仮想センサーにも割り当てない場合（つまり、そのポリシーインスタンスを使用しない場合）、そのポリシーインスタンスは展開中に Cisco Security Manager によって削除されます。

他のポリシーおよび設定はすべて、仮想センサーをホストする親デバイス上で設定します。たとえば、グローバル相関を使用する場合、親デバイスでグローバル相関を設定して、仮想センサーでその設定を共有します。

1 台のアプライアンスに最大 4 つの仮想センサーを設定できますが、ユーザ定義の仮想センサーは 3 つしか追加できません。最初の仮想センサーである vs0 は基本センサーであり、これは削除できません。Security Manager では、仮想センサーは次のように表示されます。

- デバイス ビューのデバイス セレクタには親デバイスが含まれており、これが基本仮想センサー vs0 を兼ねています。このデバイスを選択してすべてのデバイスレベル ポリシーを設定し、[Virtual Sensors] ポリシーで仮想センサーを作成します。
- ユーザ定義の仮想センサーもまた、デバイス ビューのデバイス セレクタに表示されます。リアルデバイスの表示名が、仮想センサー名の先頭に追加されます。その結果、通常は仮想センサーが存在する親（リアル）デバイスの横に仮想センサーが表示されます。たとえば、「bob」という名前のホスト（リアルデバイス）では、「vs1」という名前の仮想センサーは「bob_vs1」としてデバイスリストに表示されます。

仮想センサーのシグニチャ、異常検出、およびイベントアクションポリシーを設定するには、デバイスセレクタでその仮想センサーを選択する必要があります。親デバイスを選択してもこれらのポリシーは設定できません。親デバイスのポリシーは、vs0 基本センサー用です。

ここでは、仮想センサーについて詳しく説明します。

- 仮想化の利点および制約事項 （2153 ページ）
- インライン TCP セッション トラッキング モード （2154 ページ）
- ノーマライザ モードについて （2155 ページ）
- 仮想センサーへのインターフェイスの割り当て （2155 ページ）
- デバイスに対する仮想センサーの識別 （2156 ページ）
- 仮想センサーの定義 （2157 ページ）
- 仮想センサーのポリシーの編集 （2162 ページ）
- 仮想センサーの削除 （2162 ページ）

仮想化の利点および制約事項

仮想センサーを使用することの利点は、1 台のアプライアンスで複数の仮想センサーを操作する一方で、シグニチャの動作およびトラフィック フィードに関して個々の仮想センサーをそれぞれ異なるように設定できることです。たとえば、データセンターのポリシーを作成し、キャンパス ネットワークに別のまったく異なるポリシーを作成して、両方のポリシーを同じハードウェア デバイスで実行する場合は、別々の仮想センサーを設定してこれらのポリシーを実装できます。

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。
- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。
  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パススイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。

- 固定ストアが制限されます。
- すべての IPS センサーで複数の仮想センサーがサポートされているわけではありません。[Virtual Sensors] ポリシーはすべての IPS アプライアンスおよびサービス モジュールで表示されますが、これは、インターフェイスを基本の vs0 センサーに割り当てるために、このポリシーを使用する必要があるためです。ポリシーの [Add] ボタンがデバイスに対してディセーブルであり、ユーザ定義の仮想センサーを設定していない場合、そのデバイスでは仮想化がサポートされません。仮想化がサポートされていないデバイスの例として、Cisco IPS 4215、NM-CIDS、AIM-IPS、NME-IPS、および AIP-SSC を挙げることができます。IDSM2 では仮想化はサポートされていますが、VLAN グループとインラインインターフェイス ペアはサポートされません。
- IPS 6.0+ ソフトウェアを使用する必要があります。古いソフトウェア バージョンでは仮想化がサポートされていません。
- Cisco IOS IPS デバイスでは仮想化がサポートされていません。[IPS] > [インターフェイス ルール（Interface Rules）] ポリシーを使用して、IPS でモニターする必要があるインターフェイスを指定します。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

関連項目

- 仮想センサーについて （2151 ページ）
- 仮想センサーの定義 （2157 ページ）

インライン TCP セッション トラッキング モード

インラインでのパケット変更を選択している場合、ノーマライザエンジンでは、ストリームからのパケットを2回認識すると、ストリームの状態を適切に追跡できません。このような場合は、ストリームが頻繁にドロップされます。この状況は、ストリームが、IPS によってモニタされている複数の VLAN またはインターフェイスを介してルーティングされている場合に、最もよく発生します。また、いずれかの方向のトラフィックがそれぞれ異なる VLAN またはインターフェイスから受信された場合に、ストリームを適切に追跡するために非対称トラフィックをマージできるようにする必要があり、これにより、状況がより複雑化します。

この状況を処理するために、ストリームが別々のインターフェイスまたはVLAN（またはVLAN ペアのサブインターフェイス）で受信された場合には、これらを一意のストリームとして認識するように、モードを設定できます。

次のインライン TCP セッション トラッキング モードが適用されます。

- [インターフェイスおよびVLAN（Interface and VLAN）]：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッションキー（AaBb）を持つすべてのパケットは、同じセッションに属します。同じキーを持ち、VLANが異なるパケットは、別々に追跡されます。
- [VLANのみ（VLAN Only）]：同じ VLAN（またはインライン VLAN ペア）内で同じセッションキー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属します。同じキーを持ち、VLANが異なるパケットは、別々に追跡されます。
- [仮想センサー（Virtual Sensor）]：仮想センサー内で同じセッションキー（AaBb）を持つすべてのパケットは、同じセッションに属します。これがデフォルトであり、ほとんどの場合、最良のオプションです。

仮想センサーの定義 （2157ページ）で示すように、インライン TCP セッション トラッキング モードは、仮想センサーのプロパティとして設定します。

ノーマライザ モードについて

ノーマライザ モードは、センサーがインライン モードで動作している場合にだけ適用されます。デフォルトは [Strict Evasion Protection] であり、これは、TCP ステートとシーケンスのトラッキングが完全に強制されることを意味します。ノーマライザによって、重複パケット、変更されたパケット、順序が正しくないパケットなどの検査が強制されます。このことは、攻撃者が IPS を回避することを阻止するのに役立ちます。

非対称モードでは、ノーマライザのチェックの大部分がディセーブルになります。非対称モードはストリーム全体を検査できない場合にだけ使用してください。この状況では、攻撃者が IPS を回避できるためです。

仮想センサーの定義 （2157ページ）で示すように、ノーマライザ モードは、仮想センサーのプロパティとして設定します。

仮想センサーへのインターフェイスの割り当て

IPS センサーは、仮想センサーに割り当てられたインターフェイス、インターフェイス ペア、または VLAN ペアを通過するトラフィックをモニタします。

次のタイプの 1 つ以上のインターフェイスを仮想センサーに割り当てることができます。

- 無差別インターフェイス：VLAN グループがなく、インライン インターフェイス ペアに含まれない物理インターフェイス。
- インライン インターフェイス ペア：2 つの物理インターフェイスからなる論理インターフェイス。
- インライン VLAN ペア：2 つの VLAN からなる論理インターフェイス。
- 無差別 VLAN グループ：物理インターフェイス上のサブインターフェイスに割り当てられている VLAN グループ。

物理インターフェイスは、インライン インターフェイスまたは VLAN ペアにはまだ使用できません。同じ無差別インターフェイスに多数の無差別VLAN グループを設定できますが、VLAN を重複して割り当てることはできません。VLAN グループを無差別インターフェイスに割り当てると、このインターフェイスは単なる無差別インターフェイスではなくなり、無差別VLAN グループにだけ使用できるようになります。

- インライン VLAN グループ：インライン インターフェイス ペアのサブインターフェイスに割り当てられている VLAN グループ。

同じインライン インターフェイス ペアに多数のインライン VLAN グループを設定できますが、VLAN を重複して割り当てることはできません。VLAN グループをインライン インターフェイス ペアに割り当てると、このインターフェイス ペアは単なるインライン インターフェイス ペアではなくなり、インライン VLAN グループにだけ使用できるようになります。

VLAN グループをインライン VLAN ペアに割り当てることはできません。

インターフェイスを仮想センサーに割り当てる前に、これらを設定する必要があります。これらすべてのタイプのインターフェイスの設定については、インターフェイスの設定 （2133 ページ）を参照してください。インターフェイスを仮想センサーに割り当てる方法の詳細については、仮想センサーの定義 （2157 ページ）を参照してください。

デバイスに対する仮想センサーの識別

IPS アプライアンスまたはサービス モジュールでユーザ定義の仮想センサーを設定すると、その仮想センサーはデバイス ビューのデバイス セレクタに表示されます。

通常、仮想センサーの表示名は、device-name_virtual-sensor-name の形式になります。ここで、device-name は親デバイスの名前、virtual-sensor-name は仮想センサーの名前です。たとえば、デバイス 10.100.10.10 上の仮想センサー vs1 は 10.100.10.10_vs1 になります。

このため、通常、デバイス セレクタ内で、デバイスの仮想センサーは親デバイスのすぐあとに表示されます。ただし、仮想センサーの表示名は、デバイスのプロパティを編集して変更できます。デフォルト名を変更した場合、デバイス セレクタ内で、仮想センサーが親デバイスの近くに表示されなくなる可能性があります。

次の方法を使用すると、デバイスに定義されている仮想センサーを識別したり、仮想センサーの親デバイスを識別したりできます。

- IPS デバイスに定義されている仮想センサーのリストを表示するには、そのデバイスの [仮想センサー（Virtual Sensors）] ポリシーを選択します。テーブルに、基本の vs0 センサーを含むすべての仮想センサーが表示されます。vs0 センサーはデバイス セレクタに単独では表示されないことに注意してください。このセンサーは親デバイス自体によって示されます。

仮想センサーの表示名を根本的に変更しないかぎり、仮想センサー名と親デバイスの表示名は、デバイス セレクタ内で仮想センサーを見つけるのに役立ちます。

- 仮想センサーのホストである IPS デバイスを判断するには、デバイス セレクタで仮想センサーを右クリックして [デバイスのプロパティ（Device Properties）] を選択します。[General]

タブにある表示専用の [Hostname] フィールドに、ホスト デバイスの表示名と、デバイスに定義されている仮想センサー名が表示されます。

仮想センサーの定義

[Virtual Sensors] ポリシーを使用して、Cisco IPS デバイスに仮想センサーを設定します。IPS デバイスで複数の仮想センサーがサポートされていない場合でも、このポリシーを使用してインターフェイスを基本センサー vs0 に割り当て、その仮想センサーに関連付けられているプロパティを設定する必要があります。

ヒント　Cisco IOS IPS デバイスの場合、**[IPS] > [インターフェイスルール（Interface Rules）]** ポリシーで IPS が検査するインターフェイスを設定します。IOS IPS デバイスでは仮想センサーは設定できません。

はじめる前に

インライン インターフェイス ペア、インライン VLAN ペア、無差別 VLAN グループ、およびインライン VLAN グループなどのインターフェイスをセンサーに設定します。インターフェイスは、仮想センサーに割り当てる前に設定する必要があります。インターフェイス、インターフェイスのモード、およびこれらの設定方法については、IPS デバイスインターフェイスの管理 （2127 ページ）を参照してください。

関連項目

- インターフェイスについて （2127 ページ）
- インターフェイス モードについて （2129 ページ）
- 仮想化の利点および制約事項 （2153 ページ）
- インライン TCP セッション トラッキング モード （2154 ページ）
- インライン TCP セッション トラッキング モード （2154 ページ）
- ノーマライザ モードについて （2155 ページ）
- 仮想センサーへのインターフェイスの割り当て （2155 ページ）
- デバイスに対する仮想センサーの識別 （2156 ページ）
- 仮想センサーのポリシーの編集 （2162 ページ）

ステップ 1　（デバイス ビューだけ）ポリシーセレクタから [仮想センサー（Virtual Sensors）] を選択して、[仮想センサー（Virtual Sensors）] ポリシーを開きます。

削除できない基本の vs0 センサーを含むすべての既存仮想センサーがポリシーに一覧表示されます。各センサーの情報には、センサーに割り当てられているインターフェイス、異常検出モード、インライン TCP

トラッキング モード、ノーマライザ モードおよび説明が表示されます（ある場合）。[Assignments] セルが空白の場合、その仮想センサーにはインターフェイスが割り当てられていません。このことは、仮想センサーでトラフィックを分析できないことを意味します。

ステップ 2 次のいずれかを実行します。

- 仮想センサーを追加するには、[行の追加（Add Row）] ボタンをクリックします。[Add Virtual Sensor] ダイアログボックスが開きます。

最大で 3 つのセンサーを追加できます。デバイスでは、基本の vs0 センサーを含めて 4 つの仮想センサーがサポートされます。[Add Row] ボタンがディセーブルになっている場合は、センサーを最大数まで設定してあるか、またはデバイスで複数の仮想センサーがサポートされていないかのいずれかです。

- 仮想センサーを編集するには、仮想センサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。[Edit Virtual Sensor] ダイアログボックスが開きます。

ヒント また、仮想センサーを選択して [行の削除（Delete Row）] ボタンをクリックすると、その仮想センサーを削除できます。基本の vs0 センサーは削除できません。仮想センサーを削除する方法の詳細については、仮想センサーの削除 （2162 ページ）を参照してください。

ステップ 3 [Add Virtual Sensor]/[Edit Virtual Sensor] ダイアログボックスで、少なくとも次のオプションを設定します。その他のオプションについては、たいていの場合、デフォルトが適切です。使用可能なすべてのオプションの詳細については、仮想センサー ダイアログボックス （2159 ページ）を参照してください。

- [Virtual Sensor Name]：仮想センサーの名前。仮想センサー名には、最大 64 文字を使用できますが、スペースは使用できません。
- [Interface Assignments]（[Available]、[Assigned] リスト）：この仮想センターで使用する無差別インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、無差別 VLAN グループ、またはインライン VLAN グループ。使用可能なインターフェイスのリストに表示されるのは、インターフェイス ポリシーに設定されているインターフェイスと、まだ別の仮想センサーに割り当てられていないインターフェイスだけです。
  - インターフェイスを割り当てるには、使用可能リストでインターフェイスを選択し、[>>] をクリックします。
  - 割り当てを解除するには、割り当て済みリストでインターフェイスを選択し、[<<] をクリックします。インターフェイスを別の仮想センサーに割り当てるには、事前に割り当てを解除する必要があります。

ヒント：特定のインターフェイスの内容（たとえば、モードや割り当てられている VLAN など）がわからない場合は、ダイアログボックスを閉じて [インターフェイス（Interfaces）] ポリシーに移動し、さまざまなタブを確認します。

ステップ 4 [OK] をクリックして変更を保存し、[仮想センサー（Virtual Sensors）] ポリシーに追加します。

ステップ 5 [保存（Save）] をクリックして、[仮想センサー（Virtual Sensors）] ポリシーを保存します。

ステップ 6 新しい仮想センサーを作成した場合、新しい仮想センサーがデバイス ビューのデバイス セレクタに表示されるように、変更内容をデータベースに送信する必要があります。

- Workflow 以外のモード：[ファイル（File）] > [送信（Submit）] を選択します。
- Workflow モード：[アクティビティ（Activities）] > [アクティビティの承認（Approve Activity）] を選択するか、アクティビティ承認者で操作している場合は [アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）] を選択します。アクティビティは、仮想センサーがデバイス セレクタに表示される前に承認されている必要があります。

（注） デバイスセレクタでは、リアルデバイスの表示名が、仮想センサー名の先頭に追加されます。その結果、通常は仮想センサーが存在する親（リアル）デバイスの横に仮想センサーが表示されます。たとえば、「bob」という名前のホスト（リアルデバイス）では、「vs1」という名前の仮想センサーは「bob_vs1」としてデバイスリストに表示されます。

ステップ 7 仮想センサーに関連付けるポリシーを設定するには、デバイス ビューのデバイス セレクタでそのポリシーを選択します。これで、関連付けるポリシーを設定できます。次のトピックを参照してください。

- IPS シグニチャの定義 （2165 ページ）
- イベント アクション ルールの設定 （2211 ページ）
- 異常検出シグニチャの設定 （2251 ページ）

仮想センサー ダイアログボックス

[Add Virtual Sensor]/[Edit Virtual Sensor] ダイアログボックスを使用して、仮想センサーのプロパティを設定します。

ナビゲーション パス

（デバイス ビューだけ）ポリシーセレクタから [仮想センサー（Virtual Sensors）] を選択します。[行の追加（Add Row）] ボタンをクリックするか、既存の仮想センサーを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- 仮想センサーの定義 （2157 ページ）
- 仮想化の利点および制約事項 （2153 ページ）
- 仮想センサーへのインターフェイスの割り当て （2155 ページ）
- IPS デバイスインターフェイスの管理 （2127 ページ）
- インターフェイスについて （2127 ページ）
- インターフェイス モードについて （2129 ページ）

フィールド リファレンス

表 *518 : [Add Virtual Sensor]/[Edit Virtual Sensor]* ダイアログボックス

要素	説明
Virtual Sensor Name	仮想センサーの名前。仮想センサー名には、最大 64 文字を使用できますが、スペースは使用できません。デフォルトの仮想センサーの名前は **vs0** です。 この名前は、仮想センサーを作成したあとには変更できません。仮想センサー名を変更するには、センサーを削除してから、目的の名前で新しいセンサーを作成します。すでにセンサーのローカル ポリシー（つまり、シグニチャ、イベント アクション、および異常検出ポリシー）を設定してある場合は、最初にポリシーを共有ポリシーとして保存し、センサーを削除して、新しいセンサーを作成してから、共有ポリシーを新しい仮想センサーに割り当てます。ローカル ポリシーから共有ポリシーを作成する方法の詳細については、ローカル ポリシーの共有 （262 ページ）を参照してください。
Interface Assignments （[Available]、[Assigned]）	この仮想センターで使用する無差別インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、無差別 VLAN グループ、またはインライン VLAN グループ。使用可能なインターフェイスのリストに表示されるのは、インターフェイス ポリシーに設定されているインターフェイスと、まだ別の仮想センサーに割り当てられていないインターフェイスだけです。 • インターフェイスを割り当てるには、使用可能リストでインターフェイスを選択し、[>>] をクリックします。 • 割り当てを解除するには、割り当て済みリストでインターフェイスを選択し、[<<] をクリックします。インターフェイスを別の仮想センサーに割り当てるには、事前に割り当てを解除する必要があります。 **ヒント** 特定のインターフェイスの内容（たとえば、そのモードや割り当てられている VLAN など）がわからない場合は、ダイアログボックスを閉じて [Interfaces] ポリシーに移動し、それぞれのタブを確認します。
Anomaly Detection Mode	この仮想センサーに対する異常検出ポリシーの動作モード：[Detect]、[Inactive]、[Learn]。デフォルトの通常の動作モードは [Detect] です。ただし、非対称ノーマライザ モードを使用している場合は、異常検出モードを非アクティブに設定する必要がある場合があります。これらのモードの詳細については、異常検出モード （2249 ページ）を参照してください。

要素	説明
インライン TCP セッション トラッキング モード	同じストリームが複数回センサーを通過した場合に、同じストリームに対するビューを複数に分けるために使用されるモード。デフォルト モードは[Virtual Sensor] です。詳細については、インライン TCP セッション トラッキング モード （2154 ページ）を参照してください。次のいずれかを選択します。 • [Interface and VLAN]：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。 • [VLAN Only]：同じ VLAN（またはインライン VLAN ペア）内で同じセッション キー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。 • [Virtual Sensor]：仮想センサー内で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。
Normalizer Mode	トラフィック検査に必要なノーマライザ モードのタイプ。詳細については、ノーマライザ モードについて （2155 ページ）を参照してください。 • [Strict Evasion Protection]：（デフォルト）何らかの理由でパケットが失われた場合、失われたパケット以降のすべてのパケットが処理されなくなります。[Strict Evasion Protection] を指定すると、TCP ステートとシーケンスのトラッキングの完全な施行が提供されます。 パケットの順序が正しくないか、またはパケットが失われていると、ノーマライザ エンジンのシグニチャ 1300 または 1330 が起動する場合があります。この処理によって状況の修正が試行されますが、結果として接続が拒否されることがあります。 • [Asymmetric Mode Protection]：双方向トラフィック フローのいずれかの方向だけをモニタできます。[Asymmetric Mode Protection] を指定すると、TCP レイヤでの回避防止が緩和されます。 Asymmetric モードの場合、センサーは状態をフローと同期し、双方向を必要としないエンジンの検査を継続します。完全な保護には双方向のトラフィックを確認する必要があるため、Asymmetric モードではセキュリティが低下します。
説明	仮想センサーの説明。

仮想センサーのポリシーの編集

仮想センサーには 2 つのタイプのポリシーがあります。1 つは仮想センサーのプロパティで、もう 1 つは仮想センサーに割り当てられているポリシーです。それぞれ異なる方法を使用して、これらの項目を編集します。

- 仮想センサーのプロパティを編集するには、デバイスビューのデバイスセレクタで仮想センサーの親デバイスを選択します。次に、[仮想センサー（Virtual Sensors）]ポリシーを選択します。テーブル内で仮想センターを選択して、[行の編集（Edit Row）]ボタンをクリックできます。

[Virtual Sensors] ポリシーを使用すると、センサーに割り当てられているインターフェイス、異常検出モード、インライン TCP セッション トラッキング モードおよびノーマライザ モードを変更できます。詳細は、次のトピックを参照してください。

- 仮想センサーの定義 （2157 ページ）
- 仮想センサー ダイアログボックス （2159 ページ）

- 仮想センサーに割り当てられているポリシーを編集するには、デバイス ビューのデバイス セレクタで仮想センサーを選択します。仮想センサーの名前は、device-name_virtual-sensor-name の形式になります。device-name は親デバイスの名前、virtual-sensor-name は仮想センサーの名前です。たとえば、デバイス 10.100.10.10 上の仮想センサー vs1 は 10.100.10.10_vs1 になります。

（注） 基本仮想センサー vs0 は、親デバイスに統合されており、デバイス セレクタに単独では表示されません。基本仮想センサーを設定するには、親デバイスを選択します。

次に、ポリシーセレクタでポリシーを選択して、設定します。詳細は、次のトピックを参照してください。

- IPS シグニチャの定義 （2165 ページ）
- イベント アクション ルールの設定 （2211 ページ）
- 異常検出の設定 （2253 ページ）

その他のすべてのポリシーは親デバイスで設定します。設定は、そのデバイスに設定されているすべての仮想センサーに適用されます。

仮想センサーの削除

仮想センサーはデバイス ビューのデバイス セレクタに表示されます。ただし、他のデバイスに使用するコマンドと同じコマンドを使用しても、セレクタから仮想センサーを削除できませ

ん。代わりに、親デバイス（仮想センサーが定義されているデバイス）の [Virtual Sensors] ポリシーから仮想センサーを削除する必要があります。次の手順では、ユーザ定義の仮想センサーを削除する方法について説明します。

ヒント　基本仮想センサー vs0 は、デバイス セレクタには表示されません。代わりに、親の IPS センサーによって示されます。つまり、このセンサーが基本の IPS デバイスと見なされます。基本の vs0 センサーを削除するには、インベントリからデバイス全体を削除します。インベントリからデバイスを削除する方法の詳細については、Security Manager インベントリからのデバイスの削除　（162 ページ）を参照してください。

はじめる前に

仮想センサーを削除する場合は、シグニチャ、イベントアクション、および異常検出ポリシーなど、そのセンサーに定義されているポリシーも削除します。デフォルト以外のローカルポリシーを設定しており、他の仮想センサーで使用できるようにこれらを保持する場合は、最初にローカルポリシーを共有ポリシーに変換する必要があります。これで、仮想センサーを削除したあと、ポリシーは未割り当ての共有ポリシーとして存続するようになります。このあと、このポリシーを別の仮想センサーに割り当てることができます。ローカルポリシーから共有ポリシーを作成する方法の詳細については、ローカル ポリシーの共有　（262 ページ）を参照してください。

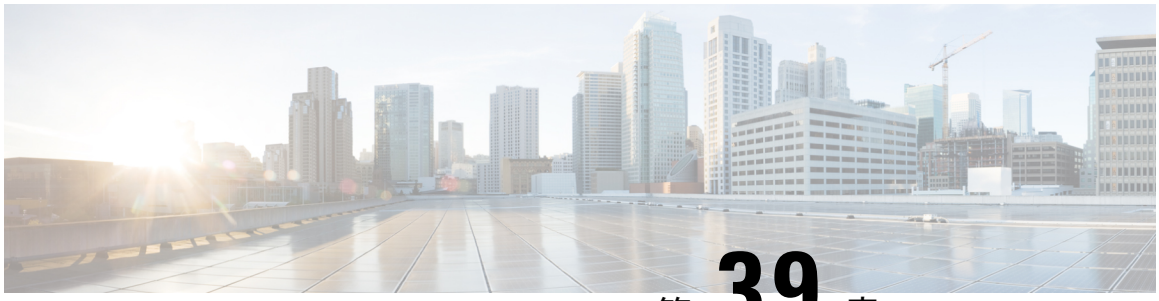
単に仮想センサーの名前を変更する手段として仮想センサーを削除する場合は、この方法を使用するのが最適です。仮想センサーの名前は変更できないため、これを削除してから、目的の名前で新しい仮想センサーを作成する必要があります。共有ポリシーを作成した場合は、これらの共有ポリシーを新しいセンサーに割り当てることができ、このセンサーは古い名前で持っていた設定と同じ設定を持つことになります。

ステップ 1　（デバイス ビューだけ）ポリシーセレクタから [仮想センサー（Virtual Sensors）] を選択して、[仮想センサー（Virtual Sensors）] ポリシーを開きます。

ステップ 2　削除するユーザー定義の仮想センサーを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 3　2 段階で確認が要求されます。最初に、ポリシーを保存してポリシーとデバイスを同期させておく必要があることを示す警告が表示されます。[OK] をクリックして続行すると、ノードを削除するかどうかの確認が求められます。

削除を確定すると、ポリシーとデバイスセレクタの両方から仮想センサーが削除されます。デバイス ビューが更新され、仮想センサーがデバイス リストに表示されなくなるまでに、しばらく時間がかかります。



第 39 章

IPS シグニチャの定義

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

Security Manager を使用すると、専用の IPS アプライアンスやサービス モジュール、または Cisco IOS IPS デバイスに IPS シグニチャを設定できます。Cisco IOS IPS のシグニチャを設定する場合、ルータでは、専用のアプライアンスやサービス モジュールほどは多くのシグニチャを使用できないことに注意してください。

この章は次のトピックで構成されています。

- シグニチャについて （2165 ページ）
- シグニチャの設定 （2169 ページ）
- シグニチャの設定値の設定 （2207 ページ）

シグニチャについて

ネットワークへの侵入とは、ネットワーク リソースへの攻撃、またはネットワーク リソースの不正使用を指しています。Cisco IPS センサーおよび Cisco IOS IPS デバイスでは、シグニチャベースのテクノロジーを使用して、ネットワーク侵入を検出します。シグニチャによって、センサーが検出およびレポートするネットワーク侵入のタイプを指定します。センサーは、ネットワーク パケットをスキャンするときに、シグニチャを使用して、Denial of Service（DoS; サービス拒絶）攻撃などの既知のタイプの攻撃を検出し、定義したアクションに従って対応します。

基本的なレベルでは、シグニチャベースの侵入検知テクノロジーは、ウイルス チェック プログラムにたとえることができます。Cisco IPS には、センサーがネットワーク アクティビティと照合するシグニチャのセットが含まれています。一致が見つかると、センサーは、イベントのロギングや、Security Manager Event Viewer へのアラームの送信などのアクションを実行します。

シグニチャによって false positive が生成される場合もあります。通常のネットワーク アクティビティであっても、悪意のあるアクティビティとして誤解される場合があるためです。たとえば、一部のネットワーク アプリケーションやオペレーティング システムは、多数の ICMP メッセージを送信することがありますが、シグニチャベースの検出システムでは、このメッセージが攻撃者によるネットワーク セグメント特定の試みであると解釈されてしまう可能性があります。シグニチャ パラメータを編集（シグニチャを調整）することにより、false positive を最小限に抑えることができます。

特定のシグニチャを使ってネットワーク トラフィックをモニタするようにセンサーを設定するには、そのシグニチャをイネーブルにする必要があります。デフォルトでは、重要なシグニチャはシグニチャ更新のインストール時にイネーブルになります。イネーブルなシグニチャに一致する攻撃が検出されると、センサーはアラートを生成します。生成されたアラートはセンサーのイベント ストアに保存されます。アラートは他のイベントと同様、Event Viewer などの Web ベースのクライアントによって、イベント ストアから取得される場合があります。デフォルトでは、センサーは Informational 以上のすべてのアラートをログに記録します。

シグニチャには、サブシグニチャを持つもの（サブカテゴリに分類されているもの）があります。サブシグニチャを設定した場合、あるサブシグニチャのパラメータを変更しても、変更が適用されるのはそのサブシグニチャだけです。たとえば、シグニチャ 3050 のサブシグニチャ 1 を編集し重大度を変更した場合、重大度の変更はサブシグニチャ 1 だけに適用され、3050 2、3050 3、および 3050 4 には適用されません。

Cisco IPS には、10,000 を超えるデフォルトの組み込みシグネチャが含まれています。組み込みシグニチャのリストにあるシグニチャの名前の変更および削除はできません。ただし、シグニチャをセンシング エンジンから削除して廃棄できます。あとで廃棄されたシグニチャをアクティブにできます。ただし、このプロセスにはセンシング エンジンの設定の再構築が必要です。この再構築には時間がかかり、トラフィックの処理を遅延させる可能性があります。組み込みシグニチャのチューニングは可能です。これには、シグニチャのいくつかのパラメータを変更します。変更された組み込みシグニチャは、チューニング済みシグニチャと呼ばれます。

（注） 使用していないシグニチャを廃棄することを推奨します。廃棄によって、センサーのパフォーマンスが向上します。

カスタム シグニチャと呼ばれるシグニチャを作成できます。カスタム シグニチャ ID は、60000 から始まります。いくつかの項目に対して、カスタム シグニチャを設定できます。たとえば、UDP 接続の文字列との一致やネットワーク フラッドの追跡、スキャンなどです。シグニチャは、モニタするトラフィックの種類に対して特別に設計されたシグニチャ エンジンを使って作成します。

シグニチャの詳細については、以下を参照してください。

- シグネチャの詳細情報の取得 （2167 ページ）
- シグニチャ継承について （2168 ページ）

関連項目

- シグニチャの設定 （2169 ページ）
- グローバル相関の設定 （2265 ページ）

シグネチャの詳細情報の取得

Cisco Security Intelligence Operations Web サイトで、各シグネチャの詳細情報を表示できます。Web サイトには、ネットワーク セキュリティに関する豊富な情報とベスト プラクティスの推奨事項が含まれており、IntelliShield アラートを設定できます。また、Web サイトでは、ネットワークを保護し、修復に優先順位を付け、組織のリスクを減らすようにシステムを構築するために役立つ高度なセキュリティ項目に関する情報も提供しています。

Security Manager の Signatures ポリシーを編集する際（[Signatures] ページ （2169 ページ）を参照）、シグネチャ ID は IPS シグネチャの Cisco Security Intelligence Operations データベースに直接リンクされています。シグネチャ ID をクリックすると、シグネチャに関する情報（説明、シグネチャが基づく脆弱性、シグネチャが作成された日時など）を含むページが開きます。このデータベースは、http://tools.cisco.com/security/center/search.x?search=Signature でユーザー自身が検索できます（データベースは以前、Cisco Network Security Database または NSDB と呼ばれていました）。

Cisco.com にアクセスできない場合、シグニチャ ID はシグネチャ データベース情報のローカル コピーにリンクされています。Security Manager によって、Cisco.com にアクセスできるかどうかが検出され、適切なリンクが作成されるため、ユーザはプリファレンスを設定する必要がありません。

データベースには、デフォルトの組み込みシグネチャの情報のみが含まれます。カスタム シグネチャ（ユーザが定義したシグネチャ）の情報は表示できません。

Security Manager 4.4 以降、[シグネチャ（Signatures）] ページ（[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]）には、各シグネチャの [説明（Explanation）] タブと [関連する脅威（Related Threats）] タブが含まれています。別のウィンドウの [シグネチャ（Signatures）] ページで、これらのタブに詳細情報が表示されます。たとえば、[説明（Explanation）] タブには、説明、シグネチャ ID などが表示されます。[関連する脅威（Related Threats）] タブには、使用している可能性のある他のソフトウェアの脆弱性などが表示されます。

ヒント このウィンドウが表示されていない場合は、[シグネチャ（Signatures）] ページの左下隅にある上矢印ボタンを使用してウィンドウを展開します。このウィンドウを非表示にするには、[シグネチャ（Signatures）] ページの左下隅にある、対応する下矢印を使用してウィンドウを折りたたみます。このウィンドウのサイズは、標準のコントロールで変更できます。

シグニチャ継承について

IPS デバイスのシグニチャ継承は、他のどの Security Manager のルール ベースのポリシーの場合とも異なります。継承とは、最初に一致したルールベースのポリシーの階層リスト（アクセス ルールなど）を適用する、Security Manager の機能のことです。シグニチャ継承での相違点は、IPS デバイスの場合、Security Manager によってシグニチャ単位の継承が可能になる点です。

次の例は、シグニチャ単位の継承がどのように行われるかを示しています。

ステップ 1 ポリシービューで、[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）] を選択します。

ステップ 2 test1 という名前のポリシーを作成します。

ステップ 3 test2 という名前の別のポリシーを作成します。

ステップ 4 [test 2] を右クリックし、[シグニチャの継承（Inherit Signatures）] を選択します。[Inherit Rules - test 2] ダイアログボックスが表示されます。

ステップ 5 [test1] を選択し、[OK] ボタンをクリックします。

ステップ 6 [test1] を選択し、シグニチャを編集します。編集した内容をメモし、変更内容を保存します。

ステップ 7 [test2] を選択し、編集したシグニチャを選択します。test2 が、test1 に対して行った編集内容を継承していることを確認します。

IPS シグネチャの削除

Security Manager 4.1 から、（導入されている一番低いシグネチャ レベルより古いシグネチャとして定義される）古いシグネチャ バージョンは、データベースの最適化を目的とする定期的な削除操作によって削除されます。

（注） 削除操作の結果、一部の未使用のチューニング コンテキストが削除されることに注意してください。

削除されたシグネチャの一部は、Cisco.com から IPS シグネチャ パッケージを次回ダウンロードする際に復元できる可能性があります。

デフォルトでは、IPS シグネチャの削除はディセーブルになっています。IPS シグネチャの削除をイネーブルにするには、次の手順を実行します。

ステップ 1 Cisco Security Manager Daemon Manager を停止します。コマンドプロンプトで、**net stop crmdmgtd** と入力します。

ステップ 2 *NMSROOT* \MDC\ips\etc\sensorupdate.properties ファイルに移動します（*NMSROOT* は Security Manager インストールディレクトリへのパスを表します）。デフォルトは C:\Program Files\CSCOpx です。

ステップ 3 sensorupdate.properties で、purgeUnusedSignautesEntriesinDB:false を purgeUnusedSignautesEntriesinDB:true に変更します。

ステップ 4 Cisco Security Manager Daemon Manager を再起動します。コマンドプロンプトで、**net start crmdmgtd** と入力します。

これで、IPS シグネチャの削除が毎日 0 時に実行されます。

シグニチャの設定

Signatures ポリシーで、Cisco IPS センサーと Cisco IOS IPS デバイスのシグニチャを設定します。

ここでは、次の内容について説明します。

- [Signatures] ページ （2169 ページ）
- シグネチャ更新レベルの表示 （2183 ページ）
- シグニチャのイネーブル化とディセーブル化 （2184 ページ）
- カスタム シグニチャの追加 （2191 ページ）
- シグニチャのクローニング （2195 ページ）
- カスタム署名の正規表現 （2195 ページ）
- シグニチャ パラメータの編集（シグニチャの調整） （2196 ページ）
- シグネチャの編集 （2185 ページ）

[Signatures] ページ

[Signatures] ページを使用して、IPS シグニチャの追加、編集および削除を実行できる、シグニチャ サマリー テーブルを表示します。このページで、シグニチャをイネーブルまたはディセーブルにして、ポリシー内のアクティブなシグニチャ セットを調整できます。このページを使用して、エンジンからシグニチャをアンロードすることもできます。

IPS デバイス バージョン 7.3(1) 以降では、Security Manager バージョン 4.6 以降で、1 つ以上のシグニチャ ポリシーにシグニチャ脅威プロファイルを適用できます。シグニチャ脅威プロファイルは、カスタマイズされた調整を含む定義済みのシグニチャ テンプレートです。これらの調整により、シグネチャ カバレッジおよび応答アクションが調整され、センサーがさまざまな展開および脅威シナリオでより適切な選択を行えるようになります。この [シグネチャ（Signatures）] ページには、ポリシーに適用されている脅威プロファイルとそのバージョンが表示されます。[変更の手順（To Change）] ボタンをクリックし、ポリシーに適用する脅威プロファイルを選択します。詳細については、シグネチャ脅威プロファイルの適用 （2177 ページ）を参照してください。脅威プロファイルに属しているシグネチャを確認するには、「**Threat Profile**」というテキストによって [ソース（Source）] 列をフィルタ処理します。テーブルを

フィルタ処理する方法については、テーブルのフィルタリング （64 ページ）を参照してください。

共有シグネチャポリシーで作成済みの脅威プロファイルが 1 つ以上含まれていない特定のシグネチャパッケージをダウンロードすると、Security Manager では、共有シグニチャのポリシービューに「現在適用されている脅威プロファイルは、このシグネチャバージョンには適用されません（Currently applied threat profile is not applicable to this signature version）」という警告メッセージが表示されます。同様に、Security Manager のデバイスビューでは、サポートされていないデバイスに共有シグネチャポリシーを適用しようとすると、同じ警告メッセージが表示されます。

脅威プロファイルの更新は個別に実行できないため、脅威プロファイルのバージョンを更新する場合は、デバイスの現在のシグネチャバージョンを更新する必要があります。脅威プロファイルのバージョンを更新すると、脅威プロファイルに関連付けられたシグネチャが変更されますが、ユーザーがすでに実行したユーザー定義シグネチャの調整は保持されることに注意してください。

（注） 脅威プロファイルは、IOS-IPS ではサポートされていません。

ヒント

- 有効になっているシグネチャと無効になっているシグネチャは、特定のシグネチャの [有効（Enabled）] チェックボックスによって示されます。Security Manager の以前のリリースでは、無効になっている署名は、テーブルの行を覆うハッシュマークによって示されていました。設定を展開すると、ディセーブルなシグネチャはデバイスから削除されます。詳細については、シグニチャのイネーブル化とディセーブル化 （2184 ページ）を参照してください。
- 多くのカラムでは、カラムを右クリックして直接プロパティを編集できます。編集した内容は、選択したすべての行に適用されます。複数の行を選択した場合、選択できるオプションは選択したすべての行に有効なものに限られます。右クリックメニューの内容は、右クリックしたセルに基づいて異なります。使用可能なコマンドの詳細については、シグネチャのショートカット メニュー （2179 ページ）を参照してください。
- 列を表示または非表示にするには、シグネチャサマリーテーブルのテーブル見出し行を右クリックし、[列の表示（Show Columns）] をクリックします。デフォルトでは、すべての列が表示されます。

（注） Security Manager のバージョン 4.5 以降には、シグネチャごとに [メモ（Notes）] 列があります。この機能によりメモを追加でき、後で特定のシグネチャに戻って、自分や他のユーザーがシグネチャやイベントに追加した内容を確認できます。この機能は、ネットワーク管理者が、ノイズの多いシグネチャや特に注意が必要なシグネチャを監視するために役立ちます。ただし、Security Manager データベースを復元すると、デフォルトでは [メモ（Notes）] 列が表示されない場合があります。[メモ（Notes）] 列を表示するには、シグネチャサマリーテーブルでテーブル見出し行を右クリックし、[列の表示（Show Columns）] をクリックして、最後に [メモ（Notes）] をクリックします。Security Manager のインストール時にデータベースをバックアップして復元すると、この状況が発生する場合があります。ただし、この状況は、インラインアップグレード時には発生しません。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- シグニチャ継承について （2168 ページ）
- シグニチャのイネーブル化とディセーブル化 （2184 ページ）
- シグニチャのクローニング （2195 ページ）
- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション ルールの設定 （2211 ページ）

フィールド リファレンス

表 519 : Signature Policy

要素	説明
ID	シグネチャ ID。このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。ID 番号をクリックすると、シグネチャの詳細情報の取得 （2167ページ）で説明したように、Web ブラウザでシグネチャの詳細情報が表示されたページが開きます。
Sub	サブシグネチャ ID。このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。
名前	証明書に割り当てられる名前を示します。
[有効（Enabled）]	このポリシーでシグネチャが有効か無効かを示すチェックボックス。シグニチャで指定されている攻撃からの保護をセンサーが提供するには、シグニチャをイネーブルにする必要があります。
重大度	シグニチャによってレポートされる重大度レベル（[High]、[Medium]、[Low]、または [Informational]）を示します。
Fidelity	ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。

要素	説明
注記	

要素	説明
	メモを追加して、後で特定のシグネチャに戻って、自分や他のユーザーがシグネチャやイベントに追加した内容を確認できるようにします。この機能は、ネットワーク管理者が、ノイズの多いシグネチャや特に注意が必要なシグネチャを監視するために役立ちます。 デバイスへの展開時には、メモはデバイスに保存されません。ここで説明する [メモ（Notes）] は、Security Manager の GUI のみの機能であり、Security Manager の IPS ポリシーの一部ではないため、デバイスへの展開時には無視されます。 [メモ（Notes）] は IPS ポリシーの一部ではないため、共有署名ポリシーの割り当てまたは継承は [メモ（Notes）] には影響しません。 シグネチャを右クリックしてメモを追加しても、アクティビティ/チケットの作成は求められません。ただし、シグネチャをダブルクリックするか [編集（Edit）] ボタンをクリックしてメモを追加すると、シグネチャポリシーの変更をともなうため、アクティビティ/チケットの作成を求められます。 シグネチャ更新操作の一部としてシグネチャにメモを追加することはできません。ただし、他のパラメータは編集できます。 メモは、グローバル検索機能では検索できません。 [メモ（Notes）] 列には、メモのテキストは表示されません。アイコンのみが表示されます。メモのテキストを表示するには、アイコンをダブルクリックする必要があります。 [ファイルにエクスポート（Export to File）] ボタンを使用すると、result.csv ファイルの [メモ（Notes）] 列には「Y」または「N」のみが表示されます。これは、それらのシグネチャにメモが付けられているかどうかを示します。実際のテキストはエクスポートされません。 メモは編集できません。追加されたすべてのメモは、新しいメモエントリとして既存のメモに付加されます。もちろん、メモを削除して、更新されたメモを新たに追加することもできます。 メモを追加するには、特定のシグネチャの行を右クリックし、[メモの追加（Add Note）] をクリックします。メモを追加したら、[保存（Save）] をクリックして [メモ（Notes）] ダイアログボックスを閉じます。[メモ（Notes）] ダイアログボックスを閉じると、特定のシグネチャの行に「メモ」アイコンが表示されます。 複数の署名にメモを追加するには、目的のシグネチャを選択し（Windows では Shift キーまたは Ctrl キーを押しながらクリック）、1 つの特定シグネチャの場合と同じ手順を続行します。 メモには、ローカルメモと共有メモがあります。ローカルポリシーのみを持つデバイスにメモを追加する場合は、ローカルメモのみを追加、編集、および削除できます。共有ポリシーが割り当てられたデバイスにメモを追加する場合は、ローカルメモと共有メモ（[このメモを共有（Share this Note）] オプショ

要素	説明
	ンをオンにする）の両方を追加、編集、および削除できます。ただし、共有ポリシーが割り当てられている場合でも、その特定のデバイスのみにメモを追加（つまり、メモのローカルオーバーライド）できます。 ヒント　デバイスに共有ポリシーが割り当てられている場合、共有ポリシーに影響を与えずに特定のシグネチャについてそのデバイスにのみメモを追加するには、デバイスビューで [このメモを共有（Share this Note）] オプションをオンにせずにメモを追加する必要があります。 ヒント　[シグネチャの編集（Edit Signature）] ダイアログボックスでメモを操作することもできます。この表で後述する「[編集（Edit）] ボタン」を参照してください。
[基本 RR（Base RR）]	シグニチャの基本リスク レーティング値を示します。
アクション（Actions）	このシグニチャが起動されたときにセンサーが実行するアクションを示します。
ソース	シグニチャの設定を上書きする、継承階層内の一番低いポリシーを示します。値は次のとおりです。 • [Default]：シグネチャはデフォルトのシスコ定義の設定を使用します。 • [Local]：シグネチャは選択したデバイス向けに特別に定義されています（デバイス ビューのみ）。 • [Policy name]：継承階層内の一番低い共有ポリシーを示します。ポリシー名はポリシー ビューで表示するか、またはデバイスに共有シグネチャ ポリシーを割り当てる場合はデバイス ビューで表示できます。

要素	説明
Retired	シグネチャが廃棄される条件（条件が存在する場合）。廃棄されたシグニチャは、シグニチャエンジンから削除されます。廃棄されたシグニチャをアクティブにして、シグニチャ エンジンに戻すことができます。 **ワンポイントアドバイス**）[廃棄（Retired）] フィールドを使用して、IOS-IPS デバイス上のディセーブルにしたシグニチャをアンロードし、そのデバイスのメモリ使用量を最適な量にします。 シグニチャ ポリシーのエンジン レベルが E-4 未満の場合、[Retired] フィールドの値は [false] と [true] のどちらかになります。[false] の場合、シグニチャは廃棄されません。[true] の場合、シグニチャは廃棄されます。 シグニチャ ポリシーのエンジン レベルが E-4 である場合、[Retired] フィールドの値は次の 4 つのいずれかになります。 • [偽（false）]：シグネチャは廃棄されません。 • [低メモリ廃棄（low-mem-retired）]：シグネチャは、メモリ容量が少ないプラットフォームで廃棄されます。メモリ容量が少ないデバイスとは、メモリが 2 GB 以下のものを指します。 • [中メモリ廃棄（med-mem-retired）]：シグニチャは、メモリ容量が中程度のプラットフォームで廃棄されます。メモリ容量が中程度のデバイスとは、メモリが 2 GB より大きく 4 GB 以下のものを指します（メモリが 4 GB を超えるデバイスは、メモリ容量が多いプラットフォームと見なされます）。 • [真（true）]：シグネチャはすべてのプラットフォームで廃棄されます。 [low-mem-retired] または [med-mem-retired] を選択すると、Security Manager はデバイスに対して、それらの条件を持ったシグネチャを設定します。デバイスでシグネチャが実際に廃棄されるかどうかはデバイスに取り付けられているメモリの容量によって異なります。デバイスによって実際に廃棄されるシグネチャが判断されます。 **ヒント**　ここで使用されているエンジンレベルという用語は、上の行で使用されているエンジンという用語とは異なります。
エンジン	このシグニチャによって指定されたトラフィックの解析と検査を行うエンジンを示します。
[View Update Level] ボタン （デバイス ビューだけ）	このデバイスのシグネチャ更新レベルを表示するには、このボタンをクリックします。詳細については、シグネチャ更新レベルの表示 （2183 ページ）を参照してください。

要素	説明
[Export to File] ボタン	このボタンをクリックして、現在のデバイスのシグニチャ サマリーを Comma Separated Value（CSV; カンマ区切り値）ファイルにエクスポートします。Security Manager サーバ上のフォルダを選択し、ファイル名を指定するように要求されます。
[追加（Add）] ボタン	カスタム シグネチャを追加するには、このボタンをクリックします。詳細は、次のトピックを参照してください。 • カスタム シグニチャの追加 （2191 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）
[編集（Edit）] ボタン	選択したシグネチャを編集するには、このボタンをクリックします。一度に編集できるシグニチャは1つです。詳細は、次のトピックを参照してください。 • シグネチャの編集 （2185 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）
[削除（Delete）] ボタン	選択したカスタムシグネチャを削除するには、このボタンをクリックします。 シスコ定義のシグネチャは削除できません。シスコ定義のシグネチャを展開しない場合は、シグネチャを廃棄またはディセーブルにできます。

シグネチャ脅威プロファイルの適用

[脅威プロファイルの適用（Apply Threat Profile）] ダイアログボックスを使用して、利用可能なプロファイルからシグネチャ脅威プロファイルを選択し、ポリシーに適用します。脅威プロファイルを適用すると、[Signatures] ページ （2169 ページ）上の [有効化（Enabled）] および [廃止（Retired）] フィールドのみが変更されます。特定の脅威プロファイルをポリシーに適用すると、対応するシグネチャチューニングが [シグネチャ（Signature）] ページの既存のシグネチャとマージされます。脅威プロファイルに属するシグニチャを表示するには、[シグニチャ（Signature）] ページで、テキスト **Threat Profile** が含まれるように [ソース（Source）] 列をフィルタリングします。テーブルをフィルタ処理する方法については、テーブルのフィルタリング （64 ページ）を参照してください。

現在シスコが提供している次の脅威プロファイルのいずれかを選択します。

- SCADA：主に産業用制御システムを保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。SCADA 署名テンプレートには、デフォルトセットの署名に加えて、一般的な SCADA プロトコル検出用の特殊な署名と、ほとんどのデバイス制御環境で共通するツールや環境に対応する特定の識別子が含まれています。

- Edge：主にインターネット接続を保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。Edge 署名テンプレートには、デフォルトセットの署名に加えて、デスクトップ オペレーティング システム、Web ブラウザ、Web テクノロジ、および一般的なデスクトップ アプリケーションに対してより広範な保護を提供する追加の署名が含まれています。
- Web_Applications：主に Web サーバーファームを保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。Web_Applications 署名テンプレートには、デフォルトセットの署名に加えて、Web サーバー、Web 開発ツールとフレームワーク、コンテンツ管理システム、ロードバランサ、およびデータベースに幅広い保護を提供する追加の署名が含まれています。
- Data Center：主にデータセンターを保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。Data Center 署名テンプレートには、デフォルトセットの署名に加えて、サーバー オペレーティング システム、Web サーバー、アプリケーションサーバー、データベース、コンテンツ管理システム、メッセージングサーバー、および仮想化システムに対してより広範な保護を提供する追加の署名が含まれています。

（注） ローカル署名（選択したデバイスに対して定義され、ソースポリシーがローカルである署名）でユーザーが実行したシグネチャチューニングは、脅威プロファイル上で保持されます。デフォルト署名の場合、脅威プロファイルのチューニングは保持されます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS デバイス）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *520 :* 脅威プロファイルの詳細

要素	説明
署名 ID	シグネチャ ID。このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。
Sub Signature ID	サブシグネチャ ID。このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。

要素	説明
[有効（Enabled）]	この脅威プロファイルでシグネチャが有効か無効かを示します。シグニチャで指定されている攻撃からの保護をセンサーが提供するには、シグニチャをイネーブルにする必要があります。
Retired	シグネチャがこの脅威プロファイルで廃止されているか、アクティブであるかを示します。
[競合あり（Has Conflict）]	適用された脅威プロファイルからのチューニングを含むシグネチャに、ユーザーによって実行されたチューニングも含まれているかどうかを示します。ユーザーおよび適用された脅威プロファイルによってチューニングされたシグネチャでは、[競合あり（Has Conflict）] 列に True のフラグが付けられます。適用された脅威プロファイルとユーザーによるシグネチャのチューニングの間に競合がない場合、そのシグネチャの [競合あり（Has Conflict）] 列に False と表示されます。 （注） ローカル署名（選択したデバイスに対して定義され、ソースポリシーがローカルである署名）でユーザーが実行したシグネチャチューニングは、脅威プロファイル上で保持されます。デフォルト署名の場合、脅威プロファイルのチューニングは保持されます。

シグネチャのショートカット メニュー

シグネチャ ポリシーのシグネチャ サマリー テーブル内を右クリックすると、選択したシグネチャに対してさまざまな機能を実行するためのショートカット メニューが表示されます。コマンドには、単一のシグネチャを選択した場合のみに表示されるものもあれば、複数のシグネチャに対して同時に使用でき、変更内容が選択したすべてのシグネチャに適用されるものもあります。シグネチャ ポリシーの詳細については、[Signatures] ページ （2169 ページ）を参照してください。

また、使用可能なコマンドは右クリックしたセルによって異なります。コマンドには、どのセルを右クリックしても使用できるものもあれば、単一のセルだけで使用できるものもあります。

ヒント 右クリック コマンドを使用してデフォルト シグネチャのセルの値を変更するときには、シグネチャはデバイス ビューでローカル シグネチャに変換されるか、ポリシー ビューで共有ポリシー固有のシグネチャに変換されます。

次の表に、使用可能なコマンドの説明を示します。

表 *521* : シグネチャのショートカット メニュー

メニュー コマンド	説明
すべてのセルに使用できるコマンド	
行を追加（Add Row）	カスタム シグネチャを追加します。詳細は、次のトピックを参照してください。 • カスタム シグニチャの追加 （2191 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）
Edit Row	選択したシグネチャを編集します。一度に編集できるシグニチャは 1 つです。詳細は、次のトピックを参照してください。 • シグネチャの編集 （2185 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）
Delete Row	選択したカスタム シグネチャを削除します。 シスコ定義のシグネチャは削除できません。シスコ定義のシグネチャを展開しない場合は、シグネチャを廃棄またはディセーブルにできます。
複製（Clone）	選択したシグネチャと同一のプロパティを持つ新規カスタム シグネチャを作成します。詳細については、 シグニチャのクローニング （2195 ページ）を参照してください。
Enable、Disable	シグニチャをイネーブルまたはディセーブルな状態にします。ディセーブルなシグニチャは、網掛けされて表示されます。詳細については、 シグニチャのイネーブル化とディセーブル化 （2184 ページ）を参照してください。
Show Events Show MARS Events	イベントビューアまたは Cisco Security MARS アプリケーションへの移動を有効にして、選択したシグニチャによって検出されたリアルタイムのイベントまたは過去のイベントを表示できるようにします。詳細については、 IPS シグニチャのイベントの表示 （3545 ページ）および IPS シグニチャの CS-MARS イベントの表示 （3738 ページ）を参照してください。
[Action] セルのコマンド	
Add to Actions	選択したシグニチャの現在のアクション リストにアクションを追加します。

メニュー コマンド	説明
Delete from Actions	選択したシグニチャの現在のアクション リストからアクションを削除します。
Replace Actions With	選択したシグニチャの現在のアクションセットを、選択した単一のアクションに置き換えます。複数のアクションを選択する場合、サブメニューから [その他（More）] を選択し、次に Ctrl キーを押した状態で目的のアクションをクリックして選択します。
Edit Actions	[Edit Actions] ダイアログボックスが開きます。このダイアログボックスで、シグネチャに対して実行するアクションを選択できます。選択したアクションで、シグニチャの現在のアクション リストを置き換えます。詳細については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （2181 ページ）を参照してください。
[Severity] セルのコマンド	
• 高い • 中規模 • 低い • 情報（Informational）	シグネチャの重大度レベルを、選択したレベルに変更します。
[Fidelity] セルのコマンド	
Edit Fidelity	シグニチャの忠実度評価を変更します。忠実度評価は、ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。
[Retired] セルのコマンド	
• 廃止（Retire） • アクティブ化 • Retire on Low Memory • Retire on Medium Memory	シグネチャの廃棄ステータスを、選択したステータスに変更します。廃棄ステータス カテゴリの詳細については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）を参照してください。

[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス

シグネチャに定義されているアクションを変更するには、[Edit Action]、[Add Action]、または [Replace Action] ダイアログボックスを使用します。これらのダイアログボックスは、シグネチャのショートカット メニュー （2179 ページ）で説明したように、右クリック メニューを使

用して [Action] セルを編集するときにのみ使用できます。動作はダイアログボックス名によって異なります。

- [Add Actions]：選択したアクションは、シグネチャですでに定義されているアクションに追加されます。このダイアログボックスを開くには、シグネチャの[アクション（Actions）] セルを右クリックし、[アクションに追加（Add to Actions）] > [さらに追加（More）] を選択します。
- [Replace Actions]：選択したアクションは、シグネチャで定義されているアクションをすべて置き換えます。このダイアログボックスを開くには、シグネチャの [アクション（Actions）] セルを右クリックし、[アクションを置換（Replace Actions With）] > [さらに追加（More）] を選択します。
- [Edit Actions]：選択したアクションは、シグネチャで定義されているアクションをすべて置き換えます。このダイアログボックスを開くには、シグネチャの[アクション（Actions）] セルを右クリックし、[アクションの編集（Edit Actions）] を選択します。

使用可能なアクションの説明については、IPS イベント アクションについて （2213 ページ）を参照してください。Ctrl キーを押した状態でクリックすることで、複数のアクションを選択できます。

（注） ダイアログボックスを開いたときに表示されるアクションのリストは、状況に応じて変わります。アクションのリストは、[Actions] カラムで 1 つのシグニチャ行だけを右クリックしたか、[Actions] カラムで右クリックする前に複数のシグニチャ行を選択したか、によって変わります。[Actions] カラムで 1 つのシグニチャ行だけを右クリックした場合、アクションのリストは、そのシグニチャのエンジンのリストになります。[Actions] カラムで右クリックする前に複数のシグニチャ行を選択した場合、アクションのリストは、影響を受ける各エンジンで使用できるリストになります（リストには、共通のアクションが含まれます。選択したシグニチャのすべてのアクションが含まれるわけではありません）。

[Edit Fidelity] ダイアログボックス

[Edit Fidelity] ダイアログボックスを使用して、特定のシグニチャの [Fidelity Rating] で変更を行います。忠実度評価、または Signature Fidelity Rating（SFR; シグニチャの忠実度評価）は、ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。この評価には、0 ～ 100 の任意の数字を指定できます。100 は、シグニチャの信頼性が最も高いことを意味します。

ナビゲーション パス

シグネチャ ポリシーで、シグネチャの [Fidelity] セルを右クリックし、[Edit Fidelity] を選択します。シグネチャ ポリシーを開く方法については、[Signatures] ページ （2169 ページ）を参照してください。シグネチャのショートカット メニューの詳細については、シグネチャのショートカット メニュー （2179 ページ）を参照してください。

シグネチャ更新レベルの表示

デバイス ビューで、Security Manager のデバイスに適用されている現在のシグネチャ更新パッケージを判定し、デバイスに展開されているパッケージと比較できます。

適用された更新レベルと展開された更新レベルとの間の相違は、次の場合に発生する可能性があります。

- デバイスが、Security Manager の外部で更新された。
- Security Manager で更新はポリシーに適用されたが、デバイスにまだパブリッシュされていない。
- Security Manager の初回の展開時に、デバイスがまだ Security Manager の制御下にない。

シグネチャ更新レベルを表示するには、デバイスビューで IPS デバイスに対して、[IPS] > [シグネチャ（Signatures）]>[シグネチャ（Signatures）]ポリシーを選択します。次に、[更新レベルの表示（View Update Level）] ボタンをクリックして [更新レベル（Update Level）] ダイアログボックスを開きます。

次の表に、ダイアログボックスに表示される情報を示します。

表 *522 : [Update Level]* ダイアログボックス

要素	説明
Applied Level	このカラムには、Security Manager でこのデバイスに適用されるパッチ レベルが表示されます。
Deployed Level	このカラムには、選択したデバイスで現在実行されているパッチ レベルが表示されます。
メジャー アップデート	メジャー更新レベルを示します。
マイナー アップデート	マイナー更新レベルを示します。
サービス パック	サービス パック レベルを示します。
パッチ	パッチ レベルを示します。
エンジン	エンジン レベルを示します。
シグニチャ アップデート	シグニチャ更新レベルを示します。 （注） このフィールドは、このページにおいて、IOS IPS デバイスに適用される唯一のフィールドです。その他のフィールドはすべて、IPS デバイス専用です。

要素	説明
[Revert] ボタン	誤って [適用レベル（Applied Level）] を変更した場合は、新しい [適用レベル（Applied Level）] を廃棄できます。[復元（Revert）] をクリックすると、[適用レベル（Applied Level）] が [展開レベル（Deployed Level）] に同期されます。 ヒント　復元が実行される前に、警告ダイアログが表示されます。アクティビティを送信するかどうかを確認する警告ダイアログも表示されます。

シグニチャのイネーブル化とディセーブル化

個別のシグネチャをイネーブルまたはディセーブルにできます。変更は、設定をデバイスに再展開すると有効になります。

シグネチャがディセーブルになっている場合、テーブルでそのルールにハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなシグネチャはデバイスから削除されます。

シグネチャのディセーブル化は、デバイスで使用するシグネチャの数を減らす場合や、カスタム シグネチャを削除せずにその使用を一時的に停止する場合に役立ちます。あとでディセーブルにしたシグネチャを再びイネーブルにできます。

（注）　廃棄されたシグニチャをイネーブルにできますが、廃棄されたシグニチャはシグニチャ マイクロ エンジンに含まれていないため、トラフィックのスキャンには使用されません。特定のシグニチャに関してネットワーク トラフィックをセンサーでスキャンする場合は、そのシグニチャをイネーブルにし、廃棄はしないでください。AIP-SSC-5 では、廃棄されたシグニチャをイネーブルにできません。

ステップ 1　次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（[Signatures] ページ （2169 ページ）を参照）。

ステップ 2 イネーブルステータスを変更するシグネチャを右クリックして、適宜[イネーブル（Enable）]または[ディセーブル（Disable）] を選択します。

シグネチャの編集

シグネチャを編集して、その動作を変更できます。たとえば、シグネチャが起動するときに実行するアクションや、シグネチャのリスク評価の計算に使用される重大度および忠実度評価を変更できます。

一部のシグニチャには、次に示す特別な要件があります。たとえば、ACL違反シグニチャを検出するようにセンサーを設定するには、ACL 違反を記録するように 1 つ以上の Cisco IOS ルータを最初に設定する必要があります。次に、センサーと通信するようにそれらのルータを設定する必要があります。最後に、これらのルータからsyslogトラフィックを受信するようにセンサーを設定する必要があります。

ヒント この手順では、シグネチャ全体を編集する方法について説明します。シグネチャポリシーの右クリック メニューを使用することで、シグネチャの個別のプロパティを選択して編集することもできます。使用可能なコマンドの詳細については、シグネチャのショートカット メニュー （2179 ページ）を参照してください。

関連項目

- シグニチャについて （2165 ページ）
- IPS イベント アクションについて （2213 ページ）
- シグニチャのイネーブル化とディセーブル化 （2184 ページ）
- シグニチャのクローニング （2195 ページ）
- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション ルールの設定 （2211 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから[IPS]>[シグネチャ（Signatures）]>[シグネチャ（Signatures）] を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）[IPS]>[シグネチャ（Signatures）] >[シグネチャ（Signatures）] を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）[IPS（ルータ） （IPS (Router)）]>[シグネチャ（Signatures）] を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（ [Signatures] ページ （2169 ページ）を参照）。

ステップ 2 編集するシグネチャを右クリックし、[行の編集（Edit Row）] を選択します。シグネチャを選択して、シグネチャ テーブルの下にある [Edit Row]（鉛筆）ボタンをクリックすることもできます。[Edit Signature] ダイアログボックスが開きます。

ヒント テーブルの上にある [Filter] フィールドを使用すると、目的のシグネチャを検索しやすくなります。テーブルのフィルタリングの詳細については、テーブルのフィルタリング （64 ページ）を参照してください。

ステップ 3 シグネチャに目的の変更を加えます。各オプションの具体的な詳細については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）を参照してください。

シグネチャを編集するときは、次の点を考慮してください。

- デフォルト シグネチャは編集できません。デフォルト シグネチャは、シスコ定義バージョンのシグネチャです。デフォルト シグネチャを編集する前に、デフォルト シグネチャをローカル シグネチャ（選択したデバイスに定義されているシグネチャ）または共有ポリシー固有のシグネチャ（共有ポリシーで定義されているシグネチャ）のいずれかに変換する必要があります。[Edit Signature] ダイアログボックスのフィールドを変更する前に、[Source Policy] フィールドから [Local] または共有ポリシー名を選択する必要があります。
- シグネチャのすべての特性を変更できるわけではありません。たとえば、シグネチャ ID またはサブシグネチャ ID は変更できません。このフィールドは読み取り専用です。
- シグネチャの詳細パラメータを変更する場合は、シグニチャ パラメータの編集（シグニチャの調整）（2196 ページ）で説明する手順に従ってください。

ステップ 4 [OK] をクリックして変更を保存します。

[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス

[Edit Signature] ダイアログボックスと [Add Custom Signature] ダイアログボックスは基本的には同じです。ほとんどのフィールドは同一ですが、レイアウトが多少異なります。このダイアログボックスは、次のように使用します。

- [Edit Signature] ダイアログボックスを使用して、デフォルト以外のシグネチャの特性を編集します（読み取り専用モードでは、デフォルト シグネチャの特性の表示のみが可能です）。

デフォルト シグネチャは編集できません。シグネチャに変更を加えるには、ダイアログボックスの一番上にある [Source Policy] フィールドで [Default] 以外のシグネチャを選択する必要があります。

- [Add Custom Signature] ダイアログボックスを使用して、カスタム シグニチャを作成します。[Add Custom Signature] ダイアログボックスで、名前を入力してから、ドロップダウン リストから既存のエンジンを選択します。シグニチャ ID とサブシグニチャ ID は、Security

Manager によって割り当てられます。残りのパラメータの選択を終了すると、新しいシグニチャは、[Signatures] ページの適切な数値位置に追加され、選択された状態になります。

（注） Security Manager 4.4 以降では、カスタムシグニチャを追加するときに、シグニチャ ID とサブシグニチャ ID を指定できます。既に存在する シグネチャ ID/サブシグニチャ ID の組み合わせを指定すると、エラーメッセージが表示されます。

ナビゲーション パス

[Signatures] ページから、次の作業ができます。

- シグネチャを編集するには、編集するポリシーを右クリックし、[行の編集（Edit Row）] を選択します。
- カスタムシグネチャを追加するには、テーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックするか、任意の行を右クリックし、[行の追加（Add Row）] を選択します。

[Signature] ページを開く方法については、[Signatures] ページ （2169 ページ）を参照してください。

関連項目

- [Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （2181 ページ）
- [Edit Signature Parameters] ダイアログボックス （2198 ページ）
- エンジンのオプション （2192 ページ）

フィールド リファレンス

表 523 : [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス

要素	説明
Source Policy （[Edit signature] のみ）	シグネチャの編集におけるポリシーは、次のとおりです。 • [Default]：デフォルトのシスコ定義のシグネチャ。このシグネチャは編集できません。シグネチャを編集するには、[Default] 以外のシグネチャを選択する必要があります。 • [Local]：選択したデバイス向けに特別に定義されているローカルシグネチャです。このオプションはポリシー ビューでは使用できません。 • [Policy name]（変数）：共有ポリシーの名前。デバイス ビューでは、デバイスに共有ポリシーを割り当てた場合のみ、ポリシー名を使用できます。ポリシー ビューでは、編集しているポリシー名を指します。ポリシー名を選択して、シグネチャを編集し、編集した内容を共有ポリシーが割り当てられているすべてのデバイスに反映します。
名前 （[Add] のみ）	シグネチャの名前。 いったん作成したシグネチャの名前は変更できません。名前を変更する場合、シグネチャの複製を作成する必要があります。
[SigID] （[Add] のみ）	カスタムシグネチャを追加するときに指定するシグネチャ ID。 値の許容範囲は 60000 ～ 65000 です。
[SubSigID] （[Add] のみ）	カスタムシグネチャを追加するときに指定するサブシグネチャ ID。 値の許容範囲は 0 ～ 255 です。
Inheritance Mandatory （[Edit signature] のみ）	選択すると、このポリシーから継承されるすべてのポリシーで、定義されたシグニチャ設定が使用されるようになります。
[有効（Enabled）]	シグニチャがイネーブルかどうかを示します。
重大度	シグニチャによってレポートされる重大度レベル（[High]、[Medium]、[Low]、または [Informational]）を示します。
Fidelity Rating	ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。

要素	説明
アクション（Actions）	このシグニチャが起動されたときにセンサーが実行するアクションを示します。アクションの一覧については、IPS イベント アクションについて （2213 ページ）を参照してください。 Ctrl キーを押した状態でクリックすることで、複数のアクションを選択できます。
Base Risk Rating Risk Rating （シグネチャの追加または編集で、フィールドの名前は若干異なります）	シグネチャの基本リスク レーティング値。この値は、忠実度評価と重大度係数を掛け合わせたものを 100 で割ることによって（忠実度評価 x 重大度係数 /100）計算されます。この値は読み取り専用です。直接変更できません。値を変更するには、[Severity] フィールドと [Fidelity] フィールドを変更します。 重大度係数は、[Severity] フィールドでの選択内容に応じて、次の値をとります。 • High = 100 • Medium = 75 • Low = 50 • Informational = 25
エンジン （編集時は読み取り専用。カスタム シグネチャの追加時は読み書き可能）	このシグニチャによって指定されたトラフィックの解析と検査を行うエンジンを示します。エンジンの詳細については、 エンジンのオプション （2192 ページ）を参照してください。 カスタム シグネチャを追加するときは、適切なエンジンを選択する必要があります。各エンジンに関する詳細情報と使用可能なパラメータについては、ご使用の IPS ソフトウェア リリースに対応したCisco Intrusion Prevention System Device Manager のインストールおよび使用法ガイド [英語] の「Signature Engines」セクションを参照してください。 **ヒント** ここで使用されているエンジンという用語は、下の行で使用されるエンジン レベルという用語とは異なります。

要素	説明
Retired	シグネチャが廃棄される条件（条件が存在する場合）。廃棄されたシグニチャは、シグニチャエンジンから削除されます。廃棄されたシグニチャをアクティブにして、シグニチャエンジンに戻すことができます。 **ワンポイントアドバイス**：[廃棄（Retired）] フィールドを使用して、IOS-IPS デバイス上のディセーブルにしたシグニチャをアンロードし、そのデバイスのメモリ使用量を最適な量にします。 シグニチャ ポリシーのエンジン レベルが E-4 未満の場合、[Retired] フィールドの値は [false] と [true] のどちらかになります。[false] の場合、シグニチャは廃棄されません。[true] の場合、シグニチャは廃棄されます。 シグニチャ ポリシーのエンジン レベルが E-4 である場合、[Retired] フィールドの値は次の 4 つのいずれかになります。 • [偽（false）]：シグネチャは廃棄されません。 • [低メモリ廃棄（low-mem-retired）]：シグネチャは、メモリ容量が少ないプラットフォームで廃棄されます。メモリ容量が少ないデバイスとは、メモリが 2 MB 以下のものを指します。 • [中メモリ廃棄（med-mem-retired）]：シグニチャは、メモリ容量が中程度のプラットフォームで廃棄されます。メモリ容量が中程度のデバイスとは、メモリが 2 MB より大きく 4 MB 以下のものを指します（メモリが 4 MB を超えるデバイスは、メモリ容量が多いプラットフォームと見なされます）。 • [真（true）]：シグネチャはすべてのプラットフォームで廃棄されます。 [low-mem-retired] または [med-mem-retired] を選択すると、Security Manager はデバイスに対して、それらの条件を持ったシグネチャを設定します。デバイスでシグネチャが実際に廃棄されるかどうかはデバイスに取り付けられているメモリの容量によって異なります。デバイスによって実際に廃棄されるシグネチャが判断されます。 **ヒント**　ここで使用されているエンジンレベルという用語は、上の行で使用されているエンジンという用語とは異なります。
Obsolete （[Edit signature] のみ）	シグニチャが古いかどうかを示します。古いシグニチャは、シグニチャエンジンから削除されます。再度アクティブにすることはできません。

要素	説明
[Restore Defaults] ボタン （カスタム以外のシグネチャのみ。[Edit signature] のみ）	このボタンをクリックして、このシグネチャをシスコ定義のデフォルト値に戻します。
[Edit Parameters] ボタン	このボタンをクリックして、[Edit Signature Parameters] ダイアログボックスを使用し、このシグネチャの詳細パラメータを編集します。詳細は、次のトピックを参照してください。 • [Edit Signature Parameters] ダイアログボックス （2198 ページ） • シグニチャ パラメータの編集（シグニチャの調整） （2196 ページ）

カスタム シグニチャの追加

組み込みシグネチャで指定されていないトラフィック パターンが必要な場合、独自のカスタム シグネチャを作成してトラフィック パターンを定義できます。

組み込みシグネチャがトラフィック パターンを網羅している場合でも、デフォルト シグネチャを変更せずに、カスタム シグネチャを作成し、詳細シグネチャ パラメータを編集できます。既存のシグネチャと同様のカスタム シグネチャを作成する場合は、シグニチャのクローニング （2195 ページ）で説明するように、シグネチャを複製するのが最も簡単な方法です。

一部の IPS デバイスにカスタムシグニチャを追加する場合、正規表現を使用できます。正規表現を使用する際の適切な構文の重要性について詳しくは、 カスタム署名の正規表現 （2195 ページ）を参照してください。

（注） AIP-SSC-5 では、カスタム シグニチャはサポートされていません。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（ [Signatures] ページ （2169 ページ）を参照）。

ステップ 2 シグネチャテーブルの下にある [行の追加（+）（Add Row (+)）] ボタンをクリックし、[カスタムシグネチャの追加（Add Custom Signature）] ダイアログボックスを開きます。

ステップ 3 必要な設定を行います。各オプションの具体的な詳細については、 [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）を参照してください。

シグネチャを作成するときは、次の点を考慮してください。

- いったん定義したシグネチャの名前は変更できません。あとで名前を変更する場合、シグネチャを複製し、複製を作成する際に名前を変更する必要があります。
- シグネチャに適したシグネチャ エンジンを選択します。シグネチャ エンジンの詳細については、 エンジンのオプション （2192ページ）を参照してください。いったんシグネチャを作成すると、エンジンは変更できません。誤ったエンジンを選択した状態で [OK] をクリックしシグネチャを保存した場合、最初からやり直して、完全に新しいシグネチャを作成する必要があります。
- デフォルトでは、イネーブルのシグネチャが作成されます。ただし、[Enabled] チェックボックスの選択を解除して、最初からディセーブルのシグネチャを作成できます。これで、パラメータの編集が終っていない場合に、シグネチャをディセーブルにできます。
- シグニチャ パラメータの編集（シグニチャの調整） （2196ページ）で説明する手順に従って、シグネチャの詳細パラメータを定義します。多くのパラメータがシグネチャ エンジンによって決まるため、パラメータを編集する前に目的のエンジンを選択する必要があります。

パラメータを設定する前にシグネチャを保存できるかどうかは、選択したエンジンによって異なります。シグネチャの定義を保存するには、少なくとも、[パラメータの編集（Edit Parameters）] をクリックして [シグネチャパラメータの編集（Edit Signature Parameters）] ダイアログボックスを開いてから、[シグネチャパラメータの編集（Edit Signature Parameters）] ダイアログボックスで [OK] をクリックする必要があります。ただし、有効なシグネチャを作成するには、パラメータを設定して目的のトラフィック パターンを指定する必要があります。

ステップ 4 [OK] をクリックして変更を保存します。

カスタム シグネチャはテーブルの最後に追加され、60000 から始まるシグネチャ ID のうち、次に使用可能なシグネチャ ID が設定されます。

（注） Security Manager 4.4 以降では、カスタムシグニチャを追加するときに、シグニチャ ID とサブシグニチャ ID を指定できます。既に存在する シグネチャ ID/サブシグニチャ ID の組み合わせを指定すると、エラーメッセージが表示されます。

エンジンのオプション

次のリストに、[Edit Signature Parameters] ダイアログボックスの [Engine] フィールドで指定できるオプションを示します。各エンジンに関する詳細情報と使用可能なパラメータについては、ご使用の IPS ソフトウェアリリースに対応したCisco Intrusion Prevention System Device Manager のインストールおよび使用法ガイド [英語] の「Signature Engines」セクションを参照してください。

- [AIC FTP]：FTP トラフィックを検査し、発行するコマンドを制御できるようにします。
- [AIC HTTP]：HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。
- [Atomic ARP]：レイヤ 2 ARP プロトコルを検査します。Atomic ARP エンジンが異なるのは、大半のエンジンはレイヤ 3 IP に基づいているためです。
- [atomic-ip]：IP プロトコル パケット、および関連付けられているレイヤ 4 トランスポート プロトコルを検査します。
- [Atomic IPv6]：不正な形式の IPv6 トラフィックによって引き起こされる IOS 脆弱性を検出します。
- [Flood Host]：ホストに向けられた ICMP フラッドと UDP フラッドを検出します。
- [Flood Net]：ネットワークに向けられた ICMP フラッドと UDP フラッドを検出します。
- Meta：スライディング時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。
- [multi-string]：1 つのシグニチャに一致する複数のストリングを使用して、レイヤ 4 トランスポート プロトコル（ICMP、TCP、および UDP）のペイロードを検査するシグニチャを定義します。シグニチャを起動するために一致する必要がある一連の正規表現パターンを指定できます。
- [normalizer]：IP および TCP ノーマライザが機能する方法を設定し、IP および TCP ノーマライザに関連するシグニチャ イベントに設定を提供します。RFC 準拠を強制できます。
- [service-dns]：DNS（TCP および UDP）トラフィックを検査します。
- [service-ftp]：FTP トラフィックを検査します。
- [Service Generic]：カスタム サービスおよびペイロードをデコードします。

Service Generic エンジンを使用すると、設定ファイルでシグニチャを更新するだけで、プログラム シグニチャを発行できます。このエンジンには、コンフィギュレーション ファイルで定義されている簡易マシンおよびアセンブリ言語が含まれています。このエンジンは、仮想マシンを介して（アセンブリ言語から導出された）マシン コードを実行します。仮想マシンは、命令を処理し、パケットから重要な情報を引き出して、マシン コードに指定されている比較および演算を実行します。このエンジンは、String エンジンと State エンジンを補足する迅速なシグニチャ応答エンジンとして設計されています。

Service Generic エンジンを使用してカスタム シグニチャを作成することはできません。

（注） 複雑な言語特有の性質上、Service Generic エンジンのシグニチャ パラメータを編集することは推奨しません。シグネチャの重大度とイベントアクションのみを変更してください。

- [Service Generic Advanced]：ネットワーク プロトコルの一般的な分析を行います。

- [Service H225]：VoIP トラフィックを検査します。
- [service-http]：HTTP トラフィックを検査します。WEBPORTS 変数では、HTTP トラフィックの検査ポートを定義します。
- [Service IDENT]：IDENT（クライアントおよびサーバ）トラフィックを検査します。
- [Service MSRPC]：MSRPC トラフィックを検査します。
- [Service MSSQL]：Microsoft SQL トラフィックを検査します。
- [Service NTP]：NTP トラフィックを検査します。
- [service-rpc]：RPC トラフィックを検査します。
- [Service SMB]：SMB トラフィックを検査します。
- [Service SMB Advanced]：Microsoft SMB パケットと Microsoft RPC over SMB パケットを処理します。
- [Service SNMP]：SNMP トラフィックを検査します。
- [Service SSH]：SSH トラフィックを検査します。
- [Service TNS]：TNS トラフィックを検査します。
- [state]：SMTP などのプロトコル内の文字列をステートフル検索します。
- [string-icmp]：ICMP プロトコルに基づいて正規表現文字列を検索します。
- [string-tcp]：TCP プロトコルに基づいて正規表現文字列を検索します。
- [string-udp]：UDP プロトコルに基づいて正規表現文字列を検索します。
- [Sweep]：1 つのホスト（ICMP と TCP）、宛先ポート（TCP と UDP）、および 2 つのノード間で RPC 要求を送受信する複数のポートからの、ポート、ホスト、およびサービスのスイープを分析します。
- [Sweep Other TCP]：1 つのホストに関する情報を取得しようとしている監視スキャンからの、TCP フラグの組み合わせを分析します。シグネチャはフラグ A、B、および C を探します。3 つすべてが検出されると、アラートが発生します。
- Traffic ICMP：TFN2K、LOKI、DDOS などの非標準プロトコルを分析します。パラメータを設定できるのは 2 つのシグニチャだけです。
- [Traffic Anomaly]：ワームに感染したホストの TCP、UDP、およびその他のトラフィックを分析します。
- [Trojan Bo2k]：非標準プロトコル BO2K からのトラフィックを分析します。このエンジンには、ユーザが設定できるパラメータはありません。
- [Trojan Tfn2k]：非標準プロトコル TFN2K からのトラフィックを分析します。このエンジンには、ユーザが設定できるパラメータはありません。

- [Trojan UDP]：UDP プロトコルからのトラフィックを分析します。このエンジンには、ユーザが設定できるパラメータはありません。

シグニチャのクローニング

既存のシグネチャと同様のカスタム シグネチャを作成する場合、シグネチャの複製、つまりコピーを作成できます。次に、複製が要件に応じて実行されるように、パラメータを編集できます。

たとえば、シスコ定義のシグネチャの複製を作成し、ニーズに合わせてカスタマイズできます。シスコのシグネチャをローカル シグネチャまたは共有ポリシー シグネチャに変換して直接パラメータを編集するよりも、実行しやすい場合があります。

シグニチャを複製するには、次の手順を実行します。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（[Signatures] ページ （2169 ページ）を参照）。

ステップ 2 複製するシグネチャを右クリックし、[複製（Clone）] を選択します。

Security Manager によるコピーの作成には、時間がかかることがあります。一部の属性は読み取り専用でコピーできない旨の警告が表示される場合があります。警告が表示されたら、[OK] をクリックします。次に、[Add Custom Signature] ダイアログボックスが表示されます。

ステップ 3 カスタム シグニチャの追加 （2191 ページ）の説明に従って、複製したシグネチャのプロパティを編集します。

ステップ 4 [OK] をクリック複製したシグニチャは、[Signatures] ページのサマリー テーブルに最後のシグネチャとして表示されます。

複製したシグニチャは、デフォルトでイネーブルおよびアクティブになります。

カスタム署名の正規表現

一部の IPS デバイスにカスタム署名を追加する際、正規表現を使用できます。

IPS デバイスのタイプやカスタム署名の特定の特性に関係なく、正規表現のシンタックスが正しくないと、カスタム署名の追加後にデバイスの展開が失敗します。

正規表現には、多くの制御文字や正規表現パターン自体を記述するための正規表現表記を含む場合があります。正規表現自体でそれらをリテラル文字として使用する場合は、「\」エスケープ文字でエスケープする必要があります。一方、それらを本来の意味で使用する場合は、適切な正規表現シンタックスに準拠するよう注意する必要があります。

展開の失敗の原因となる正規表現の例：!@#$%^&*()_+{}|:"<>?

正常に展開される正規表現の例：!@#$%\^&*\()_+\{\}|:\"<>\?

この例では、カスタム 署名での正規表現の使用について説明します。

ステップ 1 Cisco ASA 5500 シリーズ IPS セキュリティ サービス プロセッサ（5525-X など）を追加します。

ステップ 2 string-XL エンジン（string-xl-tcp など）を使用して、カスタム署名を IPS デバイスに追加します。

ステップ 3 [パラメータの編集（Edit Parameter）] をクリックして、カスタム署名の正規表現を作成します。

ステップ 4 IPS デバイスを展開します。

ステップ 5 正規表現で使用されたシンタックスが正しくないと展開は失敗しますが、正しいシンタックスを使用すると展開は成功します。

シグニチャ パラメータの編集（シグニチャの調整）

イベントアクションフィルタおよびオーバーライドポリシーを使用するか、またはシグネチャに関連したアクションを変更して、ニーズに合うようにシグネチャの動作を変更できない場合、シグネチャ パラメータの微調整が必要になる場合があります。ただし、これらのパラメータは複雑で、パケットの特性に対する深い理解がしばしば必要になる場合があるため、パラメータの編集は最後のオプションとして検討してください。

パラメータを編集する理由は、false positive と false negative を減らすためです。

- false positive は、ウイルススキャンなどの正当なネットワークアクティビティが攻撃として解釈およびレポートされた場合に発生します。これは、攻撃が行われる前に、攻撃を識別するために指定されている基準をネットワーク アクティビティが満たした場合に発生します。センサーの設定を調整することにより、false positive の数を減らすことができます。
- false negative は、攻撃が検出されなかった場合に発生します。センサーの設定を調整することにより、false negative の数を減らすことができます。

ヒント デフォルト シグネチャのパラメータは編集できません。デフォルト シグネチャのパラメータを編集する前に、シグネチャをローカル シグネチャまたは共有ポリシー シグネチャに変換する必要があります。正規表現の編集など、シグネチャを複製し、カスタム シグネチャに変換する必要がある場合があります。

この手順では、シグニチャ パラメータを編集してシグニチャを調整する方法について説明します。

関連項目

- シグネチャの編集 （2185 ページ）
- シグニチャについて （2165 ページ）
- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション オーバーライドの設定 （2227 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（ [Signatures] ページ （2169 ページ）を参照）。

ステップ 2 パラメータを編集するシグネチャを右クリックし、[行の編集（Edit Row）] を選択します。[Edit Signature] ダイアログボックスが表示されます（ [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）を参照）。

ステップ 3 [Source Policy] フィールドに [Default] が表示されている場合、パラメータを編集できるようにするには、[Source Policy] を [Local] または共有ポリシーの名前に変更する必要があります。[Local] オプションはデバイス ビューのみで使用可能です。このオプションでは、変更内容を編集中のデバイスに適用し、その他のデバイスには適用しません。共有ポリシーの名前を選択した場合、変更内容はポリシーが割り当てられているすべてのデバイスに適用されます。

ステップ 4 [パラメータの編集（Edit Parameters）] をクリックします。[Edit Signature Parameters] ダイアログボックスが表示されます。

[Edit Signature Parameters] ダイアログボックスは、フォルダ ツリー構造を保持しています。左側のツリーにはパラメータ名が表示され、右側にはパラメータの値が表示されます。

変更できる値には、名前の部分に小さなボックスがあります。これはチェックボックスです。チェックボックスが空の場合、パラメータのデフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。（フィールドを編集すると、通常ボックスにチェック マークが追加されます）。

パラメータを変更するには、右側の対象フィールドをクリックします。パラメータをクリックした場合の動作は、パラメータ タイプによって異なります。

- 読み取り専用のパラメータ：多くのパラメータは読み取り専用で変更できません（シグネチャ ID など）。これらのパラメータをクリックしても通常無効になります。ただし、パラメータ リストでは、ダイアログボックスが開きます（[Obsoletes] リストなど）。
- テキストまたは数値のパラメータ：英数字または数字の値を入力する必要があるパラメータをクリックすると、フィールドは編集ボックスになります。目的の値を入力し、Enter キーを押すか、または編集ボックスの外側をクリックします。
- 事前に定義された値のパラメータ：多くのパラメータには、数個の選択できる値があります（[Yes]/[No] など）。これらのパラメータをクリックすると、ドロップダウン リストがアクティブになります。目的のオプションを選択し、フィールドの外側をクリックします。
- リストのパラメータ：項目のリストを保持しているパラメータもあります。これらのパラメータでは、パラメータ値に [Set] または [List] などの単語と鉛筆アイコンが表示されます。フィールド内をクリックすると、ダイアログボックスが開き、項目に関連するリストを設定できます。例としては、Meta エンジン コンポーネントのリストがあります。詳細については、Meta エンジン シグネチャのコンポーネント リストの編集 （2205 ページ）を参照してください。
- 変数パラメータ：ポリシー オブジェクトを選択して、パラメータの内容を指定できるパラメータもあります。たとえば、一部のシグネチャ エンジンでは、ポート リスト オブジェクトを選択して、ポートを指定できます。これらのパラメータをクリックすると、[Select] ボタンのついた編集ボックスが表示されます。編集ボックスにポリシーオブジェクトの名前を含む項目を直接入力するか、[選択（Select）] をクリックしてリストからポリシーオブジェクトを選択するか、新しいオブジェクトを作成できます。

[Edit Signature Parameters] ダイアログボックスの詳細については、[Edit Signature Parameters] ダイアログボックス （2198 ページ）を参照してください。

ステップ 5 必要に応じて設定を変更してから、[OK] をクリックし変更を保存します。[Edit Signature] ダイアログボックスに戻ります。

ステップ 6 [シグネチャの編集（Edit Signature）] ダイアログボックスで、[OK] をクリックしてシグネチャへの変更を保存します。

ヒント 編集内容で望ましい効果が得られなかった場合、または編集を誤った可能性がある場合は、[シグネチャの編集（Edit Signature）] ダイアログボックスで [デフォルトの復元（Restore Defaults）] ボタンをクリックして、変更内容を消去できます。その後、もう一度やり直すことができます。

[Edit Signature Parameters] ダイアログボックス

[Edit Signature Parameters] ダイアログボックスを使用して、特定のシグニチャの組み込みマイクロエンジンパラメータを編集（調整とも呼びます）します。エンジンが異なると、そのパラメータも異なるため、[Edit Signature Parameters] ダイアログボックスの表示は変化します。シグネチャ パラメータの編集の詳細については、シグニチャ パラメータの編集（シグニチャの調整） （2196 ページ）を参照してください。

[Edit Signature Parameters] ダイアログボックスは、フォルダ ツリー構造を保持しています。左側のツリーにはパラメータ名が表示され、右側にはパラメータの値が表示されます。

変更できる値には、名前の部分に小さなボックスがあります。これはチェックボックスです。チェックボックスが空の場合、パラメータのデフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。（フィールドを編集すると、通常ボックスにチェック マークが追加されます）。

パラメータを変更するには、右側の対象フィールドをクリックします。パラメータをクリックした場合の動作は、パラメータ タイプによって異なります。

- 読み取り専用のパラメータ：多くのパラメータは読み取り専用で変更できません（シグネチャ ID など）。これらのパラメータをクリックしても通常無効になります。ただし、パラメータ リストでは、ダイアログボックスが開きます（[Obsoletes] リストなど）。
- テキストまたは数値のパラメータ：英数字または数字の値を入力する必要があるパラメータをクリックすると、フィールドは編集ボックスになります。目的の値を入力し、Enter キーを押すか、または編集ボックスの外側をクリックします。
- 事前に定義された値のパラメータ：多くのパラメータには、数個の選択できる値があります（[Yes]/[No] など）。これらのパラメータをクリックすると、ドロップダウン リストがアクティブになります。目的のオプションを選択し、フィールドの外側をクリックします。
- リストのパラメータ：項目のリストを保持しているパラメータもあります。これらのパラメータでは、パラメータ値に [Set] または [List] などの単語と鉛筆アイコンが表示されます。フィールド内をクリックすると、ダイアログボックスが開き、項目に関連するリストを設定できます。例としては、Meta エンジン コンポーネントのリストがあります。詳細については、Meta エンジン シグネチャのコンポーネント リストの編集 （2205 ページ）を参照してください。
- 変数パラメータ：ポリシー オブジェクトを選択して、パラメータの内容を指定できるパラメータもあります。たとえば、一部のシグネチャ エンジンでは、ポート リスト オブジェクトを選択して、ポートを指定できます。これらのパラメータをクリックすると、[Select] ボタンのついた編集ボックスが表示されます。編集ボックスにポリシー オブジェクトの名前を含む項目を直接入力するか、[選択（Select）] をクリックしてリストからポリシー オブジェクトを選択するか、新しいオブジェクトを作成できます。

ナビゲーション パス

[シグネチャの編集（Edit Signature）] ダイアログボックスまたは [カスタム シグネチャの追加（Add Custom Signature）] ダイアログボックスから、[パラメータの編集（Edit Parameters）] ボタンをクリックします。これらのダイアログボックスを開く方法については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （2186 ページ）を参照してください。

ヒント　ボタンがアクティブでない場合、最初に [Source Policy] フィールドから [Local] または共有ポリシーの名前を選択するか、シグネチャを複製しカスタム ポリシーを作成する必要があります。[Local] オプションはデバイス ビューのみで使用可能です。このオプションでは、変更内容を編集中のデバイスに適用し、その他のデバイスには適用しません。共有ポリシーの名前を選択した場合、変更内容はポリシーが割り当てられているすべてのデバイスに適用されます。

フィールド リファレンス

表 *524 : [Edit Signature Parameters]* ダイアログボックス

要素	説明
Tuning Context （ポリシー ビューだけ）	特定のシグニチャ ポリシーのシグニチャ パラメータが編集された（調整された）方法を一意に示すために、Security Manager が必要とする情報を表示します。[Tuning Context] フィールドは、次の項目が含まれている文字列です。 • [コンテキスト（Context）] : マイクロエンジンを一意に定義するために、Security Manager サーバーによって提供される識別情報。 • [SigLevel]（IPS）または [バージョン（Version）]（IOS IPS）：IPS ポリシーの場合、シグニチャマイクロエンジンの定義が適用されるシグニチャ更新レベルの範囲を示します。IOS IPS の場合、IOS IPS バージョンを示します。 • [エンジン（Engine）] : IPS エンジンの名前。 **ヒント** 例として、[Tuning Context] フィールドには、Context:9、SigLevel:302-449、Engine:atomic-ip の文字ストリングを含めることができます。 [Tuning Context] フィールドには、すべてのシグネチャ ポリシーに対して、それぞれ 1 つ以上のチューニング コンテキストを含めることができます。 • 最も高いシグネチャレベルのチューニングコンテキストには、「Reference context」が先頭に追加されます。 • 「Reference context」が先頭に追加された共有ポリシーを変更する場合、Security Manager から、ポリシーを他の適用可能なコンテキストにコピーするかどうかを尋ねられる場合があります（特定のデバイスが、複数のコンテキストで表示される場合があります）。 • ポリシーを他の適用可能なコンテキストにコピーすることを選択した場合、コピーできないパラメータがある場合はエラー メッセージが表示されます。 **（注）** Security Manager 4.1 から、（導入されている一番低いシグネチャレベルより古いシグネチャとして定義される）古いシグネチャバージョンは、データベースの最適化を目的とする定期的な削除操作によって削除されます。結果として、一部の未使用のチューニング コンテキストが削除されることに注意してください。

要素	説明
シグネチャ ID	このシグニチャに割り当てられた一意の数値。この値により、センサーは特定のシグニチャを識別します。 値は 1000 ～ 65000 です。
サブシグニチャ ID	このサブシグニチャに割り当てられた一意の数値。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。 値は 0 ～ 255 です。
Promiscuous Delta	無差別モードでの動作時におけるアラートの重大度を変更します。値は、アラートの全体的なリスクレーティングから除外されます。インラインモードでの動作時は、[Promiscuous Delta] は無視されます。指定できる値の範囲は、0 ～ 30 です。
Sig Description	シグネチャを他のシグネチャとシグネチャを識別するために役立つシグネチャの説明。 • [Alert Notes]：アラート メッセージに含まれる、シグニチャに関する追加情報。 • [User Comments]：シグニチャに関するコメント。 • [Alarm Traits]：このシグニチャについて文書化する特性。値は 0 ～ 65535 です。デフォルトは 0 です。 • [Release]：シグニチャが最後に更新されたリリース。 • [Signature Creation Date]：シグネチャが作成された日付。 • [Signature Type]：シグネチャのタイプ（[Anomaly]、[Component]、[Exploit]、[Vulnerability] または [Other]）。
エンジン	このシグニチャによって指定されたトラフィックの解析と検査を行うエンジンを示します。エンジンは、Engines フォルダで使用可能なパラメータを決定します。エンジンの詳細については、エンジンのオプション（2192 ページ）を参照してください。 各エンジンに関する詳細情報と使用可能なパラメータについては、ご使用の IPS ソフトウェアリリースに対応したCisco Intrusion Prevention System Device Manager のインストールおよび使用法ガイド [英語] の「Signature Engines」セクションを参照してください。 **ヒント** 多くのエンジンには、[Fragment Status] パラメータが含まれています。このパラメータによって、パケット フラグメントを検査する必要があるかどうかを指定できます。フラグメントを検査するかしないか、またはシグネチャをすべてのパケット ステータスに適用するかを選択できます。

要素	説明
Event Counter	センサーがイベントをカウントする方法。たとえば、センサーが、同じシグニチャが同じアドレスセットに対して5回起動した場合にだけアラートを送信するように指定できます。次の値を設定します。 • [Event Count]：アラートを生成するまでのイベントの発生回数。値は 1 ～ 65535 です。デフォルトは 1 です。 • [Event Count Key]：シグニチャのイベントをカウントするために使用されるストレージ タイプ。攻撃者のアドレス、攻撃者のアドレスと攻撃対象のポート、攻撃者と攻撃対象のアドレス、攻撃者と攻撃対象のアドレスおよびポート、または攻撃対象のアドレスを選択します。デフォルトは、攻撃者のアドレスです。 • [アラート間隔の指定（Specify Alert Interval）]：イベントカウントをリセットするアラート間の時間を指定するかどうかを示します（[はい（Yes）] または [いいえ（No）]）。[はい（Yes）] を選択した場合は、時間を秒単位で入力します（2 ～ 1000）。
Alert Frequency	シグニチャが起動した場合に、センサーがアラートを送信する回数。シグニチャに対して次のパラメータを指定します。以下に、パラメータの説明を記載します。 • Summary Mode • Summary Interval • Summary Key • Specify Global Summary Threshold

要素	説明
Summary Mode （[Alert Frequency] グループ）	アラートのサマライズのモード。Fire All、Fire Once、Summarize、および Global Summarize という 4 つのモードがあります。サマリー モードは、現在のアラート量に応じて動的に変わります。たとえば、シグニチャを Fire All に設定できますが、一定のしきい値に達するとサマライズが開始されます。選択したサマリー モードによって、[Summary Mode] グループで使用可能な他のパラメータの種類を制御します。 • [Fire All]：すべてのイベントについてアラートを起動します。 • [Fire Once]：1 回だけアラートを起動します。 • [Summarize]：アラートをサマライズします。 • [Global Summarize]：攻撃者や攻撃対象の数に関係なく 1 回だけアラートが起動されるようにアラートをサマライズします。 （注） ASA デバイスの複数のコンテキストが 1 つの仮想センサーに含まれている場合、サマリーアラートには、サマライズされた最後のコンテキストのコンテキスト名が含まれています。このため、このサマリーは、サマライズされるすべてのコンテキストのうち、このタイプのすべてのアラートの結果となります。
Specify Summary Threshold （[Summary Mode] グループ）	[Fire All] を選択すると、デバイスがサマリー モードに動的に変化した場合に使用されるサマリーのしきい値の設定値を設定するかどうかを選択できます。[Yes] を選択した場合、サマリー間隔、サマリー キー、またはグローバルなサマリーのしきい値を設定できます。
Summary Interval （[Summary Mode] グループ）	各サマリー アラートで使用される時間間隔（秒数）。値は 1 ～ 65535 です。デフォルトは 15 です。
Summary Key （[Summary Mode] グループ）	アラートのサマライズに使用されるストレージ タイプ。攻撃者のアドレス、攻撃者のアドレスと攻撃対象のポート、攻撃者と攻撃対象のアドレス、攻撃者と攻撃対象のアドレスおよびポート、または攻撃対象のアドレスを選択します。デフォルトは、攻撃者のアドレスです。
Specify Global Summary Threshold （[Summary Mode] グループ）	アラートをグローバルサマリーにサマライズするための、イベントのしきい値を指定するかどうかを示します（[はい（Yes）] または [いいえ（No）]）。[はい（Yes）] を選択した場合は、イベントのしきい値を入力します（1 ～ 65535）。デフォルトは 240 です。

要素	説明
ステータス	シグネチャの状態。 [Obsoletes] リストでは、このシグネチャで使用されていないシグネチャが表示されます。鉛筆アイコンをクリックして、リストを開きます。ほとんどの場合、この情報は読み取り専用です。リストを変更できる場合は、パラメータ フィールド内の [Set] をクリックして、リストを開きます。このリストでは、使用されていないシグネチャ ID を追加できます。
Vulnerable OS List	攻撃者がターゲットとしているオペレーティング システムのリスト。
MARS Category	シグニチャが属している、Cisco Security MARS でのカテゴリ。このメタデータを使用して、MARS が学習したイベント カテゴリに関連するシグニチャを処理するために必要なデータを MARS に提供するように生成されたイベントを特徴付けます。
[すべてを展開（Expand All）] ボタン	すべてのカテゴリおよびサブカテゴリを展開します。
[すべて折りたたみ（Collapse All）] ボタン	このカテゴリのすべてのフィールドを折りたたみます。

Meta エンジン シグネチャのコンポーネント リストの編集

[Edit Signature Parameter - Component List] ダイアログボックスを使用して、Meta エンジン シグネチャのコンポーネント リストを編集します。

Meta エンジンでは、スライディング時間間隔内に、関連した方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。シグニチャ イベントが生成されると、Meta エンジンはシグニチャ イベントを検査して、1 つ以上の Meta 定義に一致するかどうかを判定します。Meta エンジンは、すべてのイベント要件が満たされるとシグニチャ イベントを生成します。

すべてのシグニチャ イベントは、シグニチャ イベント アクション プロセッサによって Meta エンジンに渡されます。シグニチャ イベント アクション プロセッサは、最小ヒット数オプションを処理してからイベントを渡します。Meta エンジンがコンポーネント イベントを処理してから、サマライズおよびイベント アクションは処理されます。

Meta エンジンは、ほとんどのエンジンがパケットを入力としているにもかかわらず、アラートを入力としている点が他のエンジンとは異なります。このため、Meta エンジン シグネチャでは、Meta シグネチャの検索対象となるシグネチャを指定する必要があります。このシグネチャのリストは、[Component List] に含まれています。

[Component List] は、シグネチャ パラメータの一部です。パラメータを編集するには、シグニチャ パラメータの編集（シグニチャの調整） （2196 ページ）で説明した手順に従ってください。Meta エンジンを使用するシグネチャの [シグニチャパラメータの編集（Edit Signature

Parameters）] ダイアログボックスを開いて、**[エンジン（Engine）] > [コンポーネントリスト（Component List）]** パラメータを確認してください。パラメータ値には、鉛筆アイコンと単語 [List] が含まれています。[リスト（List）] をクリックして、[シグネチャパラメータの編集 - コンポーネントリスト（Edit Signature Parameter - Component List）] ダイアログボックスを開きます。

ダイアログボックスは、非アクティブ リスト（左側）とアクティブ リスト（右側）の 2 つのリストに分けられます。アクティブ リストは、Meta エンジン シグネチャが検索するシグネチャを定義します。

コンポーネント リストを変更するには、次の手順を実行します。

- 新しいコンポーネントの追加：非アクティブリストの左側にある [エントリの追加（Add Entry）]（+）ボタンをクリックします。[Add Signature Parameter -List Entry] ダイアログボックスが開きます。次の値を設定します。
  - [エントリキー（Entry Key）]：コンポーネントの名前。
  - [コンポーネントのシグネチャID（Component Sig ID）]：検索するシグネチャのシグネチャ ID。
  - [コンポーネントのサブシグネチャID（Component SubSig ID）]：サブシグネチャ ID。サブシグネチャが存在しない場合は、0 を入力します。
  - [コンポーネントカウント（Component Count）]：Meta シグネチャがトリガーされるまでにシグネチャが起動する回数。
  - [コンポーネントではない（Is a Not Component）]：このフィールドでは、ネガティブ エントリを作成できます。これにより、起動させるシグネチャと起動させないシグネチャのリストを指定できます。起動させるシグネチャには[いいえ（No）]を選択し、起動させないシグネチャには [はい（Yes）] を選択します。

[シグネチャパラメータの追加 - エントリのリスト（Add Signature Parameter - List Entry）] ダイアログボックスで [OK] をクリックすると、新しいコンポーネントが非アクティブリストに追加されます。新しいコンポーネントを選択し、[>>] ボタンをクリックしてアクティブ リストに移動します。次に、上下の矢印ボタンを使用して、アクティブ コンポーネント リストでのコンポーネントの位置を移動します。3 つめのボタンを使用して、コンポーネントの順番を前回保存した順番にリセットできます。

- 既存のコンポーネントの編集：（いずれかのリストで）コンポーネントを選択して、リストの間にある [エントリの編集（Edit Entry）]（鉛筆）ボタンをクリックします。[Edit Signature Parameter - List Entry] ダイアログボックスが開きます。コンポーネント名を変更できないこと以外は、パラメータは新しいエントリの追加と同様です。
- コンポーネントの削除：非アクティブリストのコンポーネントを選択し、非アクティブリストの左側にある [エントリの削除（Delete Entry）]（ゴミ箱）ボタンをクリックします。アクティブ コンポーネントを削除する場合、最初にアクティブ リストでアクティブ コンポーネントを選択し、[<<] ボタンをクリックして、非アクティブ リストに移動します。

- デフォルトの復元：コンポーネントのデフォルト値を復元する場合、コンポーネントを選択し、[復元（Restore）] をクリックします。

[Obsoletes] ダイアログボックス

[Obsoletes] ダイアログボックスを使用して、特定のシグニチャに関連付けられている古いシグニチャを識別します。ほとんどの場合、この情報は読み取り専用です。場合によっては、読み書き可能になります。たとえば、ローカル シグネチャまたは共有ポリシー固有のシグネチャにおける IOS IPS シグネチャ ポリシーのリストを編集できます。

リストを編集できる場合は、次の作業が実行できます。

- [エントリの追加（+）（Add Entry (+)）] ボタンをクリックして、編集中のシグネチャで使用されていないシグネチャのシグネチャ ID およびサブシグネチャ ID を追加します。
- エントリを選択し、[エントリの削除（ゴミ箱）（Delete Entry (trash can)）] ボタンをクリックして、使用されていないシグネチャのリストからエントリを削除します。

ナビゲーション パス

[Obsoletes] リストは、シグネチャ パラメータの一部です。パラメータを編集するには、シグニチャ パラメータの編集（シグニチャの調整） （2196 ページ）で説明した手順に従ってください。[シグネチャパラメータの編集（Edit Signature Parameters）] ダイアログボックスを開いて、[ステータス（Status）]>[廃止（Obsoletes）] パラメータを確認してください。パラメータ値には、鉛筆アイコンと単語 [Set] が含まれています（パラメータが読み取り専用でない場合）。鉛筆アイコンまたは単語をクリックして、[Obsoletes] ダイアログボックスを開きます。

シグニチャの設定値の設定

[Signature Settings] ページを使用して、IPS アプライアンスとサービス モジュール（Cisco IOS IPS デバイスを除く）の設定値を定義します。これらの設定値では、次のポリシーを定義します。

- **アプリケーション ポリシー**：HTTP をイネーブルまたはディセーブルにし、HTTP 要求の最大数を決定および指定し、AIC Web ポートを指定して、FTP をイネーブルまたはディセーブルにします。
- **フラグメント再構築ポリシー**：IP 再構築モードを選択して、複数のパケットにわたってフラグメント化されたデータグラムを再構築するように、センサーを設定します。
- **ストリーム再構築ポリシー**：TCP ハンドシェイクを必須とするかどうかを指定し、TCP 再構築モードを選択して、完全なスリーウェイハンドシェイクによって確立された TCP セッションだけをモニターするように、センサーを設定します。
- **IP ロギングポリシー**：許可される最大ログパケット数、IP ログ時間、および許可される最大 IP ログサイズを決定および選択して、センサーが攻撃を検出したときに IP セッション ログを生成するように、センサーを設定します。

ヒント　これらのすべての設定には、デフォルト値が存在します。このため、デフォルト以外の値を使用する必要がある場合のみ、このポリシーを設定してください。

Signature Settings ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [設定（Settings）]** を選択します。
- （ポリシービュー）**[IPS] > [シグネチャ（Signatures）] > [設定（Settings）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

その後、次の表で説明するオプションを設定できます。

表 *525 : [Signature Settings]* ページ

要素	説明
HTTP の有効化	Webサービスの保護をイネーブルにします。RFCに準拠するために、センサーで HTTP トラフィックを検査する必要がある場合は、[はい（Yes）] を選択します。
Max HTTP Requests	各接続の未処理の HTTP 要求の最大数。
AIC Web Ports	AICトラフィックを検索するポート。ポート番号またはポートを定義するポート リスト オブジェクトのカンマ区切りのリストを入力します。[選択（Select）]をクリックしてリストからポートリストオブジェクトを選択するか、新しいオブジェクトを作成できます。
Enable FTP	FTP サービスの保護をイネーブルにします。センサーで FTP トラフィックを検査する必要がある場合は、[はい（Yes）]を選択します。
IP Reassembly Mode	オペレーティング システムに基づいて、センサーがフラグメントの再構築に使用する方式。
TCP Handshake Required	センサーが、スリーウェイ ハンドシェイクが実行されたセッションだけを追跡するかどうかを示します。

要素	説明
TCP Reassembly Mode	センサーが、次のオプションを使用する TCP セッションの再構築に使用するモード。 • [Asymmetric]：双方向トラフィック フローのいずれかの方向だけをモニタします。 （注） Asymmetric モードの場合、センサーは状態をフローと同期し、双方向を必要としないエンジンの検査を継続します。完全な保護には双方向のトラフィックを確認する必要があるため、Asymmetric モードではセキュリティが低下します。 • [Loose]：パケットがドロップされる可能性がある場合に使用します。 • [Strict]：何らかの理由でパケットが失われた場合、失われたパケット以降のすべてのパケットが処理されなくなります。
Max IP Log Packets	記録するパケットの数。
IP Log Time	センサーが記録する期間（1 ～ 60 分）。デフォルトは 30 分です。
Max IP Log Bytes	記録する最大バイト数。

第 40 章

イベント アクション ルールの設定

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

IPSイベントは、アラート、ブロック要求、ステータスメッセージ、またはエラーメッセージを含むIPSメッセージです。イベントアクションは、イベントに対するセンサーの応答です。イベントがフィルタリングされていない場合にだけ発生します。指定可能なイベントアクションは、TCP リセット、ホストのブロック、接続のブロック、IP ロギング、およびアラート トリガーパケットのキャプチャです。イベントアクションは、5.x よりも前の Cisco IPS バージョンではアラームと呼ばれていました。

IPS Event Actions フォルダで、センサーのイベント アクション処理コンポーネントの設定を指定します。これらの設定により、イベント検出時にセンサーが実行するアクションが定義されます。

（注） Security Manager の Event Action ポリシーに IPv6 アドレスは使用できません。Security Manager での IPv6 サポートの詳細については、Security Manager での IPv6 サポート （11 ページ）を参照してください。

この章は次のトピックで構成されています。

- IPS イベント アクション プロセスについて （2212 ページ）
- IPS イベント アクションについて （2213 ページ）
- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション オーバーライドの設定 （2227 ページ）
- IPS イベント アクション ネットワーク情報の設定 （2233 ページ）
- イベント アクションの設定 （2242 ページ）

IPS イベント アクション プロセスについて

IPS イベントアクションルールは、イベント発生時にセンサーが実行するアクションを指示します。各シグニチャには実行される特定のアクションが設定されますが、実際に実行されるアクションはその他の要因にも依存します。

検査でシグニチャ イベントが識別されたときに実行される一般的なプロセスは次のとおりです。

1. シグニチャで指定されたアクションで、シグニチャ アラートが発生します。アラートのリスク レーティングが計算されます。

   リスクレーティングの計算方法の詳細については、Cisco.com で Cisco Intrusion Prevention System Device Manager 7.0 のインストールおよび使用法ガイド [英語] の「Calculating the Risk Rating」を参照してください。

   ターゲットの価値レーティングと OS マッピングを設定することにより、リスク レーティングに影響を与えることができます。IPS イベント アクション ネットワーク情報の設定（2233 ページ）を参照してください。

2. **イベント アクション オーバーライド** ポリシーが処理されます。イベントのリスクレーティングがオーバーライドルールと一致すると、オーバーライドルールで識別されたアクションがシグネチャで定義されているアクションに**追加**されます。オーバーライドは、シグニチャで指定されているアクションに置き換わりません。

   オーバーライドの設定方法の詳細については、イベント アクション オーバーライドの設定 （2227 ページ）を参照してください。

3. **イベント アクション フィルタ ポリシー**が処理されます。ルールがイベントに適用されると、ルールによってイベントからアクションが**取り除かれます**。このため、シグニチャ ポリシーまたはオーバーライド ルールに追加したアクションが、フィルタ ルールのいずれかによって削除されることがあります。

   フィルタ ルールの作成の詳細については、イベントアクション フィルタの設定 （2216 ページ）を参照してください。

4. イベントアクションの設定 （2242 ページ）で示すようにサマライズ機能をオフにしていないかぎり、イベントのサマライズが発生します。

5. アクションが実行されます。指定可能なアクションの説明については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （2181 ページ）を参照してください。

6. 拒否された攻撃者のリストが保持され、指定可能な設定に基づいて後続のアクセスが防止されます。デフォルト設定を変更する手順については、イベントアクションの設定 （2242 ページ）を参照してください。

IPS イベント アクションについて

イベント アクション フィルタやオーバーライド、またはシグニチャの設定時に、ルールを満たしているイベントのアクションを指定します。シグニチャおよびオーバーライドの場合は、イベントに追加するアクションを指定します。フィルタの場合は、イベントから削除するアクションを指定します。

最も一般的なアクションは Produce Alert で、このアクションでは、Security Manager Event Viewer または CS MARS のようなネットワーク管理システムで参照できるアラートが生成されます。ただし、イベントに割り当て可能なアクションは非常に多様です。指定可能なアクションを調べる場合には、次の点に注意します。

- 多数のアクションで、実行される他のアクションに加えて、アラートが作成されます。各アクションの説明には、アラートが作成されるかどうかが記載されています。
- Cisco IOS IPS では、イベント アクション オーバーライドまたはフィルタ ルールに対して少数のアクションしかサポートされません。サポートされるアクションは、Deny Attacker Inline、Deny Connection Inline、Deny Packet Inline、Product Alert、および Reset TCP Connection です。
- 必ずしも、IPS ソフトウェア バージョンおよびデバイス タイプのすべての組み合わせで、すべてのアクションを使用できるわけではありません。アクションを選択する必要がある場合は常に、有効なアクションだけが選択可能になります。
- 拒否およびブロック アクションの場合は、イベント アクション設定ポリシーを使用して、アドレスまたはパケットが拒否される期間を設定します。詳細については、イベント アクションの設定 （2242 ページ）を参照してください。

次の表に、指定可能なアクションの説明を示します。

表 *526 : IPS* イベント アクション

メニュー コマンド	説明
Deny Attacker Inline	指定された期間、この攻撃者のアドレスからの、現在のパケットおよび将来のパケットを終了します。 IPS は、インライン モードで動作している必要があります。 Cisco IOS IPS デバイスの場合、遮断時間が経過するまで攻撃者からルータへの接続は確立されません。 **ヒント** これは最も厳しい拒否アクションです。単一の攻撃者アドレスからの現在および将来のパケットが拒否されます。IPS アプライアンスおよびサービス モジュールの場合、IPS Device Manager を使用すると、拒否された攻撃者のリストを表示したり、必要に応じてリストをクリアしたりできます。

メニュー コマンド	説明
Deny Attacker/Service Pair Inline	指定された期間、この攻撃者のアドレスと攻撃対象のポートのペアについては、現在のパケットおよび将来のパケットを送信しません。 IPS は、インライン モードで動作している必要があります。
Deny Attacker/Victim Pair Inline	指定された期間、この攻撃者と攻撃対象のアドレスのペアについては、現在のパケットおよび将来のパケットを送信しません。 IPS は、インライン モードで動作している必要があります。
Deny Connection Inline	TCP フローの現在のパケットおよび将来のパケットを終了します。攻撃者からのその他の接続は確立されます。 IPS は、インライン モードで動作している必要があります。
Deny Packet Inline	パケットを終了します。 IPS は、インライン モードで動作している必要があります。 Cisco IOS IPS デバイスの場合、このアクションにより、リセットを送信しないでパケットが廃棄されます。「drop と reset」はアラームとともに使用することを推奨します。 **ヒント** IPS アプライアンスおよびサービス モジュールの場合、このアクションを高リスク イベントに追加するイベント アクション オーバーライドがあります。このオーバーライドは削除できません。使用しない場合は、オーバーライドをディセーブルにします。詳細については、イベント アクション オーバーライドの設定 （2227 ページ）を参照してください。
Log Attacker Packets	攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
Log Pair Packets	攻撃者と攻撃対象のアドレスのペアが含まれているパケットに対する IP ロギングを開始します。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
Log Victim Packets	攻撃対象のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。

メニュー コマンド	説明
Modify Packet Inline	エンドポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。 ヒント　このオプションは、イベント アクション オーバーライドまたはフィルタ ルールでは使用できません。シグニチャでは使用できます。
Product Alert	イベントをアラートとしてイベント ストアに書き込みます。Cisco IOS IPS デバイスの場合、syslog または SDEE を介して通知が送信されます。 （注）　Produce Alert イベント アクションは、グローバル相関によってイベントのリスク レーティングが増加し、Deny Packet Inline または Deny Attacker Inline のいずれかのイベント アクションが追加されたときに、イベントに追加されます。
Produce Verbose Alert	攻撃パケットの符号化されたダンプをアラートに含めます。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
Request Block Connection	この接続をブロックする要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。詳細については、IPS のブロッキングおよびレート制限の設定 （2282 ページ）を参照してください。
Request Block Host	この攻撃者ホストをブロックする要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。
Request Rate Limit	レート制限を実行するレート制限要求を送信します。レート制限デバイスは、このアクションを実行するように設定されている必要があります。
Request SNMP Trap	センサーが設定済みのトラップ宛先に SNMP トラップ通知を送信することを要求します。このアクションを実行すると、Produce Alert が選択されていない場合でも、アラートが書き込まれます。トラップが実際に送信されるようにするには、センサーに SNMP を設定しておく必要があります。詳細については、SNMP の設定 （2092 ページ）を参照してください。
TCP 接続のリセット	TCP リセットを送信して、TCP フローをハイジャックし、終了します。リセットは、発信元アドレスと宛先アドレスの両方に送信されます。Reset TCP Connection は、ハーフオープン SYN 攻撃などの単一の接続を分析する TCP シグニチャでだけ機能します。スイープまたはフラッドに対しては機能しません。

関連項目

- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション オーバーライドの設定 （2227 ページ）
- シグニチャの設定 （2169 ページ）

イベント アクション フィルタの設定

特定のアクションをイベントから削除するか、または、イベント全体を破棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。

フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありません。フィルタは、イベントからアクションを削除することで機能します。1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。フィルタ ルールを設定する前に、イベント アクション フィルタ ルールの管理に関するヒント （2218 ページ）を参照してください。

（注） スイープ シグニチャをフィルタリングする場合は、宛先アドレスをフィルタリングしないことを推奨します。複数の宛先アドレスがある場合、最後のアドレスだけがフィルタとの照合に使用されます。

関連項目

- IPS イベント アクションについて （2213 ページ）

ステップ 1 次のいずれかを実行して、Event Action Filters ポリシーを開きます。

- （デバイス ビュー）ポリシー セレクタから [IPS] > [イベント アクション（Event Actions）] > [イベント アクション フィルタ（Event Action Filters）] を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）[IPS] > [イベント アクション（Event Actions）] > [イベント アクション フィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）[IPS（ルータ） （IPS (Router)）] > [イベント アクション（Event Actions）] > [イベント アクション フィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

テーブルに、セクションごとに分類された既存のフィルタ ルールが表示されます。[Local] セクションは、（デバイス ビューで）選択したデバイスに定義されているルール用のセクションです。共有または継承されたポリシーの場合、必須ルールおよびデフォルト ルール用のセクションもあります。このポリシーの内容の詳細については、 [Event Action Filters] ページ （2219 ページ）を参照してください。

ステップ 2 フィルタルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。この操作により、[Add Filter Item] ダイアログボックスが開きます。このダイアログボックスのオプションの詳細については、[Add Filter Item]/[Edit Filter Item] ダイアログボックス （2222 ページ）を参照してください。

ヒント

- 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。
- 既存の行を選択して、行全体（[行の編集（Edit Row）] ボタンをクリックする）または特定のセルを編集することもできます。特定のセルを編集するには、セルを右クリックして、コンテキストメニューの一番上からそのセルに関連する**編集**コマンドを選択します。
- ルールを選択して [行の削除（Delete Row）] ボタンをクリックすると、そのルールを削除できます。
- フィルタ ルールのリスト全体を Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートできます。[ファイルへのエクスポート（Export to File）] をクリックして Security Manager サーバーの適切なフォルダにナビゲートし、デフォルト名を使用しない場合はファイル名を変更して [保存（Save）] をクリックします。

ステップ 3 フィルタ ルールを設定します。一般的に設定が必要な重要項目は次のとおりです。フィールドの設定に関する詳細およびここで説明していないフィールドの情報については、[Add Filter Item]/[Edit Filter Item] ダイアログボックス （2222 ページ）を参照してください。

- [Name]：ルールの名前を入力する必要があります。意味のある名前を使用してください。
- [Signature, Subsignature ID]：フィルタをすべてのシグニチャに適用する必要がある場合は、デフォルト値を使用します。特定のシグニチャをターゲットにする場合は、そのシグニチャおよびサブシグニチャの ID を入力します。これらの値は、シグニチャ ポリシーでシグニチャを検索することで取得できます（[Signatures] ページ （2169 ページ）を参照）。
- [Attacker and Victim Addresses and Ports]：だれが攻撃しているのか、または攻撃対象はだれかに関係なくフィルタを適用する必要がある場合は、デフォルト値を使用します。攻撃者または攻撃対象に固有のフィルタを作成する場合は、適切なアドレスおよびポートと一致するようにこれらのフィールドを更新します。
- [Risk Rating]：この値は、多くの場合変更が必要です。フィルタは、ここで設定した最小～最大範囲内のイベントに適用されます。デフォルト値（0-100）を指定すると、すべてのイベントにフィルタ ルールが適用されます。特定のシグニチャ ID を設定した場合、レーティングはそのシグニチャのイベントにだけ適用されます（この場合、デフォルトのリスク レーティングをそのまま使用できることがあります）。

たとえば、90 ～ 100 などの高リスク イベントだけをターゲットにできます。

- [Actions to Subtract]：イベントから除外するアクションを選択します。複数のアクションを選択するには、Ctrl を押しながらクリックします。実際にはイベントに割り当てられていないアクションを選択した場合、フィルタ ルールは基本的にはイベントに何の影響も与えません。アクションの詳細については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （2181 ページ）を参照してください。

- [Stop on Match]：このフィルタ ルールを停止ルールとして定義するかどうかを指定します。この設定によって、イベント アクション フィルタ ルール テーブルに残っているルールを処理する方法が決まります。
  - このオプションを選択し、イベントがルールの条件を満たす場合、このルールは、イベントに対してテストされる最後のルールとなります。このルールによって識別されたアクションはイベントから削除され、デバイスは、イベントに割り当てられている残りのすべてのアクションを実行します。
  - このオプションを選択していない場合、このフィルタ ルールの条件を満たすイベントも、イベント アクション フィルタ テーブル内の後続のルールと比較されます。後続のルールは、すべてのルールがテストされるか、またはイベントが停止ルールに一致するまでテストされます。

フィルタルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。停止ルールが、停止よりも前に適用させる他のルールのあとに配置されていることを確認します。

イベント アクション フィルタ ルールの管理に関するヒント

次に、イベント アクション フィルタ ルールを効果的に管理するために役立つヒントを示します。

- ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。ルールのイネーブル/ディセーブルステータスを変更するには、ルールを右クリックし、[有効化（Enable）] または [無効化（Disable）] を必要に応じて選択します。ルールの編集時にステータスを変更することもできます。

ルールを使用停止にする場合はルールをディセーブルにするのが有効ですが、将来、そのルールの使用を再開する可能性があります。ルールを再作成しなくて済むように、ディセーブルにしたルールはそのままテーブル内に保持されます。

- 既存のルールの場合、セルを右クリックしてコンテキストメニューの一番上の部分から適切な編集コマンドを選択することで、イベント アクション フィルタ ルール テーブルから直接フィールドの大部分を編集できます。たとえば、[攻撃者のポート（Attacker Ports）] セルを右クリックし、[攻撃者のポートの編集（Edit Attacker Ports）] を選択します。

これらの右クリック コマンドの多くが、選択したプロパティだけを含む [Edit Filter Item] ダイアログボックスのバージョンです。その他のコマンドは値を変更するだけか、あるいは追加または削除する値を選択するためのサブメニューを開きます。たとえば、[Action] セルを右クリックすると、次の 4 つのコマンドが表示されます。

- [アクションに追加（Add to Actions）]：アクションのリストからアクションを選択して、すでにルールに定義されているアクションに追加します。

- [アクションから削除（Delete from Actions）]：ルールに定義されているアクションのリストからアクションを選択して、ルールから削除します。
- [アクションを置換（Replace Actions With）]：アクションのリストからアクションを選択して、ルールに定義されているアクションを完全に置き換えます。
- [アクションの編集（Edit Actions）]：ルールのすべてのアクションを選択できるダイアログボックスが開きます。選択した内容でセルの内容が置き換わります。
- フィルタルールは順序リストとして設定されますが、ルールは上から下へ順に処理および適用されるものの、「最初に一致したもの勝ち」リストとして処理されるわけではありません。各ルールには Stop プロパティがあり、ルールは停止ルールであるか停止ルールでないかのどちらかになります。処理は、イベントが停止ルールと一致した場合にだけ終了します。イベントが非停止ルールと一致した場合、そのイベントは後続のフィルタ ルールと比較されます。このように、複数のフィルタ ルールを 1 つのイベントに適用できます。停止ルールを作成する場合は、イベントに対して処理される他のすべてのルールの下に停止ルールを配置するようにします。

停止ルールを定義しなかった場合、各イベントがすべてのフィルタ ルールと比較され、一致したすべてのルールが上から下に順にイベントに適用されます。

- イベント アクション フィルタ ルール ポリシーは、継承が可能です。そのため、すべてのデバイスで共有するフィルタ ルールが含まれる共有ポリシーをポリシー ビューで設定し、（デバイス ビューで）そのルールを各デバイスに継承させ、デバイス ビューで各デバイスに固有のローカル フィルタ ルールを設定することが可能です。ポリシーを継承する方法の詳細については、次を参照してください。
  - 新しい共有ポリシーの作成 （278 ページ）
  - 継承と割り当て （216 ページ）
  - ルールの継承または継承の解除 （269 ページ）

関連項目

- イベント アクション フィルタの設定 （2216 ページ）
- [Event Action Filters] ページ （2219 ページ）

[Event Action Filters] ページ

[Event Actions Filters] ページを使用して、イベント アクション フィルタ ルールを設定します。フィルタ ルールでは、特定のアクションをイベントから削除することや、イベント全体を廃棄してセンサーによる今後の処理を回避することができます。

イベント アクション フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありませ

ん。フィルタは、イベントからアクションを削除することで機能します。1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。

イベント アクション フィルタ ルールを設定する前に、次の項を参照してください。

- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション フィルタ ルールの管理に関するヒント （2218 ページ）
- IPS イベント アクションについて （2213 ページ）

ヒント ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。ルールのイネーブル/ディセーブルステータスを変更するには、ルールを右クリックし、[有効化（Enable）] または [無効化（Disable）] を必要に応じて選択します。ルールの編集時にステータスを変更することもできます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [IPS] > [イベントアクション（Event Actions）] > [イベントアクションフィルタ（Event Action Filters）] を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）[IPS] > [イベントアクション（Event Actions）] > [イベントアクションフィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [イベントアクションフィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *527 : [Event Action Filters]* ページ

要素	説明
名前	フィルタ ルールの名前。
Active	シグニチャがアクティブかどうかを示します。 このセルは Cisco IOS IPS ポリシーでは使用できません。
ID（IDs）	このルールを適用するシグニチャ ID。
Subs	サブシグニチャ ID。

要素	説明
攻撃者（Attackers）	フィルタルールをトリガーする攻撃者の IP アドレスで、ホストアドレス、アドレス範囲（IPv4 の場合は 0.0.0.0-255.255.255.255 など、IPv6 の場合は ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF など）、またはネットワーク/ホストポリシーオブジェクトを指定できます。 **ヒント** ネットワーク/ホストオブジェクトを使用している場合は、そのオブジェクトを右クリックし、[コンテンツの表示（Show Contents）] を選択すると、そのオブジェクトの内容を表示できます。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。
Attack Ports	フィルタをトリガーする攻撃者ホストによって使用されるポート。
Victims	フィルタルールをトリガーする攻撃対象の IP アドレスで、ホストアドレス、アドレス範囲（IPv4 の場合は 0.0.0.0-255.255.255.255 など、IPv6 の場合は ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF など）、またはネットワーク/ホストポリシーオブジェクトを指定できます。 **ヒント** ネットワーク/ホストオブジェクトを使用している場合は、そのオブジェクトを右クリックし、[コンテンツの表示（Show Contents）] を選択すると、そのオブジェクトの内容を表示できます。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。
Victim Ports	フィルタをトリガーする攻撃者ホストによってターゲットにされるポート。
アクション（Actions）	フィルタがトリガーされたときに、イベントから削除する必要があるアクション。
RR	このイベントアクションフィルタをトリガーするリスク レーティング範囲。 リスクレーティングの計算方法の詳細については、Cisco.com で Cisco Intrusion Prevention System Device Manager 7.0 のインストールおよび使用法ガイド [英語] の「Calculating the Risk Rating」を参照してください。
停止（Stop）	これが停止ルールであるかどうかを指定します。[Yes] の場合、イベントがこのルールの条件を満たすと、フィルタがイベントに適用されますが、イベントはイベントアクションフィルタ ルール ポリシー内の残りのルールに対してはテストされません。

要素	説明
[Export to File] ボタン	イベント アクション フィルタ要約を Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートするには、このボタンをクリックします。Security Manager サーバ上のフォルダを選択し、ファイル名を指定するように要求されます。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内で上下に移動するには、これらのボタンをクリックします。 フィルタ ルールは、イベントごとに上から下に順に処理されます。イベントの条件がフィルタに定義されている条件と一致し、さらにフィルタの [Stop] フィールドが [Yes] に設定されている場合、そのフィルタは適用され、その他のフィルタは検討されません。停止ルールが、イベントに適用させる他のルールのあとに配置されていることを確認します。 テーブルでは、一般的なルールの前により限定的なルールを配置する必要があります。
[Add Row] ボタン	[Add Filter Item] ダイアログボックス（[Add Filter Item]/[Edit Filter Item] ダイアログボックス （2222ページ）を参照）を使用して選択したテーブルの行のあとにフィルタ ルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。セルを右クリックして適切な編集コマンドを選択する方法でも、個々のセルを編集できます。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。 **ヒント** ルールを削除する代わりに、ルールを右クリックして [無効化（Disable）] を選択できます。これにより、ルールは使用できなくなりますが、あとで再び使用する場合に備えてテーブル内に保持されます。

[Add Filter Item]/[Edit Filter Item] ダイアログボックス

[Add Filter Item]/[Edit Filter Item] ダイアログボックスを使用して、イベント アクション フィルタ ルールを設定します。

ヒント　既存のルールの場合、セルを右クリックしてコンテキスト メニューの一番上の部分から適切なコマンドを選択することで、イベント アクション フィルタ ルール テーブルから直接これらのフィールドの大部分を編集できます。たとえば、[攻撃者のポート（Attacker Ports）] セルを右クリックし、[攻撃者のポートの編集（Edit Attacker Ports）] を選択します。これらの右クリック コマンドの多くが、選択したプロパティだけを含む [Edit Filter Item] ダイアログボックスのバージョンです。これらのコンテキスト編集ダイアログボックスのヘルプを参照するには、下部のテーブル内でプロパティの説明を探します。

ナビゲーション パス

[イベントアクションフィルタ（Event Action Filters）] ページ（ [Event Action Filters] ページ（2219ページ）を参照）から、[列の追加（Add Row）]ボタンをクリックするか、またはルールをフィルタして、 [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- イベント アクション フィルタの設定 （2216 ページ）
- イベント アクション フィルタ ルールの管理に関するヒント （2218 ページ）

フィールド リファレンス

表 *528 : [Add Filter Item]/[Edit Filter Item]* ダイアログボックス

要素	説明
Active [有効（Enabled）] （[Active] は Cisco IOS IPS デバイスには適用されません）	フィルタ ルールがアクティブであるかどうか、およびイネーブルであるかどうかを示します。アクティブとは、フィルタがフィルタ リストに含まれており、イベントのフィルタリングで実行されることを意味します。デフォルトでは、ルールはアクティブかつイネーブルであり、このことはイベントが処理されるときにそのルールが使用されることを意味します。 ヒント • フィルタがアクティブだがイネーブルではない場合、そのフィルタは順序リストに含まれたままになります。つまり、処理されますが、使用されません。 • フィルタがアクティブではない場合、そのフィルタはフィルタの順序に含まれません。つまり、処理されません。 • ディセーブルにしたルールは、イベント アクション フィルタ テーブルに網掛けで表示されます。

要素	説明
名前	フィルタ ルールの名前。フィルタ名に使用できる文字は次のとおりです。 a-z、A-Z、0-9、-、.（ドットまたはピリオド）、:（コロン）、および_（下線）。
Signature IDs	フィルタ ルールを適用する数字のシグニチャ ID。単一のシグニチャ ID、カンマ区切りリスト、またはIDの範囲を入力できます。デフォルトでは、900 ～ 65535 の範囲のシグニチャにルールが適用されます。
サブシグニチャ ID	フィルタ ルールを適用する指定したシグニチャのサブシグニチャ ID。サブシグニチャ ID は広範なシグニチャをより詳細に識別しますが、すべてのシグニチャに使用されるわけではありません。 指定したシグニチャ ID に適したサブシグニチャ ID を入力するか、またはサブシグニチャ ID の範囲を入力します。デフォルト値は 0 ～ 255 の範囲です。
攻撃者の IPv4 アドレス	攻撃パケットを送信するホストの IP アドレス。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値はすべての IPv4 アドレスの範囲（0.0.0.0-255.255.255.255）です。
攻撃者の IPv6 アドレス	攻撃パケットを送信するホストの IP アドレス。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値は、すべての IPv6 アドレスの範囲（::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF）です。
Attacker Port	攻撃者ホストによって使用されるポート。これは、攻撃パケットの発信元のポートです。ポートの範囲を入力することもできます。 デフォルト値はすべてのポートの範囲（0-65535）です。

要素	説明
攻撃対象の IPv4 アドレス	攻撃されているホスト（攻撃パケットの受信者）の IP アドレス。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホスト オブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値はすべての IPv4 アドレスの範囲（0.0.0.0-255.255.255.255）です。
攻撃対象の IPv6 アドレス	攻撃されているホスト（攻撃パケットの受信者）の IP アドレス。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホスト オブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値は、すべての IPv6 アドレスの範囲（::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF）です。
攻撃対象のポート	攻撃されているホスト（攻撃パケットの受信者）のポート。これは、攻撃パケットの送信先のポートです。ポートの範囲を入力することもできます。 デフォルト値はすべてのポートの範囲（0-65535）です。
リスク レーティングの最小と最大	このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲（0 ～ 100）。デフォルト値は範囲全体（0 ～ 100）です。 イベントが発生し、そのリスク レーティングがここで設定した最小-最大範囲に入っていた場合、イベントはこのイベント フィルタのルールと比較して処理されます。
OS Relevance	アラートが、攻撃対象用として識別されている OS と関連があるかどうかを示します。指定可能な値は、[Not Relevant]、[Relevant]、[Unknown] のうちの 1 つ以上です。Ctrl を押しながらクリックすることで、複数の値を選択できます。デフォルトでは、すべての値が選択されます。 （注） [OS Relevance] は、IPS 6.x 以降のソフトウェアを実行しているアプライアンスおよびサービス モジュールだけに適用可能です。Cisco IOS IPS デバイスの場合、このフィールドは読み取り専用になり、編集はできません。IPS 5.x デバイスの場合、このフィールドは空白になります。
説明	ルールの目的に関する説明など、このフィルタに関連付けるユーザ コメント。

要素	説明
Actions to Subtract	イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクション。このリスト ボックスから 1 つ以上のアクションを選択できます。選択したすべてのアクションがイベントから削除されます。Ctrl を押しながらクリックすることで、複数の値を選択できます。指定可能なアクションの詳細については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （2181 ページ）を参照してください。 IOS IPS デバイスの場合、指定できるのは次の値だけです。 • [インラインで攻撃者を拒否（Deny Attacker Inline）] は、攻撃者の送信元 IP アドレスを完全にブロックします。遮断時間が経過するまで攻撃者からルータへの接続は確立されません。この時間は、イベント アクションの設定 （2242 ページ）で説明されているように、Event Actions Settings ポリシーで設定できます。 • [インラインで接続を拒否（Deny Connection Inline）] は、攻撃者からの該当する TCP フローをブロックします。攻撃者からルータへのその他の接続は確立されます。 • [インラインでパケットを拒否（Deny Packet Inline）] は、リセットを送信せずにパケットを廃棄します。「drop と reset」はアラームとともに使用することを推奨します。 • [アラートを生成（Produce Alert）] は、syslog または SDEE を介して攻撃に関する通知を送信します。 • [TCP接続をリセット（Reset TCP Connection）] は、TCP ベースの接続に有効で、送信元アドレスおよび宛先アドレスの両方にリセットを送信します。たとえば、ハーフオープン SYN 攻撃の場合に、Cisco IOS IPS は TCP 接続をリセットできます。
% to Deny	攻撃者拒否機能で拒否するパケットのパーセンテージ。範囲は 0 ～ 100 です。デフォルトは 100% です。 （注） IOS IPS デバイスの場合、このフィールドは読み取り専用で、編集はできません。

要素	説明
Stop on Match	このフィルタ ルールを停止ルールとして定義するかどうかを指定します。この設定によって、イベント アクション フィルタ ルール テーブルに残っているルールを処理する方法が決まります。 • このオプションを選択し、イベントがルールの条件を満たす場合、このルールは、イベントに対してテストされる最後のルールとなります。このルールによって識別されたアクションはイベントから削除され、デバイスは、イベントに割り当てられている残りのすべてのアクションを実行します。 • このオプションを選択していない場合、このフィルタ ルールの条件を満たすイベントも、イベント アクション フィルタ テーブル内の後続のルールと比較されます。後続のルールは、すべてのルールがテストされるか、またはイベントが停止ルールに一致するまでテストされます。

イベント アクション オーバーライドの設定

イベント アクション オーバーライドを追加すると、イベントのリスク レーティングに基づいて、そのイベントに関連付けられているアクションを変更できます。イベントアクションオーバーライドは、各シグニチャを個別に設定しないで、グローバルにイベントアクションを追加する方法です。

各イベントアクションには、関連付けられたリスク レーティング範囲があります。シグニチャイベントが発生し、そのイベントのリスク レーティングがイベントアクションの範囲内に入っていた場合、そのアクションがイベントに追加されます。たとえば、リスク レーティングが 85 以上のイベントで SNMP トラップを生成させる場合、Request SNMP Trap のイベント アクション オーバーライドを作成し、そのリスク レーティング 85 ～ 100 を設定します。

ヒント アクション オーバーライドを使用できないようにする場合は、イベント アクションの設定 （2242 ページ）の説明に従って、イベントアクションオーバーライドコンポーネント全体をディセーブルにします。

関連項目

- IPS イベント アクションについて （2213 ページ）

ステップ 1 次のいずれかを実行して、Event Action Overrides ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [イベントアクション（Event Actions）] > [イベントアクションのオーバーライド（Event Action Overrides）] を選択します。

- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）[IPS]>[イベントアクション（Event Actions）] > [イベントアクションのオーバーライド（Event Action Overrides）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [イベントアクションのオーバーライド（Event Action Overrides）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

テーブルに既存のオーバーライドが表示され、アクション、アクションが追加されるアラートのリスクレーティング、およびルールがイネーブルかどうかが示されます。ルールの順序は関係しません。アラートに適用されるすべてのオーバーライドによって、関連付けられたアクションが追加されます。

テーブルには、指定可能なアクションごとに最大で 1 つのエントリを含めることができます。

ステップ 2 目的のオーバーライドを設定します。

- 新しいオーバーライドを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックし、[イベントアクションルールの追加（Add Event Action Rule）] ダイアログボックスに入力します。ダイアログボックスでは、追加するアクションを選択し、アクションに追加するアラートのレーティング範囲（90 ～ 100 など）を入力して、[OK] をクリックします。詳細については、[イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （2229 ページ）を参照してください。

リスク レーティング範囲は、0 ～ 100 の値である必要があります。80-90 のように、範囲の最小値と最大値をハイフンで区切ります。

新しいオーバーライドを追加するときは、独自のリスクレーティングを定義するか、事前に定義されたリスク レーティング ポリシー オブジェクトを使用できます。バージョン 4.5 以降、Security Manager にはいくつかの事前定義されたリスク レーティング ポリシー オブジェクトがあります。

- [極めて高いリスク（Extreme Risk）]（90 ～ 100）
- [高リスク（High Risk）]（76 ～ 90）
- [中-高リスク（Medium-High Risk）]（61 ～ 75）
- [中リスク（Medium Risk）]（46 ～ 60）
- [中-低リスク（Medium-Low Risk）]（30 ～ 45）
- [低リスク（Low Risk）]（16 ～ 30）
- [非常に低いリスク（Very Low Risk）]（1 ～ 15）

これらの事前定義されたポリシーオブジェクトの詳細については、リスク評価ポリシーオブジェクトの構成 （2230 ページ）を参照してください。

これらの事前定義されたポリシーオブジェクトは編集できませんが、ユーザーが定義した独自のポリシーオブジェクトを追加および編集できます。

- オーバーライドを編集するか、オーバーライドを無効にするか、またはリスクレーティングを変更するには、オーバーライドを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。イベント アクションは変更できません。

（注） IPS デバイスが再検出されると、リスク レーティング ポリシー オブジェクトの値がインライン値に置き換えられます。たとえば、高リスクポリシーオブジェクト（80 ～ 89）をいずれかのイベントアクションに割り当ててデバイスに展開した場合、再検出後、そのポリシーオブジェクトの値はそのインライン値 80 ～ 89 に置き換えられます。

- オーバーライドを削除するには、オーバーライドを選択し、[行の削除（Delete Row）] ボタンをクリックします。

（注） IPS アプライアンスおよびサービスモジュールのポリシーには、Deny Packet Inline のオーバーライドがデフォルトで含まれており、これは削除できません。そのオーバーライドを使用しない場合は、ディセーブルにします。

- オーバーライドのリスト全体をカンマ区切り値（CSV）ファイルにエクスポートするには、[ファイルへのエクスポート（Export to File）] をクリックして Security Manager サーバーの適切なフォルダにナビゲートし、デフォルト名を使用しない場合はファイル名を変更して [保存（Save）] をクリックします。

[イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス

[イベントアクションルールの追加（Add Event Action Rule）]/ [イベントアクションルールの編集（Edit Event Action Rule）]ダイアログボックスを使用して、バージョン 4.5 以降の Security Manager で使用できる事前定義されたリスク レーティング ポリシー オブジェクトの 1 つに基づいてイベントアクションルールを追加します。

ナビゲーション パス

[イベントアクションオーバーライド（Event Action Overrides）] ポリシーから、オーバーライドテーブルの下の [行の追加（Add Row）] ボタンをクリックするか、テーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。Event Action Overrides ポリシーを開く方法については、イベントアクション オーバーライドの設定 （2227 ページ）を参照してください。

フィールド リファレンス

表 *529 : [*イベントアクションルールの追加または編集（***Add or Edit Event Action Rule***）*]* ダイアログボックス

要素	説明
Risk Rating	バージョン 4.5 以降の Security Manager で使用できる、次の事前定義されたリスクレーティング ポリシー オブジェクトの 1 つ。 • 極めて高いリスク（90～100）（Extreme Risk (90-100)） • 高リスク （76～90）（High Risk (76-90)） • 中 - 高リスク（61-75）（Medium-High Risk (61-75)） • 中リスク（46～60）（Medium Risk (46-60)） • 中 - 低リスク（30～45）（Medium-Low Risk (30-45)） • 低リスク（16～30）（Low Risk (16-30)） • 非常に低いリスク（1～15）（Very Low Risk (1-15)） これらの事前定義されたリスク レーティング ポリシー オブジェクトのいずれかを使用する方法、または独自に定義する方法の詳細については、イベント アクション オーバーライドの設定 （2227ページ）を参照してください。
割り当て済み（Assigned）	特定のアクションが少なくとも 1 つのリスク レーティング ポリシー オブジェクトに割り当てられているかどうかを指定します。
アクション名	割り当てられたときに特定のリスクレーティングに対して実行されるアクション。
[有効（Enabled）]	特定のアクションがイネーブルかどうかを指定します。アクションを削除せずに一時的にディセーブルにするには、このオプションの選択を解除します。

リスク評価ポリシーオブジェクトの構成

[リスクレーティングポリシーオブジェクト（Risk Rating Policy Object）] ダイアログボックスを使用して、IPS のポリシーオブジェクトを設定します。7 つの事前定義されたポリシーオブジェクトがリスク評価に使用できます。独自に定義することもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] > [すべてのオブジェクトタイプ（All Object Types）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [リスクレーティング（Risk Rating）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集

（Edit Object）] を選択します。ただし、事前定義されたポリシーオブジェクトを編集することはできません。

[新規オブジェクト（New Object）] または [オブジェクトの編集（Edit Object）] のどちらを選択したかに応じて、[リスクレーティングの追加（ Add Risk Rating）] または [リスクレーティングの編集（Edit Risk Rating）] ダイアログボックスが表示されます。 [イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （2229 ページ）を参照してください。

このトピックの残りの部分では、[リスクレーティングポリシーオブジェクト（Risk Rating Policy Object）] ダイアログボックスに表示されるフィールドについて説明します。

関連項目

- イベント アクション オーバーライドの設定 （2227 ページ）
- [イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （2229 ページ）

フィールド リファレンス

表 *530 : [リスクレーティングポリシーオブジェクト（Risk Rating Policy Object）] ダイアログ ボックス*

要素	説明
名前	「高リスク」などの事前定義されたポリシーオブジェクトの名前、または定義したポリシーオブジェクトの名前。
範囲	数値範囲で表される、特定のポリシーオブジェクトのリスクレーティング。
カテゴリ	Cat-A ～ Cat-G を選択できます。 これは、オブジェクトに割り当てられたカテゴリです。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
オーバーライド	このポリシーオブジェクトに IPS イベント アクション オーバーライドが設定されているかどうか
説明	提供できるテキストの説明。事前定義されたポリシーオブジェクトではなく、定義したポリシーオブジェクトに適用されます。
最後のチケット	このポリシーオブジェクトに使用された最後のチケット。
最終更新日	このポリシーオブジェクトが最後に変更された日付。

[リスク レーティングの追加または編集] ダイアログボックス

[リスクレーティングの追加または編集（Add or Edit Risk Rating）] ダイアログボックスを使用して、IPS リスクレーティングのポリシーオブジェクトを定義します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] > [すべてのオブジェクトタイプ（All Object Types）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [リスク評価（Risk Rating）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。ただし、事前定義されたポリシーオブジェクトを編集することはできません。

関連項目

- イベント アクション オーバーライドの設定 （2227 ページ）
- [イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （2229 ページ）

フィールド リファレンス

表 *531 : [*リスク レーティングの追加または編集*]* ダイアログボックス

要素	説明
名前	「高リスク」などの事前定義されたポリシーオブジェクトの名前、または定義したポリシーオブジェクトの名前。
説明	提供できるテキストの説明。事前定義されたポリシーオブジェクトではなく、定義したポリシーオブジェクトに適用されます。
範囲	数値範囲で表される、特定のポリシーオブジェクトのリスクレーティング。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

IPS イベント アクション ネットワーク情報の設定

Event Actions Network Information ポリシーを使用して、次の機能を設定します。

- ターゲットの価値レーティング（[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブと [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings）] タブ）：ネットワーク資産のターゲットの価値レーティングを設定できます。センサーは、アラートの全体的なリスク レーティングを計算するときに、このレーティングを使用します。ミッションクリティカルな資産を識別することによって、より重大なシグニチャイベントアクションをトリガーできます。名前が示すように、適切なタブを選択することにより、IPv4 または IPv6 を使用できます。

ターゲットの価値レーティングは、IPS アプライアンス、サービス モジュール、および Cisco IOS IPS デバイスで使用できます。

詳細については、ターゲットの価値レーティングの設定 （2234ページ）を参照してください。

- パッシブ OS フィンガープリントおよび OS マッピング（[OS ID（OS Identification）] タブ）：デバイス上で稼働しているオペレーティングシステムの情報をセンサーが使用して、全体的なリスクレーティングのコンポーネントである攻撃関連性レーティングを決定できます。

パッシブ OS フィンガープリントおよび OS マッピングは、IPS 6.x 以降のソフトウェアを実行しているデバイスでだけ使用可能で、Cisco IOS IPS デバイスでは使用できません。

詳細については、以下を参照してください。

- パッシブ OS フィンガープリントについて （2236 ページ）
- OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （2238 ページ）

Network Information ポリシーを開くには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択します。

- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

ターゲットの価値レーティングの設定

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。IP アドレスで識別されるネットワーク資産の、認識されている重要性を特定します。

価値の高い企業リソースにはより厳しく、あまり重要でないリソースにはより緩やかなセキュリティ ポリシーを開発できます。たとえば、デスクトップ ノードに割り当てるターゲットの価値レーティングよりも高いターゲットの価値レーティングを会社の Web サーバに割り当てることができます。この場合、会社の Web サーバに対する攻撃には、デスクトップ ノードに対する攻撃よりも高いリスク レーティングが付与されます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

4 つの価値レーティングを設定できます。最も高い値から最も低い値まで順に、[Mission Critical]、[High]、[Medium]、[Low]、[No Value]（ゼロ値）となります。

リスクレーティングの計算方法の詳細については、Cisco.com で『Installing and Using Cisco Intrusion Prevention System Device Manager 7.0』の「Calculating the Risk Rating」を参照してください。

ヒント 6.0(5) よりも前の IPS 6.0 ソフトウェアを使用しているデバイスでターゲットの価値レーティングを設定する場合は、OS マップを作成する必要がなくても、Network Information ポリシーの [OS Identification] タブを更新してソフトウェア バグを回避することを推奨します。詳細については、OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （2238 ページ）を参照してください。

関連項目

- IPS イベント アクション ネットワーク情報の設定 （2233 ページ）
- IPS イベント アクション プロセスについて （2212 ページ）

ステップ 1 次のいずれかを実行して、Network Information ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択して、[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings] タブをクリックします。

- （ポリシービュー、IPSアプライアンスおよびサービスモジュール）**[IPS]>[イベントアクション（Event Actions）]>[ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings] タブをクリックします。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）]>[イベントアクション（Event Actions）]>[ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブをクリックします。

（注） Cisco IOS IPS デバイスは IPv6 をサポートしていません。

タブに、すでに設定済みのターゲットの価値レーティングが表示され、設定済みの各レーティング カテゴリに関連付けられている IP アドレスが示されます。テーブルには 1 つのレーティング カテゴリに 1 つずつ、最大で 5 つのエントリを含めることができます。

ステップ 2 目的のターゲットの価値レーティング カテゴリを設定します。

- 新しいレーティングカテゴリを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックし、[ターゲットの価値レーティングの追加（Add Target Value Rating）] ダイアログボックスに入力します。このダイアログボックスで、追加するレーティングを選択し、カテゴリに関連付けるホスト、ネットワーク、およびアドレス範囲を入力して、[OK] をクリックします。詳細については、[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックス （2235 ページ）を参照してください。

IPv4 アドレスには、単一のネットワーク/ホストオブジェクトを指定するか、10.10.10.10、10.10.10.0/24、10.10.10.2-10.10.10.254 のようなホスト、ネットワーク、またはアドレス範囲のカンマ区切りリストを指定できます。ネットワーク形式で入力したアドレスは、アドレス範囲に変換されます。IPv6 アドレスの場合は、IPv6 アドレスの表記法を使用します。

- 既存のレーティングカテゴリの IP アドレスを編集するには、カテゴリを選択して、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。価値レーティングは変更できません。
- レーティングを削除するには、そのレーティングを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックス

[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックスを使用して、資産の IP アドレスをレーティング カテゴリに関連付けます。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブから [ターゲットの価値レーティング（Target Value Ratings）] ダイアログボックスを開くと、IP アドレスは IPv4 です。[IPv6] タブから開くと、IPv6 です。

ナビゲーション パス

IPS Event Actions Network Information ポリシーの [IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value

Ratings）] タブから、[ターゲットの価値レーティング（Target Value Ratings）] テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings）] タブを開く方法については、ターゲットの価値レーティングの設定 （2234ページ）を参照してください。

フィールド リファレンス

表 *532 : [Add Target Value Rating]/[Edit Target Value Rating]* ダイアログボックス

要素	説明
値	指定したアドレスに関連付けるターゲットの価値レーティング。最も高い重要性から最も低い重要性まで順に、[Mission Critical]、[High]、[Medium]、[Low]、[No Value] となります。 このリストには、ターゲットの価値レーティング テーブルにまだ設定されていない価値レーティングだけが含まれます。 レーティング カテゴリを編集する場合は、このオプションを変更します。
target-address	この価値レーティングに割り当てられるネットワーク資産の IP アドレス。次の方法を使用して、アドレスを指定できます。 • 単一のネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクトには、ネットワーク、ホスト、およびアドレス範囲のグループを含めることができます。 • ホストやネットワークのアドレスまたはアドレス範囲の、カンマ区切りのリスト。たとえば、IPv4 を使用する場合、10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254 となります。ネットワーク形式で入力したアドレスはアドレス範囲に変換されます。たとえば、10.10.10.0/24 は 10.10.10.0-10.10.10.255 に変換されます。

パッシブ OS フィンガープリントについて

パッシブ Operating System（OS; オペレーティング システム）フィンガープリントは、IPS 6.0 以降のセンサーではデフォルトでイネーブルになっており、IPS にはシグニチャごとにデフォルトの脆弱な OS リストが含まれています。

パッシブ OS フィンガープリントにより、センサーはホストが稼働している OS を特定できます。センサーはホスト間のネットワーク トラフィックを分析して、これらのホストの OS をその IP アドレスとともに格納します。センサーはネットワーク上で交換される TCP SYN および SYNACK パケットを検査して、OS タイプを特定します。

次に、センサーはターゲット ホスト OS の OS を使用し、リスク レーティングの攻撃関連性レーティング コンポーネントを計算することによって、攻撃対象への攻撃の関連性を決定します。センサーは、攻撃の関連性に基づいて、攻撃に対するアラートのリスク レーティングを変更したり、攻撃のアラートをフィルタリングしたりする場合があります。ここで、リスク レーティングを使用すると、偽陽性アラートの数を減らしたり（IDS モードの利点）、疑わしいパケットを明確にドロップしたり（IPS モードの利点）できます。また、パッシブ OS フィンガープリントでは、攻撃対象 OS、OS ID のソース、および攻撃対象 OS との関連性をアラート内にレポートすることによって、アラート出力が拡張されます。

パッシブ OS フィンガープリントは、次の 3 つのコンポーネントで構成されます。

- パッシブ OS ラーニング。

パッシブ OS ラーニングは、センサーがネットワーク上のトラフィックを監視しているときに行われます。TCP SYN および SYNACK パケットの特性に基づいて、センサーは送信元 IP アドレスのホスト上で稼働している OS を特定します。

- ユーザ設定可能な OS ID。

OS ホスト マッピングを設定できます。これは学習した OS マッピングに優先します。

- 攻撃関連性レーティングおよびリスク レーティングの計算。

センサーは OS 情報を使用して、ターゲット ホストに対する攻撃シグニチャの関連性を決定します。攻撃の関連性は、攻撃アラートのリスク レーティング値を構成する攻撃関連性レーティング コンポーネントです。

OS 情報には 3 つのソースがあります。センサーは OS 情報のソースを次の順序でランク付けします。

1. 設定した OS マッピング：Event Actions Network Information ポリシーの [OS Identification] タブで入力した OS マッピング。仮想センサーごとに異なるマッピングを設定できます。詳細については、OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （2238 ページ）を参照してください。

   OS マッピングを設定して、重要なシステムで稼働している OS の ID を定義することを推奨します。重要なシステムの OS および IP アドレスが変更される可能性が少ない場合は、OS マッピングを設定するのが適切です。

2. インポートした OS マッピング：Management Center for Cisco Security Agents（CSA MC）からインポートした OS マッピング。

   インポートした OS マッピングはグローバルであり、すべての仮想センサーに適用されます。CSA MC を使用するようにセンサーを設定する方法の詳細については、外部製品インターフェイスの設定 （2117 ページ）を参照してください。

3. 学習した OS マッピング：SYN 制御ビットが設定されている TCP パケットのフィンガープリントを介して、センサーが検知した OS マッピング。

   学習した OS マッピングは、トラフィックを監視する仮想センサーに対してローカルです。

センサーは、ターゲット IP アドレスの OS を特定する必要がある場合に、設定した OS マッピングを調べます。ターゲット IP アドレスが設定した OS マッピングにない場合、センサーはインポートした OS マッピングを調べます。ターゲット IP アドレスがインポートした OS マッピングにない場合、センサーは学習した OS マッピングを調べます。そこでも見つからなかった場合、センサーはターゲット IP の OS を不明として処理します。

ヒント　ターゲットの OS 関連性の値を使用するように、イベント アクション フィルタ ルールを設定できます。また、シグニチャに対する OS の脆弱性を識別するようにシグニチャを設定できます。

OS ID の設定（Cisco IPS 6.x 以降のセンサー限定）

Event Actions Network Information ポリシーの [OS Identification] タブを使用して、オペレーティング システム（OS）のホスト マッピングを設定します。これは、学習した OS マッピングに優先します。[OS Identifications] タブで、設定済みの OS マップの追加、編集、および削除を行うことができます。リスト内で OS マップを上下に移動すると、特定の IP アドレスと OS タイプの組み合わせに対する攻撃関連性レーティングおよびリスク レーティングの計算をセンサーが行う順序を変更できます。

（注）　OS ID は IPS 6.0 以降のセンサーにだけ適用され、Cisco IOS IPS デバイスには適用されません。

また、リスト内で OS マップを上下に移動すると、特定の IP アドレスに関連付けられている OS をセンサーが解決する順序を変更できます。設定した OS マッピングでは、範囲を設定できます。そのため、ネットワーク 192.168.1.0/24 の場合、次のように定義できます。

IP アドレス範囲の設定	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10、192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

より特定的なマッピングをリストの先頭に配置する必要があります。IP アドレス範囲設定では重複は許可されませんが、最もリストの先頭に近いエントリが優先されます。

ヒント 6.0(5) よりも前の IPS 6.0 バージョンには、Network Information ポリシーに関連するバグがあります。[OS ID（OS Identification）] タブで変更を行わなかったが、[脅威値レーティング（Threat Value Ratings）] タブでは設定を変更した場合でも、Security Manager は OS マッピングをアドレスに限定するために **any** 変数を使用するようにデバイスを設定します。この結果、モニタリング アプリケーションでは、すべてのイベントのイベント発生場所として「any」が表示されます。この問題を解決するには、センサーの IPS バージョンをアップグレードします。また、この問題を回避するには、特定の OS マッピングを設定していなくても、[OS ID（OS Identification）] タブの [これらの IP アドレスへの制限（Restrict to these IP Addresses）] フィールドにデフォルト以外の値を入力します。たとえば、「any」の代わりに 0.0.0.1-255.255.255.255 または 0.0.0.0-255.255.255.255 を入力します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）] を選択して、[OS ID（OS Identification）] タブをクリックします。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[OS ID（OS Identification）] タブをクリックします。

関連項目

- IPS イベント アクション ネットワーク情報の設定 （2233 ページ）
- IPS イベント アクション プロセスについて （2212 ページ）

フィールド リファレンス

表 *533 : [OS Identification]* タブ

要素	説明
Enable Passive OS Fingerprinting	選択すると、センサーはパッシブなOS分析を実行します。このページで設定したマップのいずれかを使用するには、このオプションをイネーブルにする必要があります。 パッシブOSフィンガープリントは、センサーの一部として機能します。ホスト間のネットワーク トラフィックを分析するときに、センサーはホストのIPアドレスとともに、ホスト上で稼働しているOSのIDを格納します。センサーは、ネットワーク上で交換されたパケットの特性を検査することによって、ホスト上のOSのIDを特定します。次に、センサーはターゲットシステムのOS情報を使用して、RR（リスクレーティング）のARR（攻撃関連性レーティング）コンポーネントを計算します。さらに、RRは疑わしいパケットのドロップに使用できます。 パッシブOSフィンガープリントの詳細については、パッシブ OS フィンガープリントについて （2236 ページ）を参照してください。
Restricted to these IP Addresses	攻撃関連性レーティングの計算を、指定したアドレスに制限します。次の方法を使用して、アドレスを指定できます。 • 単一のネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクトには、ネットワーク、ホスト、およびアドレス範囲のグループを含めることができます。 • ホストやネットワークのアドレスまたはアドレス範囲の、カンマ区切りのリスト。たとえば、10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254 となります。

要素	説明
[OS Maps] テーブル	OS マッピングのリストであり、ホストの IP アドレスと、それらがマッピングされるオペレーティング システムが示されます。一致検索時、センサーは上から下の順に検索して、IP アドレスと一致する最初のルールを選択します。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックし、[OS マップの追加（Add OS Map）] ダイアログボックスに入力します（[Add OS Map]/[Edit OS Map] ダイアログボックス （2241 ページ）を参照）。 • マッピングを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マップを削除するには、マップを選択し、[行の削除（Delete Row）] ボタンをクリックします。 • ルールのプライオリティを変更するには、そのルールを選択し、ルールが正しい位置に配置されるまで**上**矢印ボタンまたは**下**矢印ボタンをクリックします。

[Add OS Map]/[Edit OS Map] ダイアログボックス

[Add OS Map]/[Edit OS Map] ダイアログボックスを使用し、ホストの IP アドレスを使用してホストを OS タイプにマッピングします。OS タイプを IP アドレスにスタティックに割り当てる場合にだけ、マッピングを作成します。センサーが、パッシブ OS フィンガープリントを使用して IP アドレスに関連付けられる OS を検出するため、マッピングを作成しないことや、スタティック IP アドレスを持つミッションクリティカルなデバイスに対してだけマッピングを作成することができます。アドレスに別のオペレーティング システムを搭載したデバイスを設置する場合は、作成したすべてのマッピングを更新してください。

ナビゲーション パス

IPS Event Actions Network Information ポリシーの [OS ID（OS Identification）] タブから、[OS マップ（OS Maps）] テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。[OS Identification] タブを開く方法については、OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （2238 ページ）を参照してください。

フィールド リファレンス

表 *534 : [Add OS Map]/[Edit OS Map]* ダイアログボックス

要素	説明
IP Addresses	このマッピングのIPアドレス。次の方法を使用して、アドレスを指定できます。 • 単一のネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクトには、ネットワーク、ホスト、およびアドレス範囲のグループを含めることができます。 • ホストやネットワークのアドレスまたはアドレス範囲の、カンマ区切りのリスト。たとえば、10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254 となります。
OS タイプ	識別されるホストで稼働しているオペレーティング システム。リストから最も適切なオプションを選択します。複数のオプションを選択すると（Ctrl を押しながらクリックする）、可能性のある OS が複数存在することを示すことができます。 **ヒント** これらのマッピングは学習したマッピングに優先するため、[General OS]、[Other]、または [Unknown OS] は割り当てないようにすることを推奨します。センサーがパッシブ OS フィンガープリントを介して実際の OS を学習し、これによってより適切なマッチングを得られる可能性があります。詳細については、パッシブ OS フィンガープリントについて （2236 ページ）を参照してください。

イベント アクションの設定

Event Actions Settings ポリシーを使用して、イベント アクション ルールにグローバルに適用される一般的な設定を指定します。これらのオプションのデフォルトはほとんどの状況に適しているため、個々の状況でデフォルト以外の動作を必要とすることが確実な場合にだけ、これらを変更します。

Event Actions Settings ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [イベントアクション（Event Actions）] > [設定（Settings）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [イベントアクション（Event Actions）] > [設定（Settings）]**を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [イベントアクション設定（Event Action Settings）]** を選択してから、既存のポリシーを選択するか新しいポリシーを作成します。

次の表に、設定できるオプションを示します。Cisco IOS IPS デバイスで使用可能なオプションは、IPS アプライアンスおよびサービス モジュールで使用可能なオプションよりも制限されていることに注意してください。

ヒント　トラブルシューティング目的以外では、Summarizer をディセーブルにしないでください。Summarizer をディセーブルにすると、すべてのシグニチャがサマライズなしの Fire All に設定されます。Meta Event Generator の状態を変更する必要はないことに注意してください。シスコではメタシグニチャの使用を中止しており、それらはすべて廃止されました。

表 *535 : Event Actions Settings* ポリシー

要素	説明
Enable Event Action Override （すべてのデバイス タイプ）	選択すると、[Event Action Overrides] ページで定義したオーバーライドルールがイネーブルになります。イベント アクション オーバーライドを追加すると、イベントの具体的な詳細に基づいて、そのイベントにアクションを追加できます。オーバーライド ルールの設定については、イベント アクション オーバーライドの設定 （2227 ページ）を参照してください。
Enable Event Action Filters （すべてのデバイス タイプ）	選択すると、[Event Action Filters] ページで定義したフィルタ ルールがイネーブルになります。特定のアクションをイベントから削除するか、または、イベント全体を破棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。イベント アクション フィルタ ルールの設定については、イベント アクション フィルタの設定 （2216 ページ）を参照してください。

要素	説明
Enable Event Action Summarizer （IPS アプライアンスおよびサービス モジュール限定）	選択すると、Summarizer コンポーネントがイネーブルになります。Summarizer はイベントを単一アラートにグループ化するため、センサーが送信するアラートの数が減少します。 デフォルトでは、Summarizer はイネーブルになります。ディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。サマライズするように個別のシグニチャを設定しても、この設定は Summarizer がイネーブルになっていない場合は無視されます。 Cisco Security Manager の Report Manager コンポーネントは、イベントを個別にレポートします。Cisco Security Manager の Event Viewer コンポーネントにアラートが表示されます。上述のとおり、Summarizer はイベントを単一アラートにグループ化するため、センサーが送信するアラートの数が減少します。 **ヒント** Cisco IPS Manager Express（IME）と Cisco Security Manager は、まったく同じ方法ではイベントを要約しません。
Enable Meta Event Generator （IPS アプライアンスおよびサービス モジュール限定）	シスコでは、Meta Event Generator の状態を変更しないことを推奨しています。シスコではメタシグニチャの使用を中止しており、それらはすべて廃止されました。

要素	説明
Enable Threat Rating Adjustment （IPS アプライアンスおよびサービス モジュール限定）	選択すると、脅威レーティングの調整がイネーブルになり、これによってリスク レーティングが調整されます。ディセーブルにすると、リスク レーティングは脅威レーティングと等しくなります。IPS 6.0 以降のソフトウェアを実行しているセンサーでだけ使用可能です。 脅威レーティング機能は、ネットワークの脅威環境に関する単一のビューを提供します。脅威レーティングは、脅威レーティングの値が高いイベントだけを表示するカスタマイズ ビューを使用して、アラームおよびイベントの数を最小限に抑えます。脅威レーティングの値は、次のように算出されます。 • 応答アクションの成功に基づいたイベントのリスク レーティングのダイナミック調整 • 応答アクションが適用された場合、リスク レーティングは使用されない（脅威レーティング < リスク レーティング） • 応答アクションが適用されなかった場合、リスク レーティングは変更されない（脅威レーティング = リスク レーティング） この結果、脅威のリスクを決定する単一の値が算出されます。
Deny Attacker Duration in seconds （すべてのデバイス タイプ）	インラインで攻撃者を拒否する秒数。 有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。
Block Attack Duration in minutes （IPS アプライアンスおよびサービス モジュール限定）	ホストまたは接続をブロックする分数。 指定できる範囲は 0 ～ 10000000 です。デフォルトは 30 です。
Maximum Number of Denied Attackers （IPS アプライアンスおよびサービス モジュール限定）	一度にシステム内に許容できる拒否攻撃者の数を制限します。 有効な範囲は 0 ～ 100000000 です。デフォルトは 10000 です。

要素	説明
Enable One Way TCP Reset （IPS アプライアンスおよびサービス モジュール限定）	選択すると、TCP ベースのアラートの Deny Packet Inline アクションに対して一方向の TCP リセットがイネーブルになります。IPS 6.1 以降のソフトウェアを実行しているセンサーでだけ使用可能です。 一方向の TCP リセットはインライン モードでだけ動作し、Deny Packet Inline アクションに自動追加されます。TCP リセットがアラートの攻撃対象に送信されるため、攻撃者に対してブラックホールが作成され、攻撃対象の TCP リソースがクリアされます。 **ヒント** • インラインモードでは、ネットワークに出入りするすべてのパケットがセンサーを通過する必要があります。 • インライン センサーは、リスク レーティングが 90 以上のアラートのパケットを拒否します。また、リスク レーティングが 90 以上の TCP アラートで、一方向 TCP リセットを発行します。

第 41 章

IPS 異常検出の管理

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

異常検出は、スキャン動作を示すワームトラフィックを原因とするネットワークの輻輳を認識するように設計されています。異常検出では、他の脆弱なホストをスキャンしている、ネットワーク上の感染したホストも識別されます。

異常検出はデフォルトでイネーブルになりますが、効果的に使用するために調整する必要のある設定がいくつかあります。

（注） 異常検出を設定するには、センサーで IPS ソフトウェアバージョン 6.x 以降を使用する必要があります。また、Cisco IOS IPS と AIP-SSC-5 では異常検出はサポートされません。

この章は次のトピックで構成されています。

- 異常検出について （2247 ページ）
- 異常検出の設定 （2253 ページ）

異常検出について

センサーの異常検出コンポーネントでは、ワームに感染したホストが検出されます。これによりセンサーでは、Code Red や SQL Slammer などのワームやスキャナからの保護に際してシグニチャ更新への依存度が低くなります。異常検出コンポーネントでは、センサーが正常なアクティビティを学習し、正常な動作として学習した動作から逸脱する動作に対してアラートを送信するか、または動的応答アクションを実行します。

（注） 異常検出では、Nimda などの電子メール ベースのワームは検出されません。

異常検出では、次の 2 つの状況が検出されます。

- ワーム トラフィックによって輻輳し始めたパスでネットワークが起動した場合。
- ワームに感染した単一のソースがネットワークに入り、他の脆弱なホストのスキャンを開始した場合。

ここでは、異常検出についてより詳細に説明します。

- ワーム ウイルス （2248 ページ）
- 異常検出モード （2249 ページ）
- 異常検出ゾーン （2250 ページ）
- 異常検出をオフにする場合について （2250 ページ）
- 異常検出シグニチャの設定 （2251 ページ）
- 異常検出の設定 （2253 ページ）

ワーム ウイルス

ワーム ウイルスは、自身のコピーを作成してその拡散を促進する自動化された自己伝播型侵入エージェントです。ワーム ウイルスは脆弱なホストを攻撃して感染させ、そのホストをベースとして使用して他の脆弱なホストを攻撃します。ネットワーク インスペクションの 1 つの形式（通常はスキャン）を使用して他のホストを検索し、次のターゲットに伝播します。スキャニング ワーム ウイルスは、プローブする IP アドレスのリストを収集することで脆弱なホストを特定し、ホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームは、この方法で広がるワームの例です。

異常検出では、スキャナとして動作している、ワームに感染したホストを識別します。ワーム ウイルスは、拡散するために新しいホストを見つける必要があります。TCP、UDP、およびその他のプロトコルを使用してインターネットをスキャンして、異なる宛先 IP アドレスへの失敗するアクセス試行を生成することでホストを見つけます。スキャナは、非常に多くの宛先 IP アドレスに対して（TCP および UDP で）同じ宛先ポートにイベントを生成する送信元 IP アドレスとして定義されます。

TCP にとって重要なイベントは、特定の時間内に SYN-ACK 応答のない SYN パケットなど、未確立の接続です。TCP を使用してスキャンする、ワームに感染したホストは、異常な数の IP アドレスに対して同じ宛先ポートに未確立接続を生成します。

UDP にとって重要なイベントは、すべてのパケットが一方向にのみ流れる UDP 接続など、一方向の接続です。UDP を使用してスキャンする、ワームに感染したホストは、UDP パケットを生成しますが、複数の宛先 IP アドレスに対して同じ宛先ポートでタイムアウト期間内に同じ IP アドレス上で UDP パケットを受信しません。

ICMP（プロトコル番号 1）など、その他のプロトコルにとって重要なイベントは、送信元 IP アドレスから多数のさまざまな宛先 IP アドレス、すなわち、一方向でのみ受信されるパケットです。

注意 ワーム ウイルスが感染先の IP アドレスのリストを持っていて、拡散のためにスキャンを使用する必要がない場合（たとえば、パッシブ マッピングを使用する場合は、アクティブ スキャニングとは対照的に、ネットワークをリスニングします）、異常検出ワーム ポリシーでは検出されません。感染したホスト内でファイルをプローブしてメーリング リストを受信し、このリストを電子メールで送信するワーム ウイルスは、レイヤ 3 またはレイヤ 4 の異常を生成しないため、検出されません。

異常検出モード

異常検出はまず、ネットワークの最も正常な状態が反映される「正常時」の学習プロセスを実行します。次に、異常検出は正常なネットワークに最適な一連のポリシーしきい値を生成します。この処理は、初期の学習モード フェーズとそれに続く進行中の動作検出モード フェーズの 2 つのフェーズで行われます。

異常検出には次のモードがあります。

- 学習受け入れモード（初期設定）

異常検出はデフォルトで検出モードになっていますが、デフォルトで 24 時間、初期の学習受け入れモードを実行します。このフェーズ中は攻撃が行われないことを前提とします。異常検出では、ナレッジ ベースと呼ばれるネットワーク トラフィックの初期ベースラインが作成されます。定期スケジュールのデフォルトの間隔値は 24 時間で、デフォルトのアクションは循環です。これは、新しいナレッジ ベースが保存およびロードされ、24 時間後に初期ナレッジ ベースが置換されることを意味します。

次の点を考慮してください。

- 異常検出は、空の初期ナレッジベースを処理するときには攻撃を検出しません。デフォルトの 24 時間が経過すると、ナレッジ ベースが保存されてロードされ、異常検出が攻撃を検出するようになります。
- ネットワークの複雑さによっては、異常検出の学習受け入れモードをデフォルトの 24 時間よりも長くした方がよい場合もあります。モードは仮想センサーポリシーで設定します。仮想センサーの定義 （2157ページ）を参照してください。学習期間が終了した後、仮想センサーを編集し、検出モードに変更します。
- 検出モード

操作の進行中は、センサーを検出モードのままにする必要があります。これは 1 日 24 時間、週 7 日間実行します。ナレッジベースが作成され、初期ナレッジベースが置換されたあとで、異常検出はそのナレッジ ベースに基づいて攻撃を検出します。ナレッジ ベースのしきい値に違反するネットワーク トラフィック フローを見つけると、アラートを送信します。異常検出が異常を探すとき、しきい値に違反しない漸進的な変化がナレッジベースに記録され、新しいナレッジ ベースが作成されます。新しいナレッジ ベースは定期的に保存され、古いナレッジ ベースを置き換えるため、最新のナレッジ ベースが維持されます。

- 非アクティブ モード

異常検出は、非アクティブモードにすることでオフにできます。センサーが非対称環境で稼働している場合など、特定の状況では、異常検出を非アクティブモードにする必要があります。異常検出では、トラフィックが両方向から来ることを前提とするため、センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出によってすべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

次の例で、デフォルトの異常検出設定についてまとめます。仮想センサーを午後 11:00 に追加して、デフォルトの異常検出設定を変更しなかった場合、異常検出は初期ナレッジベースを使用して動作を開始し、学習のみを実行します。これは検出モードですが、情報を 24 時間収集して初期ナレッジベースを置換するまで、攻撃は検出されません。最初の開始時刻（デフォルトでは午前 10:00）および最初の間隔（デフォルトでは 24 時間）に、学習結果が新しいナレッジベースに保存され、このナレッジベースがロードされて初期ナレッジベースを置換します。異常検出はデフォルトで検出モードとなるため、新しいナレッジベースを使用して攻撃の検出を開始します。

異常検出ゾーン

ネットワークをゾーンに分割することで、偽陰性の率を低下させることができます。ゾーンは、宛先 IP アドレスのセットです。内部、不正、外部の 3 つのゾーンがあり、それぞれに独自のしきい値があります。

外部ゾーンは、デフォルトのインターネット範囲（0.0.0.0 ～ 255.255.255.255）を持つデフォルトのゾーンです。デフォルトでは、内部ゾーンと不正ゾーンにはIPアドレスは含まれません。内部ゾーンまたは不正ゾーンに含まれる IP アドレスのセットに一致しないパケットは、外部ゾーンで処理されます

内部ネットワークの IP アドレス範囲を使用して内部ゾーンを設定することを推奨します。このように設定すると、内部ゾーンには内部ネットワークの IP アドレス範囲に到着するすべてのトラフィックが含まれ、外部ゾーンにはインターネットに送信されるすべてのトラフィックが含まれます。

不正ゾーンには、割り当てられていない IP アドレスや、使用されていない内部 IP アドレス範囲に属する IP アドレスなど、正常なトラフィックに存在してはならない IP アドレスの範囲を設定できます。不正ゾーンには適正なトラフィックが到達しないと想定されるため、このゾーンは正確な検出に非常に役立ちます。これにより、非常に迅速なワーム ウイルス検出を可能にする非常に低いしきい値を設定できます。

異常検出をオフにする場合について

異常検出では、トラフィックは双方向であると見なされます。センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出をオフにする必要があります。そうしないと、異常検出が非対称環境で実行されている場合に、すべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

Virtual Sensors ポリシーで、異常検出をオフにします。異常検出をディセーブルにする仮想センサーを編集し、[Anomaly Detection Mode] を [Inactive] に変更します。仮想センサーの編集に関する詳細については、仮想センサーのポリシーの編集 （2162ページ）を参照してください。

異常検出シグニチャの設定

トラフィック異常エンジンには、3 つのプロトコル（TCP、UDP、およびその他）をカバーする 9 つの異常検出シグニチャが含まれます。各シグニチャには 2 つのサブシグニチャがあります。一方はスキャナ用で、もう一方はワームに感染したホスト（またはワーム攻撃されているスキャナ）用です。異常検出は、異常を検出すると、これらのシグニチャのアラートをトリガーします。すべての異常検出シグニチャは、デフォルトでイネーブルになり、各シグニチャのアラート重大度は高く設定されます。

スキャナが検出されても、ヒストグラム異常が発生しない場合、スキャナ シグニチャはその攻撃者（スキャナ）の IP アドレスをファイルに保存します。ヒストグラム シグニチャがトリガーされた場合は、スキャンを行っている攻撃者のアドレスによってそれぞれ（スキャナ シグニチャではなく）ワーム シグニチャがトリガーされます。ヒストグラムがトリガーされているので、アラートの詳細には、ワーム検出に使用されたしきい値が表示されます。その時点から、すべてのスキャナがワーム感染ホストとして検出されます。

次の異常検出イベント アクションが可能です。

- Produce alert：イベント ストアにイベントを書き込みます。
- Deny attacker inline：（インラインのみ）指定された期間、この攻撃者のアドレスから発生した現在のパケットおよび将来のパケットを送信しません。
- Log attacker packets：攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始します。
- Deny attacker service pair inline：送信元 IP アドレスと宛先ポートをブロックします。
- Request SNMP trap：トラップ通知を SNMP トラップ宛先に送信します。このアクションを使用するには、SNMP の設定 （2092 ページ）の説明に従って SNMP トラップ ホストを設定する必要があります。
- Request block host：要求を ARC に送信して、このホスト（攻撃者）をブロックします。このアクションを使用するには、IPS のブロッキングおよびレート制限の設定 （2282 ページ）の説明に従ってデバイスのブロックを設定する必要があります。

Signatures ポリシーでシグニチャにアクションを直接追加するか、Event Actions Overrides ポリシーでリスク レーティングに基づいてシグニチャにより生成されたイベントにアクションを追加できます。

次の表に、異常検出ワーム シグニチャのリストを示します。

表 *536 :* 異常検出ワーム シグニチャ

シグネチャ ID	サブシグニチャ ID	名前	説明
13000	[0]	Internal TCP Scanner	内部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13000	1	Internal TCP Scanner	内部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13001	[0]	Internal UDP Scanner	内部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13002	[0]	Internal Other Scanner	内部ゾーンでほかのプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13003	[0]	External TCP Scanner	外部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13003	1	External TCP Scanner	外部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13004	[0]	External UDP Scanner	外部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13004	1	External UDP Scanner	外部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13005	[0]	External Other Scanner	外部ゾーンでその他のプロトコル上に単一スキャナを識別しました。

シグネチャ ID	サブシグニチャ ID	名前	説明
13005	1	External Other Scanner	外部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13006	[0]	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13007	[0]	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13007	1	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13008	[0]	Illegal Other Scanner	不正ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。

異常検出の設定

Anomaly Detection ポリシーを使用して、異常検出を設定します。Virtual Sensors ポリシーにも、異常検出にとって重要な設定が含まれます。

この手順では、異常検出の全体的な設定について説明します。これらの設定を設定する前に、次の項を参照してください。

- 異常検出について （2247 ページ）
- ワーム ウイルス （2248 ページ）
- 異常検出モード （2249 ページ）
- 異常検出ゾーン （2250 ページ）

- 異常検出をオフにする場合について （2250 ページ）
- 異常検出シグニチャの設定 （2251 ページ）

ステップ 1 次のいずれかを実行して、変更する異常検出ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

異常検出ポリシーには、次のタブが含まれています。

- [動作設定（OperationSettings）]：ワームタイムアウトを定義し、異常検出で無視する必要のある IP アドレスを識別します。
- [学習受け入れモード（Learning Accept Mode）]：ナレッジベースの処理方法を含む、学習モードの設定。
- [内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）]、[外部ゾーン（External Zone）]：定義するネットワークのゾーン。各ゾーンに固有の設定を設定できます。ゾーンの説明については、異常検出ゾーン （2250 ページ）を参照してください。

ステップ 2 必要な場合、[動作設定（Operation Settings）] タブをクリックして、次の項目を設定します。

- [ワームタイムアウト（Worm Timeout）]：ワーム終了タイムアウトの時間（秒単位）。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。このタイムアウトの使用方法については、異常検出しきい値とヒストグラムについて （2258 ページ）を参照してください。
- [無視したアドレスの有効化（Enable Ignored Addresses）] および [無視する送信元/宛先アドレス（Source/Destination Addresses to Ignore）]：異常検出の処理中に無視する必要があるアドレスのリストを設定するかどうか。送信元アドレス（スキャンを開始するアドレス）または宛先アドレス（スキャンされるホスト）のリストを指定できます。

アドレスには、1 つの単一ホスト（10.100.10.1 など）、1 つのアドレス範囲（10.100.10.0-10.100.10.255 など）、あるいは複数の単一ホスト、複数のアドレス範囲、または複数のホストと範囲の組み合わせを含むネットワーク/ホスト オブジェクトを指定できます。[選択（Select）] を選択して、リストからオブジェクトを選択するか、新しいオブジェクトを作成します。

ステップ 3 [学習受け入れモード（Learning Accept Mode）] タブをクリックしてナレッジベースの生成方法および使用方法を定義します。詳細については、異常検出の学習受け入れモードの設定 （2256 ページ）を参照してください。

ステップ 4 内部ゾーン、不正ゾーン、および外部ゾーンを設定します。

- 内部ゾーンと不正ゾーンの定義：内部ゾーンは、管理対象のネットワークである内部ネットワークの IP アドレスです。不正ゾーンは、正常なトラフィックでは決して見られない IP アドレス範囲を表している必要があります。たとえば、割り当てられていない IP アドレスや、使用されていない内部 IP アドレス範囲に属する IP アドレスなどです。

[内部ゾーン（Internal Zone）] タブと [不正ゾーン（Illegal Zone）] タブを順番にクリックし、[全般（General）] タブで次の項目を設定します。

- [このゾーンを有効化する（Enable this zone）]：ゾーンが異常検出によって処理されるかどうか。
- [サービスサブネット（Service Subnets）]：ゾーンを構成する IP アドレス。デフォルト（0.0.0.0）では、ゾーンにアドレスは含まれません。ゾーンのアドレスを定義するように、0.0.0.0 を置き換えます。

アドレスには、1 つの単一ホスト（10.100.10.1 など）、1 つのアドレス範囲（10.100.10.0-10.100.10.255 など）、あるいは複数の単一ホスト、複数のアドレス範囲、または複数のホストと範囲の組み合わせを含むネットワーク/ホスト オブジェクトを指定できます。[選択（Select）] を選択して、リストからオブジェクトを選択するか、新しいオブジェクトを作成します。

- [外部ゾーンを有効にするかどうかを決定する（Decide whether to enable the external zone）]：外部ゾーンは、内部ゾーンまたは不正ゾーン用に構成されていないすべての IP アドレスで構成されます。このゾーンにはアドレスを明示的に割り当てません。[外部ゾーン（External Zone）] タブの [全般（General）] サブタブで、[このゾーンを有効化する（Enable this zone）] チェックボックスを使用して、ゾーンを有効化または無効化できます。外部ゾーンはデフォルトで有効になっています。
- [スキャナしきい値とヒストグラムの設定（Configure scanner thresholds and histograms）]：各ゾーンには、[TCPプロトコル（TCP Protocol）]、[UDPプロトコル（UDP Protocol）]、および [その他のプロトコルOther Protocols] のサブタブがあります。これらのタブで、学習されたヒストグラムを上書きする非デフォルト設定を特定のサービスに対して設定できます。これらの設定の詳細については、異常検出しきい値とヒストグラムの設定 （2259 ページ）を参照してください。

この時点で、基本的な異常検出の設定が完了しました。

ステップ 5 （デバイス ビューだけ）異常検出モードを設定します。この設定は、[仮想センサー（Virtual Sensors）] ポリシーで定義します。次のヒントを考慮して、適切なポリシーを選択します。

- 仮想センサー（親 IPS デバイスで表される vs0 を除く）で異常検出ポリシーを設定した場合は、親 IPS デバイスを選択し、[Virtual Sensors] ポリシーを選択する必要があります。
- ポリシー ビューで [Anomaly Detection] ポリシーを共有ポリシーとして設定した場合は、ポリシーを割り当てる IPS デバイスまたはポリシーを割り当てる仮想センサーをホスティングする IPS デバイスを選択します。

次に、[Virtual Sensors] ポリシーで次の手順を実行します。

a) テーブルで目的の仮想センサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。
b) [仮想センサーの変更（Modify Virtual Sensors）] ダイアログボックスで、異常検出モード設定の適切なオプション（検出、非アクティブ、学習）を選択します。デフォルトの通常の動作モードは [Detect] です。ただし、非対称ノーマライザ モードを使用している場合は、異常検出モードを非アクティブに設定する必要がある場合があります。これらのモードの詳細については、異常検出モード （2249ページ）を参照してください。このダイアログボックスのその他の設定の詳細については、仮想センサー ダイアログボックス （2159 ページ）を参照してください。
c) 異常検出を [Learning] モードにした場合は、目的の学習期間の完了後にモードを忘れずに [Detect] に変更してください。

ステップ 6 必要に応じて、追加のアクションを異常検出シグニチャに追加します。たとえば、攻撃がドロップされるように拒否アクションを追加します。または、イベント アクションのオーバーライドを設定して、リスク レーティングに基づくアクションを追加できます。詳細については、異常検出シグニチャの設定 （2251 ページ）を参照してください。

ステップ 7 必要な場合、ナレッジ ベースを管理します。

（[Learning Accept Mode] タブで）ナレッジベースを自動的に循環するように設定した場合、ナレッジベースは自動的にリフレッシュされるため、手動での操作は不要です。

新しいデータベースの保存だけを行い、それらを使用しないように異常検出を設定した場合は、更新したナレッジベースを定期的に手動でロードする必要があります。Security Manager ではこれを行うことはできません。代わりに IPS Device Manager（IDM）を使用してください。

IDM（または IME）を使用して、ナレッジベースをロード、削除、および名前変更したり、ナレッジベースを外部サーバにアップロードまたは外部サーバからダウンロードしたりできます。実行できる内容の詳細については、IDM または IME のオンライン ヘルプを参照してください。

異常検出の学習受け入れモードの設定

[Anomaly Detection] ポリシーの [Learning Accept Mode] タブを使用して、センサーで新しいナレッジ ベースを何時間ごとに作成するかを設定します。ナレッジ ベースを作成およびロード（[Rotate]）するか、保存（[Save Only]）するかを設定できます。ナレッジ ベースをロードまたは保存する頻度およびタイミングをスケジュールします。

デフォルトで生成されるファイル名は YYYY-Mon-dd-hh_mm_ss（year-month-day-hour_minute_second）です。Mon は現在の月の 3 文字の略語です。

ナレッジ ベースにはツリー構造があり、次の情報を含みます。

- ナレッジ ベース名
- ゾーン名（Zone name）
- プロトコル
- サービス

ナレッジベースには、各サービスのスキャナしきい値とヒストグラムが保存されます。学習受け入れモードを自動に設定し、アクションを循環に設定した場合、新しいナレッジ ベースは 24 時間ごとに作成され、次の 24 時間に使用されます。学習受け入れモードを自動に設定し、アクションを保存だけに設定した場合、新しいナレッジベースは作成されますがロードはされず、現在のナレッジベースが使用されます。学習受け入れモードを自動に設定しない場合、ナレッジ ベースは作成されません。

ヒント Cisco Security Manager を使用してナレッジベースの生成方法を設定できますが、ナレッジベース自体は管理できません。代わりに IPS Device Manager（IDM）または IPS Manager Express（IME）を使用します。IDM（または IME）を使用して、ナレッジ ベースをロード、削除、および名前変更したり、ナレッジ ベースを外部サーバにアップロードまたは外部サーバからダウンロードしたりできます。実行できる内容の詳細については、IDM または IME のオンライン ヘルプを参照してください。

関連項目

- 異常検出モード （2249 ページ）
- 異常検出の設定 （2253 ページ）
- 異常検出しきい値とヒストグラムについて （2258 ページ）

ステップ 1 次のいずれかを実行して、変更する異常検出ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。
- （ポリシービュー）ポリシーセレクタから **[IPS] > [異常検出（Anomaly Detection）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [学習受け入れモード（Learning Accept Mode）] タブをクリックし、次のオプションを設定します。

- [学習ナレッジベースを自動的に受け入れる（Automatically accept learning knowledge base）]：センサーでナレッジベースを自動的に更新するかどうかを指定します。このオプションを選択しない場合、異常検出では新しいナレッジ ベースが自動的には作成されず、このタブの他のオプションを設定できません。
- [アクション（Action）]：ナレッジベースを作成時に保存するかどうかを指定します。

[ローテーション（Rotate）]（デフォルト）を選択した場合、定義したスケジュールに従って新しいナレッジベースが作成されてロードされます。[保存のみ（Save Only）] を選択した場合、新しいナレッジベースが作成されますが、ロードされません。IDM または IME を使用してナレッジ ベースを調べ、異常検出にロードするかどうかを決定できます。

ステップ 3 [スケジュール（Schedule）] フィールドで、新しいナレッジベースを生成するスケジュールを選択します。デフォルトのスケジュールは、定期的に午前 10 時に開始され、24 時間実行されます。次のオプションがあります。

- [定期的（Periodic）]：再帰的な期間に基づいてスケジュールします。次のオプションを設定します。
  - [開始時刻（Start Time）]：hh:mm:ss 形式（24 時間制）での学習期間の開始時刻。
  - [時間単位の学習間隔（Learning Interval in hours）]：新しいナレッジベースを作成する前に異常検出でネットワークから学習する時間の長さ。

- [カレンダーのスケジュール（Calendar Schedule）]：特定の時刻または曜日に基づいてスケジュールします。ダイアログボックスは、[Time of Day] テーブルおよび [Days of the Week] テーブルを表示するように変更されます。これらの時刻は選択したすべての日に適用されます。異なる日に異なる時刻は指定できません。
  - 時間または日を追加するには、該当するテーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックします。時刻は hh:mm:ss 形式（24 時間制）です。日の場合は、リストから日を選択します。
  - 既存の時間または日を編集するには、その時間または日を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
  - 時間または日を削除するには、その時間または日を選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。少なくとも 1 つの時間と日が設定されていることを確認してください。

異常検出しきい値とヒストグラムについて

異常検出では、しきい値およびヒストグラムを使用して、スキャン動作が攻撃であるかどうかを判断します。

学習モード中に、異常検出は各 TCP および UDP ポートのヒストグラムを作成し、その他のプロトコルについては、ネットワークの正常な動作のベースラインを作成します（異常検出モード （2249 ページ）を参照）。たとえば、TCP ポートのヒストグラムには、1 分間に特定の数の宛先アドレスに対して不完全な接続を行う送信元アドレスの「正常」な数がリストされます。ヒストグラムには、少数（5）、中程度の数（20）、および多数（100）の宛先アドレスという 3 つのバケットが含まれます（宛先バケットは固定数です）。サービスおよびゾーンごとに個別のヒストグラムが保持されます（異常検出ゾーン （2250 ページ）を参照）。

たとえば、学習モードでは、TCP ポート 80 に対して次のヒストグラムが作成される場合があります。

宛先アドレスの数	送信元アドレスの数
Low（5）	18
中程度（20）	6
高（100）	2

これらの学習したヒストグラムに加えて、異常検出スキャナではしきい値を設定します。一般的なスキャナしきい値を設定し、特定のサービス（TCP ポート、UDP ポート、またはその他のプロトコル）に対してしきい値を上書き（別の値を設定）できます。各ゾーンには独自のしきい値があります。

異常検出が、ワームがアクティブにスキャンされる検出モードに移行すると、しきい値とヒストグラムは次のように使用されます。

- サービスのしきい値を超えるまで、ヒストグラムは無視されます。たとえば、上記の TCP/80 トラフィックの表について考えます。しきい値が 200（デフォルト）に設定されている場合、スキャナアラートをトリガーするにはスキャナが 1 分間に 200 台のホストをスキャンする必要があります。7 つの送信元アドレスが 50 台のホストをスキャンし（これは、20 ～ 99 の宛先をスキャンするホストが 6 台を超えないと予想されるヒストグラムでは異常です）、単一のスキャナが 100 個のアドレスだけをスキャンした場合、アラートは生成されず、異常は検出されません。
- スキャナしきい値を超過すると、異常検出では、ヒストグラムを使用して、サービスがワームに攻撃されているかどうかが判断されます。この例では、送信元が 200 を超える宛先をスキャンする場合、異常検出はネットワーク内で収集されたアクティビティを評価します。7 台のホストが 50 台のホストをスキャンしたため、ワーム アラートが生成されます。

ワームに攻撃されている場合、異常検出は学習を停止し、現在の学習情報をクリアします。また、一時的にしきい値が下がります。

- ワーム攻撃が検出されると、ワームタイムアウトカウンターが開始されます。タイムアウトに達すると、スキャナがリセットされます。ワーム攻撃が継続する場合は、新しいアラートが生成されます。ワーム タイムアウトは、[Anomaly Detection] ポリシーの [Operation Settings] タブで設定します。

デフォルトのままにした場合、異常検出は、ネットワークの実際の動作から、ネットワークについて学習した内容に基づいてヒストグラムを生成します。ただし、ネットワークを理解していれば、これらのヒストグラムを微調整して誤検知を減らし、ゾーンごとに、TCP/UDP ポートまたはその他のプロトコルごとに予想される（または望ましいまたは許容される）動作の独自の定義を作成できます。関心のあるサービスのみについて独自のヒストグラムを作成し、他のすべてのポートについてはデフォルトのままにすることができます。また、各ゾーンの一般的なスキャナしきい値を設定し、特定のサービスに対しては異なるしきい値を設定できます。

しきい値とヒストグラムを設定する方法の詳細については、異常検出しきい値とヒストグラムの設定 （2259 ページ）を参照してください。

異常検出しきい値とヒストグラムの設定

異常検出では、しきい値およびヒストグラムを使用して、スキャン動作が攻撃であるかどうかを判断します。ほとんどの場合は、異常検出が学習モード中に生成するデフォルトのしきい値とヒストグラムを使用できます（異常検出モード （2249ページ）を参照）。ただし、これらの設定の微調整が必要な場合があります。独自のヒストグラムの作成よりも、しきい値の変更の方が行う可能性が高くなります。

これらの設定値を設定する前に、異常検出しきい値とヒストグラムについて （2258ページ）を読んでください。しきい値とヒストグラムを設定するために、これらがどのように連携して使用されるかを理解する必要があります。

ステップ 1 次のいずれかを実行して、変更する異常検出ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [異常検出（Anomaly Detection）] を選択します。
- （ポリシービュー）ポリシーセレクタから [IPS] > [異常検出（Anomaly Detection）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 しきい値またはヒストグラムを変更するゾーンのタブをクリックします。[内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）]、[外部ゾーン（External Zone）] の各ゾーンに別固の値を設定します。ゾーンの説明については、異常検出ゾーン （2250 ページ）を参照してください。

各ゾーンのタブには、[General]、[TCP Protocol]、[UDP Protocol]、[Other Protocols] の 4 つのサブタブがあります。[General] タブでは、ゾーンの IP アドレスと、ゾーンがイネーブルになっているかどうかを定義します（外部ゾーンには他のゾーンで指定されていないすべての IP アドレスが含まれるため、外部ゾーンに対して特定のアドレスは設定しません）。

その他のタブでは、しきい値とヒストグラムを定義します。

ステップ 3 しきい値またはヒストグラムを変更するプロトコルのタブを選択します。[TCPプロトコル（TCP Protocol）]、[UDPプロトコル（UDP Protocol）]、[その他のプロトコル（Other Protocol）]

各タブで、次のオプションを設定します。

- [有効（Enabled）]：プロトコルに対して異常検出を有効にするかどうか。このオプションで、すべての TCP、UDP、または TCP/UDP 以外のプロトコルでの検出をオフにできます。このオプションを選択解除した場合、タブに設定されている他の設定はすべて無視されます。
- [宛先ポートマップ（Destination Port Map）] または [プロトコル番号マップ（Protocol Number Map）] テーブル：このテーブルには、デフォルト以外のマッピングを設定している TCP/UDP ポート、またはその他のプロトコルが一覧表示されます。デフォルトでは、すべてのポートとプロトコルがイネーブルになり、デフォルト スキャナしきい値が使用されます。

次の場合にのみ、このテーブルに項目を追加します。ポートまたはプロトコルの検出を無効にする。ポートまたはプロトコルに異なるしきい値を設定する。または、学習したヒストグラムの代わりに使用されるポートまたはプロトコルの明示的なヒストグラムを設定する。

- マッピングを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[宛先またはプロトコルマップの追加（Add Dest or Protocol Map）] ダイアログボックスに入力します。詳細については、[Add Dest Port Map]/[Modify Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス （2261 ページ）を参照してください。
- マッピングを編集するには、マッピングを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- マッピングを削除するには、マッピングを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。マッピングを削除すると、サービスはデフォルト設定に戻ります。
- [スキャナしきい値（Scanner Threshold）]：TCP、UDP、またはその他のプロトコルすべてに対するしきい値。このしきい値は、マッピングテーブルでスキャナオーバーライドを設定したサービス以外のすべてのサービスに使用されます。範囲は 5 ～ 1000 です。デフォルトは 200 です。

- [しきい値ヒストグラム（Threshold Histogram）]：TCP、UDP、またはその他のプロトコルすべてに対するデフォルトのヒストグラム。このヒストグラムは、マッピングテーブルでスキャナオーバーライドを設定したサービス以外のすべてのサービスに使用されます。

このテーブルの内容は固定されています。項目の追加や削除はできません。ただし、行を選択して[行の編集（Edit Row）]（鉛筆）をクリックすると、しきい値設定に指定されている送信元アドレスの数を変更できます。 [Histogram] ダイアログボックス （2263 ページ）を参照してください。

ステップ 4 デフォルト以外の設定を定義するゾーンとプロトコルの組み合わせごとに、このプロセスを繰り返します。

[Add Dest Port Map]/[Modify Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス

[Add Dest Port Map]/[Modify Dest Port Map] ダイアログボックスを使用して、TCP または UDP の宛先ポート スキャナ設定を追加または修正し、[Add Protocol Map]/[Modify Protocol Map] ダイアログボックスを使用して、その他のプロトコルのスキャナ設定を追加または修正します。

これらの設定を設定する前に、次の項を参照してください。

- 異常検出しきい値とヒストグラムについて （2258 ページ）
- 異常検出しきい値とヒストグラムの設定 （2259 ページ）

ヒント 異常検出でワーム攻撃を探すために、ポートまたはプロトコルを追加する必要はありません。デフォルトで、すべてのポートとプロトコルが処理されます。特定の設定を設定する必要があるのは、特定のポートまたはプロトコルで検出をオフにする場合、またはデフォルト以外のしきい値またはヒストグラムが必要な場合だけです。

ナビゲーション パス

異常検出ポリシーの [内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）] または [外部ゾーン（External Zone）] タブのサブタブである [TCPプロトコル（TCP Protocol）]、[UDPプロトコル（UDP Protocol）]、または [その他のプロトコル（Other Protocol）] で、[宛先ポートマップ（Destination Port Map）] テーブルまたは [プロトコル番号マップ（Protocol Number Map）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。ここで実行する必要のある手順の詳細については、異常検出しきい値とヒストグラムの設定 （2259 ページ）を参照してください。

フィールド リファレンス

表 *537 :* 宛先ポートまたはプロトコルマップのダイアログボックス

要素	説明
宛先ポート番号 （宛先ポートマップのダイアログボックスのみ）	デフォルト以外の値を定義する宛先ポート番号。指定できる範囲は 0 ～ 65535 です。 単一のポート番号を入力するか、単一のポート番号を含むポートリスト オブジェクトの名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
プロトコル番号 （[Add Protocol Map]/[Modify Protocol Map] ダイアログボックスのみ）	TCP/UDP 以外のプロトコルのプロトコル番号。プロトコル番号のリストについては、 http://www.ietf.org/rfc/rfc1700.txt [英語] で RFC 1700 を参照し、「Protocol Numbers」を検索してください。見出しを探します（この記事の執筆時点では2つ目の検索ヒット）。指定できる範囲は 0 ～ 255 です。 たとえば、ICMP はプロトコル 1 です。
[有効（Enabled）]	このサービスをイネーブルにするかどうか。サービスをイネーブルにしない場合、関連ポートまたはプロトコルは異常検出で処理されません。
[スキャナ設定のオーバーライド（Override Scanner Settings）]	このサービスまたはプロトコルのスキャナ設定を上書きするかどうか。ダイアログボックスの残りのフィールドをイネーブルにするには、このオプションを選択する必要があります。
Scanner Threshold	このポートまたはプロトコルのスキャナしきい値。範囲は 5 ～ 1000 です。デフォルトは 200 です。

要素	説明
[Threshold Histogram] テーブル	このポートまたはプロトコルのヒストグラム。このテーブルを空のままにした場合は、デフォルトのヒストグラムが使用されます。少数、中程度、多数の宛先アドレス用に、それぞれ異なるしきい値レベル（送信元アドレス）の最大 3 行を指定できます。 • しきい値を追加するには、[行の追加（Add Row）] ボタンをクリックし、[Histogram] ダイアログボックス （2263 ページ）に入力します。すでに 3 行がある場合は、[Add] ボタンがディセーブルになります。 • しきい値を編集するには、しきい値を選択し、[行の編集（Edit Row）] ボタンをクリックします。宛先バケットは、テーブルにすでに定義されている宛先バケットには変更できません。 • しきい値を削除するには、しきい値を選択し、[行の削除（Delete Row）] ボタンをクリックします。テーブルに含まれていないバケットは、バケットのデフォルトのヒストグラムを使用します。

[Histogram] ダイアログボックス

[Histogram] ダイアログボックスを使用して、ヒストグラムのエントリを作成または修正します。作成または修正するヒストグラムによって、異常検出で生成されたデフォルトのヒストグラムが上書きされます。これらのヒストグラムの使用方法の詳細については、次の項を参照してください。

- 異常検出しきい値とヒストグラムについて （2258 ページ）
- 異常検出しきい値とヒストグラムの設定 （2259 ページ）

ナビゲーション パス

[Anomaly Detection] ポリシーで、次のいずれかを行います（異常検出の設定 （2253 ページ）を参照）。

- [内部ゾーン（Internal Zone）]、[不正ゾーン（Illegal Zone）]、または [外部ゾーン（External Zone）] タブのサブタブである [TCP プロトコル（TCP Protocol）]、[UDP プロトコル（UDP Protocol）]、または [その他のプロトコル（Other Protocol）] で、[しきい値ヒストグラム（Threshold Histogram）] テーブルの行を選択して [行の編集（Edit Row）] ボタンをクリックします。
- [宛先またはプロトコルマップの追加（Add Dest or Protocol Map）] または [宛先またはプロトコルマップの変更（Modify Dest or Protocol Map）] ダイアログボックスで、[行の追加（Add Row）] ボタンをクリックするか、行を選択して [行の編集（Edit Row）] ボタンを選択します。マップ ダイアログボックスを開く方法については、[Add Dest Port Map]/[Modify

Dest Port Map] または [Add Protocol Map]/[Modify Protocol Map] ダイアログボックス （2261 ページ）を参照してください。

フィールド リファレンス

表 *538 : [Histogram]* ダイアログボックス

要素	説明
[宛先 IP アドレス数（Number of Destination IP Addresses）]	定義しているヒストグラム バケット。バケットには、固定数の宛先アドレスがあります（低（5 アドレス）、中（20）、高（100））。 **ヒント** ヒストグラムには、宛先バケットごとに 1 つのエントリ（低、中、高）を含めることができます。このため、この値は、編集しているヒストグラムにすでに定義されている値には変更できません。
Number of Source IP Addresses	関連付けられた数の宛先アドレスを同時にスキャンすることを許可する送信元アドレスの数。目的の数値を入力します。 範囲は 0 ～ 4096 です。ヒストグラムを編集している場合は、現在の値が表示されます。

第 42 章

グローバル相関の設定

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

センサーが悪意のあるアクティビティのレピュテーションを持つネットワーク デバイスを認識し、それらのアクティビティに対処できるようにグローバル相関を設定できます。グローバル相関を使用すると、世界中のネットワークから収集された悪意のあるアクティビティに関する情報を動的に使用して、悪意のある既知のデバイスを発信元とするイベントのリスク レーティングを変更できます。

グローバル相関を設定するには、センサーで IPS 7.0+ ソフトウェアが実行されている必要があります。グローバル相関は、Cisco IOS IPS デバイスでは使用できません。

この章は次のトピックで構成されています。

- グローバル相関について （2265 ページ）
- レピュテーションについて （2267 ページ）
- ネットワーク参加について （2268 ページ）
- グローバル相関の要件および制限 （2269 ページ）
- グローバル相関インスペクションおよびレピュテーションの設定 （2271 ページ）
- ネットワーク参加の設定 （2272 ページ）

グローバル相関について

センサーが悪意のあるアクティビティのレピュテーションを持つネットワーク デバイスを認識し、それらのアクティビティに対処できるようにグローバル相関を設定できます。シスコの中央脅威データベースである SensorBase に IPS デバイスを加えることにより、グローバル相関更新を受信して取り込むことができます。グローバル相関更新に含まれているレピュテーション データは、ネットワーク トラフィックの分析に組み込まれます。これにより、トラフィックが送信元 IP アドレスのレピュテーションに基づいて拒否または許可されるため、IPS の有効性が高まります。参加している IPS デバイスは、Cisco SensorBase ネットワークにデータを送信し

て戻します。これにより、最新かつグローバルな更新を維持するフィードバック ループがもたらされます。

ヒント Adaptive Security Appliance（ASA; 適応型セキュリティ アプライアンス）の Botnet Traffic Filter 機能は、ネットワークに展開して、悪意のあるアクティビティに対する防衛を実現できるもう 1 つの動的機能です。IPS デバイスでグローバル相関を設定し、ASA ファイアウォールでボットネット トラフィック フィルタリングを設定すると、効果的な統合セキュリティ実装を実現できます。ボットネット トラフィック フィルタリングの詳細については、ファイアウォールの Botnet Traffic Filter ルールの管理 （1163 ページ）を参照してください。

グローバル相関には、次の 3 つの主要機能があります。

- グローバル相関インスペクション：IPS は、攻撃者に関するグローバル相関レピュテーション ナレッジに基づいてアラート処理を変更します。また、センサー上で悪いスコアを持つ攻撃者が認識されると、その攻撃者によるアクションを拒否します。レピュテーションの詳細については、レピュテーションについて （2267 ページ）を参照してください。
- レピュテーション フィルタリング：悪意のある既知のサイトからのパケットに対して自動拒否アクションを適用します。
- ネットワーク参加：センサーは、他のユーザがコミュニティ ナレッジで共有できるように、アラートおよび TCP フィンガープリント データを SensorBase ネットワークに送信します。詳細については、ネットワーク参加について （2268 ページ）を参照してください。

グローバル相関には、次の目的があります。

- アラートをインテリジェントに処理することにより、有効性を高める。
- 悪意のある既知のサイトに対する保護を強化する。
- テレメトリ データを SensorBase ネットワークと共有して、アラートおよびセンサー アクションの可視性をグローバル規模で向上する。
- 設定を簡素化する。
- 情報のアップロードおよびダウンロードを自動的に処理する。

ヒント Report Manager を使用して、グローバル相関により生成されたアラート数と従来の IPS 検査によって生成されたアラート数を比較するレポートを生成できます。Inspection/Global Correlation レポートの詳細については、全般 IPS レポートについて （3585 ページ）を参照してください。レポートの生成については、レポートの起動と生成 （3586 ページ）を参照してください。

グローバル相関の設定方法については、次の項を参照してください。

- グローバル相関の要件および制限 （2269 ページ）

• グローバル相関インスペクションおよびレピュテーションの設定 （2271 ページ）
• ネットワーク参加の設定 （2272 ページ）

レピュテーションについて

レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに関する評価のことです。レピュテーションは、既知のアクティビティに基づいて、特定の攻撃者の IP アドレスから悪意のある動作が開始される可能性を示します。レピュテーションを使用すると、インストール ベースの IPS センサーは、既存のネットワーク インフラストラクチャと協力して、悪意のあるネットワーク デバイスまたは感染した可能性があるネットワーク デバイスを特定できます。

グローバル相関データベースは、デバイスに関するデータを収集し、デバイスにレピュテーション スコアを割り当てることにより、IPS センサーが攻撃のリスク レーティングの調整に使用できる重要なデータを提供します。リスク レーティングは、ネットワーク イベントに悪意があるかどうかの可能性を示します。各シグニチャには、リスク レーティングが割り当てられています。グローバル相関をイネーブルにすると、IPS センサーは、攻撃者のレピュテーションに基づいてスコアを計算し、そのスコアをイベントのリスク レーティングに追加します。更新されたリスク レーティングは、イベント アクション オーバーライドおよびフィルタ ポリシーで使用でき、イベントに適用するアクションを決定するときに役立ちます。

単にアラートを生成するために初期設定されたイベントが存在する場合があります。ただし、攻撃者に悪いレピュテーションがある場合、IPS はリスク レーティングの数値を高くして、Deny Packet Inline アクションを追加するイベント アクション オーバーライド ルールをトリガーできるようにします。したがって、一部の送信元デバイスでは、イベントによって単にアラートが生成されるだけですが、他の送信元デバイスでは、アラートの生成に加えてパケットがドロップされます。

ヒント グローバル相関によってイベントのリスク レーティングが上がるたびに、またはグローバル相関によって Deny Packet Inline アクションまたは Deny Attacker Inline アクションが追加されると、Produce Alert アクションがイベントに追加されます。

グローバル相関データベースは急速に変化するため、センサーは、グローバル相関更新をグローバル相関サーバから定期的にダウンロードする必要があります。

レピュテーション スコアを使用してイベントのリスク レーティングを調整すると、次のメトリックが向上し、センサーの有効性が高まります。

- 実行可能なイベントの false positive（パーセンテージ）。
- 実行可能なイベントにはならない脅威の false negative（パーセンテージ）。
- すべてのイベントの実行可能なイベント（パーセンテージ）。

関連項目

- グローバル相関について （2265 ページ）
- ネットワーク参加の設定 （2272 ページ）
- グローバル相関インスペクションおよびレピュテーションの設定 （2271 ページ）
- ネットワーク参加の設定 （2272 ページ）

ネットワーク参加について

ネットワーク参加によって、シスコはほぼリアルタイムのデータを世界中のセンターから収集できます。カスタマーサイトにインストールされているセンサーは、SensorBase ネットワークにデータを送信できます。これらのデータは、グローバル相関データベースに提供されるため、レピュテーションの正確性が高まります。センサーと SensorBase ネットワーク間の通信には、TCP/IP を介した HTTPS 要求および応答が含まれます。

ネットワーク参加には、次の 3 つのモードがあります。

- **オフ**：ネットワーク参加サーバーは、データの収集、統計情報の追跡、または Cisco SensorBase ネットワークへの接続試行は行いません。
- **部分的参加**：ネットワーク参加サーバーは、データを収集し、統計情報を追跡して、SensorBase ネットワークと通信します。潜在的に機密性が高いと見なされるデータは、フィルタリングによって除外され、送信されません。

（注） センサーを部分的ネットワーク参加用に設定すると、第三者が、内部ネットワークに関する調査情報をグローバル相関データベースから抽出するときに制限が課されます。

- **完全な参加**：ネットワーク参加サーバーは、データを収集し、統計情報を追跡して、SensorBase ネットワークと通信します。収集されたすべてのデータが送信されます。

部分的参加または完全な参加を選択した場合、参加の契約に同意するように要求されます。参加するには契約に同意する必要があります。同意しないと、参加モードを変更できません。

次の表に、収集されるデータおよびデータ収集の目的を示します。

表 *539* : ネットワーク参加データの共有および使用

参加レベル	データのタイプ	目的
一部	プロトコル属性（TCP最大セグメントサイズおよびオプション ストリングなど）。	潜在的脅威を追跡し、脅威による影響をシスコが理解するのに役立ちます。
	攻撃のタイプ（発行されたシグニチャ [シグニチャの ID やバージョンなど]、リスク レーティング、レピュテーションなど）。	現在の攻撃および攻撃の重大度を理解するために使用されます。
	接続している IP アドレスおよびポート。	攻撃元を特定します。
	IPS のサマリー パフォーマンス（CPU 使用率、メモリ使用率、インライン対無差別など）。	製品の有効性を追跡します。
完全（Full）	攻撃対象の IP アドレスおよびポート。	脅威の動作パターンを検出します。

ネットワーク参加を設定する場合、IPS デバイスには、少なくとも 100 MB の使用可能なメモリ、センサーへのネットワーク接続、およびインターネットへのネットワーク接続が必要です。ネットワーク参加の設定の詳細については、ネットワーク参加の設定 （2272ページ）を参照してください。

グローバル相関の要件および制限

次のリストに、IPS デバイスでグローバル相関を設定し、適切に使用するために必要な要件を示します。制限についてもいくつか説明しています。

- **有効なライセンス**：グローバル相関機能が動作するには、有効なセンサーライセンスを取得している必要があります。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。ライセンスの設定については、IPS ライセンス ファイルの更新 （2299ページ）を参照してください。
- **ネットワーク参加の免責事項への同意**：ネットワーク参加を設定することを決定した場合は、免責事項に同意する必要があります。詳細については、ネットワーク参加について（2268 ページ）および ネットワーク参加の設定 （2272 ページ）を参照してください。
- **センサーおよび DNS サーバーや HTTP プロキシの外部接続**：グローバル相関では、センサーが Cisco SensorBase ネットワークに接続する必要があります。これらの機能が動作するには、ドメイン名解決も必要となります。DNS クライアントが稼働している HTTP プロキシ サーバを介して接続するようにセンサーを設定するか、またはセンサーの管理インターフェイスにルーティング可能なインターネット アドレスを割り当て、DNS サーバを

使用するようにセンサーを設定できます。詳細については、DNS サーバの識別 （2113 ページ）および HTTP プロキシ サーバの識別 （2114 ページ）を参照してください。

- **インラインモードのセンサー**：センサーは、インラインモードで動作する必要があります。これにより、グローバル相関機能でインライン拒否アクションを使用できるようになり、その有効性が高まります。
- **グローバル相関機能をサポートするセンサーと IPS バージョン**：センサーは、IPS 7.0+ ソフトウェアを実行している必要があります。Cisco IOS IPS デバイスでグローバル相関を設定することはできません。
- **使用可能な十分なメモリ**：ネットワーク参加を設定するには、IPS デバイスに少なくとも 100 MB の使用可能なメモリが必要です。
- **ポート 80、443 トラフィックのファイアウォールアクセス**：グローバル相関更新は、センサー管理インターフェイスを介して発生するため、センサーとインターネット間にあるすべてのファイアウォールで、ポート 80 および 443 のトラフィックが許可されている必要があります。HTTP プロキシを使用することもできます（HTTP プロキシ サーバの識別 （2114 ページ）を参照）。
- **外部トラフィックへの公開**：グローバル相関データベースには、外部 IP アドレスだけが含まれているため、外部ネットワークと通信できない社内ラボにセンサーを配置した場合は、グローバル相関情報を受信できません。この機能を使用しても何の効果もありません。
- **グローバル相関の更新時にバイパスモードがトリガーされる可能性がある**：シグニチャの更新と同様、センサーがグローバル相関更新を適用するときに、バイパスがトリガーされる可能性があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関更新のサイズによって決まります。バイパスモードをオフにすると、インラインセンサーはアップデートの適用中にトラフィックの送信を停止します。
- **IPv6 アドレスはサポートされない**：グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

関連項目

- グローバル相関について （2265 ページ）
- レピュテーションについて （2267 ページ）
- ネットワーク参加について （2268 ページ）
- グローバル相関インスペクションおよびレピュテーションの設定 （2271 ページ）

• ネットワーク参加の設定 （2272 ページ）

グローバル相関インスペクションおよびレピュテーションの設定

インスペクション/レピュテーション ポリシーを使用して、SensorBase ネットワークからの更新によってイベントのリスク レーティングを調整するようにセンサーを設定します。センサー上のグローバル相関クライアントは、グローバル相関更新サーバおよびファイル サーバと通信して、センサーに使用可能で適用可能な更新を特定します。グローバル相関更新サーバは、センサーにサーバ マニフェスト ドキュメントを提供します。このドキュメントによって、使用可能な更新、およびファイル サーバからそれらを取得する方法が特定されます。センサーは、サーバ マニフェストの情報を使用して、ファイル サーバからアップデート ファイルをダウンロードします。

グローバル相関を設定すると、更新は自動的に定期的な間隔で行われます。デフォルトの間隔は約 5 分ですが、この間隔はグローバル相関サーバで変更できます。センサーは、最初に完全な更新を取得し、その後は定期的に差分更新を適用します。

グローバル相関をオンにしている場合は、悪意のあるホストに対してどれだけ積極的に拒否アクションを実施するかを選択できます。次に、悪意のある既知のホストへのアクセスを拒否するために、レピュテーション フィルタリングをイネーブルにします。発生する可能性があった内容に関するレポートだけが必要な場合は、[Test Global Correlation] をイネーブルにします。これにより、センサーは監査モードに設定され、センサーが実行したと想定されるアクションがイベント内に生成されます。

ヒント Event Viewer で IPS イベントを表示すると、イベント テーブルに追加できるグローバル相関固有の複数のカラムが示されます。これらのカラムは、デフォルトでは表示されないため、使用しているビューに追加する必要があります。一般的なグローバル相関のモニタでは、IPS Device Manager（IDM）を使用して、センサー ヘルス ガジェットをモニタします。完全な機能を備えた IDM を使用するか、デバイス ビューでデバイスを右クリックして[デバイス マネージャ（Device Manager）] を選択して、Security Manager から読み取り専用コピーを開きます。

はじめる前に

- グローバル相関が機能するためには、DNS サーバまたは HTTP プロキシも設定する必要があります。詳細については、DNS サーバの識別 （2113 ページ）または HTTP プロキシ サーバの識別 （2114 ページ）を参照してください。
- グローバル相関を設定する前に、認識しておく必要がある設定上の要件および制限がいくつかあります。詳細については、グローバル相関の要件および制限 （2269 ページ）を参照してください。

関連項目

- グローバル相関について （2265 ページ）
- レピュテーションについて （2267 ページ）
- ネットワーク参加の設定 （2272 ページ）

ステップ 1 次のいずれかを実行して、[Inspection/Reputation] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [グローバル相関（Global Correlation）] > [インスペクション/レピュテーション（Inspection/Reputation）] を選択します。
- （ポリシービュー）ポリシー タイプセレクタから [IPS] > [グローバル相関（Global Correlation）] > [インスペクション/レピュテーション（Inspection/Reputation）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 次を設定します。

- [グローバル相関インスペクション（Global Correlation Inspection）]：グローバル相関インスペクションをイネーブルにするかどうか。オンの場合、センサーは、SensorBase ネットワークからの更新を使用して、リスク レーティングを調整します。インスペクションをディセーブルにするには、このオプションの選択を解除します。
- [グローバル相関の影響（Global Correlation Influence）]：センサーが拒否アクションを開始する場合にどれだけ積極的にグローバル相関情報を使用するか。次のいずれかを選択します。
  - [限定的（Permissive）]：拒否アクションに対する影響は最も少なくなります。
  - [標準（Standard）]：（デフォルト）。 拒否アクションに対する影響は中程度です。
  - [アグレッシブ（Aggressive）]：拒否アクションに対する影響は非常に大きくなります。
- [レピュテーションフィルタリング（Reputation Filtering）]：レピュテーション フィルタリングをオンにするかオフにするかを選択します。オンの場合、センサーは、グローバル相関データベースにリストされている悪意のあるホストへのアクセスを拒否します。
- [グローバル相関をテスト（Test Global Correlation）]：グローバル相関を監査モードに設定するかどうか。監査モードでは、レピュテーション フィルタリングは悪意のある既知のホストへのアクセスを拒否しません。発生した可能性がある内容に関するレポートが単に生成されます。

監査モードを使用すると、実際にホストを拒否することなく、グローバル相関機能をテストできます。望ましい効果が得られた場合は、このオプションの選択を解除して、レピュテーション フィルタリングをアクティブ化します。

ネットワーク参加の設定

ネットワーク参加ポリシーを使用して、データを SensorBase ネットワークに送信するようにセンサーを設定します。完全に参加して、すべてのデータを SensorBase ネットワークに送信する

ようにセンサーを設定するか、またはデータは収集するが、潜在的に機密性の高いデータ（トリガー パケットの宛先 IP アドレスなど）は除くようにセンサーを設定することができます。ネットワーク参加および収集されるデータの詳細については、 ネットワーク参加について（2268 ページ）を参照してください。

関連項目

- グローバル相関について （2265 ページ）
- レピュテーションについて （2267 ページ）
- グローバル相関の要件および制限 （2269 ページ）
- グローバル相関インスペクションおよびレピュテーションの設定 （2271 ページ）

ステップ 1 次のいずれかを実行して、[Network Participation] ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS]>[グローバル相関（Global Correlation）]>[ネットワーク参加（Network Participation）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [IPS]>[グローバル相関（Global Correlation）]>[ネットワーク参加（Network Participation）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [ネットワーク参加（Network Participation）] リストから、次に示す参加レベルを選択します。

- [オフ（Off）]：いずれのデータも SensorBase ネットワークに提供されません。
- [部分的（Partial）]：データが SensorBase ネットワークに提供されますが、潜在的に機密性の高いデータは除かれます。

（注） センサーを部分的ネットワーク参加用に設定すると、第三者が、内部ネットワークに関する調査情報をグローバル相関データベースから抽出するときに制限が課されます。

- [フル（Full）]：すべてのデータが SensorBase ネットワークに提供されます。

ステップ 3 [Full] または [Partial] を選択した場合、[Save] をクリックすると、[Network Participation Disclaimer] ダイアログボックスが開き、免責事項を読んで同意するように要求されます。免責事項をよく読みます。同意する場合は、[同意する（Agree）] をクリックします。

[同意しない（Disagree）] をクリックした場合、ネットワーク参加をイネーブルにすることはできません。設定を [Off] に変更し、ポリシーを保存します。

第 43 章

Attack Response Controller でのブロッキングとレート制限の設定

ブロックまたはレート制限を実装して攻撃を制御するようにIPSデバイスを設定できます。ブロッキングとレート制限は、主に無差別モードで動作している場合に使用します。インラインモードで動作している場合は、IPS でトラフィックをドロップする方がはるかに効率的です。ブロッキングとレート制限は、IPS の要求時に他のデバイスが実装するアクションです。このため、ブロッキングとレート制限の設定は、単純なインライン拒否よりも複雑な設定になります。

ブロッキングまたはレート制限を設定するには、ブロッキングを実行するネットワークデバイスを特定する必要があります。ブロッキングを実行するネットワークデバイスは、ブロッキングデバイスと呼ばれます。ブロッキングをサポートするために、Cisco IOS ルータおよびCatalyst 6500 スイッチ、Cisco セキュリティ アプライアンス（ASA、PIX、および FWSM）、Catalyst オペレーティング システムを実行しているCatalyst 6500/7600 デバイスなど、多くのネットワークデバイスを使用できます。別のIPSデバイスをメインブロッキングセンサーとして動作するように設定することもできます。

- IPS ブロッキングについて （2275 ページ）
- IPS のブロッキングおよびレート制限の設定 （2282 ページ）
- [Blocking] ページ （2285 ページ）

IPS ブロッキングについて

IPS の Attack Response Controller（ARC）コンポーネントは、攻撃しているホストとネットワークからのアクセスをブロックすることで、疑わしいイベントに対してネットワークデバイスを管理します。ARC は、管理しているデバイスの IP アドレスをブロックします。他のメインブロッキングセンサーを含め、管理しているすべてのデバイスに同じブロックを送信します。ARC は、ブロックの時間をモニタし、時間の経過後にブロックを削除します。

（注） ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IPS のマニュアルおよび設定インターフェイスでは、Network Access Controller、nac、および network-access という名前で呼ばれています。

ARCは、7秒以内に新しいブロックのアクション応答を完了します。ほとんどの場合は、より短い時間でアクション応答を完了します。このパフォーマンス目標を達成するために、センサーでのブロックの実行レートが高すぎたり、管理するブロッキングデバイスおよびインターフェイスが多すぎたりしないように設定してください。最大ブロック数は250以下にし、最大ブロッキング項目数は 10 以下にすることを推奨します。ブロッキング項目の最大数を計算するために、セキュリティ アプライアンスはブロッキング コンテキストあたり 1 つのブロッキング項目としてカウントします。ルータは、ブロッキング インターフェイス/方向あたり 1 つのブロッキング項目としてカウントします。Catalyst ソフトウェアを実行しているスイッチは、ブロッキング VLAN あたり 1 つのブロッキング項目としてカウントします。推奨される制限を超えた場合、ARC はブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりすることがあります。

マルチ コンテキスト モードで設定されているセキュリティ アプライアンスでは、Cisco IPS は VLAN 情報をブロック要求に含めません。したがって、ブロックされる IP アドレスが各セキュリティ アプライアンスに対して正しいことを確認する必要があります。たとえば、センサーは、VLAN A に対して設定されているセキュリティ アプライアンス カスタマー コンテキストでパケットをモニタリングする一方で、VLAN B に対して設定されている別のセキュリティ アプライアンス カスタマー コンテキストでブロッキングしている場合があります。VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを参照します。

（注） ブロッキングは、マルチ コンテキスト モードの管理コンテキストでは FWSM でサポートされません。

ブロックには次の 3 種類があります。

- ホスト ブロック：特定の IP アドレスからのすべてのトラフィックをブロックします。

シグニチャがトリガーされたときに自動ホストブロックを開始するように IPS を設定するには、[ホストのブロックを要求（Request Block Host）] イベントアクションをシグニチャに追加するか、イベント アクション オーバーライド ポリシーを使用してリスクレーティングに基づくイベントに追加します。イベント アクション オーバーライドの設定 （2227ページ）およびシグニチャの設定 （2169 ページ）を参照してください。

- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックによって、接続ブロックからホストブロックにブロックが自動的に切り替えられます。

シグニチャがトリガーされたときに自動接続ブロックを開始するように IPS を設定するには、[接続のブロックを要求（Request Block Connection）] イベントアクションをシグニチャに追加

するか、イベント アクション オーバーライド ポリシーを使用してリスクレーティングに基づくイベントに追加します。

- ネットワーク ブロック：特定のネットワークからのトラフィックをすべてブロックします。

ホストブロックと接続ブロックは、手動で開始するか、シグニチャがトリガーされたときに自動的に開始できます。ネットワーク ブロックは手動でだけ開始できます。ネットワーク ブロックは Security Manager から開始できません。代わりに IPS Device Manager を使用します。

ヒント　接続ブロックとネットワーク ブロックは、セキュリティ アプライアンス（ファイアウォール）ではサポートされません。セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

（注）　ブロッキングとセンサーのパケット ドロップ機能を混同しないでください。センサーでは、インライン モードのセンサーに対してパケットのインライン拒否、接続のインライン拒否、および攻撃者のインライン拒否のアクションが設定されている場合にパケットをドロップできます。

Cisco IOS ソフトウェア デバイス（ルータおよび Catalyst 6500 シリーズ スイッチ）では、ARC は、ACL を適用することでブロックを作成します。Catalyst オペレーティング システムを実行する Catalyst 6500/7600 デバイスでは、ARC は VACL を適用することでブロックを作成します。ACL および VACL は、インターフェイス方向または VLAN 上のデータ パケットの経路を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可条件と拒否条件が含まれます。セキュリティアプライアンスでは、**shun** コマンドが ACL の代わりに使用されます。

ヒント　ブロッキングデバイスとして設定できる特定のデバイスおよびオペレーティング システムバージョンのリストについては、使用している IPS ソフトウェアバージョンの『*Installing and Using Cisco Intrusion Prevention System Device Manager*』の「Configuring Attack Response Controller for Blocking and Rate Limiting」の章で、サポートされるデバイス情報を参照してください。これらの資料は、Cisco.com の http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/products_installation_and_configuration_guides_list.html [英語] から入手できます。

次の各項で、IPS ブロッキングについて詳細に説明します。

- ブロック適用のストラテジ　（2278 ページ）
- レート制限について　（2279 ページ）
- ルータおよびスイッチ ブロッキング デバイスについて　（2279 ページ）

- メインブロッキングセンサーについて （2281 ページ）
- IPS のブロッキングおよびレート制限の設定 （2282 ページ）
- [Blocking] ページ （2285 ページ）

ブロック適用のストラテジ

ブロッキングは、イベントの発生時に、イベントに [Request Block Connection] または [Request Block Host] イベント アクションが含まれる場合にだけ実行されます。これらのイベント アクションは、通常、拒否アクションを使用して不要なトラフィックをドロップするインライン モードで IPS を操作している場合には不要です。

ブロッキング アクションの実装が必要になる状況は次のとおりです。

- 無差別モード：無差別モードで実行している場合、IPS は拒否アクションを実装できません。このため、ホストからのトラフィックを防ぐには、ブロッキングを実装する必要があります。
- インラインモード：インラインモードでは、拒否アクションを実装して不要なトラフィックを即時にドロップできます。ただし、ネットワークの他のセグメントを保護するためにブロッキング アクションの追加が必要な場合があります。

たとえば、ネットワークが A、B、C、D、E の 5 つのサブネットから構成され、これらの各セグメントに、それをモニタしているインライン IPS デバイスがあるとします。サブネット A の IPS が攻撃を識別した場合、IPS は拒否アクションを使用してサブネット A を保護できるだけでなく、ブロック要求アクションを使用して B、C、D、E を保護するファイアウォールを設定し、攻撃がこれらの他のサブネットをターゲットとする前に攻撃者を避けることもできます。この例では、1 つの IPS をメインブロッキングセンサーとして指定し、他の 4 つの IPS センサーで、メインブロッキングセンサーを介したブロッキングを実行させます。

次の手法を使用して、ブロック要求アクションをイベントに追加します。

- イベント アクション オーバーライド ポリシー：イベント アクション オーバーライド ルールを設定して、イベントのリスク レーティングに基づいてすべてのイベントにアクションを追加します。これは単純なアプローチです。拒否アクションの追加に使用されるのと同じリスク レーティングでブロック要求アクションを追加できます。詳細については、イベント アクション オーバーライドの設定 （2227 ページ）を参照してください。
- シグニチャ ポリシー：ブロック要求アクションを個々のシグニチャに追加できます。これには、各シグニチャを編集してアクションを追加する必要があります。これは時間のかかるアプローチとなる場合がありますが、最も関心のあるイベント タイプだけにブロッキングを設定できます。詳細については、シグニチャの設定 （2169 ページ）を参照してください。

関連項目

- IPS ブロッキングについて （2275 ページ）

• メインブロッキングセンサーについて （2281 ページ）
• インターフェイス モードについて （2129 ページ）
• IPS のブロッキングおよびレート制限の設定 （2282 ページ）
• [Blocking] ページ （2285 ページ）

レート制限について

Attack Response Controller（ARC）は、保護されているネットワーク内のトラフィックのレート制限を行います。レート制限により、センサーはネットワークデバイス上の指定したトラフィック クラスのレートを制限できます。レート制限応答は、Host Flood エンジンと Net Flood エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC では、Cisco IOS 12.3 以降を実行しているネットワーク デバイスにレート制限を設定できます。メインブロッキングセンサーは、レート制限要求をブロッキング転送センサーに転送することもできます。

シグニチャにレート制限を追加するには、[Request Rate Limit] アクションを追加する必要があります。次に、シグニチャ パラメータを編集して、Event Actions Settings フォルダにこれらのシグニチャのパーセンテージを設定します。

ヒント　レート制限は手動でも実装できますが、Security Manager を使用した実装はできません。代わりに IPS Device Manager を使用します。

ブロッキング デバイスでは、レート制限が設定されているインターフェイス/方向にサービス ポリシーを適用しないでください。適用した場合は、レート制限アクションが失敗します。レート制限を設定する前に、インターフェイス/方向にサービス ポリシーがないことを確認し、存在する場合には削除します。ARC では、ARC が以前に追加したものでないかぎり、既存のレート制限は削除されません。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、ACL および class-map エントリを使用してトラフィックを識別し、policy-map および service-policy エントリを使用してトラフィックをポリシングします。

ルータおよびスイッチ ブロッキング デバイスについて

Cisco IOS ソフトウェアを実行しているルータまたは Catalyst 6500/7600 デバイス、あるいは Catalyst オペレーティング システムを実行している Catalyst 6500/7600 デバイスを使用して、ネットワークに IPS ブロッキングを実装できます。ルータまたはスイッチを使用する場合、Attack Response Controller（ARC）では、拡張 ACL（IOS デバイス上）または VLAN ACL（Catalyst OS デバイス上）を設定してブロックが実装されます。これらの ACL と VACL は、同じ方法で作成および管理されます。

レート制限でも ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、ACL および class-map エントリを使用してトラフィックを識別し、policy-map および service-policy エントリを使用してトラフィックをポリシングします。

ヒント　IPS は、Cisco IOS ソフトウェアを実行している Catalyst 6500/7600 デバイスをルータと同等と見なします。これらのデバイスをブロッキングデバイスとして追加する場合は、ルータとして追加します。

ルータ インターフェイスまたはスイッチ VLAN をブロッキング インターフェイスとして設定する場合は、オプションで、pre-ACL/VACL および post-ACL/VACL の名前を指定できます。ACL 名または VACL 名の指定は任意ですが、インターフェイスまたは VLAN に ACL または VACL を設定した場合は、それらも IPS に対して指定する必要があります。そうしないと、その ACL または VACL は ARC によってデバイス設定から削除されます。

pre-ACL/VACL および post-ACL/VACL には次の用途があります。

- Pre-Block ACL/VACL は、主にセンサーでブロックしない対象を許可する場合に使用します。パケットが ACL/VACL に対してチェックされると、最初に一致した行によってアクションが決定されます。最初の行が Pre-Block ACL/VACL の permit 行と一致する場合、パケットは、ACL/VACL であとに（自動ブロックからの）deny 行がある場合でも許可されます。Pre-Block ACL/VACL では、ブロックの結果の deny 行をオーバーライドできます。
- Post-Block ACL/VACL は、同じインターフェイスまたは方向で追加のブロッキングまたは許可を行う場合に最もよく使用されます。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合は、その既存の ACL を Post-Block ACL/VACL として使用できます。Post-Block ACL/VACL がない場合、センサーは新しい ACL/VACL の最後に permit ip any any を挿入します。

IOS ソフトウェア ブロッキング デバイスを Security Manager で管理している場合は、ブロッキングデバイスを選択し、[ツール（Tools）]> [設定のプレビュー（Preview Config）] を選択することで ACL 名を識別できます。インターフェイス設定で **ip access-group** コマンドを検索し、方向を確認します。たとえば、次の行は、CSM_FW_ACL_GigabitEthernet0/1 という名前の ACL が、GigabitEthernet0/1 インターフェイスに接続された In 方向に存在することを示しています。

```
interface GigabitEthernet0/1
  ip access-group CSM_FW_ACL_GigabitEthernet0/1 in
```

この例では、ブロッキング インターフェイスとして GigabitEthernet0/1 を In 方向に設定する場合、pre-ACL または post-ACL として、CSM_FW_ACL_GigabitEthernet0/1 を必ず指定してください。ほとんどの場合は、ACL を post-ACL として指定します。これにより、比較的短い IPS ブロッキング ACL によって望ましくないトラフィックが最初に除外され、その後、ブロッキング デバイスによって他のアクセス ルールが実行されます。

Security Manager では Catalyst OS デバイスが管理されないため、VACL 名を判断するには Security Manager の外部で Catalyst OS デバイス設定を調べる必要があります。IOS ソフトウェアを実行する Catalyst 6500/7600 デバイスにも VACL がある場合がありますが、デバイスが IOS ソフト

ウェアを実行している場合、IPS は Catalyst 6500/7600 VLAN で VLAN ブロッキングを実行しないことに注意してください。

センサーは、起動時に 2 つの ACL/VACL の内容を読み取ります。センサーは次のエントリをこの順序で持つ第 3 の ACL/VACL を作成し、この結合された ACL/VACL がインターフェイスまたは VLAN に適用されます。

1. センサー IP アドレス、またはセンサーの NAT アドレス（指定されている場合）がある **permit** 行

[Blocking] ポリシーの [General] タブで [Allow Sensor IP address to be Blocked] オプションを選択した場合、この permit エントリは追加されません。詳細については、[General] タブ、IPS ブロッキング ポリシー （2288 ページ）を参照してください。

1. Pre-Block ACL/VACL（指定されている場合）。
2. IPS によって生成された任意のアクティブ ブロック（deny ステートメント）。
3. Post-Block ACL/VACL（指定されている場合）。

Post-Block ACL/VACL を指定しない場合は、すべてのフィルタされないトラフィックを許可するために **permit ip any any** エントリが追加されます。これにより、インターフェイス ACL を終了する通常の暗黙の deny any が否定されます。

Catalyst OS を使用している場合、IDSM-2 は新しい VACL の最後に **permit ip any any capture** を挿入します。

ARC がデバイスを管理し、そのデバイスで ACL/VACL を設定する必要がある場合は、最初にブロッキングをディセーブルにする必要があります。ユーザと ARC の両方が同じデバイスで同時に変更を加える状況を回避する必要があります。この状況が発生すると、デバイスまたは ARC でエラーが発生します。Pre-Block ACL/VACL または Post-Block ACL/VACL を修正する必要がある場合は、次の手順に従います。

1. センサーでブロッキングをディセーブルにします。

一時的な変更を加えるため、デバイスで IPS Device Manager（IDM）を使用して、ブロッキングをディセーブルにし、再びイネーブルにできます。または、Security Manager の [Blocking] ポリシーの [General] タブで [Enable Blocking] オプションを選択解除してから、IPS センサーに設定を展開できます。ブロッキングを再びイネーブルにするには、[Enable Blocking] オプションをもう一度選択し、IPS センサーに設定を展開します。

1. デバイスの設定に変更を加えます。たとえば、Security Manager でブロッキング デバイスを管理する場合は、更新した設定を展開し、デバイスがリロードされるまで待ちます。
2. センサーでブロッキングを再びイネーブルにします。

メインブロッキングセンサーについて

複数のセンサー（ブロッキング転送センサー）が、1 つ以上のデバイスを制御する、指定したメインブロッキングセンサーに、ブロッキング要求を転送できます。メインブロッキングセン

サーは、他の 1 つ以上のセンサーに代わって 1 つ以上のデバイスでブロッキングを制御するセンサーで実行されている ARC です。ブロッキングまたはレート制限要求がイベントアクションとして設定されているシグニチャが出現した場合、センサーはブロック要求またはレート制限要求をメインブロッキングセンサーに転送し、そのセンサーがブロックまたはレート制限を実行します。

メインブロッキングセンサーを追加する場合は、センサーあたりのブロッキングデバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のファイアウォールと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、メインブロッキングセンサーに残りの 10 個を割り当てることができます。

[Blocking] ページ （2285 ページ）の説明に従って、[ブロッキング（Blocking）] ポリシーの [プライマリブロッキングセンサー（Primary Blocking Sensors）] タブで、メインブロッキングセンサーを設定します。

メインブロッキングセンサーを設定する場合は、次のヒントを考慮してください。

- 2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをメインブロッキングセンサーとして設定してデバイスを管理し、もう一方のセンサーでメインブロッキングセンサーに要求を転送できます。
- ブロッキング転送センサーで、マスターブロッキングセンサーとして機能するリモートホストを識別します。メインブロッキングセンサーでは、[許可ホスト（Allowed Hosts）] ポリシーを使用してアクセスリストにブロッキング転送センサーを追加する必要があります。 許可ホストの識別 （2091 ページ）を参照してください。
- メインブロッキングセンサーが Web 接続に TLS を必要とする場合は、メイン ブロッキング センサー リモート ホストの X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。センサーでは TLS がデフォルトでイネーブルになりますが、このオプションは変更できます。詳細については、[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス （2291 ページ） を参照してください。
- 通常、メインブロッキングセンサーはネットワークデバイスを管理するように設定します。ブロッキング転送センサーは、通常は他のネットワーク デバイスを管理するようには設定されていませんが、これを行うことは可能です。
- 1 つのセンサーだけがデバイス上のすべてのブロッキング インターフェイスを制御する必要があります。

IPS のブロッキングおよびレート制限の設定

任意のシグニチャで [Request Block Host]、[Request Block Connection]、または [Request Rate Limit] アクションを使用する場合、またはイベント アクション オーバーライド ポリシーを使用してこれらのアクションをイベントに追加する場合は、ブロッキングデバイスを設定する必要があります。これらのアクションを使用しない場合は、ブロッキングデバイスを設定する必要はありません。

ブロッキングを設定する前に、次の各項を参照してください。

- IPS ブロッキングについて （2275 ページ）
- ブロック適用のストラテジ （2278 ページ）
- レート制限について （2279 ページ）
- ルータおよびスイッチ ブロッキング デバイスについて （2279 ページ）
- メインブロッキングセンサーについて （2281 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）]>[セキュリティ（Security）] >[ブロッキング（Blocking）] を選択します。
- （ポリシー ビュー）[IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

ブロッキング ポリシーの概要については、 [Blocking] ページ （2285 ページ）を参照してください。

ステップ 2 [General] タブで、デフォルト以外の値が必要な設定を変更します。ただし、デフォルト値はほとんどのネットワークに適しています。設定の詳細については、[General] タブ、IPS ブロッキング ポリシー （2288 ページ） を参照してください。

ステップ 3 [ユーザプロファイル（User Profiles）] タブをクリックし、ブロッキングデバイスへのログインに必要なユーザプロファイルを作成します。

- プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ユーザープロファイルの追加（Add User Profile）] ダイアログボックスに入力します（ [Add User Profile]/[Modify User Profile] ダイアログボックス （2291 ページ）を参照）。
- プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。プロファイルを削除する前に、ブロッキング デバイスによって現在使用されていないことを確認してください。

ステップ 4 メインブロッキングセンサーについて （2281 ページ）で説明するようにメインブロッキングセンサーを使用する必要がある場合は、[プライマリブロッキングセンサー（Primary Blocking Sensors）] タブをクリックし、次の操作を行います。

- メインブロッキングセンサーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[メインブロッキングセンサーの追加（Add Main Blocking Sensor）] ダイアログボックスに入力します（[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス （2291 ページ）を参照）。
- メインブロッキングセンサーを編集するには、メインブロッキングセンサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。

- メインブロッキングセンサーを削除するには、メインブロッキングセンサーを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 5 （メインブロッキングセンサーだけを使用するのでないかぎり）ブロッキングデバイスを指定します。デバイスを適切なタブに追加する必要があります。

- [ルータ（Routers）] タブ：IOS ソフトウェアを実行している Catalyst 6500 スイッチを含むすべての Cisco IOS ソフトウェアデバイスの場合。
- [ファイアウォールFirewalls] タブ：ASA、PIX、および FWSM の場合。
- [Catalyst 6K] タブ：Catalyst オペレーティングシステムを実行している Catalyst 6500/7600 デバイスの場合。

各タブでの設定手順は同じです。

- デバイスを追加するには、[行の追加（Add Row]） ボタンをクリックし、[ルータデバイスの追加（Add Router Device）]/[ファイアウォールデバイスの追加（Add Firewall Device）]/[Cat6Kデバイスの追加（Add Cat6K Device）] ダイアログボックスに入力します（ [Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （2293 ページ）を参照）。
- デバイスを編集するには、そのデバイスを選択して [行の編集（Edit Row）] ボタンをクリックします。
- デバイスを削除するには、そのデバイスを選択して [行の削除（Delete Row）] ボタンをクリックします。

ステップ 6 [ブロックしないホスト（Never Block Hosts）]/[ブロックしないネットワーク（Never Block Networks）] タブをクリックし、ブロックしないホストとネットワークを指定します。これらのリストはブロッキングアクションに影響しますが、制限アクションには影響しません。信頼できるネットワークとホストを識別します。

- ホストまたはネットワークを追加するには、該当するテーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[ブロックしないホストの追加（Add Never Block Host）]/[ブロックしないネットワークの追加（Add Never Block Network）] ダイアログボックスに入力します（ [Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス （2297 ページ）を参照）。
- ホストまたはネットワークを編集するには、ホストまたはネットワークを選択し、[行の編集（Edit Row）] ボタンをクリックします。
- ホストまたはネットワークを削除するには、ホストまたはネットワークを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Blocking] ページ

[Blocking] ページを使用して、IPS センサーのブロッキング プロパティを設定します。シグニチャまたはイベント アクション ポリシーで [Request Block Connection]、[Request Block Host]、または [Request Rate Limit] のイベント アクションを使用する場合にだけ、ブロッキング ポリシーを設定します。ブロッキング ホストは、これらのアクションが割り当てられているイベントにだけ使用されます。

ヒント　ブロックしないホストとネットワークのリストは、[Request Block Connection] および [Request Block Host] イベント アクションにだけ適用されます。リストはレート制限には影響せず、[Deny Packet Inline] などの拒否アクションにも影響しません。ホストとネットワークを拒否アクションまたはレート制限アクションから免除するには、イベント アクション フィルタ ルールを使用し、ホストとネットワークを攻撃者として指定し、イベントからアクションを削除します。詳細については、イベント アクション フィルタの設定（2216 ページ）を参照してください。

ナビゲーション パス

- （デバイス ビュー）ポリシー セレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択します。
- （ポリシー ビュー）[IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。

関連項目

- IPS のブロッキングおよびレート制限の設定　（2282 ページ）
- IPS ブロッキングについて　（2275 ページ）
- ブロック適用のストラテジ　（2278 ページ）
- レート制限について　（2279 ページ）
- ルータおよびスイッチ ブロッキング デバイスについて　（2279 ページ）
- メインブロッキングセンサーについて　（2281 ページ）
- IPS イベント アクションについて　（2213 ページ）

フィールド リファレンス

表 *540 : IPS* ブロッキング ポリシー

要素	説明
[一般（General）] タブ	ブロッキングとレート制限をイネーブルにするために必要な基本設定。[General] タブのオプションの詳細については、[General] タブ、IPS ブロッキング ポリシー （2288 ページ）を参照してください。
[User Profiles] タブ	ブロッキングデバイスにログインするための接続クレデンシャル情報プロファイル。ブロッキング デバイスを定義する前に、デバイスへのログインに必要なユーザ プロファイルを作成します。この表には、プロファイル名、ユーザ名、および固定数のアスタリスクでマスクされたパスワードが表示されます。 • プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ユーザープロファイルの追加（Add User Profile）] ダイアログボックスに入力します（[Add User Profile]/[Modify User Profile] ダイアログボックス （2291 ページ）を参照）。 • プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。プロファイルを削除する前に、ブロッキングデバイスによって現在使用されていないことを確認してください。
[プライマリ ブロッキング センサー（Primary Blocking Sensors）] タブ	メインブロッキング IPS センサー（メインブロッキングセンサーについて （2281 ページ）を参照）。メインブロッキングセンサーは、他の IPS デバイスのブロックを管理します。このテーブルには、メインブロッキングセンサーの IP アドレス（またはネットワーク/ホストオブジェクト）、そのセンサーにログインするためのユーザー名とパスワード、接続に使用するポート、およびログインに TLS が使用されるかどうかが表示されます。 • メインブロッキングセンサーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[プライマリブロッキングセンサーの追加（Add Master Blocking Sensor）] ダイアログボックスに入力します（メインブロッキングセンサーについて （2281 ページ）を参照）。 • メインブロッキングセンサーを編集するには、メインブロッキングセンサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • メインブロッキングセンサーを削除するには、メインブロッキングセンサーを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
[Router] タブ	ブロッキング デバイスまたはレート制限デバイスとして使用する IOS ルータと（IOS ソフトウェアを実行している）Catalyst 6500/7600 デバイス。このテーブルに、デバイスの IP アドレス（またはネットワーク/ホスト オブジェクト）、デバイスへのログインに使用する通信方法、センサーの NAT アドレス（NAT が使用されない場合は 0.0.0.0）、デバイスへのログインに使用するプロファイルの名前、およびデバイスの応答機能（ブロッキング、レート制限、またはその両方）が表示されます。 • ルータを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ルータデバイスの追加（Add Router Device）] ダイアログボックスに入力します（[プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス （2291 ページ）を参照）。 • ルータを編集するには、ルータを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルータを削除するには、ルータを選択し、[行の削除（Delete Row）] ボタンをクリックします。
[Firewall] タブ	ブロッキング デバイスとして使用する ASA、PIX、および FWSM デバイス。この表に、デバイスの IP アドレス（またはネットワーク/ホスト オブジェクト）、デバイスへのログインに使用する通信方法、センサーの NAT アドレス（NAT が使用されない場合は 0.0.0.0）、デバイスへのログインに使用するプロファイルの名前を示します。 • ファイアウォールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ファイアウォールデバイスの追加（Add Firewall Device）] ダイアログボックスに入力します（ [Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （2293 ページ）を参照）。 • ファイアウォールを編集するには、ファイアウォールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ファイアウォールを削除するには、ファイアウォールを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
[Catalyst 6K] タブ	ブロッキング デバイスとして使用する、Catalyst ソフトウェアを使用している Catalyst 6500/7600 デバイス。この表に、デバイスの IP アドレス（またはネットワーク/ホスト オブジェクト）、デバイスへのログインに使用する通信方法、センサーの NAT アドレス（NAT が使用されない場合は 0.0.0.0）、デバイスへのログインに使用するプロファイルの名前を示します。 ヒント　Cisco IOS ソフトウェアを実行している Catalyst 6500/7600 デバイスには、このタブを使用しないでください。代わりに、[Router] タブを使用します。 • Catalyst OS デバイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Cat6Kデバイスの追加（Add Cat6K Device）] ダイアログボックスに入力します（[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （2293 ページ）を参照）。 • Catalyst OS デバイスを編集するには、そのデバイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • Catalyst OS デバイスを削除するには、そのデバイスを選択し、[行の削除（Delete Row）] ボタンをクリックします。
[Never Block Hosts]/[Never Block Networks]	ブロックしないホストとネットワーク。ホストとネットワークは別々の表に表示されます。これらの表には、ホストまたはネットワークの IP アドレスまたはネットワーク/ホスト オブジェクトが表示されます。これらのリストは、レート制限アクションに影響せず、拒否アクションにも適用されません。 • ホストまたはネットワークを追加するには、該当するテーブルの下にある [行の追加（Add Row）] ボタンをクリックし、[ブロックしないホストの追加（Add Never Block Host）]/[ブロックしないネットワークの追加（Add Never Block Network）] ダイアログボックスに入力します（[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス （2297 ページ）を参照）。 • ホストまたはネットワークを編集するには、ホストまたはネットワークを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ホストまたはネットワークを削除するには、ホストまたはネットワークを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[General] タブ、IPS ブロッキング ポリシー

[Blocking] ポリシーの [General] タブを使用して、ブロッキングとレート制限をイネーブルにするために必要な基本設定を設定します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択します。必要に応じて、[全般（General）] タブを選択します。
- （ポリシービュー）[IPS] > [プラットフォーム（Platform）] > [セキュリティ（Security）] > [ブロッキング（Blocking）] を選択してから、既存のポリシーを選択するか、新しいポリシーを作成します。必要に応じて、[全般（General）] タブを選択します。

関連項目

- IPS ブロッキングについて （2275 ページ）
- IPS のブロッキングおよびレート制限の設定 （2282 ページ）
- [Blocking] ページ （2285 ページ）

フィールド リファレンス

表 *541 : [General]* タブ、*IPS* ブロッキング ポリシー

要素	説明
Log All Block Events and Errors	開始から終了までブロックに続くイベントおよび発生したエラー メッセージをログに記録するかどうか。ブロックがデバイスに追加されるかデバイスから削除されると、イベントがログに記録されます。これらすべてのイベントおよびエラーをログに記録する必要はない可能性があります。このオプションをディセーブルにすると、新しいイベントとエラーが抑止されます。デフォルトではイネーブルになっています。 （注） すべてのブロック イベントとエラーの記録はレート制限にも適用されます。
Enable NVRAM Write	Attack Response Controller（ARC）が最初に接続するときにルータが Non-Volatile RAM（NVRAM; 不揮発性 RAM）に書き込むようにするかどうか。イネーブルになっている場合は、ACL が更新されるたびに NVRAM が書き込まれます。デフォルトではディセーブルになっています。 NVRAM の書き込みをイネーブルにすると、ブロッキングとレート制限に対するすべての変更が NVRAM に必ず書き込まれます。ルータが再起動された場合でも、適切なブロックとレート制限がアクティブになります。NVRAM の書き込みがディセーブルになっている場合、ルータの再起動後にブロッキングまたはレート制限が行われない期間が短時間発生します。NVRAM 書き込みをイネーブルにしない場合、NVRAM の寿命が延び、新しいブロックとレート制限の設定にかかる時間が短縮されます。

要素	説明
Enable ACL Logging	ARC で、アクセス コントロール リスト（ACL）または VLAN ACL（VACL）のブロック エントリにログ パラメータを追加するかどうか。これにより、デバイスはパケットがフィルタ処理されるときに syslog イベントを生成します。このオプションは、ルータとスイッチにだけ適用されます。デフォルトではディセーブルになっています。
Allow Sensor IP address to be Blocked	センサー IP アドレスをブロックできるかどうか。デフォルトではディセーブルになっています。 **ヒント** センサー アドレスのブロックを許可した場合、IPS は、IPS アドレスを許可するために明示的な permit エントリをインターフェイス ACL に追加しません。IPS アドレスがデバイス ACL によって許可されていることを確認する必要があります。そうしないと、IPS はデバイスでブロッキングを実装できません。
Enable Blocking	ホストのブロッキングおよびレート制限をイネーブルにするかどうか。デフォルトではイネーブルになっています。 **（注）** ブロッキングをイネーブルにする場合は、レート制限もイネーブルにします。ブロッキングをディセーブルにする場合は、レート制限もディセーブルにします。これは、ARC が新しいブロックまたはレート制限の追加や既存のブロックまたはレート制限の削除を行えないことを意味します。
Max Blocks	ブロックするエントリの最大数。指定できる範囲は 1 ～ 65535 です。デフォルトは 250 です。
Max Interfaces	ブロックを実行するインターフェイスの最大数。たとえば、PIX 500 シリーズ セキュリティ アプライアンスは 1 つのインターフェイスとカウントされます。1 つのインターフェイスを持つルータは 1 つとしてカウントされますが、2 つのインターフェイスを持つルータは 2 つとしてカウントされます。インターフェイスの最大数はデバイスあたり 250 です。デフォルトは 250 です。 [Max Interfaces] を使用して、ARC が管理できるデバイスとインターフェイスの数の上限を設定します。ブロッキング デバイスの合計数（メイン ブロッキング センサーを含まない）をこの値を超える数にすることはできません。ブロッキング項目の合計数もこの値を超えることはできません。ブロッキング項目は 1 つのセキュリティ アプライアンス コンテキスト、1 つのルータ ブロッキング インターフェイス/方向、または VLAN をブロッキングしている 1 つの Catalyst ソフトウェア スイッチです。 **（注）** また、デバイスあたり 100 のインターフェイス、250 台のセキュリティ アプライアンス、250 台のルータ、250 台の Catalyst ソフトウェア スイッチ、および 100 台のメイン ブロッキング センサーは上限として固定されており、変更できません。

要素	説明
Max Rate Limits	レート制限エントリの最大数。最大レート制限は、最大ブロッキングエントリ以下である必要があります。範囲は 1 ～ 32767 です。デフォルト値は 250 です。

[Add User Profile]/[Modify User Profile] ダイアログボックス

[Add User Profile]/[Modify User Profile] ダイアログボックスを使用して、IPS ブロッキング デバイスのユーザ プロファイルを追加または修正します。プロファイルでは、IPS デバイスがログインして、IPS ブロッキングを実装するルータ、スイッチ、またはファイアウォールを設定できる IPS デバイスのユーザ名とパスワードを定義します。

プロファイル名だけを持つプロファイルを保存できますが、ユーザ名、パスワード、およびイネーブル パスワードの要件はデバイスによって決定されます。デバイスに必要な項目を指定してコンフィギュレーション モードを開始する必要があります。そうしないと、IPS はデバイスにブロッキングを設定できません。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[ユーザープロファイル（User Profiles）] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存のセンサーを選択して [行の編集（Edit Row）] ボタンをクリックします。ブロッキング ポリシーを開く方法については、[Blocking] ページ （2285 ページ）を参照してください。

フィールド リファレンス

表 542 : [Add User Profile]/[Modify User Profile] ダイアログボックス

要素	説明
プロファイル名（Profile Name）	最大 64 文字の英数字のプロファイル名。
ユーザー名	ブロッキング デバイスにログインするときに使用するユーザ名。
パスワード	ユーザ名のログイン パスワード（必要な場合）。
パスワードを有効にする（Enable Password）	特権 EXEC モード（イネーブル モード）を開始するためのイネーブル パスワード（必要な場合）。

[プライマリブロッキングセンサー（Primary Blocking Sensors）]ダイアログボックス

[プライマリブロッキングセンサーの追加（Add Primary Blocking Sensor）]/[プライマリブロッキングセンサーの変更（Modify Primary Blocking Sensor）] ダイアログボックスを使用して、メ

インブロッキングセンサーを設定します。メインブロッキングセンサーの詳細については、メインブロッキングセンサーについて （2281 ページ）を参照してください。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[マスターブロッキングセンサー（Master Blocking Sensors）] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存のセンサーを選択して [行の編集（Edit Row）] ボタンをクリックします。ブロッキング ポリシーを開く方法については、[Blocking] ページ （2285 ページ）を参照してください。

フィールド リファレンス

表 *543 : [プライマリブロッキングセンサー（Primary Blocking Sensors）] ダイアログボックス*

要素	説明
IPアドレス	メインブロッキングセンサーの IP アドレス。単一のホストアドレスが含まれたネットワーク/ホストポリシーオブジェクトの IP アドレスまたは名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。
ユーザー名	メインブロッキングセンサーへのログインに使用するユーザー名。ユーザーアカウントは、メインブロッキングセンサーに設定されているアクティブなアカウントである必要があります。
パスワード	ユーザ名のログイン パスワード。
[ポート（Port）]	メインブロッキングセンサー上の接続先ポート。デフォルトは 443 です。
TLS	TLS を使用するかどうか。 [TLS] オプションを選択した場合は、メイン ブロッキング センサー リモート ホストの TLS/SSL X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります（ブロッキング転送センサーは、このブロッキング ポリシーを割り当てている任意のデバイスです）。 ブロッキング転送センサーが X.509 証明書を受け入れるように設定する最も簡単な方法は、IPS Device Manager（IDM）を使用してセンサーにログインし、[設定（Configuration）] > [センサー管理（Sensor Management）] > [証明書（Certificates）] > [信頼できるホスト（Trusted Hosts）] > [信頼できるホストの追加（Add Trusted Host）] を選択して、メインブロッキングセンサーを信頼できるホストとして追加することです。または、センサー CLI にログインし、コンフィギュレーション モードを開始して、**tls trusted-host ip-address** コマンドを使用することもできます。

[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス

[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、または [Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックスを使用して、デバイスを IPS センサーのブロッキングデバイスとして設定します。ダイアログボックスの名前は、追加するデバイスのタイプを示します。

- [Router]：IOS ソフトウェア ルータと Catalyst 6500/7600 デバイス。これらのデバイスは、レート制限とブロッキングを実行できます。ルータおよびスイッチ ブロッキング デバイスについて （2279 ページ）を参照してください。
- [Firewall]：ASA および PIX アプライアンス。
- [Cat6K]：Catalyst OS ソフトウェアを実行している Catalyst 6500/7600 デバイス。

ヒント　Catalyst 6500/7600 が Cisco IOS ソフトウェアを実行している場合は、[Router] タブでデバイスをルータとして追加します。[Cat6K] タブにデバイスを追加しないでください。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[ルータ（Router）]、[ファイアウォール（Firewall）]、または [Catalyst 6K] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存の行を選択して [行の編集（Edit Row）] ボタンをクリックします。ブロッキングポリシーを開く方法については、[Blocking] ページ （2285 ページ）を参照してください。

フィールド リファレンス

表 544 : [Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス

要素	説明
IPアドレス	デバイスの IP アドレス。単一のホストアドレスが含まれたネットワーク/ホストポリシーオブジェクトのIPアドレスまたは名前を入力するか、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。

要素	説明
Communication Type	ブロッキング デバイスへのログインに使用する通信メカニズム（[SSH 3DES]、[SSH DES]、[Telnet]）。デフォルトは [SSH 3DES] です。 [SSH 3DES] または [SSH DES] を選択した場合は、既知のホスト リストにデバイスを追加する必要があります。既知のホストリストにデバイスを追加する最も簡単な方法は、IPS Device Manager（IDM）を使用してセンサーにログインし、[設定（Configuration）]>[センサー管理（Sensor Management）] > [SSH] > [既知のホストキー（Known Host Keys）] > [既知のホストキーの追加（Add Known Host Key）] を選択して、デバイス アドレスを追加することです。または、センサーCLIにログインし、コンフィギュレーション モードを開始して、**ssh host-key** コマンドを使用することもできます。
NAT アドレス（NAT Address）	センサーとブロッキング デバイス間で NAT アドレスが使用されている場合、センサーのNATアドレス。単一のホストアドレスが含まれたネットワーク/ホストポリシーオブジェクトの NAT アドレスまたは名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか新しいオブジェクトを作成します。NAT が使用されない場合はデフォルトの 0.0.0.0 のままにします。
プロファイル名（Profile Name）	ブロッキングデバイスへのログインに使用するログインプロファイル。ブロッキング ポリシーの [User Profiles] タブでこのプロファイルを作成する必要があります。そうしないと、IPS はこのブロッキングデバイスを正常に使用できません。
Interfaces and directions where blocks will be applied（表） （ルータ専用）	ブロッキングまたはレート制限に使用する必要のあるデバイス上のインターフェイス。この表には、インターフェイス名、方向、およびIPSデバイスがブロッキング ACL に組み込む必要のある既存の ACL の名前が表示されます。 インターフェイスに、指定された方向の ACL がすでに設定されている場合は、ACL 名を pre-ACL または post-ACL として指定する必要があります。そうしないと、IPS によって ACL が削除されます。これらの ACL はブロッキングにだけ使用され、レート制限には使用されません。 • インターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、[ルータブロックインターフェイスの追加（Add Router Block Interface）] ダイアログボックスに入力します（[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス（2295 ページ）を参照）。 • インターフェイスを編集するには、インターフェイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。

要素	説明
Response Capabilities （ルータ専用）	このルータが実装できるアクション。複数のアクションを選択するには Ctrl を押しながらクリックします（強調表示されたアクションが選択されています）。次のオプションがあります。 • [ブロック（Block）]：ルータは、Request Block Connection アクションおよび Request Block Host アクションに対してブロックを実装できます。 • [レート制限（Rate Limit）]：ルータは、Request Rate Limit アクションに対してレート制限を実装できます。
VLANs where blocks will be applied（表） （Catalyst オペレーティング システムを実行している Catalyst 6500/7600 デバイスのみ）	ブロッキングに使用する必要のあるデバイス上の VLAN。この表には、VLAN 名と、IPS デバイスがブロッキング VACL に組み込む必要のある既存の VLAN ACL（VACL）の名前が表示されます。 VLAN に VACL がすでに設定されている場合は、VACL 名を pre-VACL または post-VACL として指定する必要があります。そうしないと、IPS によって VACL が削除されます。 • VLAN を追加するには、[行の追加（Add Row] ボタンをクリックし、[Cat6KブロックVLANの追加（Add Cat6K Block VLAN）] ダイアログボックスに入力します（[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス （2296 ページ）を参照）。 • VLAN を編集するには、その VLAN を選択して [行の編集（Edit Row）] ボタンをクリックします。 • VLAN を削除するには、その VLAN を選択して [行の削除（Delete Row）] ボタンをクリックします。

[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス

[Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックスを使用して、ルータ、または IPS ブロッキング デバイスとして設定されている IOS ソフトウェア Catalyst 6500/7600 デバイスに、ブロッキング インターフェイスを設定します。IPS センサーでは、ブロッキング アクションにインターフェイスが使用されます。

ナビゲーション パス

[ルータデバイスの追加（Add Router Device）]/[ルータデバイスの変更（Modify Router Device）] ダイアログボックスで、インターフェイス表の下の [行の追加（Add Row）] ボタンをクリックするか、表の行を選択して [行の編集（Edit Row）] ボタンをクリックします。[Add Router Device]/[Modify Router Device] ダイアログボックスを開く方法については、[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （2293 ページ）を参照してください。

フィールド リファレンス

表 545 : [Add Router Block Interface]/[Modify Router Block Interface] ダイアログボックス

要素	説明
Interface Name	IPS がブロッキングに使用する必要のあるルータ上のインターフェイスの名前。ルータに設定されているとおり、名前を正確に入力します（たとえば、GigabitEthernet0/1 など）。
方向	ブロッキング ACL を適用する方向（[In] または [Out]）。

Pre ACL Name
Post ACL Name
	IPS がブロッキング アクションを実装するために作成するブロッキング エントリに結合する ACL。Pre ACL はブロッキング ACL の前に追加され、Post ACL はブロッキング ACL のあとに追加されます。詳細については、ルータおよびスイッチブロッキングデバイスについて （2279ページ）を参照してください。
	ヒント 指定した方向でインターフェイスに ACL を設定した場合は、[Pre ACL Name]/[Post ACL Name] フィールドに ACL の名前を指定する必要があります。そうしないと、ACL がインターフェイスから削除されます。インターフェイスと方向をブロッキング インターフェイスとして識別した場合、IPS はそのインターフェイス/方向で ACL を制御します。
	ブロッキングデバイスを Security Manager で管理している場合は、ブロッキングデバイスを選択し、[ツール（Tools）]>[設定のプレビュー（Preview Config）] を選択することで ACL 名を識別できます。インターフェイス設定で **ip access-group** コマンドを検索し、方向を確認します。たとえば、次の行は、CSM_FW_ACL_GigabitEthernet0/1 という名前の ACL が、GigabitEthernet0/1 インターフェイスに接続された In 方向に存在することを示しています。
	`interface GigabitEthernet0/1`
	`  ip access-group CSM_FW_ACL_GigabitEthernet0/1 in`
	この例では、ブロッキング インターフェイスとして GigabitEthernet0/1 を In 方向に設定する場合、pre-ACL または post-ACL として、CSM_FW_ACL_GigabitEthernet0/1 を必ず指定してください。ほとんどの場合は、ACL を post-ACL として指定します。これにより、比較的短い IPS ブロッキング ACL によって望ましくないトラフィックが最初に除外され、その後、ブロッキング デバイスによって他のアクセス ルールが実行されます。

[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス

[Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックスを使用して、Catalyst オペレーティング システムを実行し、IPS ブロッキング デバイスとして設定されている Catalyst 6500/7600 デバイスに、ブロッキング VLAN を設定します。IPS センサーでは、ブロッキング アクションに VLAN が使用されます。

ヒント　Catalyst 6500/7600 が Cisco IOS ソフトウェアを実行している場合は、デバイスを Cat6K ではなくルータとして追加します。

ナビゲーション パス

[Cat6Kデバイスの追加（Add Cat6K Device）]/[Cat6Kデバイスの変更（Modify Cat6K Device）] ダイアログボックスで、VLAN テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、テーブルの行を選択して [行の編集（Edit Row）] ボタンをクリックします。[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックスを開く方法については、[Add Router Device]/[Modify Router Device]、[Add Firewall Device]/[Modify Firewall Device]、[Add Cat6K Device]/[Modify Cat6K Device] ダイアログボックス （2293 ページ）を参照してください。

フィールド リファレンス

表 546 : [Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス

要素	説明
VLAN	IPS がブロッキングに使用する必要のある Catalyst 6500/7600 デバイス上の VLAN の数。数値は 1 ～ 4094 で指定でき、デバイスに定義されている必要があります。
Pre VACL Name Post VACL Name	IPS がブロッキング アクションを実装するために作成するブロッキング エントリに結合する VLAN ACL。Pre VACL はブロッキング VACL の前に追加され、Post VACL はブロッキング VACL のあとに追加されます。詳細については、ルータおよびスイッチブロッキング デバイスについて （2279 ページ）を参照してください。 ヒント　VLAN に VACL を設定した場合は、[Pre VACL Name]/[Post VACL Name] フィールドに VACL の名前を指定する必要があります。そうしないと、VACL が VLAN から削除されます。VLAN をブロッキング インターフェイスとして指定した場合は、IPS によってその VLAN 上の VACL が制御されます。通常は、VACL 名を post-VACL として指定します。

[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックス

[Add Never Block Host]/[Modify Never Block Host] または [Add Never Block Network]/[Modify Never Block Network] ダイアログボックスを使用して、ブロッキングの対象にしないホストまたはネットワークを指定します。ダイアログボックスの名前は、ホスト アドレスとネットワーク アドレスのどちらを追加するかを示します。

アドレスを指定するネットワーク/ホストポリシーオブジェクトの IP アドレスまたは名前を入力します。[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成することもできます。オブジェクトを選択した場合、オブジェクトには適切なタイプのエントリを 1 つ含めることができます。ホスト アドレスにはサブネット マスクがありませんが（たとえば 10.100.10.1）、ネットワーク アドレスにはマスクがあります（たとえば 10.100.10.0/24）。

ナビゲーション パス

[IPSブロッキング（IPS Blocking）] ポリシーで、[ブロックしないホスト（Never Block Hosts）] タブまたは [ブロックしないネットワーク（Never Block Networks）] タブを選択し、[行の追加（Add Row）] ボタンをクリックするか、既存の行を選択して [行の編集（Edit Row）] ボタンをクリックします。ホストとネットワークは別々の表にリストされるため、目的の表に関連付けられているボタンをクリックしてください。ブロッキング ポリシーを開く方法については、[Blocking] ページ （2285 ページ）を参照してください。

第 44 章

IPS センサーの管理

日常的なセンサー管理を実行するには、通常 IPS Device Manager（IDM）などのデバイス マネージャを使用する必要があります。Security Manager はポリシーとイベントの管理に焦点を置いています。

ただし、次の項では、Security Manager を使用して実行できる管理作業について説明します。

- IPS ライセンスの管理 （2299 ページ）
- IPS 更新の管理 （2302 ページ）
- IPS 証明書の管理 （2310 ページ）
- IPS センサーのリブート （2313 ページ）

IPS ライセンスの管理

次の項では、IPS デバイスのライセンスを管理する方法について説明します。

IPS ライセンス ファイルの更新 （2299 ページ）

IPS 更新の管理 （2302 ページ）

IPS 証明書の管理 （2310 ページ）

IPS ライセンス ファイルの更新

Security Manager を使用して、IPS デバイスのライセンスを更新できます。ここでは、Cisco.com、または Security Manager サーバのライセンス ファイルからライセンスを手動で取得することにより、ライセンスを手動で更新する方法について説明します。自動ライセンス更新のセットアップの詳細については、IPS ライセンス ファイル更新の自動化 （2301 ページ）を参照してください。

はじめる前に

Cisco.com を使用する場合、ユーザ名とパスワードを指定できるように、最初に IPS 更新サーバを Cisco.com として設定する必要があります。デバイスによっては、ライセンス取得に Cisco.com を使用する必要があります。たとえば、IPS 4270 や ASA デバイス内の AIP SSM-40

デバイスでは、Cisco.com アカウントが必要です。Cisco.com を IPS 更新サーバとして設定する方法の詳細については、IPS 更新サーバの設定 （2303 ページ）を参照してください。

ローカル ライセンスを使用する場合、Security Manager サーバ ファイル システムに直接ダウンロードする必要があります。この作業は Security Manager では実行できません。サーバ上で Windows にログインして、ライセンスをダウンロードする必要があります。

関連項目

- IPS ライセンス ファイルの再展開 （2301 ページ）

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ライセンス（Licensing）] を選択します。

ステップ 2 [IPS] タブをクリックします（[IPS] タブ、[Licensing] ページ （720 ページ）を参照）。

表に、デバイス インベントリ内のすべての IPS デバイスおよびそのライセンス ステータスが表示されます。ステータスは、[valid]、[invalid]、[expired]、[no license]、または [trial license] です。ライセンスの有効期限も表示されます。[ライセンスの更新（Refresh License）] をクリックすると、デバイスの最新ライセンス情報で表が更新されます（1 つ以上のデバイスを選択して、更新の範囲を制限できます）。

ライセンスを更新するには、次のいずれかを実行します。

- Cisco.com から直接取得したライセンスでデバイスを更新する場合は、更新するデバイスを選択し、[CCO経由で選択内容を更新（Update Selected via CCO）] をクリックします。ダイアログボックスが開き、Cisco.com から更新可能なデバイスが表示されます。選択したすべてのデバイスが表示されるとは限りません。リストを確認し、[OK] をクリックします。[License Update Status Details] ダイアログボックスに更新作業のステータスが表示されます（[License Update Status Details] ダイアログボックス （725 ページ）を参照）。

この方法でライセンスを更新するには、選択したデバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。

ヒント ライセンスが格納されたシスコのソフトウェア ライセンス サーバ（SWIFT）は、同じサーバから 3 分間に 10 ライセンス以上の要求があると、その要求をブロックする場合があります。そのため、手動でライセンス更新を実行するときは、一度に選択するデバイスを 8 つ以下にしてください。

- Cisco Security Manager サーバーにコピーしたライセンスでデバイスを更新するには、[ライセンスファイルから更新（Update from License File）] をクリックします。ライセンス ファイルを選択するためのダイアログボックスが開きます。[参照（Browse）] をクリックして、Cisco Security Manager ローカル ファイルシステムからライセンスファイルを選択します。複数のライセンス ファイルを選択できます。目的のファイルを選択したら、[OK] をクリックして、選択したファイルをデバイスに適用します。

IPS ライセンス ファイルの再展開

IPS ライセンス更新をデバイスに適用しようとして失敗した場合は、更新を再展開できます。再展開を実行できるのは、すでに更新を試行し、ライセンスファイルがIPSデバイスに関連付けられている場合だけです。

関連項目

- IPS ライセンス ファイルの更新 （2299 ページ）
- IPS ライセンス ファイル更新の自動化 （2301 ページ）

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルから [ライセンス（Licensing）] を選択します。

ステップ 2 [IPS] タブをクリックします（ [IPS] タブ、[Licensing] ページ （720 ページ）を参照）。

ステップ 3 ライセンスを再展開するデバイスを選択し、[選択したライセンスの再展開（Redeploy Selected Licenses）] をクリックします。ライセンスを再展開するデバイスが表示されたダイアログボックスが開きます。[OK] をクリックして、更新を実行します。

[License Update Status Details] ダイアログボックスに更新作業のステータスが表示されます（[License Update Status Details] ダイアログボックス （725 ページ）を参照）。

IPS ライセンス ファイル更新の自動化

Security Manager は、IPS ライセンス更新を定期的に IPS デバイスに自動適用できます。自動更新を設定するには、IPS デバイスのシリアル番号が含まれる Cisco.com サポート契約を締結する必要があります。

ヒント Security Manager は、置き換えられるライセンスよりも未来の有効期限がダウンロードされたライセンスに設定されている場合、またはライセンス情報が異なる場合に、新しいライセンスを適用します。

はじめる前に

Cisco.com ユーザ名とパスワードを指定できるように、最初に IPS 更新サーバを Cisco.com として設定する必要があります。Cisco.com を IPS 更新サーバとして設定する方法の詳細については、 IPS 更新サーバの設定 （2303 ページ）を参照してください。

関連項目

- IPS ライセンス ファイルの更新 （2299 ページ）
- IPS ライセンス ファイルの再展開 （2301 ページ）

ステップ 1 [ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] を選択し、目次から [ライセンス（Licensing）] を選択します。

ステップ 2 [IPS] タブをクリックします（[IPS] タブ、[Licensing] ページ （720 ページ）を参照）。

ステップ 3 [ラインセンスのダウンロードと適用（Download and apply licenses）] を選択して、次の設定値を設定します。

- [有効期限までの日数（Days before the expiration date）]：Cisco Security Manager が更新されたライセンスをダウンロードする必要がある、ライセンスの有効期限までの日数を選択します。デフォルトは 1 日です。
- [毎日のデバイスの検出時刻（Discover devices daily at）]：Cisco Security Manager がライセンスをダウンロードする時刻を選択します。選択した時刻になると、Security Manager はデバイスのライセンス ステータスを確認し、ライセンスが存在しないデバイス、ライセンスの有効期限が切れているデバイス、または設定した日数の間にライセンスの有効期限が切れるデバイスに対して、新しいライセンスを Cisco.com に問い合わせます。
- [ライセンスの更新結果を電子メールで送信する（Email License Update Results）]：Cisco Security Manager がライセンス更新結果の電子メール通知を送付するかどうかを選択します。ライセンス有効期限ステータスが記載された電子メールと、ライセンス更新ジョブ結果に関する電子メールが送信されます。このオプションを選択した場合は、[電子メール通知（Email Notification）] フィールドに 1 つ以上の電子メールアドレスを入力します。カンマで複数のアドレスを区切ります。

電子メールを送信するには、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）の説明に従って SMTP サーバを設定する必要があります。

ステップ 4 [保存（Save）] をクリックして変更を保存します。

IPS 更新の管理

Security Manager を使用すると、センサーおよびシグニチャの更新を IPS デバイスおよび共有ポリシーに適用できます。Security Manager を使用して、更新をダウンロードした後、自動更新をセットアップするか、または手動で更新を適用できます。

シグニチャの更新は、IPS 5.1(4) 以降でのみ使用可能です。

ヒント パッチ、サービス パック、またはシグニチャの更新の適用中に問題が発生する場合は、IPS センサーの時刻を確認します。センサーの時刻が、関連付けられている証明書の時刻よりも進んでいる場合、証明書は拒否されます。この場合、更新が失敗する可能性があります。IPS センサーの時刻を正確に保つには、ネットワーク タイム プロトコル（NTP）を使用します。センサーで NTP を設定する方法の詳細については、NTP サーバの識別（2112 ページ）を参照してください。

Security Manager に含まれる IPS パッケージには、IPS デバイスの更新に必要なパッケージ ファイルは含まれていません。更新を適用する前に、Cisco.com またはローカル更新サーバから IPS パッケージをダウンロードする必要があります。ダウンロードされたバージョンにはすべての必要なパッケージ ファイルが含まれ、Security Manager の初期インストールに含まれていた部分的なファイルと置き換えられます。

ここでは、Security Manager を使用して IPS 更新を管理する方法について説明します。

- IPS 更新サーバの設定 （2303 ページ）
- IPS 更新の確認とダウンロード （2304 ページ）
- IPS 更新の自動化 （2305 ページ）
- IPS 更新の手動適用 （2307 ページ）

IPS 更新サーバの設定

IPS センサーおよびシグニチャの更新を適用するには、Security Manager で、指定された IPS 更新サーバから Security Manager サーバに更新をダウンロードする必要があります。

Cisco.com を IPS 更新サーバとして使用できます。Cisco.com を使用すると、最新の更新をすぐに入手できます。ただし、何らかの理由で Cisco.com を使用できない場合、独自のローカル IPS 更新 Web サーバをセットアップして、そのサーバに手動で更新をダウンロードし、ローカル サーバからの更新を取得するように Security Manager を設定できます。

ヒント ライセンスの更新に Cisco.com ログインを必要とするデバイス（IPS 4270 や ASA デバイス内の AIP SSM-40 など）を使用している場合は、IPS 更新サーバを Cisco.com として設定する必要があります。ローカル サーバを使用することはできません。

関連項目

- IPS 更新の自動化 （2305 ページ）
- IPS 更新の手動適用 （2307 ページ）

ステップ 1 [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPS更新（IPS Updates）] を選択して、[IPS更新（IPS Updates）] ページを開きます（[IPS Updates] ページ （705 ページ）を参照）。

ステップ 2 [サーバーの更新（Update Server）] 領域で、[設定の編集（Edit Settings）] をクリックして [更新サーバー設定の更新の編集（Edit Update Server Settings）] ダイアログボックスを開きます（[Edit Update Server Settings] ダイアログボックス （712 ページ）を参照）。

ステップ 3 サーバの識別情報を入力します。[Update From] フィールドで選択したサーバ タイプに基づいて、次の操作を実行します。

- [Cisco.com]：Cisco.comユーザ名およびパスワードを入力します。指定するユーザアカウントで強化暗号化ソフトウェアをダウンロードできる必要があります。アカウントに適切な権限があることを確認するには、Cisco.com にアクセスして、IPS 更新パッケージのダウンロードを試行してください。アカウントがまだ認定されていない場合は、適切な契約に合意するように求められます。
- [Local server]：サーバの IP アドレスまたは DNS ホスト名、ユーザ名とパスワード（アクセス許可の前にログインの必要がある場合）、およびファイルが含まれるフォルダへのパスを入力します。パスには、URL 全部ではなく URL のパス部分だけを入力します（たとえば、http://servername/IPSpath の中のパスは IPSpath です）。また、次のように IIS 設定を追加します。
  - ホーム ディレクトリのリストがイネーブルになっている必要があります。
  - ドキュメントの [Default Content Page] がディセーブルになっている必要があります。

証明書情報を入力します。IPS パッケージをダウンロードする前に、Cisco.com 証明書を承認する必要があります。イメージのダウンロードを正常に開始するには、「イメージメタデータロケータ」サイトと IPS パッケージのダウンロードサイトの両方からの証明書を受け入れる必要があります（[Edit Update Server Settings] ダイアログボックス （712 ページ）を参照）。

Security Manager サーバーから IPS 更新サーバーに接続するために、ネットワークでプロキシサーバーが必要な場合、[プロキシサーバーの有効化（Enable Proxy Server）] を選択し、プロキシサーバーの情報を入力します。

[OK] をクリックして変更を保存します。

ステップ 4 [IPS更新（IPS Updates）] ページで [保存（Save）] をクリックします。[保存（Save）] をクリックするまで、変更は完全には保存されません。

ステップ 5 [最新の更新をダウンロード（Download Latest Updates）] をクリックして、IPS 更新サーバーへの接続をテストします。ダイアログボックスが表示されます。[開始（Start）] をクリックすると、Security Manager が更新サーバーにログインし、新しい更新を確認してダウンロードします。ダイアログボックスに操作の結果が表示されます。

Cisco.com を使用しているときにダウンロードが失敗する場合は、ユーザ アカウントを再度確認して、強化暗号化ソフトウェアをダウンロードできるかどうかを確認してください。

IPS 更新の確認とダウンロード

Security Manager を使用して、IPS センサーとシグニチャの更新を確認し、Security Manager サーバにダウンロードできます。これらの更新は、Security Manager サーバで IPS デバイスおよびポリシーに適用できます。

手動で IPS 更新をダウンロードすることも、IPS 更新のダウンロードを自動化することもできます。または、手動で IPS 更新をデバイスに適用するときに更新をダウンロードすることもできます。ここでは、手動で更新を確認してダウンロードする方法について説明します。自動ダウンロードの設定方法の詳細については、IPS 更新の自動化 （2305 ページ）を参照してくださ

い。更新をデバイスまたはポリシーに手動で適用するときに更新をダウンロードする方法の詳細については、IPS 更新の手動適用 （2307 ページ）を参照してください。

はじめる前に

IPS 更新サーバの設定 （2303 ページ）の説明に従って IPS 更新サーバを設定する必要があります。

関連項目

- IPS 更新の自動化 （2305 ページ）
- IPS 更新の手動適用 （2307 ページ）

ステップ 1 [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPS更新（IPS Updates）] を選択して、[IPS更新（IPS Updates）] ページを開きます（[IPS Updates] ページ （705 ページ）を参照）。

ステップ 2 [Update Status] グループ内のステータス情報を確認し、次のいずれかを実行します。

- [更新の確認（Check for Updates）] をクリックします。操作の結果を示すダイアログボックスが開きます。[開始（Start）] をクリックすると、Security Manager が IPS 更新サーバーにログインし、更新を確認します。
- [最新の更新をダウンロード（Download Latest Updates）] をクリックします。操作の結果を示すダイアログボックスが開きます。[開始（Start）] をクリックすると、Security Manager が IPS 更新サーバーにログインし、更新を確認して Security Manager サーバーにダウンロードします。

ヒント Cisco.com からのダウンロードに失敗する場合は、使用しているアカウントで強化暗号化ソフトウェアをダウンロードできることを確認してください。詳細については、[Edit Update Server Settings] ダイアログボックス （712 ページ）の [User Name] の説明を参照してください。

IPS 更新の自動化

センサーイメージとシグニチャを常に最新に保つために、それらの更新を互換性のある IPS デバイスに自動的に適用できます。必要に応じて、更新を部分的に自動化して、プロセスに対する制御を必要なレベルに保つことができます。

ヒント 後でシグニチャの更新を適用する必要はなかったと判断した場合は、デバイスで [シグネチャ（Signatures）] ポリシーを選択し、[更新レベルの表示（View Update Level）] ボタンをクリックしてから [元に戻す（Revert）] をクリックすることで、直前の更新レベルに戻すことができます。

ヒント　IPS デバイスを管理しない場合は、次のパフォーマンス調整手順の実行を検討してください。*$NMSROOT*\MDC\ips\etc\sensorupdate.properties の packageMonitorInterval の値を、初期デフォルト値の 30,000 ミリ秒から、より頻度の低い値である 600,000 ミリ秒に変更します。この手順を実行することにより、いくらかパフォーマンスが向上します。*$NMSROOT* は、Common Services インストールディレクトリ（デフォルトは C:\Program Files\CSCOpx）のフルパス名です。

はじめる前に

IPS 更新サーバの設定 （2303 ページ）の説明に従って IPS 更新サーバを設定する必要があります。

関連項目

- IPS 更新の確認とダウンロード （2304 ページ）
- IPS 更新の手動適用 （2307 ページ）
- IPS ネットワーク検知について （2084 ページ）
- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）

ステップ 1　[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [IPS更新（IPS Updates）] を選択して、[IPS更新（IPS Updates）] ページを開きます（[IPS Updates] ページ （705 ページ）を参照）。

ステップ 2　ページ下部の [Auto Update Settings] グループで自動更新モードを選択して、自動化のレベルを設定します。次のオプションがあります。

- [Download, Apply, and Deploy Updates]：Security Manager はスケジュールに従って更新を確認し、更新を Security Manager サーバにダウンロードしてから、選択されたデバイスおよびポリシーに適用します。続いて、展開ジョブを開始して、影響を受けるデバイスを更新します。これを選択すると、運用スタッフの労力を最小限に抑えて、デバイスの最新の更新が確実に実行されます。
- [Disable Auto Update]：Security Manager は、IPS 更新の自動処理を実行しません。
- [Check for Updates]：Security Manager はスケジュールに従って更新を確認し、[Update Status] グループ内の情報を更新します。デバイスもポリシーも更新されません。
- [Download Updates]：Security Manager はスケジュールに従って更新を確認し、新しい更新を Security Manager サーバにダウンロードします。
- [Download and Apply Updates]：Security Manager はスケジュールに従って更新を確認し、更新をダウンロードして、選択されたデバイスおよびポリシーに適用します。影響を受けるデバイスに変更を展開する展開ジョブは、個別に作成する必要があります。

ステップ 3 [更新スケジュールの編集（Edit Update Schedule）] をクリックして、操作のスケジュールを指定できるダイアログボックスを開きます。開始日を選択し、開始時刻を 24 時間形式（hh:mm）で入力し、スケジュールをどの単位で指定するか（時間、日、週、月、または 1 回限りのイベント）を選択します。[OK] をクリックして、スケジュールを保存します。

ステップ 4 （任意）[Notify Email] フィールドに電子メール アドレスを入力します。Security Manager は、パッケージがダウンロード可能になったとき、あるいはパッケージのダウンロード、適用、または展開が完了したときに、このユーザに通知します。複数のアドレスをカンマで区切って入力できます。

ステップ 5 [Apply Update To] セレクタで、自動で更新するデバイスおよび共有ポリシーを選択します。ローカル ポリシー（デバイスの場合）と共有ポリシーを切り替えるには、[Type] フィールドを使用します。

デバイスまたはポリシーを選択するには、セレクタ内のデバイスまたはポリシーをクリックし、[行の編集（Edit Row）] ボタン（セレクタの下の鉛筆アイコン）をクリックします。この処理により、[Edit Auto Update Settings] ダイアログボックスが開きます。適用する更新のタイプ（[minor sensor updates and service packs] または [service packs only]）およびシグニチャ更新のレベルを選択します。[OK] をクリックして変更を保存します。ポリシーの適用先のデバイスが、[Devices to be Auto Updated] リストに追加されます。メッセージに、変更を有効にするために変更を送信する必要があるかどうかが示されます。

ステップ 6 [保存（Save）] をクリックします。

IPS 更新の手動適用

Apply IPS Update ウィザードを使用すると、イメージおよびシグニチャの更新を互換性のある IPS デバイスに手動で適用できます。この手順は、自動更新が設定されていないポリシーおよびデバイスに対して使用してください（IPS 更新の自動化 （2305 ページ）を参照）。

シグニチャ更新を適用するときに、このウィザードには、更新内のシグニチャのうち対象の IPS デバイス上に設定されていないものが表示されます。新しいシグニチャは、適用前に設定できます。

イメージおよびシグニチャの更新を適用する際は、更新を適用できるデバイスだけが選択可能になります。適用できないデバイスはグレー表示されます。グレー表示されているデバイスにマウスポインタを合わせると、デバイスがグレー表示されている理由がツールチップに表示されます。必要なエンジンアップグレードまたは汎用パッケージを利用できない場合、シグネチャの更新がデバイスに適用されていても、デバイスがグレー表示されることがあります。以下に、デバイスがグレー表示される例と、対応するツールチップラベルを示します。

- 選択したシグネチャまたはセンサーパッケージのバージョンがターゲット IPS デバイスのバージョンよりも低い場合、Cisco Security Manager によりデバイスがグレー表示され、マウスオーバーのツールチップに「選択されたパッケージは適用できません（Selected package is inapplicable）」というメッセージが表示されます。
- Cisco Security Manager を使用して、SNMP ポリシーが設定されているバージョン 7.2.2 からバージョン 7.3.1 に IPS デバイスをアップグレードしようとすると、マウスオーバーのツールチップに「選択されたアップグレードは推奨されません（Selected upgrade is not recommended）。デバイスの SNMP ポリシーの割り当てを解除して展開し、7.3.1 へのアップグレードを続行してください（Unassign the SNMP policy on the device and deploy it to

continue with the upgrade to 7.3.1）」と表示されます。これは、SNMPv3 が IPS バージョン 7.3.1 でサポートされていないためです。

- Cisco Security Manager を使用して、デバイスに適用されている 1 つ以上の脅威プロファイルが含まれていないシグネチャの更新を実行しようとすると、Cisco Security Manager によりデバイスがグレー表示され、マウスオーバーのツールチップに「現在適用されている脅威プロファイルは、このシグネチャバージョンには適用されません（Currently applied threat profile is not applicable to this signature version）」というメッセージが表示されます。この場合、シグネチャの更新は正常に適用できません。既存の脅威プロファイルを削除してから、シグネチャの更新を続行する必要があります。

ヒント　後にシグネチャの更新を適用する必要はなかったと判断した場合は、デバイスで [シグネチャ（Signatures）] ポリシーを選択し、[更新レベルの表示（View Update Level）] ボタンをクリックしてから [元に戻す（Revert）] をクリックすることで、直前の更新レベルに戻すことができます。

はじめる前に

IPS 更新サーバの設定　（2303 ページ）の説明に従って IPS 更新サーバを設定します。

関連項目

- IPS 更新の確認とダウンロード　（2304 ページ）
- Cisco IOS IPS のシグニチャ カテゴリの選択　（2321 ページ）

（注）　ここでは、IPS 7.1.3 の更新パッケージと以前のバージョンで使用されたパッケージの違いについて説明します。Apply IPS Update ウィザード（[ツール（Tools）] > [IPS更新の適用（Apply IPS Update）]）を開くと、ウィザードの最初のページに、使用可能なセンサーおよびシグネチャの更新パッケージが一覧表示されます。IPS 7.1.3 以降は、IPS-4270 や ASA-SSE-AIP-85 など、サポートされているすべてのプラットフォームに単一の更新パッケージ（IPS-CSM-K9-7.1.3.zip など）が使用されます。IPS 7.1.3 より前は、サポートされているプラットフォームごとに個別のパッケージ（IPS-CS-MGR-SSC_5-K9-6.2-4-E4.zip など）が使用されていました。

ステップ 1　[ツール（Tools）] > [IPS更新の適用（Apply IPS Update）] を選択して、Apply IPS Update ウィザードを開きます。

ステップ 2　ウィザードの最初のページで、適用する更新を選択します。このページに、使用可能なセンサーおよびシグニチャの更新が表示されます。このページで、次の操作を実行します。

- パッケージのリストを更新するには、[最新の更新をダウンロード（Download Latest Updates）] をクリックします。Security Manager は IPS 更新サーバにログインし、最後のダウンロード以降に使用可能になった更新をダウンロードします。これは、IPS 更新サーバの設定　（2303 ページ）の説明に従って

更新サーバを設定した場合のみ実行されます。また、次の操作を実行して、パッケージのリストを更新することもできます。

- [IPS更新（IPS Updates）] ページ（**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [IPS更新（IPS Updates）]** を選択）で自動ダウンロードを設定します。詳細については、[IPS Updates] ページ （705 ページ）を参照してください。
- Security Manager サーバ上の製品インストール フォルダ（通常は Program Files）内の CSCOpx\MDC\ips\updates フォルダに更新を手動でダウンロードします。

また、[更新の確認（Check for Updates）] をクリックすることで、ダウンロードせずに更新を確認できます。[Update Status] 情報は、[IPS Updates] ページ （705 ページ）の説明と同じです。

- [Updates Downloaded] テーブルで、IPS デバイスに適用するシグニチャまたはセンサーの更新を選択します。更新のタイプを切り替えるには、[タイプ（Type）] フィールドを使用します（適用する更新は 1 つだけ選択できます）。
  - [センター更新（Sensor Updates）]：ファイル名、メジャー、マイナー、サービスパック、パッチ バージョン、およびサポートされているエンジンリリースが表示されます。メジャー センサー更新はすべて適用する必要があります。ただし、マイナー更新は累積的です。
  - [シグネチャの更新（Signature Updates）]：ファイル名、シグネチャ番号、およびサポートされているエンジンリリースが表示されます。シグニチャ更新は累積的ですが、ネットワークの特定の要件に合わせて更新を調整しようとする場合、これらの更新を個別のパッケージとして適用すると、より管理しやすい単位に作業を分割できます。

（注） エンジン パッケージは更新ページに表示されません。ただし、上位のエンジン バージョンが必要となるシグニチャ更新の場合、Security Manager は暗黙的にエンジン パッケージをプッシュします（この処理は、エンジン パッケージで必要となる特定のバージョンでデバイスを更新する場合のみ実行されます）。

[次へ（Next）] をクリックして続行します。

ステップ 3 ウィザードの 2 ページめで、[Apply Updates To] リストから、更新対象となる（共有シグニチャ ポリシーに割り当てられていないデバイスを表す）ローカル シグニチャ ポリシーおよび共有シグニチャ ポリシーを選択します。ポリシーのタイプを切り替えるには、[タイプ（Type）] フィールドを使用します。ローカル ポリシーと共有ポリシーを自由に組み合わせて選択できます。ポリシーを選択すると、そのポリシーを使用するデバイスが更新対象として選択されます。

適用可能なすべてのデバイスまたは共有ポリシーを選択するには、[すべて選択（Select All）] をクリックします。選択内容を消去して最初からやり直すには、[すべて選択解除（Deselect All）] をクリックします。これらのボタンは、表示されているリストにだけ適用されます。

更新が適用されない IPS デバイスは、[Apply Updates To] リストでグレー表示されるため、選択できません。更新可能なデバイスを選択すると、[Devices Assigned to Selected Policies] リストにそのデバイスが示されます。更新されるのは、これらのデバイスだけです。共有ポリシーを選択すると、そのポリシーを使用しているすべてのデバイスが、[selected policies] リストに表示されますが、更新が適用されないデバイスはグレー表示されます。

ヒント　センサー更新の対象として選択できるデバイスは、エンジン リリースによって決まります。つまり、更新は、リリース バージョンに関係なく、同じエンジン バージョンを使用するデバイスだけに適用できます。たとえば、デバイスが 6.0(5) E3 を実行している場合、6.1(1) E3 には更新できますが、6.1(1) E2 には更新できません。また、6.1(1) E2 を実行しているデバイスに 6.1(1) E3 更新を適用することもできません。エンジン バージョンを更新する場合は、上位のエンジン バージョンを持つシグニチャ更新を選択します。これにより、Security Manager は、シグニチャの更新中に自動的にエンジン レベルを更新します。たとえば、デバイスのバージョンが 6.1(1) E2 の場合、E3 エンジン パッケージを適用する必要があれば、E3 エンジンを必要とするシグニチャ パッケージを選択してデバイスに適用します。これにより、シグニチャの更新中に自動的にエンジン パッケージがデバイスに適用されます。このため、更新する必要のあるデバイスがグレー表示されている場合は、[戻る（Back）] をクリックし、更新の選択内容を変更します。

シグネチャの更新を適用する際に、適用前にシグネチャを編集する場合は、[次へ（Next）] をクリックして続行します。それ以外の場合は、[終了（Finish）] をクリックして更新をポリシーに適用します。

ステップ 4　（任意）ウィザードの 3 ページ目で、必要に応じてシグニチャを変更します。

シグニチャ リストに、選択した更新のシグニチャ レベルから、選択したデバイス間で最も下位のシグニチャ レベルまでの間で、新規のシグニチャおよび変更されたシグニチャが表示されます。選択したデバイスに IPS センサーと Cisco IOS IPS デバイスの両方が含まれている場合、これらのデバイスのシグニチャは別々のタブに表示されます。

ID 番号内のリンクをクリックして、Cisco.com のシグニチャの説明を読みます。[Status] カラムは、シグニチャが新規のものか変更されたものかを示します（ウィザード ページのアイコンの説明図を参照）。

シグニチャを編集するには、表内のシグニチャを選択し、表の下にある [Edit] ボタン（鉛筆アイコン）をクリックします。シグネチャの説明については、[編集（Edit）] ボタンを押すと開くダイアログボックス内の [ヘルプ（Help）] をクリックして確認してください。

使用可能なシグニチャ情報の詳細については、[Signatures] ページ （2169 ページ）を参照してください。[Signature Summary Table] ではカスタム シグニチャの追加やシグニチャの削除ができますが、Apply IPS Update ウィザードのこのページではこれらの操作を実行できません。

[終了（Finish）] をクリックして、更新をポリシーに適用し、編集を保存します。

ステップ 5　変更を送信し、デバイスに展開します。展開ジョブの作成方法の詳細については、次の各項を参照してください。

- Workflow 以外のモードでの設定の展開 （515 ページ）
- Workflow モードでの設定の展開 （523 ページ）

IPS 証明書の管理

IPS デバイスとの通信に SSL（HTTPS）を使用するように Cisco Security Manager を設定する場合、デバイスに設定されている証明書が Cisco Security Manager の証明書ストアに保存されてい

る証明書と一致している必要があります。証明書が一致していないと、ポリシー検出または展開時に通信が失敗します。

IPS デバイスは、約 2 年間の固定の有効期間が設定された自己署名証明書を使用します。証明書の有効期限が切れた場合は、証明書を再生成し、新しい証明書で証明書ストアを更新する必要があります。

Security Manager には、デバイスに定義されている証明書との証明書ストアの同期、有効期限が切れた証明書の再生成、および管理する IPS デバイス上に存在する証明書のステータス（有効期限を含む）の表示ができるユーティリティが含まれています。

ヒント　IPS デバイスとの通信に HTTP を使用している場合、証明書は使用されず、証明書を管理することもできません。IPS デバイスの通信の設定値は、[Security Manager Administration Device Communication] ページで設定します（[Device Communication] ページ （668 ページ）を参照）。

ここでは、Security Manager を使用して IPS 証明書を管理する方法について説明します。

関連項目

- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）
- HTTPS 通信を使用するデバイスでの SSL 証明書の手動追加 （578 ページ）
- デバイス検出時にセキュリティ証明書が拒否される （579 ページ）
- デバイス検出中の無効な証明書のエラー （580 ページ）

ステップ 1　[管理（Manage）] > [IPS] > [IPS証明書（IPS Certificates）] を選択して、[IPS証明書（IPS Certificates）] ダイアログボックスを開きます。

ヒント　このダイアログボックスに表示されるリストは、自動的には更新されません。ダイアログボックスを開くたびに [更新（Refresh）] をクリックして、最新の証明書の有効期限情報を参照してください。

ダイアログボックスには、インベントリにあるすべての IPS センサーが Security Manager の表示名のとおりに表示されます。すべてのカラムが表示されるわけではありません（他のカラムを選択するには、任意のセルの見出しを右クリックします）。主要なカラムは次のとおりです。

- [証明書の不一致（Certificate Mismatch?）]：デバイスに定義されている証明書が Cisco Security Manager の証明書と同一かどうかを示します。証明書が使用できない、または取得できない場合は、このフィールドはブランクになります。証明書が取得できた場合は、次のいずれかの値になります。
  - [いいえ（No）]：デバイスと Cisco Security Manager は同一の証明書を保持しています。特に対処の必要はありません。

- [はい（Yes）]：デバイスと Cisco Security Manager は異なる証明書を保持しています。証明書の有効期限が切れていない場合、デバイスを選択し、[証明書の同期（Sync Certificates）] をクリックして、Cisco Security Manager の証明書ストアの証明書をデバイスの証明書と置き換えます。

- [デバイスの有効期限最終日（Valid Until on Device）]、[デバイスの有効期限開始日（Valid From on Device）]：この 2 つの列には、証明書が有効である日付の範囲が表示されます。[Valid Until] の日付を迎えると、証明書の有効期限は切れます。この日付が近づいてきたら、証明書の再生成を検討してください。

- [デバイスの証明書ステータス（Certificate Status on Device）]：デバイスに存在する証明書の現在のステータスを示します。
  - [有効な証明書（Valid Certificate）]：証明書は正常で、有効期間内です。
  - [期限切れの証明書（Expired Certificate）]：[有効期限最終日（Valid Until）] の日付が過ぎ、証明書は有効期限が切れています。デバイスを選択し、[証明書の再生成（Regenerate Certificate）] をクリックすると、デバイス上に新しい有効な証明書が作成され、Cisco Security Manager の証明書ストアに証明書がロードされます。
  - [有効期限前の証明書（Certificate Not Yet Valid）]：証明書は [有効期限開始日（Valid From）] の日付に達していないため、まだ使用できません。デバイス上の時刻設定と Security Manager サーバの時刻設定との間に不一致がある可能性があります。時刻設定が同一であることを確認してください（NTP サーバの使用を検討してください）。証明書の再生成を検討してください。
  - [使用不可：更新して証明書情報を取得する（Unavailable – Refresh to get Cert Info）]：証明書は現在 Cisco Security Manager の証明書ストアに存在しません。[更新（Refresh）] をクリックして、Cisco Security Manager がデバイスから証明書を取得し、証明書ストアにロードするようにします。
  - [取得不可能：証明書情報を利用できない（Nonretrievable – Cert Info not available）]：Cisco Security Manager はデバイスにログインして証明書を取得できませんでした。または、通信に HTTP を使用しています。デバイスを選択して、[更新（Refresh）] をクリックします。

更新により問題が解決されない場合、デバイスが正常に動作していること（つまり、ダウンしていないこと）を確認してください。次に、デバイスのプロパティを確認して、正しいクレデンシャルがアクセスのために設定されていることを確認してください（デバイス プロパティの表示または変更 （136 ページ）を参照）。クレデンシャルに問題がない場合、デバイスに設定されている Allowed Hosts ポリシーも確認して、Security Manager サーバが許可ホストとして含まれていることを確認してください（許可ホストの識別（2091 ページ）を参照）。また、Security Manager サーバ上の Windows にログインし、ping を使用してサーバと IPS デバイスとの間にルートが存在するかどうかを確認することもできます。

- [CSMのサムプリント（Thumbprint on CSM）]、[デバイスのサムプリント（Thumbprint on Device）]：これらの列には、証明書ストア内とデバイス上にある証明書のサムプリントが表示されます。

ステップ 2 次のいずれかのボタンを使用して、指示されたアクションを実行します。指示されている箇所を除いて、デバイスを 1 つも選択せずにボタンをクリックした場合、表示されているすべてのデバイスにアクションが実行されます。この操作は、多くの IPS デバイスが存在する場合に、時間がかかる可能性があります。操作がすべてのデバイスに実行される前に警告が表示され、操作を中止するオプションが表示されます。

- [証明書の同期（Sync Certificate）]：Cisco Security Manager の証明書ストア内の証明書情報と、デバイスの証明書を同期します。デバイスの証明書によって、証明書ストア内の証明書が置き換えられます。
- [証明書の再生成（Regenerate Certificate）]：デバイス上に新しい証明書を生成し、新しい証明書を証明書ストア内にロードします。
- [更新（Refresh）]：Cisco Security Manager がデバイスに問い合わせて、有効期限などの証明書情報を取得し、証明書ストア内の証明書とデバイスの証明書を比較することで、ステータス情報を更新します。このアクションによって [Certificate Status on Device] カラムが更新され、証明書の不一致があるかどうかも判断します。
- [エクスポート（Export）]：証明書テーブル全体をカンマ区切り値（CSV）ファイルにエクスポートします。テーブル全体より小さな単位でのエクスポートはできません。Security Manager サーバ上のファイル名とフォルダの入力を求められます。

IPS センサーのリブート

Security Manager から IPS センサーをリブートできます。

センサーをリブートするには、[デバイス（Device）] ビューでセンサーを選択して、[デバイスのリブート（Reboot Device）] を右クリックして選択します。リブートを確認するように求められます。

Security Manager はリブート プロセスのステータス情報を表示しません。

第 45 章

IOS IPS ルータの設定

サービス統合型ルータ（ISR）などの一部の Cisco IOS ルータは、IPS 5.1 ソフトウェアに基づいたネイティブな IPS 機能を備えています。これらのデバイス上で基本的な IPS インスペクションを設定することにより、IPSセンサーによるインスペクションを補強したり、小規模ネットワークをサポートしたりできます。

この章は次のトピックで構成されています。

- Cisco IOS IPS について （2315 ページ）
- Cisco IOS IPS 設定の概要 （2318 ページ）

Cisco IOS IPS について

Cisco Security Manager を Cisco IOS Intrusion Prevention System（IOS IPS; IOS 侵入防御システム）とともに使用して、サポートされている Cisco IOS ソフトウェアリリース 12.4(11)T2 以降を使用する Cisco ルータで侵入防御を管理できます。

Cisco IOS IPS は、インライン侵入防御センサーとして機能し、パケットとセッションがルータを通過するときに監視し、各パケットをスキャンして Cisco IOS IPS シグニチャと照合します。疑わしいアクティビティを検出すると、ネットワークセキュリティが侵害される前に対応し、Cisco IOS syslog メッセージまたは Security Device Event Exchange（SDEE）を使用してイベントを記録します。

さまざまな脅威に対して適切な対応を選択するように Cisco IOS IPS を設定できます。Signature Event Action Processor（SEAP）は、忠実度、重大度、ターゲットの価値レーティングなどのパラメータに基づいて、シグニチャイベントが実行するアクションを動的に制御できます。これらのアクションは、[Signatures] ポリシーおよび [Event Actions] ポリシーを使用して Security Manager で設定できます。

セッション内のパケットがシグニチャと一致すると、Cisco IOS IPS は必要に応じて次のいずれかのアクションを実行できます。

- syslog サーバまたは中央管理インターフェイスにアラームを送信する。
- パケットをドロップします。
- 接続をリセットする。

- 指定した期間、攻撃者の送信元 IP アドレスからのトラフィックを拒否する。
- 指定した期間、シグニチャが確認された接続上のトラフィックを拒否する。

シスコでは、柔軟性を念頭に置いてCisco IOS ソフトウェアベースの侵入防御機能およびCisco IOS Firewall を開発しているため、false positive の場合にシグニチャを個別にディセーブルにできます。通常は、ネットワーク セキュリティ ポリシーをサポートするために、ファイアウォールと Cisco IOS IPS の両方をイネーブルにすることを推奨します。ただし、異なるルータ インターフェイス上で、これらの機能を個別にイネーブルにすることもできます。

Cisco IOS IPS 設定プロセスの全般的な説明については、を参照してください。 Cisco IOS IPS 設定の概要 （2318 ページ）

ここでは、次の内容について説明します。

- IPS サブシステムおよび IOS IPS リビジョンのサポートについて （2316 ページ）
- ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャン （2316 ページ）
- ルータ設定ファイルおよびシグニチャ イベント アクション プロセッサ（SEAP） （2317 ページ）
- Cisco IOS IPS の制限事項および制約事項 （2317 ページ）

IPS サブシステムおよび IOS IPS リビジョンのサポートについて

Cisco Security Manager では IOS IPS のマイナー リビジョンが自動的にサポートされます。サポートされているマイナーリビジョンを確認するには、IPS サブシステム バージョンが必要です。

IPS サブシステム バージョンは、Cisco IOS IPS 機能の変更の追跡に使用されるバージョン番号です。サブシステム番号は、デバイスのプロパティで表示されます（デバイスを右クリックして [デバイスプロパティ（Device Properties）] を選択）。Cisco IOS IPS を実行しているルータ上のコマンドラインで **show subsys name ips** コマンドを使用して、詳細な Cisco IOS IPS サブシステムのバージョンを表示することもできます。3.x サブシステムは、IPS 5.x に相当します。Cisco IOS ソフトウェアリリースでサポートされているサブシステムのリストについては、Cisco.com で、該当するリリースの Security Manager の『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください。

IPS サブシステムのバージョンは、バージョンの相違がポストフィックスだけである場合は、マイナーとなります。たとえば、3.0.1 から 3.0.2 へのリビジョンはマイナーと見なされます。別の例として、3.0.1 から 3.1.1 もマイナーなバージョン変更と見なされます。ただし、新機能を含むマイナーリビジョンは、Cisco Security Manager によって自動的にサポートされません。

ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャン

ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャンを Cisco IOS Release 15.0(1)M に追加することにより、Cisco IOS IPS の機能が拡張されます。この機能拡張により、既存のシグニチャ セットと機能的に同等だがより軽量なシグニチャをロードして、より大規模なシグニ

チャセットをロードできるようになります。このとき、追加メモリを大幅に消費したり、既存のシグニチャセットによって消費されるメモリ量を減らしたりする必要はありません。これらのシグニチャは、ライトウェイト シグニチャと呼ばれています。

Security Manager は、ISR およびモジュラ アクセス ルータ上で、LWE のカスタム シグニチャを検出および調整できます。また、ISR およびモジュラ アクセス ルータ上の LWE シグニチャ向けに、次の機能をサポートしています。

- 新しいシグニチャ タイプ
- シグニチャ カテゴリ
- デフォルトの新しいシグニチャ カテゴリ認識
- 新しいエンジン更新レベル
- ライセンス ステータス：バイパス、期限切れ、または未インストール

ルータ設定ファイルおよびシグニチャ イベント アクション プロセッサ（SEAP）

Cisco IOS Release 12.4(11)T 以降、Cisco IOS IPS では、Signature Definition File（SDF; シグニチャ定義ファイル）が使用されなくなりました。このため、Security Manager では、廃止予定の組み込みシグニチャ セットである 128.sdf、256.sdf、および attack-drop.sdf を使用できません。

代わりに、ルータは、3つの設定ファイル（デフォルト設定、デルタ設定、およびSEAP設定）が含まれているディレクトリを介して、シグニチャ定義情報にアクセスします。この場所は、[IPS] > [一般設定（General Settings）] ポリシーを使用して設定できます。

SEAP は、シグネチャイベントのデータフローの調整をする制御ユニットです。SEAP を使用すると、Event Risk Rating（ERR; イベント リスク レーティング）フィードバックに基づく高度なフィルタリングおよびシグニチャの上書きを実行できます。ERR は、false positive を最小限に抑えるために、ユーザが選択するアクション適用レベルを制御するために使用します。

シグニチャは、以前はNVRAMに格納されていましたが、現在はデルタ設定ファイルに格納されます。

Cisco IOS IPS の制限事項および制約事項

Cisco IOS IPS ルータは、専用 IPS センサー アプライアンスおよびサービス モジュールでサポートされているすべての機能をサポートしているわけではありません。また、IOS IPS をサポートするルータが IPS 機能に割り当てるメモリの量は、IPS センサーが割り当てるメモリの量よりも多くはない可能性があります。次の制限事項および制約事項を考慮する必要があります。

- IOS IPS デバイスを設定する場合は、必要なシグニチャだけを選択します。Security Manager で使用可能なシグニチャをすべて選択すると、IOS IPS ルータで使用できるメモリを超過する可能性があります。これにより、配布が失敗したり、デバイスが一部のシグニチャしかロードできなかったり、パフォーマンスが大幅に低下したりする可能性があります。配

布に失敗した場合は、選択するシグニチャセットの数を減らしてから、デバイスに設定を再配布します。

- 初めて IOS-IPS を使用するように設定されている Cisco Security Manager 管理対象ルータでは、シグネチャの更新に自動更新プロセスを使用できません。自動更新プロセスを使用する前に、ルータを更新する必要があります。次の手順に従ってください。

  1. E3 シグネチャ（S317 など）をプッシュします。
  2. S470 などの中間シグネチャをプッシュします。
  3. 最初の E4 シグネチャ（S485 など）をプッシュします。
  4. 目的のレベルに達するまで、後続の E4 シグネチャをプッシュします。各差分のサイズは 10 MB 未満にする必要があります。

ルータを更新したら、自動更新プロセスを使用してシグネチャを更新できます。各増分変更がルータで使用可能なメモリを超えないため、自動更新プロセスは成功します。自動更新の設定については、IPS 更新の自動化 （2305 ページ）を参照してください。

- 仮想センサーは、IOS IPS ではサポートされていません。
- IOS IPS ルータでイベント アクション フィルタを使用する場合は、イベント アクション フィルタの基準に一致したイベントから IPS アクションのサブセットだけを削除できます。使用可能なイベント アクションの詳細については、[Add Filter Item]/[Edit Filter Item] ダイアログボックス （2222 ページ）およびIPS イベント アクションについて （2213 ページ）を参照してください。
- IOS IPS は、IPS ソフトウェア 5.1 に基づいています。したがって、これ以降のバージョンの IPS ソフトウェアで導入された機能は、通常、IOS IPS では使用できません。たとえば、次の機能は設定できません。
  - グローバル相関。
  - 異常検出。
  - イベント アクション ネットワーク識別ポリシーでの OS ID。

Cisco IOS IPS 設定の概要

さまざまなデバイスに侵入防御システムを設定できます。設定の視点から、デバイスは2つのグループに分けられます。1 つは、完全な IPS ソフトウェアを実行する専用アプライアンスおよびサービス モジュール（ルータ、スイッチ、および ASA デバイスの場合）です。もう 1 つは、Cisco IOS ソフトウェア 12.4(11)T 以降（Cisco IOS IPS）を実行する IPS 対応ルータです。

次の手順では、Cisco IOS IPS ルータでの IPS 設定の概要について説明します。ルータにインストールされている IPS サービス モジュールを含む、専用 IPS デバイスについては、IPS 設定の概要 （2088 ページ）を参照してください。

Cisco IOS IPS は機能が限定されています。ブランチ オフィスや中小規模のネットワーク向けであり、1 つのネットワークで IPS を展開するときに使用します。Cisco IOS IPS ルータでは、通常、専用アプライアンスと同数のシグニチャを使用することはできません。また、Cisco IOS IPS は IPS ソフトウェア バージョン 5.1 に基づいているため、グローバル相関などの高度な機能を設定できません。Cisco IOS IPS デバイスを設定する場合、このデバイスは少数の IPS 機能を実行するルータであるため、通常は標準のルータ ポリシーを設定します。一方、IPS アプライアンスおよびサービスモジュール用のプラットフォーム ポリシーは、IPS ソフトウェア専用となります。

ヒント　Cisco IOS IPS を設定する前に、Cisco.com で『*Cisco IOS Intrusion Prevention System Deployment Guide*』を読んでください。

ステップ 1　デバイスを設置し、ネットワークに接続します。デバイス ソフトウェアをインストールし、基本的なデバイス構成を実行します。デバイス上で実行するすべてのサービスに必要なライセンスをインストールします。最初に実行する設定量は、Security Manager で設定する必要がある内容に影響します。必要な基本設定については、次を参照してください。

- Cisco IOS ルータでの SSL の設定　（75 ページ）
- SSH の設定　（77 ページ）
- Cisco IOS デバイスでのライセンスの設定　（84 ページ）
- Cisco IOS IPS ルータでの最初の準備　（2320 ページ）
- Cisco IOS IPS のシグニチャ カテゴリの選択　（2321 ページ）

ステップ 2　デバイスを Security Manager のデバイス インベントリに追加します（デバイス インベントリへのデバイスの追加　（94 ページ）を参照してください）。デバイスを追加するときは、必ず次の選択を行ってください。

- ネットワークまたはエクスポートファイルから追加する場合は、ポリシー検出に [IPS ポリシー（IPS Policies）] を選択します。
- 設定ファイルから、または手動定義によって追加する場合は、[オプション（Options）] リストから [IPS] を選択します。そうしないと、Security Manager から見て、デバイスが IPS 対応ではなくなります。

ステップ 3　ルータ上の IPS ファイルの場所を指定するように、IPS の一般的な設定値を設定します。詳細については、Cisco IOS IPS の一般的な設定値の設定　（2322 ページ）を参照してください。

ステップ 4　IPS をイネーブルにし、IPS インスペクションの適用対象トラフィックのインターフェイスを識別するように、IPS インターフェイス ルールを設定します。詳細については、IOS IPS インターフェイス ルールの設定　（2325 ページ）を参照してください。

ステップ 5　IPS シグニチャおよびイベント アクションを設定します。イベント アクション ポリシーの設定は、カスタムのシグニチャの作成よりも簡単であるため、特定のシグニチャを編集する前に、イベント アクション

フィルタを使用して、シグニチャの動作を変更するように上書きしてみてください。詳細は、次のトピックを参照してください。

- イベント アクション ルールの設定 （2211 ページ）
- シグニチャの設定 （2169 ページ）

ステップ 6 デバイスを次のように保守します。

- 必要に応じて、設定を更新および再配布します。
- 更新したシグニチャおよびエンジン パッケージを適用します。更新の確認、更新の適用、および定期的な自動更新の設定については、 IPS 更新の管理 （2302 ページ）を参照してください。

Cisco IOS IPS ルータでの最初の準備

Cisco IOS IPS ルータを Security Manager インベントリに追加する前に、いくつかの準備手順を実行する必要があります。ホワイト ペーパー『Getting Started with Cisco IOS IPS with 5.x Format Signatures』では、基本設定の各手順について説明しています。ルータを Security Manager に追加した後で、インターフェイスルールの設定など、いくつかの手順を実行できますが、少なくとも基本的な手順を実行する必要があります。

次の手順では、CLI で実行する必要がある手順について説明しています。Security Manager でこれらの手順を完了することができないか、CLI で（1 回限りの設定として）実行する方が簡単であるため、これらの手順が必要です。このホワイト ペーパーには、CLI で実行できる追加の手順が含まれており、デバイスをインベントリに追加したときに Security Manager によってこれらの設定が検出されます。多くの設定を CLI で実行しておくと、Security Manager で実行する必要がある設定が少なくなります。

ヒント Cisco IOS ルータでの SSL の設定 （75 ページ）、 SSH の設定 （77 ページ）、および Cisco IOS デバイスでのライセンスの設定 （84 ページ）で説明されている基本的なルータ設定手順も完了する必要があります。次に示すのは、IPS 設定だけに適用される手順です。

ステップ 1 フラッシュ上に IPS ファイルのディレクトリを作成します。たとえば、次のコマンドによって ips という名前のディレクトリが作成されます。

例：

```
router# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

この時点で、IPS 用のこのディレクトリをルータが使用するように任意で設定できます。または、あとで Security Manager で設定することもできます（[IPS] > [General Settings] ポリシー）。次のコマンドを使用して、CLI でこの設定を行います。

例：

```
router# configure terminal
router(config)# ip ips config location flash:ips
```

ステップ 2 Cisco IOS IPS 暗号化キーを設定します。暗号化キーは、メインシグニチャファイル（sigdef-default.xml）のデジタル署名を検証するために使用されます。メインシグニチャファイルの内容は、すべてのリリースでの真正性および完全性を保証するために、シスコの秘密キーによって署名されています。

キーに必要な CLI は、http://download-sj.cisco.com/cisco/ciscosecure/ids/sigup/5.0/ios/realm-cisco.pub.key.txt から取得できます（Cisco.com へのログインが必要）。

ヒント 暗号化キーの設定は、CLI を使用して行うのが最も簡単な方法です。または、IOS_IPS_PUBLIC_KEY 事前定義 FlexConfig オブジェクトをルータの FlexConfig ポリシーに割り当てて、Security Manager で設定することもできます。FlexConfig の詳細については、FlexConfig の管理 （431 ページ）を参照してください。

a) テキスト ファイルを開き、その内容をクリップボードにコピーします（すべてのテキストを選択し、Ctrl を押した状態で C を押します）。
b) 必要に応じて、ルータ CLI プロンプトで **configure terminal** を入力します。
c) コピーしたテキスト ファイルをルータ プロンプトに貼り付けます。
d) コンフィギュレーション モードを終了します。
e) **show run** コマンドを入力して、キーが正しく設定されたことを確認します。

ステップ 3 Syslog は、デフォルトで IPS 通知用に構成されています。SDEE を通知に使用する場合は、次のように SDEE をイネーブルにします。

例：

```
router# configure terminal
router(config)# ip ips notify sdee
```

ステップ 4 編集するシグニチャ カテゴリを選択します。詳細については、Cisco IOS IPS のシグニチャ カテゴリの選択 （2321 ページ）を参照してください。

Cisco IOS IPS のシグニチャ カテゴリの選択

IPS 5.x 形式のシグニチャを使用する Cisco IPS アプライアンスおよび Cisco IOS IPS は、シグニチャ カテゴリで機能します。すべての署名はカテゴリに分類されます。カテゴリは階層的です。個々のシグニチャは、複数のカテゴリに属することができます。最上位のカテゴリによって、一般的なシグニチャ タイプを定義できます。各最上位シグニチャ カテゴリの下には、サブカテゴリが存在します（サポートされているトップレベルカテゴリのリストについては、ルータの CLI ヘルプ （?）と **category** コマンドを使用してください。）

ルータにはメモリとリソースの制約があるため、一部の Cisco IOS IPS シグニチャしかロードできません。したがって、カテゴリによって定義された選択された一連の署名のみをロードすることをお勧めします。カテゴリは、「上から下」の順に適用されるため、最初にすべてのシグニチャを廃棄してから、特定のカテゴリの廃棄を「解除」します。シグニチャが廃棄された場合、ルータは、すべてのシグニチャに関する情報をロードできますが、並行スキャンデータ構造を構築しません。

廃棄されたシグニチャは Cisco IOS IPS によってスキャンされないため、アラームは起動しません。シグニチャがご使用のネットワークに関係ない場合、またはルータのメモリを節約する必要がある場合は、必要に応じてシグニチャを廃棄してください。

Security Manager では、シグニチャ カテゴリ コマンドは管理されません。このコマンドは、ポリシーを使用して直接設定できません。ただし、このコマンドを設定する FlexConfig オブジェクトを含めるように、FlexConfig ポリシーを設定できます。使用できる事前定義されたオブジェクト IOS_IPS_SIGNATURE_CATEGORY があります。基本とは異なるカテゴリを設定する場合は、このオブジェクトをコピーして、編集します。FlexConfig の使用方法については、FlexConfig の管理 （431 ページ）を参照してください。

ヒント　デバイスによって編集が試行される IPS シグニチャのサブセットの選択に **category** コマンドを使用しない場合は、Security Manager によって、デバイスリソースのオーバーロードを回避するための IOS IPS 基本カテゴリをイネーブルにするようにカテゴリコマンドが設定されます。デバイスでカテゴリを手動で変更して、編集する別のシグニチャ セットを選択できます。カテゴリを設定してから、デバイスを Security Manager に追加することを推奨します。ただし、これは、デバイスを手動定義で追加している場合は実行できません。

次の例は、最初にすべてのシグニチャを廃棄し、次に基本的なカテゴリを設定し、基本的なシグニチャの廃棄を解除する方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
```

Cisco IOS IPS の一般的な設定値の設定

[General Settings] ページを使用して、特定のルータ用に定義された Cisco IOS IPS プロパティに対して使用するグローバル設定を指定します。デフォルト設定は、大半の状況に適していますが、IPS 設定ファイルの場所を指定する必要があります。設定ファイルをルータに格納する場合は、Cisco IOS IPS ルータでの最初の準備 （2320 ページ）で説明しているように、最初にディレクトリを作成する必要があります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [IPS] > [一般設定（General Settings）] を選択します。
- （ポリシービュー）[IPS（ルータ）（IPS (Router)）] > [一般設定（General Settings）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- Cisco IOS IPS 設定の概要 （2318 ページ）
- Cisco IOS IPS について （2315 ページ）

フィールド リファレンス

表 *547 : [General Settings]* ページ

要素	説明
Block Traffic when IPS engine is unavailable	IPS エンジンが使用できない場合（シグニチャ エンジンが構築中であったり、構築に失敗した場合など）に、検査されていないすべてのトラフィックをブロックするかどうか。 このオプションをオンにすると、インスペクションに指定されたトラフィックは、IPSが処理できない場合にすべてドロップされます（「フェールクローズモード」とも呼ばれます）。選択しなかった場合、トラフィックはルータ上の他のルールに従って通過を許可されます（デフォルト）。
Apply Deny Action On	[インラインで攻撃者を拒否（Deny Attacker Inline）] イベントまたは [インラインでフローを拒否（Deny Flow Inline）] イベントの場合にトラフィックをドロップするには、ここでACLエントリを適用します。次のいずれかの値を選択します。 • [入力インターフェイス（Ingress Interface）]（デフォルト）：トラフィックの発信元ネットワークに接続されたインターフェイスで拒否アクションを強制的に実行します。 • [IPS 有効インターフェイス（IPS enabled interfaces）]：トリガーされた IPS ルールが適用されるインターフェイスで拒否アクションを強制的に実行します。 このオプションをイネーブルにすると、IOS IPS は、ACL を IPS インターフェイスに直接適用し、攻撃トラフィックを最初に受信したインターフェイスには適用しません。ルータでロードバランシングが実行されていない場合は、この設定をイネーブルにしないでください。ルータでロードバランシングが実行されている場合は、この設定をイネーブルにすることを推奨します。

要素	説明
SDEE Properties	
[最大サブスクリプション（Maximum Subscriptions）]	許可される同時 SDEE サブスクリプションの最大数（1 ～ 3 の範囲）。SDEE サブスクリプションは、SDEE イベントのライブ フィードです。 デフォルトは 1 です。
Maximum Alerts	ルータが格納する SDEE アラートの最大数。10 ～ 2000 の範囲で指定します。格納するアラートの数が増えると、より多くのルータメモリが使用されます。 デフォルトは 200 です。
Maximum Messages	ルータが格納する SDEE メッセージの最大数。10 ～ 500 の範囲で指定します。格納するメッセージの数が増えると、より多くのルータ メモリが使用されます。 デフォルトは 200 です。
[IPS 設定ロケーションのプロパティ（IPS Config Location Properties）]	
IPS Config Location	ルータが IOS IPS 固有の設定ファイルを保存する場所。これらの設定ファイルは、IOS IPS 設定が Security Manager で変更または更新されるたびに、自動的に更新されます。ルータが再起動すると、これらの設定ファイルから IOS IPS 設定が取得および復元されます。 ルータ上の場所を指定するには、ディレクトリの名前を入力します。すでに存在しているディレクトリである必要があります。Security Manager によってディレクトリは作成されません。flash:ips などです。 （注） ルータに LEFS ベースのファイル システムがある場合、ルータのメモリにディレクトリを作成することはできません。この場合、flash: は設定場所として使用されます。 リモート システム上の場所を指定する場合は、その場所に到達するために必要なプロトコルおよび URL のパスを指定します。たとえば、設定ファイルを HTTP サーバに保存する場合は、http://172.27.108.5/ips-cfg と入力します。 IOS IPS 設定ファイルを保存するためにサポートされるサーバーは、http://、https://、ftp://、rcp://、scp://、および tftp:// です。
Max retries	リモート システムに設定ファイルを保存する場合に、ルータがそのリモート システムへの接続を試行する回数。 デフォルトは 1 です。

要素	説明
Timeout seconds between retries	リモート システムに設定ファイルを保存する場合に、設定場所への接続を再試行するまでにルータが待機する時間。 デフォルトは 1 です。

IOS IPS インターフェイス ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IPS インターフェイス ルール ポリシーを使用して、IPS インスペクションを Cisco IOS IPS ルータでイネーブルにし、IPS インスペクションが適用されるインターフェイスを指定します。ACL を設定し、インターフェイスに対するトラフィックの方向を指定することにより、インスペクションの対象となるインターフェイス上のトラフィックのサブセットを特定できます。

関連項目

- Cisco IOS IPS 設定の概要 （2318 ページ）
- Cisco IOS IPS について （2315 ページ）

ステップ 1 次のいずれかを実行して、変更するインターフェイス ルール ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [インターフェイスルール（Interface Rules）] を選択します。
- （ポリシービュー）ポリシーセレクタから [IPS（ルータ）（IPS (Router)）] > [インターフェイスルール（Interface Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ポリシーには、ルールの名前、検査されるトラフィックを定義する ACL の名前（ある場合）、検査されるインターフェイスやトラフィック方向など、既存のインターフェイス ルールが示されます。ACL が指定されていない場合、指定された方向のインターフェイス上のすべてのトラフィックが検査されます。

ルールには番号が付けられていますが、ルールの順序は IPS 処理に影響しません。

ステップ 2 [IPS の有効化（Enable IPS）] を選択して、IOS IPS 設定のデバイスへの展開を有効にします。

[Enable IPS] が選択されていない場合、IPS ルールはすべてのルータ インターフェイスから削除され、IPS はディセーブルになります。また、署名またはイベントアクションポリシーは展開されません。

ステップ 3 インターフェイス ルールを設定します。このルールにより、IPS によって検査されるインターフェイス（およびインターフェイス上のトラフィックの方向）が特定されます。これらのルールには、検査するトラフィックのサブセットを識別するための ACL を任意で含めることができます。

- ルールを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[IP ルールの追加（Add IPS Rule）] ダイアログボックスに入力します。詳細については、[IPS Rule] ダイアログボックス （2326 ページ）を参照してください。
- ルールを編集するには、ルールを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

[IPS Rule] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

[Add IPS Rule] または [Edit IPS Rule] ダイアログボックスを使用して、アクティブ シグニチャ ポリシーを使用して検査するトラフィック フローを特定します。

ナビゲーション パス

[インターフェイスルールポリシー（Interface Rules policy）] から、[行の追加（Add Row）] ボタンをクリックして新しいルールを追加するか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。[インターフェイスルールポリシー（Interface Rules policy）] を開く詳細については、IOS IPS インターフェイス ルールの設定 （2325 ページ）を参照してください。

フィールド リファレンス

表 548 : [Add IPS Rule]/[Edit IPS Rule] ダイアログボックス

要素	説明
ルール名（Rule Name）	この IPS ルールの一意の名前。 IPS ルール名では、大文字と小文字が区別されません。以前に定義された別の文字と同じ文字を含むけれど、大文字と小文字が異なるルール名を使用することはできません。たとえば、MYRULE と MyRule は同じです。

要素	説明
ACL Name	IPS インスペクションの対象となるトラフィックを定義する ACL ポリシーオブジェクトの名前。ACL を指定しなかった場合は、[Interface Pairs] テーブルに示されているインターフェイス/方向のペアに該当するすべてのトラフィックに対してインスペクションが適用されます。 ヒント ACL を作成している場合は、許可エントリによって、検査が適用されるトラフィックが特定され、拒否エントリによって、検査が免除されるトラフィックが特定されます。ACL の最後には暗黙的な deny any any ルールがあるため、免除トラフィックを特定する場合は、permit any any ルールを ACL の最後に必ず追加してください。 ACL ポリシーオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。
[Interface Pairs] テーブル	IPS インスペクションの対象となるインターフェイスとトラフィック方向のペア。 • ペアを追加するには、[行の追加（+）（Add Row (+)）] ボタンをクリックし、[ペアの追加（Adding Pair）] ダイアログボックスに入力します。ペアのダイアログボックス （2327 ページ）を参照してください。 • ペアを編集するには、URL を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 • ペアを削除するには、ペアを選択し、[Delete Row（行の削除）]（ゴミ箱）ボタンをクリックします。

ペアのダイアログボックス

[ペアの追加または編集（Adding or Editing Pair）] ダイアログボックスを使用して、Cisco IOS IPS インターフェイスルールに追加するインターフェイスとトラフィック方向のペアを特定します。インターフェイスルールの設定の詳細については、IOS IPS インターフェイス ルールの設定 （2325 ページ）を参照してください。

ナビゲーション パス

[IPSルールの追加または編集（Add or Edit IPS Rule）] ダイアログボックスで、[行の追加（Add Row）]ボタンをクリックして新しいペアを追加するか、またはペアを選択して[行の編集（Edit Row）] ボタンをクリックします。[IPSルールの追加または編集（Add or Edit IPS Rule）] ダイアログボックスを開く方法については、[IPS Rule] ダイアログボックス （2326 ページ）を参照してください。

フィールド リファレンス

表 *549 : [Adding Pair]/[Editing Pair]* ダイアログボックス

要素	説明
方向（Direction）	IPS インスペクションが実行される、インターフェイスにおけるトラフィック方向。次のいずれかを選択します。 • [イン（In）]（デフォルト）：IPS ルールは、インバウンドトラフィックに適用されます。 • [アウト（Out）]：IPS ルールは、アウトバウンドトラフィックに適用されます。 • [両方（Both）]：IPS ルールは、インバウンドとアウトバウンドトラフィックの両方に適用されます。
インターフェイス	IPS ルールを適用するインターフェイス。インターフェイスまたはインターフェイスロールオブジェクトの名前を入力します。あるいは、[選択（Select）]をクリックして、リストからインターフェイスまたはインターフェイスロールを選択するか、または新しいインターフェイスロールを作成します。 インターフェイスロールを使用する場合、ルールは、ロールによって定義されたデバイス上のすべてのインターフェイスに適用されます。ロールに一致するインターフェイスは、既存のルールと競合できません。複数のインターフェイス ルールに同じインターフェイスを指定することはできません。

第 V 部

PIX/ASA/FWSM デバイスの設定

- ファイアウォール デバイスの管理 （2331 ページ）
- ファイアウォール デバイスでのブリッジング ポリシーの設定 （2449 ページ）
- ファイアウォール デバイスでのデバイス管理ポリシーの設定 （2467 ページ）
- ファイアウォール デバイスでのデバイス アクセスの設定 （2497 ページ）
- フェールオーバーの設定 （2541 ページ）
- ホスト名、リソース、ユーザ アカウントおよび SLA の設定 （2581 ページ）
- ファイアウォール デバイスでのサーバ アクセスの設定 （2597 ページ）
- Firepower 2100 シリーズ デバイスでの FXOS サーバーアクセス設定の構成 （2629 ページ）
- ファイアウォール デバイスでのロギング ポリシーの設定 （2635 ページ）
- ファイアウォール デバイスでのマルチキャスト ポリシーの設定 （2675 ページ）
- ファイアウォール デバイスでのルーティング ポリシーの設定 （2703 ページ）
- ファイアウォール デバイスのセキュリティ ポリシーの設定 （2931 ページ）
- ファイアウォール デバイスでのサービス ポリシールールの設定 （2941 ページ）
- ファイアウォール デバイスでのセキュリティ コンテキストの設定 （2979 ページ）
- ユーザー設定 （2995 ページ）

第 46 章

ファイアウォール デバイスの管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチ、PIX、FWSM、IOS デバイス、および IPS をサポートしていますが、バグ修正や拡張機能はサポートしていません。

ここでは、Cisco セキュリティ デバイス上のセキュリティ サービスおよびポリシーの設定と管理について説明します。Cisco セキュリティ デバイスとは、Adaptive Security Appliances（ASA; 適応型セキュリティ アプライアンス）、PIX ファイアウォール、および Catalyst 6500 シリーズ スイッチ サービス モジュール（Firewall Services Module（FWSM; ファイアウォール サービス モジュール）および ASA-SM）を指しています。

この章は次のトピックで構成されています。

- ファイアウォールデバイスのタイプ （2331 ページ）
- ファイアウォールのデフォルト設定 （2333 ページ）
- ファイアウォール デバイスのインターフェイスの設定 （2333 ページ）
- VXLAN （2446 ページ）

ファイアウォールデバイスのタイプ

Security Manager は、さまざまな Cisco セキュリティ アプライアンスやファイアウォール デバイスを検出および管理できます。その中には、特に次のものが含まれます。

- PIX 500 シリーズ ファイアウォール デバイス
- Cisco Virtual Security Appliance（ASAv）を含む ASA 5500 シリーズ セキュリティ アプライアンス
- Firepower 3100 シリーズ ファイアウォール デバイス
- セキュリティ固有の Catalyst サービスモジュール

PIX 500 シリーズ

Private Internet eXchange（PIX）500 シリーズ ファイアウォール アプライアンスは販売終了となっていますが、現在でもサポートされており、世界中で多数が使用されています。

ASA 5500 シリーズ

適応型セキュリティアプライアンス（ASA）5500 シリーズデバイスは、コンテキスト認識型ファイアウォール機能やリアルタイム脅威防御など、包括的なセキュリティサービスを提供します。ASA 5500 は、シスコのプライマリ セキュリティ アプライアンスとして PIX 500 に代わるものです。詳細については、cisco.com の 「Cisco ASA 5500 Series Adaptive Security Appliance」のページを参照してください。

Cisco ASAv 仮想アプライアンスは、ASA 9.2(1) で導入され、仮想環境に包括的なファイアウォール機能を提供し、データセンタートラフィックとマルチテナント環境のセキュリティを強化します。ASAv は、VMware vSphere 上で稼働します。ASAv は仮想デバイスですが、Security Manager で他の ASA デバイスと同様に管理されます。ASAv の詳細については、「http://www.cisco.com/c/en/us/support/security/virtual-adaptive-security-appliance-firewall/tsd-products-support-series-home.html」を参照してください。

（注） ASAv は、次の ASA 機能をサポートしていません：クラスタリング、マルチコンテキストモード、アクティブ/アクティブフェールオーバー、イーサチャネル、共有 AnyConnect プレミアムライセンス。

Firepower 3100 シリーズ

Firepower 3100 シリーズ ファイアウォール デバイスのサポートは、CSM 4.24 の ASA 9.17(1) デバイスに導入されました。

Catalyst サービス モジュール

Catalyst 6500 スイッチには、ファイアウォールサービスとセキュリティサービスを提供する 2 つを含む、さまざまなサービスモジュール（SM）が用意されています。これは、スイッチ シャーシに直接インストールするブレード タイプのモジュールです。

ファイアウォール サービス モジュール（FWSM）を使用すると、スイッチ上の任意のポートをファイアウォールポートとして動作させることができ、ネットワーク構造の内部のファイアウォールセキュリティを統合できます。

Adaptive Security Appliance Service Module（ASA-SM; 適応型セキュリティ アプライアンス サービス モジュール）は、レイヤ 2 から 7 で高速のセキュリティ サービスを提供し、1 台のスイッチに 4 台の ASA-SM ブレードをインストール可能にすることで、64 Gbps のスケーラビリティを提供します。

（注） ASA-SM は、物理的に FWSM と同じように、Catalyst 6500 スイッチにインストールされたブレードですが、ASA デバイスであり、そのように文書化されています。ASA-SM に関する情報については、ASA 関連のトピックを参照してください。必要な場合には、サービス モジュールと ASA アプライアンスに関する注意点および相違点が記載されています。

ファイアウォールのデフォルト設定

ファイアウォールデバイスは、すでにある程度設定された状態で出荷されています。新規で設置したファイアウォール デバイスを手動で Cisco Security Manager に追加する場合は、そのデバイスのプリセットまたはデフォルト ポリシーを見つける（インポートする）必要があります。これらのポリシーを Security Manager にインポートすることによって、そのデバイスに最初に設定を展開したときに、これらのポリシーを意図せずに削除してしまわずにすみます。ポリシーをインポートする方法の詳細については、ポリシーの検出 （223 ページ）を参照してください。

Cisco Security Manager には、多数のデバイス タイプやバージョンのデフォルト ポリシーを含む設定ファイルのセットが用意されています。これらの設定ファイルは、<install_dir>\CSCOpx\MDC\fwtools\pixplatform\ ディレクトリ（たとえば、C:\Program Files\CSCOpx\MDC\fwtools\pixplatform\）に格納されています。

ファイル名は、デバイス タイプ、オペレーティング システムのバージョン、コンテキストのサポート、および動作タイプを表しています。たとえば、「FactoryDefault_FWSM2_2_MR.cfg」は、FWSM、バージョン 2.2 で、マルチコンテキストをサポートし、ルーテッドモードで動作する場合の設定ファイルです。同様に、「FactoryDefault_ASA7_0_1_ST.cfg」は、ASA、バージョン 7.0.1、シングルコンテキストのトランスペアレントモードの設定ファイルです。

セキュリティ コンテキストの詳細については、シングルおよびマルチ コンテキストのインターフェイス （2337 ページ）を、ルーテッドおよびトランスペアレント動作の詳細については、ルーテッド モードおよびトランスペアレント モードのインターフェイス （2336 ページ）を参照してください。

提供されている設定ファイルから新しいデバイスを追加する方法については、設定ファイルからのデバイスの追加 （112 ページ）を参照してください。

ファイアウォール デバイスのインターフェイスの設定

[Interfaces] ページには、設定されている物理インターフェイス、論理インターフェイス、および冗長インターフェイスが表示されます。また、選択したデバイスのハードウェア ポートとブリッジ グループも表示されます。このページでは、インターフェイスを追加、編集、および削除できます。また、同じセキュリティ レベルのインターフェイス間の通信を可能にしたり、VPDN グループおよび PPPoE ユーザを管理したりできます。

（注） ASA 5505 デバイスに表示される [Interfaces] ページには、[Hardware Ports] および [Interfaces] の 2 つのタブ付きパネルが表示されます。同様に、トランスペアレントモードで動作している Catalyst 6500 サービス（ASA-SM および FWSM）に表示される [インターフェイス（Interfaces）] ページにも、[インターフェイス（Interfaces）] と [ブリッジグループ（Bridge Groups）] の 2 つのタブ付きパネルが表示されます。

ナビゲーション パス

[インターフェイス（Interfaces）] ページにアクセスするには、デバイスビューでセキュリティ デバイスを選択し、デバイスポリシーセレクタから [インターフェイス（Interfaces）] を選択します。

ここでは、次の内容について説明します。

- デバイス インターフェイスについて （2334 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）
- 高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）

デバイス インターフェイスについて

インターフェイスは、セキュリティ デバイスと他のネットワーク デバイスとの間の接続ポイントです。インターフェイスは、最初はディセーブルになっています。そのため、ファイアウォール設定に不可欠な作業として、インターフェイスをイネーブルにし、適切なパケット インスペクションおよび転送を許可するように設定する必要があります。

インターフェイスには、物理インターフェイスと論理インターフェイスの2つのタイプがあります。物理インターフェイスは、ネットワーク ケーブルが差し込まれるデバイス上の実際のスロットであり、論理インターフェイスは、特定の物理ポートに割り当てられる仮想ポートです。一般的に、物理ポートはインターフェイスと呼ばれます。また、論理ポートは機能に応じて、サブインターフェイス、仮想インターフェイス、VLAN、または EtherChannel と呼ばれます。定義できるインターフェイスの数とタイプは、アプライアンス モデルおよび購入したライセンスのタイプによって異なります。

（注） PIX オペレーティングシステムのバージョン 6.3 を実行しているデバイスでは、「インターフェイス」および「サブインターフェイス」ではなく、「物理」および「論理」というラベルが使用されます。また、トランスペアレントモードとマルチコンテキストは、これらのデバイスではサポートされていません。

サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLANにより、特定の物理インターフェイ

ス上でトラフィックを分離しておくことができるため、物理インターフェイスやセキュリティアプライアンスを追加しなくても、ネットワークで使用できるインターフェイスの数を増やすことができます。この機能は、マルチ コンテキスト モードで特に役立ち、これにより、各コンテキストに一意のインターフェイスを割り当てることができます。

原則として、インターフェイスはルータベースのネットワークに接続し、サブインターフェイスはスイッチベースのネットワークに接続します。すべてのサブインターフェイスが、許可トラフィックを正しくルーティングする物理インターフェイスに関連付けられている必要があります。

物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。サブインターフェイスでトラフィックを通過させるために、物理インターフェイスはイネーブルにしておく必要がありますが、物理インターフェイスではトラフィックを通過させないように、物理インターフェイスには名前を付けないでください。ただし、物理インターフェイスでタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます（インターフェイスの命名の詳細については、デバイスインターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください）。

（注） スイッチ機能とセキュリティ アプライアンス機能を組み合わせた ASA 5505 は、物理スイッチ ポートと論理 VLAN インターフェイスの両方を設定する特殊な事例です。詳細については、ASA 5505 のポートおよびインターフェイスについて （2338 ページ）を参照してください。

Catalyst 6500 サービスモジュール（ASA-SM および FWSM）には外部物理インターフェイスは含まれません。代わりに、内部 VLAN インターフェイスを使用します。たとえば、VLAN 201 を FWSM 内部インターフェイスに割り当てて、VLAN 200 を外部インターフェイスに割り当てるとします。これらの VLAN を物理スイッチ ポートに割り当てると、ホストがこれらのポートに接続します。VLAN 201 と 200 間で通信が行われる場合は、FWSM が VLAN 間で唯一使用可能なパスであり、トラフィックはステートフルに検査されるように強制されます。

デバイス インターフェイスの追加情報については、次の項を参照してください。

- ルーテッド モードおよびトランスペアレント モードのインターフェイス （2336 ページ）
- シングルおよびマルチ コンテキストのインターフェイス （2337 ページ）
- ASA 5505 のポートおよびインターフェイスについて （2338 ページ）
- サブインターフェイスの設定（PIX/ASA） （2339 ページ）
- 冗長インターフェイスの設定 （2341 ページ）
- EtherChannel の設定 （2343 ページ）
- VNI インターフェイスの設定 （2350 ページ）
- トンネルインターフェイスの設定 （2360 ページ）

セキュリティ アプライアンスの設定

ファイアウォールデバイスではさまざまな設定が可能であり、設定によって、特定のデバイスに関連付けられるインターフェイスの定義方法が決まります。次の表に、さまざまな設定の概要を示します。

表 *550* : セキュリティ アプライアンスの設定

デバイスタイプ	動作モード（ルータまたはトランスペアレント）	コンテキストのサポート（シングルまたはマルチ）
PIX 6.3.x	該当なし	該当なし
PIX 7.0 以降/ASA	ルータまたはトランスペアレント	シングル
PIX 7.0 以降/ASA、または管理対象外の PIX 7.0 以降/ASA のセキュリティ コンテキスト	ルータまたはトランスペアレント	マルチ（マルチ セキュリティ コンテキストを設定するためのチェックリスト （2981 ページ）を参照）
FWSM、または管理対象外スイッチのセキュリティ コンテキスト（マルチ モード）	ルータまたはトランスペアレント	シングルまたはマルチ

ルーテッド モードおよびトランスペアレント モードのインターフェイス

ASA/PIX 7.0 および FWSM 2.2.1 以降、2 つのモード（ルーテッドまたはトランスペアレント）のどちらかで動作するように、セキュリティデバイスを設定できるようになりました。（PIX 6.3 はルーテッド モードでだけ動作します）。

ルーテッドモードの場合、セキュリティアプライアンスは接続されているネットワークのゲートウェイまたはルータとして機能します。つまり、そのインターフェイスの IP アドレスを保持し、IP アドレス（レイヤ 3）情報に基づいて、これらのインターフェイスを通過するトラフィックを検査およびフィルタリングします。このモードでは、各デバイスインターフェイスが別の IP サブネットに接続され、そのサブネット上で専用の IP アドレスを持ちます。ルーテッドモードは、シングルモードで、またはコンテキストごとに、最大256個のインターフェイスをサポートし、最大で 1000 個のインターフェイスがすべてのコンテキスト間で分配されます。

トランスペアレントモードの場合、セキュリティアプライアンスはレイヤ 2（データリンク）デバイス、またはトランスペアレントブリッジとして動作し、多くの場合、「Bump In The Wire」または「ステルスファイアウォール」と呼ばれます。このモードでは、内部と外部の 2 つのインターフェイスのみを定義できます。これらのインターフェイスには IP アドレスは必要ありません。VLAN ID を使用して検査済みのトラフィックを転送します。ただし、デバイスに専用の管理インターフェイスが含まれている場合は、これ（物理インターフェイスまたはサブインターフェイスのどちらか）をデバイス管理トラフィック用の3番めのインターフェイスとして使用できます。

（注） Cisco Security Manager は、検出中に FWSM 2.x デバイスのインターフェイス情報を読み込みません。

ブリッジ グループ

ASA 8.4.1 および FWSM 3.1 から、トランスペアレント モードでブリッジ グループを使用して、デバイスやコンテキストで使用可能なインターフェイスの数を増やすことができるようになりました。ブリッジグループは 8 個まで設定できます。FWSM では各グループに 2 つのインターフェイスを含めることができ、ASA 9.7.1（Cisco Security Manager 4.13）では各グループに最大 64 のインターフェイスを含めることができます。詳細については、[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （2432 ページ）を参照してください。

シングルおよびマルチ コンテキストのインターフェイス

セキュリティの「コンテキスト」によって、単一の物理デバイスが複数の独立したファイアウォールとして動作できます。マルチ コンテキスト モードの場合、個々のコンテキストは独自の設定を備えた単一の仮想ファイアウォールを定義します。各コンテキストは一意の仮想ファイアウォールとして機能して、そのコンテキストに割り当てられたインターフェイスを通過するトラフィックを検査およびフィルタリングします。コンテキストはそれぞれ、同じセキュリティアプライアンスに定義されている他のコンテキストを「認識しません」。

シングル コンテキストのルーテッド モード デバイスの場合、マルチ コンテキスト デバイス上のインターフェイスはルータベースのネットワークに接続し、サブインターフェイスはスイッチベースのネットワークに接続します。さらに、各サブインターフェイスは、許可トラフィックを正しくルーティングするインターフェイスに関連付けられている必要があります。

ただし、コンテキストを定義して展開するまで、設定のルーテッド モード部分である IP アドレスは定義できず、管理インターフェイスも指定できません。しかし、必要なインターフェイスおよびサブインターフェイスを定義するまで、セキュリティ コンテキストは定義できません。

つまり、セキュリティ コンテキスト自体を定義および設定する前に、（ルーテッド モードまたはトランスペアレント モードのどちらの場合でも）複数のセキュリティ コンテキストを提供するデバイス上でインターフェイスおよびサブインターフェイスをイネーブルにして設定する必要があります。

非対称ルーティング グループについて

場合によっては、セッションのリターン トラフィックは、そのセッションが送信されたインターフェイスとは別のインターフェイスでルーティングされることがあります。同様に、フェールオーバー設定では、ある装置から発信された接続のリターン トラフィックが、ピア装置を経由して返送されることがあります。これは一般に、1 つの FWSM 上の 2 つのインターフェイス、またはフェールオーバー ペアの 2 つの FWSM が別々のサービス プロバイダーに接続され、発信接続で NAT アドレスを使用しない場合に起こります。デフォルトでは、リターン トラフィックには接続情報がないため、FWSM はそのトラフィックをドロップします。

ドロップが発生する可能性のある VLAN インターフェイスに、Asymmetric Routing（ASR; 非対称ルーティング）グループを割り当てることで、リターン トラフィックのドロップを防止できます。メンバインターフェイスがセッション情報のないパケットを受信すると、そのインターフェイスは同じグループのメンバである他のインターフェイスのセッション情報を確認します。

一致が検出されない場合は、パケットはドロップされます。一致が検出された場合は、次のいずれかのアクションが実行されます。

- 着信トラフィックが同一 FWSM 上の異なるインターフェイスで発信された場合、レイヤ 2 ヘッダーの一部または全部が書き換えられ、パケットは再度ストリームに入れられます。
- 着信トラフィックがフェールオーバー設定のピア装置で発信された場合、レイヤ 2 ヘッダーの一部または全部が書き換えられ、パケットはもう一方の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。

（注） フェールオーバー設定では、スタンバイ ユニットやフェールオーバー グループからアクティブ ユニットやフェールオーバー グループに転送されるセッション情報について、ステートフル フェールオーバーをイネーブルにする必要があります。

FWSM 仮想インターフェイスを非対称ルーティング グループに割り当てるには、単に ASR Group ID を [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）（2396 ページ）に指定します。グループが存在しない場合はグループが作成され、インターフェイスがそのグループに割り当てられます。

この ASR グループに参加するインターフェイスごとに、この割り当てを繰り返す必要があります。最大 32 個の ASR グループを作成して、各グループに最大 8 個のインターフェイスを割り当てることができます。

（注） フェールオーバー設定のスタンバイ ユニットからアクティブ ユニットにパケットをリダイレクトできるようにするには、アップストリーム ルータとダウンストリーム ルータは、VLAN ごとに 1 つの MAC アドレスを使用し、異なる VLAN には異なる MAC アドレスを使用する必要があります。

ASA 5505 のポートおよびインターフェイスについて

ASA 5505 は組み込みスイッチを含んでいるという点で独特であり、また、設定に必要なポートおよびインターフェイスが 2 種類存在します。

- 物理スイッチ ポート：ASA 5505 には、ハードウェアのスイッチング機能を使用して、レイヤ 2 でトラフィックを転送するファストイーサネット スイッチ ポートが 8 個あります。これらのポートのうちの 2 つは、Power-over-Ethernet（PoE）ポートです。これらのポートは、PC、IP Phone、または DSL モデムなどのユーザ機器に直接接続できます。または、別のスイッチに接続できます。

- 論理 VLAN インターフェイス：ルーテッド モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ 3 の VLAN ネットワーク間でトラフィックを転送します。トランスペアレント モードでは、これらのインターフェイスは、設定済みのセキュリティ ポリシーを使用してファイアウォール サービスを適用することによって、レイヤ 2 の同じネットワーク上の VLAN 間でトラフィックを転送します。

スイッチ ポートを別々の VLAN に分離するには、各スイッチ ポートを VLAN インターフェイスに割り当てます。同じ VLAN 上のスイッチ ポートは、ハードウェア スイッチングを使用して相互に通信できます。ただし、1 つの VLAN 上のスイッチ ポートが別の VLAN 上のスイッチ ポートとの通信を試行した場合は、ASA 5505 によって、トラフィックおよび 2 つの VLAN 間のルートまたはブリッジにセキュリティ ポリシーが適用されます。

（注） サブインターフェイスと冗長インターフェイスは、ASA 5505 では使用できません。

ナビゲーション パス

ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[ハードウェア ポート（Hardware Ports）] および [インターフェイス（Interfaces）] の 2 つのタブ付きパネルが表示されます。これらのパネルにアクセスするには、[デバイスビュー（Device View）] で ASA 5505 を選択し、デバイスポリシーセレクタから [インターフェイス（Interfaces）] を選択します。

ASA 5505 スイッチのポートとインターフェイスの設定

スイッチ ポートの設定については、ASA 5505 でのハードウェア ポートの設定 （2429 ページ）を参照してください。

インターフェイスの設定については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）を参照してください。

関連項目

- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）

サブインターフェイスの設定（PIX/ASA）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

サブインターフェイスを使用すると、物理インターフェイスを異なる VLAN ID がタグ付けされた複数の論理インターフェイスに分割できます。VLAN により、特定の物理インターフェイ

ス上でトラフィックを分離しておくことができるため、物理インターフェイスやセキュリティアプライアンスを追加しなくても、ネットワークで使用できるインターフェイスの数を増やすことができます。この機能はマルチ コンテキスト モードで特に役立ち、これにより、各コンテキストに一意のインターフェイスを割り当てることができます。

（注） 物理インターフェイスはタグの付いていないパケットを通過させるため、サブインターフェイスを使用する場合、通常は物理インターフェイスでトラフィックを通過させないようにします。サブインターフェイスでトラフィックを通過させるために、物理インターフェイスはイネーブルにしておく必要がありますが、物理インターフェイスではトラフィックを通過させないように、物理インターフェイスには名前を付けないでください。ただし、物理インターフェイスでタグの付いていないパケットを通過させる場合には、通常のようにインターフェイスに名前を付けることができます

（注） このオプションは PIX 7.0 以降のデバイスと 5505 ASA 以外のデバイスでのみ使用できます。

サブインターフェイスの定義

サブインターフェイスを [Add Interface] または [Edit Interface]（ASA/PIX 7.0 以降）ダイアログボックスで設定するには、次の手順を行います。このダイアログボックスには、デバイスの [Interfaces] ページからアクセスできます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照）。

1. [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、インターフェイスの [タイプ（Type）] として [サブインターフェイス（Subinterface）] を選択します。

[VLAN ID] と [サブインターフェイスID（Subinterface ID）] のフィールドが [ハードウェアポート（Hardware Port）]、[名前（Name）]、[セキュリティレベル（Security Level）] のフィールドの下に表示されます。

1. 以前に定義したインターフェイスポートのリストから、目的の [ハードウェアポート（Hardware Port）] を選択します。目的のインターフェイス ID が表示されない場合は、インターフェイスが定義済みで、イネーブルにされていることを確認してください。
2. [VLAN ID]：このサブインターフェイスの VLAN ID を指定します。1 ～ 4094 の値を入力します。指定した VLAN ID は、どの接続デバイスでも使用されていない必要があります。

一部の VLAN ID は接続されているスイッチで予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。マルチコンテキスト モードでは、VLAN ID はシステム設定でのみ設定できます。

1. [セカンダリ VLAN ID（Secondary VLAN ID）]：このサブインターフェイスのセカンダリ VLAN ID 値を指定します。これにより、ASA は、セカンダリ VLAN 上の ASA に到着する

パケットをプライマリ VLAN にマッピングできます。設定：1 ～ 4090 の値を入力します。セカンダリ VLAN ID は一意である必要があり、VLAN ID と同じであってはなりません。セカンダリ VLAN は、シングルコンテキストのルーテッドモードまたはファイアウォールモードで、または L2 クラスタとして、ASA 9.5.2 以降を実行しているデバイスでサポートされます。

（注） 複数の VLAN ID はスペースまたはコンマで区切って追加できます。56 ～ 78 などの VLAN ID の範囲を指定することもできます。

1. [サブインターフェイスID（Subinterface ID）]：サブインターフェイス ID として 1 ～ 4294967293 の整数を指定します。許可されるサブインターフェイスの番号は、プラットフォームによって異なります。

サブインターフェイスのポート ID の場合、この ID は選択したハードウェア ポートに付加されます。たとえば、*GigabitEthernet0.4* は、GigabitEthernet0 ポートで動作する、4 の ID を割り当てられたサブインターフェイスを示します。

（注） 設定後は ID を変更できません。

1. [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）の説明に従って、このインターフェイスの設定を続けます。

冗長インターフェイスの設定

Security Manager 3.2.2 から、論理的な「冗長」インターフェイスを定義して、セキュリティアプライアンスの信頼性を向上させることができるようになりました。冗長インターフェイスは物理インターフェイスの特定のペアであり、1 つをアクティブ（またはプライマリ）として指定し、もう 1 つをスタンバイ（またはセカンダリ）として指定します。アクティブ インターフェイスで障害が発生すると、スタンバイインターフェイスがアクティブになり、トラフィックの送信を開始します。この機能はデバイスレベルのフェールオーバーとは別のものですが、必要な場合には、フェールオーバーと同様に冗長インターフェイスを設定できます。最大 8 個の冗長インターフェイス ペアを設定できます。

冗長インターフェイスは、常にメンバペアの 1 つだけがアクティブになる単一のインターフェイス（内部、外部など）として機能します。この冗長インターフェイスは、一意のインターフェイス名、セキュリティ レベル、および IP アドレスを使用して通常どおりに設定します。各メンバインターフェイスは同じタイプ（ギガビットイーサネットなど）である必要があり、名前、セキュリティ レベル、または IP アドレスを割り当てられないことに注意してください。実際には、メンバー インターフェイスに対して [Duplex] および [Speed] 以外のオプションを設定しないでください。

冗長インターフェイスは、指定した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバ インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに明示的に MAC アドレスを割り当てることもできます。この場合、メンバインターフェイスの MAC アドレスに関係なく、このアドレスが使用されます。どちらの場合にも、アクティブインターフェイスがスタンバイにフェールオーバーしたときには、トラフィックが中断されないように同じ MAC アドレスが保持されます。

（注） このオプションは PIX 8.0 以降のデバイスと 5505 ASA 以外のデバイスでのみ使用できます。

冗長インターフェイスの定義

2 つの物理インターフェイスを単一の論理的な「冗長インターフェイス」として [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）]（ASA/PIX 7.0 以降）ダイアログボックスで設定するには、次の手順を行います。このダイアログボックスには、デバイスの [インターフェイス（Interfaces）] ページからアクセスできます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照）。

1. [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、インターフェイスの [タイプ（Type）] として [冗長（Redundant）] を選択します。

[Redundant ID]、[Primary Interface]、および [Secondary Interface] オプションが表示されます。

1. この冗長インターフェイスの ID を [冗長ID（Redundant ID）] フィールドに指定します。有効な ID は、1 ～ 8 の整数です。
2. [プライマリインターフェイス（Primary Interface）]：この使用可能なインターフェイスのリストから、冗長インターフェイスペアのプライマリメンバーを選択します。名前付きインターフェイスは冗長インターフェイス ペアでは指定できないため、使用可能なインターフェイスが [Hardware Port ID] に表示されます。
3. [セカンダリインターフェイス（Secondary Interface）]：この使用可能なインターフェイスのリストから、冗長インターフェイスペアのセカンダリメンバーを選択します。名前付きインターフェイスは冗長インターフェイス ペアでは指定できないため、使用可能なインターフェイスが [Hardware Port ID] に表示されます。

（注） メンバ インターフェイスはイネーブルである必要があります。また、メンバ インターフェイスは同じタイプ（GigabitEthernet など）である必要があります。[Name]、[IP Address]、または [Security Level] を割り当てることはできません。実際には、メンバーインターフェイスに対して [Duplex] および [Speed] 以外のオプションを設定しないでください。

1. [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）の説明に従って、このインターフェイスの設定を続けます。

EtherChannel の設定

ASA 8.4.1 から、論理 EtherChannel インターフェイスを定義できるようになりました。ポートチャネル インターフェイスとも呼ばれる EtherChannel は、個別のイーサネット リンクのバンドル（チャネル グループ）で構成される論理インターフェイスです。EtherChannel を使用すると、個別のリンクと比較して帯域幅と耐障害性を強化できます。

EtherChannel インターフェイスは、単一の物理インターフェイスと同様の方法で設定および使用されます。最大 48 個の EtherChannel を設定できます。各 EtherChannel は 1 ～ 8 個のアクティブなファスト イーサネット ポート、ギガビット イーサネット ポート、または Ten-Gigabit イーサネット ポートで構成されます。ASA 9.2(1) では、アクティブインターフェイスの数が 16 に増加しました。

（注） EtherChannel の一部として冗長インターフェイスを使用することはできません。また、冗長インターフェイスの一部として EtherChannel を使用することはできません。冗長インターフェイスと EtherChannel インターフェイスでは同じ物理インターフェイスを使用できません。ただし、冗長インターフェイスと EtherChannel インターフェイスが同じ物理インターフェイスを使用しない場合は、両方のタイプを ASA に設定できます。

EtherChannel MAC アドレス指定

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。これにより、ネットワーク アプリケーションとユーザに対して EtherChannel がトランスペアレントになります。これは、ネットワーク アプリケーションとユーザは 1 つの論理接続のみを認識し、個別のリンクは認識しないためです。デフォルトでは、EtherChannel は最も番号の小さいメンバ インターフェイスの MAC アドレスをその EtherChannel の MAC アドレスとして使用します。

または、ポートチャネル インターフェイスの MAC アドレスを手動で設定することもできます。チャネル インターフェイスのメンバーシップを変更する場合は、MAC アドレスを手動で設定することを推奨します。たとえば、ポートチャネル MAC アドレスを提供するインターフェイスを削除する場合、そのポートチャネルには次に番号の小さいインターフェイスの MAC アドレスが割り当てられるため、トラフィックが分断されます。手動で一意の MAC アドレスを EtherChannel インターフェイスに割り当てることにより、この分断を防止できます（マルチコンテキスト モードでは、EtherChannel インターフェイスを含め、個別のコンテキストに割り当てられているインターフェイスに一意の MAC アドレスを割り当てることができます）。

管理専用 EtherChannel インターフェイスについて

EtherChannel グループは管理専用インターフェイスとして指定できますが、次の点に注意してください。

- ルーテッド モード：EtherChannel を管理専用として明示的に [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）で設定する必要があります。管理専用ポートチャネルに追加された管理用ではないすべてのインターフェイスは、管理ポートとして扱われます。すでに管理専用として定義されているインターフェイスを管理専用グループに追加する場合、物理インターフェイスではその属性は無視されます。同様に、インターフェイスがすでに管理専用ポートチャネルのメンバである場合は、そのインターフェイスを管理専用として指定できません。
- トランスペアレント モード：このモードでは、管理専用 EtherChannel のメンバ自体は管理専用ポートにしかなれません。そのため、管理専用メンバをトランスペアレント モードの EtherChannel に追加する場合、チャネルは管理専用の指定を継承する一方、その指定はメンバ インターフェイスから削除されます。反対に、そのようなインターフェイスが EtherChannel から削除されると、その指定は個別のインターフェイス上で復元されます。

EtherChannel インターフェイスのフェールオーバーリンクとしての使用

EtherChannel インターフェイスがフェールオーバー リンクとして指定されている場合、そのリンクのすべての状態同期トラフィックは単一の物理インターフェイスで送信されます。その物理インターフェイスに障害が発生すると、状態同期トラフィックは EtherChannel 集約リンクに含まれる別の物理インターフェイスを通過します。フェールオーバー用に指定された EtherChannel リンクに使用可能な物理インターフェイスが残っていない場合、冗長インターフェイスが指定されていれば、ASA は冗長インターフェイスに切り替えます。

EtherChannel インターフェイスはアクティブなフェールオーバー リンクとして使用されますが、その EtherChannel 設定を変更することはできません。そのリンクの EtherChannel 設定を変更するには、次のようにして、リンクまたはフェールオーバーのいずれかをディセーブルにする必要があります。

- 設定を変更している間は EtherChannel リンクをディセーブルにし、その後リンクを再アクティブ化します（リンクがディセーブルになっている間はフェールオーバーは発生しません）。
- 設定を変更している間はフェールオーバーをディセーブルにし、その後フェールオーバーをイネーブルにします（その間フェールオーバーは発生しません）。

（注） フェールオーバー リンクとして割り当てられている他のタイプのインターフェイスと同様、EtherChannel インターフェイスに名前を付けることはできません。さらに、EtherChannel のメンバ インターフェイスに名前を付けることもできません。

ASA での EtherChannel の定義

複数の物理インターフェイスを単一の論理 EtherChannel インターフェイスとして ASA の [Add Interface] または [Edit Interface] ダイアログボックスで設定するには、次の手順を行います。このダイアログボックスには、デバイスの [Interfaces] ページからアクセスできます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照）。

ステップ 1 インターフェイスの [タイプ（Type）] として [EtherChannel] を選択します。

[EtherChannel ID] およびインターフェイスの選択オプション（[ロードバランシング（Load Balancing）]、[LACP モード（LACP Mode）]、および [アクティブ物理インターフェイス（Active Physical Interfaces）]）がダイアログボックスの [全般（General）] パネルに表示されます。[最小（Minimum）] と [最大（Maximum）] フィールドが [詳細設定（Advanced）] パネルに表示されます。

ステップ 2 この EtherChannel の ID を [EtherChannel ID] フィールドに指定します。有効な ID は、1 ～ 48 の整数です。この数字は「Port-channel」に追加され、デバイスの [インターフェイス（Interfaces）] ページにあるテーブルの [インターフェイス（Interface）] 列で、EtherChannel を識別します。

ステップ 3 [使用可能なインターフェイス（Available Interfaces）]：この使用可能なインターフェイスのリストで 1 つ以上のインターフェイスを選択して、[>>] ボタンをクリックして右のメンバリストに追加して、このポートチャネルグループのメンバを指定します。

（注） チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

最大 16 個のインターフェイスをチャネル グループに割り当てられます。ASA 9.2(1) 以降の場合、各チャネルグループに、最大 16 個のアクティブインターフェイスを設定できます。8 個のアクティブインターフェイスだけをサポートするスイッチを使用していて、ASA のバージョンが 9.2(1) より前の場合、8 個のインターフェイスのみアクティブにできるため、残りのインターフェイスは、インターフェイス障害発生時のスタンバイリンクとして動作できます。または、[LACP Mode] を [On] に設定すると、スタティックな EtherChannel を作成できます（次に説明されているとおり、[Advanced] パネルで設定）。これにより、グループ内のすべてのインターフェイスでトラフィックを通過させることができます。

（注） この EtherChannel グループにインターフェイスを割り当てたら、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （2346 ページ）の説明に従って、各メンバインターフェイスの [LACP Port] パラメータを編集できます。

ステップ 4 [詳細設定（Advanced）] タブをクリックして、そのパネルを表示します。

ステップ 5 EtherChannel のセクションで、[ロードバランシング（Load Balancing）] オプションを選択します。このオプションの詳細については、EtherChannel のロードバランシングについて （2348 ページ）を参照してください。

ステップ 6 目的の [LACP モード（LACP Mode）] を選択します。デフォルトの [アクティブ（Active）] を選択すると、[アクティブ物理インターフェイス（Active Physical Interfaces）] の [最小（Minimum）] 値と [最大（Maximum）] 値で指定されているとおり、最大 8 個のインターフェイスをアクティブにして、最大 8 個のインターフェイスをスタンバイモードにできます。

[オン（On）] を選択すると、すべてのメンバインターフェイスが「オン」になっているスタティックポートチャネルが作成されます。つまり、トラフィックを通過する最大 16 個のポートを設定できます。この場合、スタンバイポートはありません。このオプションを選択すると、この EtherChannel グループに割り当てられているすべてのインターフェイスの [Mode] は [On] に切り替わります（それぞれの [Mode] が [On] ではない場合）。このモードの詳細については、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （2346 ページ）を参照してください。

ステップ 7 この EtherChannel のアクティブな物理インターフェイスの最小数と最大数を [Minimum] と [Maximum] に指定します。

前述のように、EtherChannel は、9.2(1) より前の ASA デバイスの場合は 1 ～ 8 個のアクティブリンク、ASA 9.2(1) 以降の場合は 1 ～ 16 個のアクティブリンクで構成できます。これらのフィールドを使用して、特定の時点でこのチャネル グループでアクティブにできるインターフェイスの最小値と最大値を指定します。スイッチが 16 個のアクティブインターフェイスをサポートしていない場合、最大数は必ず 8 以下に設定する必要があります。

ステップ 8 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（2380 ページ）の説明に従って、このインターフェイスの設定を続けます。

（注） このデバイスの EtherChannel の [LACP システム優先順位（LACP System Priority）] は、高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）ダイアログボックスで指定します。

EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集

インターフェイスを EtherChannel（ポートチャネル）グループに割り当てたら、ここでの説明に従って、各メンバ インターフェイスの [LACP Port] パラメータを編集できます。

（注） この機能は ASA 8.4.1 以降のデバイスでのみ使用できます。

Link Aggregation Control Protocol（LACP; リンク集約制御プロトコル）は、物理的なファストイーサネット、ギガビットイーサネット、または Ten-Gigabit イーサネットのインターフェイスを集約して 1 つの EtherChannel グループに転送します。また、互換性のあるポートセットが見つかった場合に、リモートパートナーデバイスを現在の情報に更新し、「操作キー」と呼ばれる一意の値をグループに割り当てます。操作キーは自動で割り当てられます。設定することはできません。

注意 EtherChannel がフェールオーバーリンクとして割り当てられている場合、これらの LACP パラメータは使用できません。

LACP システムプライオリティ

各 LACP 対応デバイスには一意のシステム ID があります。この ID は、システムプライオリティ ID とシステムの MAC アドレスの組み合わせによって構成されます。特定の状況では、EtherChannel でリンクされている 2 つのシステムのポート セットに割り当てられている操作キーを変更して、集約を最適化する必要がある場合があります。そのような場合、プライオリティの高いシステムのポートに割り当てられている操作キーの値を動的に変更して、集約を向上させることができます。プライオリティの低いシステムでは、操作キーの値を変更することはできません。システム プライオリティ ID は、高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）の説明に従って、ユーザが設定できます。

LACP ポートパラメータ

ポート ID は、各グループ インターフェイスに割り当てられている一意の数字で指定されます。この ID は設定可能な [Port Priority] の数字と、インターフェイスに割り当てられているポート番号の組み合わせで構成されます。

ポート ID はポート集約のプライオリティを指定します。集約では、システム内で最も集約プライオリティの高いポートからアクティブ ポートとして使われ始め、ポート ID のリストに従って上から順番に使用されていきます。このポート集約プライオリティを使用すると、すべてのリンクで LACP を同時に実行している場合と同様の方法で集約のリンクが選択されるため、集約を予測したり再現したりできるようになります。

さらに、各ポートのプライオリティを設定して、スタンバイ ポートのセットを管理制御できます。たとえば、プライオリティの最も低いポートは、グループの集約で最後に使用されるため、スタンバイ ポートになります（スタンバイ ポートを用意するために十分なメンバがグループに割り当てられていることが前提です）。

関連項目

- EtherChannel の設定 （2343 ページ）

既存の EtherChannel インターフェイスの LACP ポートパラメータの編集

既存の EtherChannel が割り当てられているインターフェイスを編集するには、次の手順を行います。

ステップ 1 デバイスの [インターフェイス（Interfaces）] ページにあるテーブルで、ポートチャネルグループのメンバであるインターフェイスを選択します。（このテーブルのアクセスと使用については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください）。

ステップ 2 [行の編集（Edit Row）] をクリックして、そのインターフェイスで [インターフェイスの編集（Edit Interface）] ダイアログボックスを開きます。

[Enable Interface] チェックボックス、[LACP Port] パラメータ、および [Description] フィールドのみを変更できます。

ステップ 3 必要に応じて、[LACPポート（LACP Port）] パラメータを編集します。

- [優先順位（Priority）]：この数字とインターフェイスに割り当てられているポート番号が組み合わさって、一意のポート ID 番号が生成されます。この値には 1 ～ 65535 を指定できます。数字が大きいほど、プライオリティは低くなります。デフォルトは32768 です。このパラメータは、ポートが [Active] モードまたは [Passive] モードの場合にのみ適用されます。
- [モード（Mode）]：これらの LACP モードの 1 つを選択します。
  - [アクティブ（Active）]：アクティブモードでは、ポートはパートナーデバイスとの LACP の交換を開始して、定期的にパートナーに更新を送信します。アクティブな LACP は、パートナーの制御モードに関係なく、プロトコルに参加するポートの優先度を反映します。
  - [パッシブ（Passive）]：パッシブモードのポートは LACP の交換を開始しませんが、パートナーからの要求を受信すると、ポートはそのパートナーと LACP 情報の交換を開始します。パッシブモードは、リモート ポートが LACP をサポートしているかどうかがわからない場合に便利です。

一部のデバイスは、LACP がイネーブルになっていない場合に定期的な LACP 更新を受信すると、正常に動作しないことがあります。ただし、正常に動作するようにチャネルを設定するには、少なくとも 1 つのポートがアクティブ モードに設定されている必要があります。

- • [オン（On]）：このモードは、すべてのメンバーのインターフェイスがオンになっているスタティックポートチャネルを、スタンバイ ポートなしで設定するために使用します。ネゴシエーションは行われず、他の 2 つのモードに関連するほとんどの制約も適用されません。たとえば、すべてのメンバーポートの速度設定とデュプレックス設定を同じにする必要はありません。また、すべてのメンバーポートはアクティブのままになります。リモート ポートもオンにする必要があります。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

- [VSSまたはvPCスイッチID（VSS or vPC Switch ID）]：インターフェイスが接続されている仮想スイッチングシステム（VSS）または仮想ポート チャネル（vPC）スイッチ ID を識別します。

ステップ 4 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（2380 ページ）の説明に従って、このインターフェイスの編集を続けます。

EtherChannel のロード バランシングについて

EtherChannel のトラフィックは、バンドルされている個別のリンク間で決定論的手法により分散されます。ただし、すべてのリンクで負荷が均等に分配されるわけではありません。代わりに、ハッシュ アルゴリズムの結果として、フレームは特定のリンクに転送されます。このアルゴリズムでは、特定のフィールドまたはフィールドの組み合わせをパケット ヘッダーで使用して、使用するリンクを示す固定の Result Bundle Hash（RBH）値を生成します。

アルゴリズムは、パケット ヘッダー フィールド（送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、宛先 MAC アドレス、TCP/UDP ポート番号、VLAN ID）の 1 つまたはそれらのフィールドの組み合わせを使用して、リンクの割り当てを決定します。このアルゴリズムで使用するフィールドの組み合わせは、[ロードバランシング（Load Balancing）] リストから選択されます（ASA の [インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [詳細設定（Advanced）] タブ）。これらのオプションは、後続の項で説明されています。詳細については、 EtherChannel の設定 （2343 ページ）を参照してください。

たとえば、フィールドに送信元 MAC アドレス（src-mac）を選択した場合、パケットが EtherChannel に転送されると、それらのパケットは各着信パケットの送信元 MAC アドレスに基づいて、チャネル内のポート間で分散されます。そのため、ロード バランシングを行うには、異なるホストからのパケットはチャネル内の異なるポートを使用しますが、同じホストからのパケットはチャネル内の同じポートを使用します（また、デバイスが学習した MAC アドレスは変更されません）。

同様に、宛先 MAC アドレス転送では、パケットが EtherChannel に転送されると、各パケットはパケットの宛先ホスト MAC アドレスに基づいて、チャネル内のポート間で分散されます。したがって、宛先が同じパケットは同じポートに転送され、宛先の異なるパケットはそれぞれ異なるチャネル ポートに転送されます。

そのため、ロード バランシング オプションを選択するときには、柔軟に設定できるオプションを使用します。たとえば、チャネル上のほとんどのトラフィックが 1 つの MAC アドレスにのみ送信される場合、宛先 MAC アドレスを選択すると、ほとんどのトラフィックが常にチャネル内の同じリンクを使用するようになります。別の方法として、送信元アドレスや IP アドレスを使用すると、ロード バランシングが向上する場合があります。また、UDP ポート番号や TCP ポート番号とともに送信元アドレスと宛先アドレスを使用すると、まったく異なる方式でトラフィックを分配できます。

（注） このオプションは ASA 8.4.1 以降のデバイスでのみ使用できます。

ロード バランシング オプション

単一の論理 EtherChannel インターフェイスを ASA の [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで定義する場合、次のいずれかの [ロードバランシング（Load Balancing）] のオプションを選択し（[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （2396 ページ）で設定）、負荷分散の基本を指定します。

- [dst-ip]：宛先ホストの IP アドレスにのみ基づいて負荷分散が行われます。パケットの送信元は考慮されません。同じ宛先 IP アドレスを持つ各パケットは、同じリンクで転送されます。
- [dst-ip-port]：宛先ホストの IP アドレスと TCP/UDP ポートに基づいて負荷分散が行われます。このオプションを使用すると、宛先 IP アドレスだけの場合より、よりきめ細かく多少複雑な負荷分散を実行できます。
- [dst-mac]：着信パケットの宛先ホストの MAC アドレスに基づいて負荷分散が行われます。
- [dst-port]：宛先ポートに基づいて負荷分散が行われます。つまり、物理インターフェイスではなく、TCP ポートまたは UDP ポートに基づいて行われます。
- [src-dst-ip]：送信元 IP アドレスと宛先 IP アドレスに基づいて負荷分散が行われます。ハッシュ計算では、送信元 IP アドレスと宛先 IP アドレスがペアで使用されます。この方式を使用すると、宛先 IP アドレスよりもきめ細かい負荷分散を実行できます。たとえば、同じ宛先へのパケットが異なる IP 送信元から送信されている場合、ポートチャネル内の異なるリンクからそのパケットを転送できます。
- [src-dst-ip-port]：分散の計算では、送信元 IP アドレスと宛先 IP アドレス、および TCP/UDP ポートが考慮されます。さらにきめ細かい負荷分散を実行できます。
- [src-dst-mac]：送信元 MAC アドレスと宛先 MAC アドレスのペアに基づいて計算が行われます。
- [src-dst-port]：送信元と宛先の TCP/UDP ポートに基づいて負荷分散が行われます。
- [src-ip]：送信元のホスト IP アドレスのみに基づきます。
- [src-ip-port]：送信元 IP アドレスおよび TCP/UDP ポート。

- [src-mac]：送信元 MAC アドレスのみ。
- [src-port]：送信元 TCP/UDP ポートのみ。
- [vlan-dst-ip]：宛先 IP アドレスと VLAN ID のペア。
- [vlan-dst-ip-port]：宛先 IP アドレス、TCP/UDP ポート、および VLAN ID の組み合わせ。
- [vlan-only]：VLAN ID のみ。
- [vlan-src-dst-ip]：送信元 IP アドレスと宛先 IP アドレス、および VLAN ID。
- [vlan-src-dst-ip-port]：送信元 IP アドレスと宛先 IP アドレス、TCP/UDP ポート、および VLAN ID。
- [vlan-src-ip]：送信元 IP アドレスと VLAN ID。
- [vlan-src-ip-port]：送信元 IP アドレス、TCP/UDP ポート、および VLAN ID。

VNI インターフェイスの設定

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。

VXLAN を設定するには、最初にVXLAN ポリシーの設定 （2446 ページ）の手順を実行してから VNI インターフェイスを作成し、設定された VXLAN ポリシーを VNI インターフェイスに関連付ける必要があります。

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、オプションとして [全般（General）]、[詳細設定（Advanced）]、[IPv6] の 3 つタブ付きパネルが表示されます。以下の各項では、3 つのタブ付きパネルを使用した VNI インターフェイスの設定方法について説明します。

- VXLAN （2446 ページ）
- VNI インターフェイス：[全般（General）] タブ （2350 ページ）
- VNI インターフェイス：[詳細（Advanced）] タブ （2354 ページ）
- VNI インターフェイス：[IPv6] タブ （2355 ページ）

VNI インターフェイス：[全般（General）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、このダイアログボックスには、[全般（General）]、[詳細設定（Advanced）]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[全般（General）] パネルに表示される各オプションについて説明します。

ナビゲーション パス

[全般（General）] パネルには [インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスからアクセスできます。各ダイアログボックスには、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）の説明に従って、ASA の [インターフェイス（Interfaces）] ページからアクセスできます。

関連項目

- VNI インターフェイスの設定 （2350 ページ）
- VNI インターフェイス：[詳細（Advanced）] タブ （2354 ページ）
- VNI インターフェイス：[IPv6] タブ （2355 ページ）

フィールド リファレンス

表 *551 : [全般（General）] タブ：[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（ASA）*

要素	説明
[Enable Interface]	VNI インターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。
名前	[Interface Name] を入力します。name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。
セキュリティ レベル（Security Level）	[Security Level] に 0（最低）～100（最高）を入力します。
VXLAN	
VNI ID	[VNI ID] は 1 ～ 10000 の間で入力します。この ID は内部インターフェイス識別子です。
VNIセグメントID（VNI Segment ID）	[VNI Segment ID] は 1 ～ 16777215 の間で入力します。セグメント ID は VXLAN タギングに使用されます。
Multicast Group IP Address	（シングル モード）[Multicast Group IP Address] を入力します。 VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

要素	説明
VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）	[NVE Mapped to VTEP Interface] チェック ボックスをオンにします。この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。
IP タイプ（IP Type）	利用可能なオプションから [IPタイプ（IP Type）] を選択します。
スタティック IP（Static IP）	[IPアドレス（IP Address）]：（ルーテッドモード）[IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 [サブネットマスク（Subnet Mask）]：サブネットマスクを指定します。
DHCP を使用する	[DHCP学習済みルートメトリック（DHCP Learned Route Metric）]：（必須）学習したルートにアドミニストレーティブディスタンスを割り当てるには、[DHCP学習済みルートメトリック（DHCP Learned Route Metric）] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブディスタンスは 1 になります。 [DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：（任意）デフォルトのスタティックルートを設定する必要がないようにDHCPサーバーからデフォルトルートを取得するには、このオプションを選択します。 [DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）]：（任意）[DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）] を選択した場合、このオプションを選択し、特定のサービスレベル契約（SLA）モニターによるルートトラッキングを有効にできます。次のオプションが使用可能になります。 [トラッキング済みSLAモニター（Tracked SLA Monitor）]：[DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルートトラッキング（接続性のモニタリング）を定義している SLA モニタ オブジェクトの名前を入力または選択します。
説明	（任意）インターフェイスの説明を指定します。

表 *552 : [*全般（*General*）*]* タブ：*[*インターフェイスの追加/編集（*Add/Edit Interface*）*]* ダイアログボックス（*ASAv*）

要素	説明
[Enable Interface]	VNIインターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。
名前	[Interface Name] を入力します。name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。
セキュリティ レベル（Security Level）	[Security Level] に 0（最低）～100（最高）を入力します。
VXLAN	
Proxy Single-Arm	ASAv デバイスの AWS GWLB をサポートする Proxy Single-Arm を選択します。 **重要** CSM UI で Proxy Single-Arm を表示および設定するには、ハイパーバイザ XENAWS または KVMAWS を備えた ASAv デバイスで AWS を有効にする必要があります。ASAv30 は、Proxy Single-Arm 構成でサポートされる最小のプラットフォームです。
VNI ID	[VNI ID] は 1 ～ 10000 の間で入力します。この ID は内部インターフェイス識別子です。
VNIセグメントID（VNI Segment ID）	[VNI Segment ID] は 1 ～ 16777215 の間で入力します。セグメント ID は VXLAN タギングに使用されます。
Multicast Group IP Address	（シングル モード）[Multicast Group IP Address] を入力します。 VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、マルチコンテキストモードではサポートされていません。
VTEPインターフェイスにマッピングされているNVE（NVE Mapped to VTEP Interface）	[NVE Mapped to VTEP Interface] チェック ボックスをオンにします。この設定により、VNI インターフェイスが VTEP 送信元インターフェイスに関連付けられます。
IP タイプ（IP Type）	利用可能なオプションから [IPタイプ（IP Type）] を選択します。

要素	説明
スタティック IP（Static IP）	[IPアドレス（IP Address）]：（ルーテッドモード）[IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 [サブネットマスク（Subnet Mask）]：サブネットマスクを指定します。

VNI インターフェイス：[詳細（Advanced）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、このダイアログボックスには、[全般（General）]、[詳細（Advanced）]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[詳細（Advanced）] パネルに表示されるこれらのオプションについて説明します。

ナビゲーション パス

[詳細（Advanced）] タブには [インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスからアクセスできます。各ダイアログボックスには、デバイスインターフェイス、ハードウェアポート、ブリッジグループの管理 （2373 ページ）の説明に従って、ASA の [インターフェイス（Interfaces）] ページからアクセスできます。

関連項目

- VNI インターフェイスの設定 （2350 ページ）
- VNI インターフェイス：[全般（General）] タブ （2350 ページ）
- VNI インターフェイス：[IPv6] タブ （2355 ページ）

フィールド リファレンス

表 *553: [詳細（Advanced）] タブ：[インターフェイスの追加（Add Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックス（ASA）*

要素	説明
Active MAC Address	[アクティブMACアドレス（Active MAC Address）] フィールドを使用して、プライベート MAC アドレスをインターフェイスに手動で割り当てます。
Standby MAC Address	[スタンバイ MAC アドレス（Standby MAC Address）] フィールドを使用して、デバイスレベルのフェールオーバーで使用するスタンバイ MAC アドレスを設定できます。

要素	説明
ロール（Roles）	このインターフェイスに割り当てられているすべてのインターフェイス ロールが、このフィールドに一覧表示されます。ロールの割り当ては、このインターフェイスに指定されている名前と、Cisco Security Manager に現在定義されているインターフェイス ロール オブジェクト間のパターン マッチングに基づきます。インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイスの IP アドレスで置き換えられます。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。
DHCP リレーサーバー	IP アドレスを入力するか、またはこのインターフェイスの DHCP 要求をリレーする先のインターフェイス固有の DHCP サーバーを示すネットワーク/ホスト オブジェクトを選択します。複数の値はカンマで区切ります。最大4台のインターフェイス固有の DHCP リレーサーバーと、最大 10 台のグローバルおよびインターフェイス固有の DHCP リレーサーバーを設定できます。
DHCP リレー信頼情報（オプション82）	信頼するこの DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。

VNI インターフェイス：[IPv6] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスの [タイプ（Type）] で [VNIインターフェイス（VNI Interface）] を選択した場合、このダイアログボックスには、[全般（General）]、[詳細設定（Advanced）]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[IPv6] パネルに表示されるこれらのオプションについて説明します。

ナビゲーション パス

IPv6 パネルには [インターフェイスの追加（Add Interface）] と [インターフェイスの編集（Edit Interface）] のダイアログボックスでアクセスできます。これらのダイアログボックスには、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）の説明に従って、ASA の [インターフェイス（Interfaces）] ページからアクセスできます。

関連項目

- VNI インターフェイスの設定 （2350 ページ）
- VNI インターフェイス：[全般（General）] タブ （2350 ページ）
- VNI インターフェイス：[詳細（Advanced）] タブ （2354 ページ）

フィールド リファレンス

表 *554 : [IPv6]* タブ：*[*インターフェイスの追加（*Add Interface*）*]/[*インターフェイスの編集（*Edit Interface*）*]* ダイアログ ボックス（*ASA/FWSM*）

要素	説明
IPv6を有効化（Enable IPv6）	IPv6 をイネーブルにして、このインターフェイスで IPv6 アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると、このインターフェイスで IPv6 をディセーブルにできますが、設定情報は保持されます。
Enforce EUI-64	オンにすると、ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用します。 このオプションがインターフェイスでイネーブルにされると、そのインターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに対して検証され、インターフェイス ID が Modified EUI-64 形式を使用していることが確認されます。IPv6 パケットのインターフェイス ID が Modified EUI-64 形式でない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。 「%PIX|ASA-3-325003: EUI-64 source address check failed.」 アドレス形式の検証は、フローが作成された場合にのみ行われます。既存のフローからのパケットは確認されません。さらに、アドレス検証はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

要素	説明
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに 0 ～ 600 の数を入力します。0 を入力すると、インターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカルアドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバルアドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカルアドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカル アドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

要素	説明
管理対象設定フラグ	IPv6 ルータ アドバタイズメント パケットの「managed-config-flag」フラグを設定するかどうか。
その他の設定フラグ	IPv6 ルータ アドバタイズメント パケットの「other-config-flag」フラグを設定するかどうか。
Enable RA	オンにすると、インターフェイスで IPv6 ルータ アドバタイズメントの送信がイネーブルになります。次のオプションを使用できます。 • [RA Lifetime]：「ルータライフタイム」値は、ローカルリンク上のノードがセキュリティアプライアンスをリンク上のデフォルトルータと見なし続ける期間を指定します。有効な値の範囲は 0 ～ 9000 秒で、デフォルトは 1800 秒です。0 を入力すると、セキュリティ アプライアンスは選択したインターフェイスのデフォルト ルータとは見なされません。 0 以外の任意の値は、次の [RA Interval] 値より小さい値にはできません。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。 • [RA Interval]：このインターフェイスでの IPv6 ルータアドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1800 秒です（次の [RA Interval in Milliseconds] オプションがオンの場合は 500 ～ 1800000 ミリ秒）。デフォルトは 200 秒です。 [RA Lifetime] が 0 以外の場合、送信の間隔は [RA Lifetime] の値以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。 • [RA Interval in Milliseconds]：このオプションをオンにすると、指定した [RA Interval] の値が秒ではなくミリ秒になります。

要素	説明
Interface IPv6 Addresses	ダイアログボックスのこのセクションで、インターフェイスに割り当てられている IPv6 アドレスを指定します。 • [Link-Local Address]：インターフェイスに自動的に生成されたリンクローカルアドレスを上書きするには、このフィールドに目的の IPv6 リンクローカルアドレスを入力します。 リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンクローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラーが表示されます。 • [Enable Address Auto-Configuration]：ステートレス自動設定を使用して、インターフェイスで IPv6 アドレスの自動設定をイネーブルにするには、このオプションをオンにします。アドレスは、Router Advertisement（RA; ルータ アドバタイズメント）メッセージで受信されたプレフィックスに基づいて設定されます。リンクローカルアドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。生成されたリンクローカルアドレスを別のホストが使用している場合は、エラーが発生されます。 • [Trust the DHCP Servers for default gateway]：このラジオボタンを選択して、信頼できる送信元（直接接続されたネットワーク）からのルータアドバタイズメントから、デフォルトのルートをインストールします。 • [Ignore trust and accept router advertisements]：このラジオボタンを選択して、別のネットワークからのルータアドバタイズメントから、デフォルトのルートをインストールします。 • このセクションのテーブルには、このインターフェイスに割り当てられている IPv6 アドレスが表示されます。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Address for Interface] ダイアログボックス （2417 ページ）が開きます。
Interface IPv6 Prefixes	このセクションのテーブルを使用して、IPv6 ルータ アドバタイズメントに含まれる IPv6 プレフィックス（つまり、IPv6 アドレスのネットワーク部分）を設定します。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Prefix Editor] ダイアログボックス （2419 ページ）が開きます。

トンネルインターフェイスの設定

Cisco Security Manager 4.13 は、サイト間 VPN でルートベースの VPN 方式をサポートしています。このサポートには、スタティック クリプト マップ アクセス リストの設定とインターフェイスへのマッピングが必要です。この要件により、大企業および仮想プライベートクラウドは、すべてのリモートサブネットを追跡し、それらをクリプト マップ アクセス リストに含める必要があります。この課題を克服するために、ASA 9.7.1 は、VTI（仮想トンネルインターフェイス）を使用したルートベースの VPN 方式をサポートするよう強化されています。したがって、Cisco Security Manager 4.13 以降では、VPN とそれに関連付けられた IPSec ポリシーのトンネルインターフェイスを定義できます。

VTI は、ハブアンドスポークを使用した通常の IPsec、およびポイントツーポイント VPN トポロジでのみサポートされます。VTI は、フルメッシュトポロジ、エクストラネット VPN トポロジ、および RAVPN ポリシーなどの他のトポロジではサポートされていません。

マルチハブおよびマルチスポークのシナリオでは、トンネルインターフェイスが 1 つのピアから別のピアへの接続を確立するために、インターフェイスロールがハブアンドスポークに適用されていることを確認します。

（注） BGPv6 アドレスは、ASA 9.16(1) 以降のバージョンのデバイスで、ポイントツーポイントおよびハブアンドスポークトポロジのもと、通常の IPSec VTI の IPv6 ファミリでサポートされています。設定した BGPv6 アドレスは、トンネルの IP アドレスと一致する必要があります。一致しない場合、検証エラーがトリガーされます。

（注） [詳細（Advanced ）] タブと [IPv6] タブのオプションは、VTI には適用されません。

ここでは、トンネルインターフェイスの設定方法について説明します。

- [トンネル（Tunnel）] : [全般（General）] タブ （2360 ページ）
- トンネルインターフェイス向け IPSec ポリシーの設定 （2364 ページ）

[トンネル（Tunnel）] : [全般（General）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、[タイプ（Type）] ドロップダウンから [トンネル（Tunnel）] を選択すると、ダイアログボックスに [全般（General）]、[詳細（Advanced）]、および [IPv6] の 3 つのタブが表示されます。ここでは、[全般（General）] パネルに表示されるオプションについて説明します。

ナビゲーション パス

デバイスインターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）で説明されているように、[ASAインターフェイス（ASA Interfaces）] ページから [全般（General）] パネルにアクセスできます。

関連項目

- トンネルインターフェイスの設定 （2360 ページ）
- トンネルインターフェイス向け IPSec ポリシーの設定 （2364 ページ）

フィールド リファレンス

表 *555*：*[*全般（*General*）*]*タブ：*[*インターフェイスの追加/編集（*Add/Edit Interface*）*]*ダイアログボックス（*ASA*）

要素	説明
[Enable Interface]	トンネルインターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。
名前	[Interface Name] を入力します。name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。
トンネル インターフェイス	
Tunnel ID	0 ～ 10413 の範囲で一意のトンネル ID を入力します。この ID は内部インターフェイス識別子です。指定し ID はインターフェイス名にマッピングされます。名前と ID のペアは一意である必要があります。 通常の IPSEC VTI VPN では、このフィールドは必須です。
送信元インターフェイス（Source Interface）	VTI の作成に使用する送信元インターフェイスを入力します。IP アドレスはこのインターフェイスから取得されます。 [選択（Select）] ボタンをクリックして、使用可能なインターフェイスから送信元インターフェイスを選択します。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。 • IPv6：このボックスをオンにして、IPv6 アドレスを入力します。 • 送信元IPv6アドレス：送信元 IPv6 アドレスを入力します。 （注） トンネルの送信元と宛先のペアは一意である必要があります。
宛先 IP/ホスト名	VTI に使用されるトンネルの宛先 IP アドレス。4.14 以降、Cisco Security Manager では、宛先 IP としてホスト名を指定できます。 （注） トンネルの送信元と宛先のペアは一意である必要があります。

要素	説明
IPSec トンネルモードを有効にする	IPv4 または IPv6 トンネル保護モードをパスするには、このボックスをオンにします。 次に、2 つの IPSec トンネルモードを示します。 • IPv4：IPv4 を選択して、トンネル保護モードとして IPv4 をパスします。現在、IPSec のみがサポートされています。IPv4 ネットワークはトンネル内にカプセル化されます。 • IPv6：IPv6 を選択して、トンネル保護モードとして IPv6 をパスします。現在、IPSec のみがサポートされています。IPv6 ネットワークはトンネル内にカプセル化されます。
IPv4 モード	チェックボックスをオンにして、IPv4 をトンネル保護モードとしてパスします。現在、IPSec のみがサポートされています。IPv4 ネットワークはトンネル内にカプセル化されます。
IPSec プロファイル	トンネルインターフェイスに添付される IPSec プロファイルを入力します。 ポリシーオブジェクトが Policy Object Manager で作成されている必要があります。ポリシーオブジェクトの作成については、トンネルインターフェイス向け IPSec ポリシーの設定 （2364 ページ）を参照してください。 （注） ピアに対して異なる IKEV1 トランスフォームセットを持つ IPSec プロファイルを選択すると、Cisco Security Manager はトンネルインターフェイスを作成しますが、2 つのピア間の接続は確立されません。 [IPSecオブジェクトセレクタ（IPSec Object Selector）] ダイアログからプロファイルを選択するには、[選択（Select）] ボタンをクリックします。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。 （注） ポリシーを指定する場合、トンネル名が入力されていることを確認してください。[名前（Name）] フィールドが空白の場合、Cisco Security Manager はエラーメッセージを表示します。

要素	説明
Profile	トンネルインターフェイスに添付されるIPSecプロファイルを入力します。 ポリシーオブジェクトがPolicy Object Managerで作成されている必要があります。ポリシーオブジェクトの作成については、トンネルインターフェイス向け IPSec ポリシーの設定 （2364 ページ）を参照してください。 （注） ピアに対して異なる IKEV1 トランスフォームセットを持つ IPSec プロファイルを選択すると、Cisco Security Manager はトンネルインターフェイスを作成しますが、2 つのピア間の接続は確立されません。 [IPSecオブジェクトセレクタ（IPSec Object Selector）] ダイアログからプロファイルを選択するには、[選択（Select）] ボタンをクリックします。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。 （注） ポリシーを指定する場合、トンネル名が入力されていることを確認してください。[名前（Name）] フィールドが空白の場合、Cisco Security Manager はエラーメッセージを表示します。
IP タイプ（IP Type）	ドロップダウンから、[スタティック IP（ Static IP）] を選択します。 • [IP アドレス（IP Address）] :（ルーテッドモード）[IP アドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 • [サブネットマスク（Subnet Mask）] : サブネットマスクを指定します。
説明	（任意）インターフェイスの説明を指定します。

通常の IPSec VPN トンネルの確立

以下のチェックポイント（トンネルの設定中：トンネルインターフェイスの設定 （2360 ページ））は、通常の IPSec VPN トンネル接続を正常に確立するのに役立ちます。

1. トンネル ID 値を入力する必要があります。
2. 送信元インターフェイスが設定されている必要があり、ISP またはルーティングを介してピアに到達できる必要があります。
3. [宛先IP（Destination IP）] フィールドにピア送信元インターフェイスの IP アドレスを入力する必要があります。
4. [IPSecプロファイル（IPSec Profile）] フィールドの場合：
   1. 両方のピアデバイスに同じ IKEV1 トランスフォームセットを選択します。
   2. ポイントツーポイントトポロジでは、いずれかのピアがレスポンダである必要があります。

3. ハブアンドスポークトポロジでは、ハブをレスポンダとして選択し、すべてのスポークをイニシエータとして選択します。

5. 対象トラフィックを有効にするには、IPV4 モードを設定する必要があります。
6. VPN を確立するには IP アドレスを入力する必要があります。ダイナミック IP アドレスはサポートされていません。
7. 対象トラフィックを有効にするには、スタティックまたは BGP ルーティングを選択します。ファイアウォールポリシーの場合、VTI はスタティックルーティングでのみサポートされます。

（注） ポイントツーポイント トポロジ、および 1 つのハブと 1 つのスポークを持つハブアンドスポークトポロジに対して BGP/スタティックルートが正しく設定されていない場合、Cisco Security Manager からエラーメッセージが表示されます。マルチハブ/スポークシナリオの場合、エラーメッセージは表示されません。

トンネルインターフェイス向け IPSec ポリシーの設定

[IPsecポリシー（IPsec Policy）]ページを使用して、ハブアンドスポークおよびポイントツーポイント VPN トポロジによる通常の IPsec の IKE フェーズ 1 および IKE フェーズ 2 ネゴシエーション中に使用される IPsec ポリシーを設定します。

ポイントツーポイントおよびハブアンドスポークトポロジで、通常の IPSec VTI に対して BGPv6 を有効にできるようになりました。[BGP] ページの [ファミリ（Family）] タブで IPv6 IP アドレスを設定することもできます。

ナビゲーション パス

- [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] を開きます。[すべてのオブジェクトタイプ（All Object Types）] で、[IPSecプロファイル（IPSec Profile）]をクリックします。プロファイルを追加するには、[追加（Add）] ボタンをクリックします。

フィールド リファレンス

表 *556 : IPsec* プロファイル

要素	説明
名前	IPSec ポリシーの名前。
説明	ポリシーの説明。

要素	説明
IKE Version	関連する IKE バージョン（IKEv1 または IKEv2）を選択します。 （注） 4.14 以降、Cisco Security Manager は IKEv2 をサポートしています。ただし、一度に選択できる IKE のバージョンは 1 つだけです。
IKEv1 トランスフォーム セット	トンネルポリシーに使用される IKEv1 トランスフォームセット。トランスフォーム セットは、トンネル内のトラフィックを保護するために使用される認証および暗号化アルゴリズムを指定します。最大 11 個のトランスフォーム セットを選択できます。詳細については、トランスフォーム セットの概要 （1501 ページ）を参照してください。 トランスフォーム セットでは、トンネル モードの IPsec 動作だけを使用できます。 複数の IKEv1 トランスフォームセットを関連付けることができます。選択したトランスフォーム セットの 2 つ以上が両方のピアでサポートされている場合は、最も高いセキュリティを提供するトランスフォームセットが使用されます。 （注） トンネルが機能するには、両方のピアの IKEv1 トランスフォームセットが同じである必要があります。 [選択（Select）] をクリックして、トポロジで使用する IPSec トランスフォーム セット ポリシー オブジェクトを選択します。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。 このフィールドは IKEv2 では使用できません。
[IKEv2 IPSecプロポーザル（IKEv2 IPSec Proposal）]（ASA 9.8(1) 以降）	[選択（Select）] をクリックして、トンネルポリシーに使用する IPSec プロポーザルを選択します。Cisco Security Manager では、複数のプロポーザルを選択できます。必要なオブジェクトがまだ定義されていない場合、選択ダイアログボックスの使用可能なオブジェクトリストの下にある [作成（Create）]（+）ボタンをクリックして、新しいオブジェクトを作成できます。詳細については、IPSec IKEv1 または IKEv2 トランスフォーム セット ポリシー オブジェクトの設定 （1510 ページ）を参照してください。 このフィールドは IKEv1 では使用できません。

要素	説明
[トラストポイント（Trustpoint）]（ASA 9.8(1) 以降）	[選択（Select）] をクリックして、参加している IPSec ネットワークデバイスに証明書を発行する CA サーバーを選択します。このポリシーで設定されたピアは、選択した CA サーバーからデジタル証明書を取得します。指定できるトラストポイントは 1 つのみです。 IKEv1 の場合、認証にトラストポイントが使用されるときに、イニシエータは IPSec プロファイルのトラストポイント設定で指定されたトラストポイントを持っている必要があります。レスポンダの場合、トラストポイントはトンネルグループ CLI で指定する必要があります（非 VTI 設定と同様）。 （注） サイト間 VPN でトラストポイント設定が認証として使用される場合、IKE プロファイルが証明書に含まれている必要があります。トンネルを稼働させるには、VTI VPN のサイト間 VPN マネージャで、IKE プロファイル CLI とトンネルグループ CLI の間におけるアクティビティの検証が必要です。 IKEv2 の場合、認証にトラストポイントが使用されるときに、トラストポイント CLI は、イニシエータとレスポンダ両方のトンネルグループ CLI で指定されます。
[証明書チェーン（Certificate Chain）]（ASA 9.8(1) 以降）	許可のための証明書チェーン送信を有効にするには、このチェックボックスを選択します。 証明書チェーンには、ルート CA 証明書、ID 証明書、およびキー ペアが含まれます。
[レスポンダのみ（Responder Only）]	このポリシーに関連付けられたピアがレスポンダとして機能するように設定するには、このチェックボックスをオンにします。ピアの一方だけがレスポンダのみの設定になっていることを確認します。

要素	説明
Enable Perfect Forward Secrecy (PFS) 係数グループ（Modulus Group）	暗号化された各交換で一意のセッション キーを生成および使用するために、Perfect Forward Secrecy（PFS; 完全転送秘密）の使用をイネーブルにするかどうかを指定します。IPsec ネゴシエーションでは、PFS によって、新しい各暗号キーが以前のいずれのキーとも関連しないことが保証されます。 このオプションを選択する場合は、[係数グループ（Modulus Group）] リストで、PFS セッションキーの生成時に使用する Diffie-Hellman キー導出アルゴリズムも選択します。オプションの説明については、使用する Diffie-Hellman 係数グループの決定 （1485 ページ）を参照してください。 次の係数グループは、IKEv1 ではサポートされていません。IKEv1 ではこれらを選択しないでください。 • group19 • group20 • group21 • group24 • group1 （注） Cisco Security Manager 4.19 以降、DH グループ 1 オプションは、ASA 9.12(1) 以降のデバイスではサポートされません。
[ライフタイム（秒）（Lifetime (Seconds)）] [ライフタイム（KB）（Lifetime (Kilobytes)）]	暗号化 IPsec セキュリティ アソシエーション（SA）のグローバルなライフタイム設定。IPSec ライフタイムは、秒、KB、またはその両方で指定できます。 • [秒（Seconds）]：SA が期限切れになるまでに存続できる秒数。120 ～ 2147483647 秒の範囲内の値を入力します。 • [KB（Kilobytes）]：特定の SA が期限切れになる前にその SA を使用して IPSec ピア間を通過できるトラフィック量（KB 単位）。有効な値は、デバイス タイプに応じて異なります。10 ～ 2147483647 の範囲内の値を入力します。 無制限に許可するには、[無制限のライフタイムを有効にする（KB）（Enable Unlimited Lifetime (Kilobytes)）] チェックボックスをオンにします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可	このオブジェクトのプロパティを個々のデバイスで再定義できるようする場合に選択します。 デバイスのオーバーライドを許可した場合は、[Edit] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[Overrides] フィールドは、このオブジェクトに対するオーバーライドを持つデバイスの数を示します。

（注） DH グループ 2、5、および 24 は、ASA 9.14(1) 以降のデバイスではサポートされません。

VLAN インターフェイスの設定

バージョン 4.20 以降、Cisco Security Manager は、Cisco FPR-1010 適応型セキュリティアプライアンスでの L2 ハードウェアスイッチングをサポートしています。L2 スイッチングのサポートを利用するには、それぞれの VLAN インターフェイスを設定する必要があります。

[VLANインターフェイス（VLAN Interface）] : [全般（General）] タブ

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、[タイプ（Type）] ドロップダウンリストから [VLANインターフェイス（VLAN Interface）] を選択すると、ダイアログボックスに [全般（General）]、[詳細（Advanced）]、[IPv6]、[スイッチポート（Switch Port）]、および [Power over Ethernet] の 5 つのタブが表示されます。

（注） VLAN インターフェイスに [スイッチポート（Switch Port）] と [Power over Ethernet] を設定することはできません。

ナビゲーション パス

デバイスポリシーセレクタから [インターフェイス（Interfaces）] > [インターフェイスの追加（Add Interface）] を選択し、[タイプ（Type）] ドロップダウンリストから [VALNインターフェイス（VLAN Interface）] を選択します。

フィールド リファレンス

表 *557 : [General]* タブ : *[Add Interface]/[Edit Interface]* ダイアログボックス

要素	説明
インターフェイスの有効化	VLAN インターフェイスがまだ有効になっていない場合は、このボックスをオンにして有効にします。

要素	説明
管理専用	[管理専用（Management Only）] 機能を有効にするには、このチェックボックスをオンにします。オンにすると、このデバイスへのトラフィックのみを許可するデバイス管理用にインターフェイスが予約されます。他のインターフェイスおよびデバイスへのパススルートラフィックは拒否されます。
名前	[Interface Name] を入力します。name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。
セキュリティレベル	[Security Level] に 0（最低）～100（最高）を入力します。
L2 VLAN ID	0（最低）～ 4090（最高）の L2 VLAN ID を入力します。これは必須フィールドです。
非転送インターフェイス VLAN ID	0（最低）～ 4090（最高）の非転送インターフェイス VLAN ID を入力します。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] ダイアログボックスから [ルートマップ（Route Map）] を選択します。[フィルタ（Filter）] ドロップダウンリストから適用するフィルタを選択するか、[フィルタの作成（Create Filter）] オプションを使用して新しいフィルタを作成します。
IP タイプ	使用可能な次のオプションから IP タイプを選択します。[スタティックIP（Static IP）]、[DHCPを使用（Use DHCP）]、および [PPPoE（PIXおよびASA 7.2+）（PPPoE (PIX and ASA 7.2+)）]
スタティック IP	[IPアドレス（IP Address）]：（ルーテッドモード）[IPアドレス（IP Address）] 領域で、IPv4 アドレスを設定します。IPv6 を設定するには、[IPv6] タブをクリックします。 [サブネットマスク（Subnet Mask）]：サブネットマスクを指定します。

要素	説明
DHCP を使用する	[DHCP学習済みルートメトリック（DHCP Learned Route Metric）]：（必須）アドミニストレーティブ ディスタンスを学習したルートに割り当てるには、[DHCP学習済みルートメトリック（DHCP Learned Route Metric）] フィールドに 1 ～ 255 の値を入力します。このフィールドを空白のままにすると、既知のルートのアドミニストレーティブ ディスタンスは 1 になります。 [DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：デフォルト スタティック ルートを設定する必要がないように DHCP サーバーからデフォルトルートを取得するには、このオプションを選択します。 [DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）]：（任意）[DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）] を選択した場合、このオプションを選択し、特定のサービスレベル契約（SLA）モニターによるルートトラッキングを有効にできます。次のオプションが使用可能になります。 [トラッキング済みSLAモニター（Tracked SLA Monitor）]：[DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルート トラッキング（接続性のモニタリング）を定義している SLA モニタ オブジェクトの名前を入力または選択します。

要素	説明
PPPoE（PIXおよびASA 7.2+）	

要素	説明
	Point-to-Point Protocol over Ethernet（PPPoE）を有効にして、接続ネットワーク上のPPPoEサーバーからIPアドレスが自動的に割り当てられるようにします。このオプションは、フェールオーバーではサポートされません。[IPタイプ（IP Type）] ドロップダウンから [PPPoE（PIXおよびASA 7.2+）（PPPoE (PIX and ASA 7.2+)）] を選択すると、次のオプションが使用可能になります。 [VPDNグループ名（VPDN Group Name）]（必須）：ネットワーク接続、ネゴシエーション、および認証に使用する認証方式とユーザー名/パスワードが含まれるバーチャル プライベート ダイヤルアップ ネットワーク（VPDN）グループを選択します。詳細については、VPDNグループの管理 （2444ページ）を参照してください。 [IPアドレス（IP Address）]：指定した場合、ネゴシエートされたアドレスではなく、このスタティック IP アドレスが接続および認証に使用されます。 [サブネットマスク（Subnet Mask）]：指定した IP アドレスとともに使用されるサブネットマスク。 [PPPoE学習済みルートメトリック（PPPoE Learned Route Metric）]（必須）：学習したルートにアドミニストレーティブ ディスタンスを割り当てます。有効な値は 1 ～ 255 です。デフォルトは 1 です。 すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブ ディスタンス」とも呼ばれます）同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。 [PPPoEを使用したデフォルトルーティングの取得（Obtain Default Routing Using PPPoE）]：このオプションを選択して、PPPoE サーバーからデフォルトルートを取得します。このオ

要素	説明
	プションを選択すると、PPPoE クライアントが接続をまだ確立していない場合に、デフォルトルートが設定されます。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。 [PPPoE学習ルートのトラッキングの有効化（Enable Tracking for PPPoE Learned Route）]：[PPPoEを使用したデフォルトルーティングの取得（Obtain Default Routing Using PPPoE）] を選択した場合、このオプションを選択して、PPPoE が学習したルートのルートトラッキングを有効化できます。選択すると、次のオプションが使用可能になります。 [デュアルISPインターフェイス（Dual ISP Interface）]：デュアル ISP サポート用のインターフェイスを定義する場合、設定中の接続を示す [プライマリ（Primary）] または [セカンダリ（Secondary）] を選択します。 [トラッキング済みSLAモニター（Tracked SLA Monitor）]：[DHCP学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルート トラッキング（接続性のモニタリング）を定義している SLA モニタ オブジェクトの名前を入力または選択します。
説明	（任意）インターフェイスの説明を指定します。

デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理

[Interfaces] ページには、インターフェイス、サブインターフェイス、冗長インターフェイス、仮想インターフェイス（VLAN）、および EtherChannel インターフェイスが表示されます。また、選択したデバイスに設定されているハードウェア ポートとブリッジ グループが表示され、それらを追加、編集、および削除できます。

使用可能なインターフェイスのタイプは、デバイス タイプ、オペレーティング システムのバージョン、およびモード（ルーテッドまたはトランスペアレント）によって異なります。たとえば、EtherChannel インターフェイスは、ルーテッドとトランスペアレントの両方のモードにあ

る ASA 8.4.1 以降のデバイスでのみ使用できます。詳細については、デバイス インターフェイスについて （2334 ページ）を参照してください。

（注） ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[インターフェイス（Interfaces）] および [ハードウェアポート（Hardware Ports）] の 2 つのタブ付きパネルが表示されます。同様に、トランスペアレントモードで動作している Firewall Services Module（FWSM; ファイアウォール サービス モジュール）バージョン 3.1 以降と ASA バージョン 8.4.1 以降の両方に表示される [インターフェイス（Interfaces）] ページにも、[インターフェイス（Interfaces）] および [ブリッジグループ（Bridge Groups）] の 2 つのタブ付きパネルが表示されます。これらの機能の設定については、次の手順にあるリンクを参照してください。

各セキュリティ デバイスが設定され、各アクティブ インターフェイスがイネーブルになっている必要があります。非アクティブインターフェイスをディセーブルにすることができます。ディセーブルにした場合、インターフェイスでデータの送受信は行われませんが、その設定情報は保持されます。

新しいセキュリティ デバイスをブートストラップした場合、設定機能で設定されるのは、内部インターフェイスに関連付けられたアドレスおよび名前だけです。そのセキュリティ デバイスを通過するトラフィックのアクセス ルールおよび変換ルールを指定する前に、そのデバイス上の残りのインターフェイスを定義する必要があります。

トランスペアレント ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを渡すことができます。ただし、専用の管理インターフェイスがプラットフォームに含まれている場合は、そのインターフェイス（物理インターフェイスまたはサブインターフェイスのいずれか）を、管理トラフィック用の第 3 のインターフェイスとして使用できます。

セキュリティ デバイスのインターフェイスと関連オプションを管理するには、次の手順を行います。選択したデバイスのタイプに応じて、設定されているインターフェイス、サブインターフェイス、冗長インターフェイス、仮想インターフェイス（VLAN）、EtherChannel インターフェイス、ハードウェア ポート、およびブリッジ グループを追加、編集、および削除できます。

ステップ 1 デバイスビューが現在のアプリケーションビューであることを確認します。必要に応じて、ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

（注） デバイス ビューを使用したデバイス ポリシーの設定の詳細については、デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）を参照してください。

ステップ 2 設定するセキュリティ デバイスを選択します。

ステップ 3 デバイスポリシーセレクタで [インターフェイス（Interfaces）] を選択します。

[Interfaces] ページが表示されます。表示される情報およびページは、選択したデバイス タイプおよびバージョン、動作モード（ルーテッドまたはトランスペアレント）、およびデバイスでホストするコンテキスト（シングルコンテキストまたはマルチコンテキスト）によって異なります。

ASA 5505 デバイスの [Interfaces] ページには、[Hardware Ports] および [Interfaces] の 2 つのタブ付きパネルが表示されます。同様に、トランスペアレント モードで動作している FWSM（バージョン 3.1 以降）および ASA（バージョン 8.4.1 以降）の両方に表示される [Interfaces] ページにも、[Interfaces] および [Bridge Groups] の 2 つのタブ付きパネルが表示されます。

ステップ 4 必要に応じて、インターフェイスと関連オプションを追加、編集、および削除します。

[Interfaces] ページまたはパネルと [Bridge Groups] および [Hardware Ports] パネルには、Security Manager の標準のテーブルが表示されます。 テーブルの使用 （64 ページ）で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。

[行の追加（Add Row）] または [行の編集（Edit Row）] ボタンをクリックして表示される実際のダイアログボックスは、選択したデバイス（およびパネル）のタイプによって異なります。デバイス固有のダイアログボックスについては、次のトピックを参照してください。

- [Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3） （2375 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）
- ASA 5505 でのハードウェア ポートの設定 （2429 ページ）
- [Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （2432 ページ）

ステップ 5 同じセキュリティ レベルが設定されているインターフェイス間の通信のイネーブル化などを設定する [Advanced Interface Settings] を管理するには、[Interfaces] ページの下部にある [Add Row] ボタンをクリックして、[Advanced Interface Settings] ダイアログボックスを開きます。詳細については、高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）を参照してください。

ステップ 6 インターフェイスの追加、編集、削除が終わったら、ウィンドウの下部にある [保存（Save）] をクリックして、インターフェイス定義を Cisco Security Manager サーバーに保存します。

[Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

表 *558 : [Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3）*

要素	説明
[Enable Interface]	このインターフェイスでトラフィックを渡せるようにします。セキュリティ ポリシーに応じてトラフィックが通過できるようにするには、この設定に加えて、[IP Type] と [Name] を指定する必要があります。 イネーブルにした任意のサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスをイネーブルにする必要があります。

要素	説明
タイプ（Type）	インターフェイスのタイプを選択します。 • [物理（Physical）]：VLANは、その基礎となるハードウェアインターフェイスと同じネットワーク上にあります。 • [論理（Logical）]：VLANは論理インターフェイスに関連付けられます。
名前	最大48文字のインターフェイス名を指定します。[Name]には、インターフェイスの用途に関係する覚えやすい名前を付けます。サポートされるインターフェイス名は、次のとおりです。 • [Inside]：内部ネットワークに接続します。最もセキュアなインターフェイスにする必要があります。 • [DMZ]：非武装地帯（中間インターフェイス）。境界ネットワークとも呼ばれます。 • [Outside]：外部ネットワークまたはインターネットに接続します。セキュア度の最も低いインターフェイスにする必要があります。
Hardware Port	物理ネットワーク インターフェイスを定義する場合、この値は、デバイスでのインターフェイス タイプとそのスロットまたはポートを識別する名前を表します。 論理ネットワーク インターフェイスを追加する場合、論理インターフェイスを追加する、イネーブル化された任意の物理インターフェイスを選択できます。目的のハードウェア ポートが表示されない場合は、インターフェイスがイネーブルであることを確認してください。 有効な値は次のとおりです。 • ethernet0 ～ ethernet*n*。 • gb-ethernet*n* 。 *n* は、デバイスでのネットワーク インターフェイスの番号を表します。
IP タイプ（IP Type）	[IPタイプ（IP Type）] では、インターフェイスに使用する IP アドレス指定のタイプを定義します。[スタティックiP（Static IP）] または [DHCPの使用（Use DHCP）] を選択します（デバイス インターフェイス：IP タイプ（PIX 6.3）（2378 ページ）を参照）。（PPPoE オプションは PIX 6.3 デバイスには適用できません）。 （注） DHCP は、セキュリティアプライアンスの外部インターフェイスにのみ設定できます。

要素	説明
Speed and Duplex	物理インターフェイスの速度オプションが表示されます。論理インターフェイスには適用されません。次のいずれかのオプションを選択します。 • [auto]：イーサネットの速度を自動的に設定します。[auto] キーワードは、Intel 10/100 自動速度検出ネットワーク インターフェイス カードでのみ使用できます。 • [10baset]：10 Mbps イーサネット半二重。 • [10full]：10 Mbps イーサネット全二重。 • [100basetx]：100 Mbps イーサネット半二重。 • [100full]：100-Mbps イーサネット全二重。 • [1000auto]：1000 Mbps イーサネット（全二重または半二重をオートネゴシエーション）。 ヒント　ネットワーク内のスイッチなどのデバイスとの互換性を維持するために、このオプションを使用しないことを推奨します。 • [1000full]：オートネゴシエーション、アドバタイジング 1000 Mbps イーサネット全二重。 • [1000full nonnegotiate]：1000 Mbps イーサネット全二重。 • [aui]：AUI ケーブルインターフェイスとの 10 Mbps イーサネット半二重通信。 • [bnc]：BNC ケーブルインターフェイスとの 10 Mbps イーサネット半二重通信。 （注）　自動検知を正しく処理しないスイッチなどのデバイスがネットワーク環境に含まれている場合に、ネットワーク インターフェイスの速度を指定することを推奨します。
MTU	最大パケット サイズ、つまり最大伝送単位（MTU）をバイト数で指定します。この値は、インターフェイスに接続されているネットワークのタイプによって異なります。有効な値は 300 ～ 65535 バイトです。デフォルトは 1500 です。
Physical VLAN ID	物理インターフェイスでは、VLAN ID を 1 ～ 4094 の範囲で入力します。この VLAN ID は、接続されているデバイスで使用中であってはなりません。
Logical VLAN ID	この論理インターフェイスに関連付けられた VLAN のエイリアスを 1 ～ 4094 の値で指定します。この値は、論理インターフェイスのタイプが選択されている場合に必要です。

要素	説明
セキュリティ レベル（Security Level）	インターフェイスのセキュリティ レベルを指定します。0（最もセキュア度の低い）～ 100（最もセキュア度の高い）の値を入力します。セキュリティ アプライアンスにより、トラフィックは、内部ネットワークから外部ネットワーク（セキュリティ レベルがより低い）まで自由に通過できます。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。 • 外部インターフェイスは、常に 0 です。 • 内部インターフェイスは、常に 100 です。 • DMZ インターフェイスの値の範囲は 1 ～ 99 です。
ロール（Roles）	ロールの詳細とその定義方法および使用方法については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。 このインターフェイスに割り当てられているすべてのインターフェイス ロールが、このフィールドに一覧表示されます。ロールの割り当ては、このインターフェイスに指定されている名前と、Cisco Security Manager に現在定義されているインターフェイス ロール オブジェクト間のパターン マッチングに基づきます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイスの IP アドレスで置き換えられます。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 ロールの詳細とその定義方法および使用方法については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

デバイス インターフェイス：IP タイプ（PIX 6.3）

PIX 6.3 のセキュリティ デバイスには、そのインターフェイスの IP アドレス指定が必要です。ただし、ファイアウォール インターフェイスには、割り当てられるまで IP アドレスがありません。

PIX 6.3 セキュリティ デバイスで表示される [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスには、[IPタイプ（IP Type）] セクションがあります。次の説明に従って、インターフェイスの IP アドレス指定のタイプをここに指定して、関連するパラメータを入力します。ダイアログボックスの他のセクションについては、[Add Interface]/[Edit Interface] ダイアログボックス（PIX 6.3） （2375 ページ）を参照してください。

（注） その他のセキュリティ アプライアンス用に表示される [IP Type] オプションについては、デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降） （2424 ページ）を参照してください。

[インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、次のように、[IPタイプ（IP Type）] リストからアドレス割り当て方式を選択し、関連パラメータを指定します。

- [スタティック IP（Static IP）]：このインターフェイスが接続するネットワーク上のセキュリティデバイスを示すスタティック IP アドレスおよびサブネットマスクを指定します。IP アドレスは、インターフェイスごとに一意でなければなりません。

サブネット マスクは、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。バージョン 4.13 以降、Cisco Security Manager では、ポイント ツー ポイント インターフェイスに 255.255.255.254 を使用できます。ネットワークに接続するインターフェイスには 255.255.255.255 を使用しないでください。使用すると、トラフィックがこのインターフェイスで停止します。サブネット マスク値を指定しない場合は、次に示すように「クラスフル」ネットワークが使用されます。

- - IP アドレスの最初のオクテットが 1 ～ 126 の場合（つまり、アドレスが 1.0.0.0 ～ 126.255.255.255 の場合）、クラス A ネットマスク（255.0.0.0）が使用されます。
  - IP アドレスの最初のオクテットが 128 ～ 191 の場合（つまり、アドレスが 128.0.0.0 ～ 191.255.255.255 の場合）、クラス B ネットマスク（255.255.0.0）が使用されます。
  - IP アドレスの最初のオクテットが 192 ～ 223 の場合（つまり、アドレスが 192.0.0.0 ～ 223.255.255.255 の場合）、クラス C ネットマスク（255.255.255.0）が使用されます。

（注） グローバル プールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。

- [Use DHCP]：Dynamic Host Configuration Protocol（DHCP）をイネーブルにして、接続ネットワーク上の DHCP サーバから IP アドレスが自動的に割り当てられるようにします。次のオプションを使用できます。
  - [DHCPを使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：デフォルトのスタティックルートを設定する必要がないように DHCP サーバーからデフォルトルートを取得するには、このチェックボックスをオンにします。
  - [再試行回数（Retry Count）]：PIX が DHCP 要求を再送信する回数。有効な値は 4 ～ 16 です。デフォルトは 2 です。
- [PPPoE（PIX および ASA 7.2 以降）（PPPoE (PIX and ASA 7.2+)）]：このオプションは PIX 6.3 デバイスには適用されません。

（注） DHCP は、ファイアウォール デバイスの外部インターフェイスにのみ設定できます。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

これらの [インターフェイスの追加（Add Interface）] と [インターフェイスの編集（Edit Interface）] ダイアログボックスは、PIX 7.0 以降、ASA、FPR、および FWSM デバイスでインターフェイス、サブインターフェイス、冗長インターフェイス、および EtherChannel インターフェイスを定義および設定するために使用します。[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください。

（注） バージョン 4.24 以降、Cisco Security Manager は、ASA 9.17(1) 以降のデバイスの FPR-3100 シリーズのデバイスをサポートします。

（注） スイッチ機能とセキュリティ アプライアンス機能を組み合わせた ASA 5505 は、物理スイッチ ポートと論理 VLAN インターフェイスの両方を設定する特殊な事例です。したがって、ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[ハードウェアポート（Hardware Ports）] および [インターフェイス（Interfaces）] の 2 つのタブ付きパネルが表示されます。詳細については、ASA 5505 のポートおよびインターフェイスについて （2338 ページ）を参照してください。トランスペアレントモードで動作している ASA 8.4.1 以降および FWSM 3.1 以降のデバイスにも、[インターフェイス（Interfaces）] および [ブリッジグループ（Bridge Groups）] の 2 つのタブ付きパネルが表示されます。ブリッジ グループの設定については、[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （2432 ページ）を参照してください。

これらのダイアログボックスに表示されるパラメータの多くは、デバイス タイプとバージョン、動作モード（ルーテッドまたはトランスペアレント）、およびデバイスでホストするコンテキスト（シングルコンテキストまたはマルチコンテキスト）によって異なります。

（注） フェールオーバーにインターフェイスを使用する場合は、[インターフェイスの追加（Add Interface）] ダイアログボックスでそのインターフェイスを定義できますが、ここでは設定せずに、代わりに [フェールオーバー（Failover）] ページを使用してください。特に、インターフェイス名は指定しないでください。このパラメータを指定すると、インターフェイスをフェールオーバー リンクとして使用できなくなります。

[Add Interface] と [Edit Interface] ダイアログボックスの使用

次の手順では、これらのダイアログボックスの一般的な使用方法を説明します。

1. [Add Interface] と [Edit Interface] ダイアログボックスの上部に、インターフェイスの [Type] ドロップダウン リストが表示されます

（注） Catalyst 6500 サービスモジュール（ASA-SM および FWSM）および ASA 5505 では、[タイプ（Type）] リストは表示されません。

デバイスタイプ、オペレーティングシステムのバージョン、動作モード（ルータまたはトランスペアレント）に応じて、[タイプ（Type）] には次のうちの 2 ～ 3 個のオプション、またはすべてのオプションが表示されます。

- • [物理インターフェイス（Physical Interface）]：デバイスに物理インターフェイスを設定するには、このオプションを選択します。
  - [サブインターフェイス（Sub-Interface）]：以前に定義した物理インターフェイスに関連付けられる論理インターフェイス（またはVLAN接続）を設定するには、このオプションを選択します。詳細については、サブインターフェイスの設定（PIX/ASA）（2339 ページ）を参照してください。
  - [冗長（Redundant）]：2 つの物理インターフェイスを単一の論理的な「冗長インターフェイス」として設定するには、このオプションを選択します。詳細については、冗長インターフェイスの設定 （2341 ページ）を参照してください。
  - [EtherChannel]：最大 8 つの個別のイーサネットリンクのバンドルで構成されている論理インターフェイスを設定するには、このオプションを選択します。このバンドルは EtherChannel またはポートチャネルインターフェイスと呼ばれます（このオプションは ASA 8.4 以降のデバイスでのみ使用できます）。詳細については、EtherChannel の設定 （2343 ページ）を参照してください。
  - [VNIインターフェイス（VNI Interface）]：VNI インターフェイスを設定するには、このオプションを選択します。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。各VNIインターフェイスにセキュリティ ポリシーを直接適用します。すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられま

す。詳細については、VNIインターフェイスの設定 （2350ページ）を参照してください。

- [トンネル（Tunnel）]：このオプションを選択して論理インターフェイス（VTI）を構成し、サイト間 VPN トポロジのルートベースの VPN 方式をサポートします。詳細については、 トンネルインターフェイスの設定 （2360 ページ）を参照してください。

- [Type] オプションの下部のダイアログボックスには、最大 3 つのタブ付きパネルが表示されます。このパネルもデバイス タイプ、オペレーティング システムのバージョン、および動作モードによって異なります。

PIX 7.0 以降の [Add Interface] と [Edit Interface] ダイアログボックスには、[General] と [Advanced] の 2 つのタブ付きパネルが表示されます。ASA 7.0 以降の [Add Interface] と [Edit Interface] ダイアログボックスには、[General]、[Advanced]、[IPv6] の 3 つのタブ付きパネルが表示されます。

FPR-3100 の [インターフェイスの追加（Add Interface）] と [インターフェイスの編集（Edit Interface）] ダイアログボックスには、[一般（General）]、[詳細（Advanced）]、[IPv6] の 3 つのタブ付きパネルが表示されます。

- - [General] オプションを必要に応じて設定します。このパネルについては、 [Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（2382 ページ）を参照してください。

  - [Advanced] パネル オプションを必要に応じて設定します。このパネルについては、[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （2396 ページ）を参照してください。

  - [IPv6] オプションを必要に応じて設定します。このパネルについては、IPv6インターフェイスの設定（ASA/FWSM） （2409 ページ）を参照してください。

  - 必要に応じて、[スイッチ ポート（Switch Port）] のオプションを設定します。このオプションの詳細については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[スイッチポート（Switch Port）] タブ （2428 ページ）を参照してください。

  - 必要に応じて [Power Over Ethernet] のオプションを設定します。このオプションの詳細については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[Power Over Ethernet] タブ （2429 ページ）を参照してください。

- このインターフェイスの設定が終了したら、[OK] をクリックしてダイアログボックスを閉じ、デバイスの [インターフェイス（Interfaces）] ページに戻ります。

[Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380ページ）は、ファイアウォールデバイスでインターフェイス、サブインターフェイス、VLANインターフェイス、冗長インターフェイスおよびEtherChannelインターフェイスを定義および設定するために使用します。[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。詳細については、 デバイス

インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください。

（注） 以下の説明では、「インターフェイス」という用語はインターフェイスのタイプを表す一般的な用語として使用されます。

このダイアログボックスの [General] パネルは、[Name]、[Security Level]、[IP Type] パラメータなどの一般的なインターフェイスの値を設定するために使用します。このパネルに表示されるパラメータの多くは、デバイスタイプとバージョン、動作モード（ルーテッドまたはトランスペアレント）、およびデバイスでホストするコンテキスト（シングルコンテキストまたはマルチコンテキスト）によって異なります。そのため、次の表のオプションによっては、設定しているデバイスに表示されないものもあります。

関連項目

- サブインターフェイスの設定（PIX/ASA） （2339 ページ）
- 冗長インターフェイスの設定 （2341 ページ）
- EtherChannel の設定 （2343 ページ）
- [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）（2396 ページ）
- IPv6 インターフェイスの設定（ASA/FWSM） （2409 ページ）
- ASA 5505 のポートおよびインターフェイスについて （2338 ページ）
- ASA 5505 でのハードウェア ポートの設定 （2429 ページ）

表 *559 : [General]* タブ：*[Add Interface]/[Edit Interface]* ダイアログボックス

要素	説明
[Enable Interface]	このインターフェイスでトラフィックを渡せるようにします。 デフォルトでは、すべての物理インターフェイスがシャットダウンされています。インターフェイスがイネーブルでない場合、トラフィックはあらゆるタイプのインターフェイスを通過できません。サブインターフェイスなどの論理インターフェイスを定義する場合は、サブインターフェイスを定義する前に、関連付ける物理インターフェイスをイネーブルにします。冗長インターフェイスまたは EtherChannel インターフェイスを定義する場合は、グループインターフェイスを定義する前に、メンバインターフェイスをイネーブルにします。 このオプションをオンにする場合、セキュリティ ポリシーに従ってトラフィックが通過できるようにするためには [Name] も指定し、ルーテッドモードでは [IP Type] も指定します（または FWSM または ASA-SM では [IP Address] および [Subnet Mask] を指定します）。 マルチコンテキスト モードでは、物理インターフェイスまたは論理インターフェイスを 1 つのコンテキストに割り当てると、そのコンテキスト内のインターフェイスがデフォルトではイネーブルになります。ただし、トラフィックがコンテキストインターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスはそのインターフェイスを共有しているすべてのコンテキストでシャットダウンされます。
Management Only	このインターフェイスをデバイス管理用に予約します。このデバイスの管理用トラフィックだけが受け入れられます。他のインターフェイスおよびデバイスのパススルー トラフィックは拒否されます。 プライマリまたはセカンダリの ISP インターフェイスは管理専用に設定できません。 管理専用 EtherChannel インターフェイスの定義には、特定のメンバ インターフェイスの制限があります。詳細については、EtherChannel の設定（2343 ページ）を参照してください。 （注） これは、トランスペアレントモードのデバイスでは使用できません。インターフェイスが [管理専用（Management Only）] として割り当てられている場合、[ルートマップ（Route Map）] をそのインターフェイスに割り当てることはできません。つまり、インターフェイスには [管理専用（Management Only）] または [ルートマップ（Route Map）] のいずれかのみ割り当てることができます。

要素	説明
インターフェイス	

要素	説明
	ASA 5505 では、[Hardware Port] は [Hardware Ports] パネルで指定します（ASA 5505 でのハードウェア ポートの設定 （2429 ページ）を参照）。また、このオプションは、Catalyst 6500 サービス モジュール（ASA-SM と FWSM）設定の一部ではありません。 物理インターフェイスの場合、ネットワークタイプ、スロット、およびポート番号を含む物理ポート ID を type[slot/]port の形式で入力して、インターフェイスに割り当てる固有のハードウェアポートを指定します。これは、サブインターフェイスをインターフェイスに関連付ける名前でもあります。 物理インターフェイスのネットワーク タイプには、Ethernet または GigabitEthernet のいずれかを指定できます。ASA 5580 の場合は、TenGigabitEthernet も使用できます。このフィールドでは自動パターンマッチングが行われます。たとえば、e という文字を最初に入力すると、「Ethernet」がこのフィールドに挿入されます。同様に、g という文字を入力すると、「GigabitEthernet」が挿入されます。したがって、有効な値は次のとおりです。 • Ethernet0 ～ Ethernetn • GigabitEthernet0 ～ GigabitEthernetn • GigabitEthernets /n • TenGigabitEthernets/n（ASA 5580 のみ） s はスロット番号、n はポート番号を表し、スロットまたはデバイスのネットワークポートの最大数が上限です。 ASA 5500 シリーズ アプライアンスの場合は、タイプとスロット/ポートのペアを入力します（gigabitethernet0/1 など）。シャーシに組み込まれているポートはスロット 0 に割り当てられ、4-Port Gigabit Ethernet Security Services Module（4 GE SSM; 4 ポート ギガビット イーサネット セキュリティ サービス モジュール）のポートはスロット 1 に割り当てられます。スロットとポートのペアを入力すると、[Media Type] オプションがイネーブルになります。 ASA 5500 シリーズ アプライアンスには、**管理**インターフェイスタイプも含まれています。管理インターフェイスは、デバイス管理トラフィック専用のファスト イーサネット インターフェイスであり、management0/0 のように指定します。ただし、必要な場合には、この物理インターフェイスを通過トラフィックに使用できます（[Management Only] オプションは選択しないでください）。そのため、トランスペアレント ファイアウォール モードでは、通過トラフィックに使用できる 2 つのインターフェイスに加えて、管理インターフェイスも使用できます。また、管理インターフェイスにサブインターフェイスを追加して、マルチ コンテキスト モードの各セキュリティ コンテキストにおける管理を提供することもできます。

要素	説明
	サブインターフェイスを定義する場合は、定義済みのポートのリストから簡単に目的のハードウェア ポートを選択できます（VLAN ID も指定する必要があります）。目的のインターフェイス ID が表示されない場合は、インターフェイスが定義済みで、イネーブルにされていることを確認してください。
名前	このインターフェイスに最大 48 文字の ID を指定します。名前には、インターフェイスの用途に関係する覚えやすい名前を付けます。ただし、フェールオーバーを使用している場合は、フェールオーバー通信用に予約しているインターフェイスに名前を付けないでください。これには、フェールオーバー用に使用する EtherChannel およびそのメンバ インターフェイスも含まれます。また、冗長インターフェイス ペアのメンバとして使用するインターフェイスに名前を付けないでください。 セキュリティ アプライアンスのインターフェイス命名ルールに従って、いくつかの名前が特定のインターフェイス用に予約されています。そのため、これらの予約名を使用すると、次のように、デフォルトの予約済みセキュリティ レベルが適用されます。 • [Inside]：内部ネットワークに接続します。最もセキュアなインターフェイスにする必要があります。 • [DMZ]：中間インターフェイスに接続された「緩衝地帯」。DMZ は境界ネットワークとも呼ばれます。DMZ インターフェイスに任意の名前を付けることができます。一般的に、DMZ インターフェイスには、インターフェイスタイプを識別するために「DMZ」というプレフィックスを付けます。 • [Outside]：外部ネットワークまたはインターネットに接続します。セキュア度の最も低いインターフェイスにする必要があります。 同様に、一般的にサブインターフェイス名には、一意の ID に加えて、関連付けられているインターフェイスも示されます。たとえば、DMZoobmgmt で、DMZ インターフェイスに接続されているアウトオブバンド管理ネットワークを示すことができます。 （注） この場合でも、**インターフェイスをフェールオーバー用または冗長インターフェイスのメンバーとして使用する場合は、そのインターフェイスの名前を付けないでください**。詳細については、冗長インターフェイスの設定 （2341 ページ）を参照してください。

要素	説明
セキュリティ レベル（Security Level）	インターフェイスのセキュリティ レベルを指定します。0（最もセキュア度の低い）～ 100（最もセキュア度の高い）の値を入力します。セキュリティ アプライアンスにより、トラフィックは、内部ネットワークから外部ネットワーク（セキュリティ レベルがより低い）まで自由に通過できます。他の多くのセキュリティ機能が、2 つのインターフェイスの相対的なセキュリティ レベルによる影響を受けます。 • 外部インターフェイスは、常に 0 です。 • 内部インターフェイスは、常に 100 です。 • DMZ インターフェイスの値の範囲は 1 ～ 99 です。
メディア タイプ（Media Type）	[Interface] が [Type] で選択されているタイプである場合に、[Hardware Port] フィールドにハードウェア ポート ID とスロット番号またはポート番号を入力すると、これらのオプションがイネーブルになります（これらのオプションはASAのスロットまたはポートのインターフェイスにのみ適用されます）。 ASA 5505 を除くすべての 5500 シリーズのアプライアンスでは、シャーシに組み込まれているポートはスロット 0 に割り当てられ、4GE SSM のポートはスロット 1 に割り当てられます。デフォルトでは、ASA で使用されるコネクタはすべて RJ-45 コネクタです。ただし、4GE SSM のポートには、ファイバ SFP コネクタを含めることができます。これらのファイバベースの接続のインターフェイス設定の一環として、[Media Type] の設定をデフォルト（RJ45）からファイバコネクタ設定（SFP）に変更する必要があります。 ファイバベースのインターフェイスではデュプレックス設定はサポートされず、また固定速度もありません。そのため、[Duplex] オプションはディセーブルになり、[Speed] オプションは [auto] および [nonegotiate] のみを選択できます。 このスロット 1 インターフェイスで使用するコネクタ タイプを選択します。 • [RJ45]：ポートは RJ-45（銅線）コネクタを使用します。 • [SFP]：ポートはファイバ SFP コネクタを使用します。10 ギガビット イーサネット カードの場合に必要です。

要素	説明
VLAN ID（Admin. VLAN ID）	インターフェイスの [タイプ（Type）] として [サブインターフェイス（Subinterface）] を選択した場合や、トランスペアレントモードで動作しているデバイス、ASA 5505、または Catalyst 6500 サービスモジュール上で論理インターフェイスを定義している場合は、このインターフェイスの VLAN ID を指定します。 7.2(2)18 以前のオペレーティング システムを PIX/ASA デバイスで実行している場合、有効な VLAN ID は 1 ～ 1001 です。バージョン 7.2(2)19 以降での有効な ID は 1 ～ 4090 です。Catalyst 6500 サービス モジュールでは、有効な ID は 1 ～ 4096 です。指定した VLAN ID は、どの接続デバイスでも使用されていない必要があります。 一部の VLAN ID は接続されているスイッチで予約されている場合があります。詳細については、スイッチのマニュアルを確認してください。マルチコンテキストモードでは、VLAN ID はシステム設定でのみ設定できます。 詳細については、サブインターフェイスの設定（PIX/ASA）（2339ページ）を参照してください。
Subinterface ID	インターフェイスの [Type] として [Subinterface] を選択した場合や、トランスペアレントモードで動作しているデバイス上でインターフェイスを定義している場合、サブインターフェイス ID として 1 ～ 4294967293 の整数を指定します。 サブインターフェイスのポート ID の場合、この ID は選択したハードウェア ポートに付加されます。たとえば、*GigabitEthernet0.4* は、GigabitEthernet0 ポートで動作する、4 の ID を割り当てられたサブインターフェイスを示します。 （注） 設定後は ID を変更できません。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] ダイアログボックスから [ルートマップ（Route Map）] を選択します。 （注） VNI インターフェイスを除き、他のすべてのインターフェイスタイプでは、ソフトウェアバージョン 9.4(1) 以降を実行している ASA デバイスのポリシーベースルーティングがサポートされています。VNI インターフェイスでは、ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスのポリシーベースルーティングがサポートされています。

要素	説明
IP タイプ（IP Type）	**PIX 7.0 以降と ASA（トランスペアレント モードの 5505 を除く）のみ。** [IPタイプ（IP Type）] では、インターフェイスに使用する IP アドレス指定のタイプを定義します。[スタティックiP（Static IP）]、[DHCPの使用（Use DHCP）]、または [PPPoE] を選択します（デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降） （2424 ページ）を参照）。 （注） DHCP および PPPoE は、セキュリティ アプライアンスの外部インターフェイスにかぎり設定できます。

要素	説明
IPアドレス サブネットマスク	**ルーテッドモードの Catalyst 6500 サービスモジュール（ASA-SM および FWSM）のみ。** これらの 2 つのフィールドを使用して、IP アドレスとサブネット マスクを VLAN インターフェイスに割り当てます。IP アドレスは、インターフェイスごとに一意でなければなりません。 サブネット マスクは、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。 バージョン 4.12、255.255.255.254 および 255.255.255.255 までは、ネットワークに接続するインターフェイスに使用しないでください。使用すると、トラフィックがインターフェイス上で停止します。 バージョン 4.13 以降、/31 サブネットマスク（または 2555.2555.255.254）は、ネットワークに接続されたポイントツーポイント インターフェイスでサポートされています。Cisco Security Manager では、インターフェイス レコードの保存時に警告メッセージが表示されます。 サブネット マスク値を指定しない場合は、次に示すように「クラスフル」ネットワークが使用されます。 • IP アドレスの最初のオクテットが 1 ～ 126 の場合（つまり、アドレスが 1.0.0.0 ～ 126.255.255.255 の場合）、クラス A ネットマスク（255.0.0.0）が使用されます。 • サブネットマスク IP アドレスの最初のオクテットが 128 ～ 191 の場合（つまり、アドレスが 128.0.0.0 ～ 191.255.255.255 の場合）、クラス B ネットマスク（255.255.0.0）が使用されます。 • IP アドレスの最初のオクテットが 192 ～ 223 の場合（つまり、アドレスが 192.0.0.0 ～ 223.255.255.255 の場合）、クラス C ネットマスク（255.255.255.0）が使用されます。 （注） グローバル プールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォールデバイス コマンドに使用したアドレスは使用しないでください。

要素	説明
説明	復帰を使用しないで 1 行に最大 240 文字の任意の説明を入力できます。マルチコンテキスト モードでは、システムの説明とコンテキストの説明に関係はありません。 フェールオーバーまたはステートリンクの場合、説明は「LAN Failover Interface」、「STATE Failover Interface」、または「LAN/STATE Failover Interface」などに固定されます。この説明は編集できません。このインターフェイスをフェールオーバーまたはステートリンクにした場合、ここで入力したすべての説明が、この固定の説明で上書きされます。
冗長インターフェイス。以下のオプションは、ASA 5505 デバイス上または Catalyst 6500 サービス モジュール（ASA-SM と FWSM）上では使用できません。	
Redundant ID	インターフェイスの [Type] に [Redundant Interface] が選択されている場合、この冗長インターフェイスの ID を指定します。有効な ID は 1 ～ 8 の整数です。 詳細については、冗長インターフェイスの設定 （2341 ページ）を参照してください。
プライマリ インターフェイス（Primary Interface） Secondary Interface	インターフェイスの [Type] に [Redundant Interface] が選択されている場合、使用可能なインターフェイスの [Primary Interface] リストから、冗長インターフェイス ペアのプライマリ メンバを選択します。名前付きインターフェイスは冗長インターフェイス ペアでは指定できないため、使用可能なインターフェイスが [Hardware Port ID] に表示されます。 同様に、使用可能なインターフェイスの [Secondary Interface] リストから、冗長インターフェイス ペアのセカンダリ メンバを選択します。 （注） メンバインターフェイスはイネーブルである必要があります。また、メンバ インターフェイスは同じタイプ（GigabitEthernet など）である必要があります。[Name]、[IP Address]、または [Security Level] を割り当てることはできません。実際には、メンバーインターフェイスに対して [Duplex] および [Speed] 以外のオプションを設定しないでください。
これらのオプションは ASA 5505 デバイスでのみ使用できます。	
Block Traffic To	この VLAN インターフェイスが、ここで選択された VLAN との接続を開始するのを制限します。

要素	説明
バックアップ インターフェイス	たとえば、ISP へのバックアップ インターフェイスとして VLAN インターフェイスを選択します。プライマリ インターフェイスによるデフォルト ルートに障害が発生しないかぎり、バックアップ インターフェイスはトラフィックを通過させません。トラフィックがバックアップ インターフェイスを必ず通過できるようにするには、プライマリ インターフェイスに障害が発生したときにバックアップ インターフェイスを使用できるように、プライマリ インターフェイスとバックアップ インターフェイスの両方でデフォルト ルートを設定します。
Active MAC Address Standby MAC Address	プライベート MAC アドレスを手動でインターフェイスに割り当てるには、[Active MAC Address] フィールドを使用します。[Standby MAC Address] フィールドを使用すると、デバイス レベルのフェールオーバーで使用するスタンバイ MAC アドレスを設定できます。 これらのフィールドの詳細については、デバイス インターフェイス：MAC アドレス （2427 ページ）を参照してください。
[EtherChannel Interface] オプションは、ASA 8.4.1 以降のデバイスでのみ使用できます。	
EtherChannel:ID	インターフェイスの [Type（タイプ）] に EtherChannel が選択されている場合、その EtherChannel（別名「ポートチャネル」）の ID を入力します。有効な値は 1 ～ 48 です。最大 48 個のポートチャネル グループを定義できます。詳細については、EtherChannel の設定 （2343 ページ）を参照してください。

要素	説明
Available Interfaces/Members in Group	インターフェイスの [Type] に EtherChannel が選択されている場合、[Available Interfaces] リストからインターフェイスを選択して、[>>] ボタンをクリックして右のメンバ リストに追加すると、この EtherChannel グループにインターフェイスを割り当てることができます。 最大 16 個のインターフェイスをチャネル グループに割り当てられます。ASA 9.2(1) 以降の場合、各チャネルグループに、最大 16 個のアクティブインターフェイスを設定できます。8 個のアクティブインターフェイスのみサポートするスイッチを使用していて、ASA のバージョンが 9.2(1) より前の場合、8 個のインターフェイスのみアクティブにできるため、残りのインターフェイスは、インターフェイス障害発生時のスタンバイリンクとして動作できます。または、[LACPモード（LACP Mode）] を [オン（On）] に設定すると、スタティック EtherChannel を作成できます（[詳細設定（Advanced）] タブで設定、 [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （2396 ページ）を参照）。作成すると、グループ内のすべてのインターフェイスでトラフィックを通過させることができます。 （注） チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、グループのタイプと速度が決まります。 詳細については、 EtherChannel の設定 （2343 ページ）を参照してください。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：Cisco Firepower 9000（[全般（General）] タブと [詳細（Advanced）] タブ）

Cisco Firepower 9000 デバイスの [全般（General）] タブと [詳細（Advanced）] タブでサポートされる要素については、 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）を参照してください。さらに、次の変更は Cisco Firepower 9000 デバイスにのみ適用されます。

表 *560 : [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：Cisco Firepower 9000*

要素	説明
タイプ	インターフェイスのタイプを選択します。冗長インターフェイスは、Cisco Firepower 9000 デバイスではサポートされていません。

要素	説明
[管理専用個別（Management Only Individual）]	Cisco Firepower 9000 デバイスでのみ、デバイスがクラスタモードの場合にのみ適用されます。 （注） [管理専用（Management Only）] チェックボックスと [管理専用個別（Management Only Individual）] チェックボックスの両方を同時に有効にすることはできません。[管理専用個別（Management Only Individual）] チェックボックスがオンになっている場合にのみ、クラスタプールを設定できます。
名前	最大48文字のインターフェイス名を指定します。[Name] には、インターフェイスの用途に関係する覚えやすい名前を付けます。 インターフェイス名は「Ethernet」で始めて、次の形式にする必要があります。 Ethernet[スロット]/[ポート]/サブポート。ここで、 • スロットは 1 ～ 3 で指定します。 • ポートは 1 ～ 8 で指定します。 • サブポートは 1 ～ 4 で指定します。 • サブポートはスロット 1 には適用されません。
次の要素は、Cisco Firepower 9000 デバイスではサポートされていません。	
[メディアタイプ（Media Type）]（[全般（General）] タブ）	
[デュプレックス（Duplex）]（[詳細（Advanced）] タブ）	
[速度（Speed）]（[詳細（Advanced）] タブ）	
[使用可能なインターフェイス（Available Interfaces）]/[グループ内のメンバー（Members In Group）]（[全般（General）] タブ）	
[ロードバランシング（Load Balancing）]（[詳細（Advanced）] タブ）	
[LACPモード（LACP Mode）]（[詳細（Advanced）] タブ）	
[VSSスイッチID（VSS Switch ID）]/[vPCスイッチID（vPC Switch ID）]（[詳細（Advanced）] タブ）	
[アクティブな物理インターフェイス（Active Physical Interfaces）]（[詳細（Advanced）] タブ）	
[ASAクラスタでのEtherChannelのスパン（Span EtherChannel across the ASA Cluster）]（[詳細（Advanced）] タブ）	

要素	説明
[VSSまたはvPCモードでスイッチペア間のロードバランシングを有効にする（Enable load balancing between switch pairs in VSS or vPC mode）]（[詳細（Advanced）] タブ）	
[メンバーインターフェイスの設定（Member Interface Configuration）]（[詳細（Advanced）] タブ）	

[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）は、ASA および PIX 7.0 以降のデバイスでインターフェイス、サブインターフェイス、冗長インターフェイスおよびEtherChannel インターフェイスを定義および設定するために使用します。[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください。

このダイアログボックスの [Advanced] パネルは、[Duplex]、[Speed]、最大伝送単位（MTU）パラメータなど、基本のインターフェイス設定を設定するために使用します。次の表ではこれらの設定の詳細を説明します。

関連項目

- [Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（2382 ページ）
- IPv6 インターフェイスの設定（ASA/FWSM） （2409 ページ）

表 *561 : [Advanced]* タブ：*[Add Interface]/[Edit Interface]* ダイアログボックス（*ASA/PIX 7.0* 以降）

要素	説明
デュプレックス	インターフェイスのデュプレックス オプションが一覧表示されます。インターフェイス タイプに応じて、[Full]、[Half]、または [N/A] があります。 [TenGigabitEthernet (ASA 5580 only)] の場合、[Duplex] は自動的に [Full] に設定されます。 （注） [Interface] のタイプとして [Subinterface] または [Redundant] が選択されている場合、このオプションは使用できません。

要素	説明
速度	

要素	説明
	物理インターフェイスの速度オプションがビット/秒で表示されます。論理インターフェイスには適用されません。使用できる速度は、インターフェイス タイプによって異なります。 • auto • 10 • 100 • 1000 • 10000（TenGigabitEthernet インターフェイスに自動的に設定されます。ASA 5580 でのみ使用できます） • nonegotiate （注） [Interface] のタイプとして [Subinterface] または [Redundant] が選択されている場合、このオプションは使用できません。 管理インターフェイスのポート PID は、パス C:\Program Files (x86)\CSCOpx\MDC\athena\config\csm.properties で指定する必要があります。管理対象インターフェイスでサポートされる速度オプションは次のとおりです。 • 1000 • 10000 • Detect SFP FPR-3100 デバイスの Ethernet1/1 から Ethernet1/8 までででサポートされる RJ 45 インターフェイスの設定可能な速度オプションは次のとおりです。 • 10 • 100 • 1000 RJ45 インターフェイスでは、次の速度オプションの組み合わせはサポートされていません。 • 1000 およびデュプレックスハーフ • 自動およびデュプレックスハーフ SFP ポート（Ethernet1/9 から Ethernet1/16）で設定可能な速度オプションは、CSM.properties で設定できる SFP ポート PID に基づいて識別されます。SFP ポートのポート PID は、パス C:\Program Files (x86)\CSCOpx\MDC\athena\config\csm.properties

要素	説明
	で指定する必要があります。 （注） SFP ポートに半二重の値を設定することはできません。全二重のみが許可されます。 • FPR-3110 および FPR-3120 でサポートされる速度オプションは次のとおりです。 • 1000 • 10000 • no-negotiate • sfp-detect • FPR-3130 および FPR-3140 でサポートされる速度オプションは次のとおりです。 • 1000 • 10000 • 25000 • no-negotiate • sfp-detect EPM ポート（Ethernet2/1 から Ethernet2/8）の FPR-3100 シリーズデバイスで設定可能な速度オプションは、デバイスショーインベントリからのモジュールタイプに基づいて識別されます。EPM ポートは、パス C:\Program Files (x86)\CSCOpx\MDC\athena\config\csm.properties で指定する必要があります。サポートされている速度オプションは次のとおりです。

要素	説明
	• FPR-X-NM-8X10G モジュール： • 1000 • 10000 • no-negotiate • sfp-detect • FPR-X-NM-8X25G モジュール： • 1000 • 10000 • 25000 • no-negotiate • sfp-detect • FPR-X-NM-4X40G モジュール： • 40000 • sfp-detect • no-negotiate

要素	説明
FEC モード（FEC Mode）	**物理インターフェイス**を選択した場合、ノイズの多いチャネルを介したデータ送信のエラーを減らすように **FEC モード**を設定できます。 **FEC モード**は、Ethernet1/9 から Ethernet1/16 までの**物理インターフェイス** ハードウェア ポートをサポートします。デフォルト値は auto です。**FEC モード**設定は、次の Firepower デバイスでサポートされています。 • FPR-3130 • FPR-3140 使用可能な FEC モードの値は次のとおりです。 • auto • cl108-rs • cl74-fc • disable （注） FEC モードの設定は、ASA 9.17(1) 以降のデバイスにのみ適用されます。FECモードは管理インターフェイスには適用されません。
Negotiate-Auto	**物理インターフェイス**を選択した場合、ピアとの相互運用性の問題がある場合はいつでも **Negotiate-Auto** を設定できます。 **Negotiate-Auto** 設定は、次の Firepowerデバイスでサポートされています。 • FPR-3110 • FPR-3120 • FPR-3130 • FPR-3140 （注） **Negotiate-Auto** 設定は、ASA 9.17(1) 以降のデバイスにのみ適用されます。Negotiate-Auto（AP-port）は管理インターフェイスには適用されず、インターフェイスがポート チャネル インターフェイスのメンバーである場合はサポートされません。

要素	説明
MTU	最大パケット サイズ、つまり最大伝送単位（MTU）をバイト数で指定します。この値は、インターフェイスに接続されているネットワークのタイプによって異なります。有効な値は 300 ～ 65535 バイトです。PPPoE を除くすべてのタイプのデフォルトは 1500 で、PPPoE のデフォルトは 1492 です。マルチコンテキスト モードでは、コンテキスト設定で MTU を設定します。
Active MAC Address Standby MAC Address	**PIX 7.2 以降および ASA 7.2 以降のデバイスでのみ使用できます。** プライベート MAC アドレスを手動でインターフェイスに割り当てるには、[Active MAC Address] フィールドを使用します。[Standby MAC Address] フィールドを使用すると、デバイス レベルのフェールオーバーで使用するスタンバイ MAC アドレスを設定できます。 これらのフィールドの詳細については、デバイス インターフェイス：MAC アドレス （2427 ページ）を参照してください。
ロール（Roles）	このインターフェイスに割り当てられているすべてのインターフェイス ロールが、このフィールドに一覧表示されます。ロールの割り当ては、このインターフェイスに指定されている名前と、Cisco Security Manager に現在定義されているインターフェイス ロール オブジェクト間のパターン マッチングに基づきます。 インターフェイス ロール オブジェクトは、各デバイスの設定が生成されるときに、実際のインターフェイスの IP アドレスで置き換えられます。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 ロールの詳細とその定義方法および使用方法については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
MAC アドレス	サイト固有の MAC アドレス。
サイト ID（Site ID）	現在のユニットが属するサイトを指定するサイト ID。
ソフトウェアバージョン 9.5(1) 以降を実行している ASA デバイスの Security Manager バージョン 4.9 以降、ルーテッドモードのスパンド EtherChannel にサイト間クラスタリングを使用できます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。	
[EtherChannel Interface] オプションは、ASA 8.4.1 以降のデバイスでのみ使用できます。	

要素	説明
ロード バランシング	（[General] パネルで）インターフェイスの [Type] に EtherChannel が選択されている場合、チャネル リンクのロード バランシング方式を設定します。このオプションの詳細については、EtherChannel のロードバランシングについて （2348 ページ）を参照してください。
LACP Mode	目的の [LACP モード（LACP Mode）] を選択します。デフォルトの [アクティブ（Active）] を選択すると、[アクティブ物理インターフェイス（Active Physical Interfaces）] の [最小（Minimum）] 値と [最大（Maximum）] 値で指定されているとおり、最大 8 個のインターフェイスをアクティブにして、最大 8 個のインターフェイスをスタンバイモードにできます。 [オン（On）] を選択すると、すべてのメンバーインターフェイスが「オン」になっているスタティックポートチャネルが作成されます。つまり、スタンバイポートなしで、最大 16 個のポートにトラフィックを通過させることができます。このオプションを選択すると、この EtherChannel グループに割り当てられているすべてのインターフェイスの [Mode] は [On] に切り替わります（それぞれの [Mode] が [On] ではない場合）。このモードの詳細については、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （2346 ページ）を参照してください。

要素	説明
Active Physical Interfaces	（[General] パネルで）インターフェイスの [Type] に EtherChannel が選択されている場合、この EtherChannel グループでアクティブにできるインターフェイスの最小数と最大数を [Minimum] と [Maximum] に指定します。 • [最少（Minimum）]：このグループでアクティブなインターフェイスの最小数を指定します。ASA 9.2(1)+ の場合、1 ～ 16 の値を指定できます。これより以前のバージョンでは、1 ～ 8 の値を入力します。 チャネル グループ内のアクティブ インターフェイス数がこの値よりも小さい場合、ポートチャネル インターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。 • [最大（Maximum）]：アクティブにできるインターフェイスの最大数を指定します。ASA 9.2(1)+ の場合、1 ～ 16 の値を指定できます。これより以前のバージョンでは、1 ～ 8 の値を入力します。 16 個のアクティブ インターフェイスの場合、スイッチがこの機能をサポートしている必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。 チャネルに使用できるインターフェイスは、このダイアログボックスの [General] タブで選択されます（[Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（2382 ページ））。 EtherChannel バンドルに 3、5、6、7 個のアクティブ ポートを指定すると、一部のポートが他の最大 2 倍の負荷を処理するため、ロード バランシングの効率が低下します。EtherChannel ごとに 2、4、8 個のアクティブ ポートを指定して、効率的なロードバランシングを実行することを推奨します（1 の値を指定すると、ロード バランシングはまったく実行されません）。
DHCP リレーオプション。 ASA-SM 9.1.2+ デバイスでのみ使用可能。	

要素	説明
DHCP リレーサーバー	IP アドレスを入力するか、またはこのインターフェイスの DHCP 要求をリレーする先のインターフェイス固有の DHCP サーバーを示すネットワーク/ホスト オブジェクトを選択します。複数の値はカンマで区切ります。最大4台のインターフェイス固有の DHCP リレーサーバーと、最大 10 台のグローバルおよびインターフェイス固有の DHCP リレーサーバーを設定できます。 （注） インターフェイス固有のサーバーでは、IPv6 はサポートされていません。 インターフェイスに DHCP 要求が届くと、ユーザーの設定に基づいて、ASA からその要求がリレーされる DHCP サーバーが決定されます。設定できるサーバのタイプは次のとおりです。 • インターフェイス固有の DHCP サーバー：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバーにだけリレーします。 • グローバル DHCP サーバー：インターフェイス固有のサーバーが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバル サーバーは使用されません。詳細については、[DHCP Relay] ページ （2602 ページ）を参照してください。
DHCP リレー信頼情報（オプション 82）	信頼するこの DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。 （注） すべての DHCP クライアント インターフェイスを信頼することもできます。詳細については、[DHCP Relay] ページ （2602 ページ）を参照してください。 DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレーエージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。

要素	説明
セキュアグループのタギングオプション。 ASA 9.3.1 以降のデバイスでのみ使用できます。 SGT とイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）を利用すると、ASA でシスコ独自のイーサネット フレーミング（EtherType 0x8909）を使用して、イーサネット インターフェイスでセキュリティ グループ タグを送受信できます。これにより、送信元のセキュリティ グループ タグをプレーンテキストのイーサネット フレームに挿入できます。ASA は、インターフェイスごとの手動設定に基づいて、発信パケットにセキュリティ グループ タグを挿入し、着信パケットのセキュリティ グループ タグを処理します。この機能を使用することで、ネットワーク デバイス間におけるエンドポイント ID の伝搬をインラインかつホップバイホップで実行できます。また、各ホップ間でシームレスなレイヤ 2 SGT インポジションを実現できます。 （注） 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。フェールオーバーリンクまたはクラスタ制御リンクはサポートしません。	
Cisco TrustSec のセキュアグループタギングの有効化	SGT とイーサネットタギングを有効にします（レイヤ 2 SGT インポジションとも呼ばれます）。
セキュアグループタグで出力パケットにタグ付け	インターフェイスでのセキュリティ グループ タグ（sgt と呼ばれる）の伝播をイネーブルにします。
すべての入力パケットにスタティック セキュア グループ タグを割り当て	ピアからの着信トラフィックにスタティック セキュリティ グループ タグを適用します。有効になっている場合、使用する SGT 番号を [セキュアグループタグ（Secure Group Tag）] フィールドで指定する必要があります。
セキュリティ グループ タグ（SGT）	ピアからの着信トラフィックに適用する SGT 番号を指定します。有効な値の範囲は 2 ～ 65519 です。
信頼できるインターフェイス	インターフェイス上の入力トラフィックにより、既存の SGT を、指定したスタティック SGT で上書きしてはならないことを示します。
ASA クラスタ（レイヤ 3）。クラスタモードの ASA 5580 および 5585 デバイスでのみ使用可能。 ASA クラスタがルータモードの場合はすべてのインターフェイスでサポートされ、ASA クラスタがトランスペアレントモードの場合は管理インターフェイスでサポートされます。	
IPv4 アドレスプール	使用するアドレスのプールを表す IPv4 プールオブジェクトを入力または選択します。
MAC アドレス プール	使用する MAC アドレスのプールを表す MAC プールオブジェクトを入力または選択します。

要素	説明
ASA クラスタ（レイヤ 2）。クラスタモードの ASA 5580 および 5585 デバイスでのみ使用可能。 ASA クラスタの EtherChannel インターフェイスでのみサポートされます。ASA クラスタがトランスペアレントモードの場合、管理インターフェイスではサポートされません。	
ASA クラスタに広がるスパン EtherChannel	選択して、クラスタ内のすべての ASA に広がる EtherChannel を設定し、EtherChannel の動作の一部としてロードバランシングを提供します。
VSS または vPC モードのスイッチペア間のロードバランシングを有効にする	（任意）仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）の 2 台のスイッチに ASA を接続する場合は、[VSSまたはvPCモードのスイッチペア間のロードバランシングを有効にする（Enable load balancing between switch pairs in VSS or vPC mode）] チェックボックスをオンにして、ロードバランシングを有効にする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。
メンバー インターフェイスの設定	インターフェイスの LACP モード、および指定したインターフェイスが接続されている仮想スイッチングシステム（VSS）または仮想ポート チャネル（vPC）のスイッチ（1 または 2）を識別します。
ASA 5505 デバイス固有の [Advanced] タブ オプション（ルーテッド モードのみ）	
Block Traffic To	この VLAN インターフェイスが、ここで選択された VLAN との接続を開始するのを制限します。
バックアップ インターフェイス	たとえば、ISP へのバックアップ インターフェイスとして VLAN インターフェイスを選択します。プライマリ インターフェイスによるデフォルト ルートに障害が発生しないかぎり、バックアップ インターフェイスはトラフィックを通過させません。トラフィックがバックアップ インターフェイスを必ず通過できるようにするには、プライマリ インターフェイスに障害が発生したときにバックアップ インターフェイスを使用できるように、プライマリ インターフェイスとバックアップ インターフェイスの両方でデフォルト ルートを設定します。
FWSM 3.1 以降のデバイス固有の [Advanced] タブ オプション	
ブリッジ グループ	トランスペアレント モードで動作している FWSM 3.1 以降では、この読み取り専用フィールドで、このインターフェイスが割り当てられるブリッジ グループを指定します。詳細については、[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス （2432 ページ）を参照してください。

要素	説明
ASR Group	このインターフェイスを非対称ルーティング グループに追加するには、このフィールドにASR グループ番号を入力します。フェールオーバー設定の装置間で非対象ルーティング サポートを適切に機能させるためには、ステートフル フェールオーバーをイネーブルにする必要があります。ASR グループの有効な値の範囲は 1 ～ 32 です。詳細については、非対称ルーティング グループについて （2337 ページ）を参照してください。
フロー制御のポーズフレームオプション ネットワーク インターフェイスが過負荷になると、フロー制御が、データを送信するデバイスに一次停止要求を送信することをネットワーク インターフェイスに許可し、過負荷状態を解消します。フロー制御が有効になっていないときに過負荷状態が発生すると、デバイスはパケットをドロップします。 インターフェイスの受信側が高ウォーターマークに達すると、インターフェイスの送信側はポーズフレームの生成を開始します。リモートデバイスは、ポーズフレームで指定された一次停止時間、パケットの送信を停止または削減することが期待されます。インターフェイスの受信側がそのキューをクリアできるか、一時停止時間内に低ウォーターマークに達した場合、インターフェイスの送信側は、一時停止時間を 0 とする特別なポーズフレームを送信します。これにより、リモートデバイスはパケットの送信を開始できます。インターフェイスの受信側がまだキューで動作している場合、一時停止時間が経過すると、インターフェイスの送信側は、新しい一時停止時間を持つ新しいポーズフレームを再度送信します。 （注） フロー制御のポーズフレームは、シングルコンテキストモードおよびマルチコンテキストモードの ASA 8.2 以降の物理インターフェイスでのみサポートされます。BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。	
Enable Pause Frame	（任意）フロー制御用のポーズフレームの送信を有効にします。
デフォルト値を使用する	（任意）デバイスに基づいて、低ウォーターマーク、高ウォーターマーク、および一次停止時間のデフォルト値を使用します。 これがオンになっていない場合は、デバイス固有のポーズフレームのフロー制御値の参照表に従って値を指定します。
低ウォーターマーク（キロバイト）	低ウォーターマークの値を入力します。インターフェイスからポーズフレームが送信された後、バッファの使用率が低ウォーターマークを下回ると、インターフェイスから「送信オン」フレームが送信されます。リモートデバイスはデータの送信を再開できます。
高ウォーターマーク（キロバイト）	高ウォーターマークの値を入力します。バッファの使用率が高ウォーターマークを超えると、インターフェイスからポーズフレームが送信されます。

要素	説明
一時停止時間	一次停止のリフレッシュのしきい値を 0 ～ 65535 スロットの範囲で設定します。各スロットは 64 バイトを転送するために必要な時間なので、ユニットあたりの時間はリンク速度によって異なります。リモートデバイスは、ポーズフレーム内のタイマー値による制御に従い、送信オンフレームを受信した後、または送信オフフレームの期限が切れた後、トラフィックを再開できます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズリフレッシュのしきい値に指定された間隔でポーズフレームが繰り返し送信されます。

表 *562 :* デバイス固有のポーズフレームフロー制御値

デバイスタイプ	低ウォーターマーク範囲（Kb）	デフォルト低ウォーターマーク範囲（Kb）	高ウォーターマーク範囲（Kb）	デフォルト高ウォーターマーク範囲（Kb）	一次停止時間の範囲	デフォルトの一時停止時間
ASA 5515	0 ～ 20	8	0 ～ 20	16	0 ～ 65535	26624
ASA 5525	0 ～ 20	8	0 ～ 20	16	0 ～ 65535	26624
ASA 5545	0 ～ 20	8	0 ～ 20	16	0 ～ 65535	26624
ASA 5510	0 ～ 48	16	0 ～ 48	24	0 ～ 65535	26624
ASA 5585	値はサポートされていません。「フロー制御送信オン」のみがサポートされています。					
ASA 5506	1 ～ 25	3	1 ～ 25	8	1 ～ 65535	18432
ISA-3000-2C2F	0-64	27	0-64	34	0 ～ 65535	26624
ISA-3000-4C	0-64	27	0-64	34	0 ～ 65535	26624
1783-SAD4T0S	0-64	27	0-64	34	0 ～ 65535	26624

IPv6 インターフェイスの設定（ASA/FWSM）

[Add Interface] または [Edit Interface] ダイアログボックスの [Type] で [Interface]、[Subinterface]、[Redundant]、[EtherChannel] を選択した場合、このダイアログボックスには、[General]、[Advanced]、[IPv6] の 3 つオプションのタブ付きパネルが表示されます。ここでは、[IPv6] パネルに表示されるこれらのオプションについて説明します。

（注） これらのオプションは、ルーテッドモードの ASA 7.0 以降のデバイス、トランスペアレントモードの ASA 8.2 以降のデバイス、ルーテッドモードの FWSM 3.1 以降のデバイスでのみ使用できます。

ナビゲーション パス

IPv6 パネルには [Add Interface] と [Edit Interface] のダイアログボックスでアクセスできます。これらのダイアログボックスには、デバイスインターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）の説明に従って、ASA または FWSM の [Interfaces] ページからアクセスできます。

関連項目

- Security Manager での IPv6 サポート （11 ページ）
- [Add Interface]/[Edit Interface] ダイアログボックス - [General] タブ（PIX 7.0 以降/ASA/FWSM）（2382 ページ）
- [Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降）（2396 ページ）

フィールド リファレンス

表 *563 : IPv6* タブ：*[Add Interface]/[Edit Interface]* ダイアログボックス（*ASA/FWSM*）

要素	説明
IPv6を有効化（Enable IPv6）	IPv6 をイネーブルにして、このインターフェイスで IPv6 アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると、このインターフェイスで IPv6 をディセーブルにできますが、設定情報は保持されます。

要素	説明
Enforce EUI-64	オンにすると、ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用します。 このオプションがインターフェイスでイネーブルにされると、そのインターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに対して検証され、インターフェイス ID が Modified EUI-64 形式を使用していることが確認されます。IPv6 パケットのインターフェイス ID が Modified EUI-64 形式でない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。 「%PIX|ASA-3-325003: EUI-64 source address check failed.」 アドレス形式の検証は、フローが作成された場合にのみ行われます。既存のフローからのパケットは確認されません。さらに、アドレス検証はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

要素	説明
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに 0 ～ 600 の数を入力します。0 を入力すると、インターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバル アドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカル アドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカル アドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

要素	説明
管理対象設定フラグ	IPv6 ルータ アドバタイズメント パケットの「managed-config-flag」フラグを設定するかどうか。
その他の設定フラグ	IPv6 ルータ アドバタイズメント パケットの「other-config-flag」フラグを設定するかどうか。
Enable RA	オンにすると、インターフェイスで IPv6 ルータ アドバタイズメントの送信がイネーブルになります。次のオプションを使用できます。 • [RA Lifetime]：「ルータライフタイム」値は、ローカルリンク上のノードがセキュリティアプライアンスをリンク上のデフォルトルータと見なし続ける期間を指定します。有効な値の範囲は 0 ～ 9000 秒で、デフォルトは 1800 秒です。0 を入力すると、セキュリティ アプライアンスは選択したインターフェイスのデフォルト ルータとは見なされません。 0 以外の任意の値は、次の [RA Interval] 値より小さい値にはできません。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。 • [RA Interval]：このインターフェイスでの IPv6 ルータアドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1800 秒です（次の [RA Interval in Milliseconds] オプションがオンの場合は 500 ～ 1800000 ミリ秒）。デフォルトは 200 秒です。 [RA Lifetime] が 0 以外の場合、送信の間隔は [RA Lifetime] の値以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。 • [RA Interval in Milliseconds]：このオプションをオンにすると、指定した [RA Interval] の値が秒ではなくミリ秒になります。

要素	説明
Interface IPv6 Addresses	ダイアログボックスのこのセクションで、インターフェイスに割り当てられている IPv6 アドレスを指定します。 • [Link-Local Address]：インターフェイスに自動的に生成されたリンクローカルアドレスを上書きするには、このフィールドに目的の IPv6 リンクローカルアドレスを入力します。 リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンクローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラーが表示されます。 • [Enable Address Auto-Configuration]：ステートレス自動設定を使用して、インターフェイスで IPv6 アドレスの自動設定をイネーブルにするには、このオプションをオンにします。アドレスは、Router Advertisement（RA; ルータアドバタイズメント）メッセージで受信されたプレフィックスに基づいて設定されます。リンクローカル アドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。生成されたリンクローカル アドレスを別のホストが使用している場合は、エラーが発生されます。 • [Trust the DHCP Servers for default gateway]：このラジオボタンを選択して、信頼できる送信元（直接接続されたネットワーク）からのルータアドバタイズメントから、デフォルトのルートをインストールします。 • [Ignore trust and accept router advertisements]：このラジオボタンを選択して、別のネットワークからのルータアドバタイズメントから、デフォルトのルートをインストールします。 • このセクションのテーブルには、このインターフェイスに割り当てられている IPv6 アドレスが表示されます。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Address for Interface] ダイアログボックス （2417 ページ）が開きます。

要素	説明
Interface IPv6 Prefixes	このセクションのテーブルを使用して、IPv6 ルータ アドバタイズメントに含まれる IPv6 プレフィックス（つまり、IPv6 アドレスのネットワーク部分）を設定します。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Prefix Editor] ダイアログボックス （2419 ページ）が開きます。

要素	説明
Interface IPv6 DHCP	このセクションを使用して、1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。 次のいずれかを選択します。 • [Server Pool]：これを選択して、DHCPv6 サーバーに提供させる情報が含まれる IPv6 DHCP プールを設定します。必要に応じてインターフェイスごとに個別のプールを設定できます。また、複数のインターフェイスで同じプールを使用することもできます。[DHCPプールセレクタ（DHCP Pool Selector）] ダイアログの [行の追加（Add Row）] ボタンと [行の編集（Edit Row）] ボタンを使用して、これらのエントリを管理します。（これらは テーブルの使用 （64 ページ）で説明されている標準ボタンです。）[行の追加（Add Row）] と [行の編集（Edit Row）] で [DHCPv6 プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス （2422 ページ）が開きます。 または • [Client Prefix Delegation Name]：このインターフェイスで取得したプレフィックスに名前を入力して、DHCPv6 プレフィックス委任クライアントを有効にします。有効な値は、200 文字を超えない文字列です。 • [DHCPv6 Prefix Hint]：[行の追加（Add Row）] ボタンを使用して、受信したい委任されたプレフィックスに関する 1 つ以上のヒントを提供します。通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバーによって決定されます。 （注） ヒントとして提案されたプレフィックスが関連付けられたローカルプレフィックスプールの有効なプレフィックスで、いずれにも割り当てられていない場合、サーバーはクライアントが提案したプレフィックスを委任します。それ以外の場合、ヒントは無視され、プレフィックスはプールのフリー リストから委任されます。 • • [Enable DHCP]：DHCPv6 を使用してアドレスを取得するには、これを選択します。オプションとして、ルータアドバタイズメントからデフォルトルートを取得するには、[デフォルトルートを有効にする（Enable Default Route）] を選択します。

要素	説明
（注）	DHCPv6 クライアントまたはサーバープールが IPv6 インターフェイスで設定されている場合、同じインターフェイスを使用して DHCPv6 リレーを設定することはできません。

[IPv6 Address for Interface] ダイアログボックス

このダイアログボックスは、ASA または FWSM のインターフェイスに割り当てられている IPv6 アドレスを追加または編集するために使用します。[Add Interface] または [Edit Interface] ダイアログボックスの [IPv6] パネルでは、インターフェイスに複数の IPv6 アドレスを割り当てることができます。

（注） このダイアログボックスは、ルーテッド モードの ASA 7.0 以降のデバイス、トランスペアレント モードの ASA 8.2 以降のデバイス、ルーテッド モードの FWSM 3.1 以降のデバイスでのみ使用できます。

ナビゲーション パス

[IPv6 Address for Interface] ダイアログボックスには、次の場所からアクセスできます。

- ASA または FWSM の [Add Interface] と [Edit Interface] ダイアログボックスの [IPv6 パネル]。
- トランスペアレント ファイアウォール モードの ASA 5505（バージョン 8.2 と 8.3 のデバイスのみ）の [Management IPv6] ページ。

[Interfaces IPv6 Addresses] セクションのテーブルの下にある [Add Row] または [Edit Row] ボタンをクリックすると、ダイアログボックスが開きます。

関連項目

- [IPv6 Prefix Editor] ダイアログボックス （2419 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）
- [Management IPv6] ページ（ASA 5505） （2462 ページ）

フィールド リファレンス

表 *564 : [IPv6 Address for Interface]* ダイアログボックス

要素	説明
プレフィックス名（Prefix Name）	（任意）委任されたプレフィックスを使用するプレフィックス名を入力します。有効な値は、200 文字を超えない文字列です。 **ヒント** 「DHCP」は予約語なので、Cisco Security Manager では [プレフィックス名（Prefix Name）] として使用できません。 **（注）** ASA インターフェイスで DHCPv6 プレフィックス委任クライアントが有効になっていることを確認します。詳細については、表 563 : IPv6 タブ : [Add Interface]/[Edit Interface] ダイアログボックス（ASA/FWSM） （2410 ページ）のインターフェイス IPv6 DHCP 要素を参照してください。
Address/Prefix Length	インターフェイスに割り当てられる IPv6 ネットワーク アドレスを入力し、プレフィックス長を [Prefix Length] に追加します。[Prefix Length] の整数は、アドレスのネットワーク部分を構成するアドレスの上位ビット秒の数を示します。プレフィックス長の前にスラッシュ（/）を付ける必要があります。たとえば、3FFE:C00:0:1::/64 です。 通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（::1:0:0:0:1 など）を指定する必要があります。 プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

要素	説明
EUI-64	このチェックボックスをオンにすると、IPv6 アドレスの低位の 64 ビットに EUI-64 インターフェイス ID が使用されます。[Prefix Length] に指定される値が 64 ビットを超える場合、プレフィックス ビットはインターフェイス ID より優先されます。指定されたアドレスを別のホストが使用している場合は、エラーが発生します。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。
IPv6アドレス プール（IPv6 Address Pool）	使用するアドレスのプールを表す IPv6 プールオブジェクトを入力または選択します。

[IPv6 Prefix Editor] ダイアログボックス

このダイアログボックスは、プレフィックスを IPv6 ルータ アドバタイズメントに含めるかどうかなどの個別のパラメータを制御して、IPv6プレフィックス（つまり、IPv6アドレスのネットワーク部分）を追加または編集するために使用します。ASA または FWSM の [Add Interface] または [Edit Interface] ダイアログボックスの [IPv6] パネルでは、複数のプレフィックスを設定できます。

（注） このダイアログボックスは、ルーテッド モードの ASA 7.0 以降のデバイス、トランスペアレント モードの ASA 8.2 以降のデバイス、ルーテッド モードの FWSM 3.1 以降のデバイスでのみ使用できます。

デフォルトでは、アドレスとしてインターフェイスに設定されているプレフィックスがルータ アドバタイズメントでアドバタイズされます。アドバタイズメントに特定のプレフィックスを設定する場合、これらのプレフィックスだけがアドバタイズされます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。または、日付を設定して、プレフィックスの有効期限を指定できます。期限に達すると、プレフィックスはアドバタイズされなくなります。

ナビゲーション パス

[IPv6 Prefix Editor] ダイアログボックスには、[Add Interface] と [Edit Interface] ダイアログボックスの [IPv6] パネルからアクセスできます。これらのダイアログボックスの [Interfaces IPv6

Prefixes] セクションにあるテーブルの下にある [Add Row] または [Edit Row] ボタンをクリックします。

関連項目

- [IPv6 Address for Interface] ダイアログボックス （2417 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）
- デバイスインターフェイス、ハードウェアポート、ブリッジグループの管理 （2373 ページ）

フィールド リファレンス

表 *565 : [IPv6 Prefix Editor]* ダイアログボックス

要素	説明
Address/Prefix Length	IPv6 ネットワーク アドレスを入力し、プレフィックス長を [Prefix Length] に追加します。[Prefix Length] の整数は、アドレスのネットワーク部分を構成するアドレスの上位ビット秒の数を示します。プレフィックス長の前にスラッシュ（/）を付ける必要があります。たとえば、3FFE:C00:0:1::/64 です。
デフォルト	このチェックボックスをオンにすると、このダイアログボックスの設定は 1 つのアドレスではなく、すべてのプレフィックスに適用されます（オンにすると、[Address/Prefix Length] フィールドはディセーブルになります）。
No Advertisements	オンにすると、ローカルリンクのホストでは、指定したプレフィックスをアドバタイズメントで使用できません。
Off Link	オンにすると、指定したプレフィックスは「オフリンク」になります。つまり、リンクにはローカルから到達できなくなります。 オンリンク（デフォルト）の場合、指定したプレフィックスがリンクに割り当てられます。指定したプレフィックスを含むアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。
No Auto-Configuration	オンにすると、ローカル リンクのホストでは、IPv6 自動設定に指定したプレフィックスを使用できません。 自動設定がオンの場合（デフォルト）、ローカル リンク上のホストは IPv6 自動設定に指定したプレフィックスを使用します。

要素	説明
Prefix Lifetime	ダイアログボックスのこのセクションを展開すると、次の期限オプションを表示できます。 • [ライフタイム期間（Lifetime Duration）]：このオプションを選択して、プレフィックスの期限を時間の長さとして定義します。次のオプションがイネーブルになります。 • [有効期間（Valid Lifetime）]：指定された IPv6 プレフィックスが有効なものとしてアドバタイズされる時間（秒）。値を 0 ～ 4294967295 秒の範囲で入力します。最大値は無限を示します（つまり、ライフタイムの期限は切れません）。これは、[無限（Infinite）] ボックスをオンにしても指定できます。デフォルトは 2592000（30 日間）です。 • [優先ライフタイム（Preferred Lifetime）]：指定された IPv6 プレフィックスが優先プレフィックスとしてアドバタイズされる期間（秒単位）。値を 0 ～ 4294967295 秒の範囲で入力します。最大値は無限を示します（つまり、ライフタイムの期限は切れません）。これは、[無限（Infinite）] ボックスをオンにしても指定できます。デフォルトは 604800（7 日間）です。[優先ライフタイム（Preferred Lifetime）] は、[有効期間（Valid Lifetime）] の値以下である必要があります。 • [ライフタイムの有効期限（Lifetime Expiration Date）]：このオプションをオンにて、プレフィックスの期限を特定の日付として定義します。この日付には、今日から 1 年後までの日付の値を指定できます。次のオプションを使用できます。 • [有効（Valid）]：この日時まで、プレフィックスは有効としてアドバタイズされます。 Mmm dd yyyy の形式で日付を入力します（つまり、3 文字の月の短縮形、2 桁の日、4 桁の年）。またはカレンダー アイコンをクリックして、カレンダーをスクロールして日付を選択します。また、指定した日付に期限が切れる時間を入力します。形式は 24 時間形式で hh:mm です。 • [優先（Preferred）]：この日時まで、プレフィックスは優先としてアドバタイズされます。 Mmm dd yyyy の形式で日付を入力します（つまり、3 文字の月の短縮形、2 桁の日、4 桁の年）。またはカレンダー アイコンをクリックして、カレンダーをスクロールして日付を選択します。また、指定した日付に期限が切れる時間を入力します。形式は 24 時間形式で hh:mm です。[Preferred] の日時は [Valid] の日時以前である必要があります。

[DHCPv6 プールの追加または編集（Add or Edit DHCPv6 Pool）] ダイアログボックス

このダイアログボックスを使用して、DHCPv6 サーバープールを追加または編集します。ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併用するクライアントについては、クライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。

ナビゲーション パス

- [管理（Manage）] メニューから [ポリシーオブジェクト（Policy Objects）] を選択するか、ボタンバーの [Policy Object Manager] ボタンをクリックして、[Configuration Manager] ウィンドウの下部にある [Policy Object Manager] ペインを開きます。オブジェクトタイプセレクタから **[プールオブジェクト（Pool Objects）]>[DHCPv6 プールオブジェクト（DHCPv6 Pool Object）]** を選択します。作業領域内で右クリックして [新規オブジェクト（New Object）] を選択し、オブジェクトタイプを選択するか、または行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。ペインの下部にある関連するボタンを使用して、いずれかのダイアログボックスを開くこともできます。

または

- [DHCPv6 プールの追加（Add DHCPv6 Pool）] ダイアログボックスには、[DHCPv6 プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスからアクセスできます。[使用可能な DHCPv6 プール（Available DHCPv6 Pool）] テーブルの下にある [行の追加（Add Row）] または [行の編集（Edit Row）] ボタンをクリックします。[DHCPv6 プールセレクタ（DHCPv6 Pool Selector）] ダイアログボックスには、[インターフェイスの追加（Add Interface）] および [インターフェイスの編集（Edit Interface）] ダイアログボックスの [IPv6] パネルの [インターフェイス IPv6 DHCP（Interface IPv6 DHCP）] セクションにある [サーバープール（Server Pool）] オプションボタンからアクセスできます。

関連項目

- [IPv6 Address for Interface] ダイアログボックス （2417 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）
- デバイスインターフェイス、ハードウェア ポート、ブリッジグループの管理 （2373 ページ）

フィールド リファレンス

表 *566 : [DHCPv6 プールの追加（Add DHCPv6 Pool）] ダイアログボックス*

要素	説明
名前	DHCPv6 プール名は 200 文字までです。オブジェクト名では、大文字と小文字が区別されません。

要素	説明
• 1 つ以上のタブでパラメータを設定し、IR メッセージに対する応答をクライアントに提供します。 • タブごとに、必要に応じて次の内容を指定します。 • DNS/SIP/NIS/NISP/SNTP サーバー：サーバー名を入力します。IPv6 アドレスが正しい形式であることを確認してください。IPv6 アドレス形式の詳細については、http://www.ietf.org/rfc/rfc2373.txt を参照してください。 • DNS/SIP/NIS/NISP ドメイン名：ドメイン名を入力します。ドメイン名の先頭と末尾は数字または文字にする必要があります。内部文字として使用できるのは文字、数字、ハイフンのみです。ラベルはドットで区切ります。各ラベルは最大 63 文字で、ホスト名全体は最大 255 文字です。ドメイン名形式の詳細については、http://www.ietf.org/rfc/rfc1123.txt を参照してください。 （注） import コマンドは、プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバから取得した 1 つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じコマンドを手動と import コマンドで設定することはできません。	
[サーバ（Server）] タブ	（任意）DNS サーバー名とドメイン名を指定します。
[SIP] タブ	（任意）SIP サーバー名と SIP ドメイン名を指定します。
[NIS] タブ	（任意）NIS サーバー名と NIS ドメイン名を指定します。
[NISP] タブ	（任意）NISP サーバー名と NISP ドメイン名を指定します。
[SNTP] タブ	（任意）SNTP サーバー名を指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降）

シングルコンテキストのルーテッド モードで動作しているセキュリティ デバイスには、そのインターフェイスの IP アドレス指定が必要です。ただし、ファイアウォール インターフェイスには、割り当てられるまで IP アドレスがありませんトランスペアレントモードでは、デバイスはアクセス制御ブリッジ（「Bump In The Wire」）として機能することに注意してください。つまり、インターフェイスにそれぞれ異なる VLAN を割り当てますが、IP アドレス指定は必要ありません。

シングルコンテキスト、ルーテッドモードの独立した ASA または PIX 7.0 以降のデバイスに表示される [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスには、[IP タイプ（IP Type）] セクションがあります。次の説明に従って、ここにインターフェイスの IP アドレス指定のタイプを指定し、関連するパラメータを入力します。（PIX 6.3 デバイス用の [Add Interface] または [Edit Interface] ダイアログボックスの [IP Type] セクションについては、デバイス インターフェイス：IP タイプ（PIX 6.3）（2378 ページ）を参照してください）。

マルチコンテキスト モードでは、インターフェイス IP アドレスはコンテキスト設定で設定されます。

（注） グローバルプールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。また、冗長インターフェイスとして使用するインターフェイスには、IP タイプの情報を指定しないでください。

ステップ 1 [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、次のように、[IP タイプ（IP Type）] リストからアドレス割り当て方式（[スタティック IP（Static IP）]、[DHCP の使用（Use DHCP）]、または [PPPoE]（PIX および ASA 7.2 以降））を選択し、関連パラメータを指定します。

- [スタティック IP（Static IP）]：このインターフェイスが接続するネットワーク上のセキュリティデバイスを示すスタティック IP アドレスおよびサブネットマスクを指定します。IP アドレスは、インターフェイスごとに一意でなければなりません。

サブネット マスクは、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。バージョン 4.13 以降、Cisco Security Manager では、ポイント ツー ポイント インターフェイスに 255.255.255.254 を使用できます。ネットワークに接続するインターフェイスには 255.255.255.255 を使用しないでください。使用すると、トラフィックがこのインターフェイスで停止します。サブネット マスク値を指定しない場合は、次に示すように「クラスフル」ネットワークが使用されます。

- IP アドレスの最初のオクテットが 1 ～ 126 の場合（つまり、アドレスが 1.0.0.0 ～ 126.255.255.255 の場合）、クラス A ネットマスク（255.0.0.0）が使用されます。
- IP アドレスの最初のオクテットが 128 ～ 191 の場合（つまり、アドレスが 128.0.0.0 ～ 191.255.255.255 の場合）、クラス B ネットマスク（255.255.0.0）が使用されます。
- IP アドレスの最初のオクテットが 192 ～ 223 の場合（つまり、アドレスが 192.0.0.0 ～ 223.255.255.255 の場合）、クラス C ネットマスク（255.255.255.0）が使用されます。

（注） グローバル プールやスタティック NAT エントリの IP アドレスなど、以前にルータ、ホスト、または他のファイアウォール デバイス コマンドに使用したアドレスは使用しないでください。

- [Use DHCP]：Dynamic Host Configuration Protocol（DHCP）をイネーブルにして、接続ネットワーク上の DHCP サーバから IP アドレスが自動的に割り当てられるようにします。次のオプションを使用できます。
  - [DHCP 学習済みルートメトリック（DHCP Learned Route Metric）]（必須）：学習したルートにアドミニストレーティブ ディスタンスを割り当てます。有効な値は 1 ～ 255 です。学習されたルートのアドミニストレーティブ ディスタンスはデフォルトで 1 になります。

すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブ ディスタンス」とも呼ばれます）。同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。

- [DHCP を使用したデフォルトルートの取得（Obtain Default Route using DHCP）]：デフォルトのスタティックルートを設定する必要がないように DHCP サーバーからデフォルトルートを取得するには、このオプションを選択します。スタティック ルートの設定 （2891 ページ）も参照してください。
  - [DHCP 学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）]：[DHCP を使用したデフォルトルートの取得（Obtain Default Route using DHCP）] を選択した場合、このオプションを選択し、特定のサービスレベル契約（SLA）モニターによるルートトラッキングを有効にできます。次のオプションが使用可能になります。
  - [トラッキング済み SLA モニター（Tracked SLA Monitor）]：[DHCP 学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルートトラッキング（接続性のモニタリング）を定義している SLA モニタ

オブジェクトの名前を入力または選択します。詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）を参照してください。

- [PPPoE]（PIX および ASA 7.2 以降）：Point-to-Point Protocol over Ethernet（PPPoE）をイネーブルにして、接続ネットワーク上の PPPoE サーバーから IP アドレスが自動的に割り当てられるようにします。このオプションは、フェールオーバーではサポートされません。次のオプションを使用できます。
  - [VPDN グループ名（VPDN Group Name）]（必須）：ネットワーク接続、ネゴシエーション、および認証に使用する認証方式とユーザー名/パスワードが含まれるバーチャル プライベート ダイヤルアップ ネットワーク（VPDN）グループを選択します。詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）を参照してください。
  - [IP アドレス（IP Address）]：指定した場合、ネゴシエートされたアドレスではなく、このスタティック IP アドレスが接続および認証に使用されます。
  - [サブネットマスク（Subnet Mask）]：指定した IP アドレスとともに使用されるサブネットマスク。
  - [PPPoE 学習済みルートメトリック（PPPoE Learned Route Metric）]（必須）：学習したルートにアドミニストレーティブ ディスタンスを割り当てます。有効な値は 1 ～ 255 です。デフォルトは 1 です。

すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブ ディスタンス」とも呼ばれます）。同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブ ディスタンスを使って使用するルートを決定します。

-
  - [PPPoE を使用してデフォルトルートを取得（Obtain Default Route using PPPoE）]：PPPoE サーバーからデフォルトルートを取得するには、このオプションをオンにします。PPPoE クライアントでまだ接続が確立されていない場合には、デフォルトルートを設定します。このオプションを使用する場合は、スタティックに定義されたルートを設定に含めることができません。
  - [PPPoE 学習ルートのトラッキングの有効化（Enable Tracking for PPPoE Learned Route）]：[PPPoE を使用したデフォルトルーティングの取得（Obtain Default Routing Using PPPoE）] を選択した場合、このオプションを選択して、PPPoE が学習したルートのルートトラッキングを有効化できます。次のオプションを使用できます。
  - [デュアル ISP インターフェイス（Dual ISP Interface）]：デュアル ISP サポート用のインターフェイスを定義する場合、設定中の接続を示す [プライマリ（Primary）] または [セカンダリ（Secondary）] を選択します。
  - [トラッキング済み SLA モニター（Tracked SLA Monitor）]：[DHCP 学習済みルートのトラッキングの有効化（Enable Tracking for DHCP Learned Route）] を選択した場合は必須です。このインターフェイスに適用されるルートトラッキング（接続性のモニタリング）を定義している SLA モニタオブジェクトの名前を入力または選択します。詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）を参照してください。

（注） DHCP および PPPoE は、ファイアウォール デバイスの外部インターフェイスでだけ設定できます。外部インターフェイスで PPPoE がすでに設定されている場合は、オプションとして使用できません。

ステップ 2 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（2380 ページ）に従ってデバイス インターフェイスの設定を続けます。

デバイス インターフェイス：MAC アドレス

デフォルトでは、物理インターフェイスは「バーンドイン」MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

冗長インターフェイスでは、最初に追加された物理インターフェイスの MAC アドレスが使用されます。構成でメンバーインターフェイスの順序を変更すると、MAC アドレスがリストの先頭にあるインターフェイスの MAC アドレスと一致するように変更されます。手動で冗長インターフェイスに MAC アドレスを割り当てた場合、物理インターフェイスの MAC アドレスに関係なく、このアドレスが使用されます。

同様に、EtherChannel グループに割り当てられているすべてのインターフェイスは、同じ MAC アドレスを共有します。デフォルトでは、EtherChannel は最も番号の小さいメンバ インターフェイスの MAC アドレスを使用します。ただし、最も小さい番号のインターフェイスがグループから削除された場合にトラフィックの分断を防止するため、EtherChannel の MAC アドレスを手動で設定できます。

サブインターフェイスに一意の MAC アドレスを割り当てることが必要になる場合もあります。たとえば、サービス プロバイダーが MAC アドレスに基づいてアクセスを制御している場合などです。

さらに、フェールオーバーを使用する場合は、スタンバイ MAC アドレスを指定できます。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

（注） 次のオプションは、PIX 7.2 以降と ASA 7.2 以降のデバイスの [Add Interface] と [Edit Interface] ダイアログボックスの [Advanced] タブにのみ表示されます。

（任意）プライベート MAC アドレスを現在のインターフェイスに手動で割り当てるには、次の手順を実行します。

ステップ 1 [インターフェイスの追加（Add Interface）] または [インターフェイスの編集（Edit Interface）] ダイアログボックスで、[アクティブなMACアドレス（Active MAC Address）] フィールドに目的の MAC アドレスを入力します。

MAC アドレスは、H.H.H の形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。

（注） 場合によっては、[Standby MAC Address] フィールドをアクティブにするためには、[Active MAC Address] に入力したあとに、Tab キーを押す必要がある場合があります。

ステップ 2 必要に応じて、デバイスレベルのフェールオーバーで使用する**スタンバイ MAC アドレス**を指定します。

アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

ステップ 3 [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM）（2380 ページ）に従ってデバイス インターフェイスの設定を続けます。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[スイッチポート（Switch Port）] タブ

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックスの [スイッチポート（Switch Port）] パネルを使用して、Firepower 1010 デバイスのモード、アクセス VLAN ID、トランクタイプ、VLAN ID などを設定します。

ナビゲーション パス

[Add Interface] と [Edit Interface] ダイアログボックスには、[Interfaces] ページからアクセスできます。[スイッチポートの有効化（Enable Switchport）] チェックボックスをオンにして、これらを設定します。

フィールド リファレンス

表 *567 : [スイッチポート（Switch Port）] タブ：[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス*

要素	説明
[スイッチポートの有効化（Enable Switchport）]	選択したインターフェイスでスイッチポートを有効にするには、このボックスをオンにします。このオプションをオフにすると、インターフェイスのスイッチポートが無効になりますが、設定情報はそのまま保持されます。
[モード（Mode）]	利用可能な 2 つのモードであるアクセスまたはトランクのいずれかを選択します。
アクセス VLAN ID	このダイアログボックスは、アクセスモードが選択されている場合にのみ有効になります。0 ～ 4190 の範囲内で値を入力します。インターフェイスに設定されている VLAN ID がここに入力されます。
トランク タイプ	使用可能な 2 つのトランクタイプである許可またはネイティブのいずれかを選択します。

要素	説明
VLAN ID（Admin. VLAN ID）	選択したモードに従って、このポートの VLAN ID を入力します。
[保護の有効化（Enable Protected）]	このオプションは、このポートが同じ VLAN 上の他のスイッチポートと通信できないようにする場合に選択します。

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス：[Power Over Ethernet] タブ

[インターフェイスの追加（Add Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスの [Power Over Ethernet (POE)] は、電力消費モードとワット数を設定するために使用されます。ASA 9.13(1) 以降、この機能は Firepower 1010 デバイスでサポートされ、ポート Ethernet1/7 および Ethernet1/8 の物理インターフェイスの一部です。

POE機能を使用すると、物理インターフェイスを構成して、クラス制限ワット数に従って、接続されたデバイスに電力が自動的に供給されるようにできます。指定されたポート（Ethernet1/7 または Ethernet1/8）から電源が遮断されます。指定されたポートに必要なワット数は、LLDP ネゴシエーションなしでミリワット単位で事前に設定されています。

フィールド リファレンス

表 *568 : [スイッチポート（Switch Port）] タブ：[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス*

要素	説明
POEを無効にする（Disable POE）	指定したポート（Ethernet 1/7 または Ethernet 1/9）への電源を遮断するには、このチェックボックスをオンにします。
消費モード（Consumption Mode）	電力消費モードを選択します。 • [自動（Auto）]（デフォルト）：これを選択すると、クラス制限ワット数に従って、接続されたデバイスに自動的に電力が供給されます。 • [設定（Configure）]：これを選択して、選択したポートに必要な消費ワット数を手動で指定します。
消費ワット数（Consumption Wattage）	選択したポートに必要な消費ワット数（ミリワット）を指定します。

ASA 5505 でのハードウェア ポートの設定

ASA 5505 デバイスに表示される [インターフェイス（Interfaces）] ページには、[ハードウェアポート（Hardware Ports）] および [インターフェイス（Interfaces）] の 2 つのタブ付きパネルが表示されます。[Hardware Ports] パネルのテーブルには、選択した ASA 5505 に現在設定されているスイッチ ポートが表示されます。

[Configure Hardware Ports] ダイアログボックスを使用して、ASA 5505 のスイッチ ポートを設定します。モードの設定、スイッチ ポートの VLAN への割り当て、[Protected] オプションの設定などが含まれます。（次のダイアログボックス パラメータの説明では、[Hardware Ports] テーブルのフィールドも説明します）。

注意 ASA 5505 では、ネットワーク内のループ検出のためのスパニングツリー プロトコルはサポートされません。そのため、アプライアンスとの接続がネットワーク ループにならないようにする必要があります。

ナビゲーション パス

[Configure Hardware Ports] ダイアログボックスには、ASA 5505 の [Interfaces] ページにある [Hardware Ports] パネルの [Add Row] または [Edit Row] をクリックするとアクセスできます。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理（2373 ページ）を参照してください。

関連項目

- ASA 5505 のポートおよびインターフェイスについて （2338 ページ）
- [インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）

フィールド リファレンス

表 569 : [Configure Hardware Ports] ダイアログボックス

要素	説明
[Enable Interface]	このオプションを選択すると、このスイッチ ポートがイネーブルになります。このオプションをオフにすると、このポートをディセーブルにできますが、設定情報は保持されます。
隔離（Isolated）	このオプションは、このポートが同じ VLAN 上の他の隔離されたスイッチポートまたは「保護された」スイッチポートと通信できないようにする場合に選択します。 スイッチ ポート上のデバイスが主に他の VLAN からアクセスされ、VLAN 内アクセスを許可する必要がなく、感染などのセキュリティ違反があったときにデバイスを相互に分離する必要がある場合、それらのポートが相互に通信できないようにすることがあります。たとえば、3 つの Web サーバをホストする DMZ がある場合、各スイッチ ポートに [Protected] オプションを適用すると、Web サーバを相互に分離できます。内部および外部ネットワークはいずれも 3 つすべての Web サーバと通信でき、またその逆も可能ですが、Web サーバどうしは通信できません。

要素	説明
Hardware Port	設定しているスイッチ ポートを選択します。すべてのデバイス ポートが一覧表示されます。
[モード（Mode）]	このポートのモードを選択します。 • [アクセスポート（Access Port）]：ポートをアクセスモードに設定します。各アクセス ポートは 1 つの VLAN に割り当てることができます。 • [トランクポート（Trunk Port）]：ポートを 802.1Q タギングを使用するトランクモードに設定します。トランク ポートは、802.1Q タギングを使用して複数の VLAN を伝送できます。 トランク モードが使用できるのは Security Plus ライセンスだけです。トランク ポートでは、タグが付いていないパケットはサポートされません。ネイティブ VLAN サポートはなく、すべてアプライアンスはタグが含まれていないパケットをドロップします。
VLAN ID（Admin. VLAN ID）	選択した [Mode] に従って、このポートの VLAN ID を入力します。 • [Access Port] モードでは、このスイッチ ポートが割り当てられる VLAN ID を入力します。 • [Trunk Port] モードでは、複数の VLAN ID および複数の ID 範囲（4-8 など）をカンマで区切って入力できます。 （注） 7.2(2)18 以前のオペレーティング システムをデバイスで実行している場合、有効な VLAN ID は 1 ～ 1001 です。バージョン 7.2(2)19 以降での有効な ID は 1 ～ 4090 です。
デュプレックス	ポートのデュプレックスオプションを [フル（Full）]、[ハーフ（Half）]、[自動（Auto）] から選択します。デフォルトである [Auto] 設定を推奨します。 PoE ポート Ethernet 0/6 または 0/7 のデュプレックスを [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。

要素	説明
速度	ポートの速度を [10]、[100]、[自動（Auto）] から選択します。デフォルトである [Auto] 設定を推奨します。 PoE ポート Ethernet 0/6 または 0/7 の速度を [Auto] 以外に設定した場合、IEEE 802.3af をサポートしない Cisco IP Phone および Cisco ワイヤレス アクセス ポイントは検出されず、電力は供給されません。 デフォルトの [Auto] 設定には、Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、[Speed] または [Duplex] のいずれかを [Auto] に設定する必要があります。[Speed] と [Duplex] の両方を明示的に固定値に設定し、したがって両方の設定のオートネゴシエーションをディセーブルにした場合、Auto-MDI/MDIX もディセーブルになります。

[Add Bridge Group]/[Edit Bridge Group] ダイアログボックス

トランスペアレント ファイアウォールは、その内部インターフェイスと外部インターフェイスで同じネットワークを接続し、コンテキストにつき 2 つのインターフェイスだけをサポートします。ただし、ブリッジ グループを使用すると、コンテキストに使用できるインターフェイスの数を増やすことができます。ブリッジグループは 8 個まで設定できます。FWSM では各グループに 2 つのインターフェイスを含めることができ、ASA 9.6.1 では各グループに 64 のインターフェイスを含めることができます。

各ブリッジ グループは、別々のネットワークに接続します。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックはセキュリティ アプライアンス内の別のブリッジグループにはルーティングされません。また、トラフィックは外部ルータからセキュリティ アプライアンス内の別のブリッジ グループにルーティングされる前に、セキュリティ アプライアンスから出る必要があります。

セキュリティ コンテキストのオーバーヘッドを防ぐ場合、またはセキュリティ コンテキストの使用を最小限に抑える場合、複数のブリッジグループを使用することがあります。ブリッジング機能はブリッジグループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバーまたは AAA サーバーの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジグループにして、セキュリティ コンテキストを使用します。

Cisco Security Manager 4.13 以降、ブリッジグループ仮想インターフェイス（BV） 機能がルーテッドファイアウォールモードに拡張されています。ルーテッドファイアウォールは、ブリッジグループを設定することによって実装されます。ユーザは、最大 8 つのブリッジグループを設定でき、ASA 9.7.1（Cisco Security Manager 4.13）では、各グループに最大 64 のインターフェイスを含めることができます。Cisco Security Manager 4.13 以前のバージョンでは、ユーザは最大 2 つのブリッジグループを設定できます。各グループには、最大 4 つのインターフェイスが含まれます。トランスペアレントモードでサポートされる BVI 機能に加えて、ルーテッド ファイアウォール モードには、次の追加の通信モードのサポートが含まれます。

- BVI 間通信
- BVI からデータポートへの通信（レイヤ 2 からレイヤ 3）およびその逆

トランスペアレントモードの FWSM 3.1 以降および ASA 8.4.1 以降のデバイスでは、[Interfaces] ページには [Interfaces] および [Bridge Groups] の 2 つのタブ付きパネルが表示されます。次の情報は [Bridge Groups] パネルと [Add Bridge Group] または [Edit Bridge Group] ダイアログボックスに適用されます。[Interfaces] パネルについては、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（PIX 7.0 以降/ASA/FPR/FWSM） （2380 ページ）を参照してください。

ナビゲーション パス

[ブリッジグループの追加（Add Bridge Group）] または [ブリッジグループの編集（Edit Bridge Group）] ダイアログボックスには、[インターフェイス（Interfaces）] ページの [ブリッジグループ（Bridge Groups）] パネルからアクセスできます。

関連項目

- ルーテッドモードおよびトランスペアレントモードのインターフェイス （2336 ページ）
- FWSM 3.1 のブリッジング サポート （2452 ページ）
- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）

フィールド リファレンス

表 *570 : [Add Bridge Group]/[Edit Bridge Group]* ダイアログボックス

要素	説明
[General] タブ	
ブリッジ グループ	このブリッジ グループの名前を入力します。

要素	説明
名前	このインターフェイスに最大 48 文字の ID を指定します。名前には、インターフェイスの用途に関係する覚えやすい名前を付けます。ただし、フェールオーバーを使用している場合は、フェールオーバー通信用に予約しているインターフェイスに名前を付けないでください。これには、フェールオーバー用に使用する EtherChannel およびそのメンバインターフェイスも含まれます。また、冗長インターフェイスペアのメンバとして使用するインターフェイスに名前を付けないでください。 セキュリティアプライアンスのインターフェイス命名ルールに従って、いくつかの名前が特定のインターフェイス用に予約されています。そのため、これらの予約名を使用すると、次のように、デフォルトの予約済みセキュリティ レベルが適用されます。 • [Inside]：内部ネットワークに接続します。最もセキュアなインターフェイスにする必要があります。 • [DMZ]：中間インターフェイスに接続された「緩衝地帯」。DMZ は境界ネットワークとも呼ばれます。DMZ インターフェイスに任意の名前を付けることができます。一般的に、DMZ インターフェイスには、インターフェイスタイプを識別するために「*DMZ*」というプレフィックスを付けます。 • [Outside]：外部ネットワークまたはインターネットに接続します。セキュア度の最も低いインターフェイスにする必要があります。 同様に、一般的にサブインターフェイス名には、一意の ID に加えて、関連付けられているインターフェイスも示されます。たとえば、*DMZoobmgmt* は、DMZ インターフェイスに接続されている Out of Band Management Network を示すことができます。 （注） この場合でも、**インターフェイスをフェールオーバー用または冗長インターフェイスのメンバーとして使用する場合は、そのインターフェイスに名前を付けないでください**。詳細については、冗長インターフェイスの設定 （2341 ページ）を参照してください。
ID	1 ～ 100 の整数でこのブリッジ グループの ID を入力します。
セキュリティ レベル（Security Level）	VLAN インターフェイスにセキュリティレベルを割り当てます。有効な値は 0 ～ 100 で、100 が最も安全です。

要素	説明
Available Interfaces	使用可能なインターフェイスまたはVLANのリストから選択して、このブリッジグループに割り当てます。使用可能なすべてのインターフェイスが一覧表示されます。 （注） ASA 9.7.1（Cisco Security Manager 4.13）以降、ブリッジグループごとに最大 64 のインターフェイスがサポートされます。
グループ内のメンバー（Members In Group）	現在のブリッジグループのインターフェイスの数を表示します
IP タイプ（IP Type）	インターフェイスの IP タイプを選択します。 • [スタティック IP（Static IP）]：ブリッジグループのインターフェイスに IP アドレスとサブネットマスクを割り当てます。 • [DHCP]： DHCP を使用して インターフェイスの IP アドレスを取得します。 • [DHCPを使用してデフォルトルートを取得する（Obtain Default Route using DHCP）]：選択すると、Cisco Security Manager は DHCP サーバーによって提供されるデフォルトルートを使用します。
IPアドレス	ブリッジ グループの管理 IP アドレスを入力または選択します。トランスペアレント ファイアウォールは、IP ルーティングに参加しません。したがって、ブリッジ グループに必要な IP 設定は、この管理 IP アドレスだけです。このアドレスは、システム メッセージや AAA サーバとの通信など、セキュリティ アプライアンスで発信されるトラフィックの送信元アドレスです。このアドレスは、リモート管理アクセスにも使用できます。 （注） IPv6 アドレスはブリッジ グループではサポートされていません。
ネットマスク	指定した IP アドレスのネットワーク マスク。値は、ドット区切り 10 進表記（255.255.255.0 など）で表すか、またはネットワーク マスクのビット数（24 など）を入力して表すことができます。 （注） ネットワークに接続するインターフェイスには 255.255.255.255 を使用しないでください。使用すると、トラフィックがこのインターフェイスで停止します。
説明	このブリッジ グループの説明（任意）を入力できます。
[IPv6] タブ	
IPv6を有効化（Enable IPv6）	IPv6 を有効化して、このブリッジグループで IPv6 アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると、このブリッジグループで IPv6 を無効化できますが、設定情報は保持されます。

要素	説明
Enforce EUI-64	オンにすると、ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用します。 このオプションがブリッジグループで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、ブリッジ グループ インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして検査されます。IPv6 パケットのインターフェイス ID が Modified EUI-64 形式でない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。 「%PIX|ASA-3-325003: EUI-64 source address check failed.」 アドレス形式の検証は、フローが作成された場合にのみ行われます。既存のフローからのパケットは確認されません。さらに、アドレス検証はローカル リンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗してドロップされます。これは、その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

要素	説明
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にブリッジ グループインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに0～600の数を入力します。0を入力すると、インターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカルアドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバルアドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカルアドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカルアドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

要素	説明
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。
管理対象設定フラグ	IPv6 ルータ アドバタイズメント パケットの「managed-config-flag」フラグを設定するかどうか。
その他の設定フラグ	IPv6 ルータ アドバタイズメント パケットの「other-config-flag」フラグを設定するかどうか。
Enable RA	オンにすると、インターフェイスで IPv6 ルータ アドバタイズメントの送信がイネーブルになります。次のオプションを使用できます。 • [RA Lifetime]：「ルータライフタイム」値は、ローカルリンク上のノードがセキュリティアプライアンスをリンク上のデフォルトルータと見なし続ける期間を指定します。有効な値の範囲は 0 ～ 9000 秒で、デフォルトは 1800 秒です。0 を入力すると、セキュリティ アプライアンスは選択したインターフェイスのデフォルト ルータとは見なされません。 0 以外の任意の値は、次の [RA Interval] 値より小さい値にはできません。 （注） この値は、このインターフェイスで送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。 • [RA Interval]：このインターフェイスでの IPv6 ルータアドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1800 秒です（次の [RA Interval in Milliseconds] オプションがオンの場合は 500 ～ 1800000 ミリ秒）。デフォルトは 200 秒です。 [RA Lifetime] が 0 以外の場合、送信の間隔は [RA Lifetime] の値以下にする必要があります。他の IPv6 ノードと同期しないようにするには、使用する実際値を必要値の 20 % 以内にランダムに調整します。 • [RA Interval in Milliseconds]：このオプションをオンにすると、指定した [RA Interval] の値が秒ではなくミリ秒になります。

要素	説明
Interface IPv6 Addresses	ダイアログボックスのこのセクションで、ブリッジ グループ インターフェイスに割り当てられている IPv6 アドレスを指定します。 • [Link-Local Address]：インターフェイスに自動的に生成されたリンクローカルアドレスを上書きするには、このフィールドに目的の IPv6 リンクローカルアドレスを入力します。 リンクローカル アドレスは、リンクローカル プレフィックス FE80::/64 と修正 EUI-64 形式のインターフェイス ID で形成されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンクローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラーが表示されます。 • [Enable Address Auto-Configuration]：ステートレス自動設定を使用して、インターフェイスで IPv6 アドレスの自動設定をイネーブルにするには、このオプションをオンにします。アドレスは、Router Advertisement（RA; ルータ アドバタイズメント）メッセージで受信されたプレフィックスに基づいて設定されます。リンクローカルアドレスが設定されていなければ、アドレスはこのインターフェイス用に自動的に生成されます。生成されたリンクローカルアドレスを別のホストが使用している場合は、エラーが発生されます。 • [Trust the DHCP Servers for default gateway]：このラジオボタンを選択して、信頼できる送信元（直接接続されたネットワーク）からのルータアドバタイズメントから、デフォルトのルートをインストールします。 • [Ignore trust and accept router advertisements]：このラジオボタンを選択して、別のネットワークからのルータアドバタイズメントから、デフォルトのルートをインストールします。 • このセクションのテーブルには、このインターフェイスに割り当てられている IPv6 アドレスが表示されます。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Address for Interface] ダイアログボックス （2417 ページ）が開きます。

要素	説明
Interface IPv6 Prefixes	このセクションのテーブルを使用して、IPv6 ルータ アドバタイズメントに含まれる IPv6 プレフィックス（つまり、IPv6 アドレスのネットワーク部分）を設定します。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Prefix Editor] ダイアログボックス （2419 ページ）が開きます。

高度なインターフェイス設定（PIX/ASA/FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

高度な設定オプションは、シングルコンテキストモードで動作している FWSM および ASA/PIX 7.0 以降のデバイスと、シングルコンテキストモードまたはマルチコンテキストモードで動作している ASA 9.0 以降のデバイス上のインターフェイスに使用可能です。

これらは全般的なデバイス関連設定です。つまり、個別のインターフェイスには適用されません。

（注） この項の情報は、PIX 6.3 デバイスにも、マルチコンテキスト モードのセキュリティ デバイスにも適用されません。

[Advanced Interface Settings] ダイアログボックスには、次の要素があります。

- [MACアドレス自動（MAC Address Auto）]：各共有コンテキスト インターフェイスにプライベート MAC アドレスを自動的に割り当てることができます。オプションで、MAC アドレスの一部として使用するユーザー定義のプレフィックスを設定できます。prefix は、0 ～ 65535 の 10 進数です。プレフィックスを入力しない場合、ASA によりデフォルトのプレフィックスが生成されます。このプレフィックスは、4 桁の 16 進数値に変換されます。プレフィックスにより、各 ASA は固有の MAC アドレスを使用（異なるプレフィックスの値を使用）することになるため、たとえば 1 つのネットワークセグメントに複数の ASA を配置できます。
- [同じセキュリティレベルのインターフェイス間でのトラフィック（Traffic between interfaces with same security levels）]：このパラメータでは、同じセキュリティレベルのインターフェイスとサブインターフェイス間の通信を制御します。同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。詳細については、同じセキュリティ レベルを持つインターフェイス間のトラフィックのイネーブル化 （2442 ページ）を参照してください。

- [PPPoEユーザー（PPPoE Users）] ボタン：このボタンをクリックして、[PPPoEユーザー（PPPoE Users）] ダイアログボックスを開きます。このダイアログボックスでは、PPPoE ユーザ リストの管理 （2443 ページ）で説明されているとおり、PPPoEユーザーを追加、編集、および削除できます。このオプションは、ASA および PIX 7.0 以降のデバイスでのみ使用できます。
- [VPDNグループ（VPDN Groups）]（PIX および ASA 7.2 以降）：このテーブルには、現在定義されている VPDN グループが一覧表示されます。テーブルの下にあるボタンは、VPDN グループの管理 （2444 ページ）の説明に従って、VPDN グループのエントリを追加、編集、および削除するために使用します。
- [LACPシステムプライオリティ（LACP System Priority）]（ASA 8.4.1 以降）：EtherChannel リンク集約に参加するすべてのシステムには、Link Aggregation Control Protocol（LACP）システムプライオリティが必要です。この値には 1 ～ 65535 を指定できます。数字が大きいほど、プライオリティは低くなります。デフォルトは 32768 です。

この値とシステムの MAC アドレスが組み合わされて、システムの LACP 識別子が形成されます。したがって、EtherChannel インターフェイスにのみ適用されます。詳細については、EtherChannel の設定 （2343 ページ）を参照してください。

（注） EtherChannel に割り当てられている個別のインターフェイスの [Edit Interface] ダイアログボックスでは、追加の LACP パラメータを使用できます。詳細については、EtherChannel に割り当てられているインターフェイスの LACP パラメータの編集 （2346 ページ）を参照してください。

（注） LACP システムプライオリティは、Cisco Firepower 9000 デバイスではサポートされていません。

- [スタティックポートプライオリティ（Static Port Priority）]（スパンドモードの ASA 9.2.1 以降のクラスタ）：LACP のダイナミック ポート プライオリティを無効にします。一部のスイッチはダイナミック ポート プライオリティをサポートしていないので、このパラメータによりスイッチの互換性が向上します。スタティック ポート プライオリティを有効にすると、16 のアクティブなスパンド EtherChannel メンバーのサポートが有効になります。このパラメータを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。このパラメータをイネーブルにした場合、スタンバイ メンバは使用できません。すべてのメンバがアクティブです。このパラメータは、ブートストラップ設定には含まれておらず、制御ユニットからメンバーユニットに複製されます。

（注） スタティック ポート プライオリティを有効にすると、8 ノードではなく 16 ノードをクラスタに含めることができます。

- [ディレクタのローカリゼーション（Director-Localization）]：複数のデータセンターサイトがサポートされている Geo クラスタリングでは、クラスタ間のラウンドトリップ時間（RTT）の待機時間が DC 内よりも長くなります。この遅延は、VoIP メディアストリームなどのアプリケーションのパフォーマンスに影響します。4.13 以降、ディレクタのローカリゼーションを使用して、RTT 遅延とパフォーマンス ルックアップ メッセージの遅延を最小限に抑えます。このオプションを有効にすると、フローの所有者とディレクタが同じ DC サイトに配置されるため、フローの所有者のルックアップはローカル DC サイトで実行され、トラフィックが同じサイト内で競合します。

（注） ディレクタのローカリゼーションは、Cisco Firepower 2100 シリーズ、Firepower 4000 シリーズ、および Firepower 9000 シリーズ デバイスではサポートされていません。

- [サイト冗長性の有効化（Enable Site Redundancy）]：4.16 以降、サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。サイトの冗長性は、制御ユニットでのみ有効にすることができ、クラスタグループのメンバーユニットに複製されます。接続バックアップオーナーがオーナーと同じサイトにある場合は、障害の発生しているサイトからフローを保護するために、追加のバックアップオーナーが別のサイトから選択されます。ディレクタ ローカリゼーションとサイトの冗長性は別々の機能です。そのうちの 1 つまたは両方を設定することができます。

（注） サイトの冗長性は、Cisco Firepower 2100 シリーズ、Firepower 4000 シリーズ、および Firepower 9000 シリーズ デバイスではサポートされていません。

ナビゲーション パス

[Advanced Interface Settings] ダイアログボックスは、[Interfaces] ページの下部にある [Advanced] ボタンをクリックすると開きます（5505 ASA 以外のデバイス、PIX 7.0 以降のデバイス、および FWSM）。また、ASA 5505 の [Ports] および [Interfaces] ページの [Interfaces] タブの下部にある [Advanced] ボタンをクリックすると開きます。

関連項目

- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）

同じセキュリティ レベルを持つインターフェイス間のトラフィックのイネーブル化

この項で説明するように、シングルコンテキストのセキュリティデバイスに表示される高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）ダイアログボックスには、[同じセキュリティレベルのインターフェイス間のトラフィック（Traffic between interfaces with the same security level）] ドロップダウンリストがあります。

デフォルトでは、同じセキュリティ レベルのインターフェイスまたはサブインターフェイスは、相互に通信できません。同じセキュリティ レベルのインターフェイス間で通信できるようにすると、次の利点が得られます。

- 101 より多い数の通信インターフェイスを設定できます。

インターフェイスごとに異なるレベルを使用し、同じセキュリティ レベルにインターフェイスを割り当てないようにすると、1 レベルにつき 1 つのインターフェイスしか設定できません（0 ～ 100）。

- アクセス リストを使用しないで、同じセキュリティ レベルのすべてのインターフェイス間でトラフィックを自由に通過させることができます。

（注） NAT 制御をイネーブルにしている場合、同じセキュリティ レベルのインターフェイス間で NAT を設定する必要はありません。

ステップ 1 [高度なインターフェイスの設定（Advanced Interface Settings）] ダイアログボックスで、このデバイスに [同じセキュリティ レベルのインターフェイス間のトラフィック（Traffic between interfaces with the same security level）] を処理させる方法を示すオプションを選択します。

- [無効（Disabled）]：同じセキュリティ レベルのインターフェイス間の通信を許可しません。
- [インターフェイス間（Inter-interface）]：同じセキュリティ レベルが設定されているインターフェイス間のトラフィック フローをイネーブルにします。このオプションをイネーブルにした場合、ファイアウォール デバイス内のインターフェイス間のトラフィック フローをイネーブルにするために変換ルールを定義する必要はありません。
- [インターフェイス内（Intra-interface）]：同じセキュリティ レベルが設定されているサブインターフェイス間のトラフィック フローをイネーブルにします。このオプションをイネーブルにした場合、インターフェイスに割り当てられているサブインターフェイス間のトラフィック フローをイネーブルにするために変換ルールを定義する必要はありません。
- [両方（Both）]：同じセキュリティ レベルのインターフェイスおよびサブインターフェイスで、インターフェイス内およびインターフェイス間の両方の通信を許可します。

ステップ 2 高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）の設定に進むか、または [OK] をクリックして [Advanced Interface Settings] ダイアログボックスを閉じます。

PPPoE ユーザ リストの管理

Point-to-Point Protocol over Ethernet（PPPoE）では、デバイス上のイーサネット インターフェイスを介して、セキュリティ デバイスと外部 ISP 間で標準の PPP 通信を実行できます。通信リンクを確立するには、デバイスで認証クレデンシャルを提供して、ネットワーク パラメータを取得する必要があります。これは、Virtual Private Dialup Network（VPDN; バーチャル プライ

ベート ダイヤルアップ ネットワーク）グループを使用することで実行されます。VPDN グループは、基本的には既定の PPPoE ユーザ クレデンシャル（ユーザ名およびパスワードなど）と認証プロトコルで構成されます。VPDN グループの詳細については、VPDN グループの管理（2444 ページ）を参照してください。

VPDN グループで使用できる PPPoE ユーザのクレデンシャルは、[PPPoE Users] ダイアログボックスに保持されます。このダイアログボックスには、高度なインターフェイス設定（PIX/ASA/FWSM）（2440 ページ）ダイアログボックスおよび [Add VPND Group] または [Edit VPND Group] ダイアログボックスからアクセスできます。

PPPoE ユーザの追加と編集

[PPPoE Users] ダイアログボックスには、標準の [Add Row]、[Edit Row]、および [Delete Row] ボタンとともに、現在定義されている PPPoE ユーザのテーブルが表示されます。[Add Row] ボタンをクリックすると [Add PPPoE User] ダイアログボックスが開き、[Edit Row] ボタンをクリックすると、実質的に同一の [Edit PPPoE User] ダイアログボックスが開きます。

次の PPPoE ユーザ パラメータを入力または編集してから、[OK] をクリックして [Add PPPoE User] または [Edit PPPoE User] ダイアログボックスを閉じ、[AdvancedInterface Settings] ダイアログボックスに戻ります。

（注） PPPoE ユーザ オプションは、Firewall Service Modules（FWSM; ファイアウォール サービス モジュール）では使用できません。

フィールド リファレンス

表 *571 : [Add PPPoE User]/[Edit PPPoE User]* ダイアログボックス

要素	説明
[ユーザー名（Username）]	このユーザーアカウントに割り当てられる名前。通常、外部 ISP によって提供されます。
パスワード	このユーザアカウントに割り当てられるパスワード。通常、外部 ISP によって提供されます。
確認（Confirm）	パスワードを再入力します。
Store Username and Password in Local Flash	オンにすると、この PPPoE ユーザ情報は、間違って上書きされないように、デバイスのローカルフラッシュメモリに保存されます。

VPDN グループの管理

Virtual Private Dialup Network（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）グループ（基本的には、既定の PPPoE ユーザと認証プロトコル）は、PPPoE 通信リンクを確

立してネットワーク パラメータを取得することを目的として、セキュリティ デバイスが外部 ISP にアクセスし、自分自身を認証するために使用します（PPPoE ユーザを確立する方法の詳細については、 PPPoE ユーザ リストの管理 （2443 ページ）を参照してください）。

使用可能な VPDN グループが [Advanced Interface Settings] ダイアログボックスに保持されます。このダイアログボックスは、高度なインターフェイス設定（PIX/ASA/FWSM） （2440 ページ）の説明に従って、[Interfaces] ページの下部にある [Advanced] ボタンをクリックすると開きます。

VPND グループの追加または編集

[Advanced Interface Settings] ダイアログボックスには、現在定義されている VPDN グループのテーブルと、標準の [Add Row]、[Edit Row]、および [Delete Row] ボタンがあります。[Add Row] ボタンをクリックすると [Add VPDN Group] ダイアログボックスが開き、[Edit Row] ボタンをクリックすると、実質的に同一の [Edit VPDN Group] ダイアログボックスが開きます。

次の PPPoE グループ パラメータを入力または編集してから、[OK] をクリックして [Add VPDN Group] または [Edit VPDN Group] ダイアログボックスを閉じ、[AdvancedInterface Settings] ダイアログボックスに戻ります。

（注） VPDN グループ オプションは、Firewall Service Modules（FWSM; ファイアウォール サービス モジュール）では使用できません。

フィールド リファレンス

表 *572 : [Add VPND Group]/[Edit VPND Group]* ダイアログボックス

要素	説明
グループ名（Group Name）	このグループを Security Manager 内で識別する最大 63 文字の名前。
PPPoE Username	このグループが ISP との認証に使用する PPPoE クレデンシャルを識別する名前。使用可能な PPPoE ユーザのリストから選択します。 このリストから [ユーザの編集（Edit User）] を選択して、[PPPoEユーザ（PPPoE Users）] ダイアログボックスを開きます。このダイアログボックスでは、このオプションのユーザを追加または編集できます。ユーザの作成および編集の詳細については、PPPoEユーザ リストの管理 （2443 ページ）を参照してください。

要素	説明
PPP Authentication	PPP 認証方式を選択します。 • [PAP]：パスワード認証プロトコル。クリアテキストでクレデンシャルを交換します。 • [CHAP]：チャレンジ ハンドシェイク認証プロトコル。暗号化されたクレデンシャルを交換します。 • [MSCHAP]：Microsoft 社の CHAP。バージョン 1 だけです。

VXLAN

仮想拡張 LAN（VXLAN）は、レイヤ 3 物理ネットワークの上のレイヤ 2 仮想ネットワークとして機能し、レイヤ 2 ネットワークを拡張します。VXLAN は、VLAN の場合と同じイーサネットレイヤ2ネットワークサービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1,600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

バージョン 4.9 以降、Security Manager は、バージョン 9.4(1) 以降の ASA、ASAv、および ASASM デバイスの VXLAN をサポートします。

（注） VxLAN は FWSM デバイスではサポートされていません。

VXLAN を設定するには、次の手順を実行します。

1. VXLAN ポリシーの設定 （2446 ページ）
2. VNI インターフェイスの設定 （2350 ページ）を作成し、設定された VXLAN ポリシーを VNI インターフェイスに関連付けます。

VXLAN ポリシーの設定

VXLAN を構成するには、最初に VXLAN ポリシーを設定してから VNI インターフェイスを作成し、設定された VXLAN ポリシーを VNI インターフェイスに関連付ける必要があります。ここでは、VXLAN ポリシーの設定方法について説明します。

ナビゲーション パス

VXLANページにアクセスするには、[デバイスビュー（Device View）]に移動し、ASA、ASAv、またはASASMデバイスを選択して、[ポリシー（Policies）]から[VxLAN]をクリックします。

関連項目

- VXLAN （2446 ページ）
- VNI インターフェイスの設定 （2350 ページ）

フィールド リファレンス

表 573 : VxLAN

要素	説明
VXLAN ポート番号の有効化 VxLAN 宛先ポート	[VXLAN宛先ポート（VXLAN Destination Port）] の値をデフォルト 4789 から変更する場合は、このチェックボックスをオンにします。オンにした場合、1024 ～ 65535 の範囲の数値を入力します。
ネットワーク仮想化エンドポイント（NVE）	
NVE の有効化	選択すると、VTEP トンネルインターフェイスを選択できます。
VXLAN NVE 番号	VXLAN NVE 番号の値は「1」です。この値は編集できません。
VxLan NVE または GENEVE カプセル化の有効化	[NVEカプセル化の有効化（Enable NVE Encapsulation）]：VXLANを使用してNVEカプセル化を有効にするには、このチェックボックスをオンにします。 [Genevеカプセル化の有効化（Enable Geneve Encapsulation）]：VXLANを使用してGeneveカプセル化を有効にするには、このオプションを選択します。
VTEP トンネルインターフェイス	[選択（Select）]をクリックして、VTEP トンネルインターフェイスを選択します。

要素	説明
VTEP IP アドレスまたはマルチキャスト トラフィック アドレスの有効化	次のいずれかを選択します。 • [ピアVTEP IPアドレス（Peer VTEP IP Address）]：ピア VTEP IP アドレスを手動で指定します。ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。VTEPには1つのピアのみを指定できます。ピア VTEP IP アドレスは VTEP トンネルインターフェイスから到達可能である必要があることに注意してください。そうでない場合、展開は失敗します。VXLAN ポリシーでピア IP アドレスを使用した場合、VNIインターフェイスを含む[インターフェイス（Interface）] ページでマルチキャスト IP アドレスを設定することはできません。 • [デフォルトマルチキャストIPアドレス（Default Multicast IP Address）]：関連するすべての VNI インターフェイスのデフォルト マルチキャスト グループを指定します。IP アドレスの有効な範囲は 224.0.0.0 ～ 239.255.255.255 です。VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。 • [Geneveポート番号の有効化（Enable Geneve Port Number）]：Geneve 宛先ポートの値を変更するには、このチェックボックスをオンにします。デフォルト値は 6081 です。1024 ～ 65535 の数値を入力します。 （注） デフォルトのポート番号 6081 の場合、CSM はデルタ設定を構築しません。
保存	[保存（Save）]をクリックして、VXLAN 設定を保存します。

第 47 章

ファイアウォール デバイスでのブリッジング ポリシーの設定

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2デバイスであり、接続されたデバイスへのルータホップとしては認識されません。セキュリティアプライアンスは、その内部および外部ポート上で同じネットワークを接続し、アクセス コントロール ブリッジとして機能します。各インターフェイスに異なる VLAN を割り当てます。IP アドレッシングは使用しません。

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- FWSM 3.1 のブリッジング サポート （2452 ページ）
- [ARP Table] ページ （2453 ページ）
- [ARP Inspection] ページ （2455 ページ）
- IPv6 ネイバー キャッシュの管理 （2457 ページ）
- [MAC Address Table] ページ （2458 ページ）
- [MAC Learning] ページ （2460 ページ）
- [Management IP] ページ （2461 ページ）
- [Management IPv6] ページ（ASA 5505） （2462 ページ）

ファイアウォール デバイスでのブリッジングについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように機能するレイヤ2デバイスであり、接続されたデバイスへのルータホップとしては認識されません。セキュリティアプライアンスは、その内部および外部ポート上で同じネットワークを接続し、アクセス コントロール ブリッジとして機能します。各インターフェイスに異なる VLAN を割り当てます。IP アドレッシングは使用しません。

このように、既存のネットワークに簡単にトランスペアレントファイアウォールを導入できます。IP の再アドレッシングは必要ありません。また、トラブルシューティングすべき複雑なルーティング パターンも NAT 設定もないため、メンテナンスが容易になります。

トランスペアレント モードのデバイスはブリッジとして機能しますが、IP トラフィックのようなレイヤ 3 トラフィックは、特別なアクセス ルールで明示的に許可しないかぎり、セキュリティ アプライアンスを通過できません。アクセス リストなしでファイアウォールを通過できるトラフィックは ARP トラフィックだけであり、このトラフィックは ARP インスペクションおよび IPv6 ネイバー探索を使用して制御できます。

セキュリティ アプライアンスがトランスペアレント モードで実行している場合、パケットの発信インターフェイスは、ルート ルックアップではなく MAC アドレス ルックアップを実行することによって決定されます。ルート ステートメントは引き続き設定可能ですが、セキュリティアプライアンスから発信されたトラフィックにだけ適用されます。たとえば、syslog サーバがリモート ネットワークに配置されている場合は、セキュリティ アプライアンスがそのサブネットにアクセスできるように、スタティック ルートを使用する必要があります。

Cisco Security Manager 4.13 以降、ブリッジグループ仮想インターフェイス（BV） 機能がルーテッドファイアウォールモードに拡張されています。ルーテッドファイアウォールは、ブリッジグループを設定することによって実装されます。ユーザは、最大 8 つのブリッジグループを設定でき、ASA 9.7.1（Cisco Security Manager 4.13）では、各グループに最大 64 のインターフェイスを含めることができます。Cisco Security Manager 4.13 以前のバージョンでは、ユーザは最大 2 つのブリッジグループを設定できます。各グループには、最大 4 つのインターフェイスが含まれます。トランスペアレントモードでサポートされる BVI 機能に加えて、ルーテッド ファイアウォール モードには、次の追加の通信モードのサポートが含まれます。

- BVI 間通信
- BVI からデータポートへの通信（レイヤ 2 からレイヤ 3）およびその逆

トランスペアレント ファイアウォールを設定するには、次のポリシーを使用します。マルチコンテキスト モードの ASA/PIX/FWSM デバイスを設定する場合は、トランスペアレントのセキュリティ コンテキストごとに次のポリシーを設定します。

- **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]**：アクセスルールは、拡張アクセスコントロールリストを使用して、レイヤ 3 以上のトラフィックを制御します。ルーテッド モードでは、一部のタイプのトラフィックは、アクセス リストで許可されていても、セキュリティアプライアンスを通過できません。たとえば、トランスペアレント ファイアウォールを介してルーティング プロトコルの隣接関係を確立できます。これにより、アクセス ルールに基づいて、OSPF、RIP、EIGRP、または BGP トラフィックの通過を許可できます。同様に、HSRP または VRRP のようなプロトコルもセキュリティアプライアンスを通過できます。ただし、トランスペアレント モードのセキュリティ アプライアンスは CDP パケットを通過させません。

トランスペアレントファイアウォールで直接サポートされていない機能については、上流および下流のルータでこれらの機能を提供できるように、トラフィックを通過させることがきます。たとえば、アクセス ルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックの通過を許可したり、IP/TV で作成されるようなマルチキャスト トラフィックの通過を許可したりできます。

詳細については、アクセス ルールについて （913 ページ）およびアクセス ルールの設定 （920 ページ）を参照してください。

- **[ファイアウォール（Firewall）] > [トランスペアレント ルール（Transparent Rules）]**：トランスペアレントルールは、Ethertype アクセスコントロールリストを使用して、非 IP のレイヤ 2 トラフィックを制御します。たとえば、AppleTalk、IPX、BPDU、および MPLS がデバイスを通過できるようにルールを設定できます。詳細については、トランスペアレント ファイアウォール ルールの設定 （1297 ページ）を参照してください。
- **[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [ARPテーブル（ARP Table）]**、[ARPインスペクション（ARP Inspection）] および [IPv6ネイバーキャッシュ（IPv6 Neighbor Cache）]：これらのポリシーを使用して、ブリッジを通過できる ARP および IPv6 トラフィックのタイプを制御します。必要に応じて、スタティックな ARP エントリおよび IPv6 ネイバー キャッシュ エントリを設定して、これらのスタティック ルールで定義されていないトラフィックをドロップできます。MAC アドレス、IP アドレス、またはインターフェイス間に不一致がある場合に、セキュリティ アプライアンスがパケットをドロップするように、ARP インスペクションをイネーブルにします。これによって、ARP スプーフィングを防ぐことができます。詳細については、[ARP Table] ページ （2453 ページ）および [ARP Inspection] ページ （2455 ページ）を参照してください。

（注） 非トランスペアレントの ASA/PIX/FWSM デバイスで使用できるブリッジング ポリシーは、[ARP Table] と [IPv6 Neighbor Cache] のみです。

- **[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [MACアドレステーブル（MAC Address Table）]** および [MACラーニング（MAC Learning）]：これらのポリシーを使用して、スタティックな MAC-IP アドレスマッピングを設定し、MAC 学習をイネーブルまたはディセーブルにします。MAC学習はデフォルトではイネーブルになっており、これによってアプライアンスは、トラフィックがインターフェイスを通過するときに MAC-IP アドレス マッピングを追加できます。スタティック エントリ以外のすべてのトラフィックを阻止する場合は、MAC 学習をディセーブルにできます。詳細については、[MAC Address Table] ページ （2458 ページ）および [MAC Learning] ページ （2460 ページ）を参照してください。
- [プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理IP（Management IP）]
- および [プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理IPv6（Management IPv6）]：これらのポリシーを使用して、Security Manager がデバイスとの通信に使用する管理 IP アドレスを設定します。

（注） [Management IP] ページおよび [Management IPv6] ページは Catalyst 6500 サービス モジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

管理 IP アドレスを変更する場合は、デバイスまたはセキュリティ コンテキストのデバイス プロパティも更新する必要があります。次の手順に従ってください。

- 管理 IP アドレスを変更し、変更を保存して送信します。
- 変更をデバイスに展開します。
- デバイスビューで、デバイスまたはセキュリティコンテキストを選択してから、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] を選択します。[General] ページで、新しい管理 IP アドレスを [IP Address] フィールドに入力します。[Credentials] タブで、管理インターフェイスにログインできるアカウントのクレデンシャルで、ユーザ名およびパスワードのフィールドを更新します。これで、Security Manager は、以降の展開およびデバイス通信に、このアドレスおよびユーザ アカウントを使用するようになります。

詳細については、[Management IP] ページ （2461 ページ）を参照してください。

関連項目

- FWSM 3.1 のブリッジング サポート （2452 ページ）
- ルーテッド モードおよびトランスペアレント モードのインターフェイス （2336 ページ）
- [Transparent Rules] ページ （1300 ページ）

FWSM 3.1 のブリッジング サポート

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

FWSM 3.1 では複数の L2 インターフェイスのペアをサポートできますが、Security Manager では 2 つの L2 インターフェイス（1 つのインターフェイス ペア）と、関連付けられた 1 つの管理 IP アドレスしか指定できません。つまり、関連付けられた 2 つの指定済みインターフェイスを含む 1 つのブリッジ グループだけが、管理 IP アドレスでプロビジョニングされます。デバイス設定に最大で 1 つのブリッジ グループと 2 つの指定済みインターフェイスが含まれている場合、このデバイス設定は検出対象になります。他のすべてのシナリオは、結果としてエラー メッセージが表示され、コマンドは検出時に拒否されます。さらに、検出では Security Manager にブリッジ グループ情報は表示されませんが、展開中にはブリッジ グループ コマンドが生成されます。ブリッジ グループがデバイス設定に存在しない場合、トランスペアレント ルール ポリシーでは、ブリッジ グループ 1 が展開および使用されます。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）

[ARP Table] ページ

[ARP Table] ページを使用して、MAC アドレスを IP アドレスにマッピングするスタティック ARP エントリを追加し、ホストに到達するために使用されるインターフェイスを識別します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [ARPテーブル（ARP Table）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [ARPテーブル（ARP Table）] を選択します。[ARPテーブル（ARP Table）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス （2454 ページ）
- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Inspection] ページ （2455 ページ）
- [MAC Address Table] ページ （2458 ページ）
- [MAC Learning] ページ （2460 ページ）
- [Management IP] ページ （2461 ページ）

フィールド リファレンス

表 *574 : [ARP Table]* ページ

要素	説明
タイムアウト（秒）	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間（60 ～ 4294967 秒）。デフォルトは 14400 秒です。 ARP テーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。 （注） タイムアウトはダイナミック ARP テーブルに適用されます。ARP テーブルに含まれているスタティックエントリではありません。
ARP テーブル	
インターフェイス	ホストが接続されるインターフェイス。

要素	説明
IPアドレス	ホストの IP アドレス。
MAC アドレス	ホストの MAC アドレス。
Alias Enabled	セキュリティ アプライアンスがこのマッピングのプロキシ ARP を実行するかどうかを示します。この設定がイネーブルにされ、指定したIPアドレスの ARP 要求をセキュリティ アプライアンスが受信した場合、セキュリティアプライアンスのMACアドレスで応答します。セキュリティアプライアンスは、このIPアドレスに属するホスト宛てのトラフィックを受信すると、このコマンドで指定したホストの MAC アドレスにそのトラフィックを転送します。この機能は、ARP を実行しないデバイスがある場合などに役立ちます。 （注） この設定は、トランスペアレント ファイアウォール モードでは無視され、セキュリティ アプライアンスはプロキシ ARP を実行しません。

[Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス

[Add ARP Configuration] と [Edit ARP Configuration] ダイアログボックスを使用して、MAC アドレスを IP アドレスにマッピングするスタティック ARP エントリを追加し、ホストに到達するために使用されるインターフェイスを識別します。

ナビゲーション パス

[Add/Edit ARP Configuration] ダイアログボックスには、[ARP Table] ページからアクセスできます。[ARP Table] ページの詳細については、を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Table] ページ （2453 ページ）

フィールド リファレンス

表 *575 : [Add/Edit ARP Configuration]* ダイアログボックス

要素	説明
インターフェイス（Interface）	ホスト ネットワークが接続されるインターフェイスの名前。
IPアドレス	ホストの IP アドレス。
MAC アドレス	ホストの MAC アドレス（00e0.1e4e.3d8b など）。

要素	説明
Enable Alias	選択すると、このマッピングのプロキシ ARP がイネーブルになります。指定した IP アドレスの ARP 要求をセキュリティ アプライアンスが受信した場合、セキュリティ アプライアンスの MAC アドレスで応答します。セキュリティ アプライアンスは、この IP アドレスに属するホスト宛てのトラフィックを受信すると、このコマンドで指定したホストの MAC アドレスにそのトラフィックを転送します。この機能は、ARP を実行しないデバイスがある場合などに役立ちます。 （注） この設定は、トランスペアレント ファイアウォール モードでは無視され、セキュリティアプライアンスはプロキシARPを実行しません。

[ARP Inspection] ページ

[ARP Inspection] ページを使用して、トランスペアレント ファイアウォールの ARP インスペクションを設定します。ARP インスペクションは、ARP スプーフィングを防ぐために使用されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [ARPインスペクション（ARP Inspection）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [ARPインスペクション（ARP Inspection）] を選択します。[ARPインスペクション（ARP Inspection）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス （2454 ページ）
- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Table] ページ （2453 ページ）
- [MAC Address Table] ページ （2458 ページ）
- [MAC Learning] ページ （2460 ページ）
- [Management IP] ページ （2461 ページ）

フィールド リファレンス

表 576 : [ARP Inspection] ページ

要素	説明
[ARP Inspection] テーブル	
インターフェイス	ARP インスペクション設定が適用されるインターフェイスの名前。
ARP Inspection Enabled	指定したインターフェイスでARPインスペクションをイネーブルにするかどうかを示します。
Flood Enabled	スタティック ARP エントリのどの要素とも一致しないパケットが、発信元インターフェイス以外のすべてのインターフェイスからフラッドされるかどうかを示します。MAC アドレス、IP アドレス、またはインターフェイス間に不一致がある場合、セキュリティアプライアンスはパケットをドロップします。このチェックボックスをオフにすると、すべての不一致パケットがドロップされます。 （注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

[Add/Edit ARP Inspection] ダイアログボックス

[Add/Edit ARP Inspection] ダイアログボックスを使用して、トランスペアレント ファイアウォール インターフェイスの ARP インスペクションをイネーブルまたはディセーブルにします。

ナビゲーション パス

[Add/Edit ARP Inspection] ダイアログボックスには、[ARP Inspection] ページからアクセスできます。[ARP Inspection] ページの詳細については、[ARP Inspection] ページ （2455 ページ）を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Inspection] ページ （2455 ページ）

フィールド リファレンス

表 *577 : [Add ARP Inspection]/[Edit ARP Inspection]* ダイアログボックス

要素	説明
インターフェイス（Interface）	ARP インスペクションをイネーブルまたはディセーブルにするインターフェイスの名前。
Enable ARP Inspection on this interface	選択すると、指定したインターフェイスで ARP インスペクションがイネーブルになります。
Flood ARP packets	選択すると、スタティック ARP エントリのどの要素とも一致しないパケットは、発信元インターフェイス以外のすべてのインターフェイスからフラッドされます。MAC アドレス、IP アドレス、またはインターフェイス間に不一致がある場合、セキュリティ アプライアンスはパケットをドロップします。このチェックボックスをオフにすると、すべての不一致パケットがドロップされます。 （注） 専用の管理インターフェイス（存在する場合）は、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

IPv6 ネイバー キャッシュの管理

[IPv6 Neighbor Cache] ページを使用して、MAC アドレスを IPv6 アドレスにマッピングするスタティック IPv6 ネイバー エントリを管理します。また、ネイバー ホストに到達するために使用されるインターフェイスを識別して、IPv6 のアドレス解決機能を提供します。これは ASA 7.0 以降のデバイスでのみ使用できます。

（注） IPv6 ネイバー キャッシュ エントリは IPv6 におけるスタティック ARP エントリに相当し、[ARP Table] ページ （2453 ページ）で管理されます。

指定された IPv6 アドレスのエントリがすでにネイバー探索キャッシュにある場合、つまり IPv6 ネイバー探索プロセスで取得されている場合、そのエントリは自動的にスタティック エントリに変換されます。IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

[IPv6 Neighbor Cache] ページは、Security Manager の標準のテーブルです。このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。[行の追加（Add Row）] ボタンでは [IPv6 ネイバーキャッシュ設定の追加（Add IPv6 Neighbor Cache Configuration）] ダイアログボックスが開き、[行の編集（Edit Row）] ボタンでは [IPv6 ネイバーキャッシュ設定の編集（Edit IPv6 Neighbor Cache Configuration）] ダイアログボックスが開きます。タイトルを除き、この 2 つのダイアログボックスは同じです。

（注） 必ず少なくとも 1 つのインターフェイスで IPv6 をイネーブルにしてからネイバーを追加します。

フィールド リファレンス

表 *578 : [Add Pv6 Neighbor Cache Configuration]/[Edit IPv6 Neighbor Cache Configuration]* ダイアログボックス

要素	説明
インターフェイス（Interface）	ネイバーを追加するインターフェイスの名前を入力または選択します。
IPアドレス	ローカルのデータリンク アドレスに対応する IPv6 アドレスを入力します（指定された IPv6 アドレスのエントリがすでにネイバー探索キャッシュにある場合、つまり IPv6 ネイバー探索プロセスで取得されている場合、そのエントリは自動的にスタティック エントリに変換されます）。
MAC アドレス	ホストのローカル データ回線（ハードウェア）の MAC アドレスを入力します（00e0.1e4e.3d8b など）。

[MAC Address Table] ページ

[MAC Address Table] ページを使用して、スタティック MAC アドレス エントリを MAC アドレス テーブルに追加します。このテーブルによって、MAC アドレスは送信元インターフェイスに関連付けられ、デバイスにアドレス指定されたパケットを正しいインターフェイスから送信することがセキュリティ アプライアンスで認識されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [MACアドレステーブル（MAC Address Table）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [MACアドレステーブル（MAC Address Table）] を選択します。[MACアドレステーブル（MAC Address Table）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add ARP Configuration]/[Edit ARP Configuration] ダイアログボックス （2454 ページ）

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Table] ページ （2453 ページ）
- [ARP Inspection] ページ （2455 ページ）
- [MAC Learning] ページ （2460 ページ）
- [Management IP] ページ （2461 ページ）

フィールド リファレンス

表 *579 : [MAC Address Table]* ページ

要素	説明
Aging Time (minutes)	MAC アドレス エントリがタイムアウトになるまでに MAC アドレス テーブル内に存在する時間を分（5 ～ 720（12 時間））で設定します。5 分がデフォルトです。
MAC アドレス テーブル	
インターフェイス	MAC アドレスを関連付けるインターフェイス。
MAC アドレス	MAC アドレス（00e0.1e4e.3d8b など）。

[Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックス

[Add MAC Table Entry] と [Edit MAC Table Entry] ダイアログボックスを使用して、スタティック MAC アドレス エントリを MAC アドレス テーブルに追加するか、MAC アドレス テーブル内のエントリを変更します。

ナビゲーション パス

[Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックスには、[MAC Address Table] ページからアクセスできます。[MAC Address Table] ページの詳細については、 [MAC Address Table] ページ （2458 ページ）を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [MAC Address Table] ページ （2458 ページ）

フィールド リファレンス

表 580 : [Add MAC Table Entry]/[Edit MAC Table Entry] ダイアログボックス

要素	説明
インターフェイス（Interface）	MACアドレスを関連付けるインターフェイス。
MAC アドレス	MAC アドレス（00e0.1e4e.3d8b など）。

[MAC Learning] ページ

[MAC Learning] ページを使用して、インターフェイスで MAC アドレス ラーニングをイネーブルまたはディセーブルにします。デフォルトでは、各インターフェイスで入力トラフィックの MAC アドレスが学習され、対応するエントリがセキュリティ アプライアンスによって MAC アドレス テーブルに追加されます。必要な場合は、MAC アドレス ラーニングをディセーブルにすることができます。ただし、MAC アドレスをスタティックにテーブルに追加しないかぎり、トラフィックはセキュリティ アプライアンスを通過できません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [MAC ラーニング（MAC Learning）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [MAC ラーニング（MAC Learning）] を選択します。[MAC インスペクション（MAC Inspection）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Add MAC Learning]/[Edit MAC Learning] ダイアログボックス （2461 ページ）
- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Table] ページ （2453 ページ）
- [ARP Inspection] ページ （2455 ページ）
- [MAC Address Table] ページ （2458 ページ）
- [Management IP] ページ （2461 ページ）

フィールド リファレンス

表 *581 : [MAC Learning]* ページ

要素	説明
MAC Learning Table	
インターフェイス	MAC 学習設定を適用するインターフェイス。
MAC Learning Enabled	セキュリティ アプライアンスがインターフェイスに入るトラフィックから MAC アドレスを学習するかどうかを示します。

[Add MAC Learning]/[Edit MAC Learning] ダイアログボックス

[Add MAC Learning] と [Edit MAC Learning] ダイアログボックスを使用して、インターフェイスで MAC アドレス ラーニングをイネーブルまたはディセーブルにします。

ナビゲーション パス

[Add/Edit MAC Learning] ダイアログボックスには、[MAC Learning] ページからアクセスできます。[MAC Learning] ページの詳細については、[MAC Learning] ページ （2460 ページ）を参照してください。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [MAC Learning] ページ （2460 ページ）

フィールド リファレンス

表 *582 : [Add MAC Configuration]/[Edit MAC Configuration]* ダイアログボックス

要素	説明
インターフェイス（Interface）	MAC 学習設定を適用するインターフェイス。
MAC Learning Enabled	選択すると、セキュリティ アプライアンスはインターフェイスに入るトラフィックから MAC アドレスを学習します。

[Management IP] ページ

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。デバイスに必要な IP 設定は、管理 IP アドレスの指定のみです。管理 IP アドレスは、システム メッセージや AAA サーバとの通信など、デバイスで発信されるトラフィックの送信元アドレスとして使用されます。このアドレスは、リモート管理アクセスにも使用できます。

IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、管理 IP アドレスが必要です。

（注） デバイスの管理 IP アドレスに加えて、Management 0/0 または 0/1 の管理専用インターフェイスの IP アドレスを設定できます。この IP アドレスは、メインの管理 IP アドレスとは別のサブネットに設定できます。

[Management IP] ページを使用して、セキュリティ デバイスの管理 IP アドレス、またはトランスペアレント ファイアウォール モードのコンテキストの管理 IP アドレスを設定します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理IP（Management IP）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [管理IP（Management IP）] を選択します。[管理IP（Management IP）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Table] ページ （2453 ページ）
- [ARP Inspection] ページ （2455 ページ）
- [MAC Address Table] ページ （2458 ページ）
- [MAC Learning] ページ （2460 ページ）

フィールド リファレンス

表 583 : [Management IP] ページ

要素	説明
管理 IP アドレス（Management IP Address）	管理 IP アドレス。
サブネットマスク	管理 IP アドレスに対応するサブネット マスク。

[Management IPv6] ページ（ASA 5505）

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。デバイスに必要な IP 設定は、管理 IP アドレスの指定のみです。管理 IP アドレスは、システム メッセージや

AAA サーバとの通信など、デバイスで発信されるトラフィックの送信元アドレスとして使用されます。このアドレスは、リモート管理アクセスにも使用できます。

IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカル アドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。グローバルアドレスを設定する場合、各インターフェイスにリンクローカル アドレスが自動的に設定されるため、特にリンクローカルアドレスを設定する必要はありません。ただし、グローバル管理アドレスを設定しない場合、IPv6インターフェイスの設定（ASA/FWSM）（2409ページ）の説明に従って、インターフェイス リンクローカル アドレスを設定する必要があります。1 つのデバイスには IPv6 管理アドレスと IPv4 管理アドレスの両方を設定できます。

トランスペアレント モードの ASA 5505 では、[Management IPv6] ページを使用して IPv6 をイネーブルにし、ネイバー送信要求を設定して、IPv6インターフェイスアドレスを管理します。

（注） このページは、トランスペアレント モードの ASA 5505 バージョン 8.2 および 8.3 のデバイスでのみ使用できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ブリッジング（Bridging）] > [管理 IPv6（Management IPv6）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ブリッジング（Bridging）] > [管理 IPv6（Management IPv6）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ファイアウォール デバイスでのブリッジングについて （2449 ページ）
- [ARP Table] ページ （2453 ページ）
- [ARP Inspection] ページ （2455 ページ）
- [MAC Address Table] ページ （2458 ページ）
- [MAC Learning] ページ （2460 ページ）

フィールド リファレンス

表 *584 : [Management IPv6]* ページ

要素	説明
IPv6を有効化（Enable IPv6）	IPv6 をイネーブルにして、IPv6 管理インターフェイス アドレスを設定するには、このチェックボックスをオンにします。このオプションをオフにすると IPv6 をディセーブルにできますが、設定情報は保持されます。
DAD Attempts	Duplicate Address Detection（DAD; 重複アドレス検出）の実行中にインターフェイスで送信される連続ネイバー送信要求メッセージの数を指定するには、このフィールドに 0 ～ 600 の数を入力します。0 を入力すると、重複アドレス検出がディセーブルになります。1 を入力すると、フォローアップ送信のない一度の送信を設定します。これはデフォルトです。 アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。 重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカルアドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。 %PIX-4-DUPLICATE: Duplicate address FE80::1 on outside 重複アドレスがインターフェイスのグローバルアドレスの場合は、そのアドレスは使用されず、前述のリンクローカル アドレスと同様のエラー メッセージが発行されます。 重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。インターフェイスのリンクローカルアドレスに変更があると、新しいリンクローカルアドレスに対して重複アドレス検出が行われ、そのインターフェイスに関連付けられている他のすべての IPv6 アドレスが再生成されます（つまり、重複アドレス検出は、新しいリンクローカルアドレスでのみ行われます）。
NS Interval	IPv6 ネイバー送信要求メッセージの再送信間隔（ミリ秒単位）。有効な値の範囲は 1000 ～ 3600000 ミリ秒で、デフォルト値は 1000 ミリ秒です。

要素	説明
Reachable Time	リモート IPv6 ノードが到達可能であることが最初に確認されてから、このノードが到達可能であると見なされ続ける時間（ミリ秒単位）。有効な値の範囲は 0 ～ 3600000 ミリ秒で、デフォルト値は 0 です。この値に 0 を使用する場合、到達可能時間は未定に設定されます。つまり、到達可能時間の設定および追跡は受信デバイス次第です。 設定時間によって、使用不可のネイバーを検知できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。
Interface IPv6 Addresses	このテーブルに一覧表示される管理インターフェイスに割り当てられている IPv6 アドレス。このテーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。 [Add Row] および [Edit Row] を使用すると、[IPv6 Address for Interface] ダイアログボックス （2417 ページ）が開きます。

第 48 章

ファイアウォール デバイスでのデバイス管理ポリシーの設定

[Device Admin] セクションには、ファイアウォール デバイスのデバイス管理ポリシーを設定するページが含まれています。

この章は次のトピックで構成されています。

- セキュリティ デバイスでの AAA について （2467 ページ）
- バナーの設定 （2478 ページ）
- [Boot Image/Configuration] の指定 （2479 ページ）
- CLI プロンプトの設定 （2481 ページ）
- デバイス クロックの設定 （2483 ページ）
- FIPS の有効化/無効化 （2485 ページ）
- Cisco Success Network の有効化 （2486 ページ）
- Umbrella グローバルポリシーの設定 （2487 ページ）
- デバイス クレデンシャルの設定 （2488 ページ）
- マウント ポイントの管理 （2491 ページ）
- IP クライアント （2494 ページ）
- アプリケーション エージェント （2495 ページ）

セキュリティ デバイスでの AAA について

認証、許可、アカウンティング（AAA）によって、セキュリティ アプライアンスは、ユーザがだれか（認証）、ユーザは何を実行できるか（認可）、ユーザは何を実行したか（アカウンティング）を特定できます。認証は、単独で使用することも、認可およびアカウンティングとともに使用することもできます。認可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングもまた、単独で使用することも、認証および認可とともに使用することもできます。

認証、許可、アカウンティングでは、ユーザ アクセスに関して、アクセス リストだけを使用する場合よりも、さらに高度な保護および制御が実現されます。たとえば、すべての外部ユーザに DMZ ネットワーク上のサーバにある Telnet へのアクセスを許可する ACL を作成できま

すが、サーバへのユーザ アクセスを制限する場合に、これらのユーザの IP アドレスが常に認識できるわけではないときには、AAA をイネーブルにして、認証されたユーザか認可されたユーザ、またはその両方だけにセキュリティ アプライアンスを通過させることができます（Telnet サーバも認証を強制します。セキュリティ アプライアンスは非認可ユーザがサーバにアクセスしようとするのを防ぎます）。

- **認証**：認証は、ユーザー ID に基づいてアクセスを付与します。認証は、一般的にユーザ名とパスワードからなる有効なユーザ クレデンシャルを要求することによってユーザ ID を確立します。次の項目を認証するように、セキュリティ アプライアンスを設定できます。
  - Telnet、SSH、HTTPS/ASDM、またはシリアル コンソールを使用した、セキュリティ アプライアンスへの管理接続
  - **enable** コマンド。
- **認可**：認可は、認証された後のユーザーの能力を制御します。許可は、認証された個々のユーザが使用できるサービスおよびコマンドを制御します。認可をイネーブルにしなかった場合、認証が単独で、すべての認証済みユーザに対して同じサービス アクセスを提供します。

許可で提供される制御を必要とする場合は、広範な認証ルールを設定してから、詳細な許可を設定できます。たとえば、外部ネットワーク上の任意のサーバにアクセスしようとする内部ユーザを認証してから、認可を使用して、特定のユーザがアクセスできる外部サーバを制限できます。

セキュリティ アプライアンスはユーザごとに最初の 16 個の認可要求をキャッシュします。そのため、ユーザが現在の認証セッション中に同じサービスにアクセスする場合、セキュリティ アプライアンスは要求を認可サーバに再送信しません。

- **アカウンティング**：アカウンティングはセキュリティアプライアンスを通過するトラフィックを追跡して、ユーザーアクティビティのレコードを提供します。トラフィックの認証をイネーブルにすると、ユーザごとにトラフィックをアカウンティングできます。トラフィックを認証しない場合は、IP アドレスごとにトラフィックをアカウンティングできます。アカウンティング情報には、セッションの開始および停止時間、ユーザ名、セッション中にセキュリティ アプライアンスを通過したバイト数、使用したサービス、および各セッションの持続時間が含まれます。

AAA の準備

AAA サービスは、ローカル データベースまたは 1 つ以上の AAA サーバの使用に依存します。また、ローカル データベースを AAA サーバによって提供される大多数のサービスのフォールバックとして使用することもできます。AAA を実装する前に、ローカル データベースを設定し、AAA サーバ グループおよびサーバを設定する必要があります。

ローカル データベースおよび AAA サーバの設定は、セキュリティ アプライアンスにサポートさせる AAA サービスによって異なります。AAA サーバを使用するかどうかに関係なく、管理アクセスをサポートするユーザ アカウントでローカル データベースを設定して予想外のロッ

クアウトを防いだり、また必要であれば、AAA サーバが到達不能のときにフォールバック方式を提供したりする必要があります。詳細については、ユーザアカウントの設定 （2588 ページ）を参照してください。

次の表に、AAA サービスのサポートの概要を AAA サーバタイプ別およびローカルデータベース別に示します。ローカルデータベースは、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** ページでユーザーアカウントを設定することによって管理します（ユーザ アカウントの設定 （2588 ページ）を参照）。[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA] ページを使用して、AAA サーバーグループを確立し、個々の AAA サーバーをサーバーグループに追加します。

表 *585 : AAA* サポートの要約

AAA サービス	データベース タイプ							
	Local	RADIUS	TACACS+	SDI	NT	Kerberos	LDAP	HTTP Form
認証								
VPN ユーザ	対応	対応	対応	対応	対応	対応	対応	○ 1
ファイアウォールセッション	対応	対応	対応	×	×	×	×	×
管理者	対応	対応	対応	×	×	×	×	×
許可								
VPN ユーザ	対応	対応	×	×	×	×	対応	×
ファイアウォールセッション	なし	はい 2	対応	×	×	×	×	×
管理者	はい 3	×	対応	×	×	×	×	×
アカウンティング								
VPN 接続	×	対応	対応	×	×	×	×	×
ファイアウォールセッション	×	対応	対応	×	×	×	×	×
管理者	×	対応	対応	×	×	×	×	×

1 HTTP Form プロトコルは、WebVPN ユーザだけを対象にしたシングル サインオン認証をサポートします。

2 ファイアウォールセッションでは、RADIUS 認可はユーザ固有の ACL でだけサポートされ、ユーザ固有の ACL は RADIUS 認証応答で受信または指定されます。

3 ローカル コマンド認可は、権限レベルでだけサポートされます。

ローカル データベース

セキュリティ アプライアンスにより、ユーザ アカウントを入力できるローカル データベースが保持されます。ユーザアカウントには、最低でもユーザ名が含まれます。一般的には、パスワードおよび権限レベルを各ユーザ名に割り当てますが、パスワードは任意です。ローカル ユーザーアカウントは、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** ページで管理できます（ユーザ アカウントの設定（2588 ページ）を参照）。

ローカル データベースを使用してコマンド認可をイネーブルにすると、セキュリティ アプライアンスは割り当て済みのユーザ権限レベルを参照して、どのコマンドが使用可能かを判断します。デフォルトでは、すべてのコマンドに権限レベル 0 またはレベル 15 のどちらかが割り当てられます。

（注） CLI へのアクセスは許可するが、特権モードには入れないようにするユーザをローカル データベースに追加する場合は、コマンド認可をイネーブルにする必要があります。コマンド認可がない場合、ユーザの特権レベルが 2 以上（2 がデフォルト）あると、ユーザは自身のパスワードを使用して、CLI で特権モード（およびすべてのコマンド）にアクセスできます。また、ユーザがログイン コマンドを使用できないように、コンソール アクセスに対して RADIUS または TACACS+ 認証を使用することや、システムのイネーブル パスワードを使用して特権モードにアクセスできるユーザを制御できるように、すべてのローカル ユーザをレベル 1 に設定することもできます。

ローカル データベースはネットワーク アクセス認可には使用できません。

ローカル データベースのユーザ アカウントによって、コンソールとイネーブル パスワードの認証、コマンド認可、および VPN 認証と認可のフォールバック サポートが提供されます。この動作は、セキュリティ アプライアンスからの予想外のロックアウトを防ぐように設計されています。

フォールバック サポートを必要とするユーザについては、ローカル データベース内のユーザ名およびパスワードと、AAA サーバ上のユーザ名およびパスワードとを一致させることを推奨します。これにより、トランスペアレント フォールバック サポートが提供されます。ユーザは、サービスを提供しているのが AAA サーバなのかローカル データベースなのかを判断できないため、AAA サーバでローカルデータベースのユーザ名およびパスワードとは異なるユーザ名およびパスワードを使用するということは、どちらのユーザ名およびパスワードを提供する必要があるのかがユーザにはわからないということになります。

マルチコンテキストモードの場合、システム実行スペースでユーザー名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する **aaa** コマンドは設定できません。

（注） VPN 機能は、マルチ モードではサポートされません。

デバイス管理用の AAA

セキュリティ アプライアンスに対する次のすべての管理接続を認証できます。

- [Telnet]
- SSH
- シリアル コンソール
- ASDM
- VPN 管理アクセス

また、イネーブル モードに入ろうとする管理者も認証できます。管理コマンドを認可できます。管理セッションおよびセッション中に発行されたコマンドのアカウンティング データをアカウンティング サーバに送信させることができます。

[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA] ページを使用すると、AAA をデバイス管理用に設定できます（セキュリティ デバイスでの AAA について（2467 ページ）を参照）。

ネットワーク アクセス用の AAA

[ファイアウォール（Firewall）] > [AAAルール（AAA Rules）] ページ（ファイアウォール AAA ルールの管理（869 ページ）を参照）を使用すると、ファイアウォールを通過するトラフィックの認証、許可、アカウンティングのルールを設定できます。作成するルールはアクセス ルールと同様ですが、定義済みのトラフィックに対して認証、許可、またはアカウンティングを行うかどうか、および AAA サービス要求を処理するためにセキュリティ アプライアンスが使用する AAA サーバ グループを指定する点だけが異なります。

VPN アクセス用の AAA

VPN アクセス用の AAA サービスには次のものがあります。

- ユーザーを VPN グループに割り当てるためのユーザーアカウント設定。**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** ページで設定します（ユーザ アカウントの設定 （2588 ページ）を参照）。
- 多数のユーザーアカウントまたはトンネルグループによって参照される可能性がある VPN グループポリシー。**[ユーザーアカウントVPN（Remote Access VPN）] > [RA VPNポリシー（RA VPN Policies）] > [ユーザーグループポリシー（User Group Policy）]** または **[サイト間VPN（Site to Site VPN）] > [ユーザーグループポリシー（User Group Policy）]** ページで設定します。
- トンネルグループポリシー。**[リモートアクセスVPN（Remote Access VPN）] > [RA VPNポリシー（RA VPN Policies）] > [PIX7.0/ASAトンネルグループポリシー（PIX7.0/ASA Tunnel Group Policy）]** または **[サイト間VPN（Site to Site VPN）] > [PIX7.0/ASAトンネルグループポリシー（PIX7.0/ASA Tunnel Group Policy）]** ページで設定します。

[AAA] の [Authentication] タブの設定

[AAA] ページには 3 つのタブ付きパネルがあり、[AAA] ページに移動すると、[認証（Authentication）] パネルが表示されます。これらのオプションを使用して、デバイス コンソールへの権限付きアクセスを制御し、接続タイプによってアクセスを制限し、アクセス メッセージを定義します。

[Authorization] タブ （2475 ページ）を使用して、認証されたユーザーが使用できるサービスとコマンドを制御します。

[Accounting] タブ （2476 ページ）を使用して、コンソール トラフィックのトラッキングをアクティブにして、ユーザ アクティビティを記録します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- セキュリティ デバイスでの AAA について （2467 ページ）
- ユーザ アカウントの設定 （2588 ページ）

[Authentication] タブの使用

[Authentication] タブを使用して、セキュリティ アプライアンスへの管理者アクセスの認証をイネーブルにします。[Authentication] タブでは、AAA サーバによって認証されたときにユーザに表示されるプロンプトとメッセージを設定することもできます。

コマンドを入力する前に、デバイスによってユーザ名とパスワードの入力を求められます。認証サーバがオフラインの場合は、コンソールのログイン要求がタイムアウトになるまで待機します。そのあとで、ファイアウォールのユーザ名とイネーブル パスワードでコンソールにアクセスできます。

フィールド リファレンス

表 586 : [Authentication] タブ

要素	説明
Require AAA Authentication to allow use of privileged commands	

要素	説明
有効	ファイアウォール上で EXEC モードでのアクセスをユーザーに許可するために、AAA サーバーからの認証を要求します。このオプションは、ファイアウォール コンソールへのアクセス試行を3回まで許可します。この数を超えた場合、「アクセスが拒否されました」というメッセージが表示されます。 オンにすると、[Server Group] フィールドがイネーブルになります。
Server Group	ユーザ認証のために接続する AAA サーバの名前を入力または選択します。
Use LOCAL when server group fails	選択したサーバで障害が発生した場合に、バックアップとしてローカル データベースを使用するには、このチェックボックスをオンにします（[Server Group] を指定しないと、このオプションはイネーブルにはなりません）。
Require AAA Authentication for the following types of connections	
認証を必要とする接続を選択します。各タイプで、ファイアウォール コンソールへのアクセス試行は 3 回まで許可されます。この数を超えた場合、「アクセスが拒否されました」というメッセージが表示されます。 次の接続オプションをそれぞれ個別に選択します。 • [HTTP]：ユーザーがファイアウォール コンソールへの HTTPS 接続を開始するときに AAA 認証を必要とします。 • [シリアル（Serial）]：ユーザーがシリアルコンソールケーブルを介してファイアウォールコンソールへの接続を開始するときに AAA 認証を必要とします。 • [SSH]：ユーザーがコンソールへのセキュアシェル（SSH）接続を開始するときに AAA 認証を必要とします。 • [Telnet]：ユーザーがファイアウォールコンソールへの Telnet 接続を開始するときに AAA 認証を必要とします。 選択した各接続で、[Server Group] を指定して、ローカルデータベースをバックアップとして使用するかどうかを指定します。 • [サーバーグループ（Server Group）]：ユーザー認証のために接続する AAA サーバーの名前を入力または選択します。 • [サーバーグループに障害が発生した場合はローカルを使用（Use LOCAL when server group fails）]：選択したサーバーに障害が発生した場合に、ローカルデータベースをバックアップとして使用するには、このチェックボックスをオンにします。（[Server Group] を指定しないと、このオプションはイネーブルにはなりません）。	

要素	説明
Authentication Prompts	
Login Prompt	セキュリティ アプライアンスにログインするときにユーザに表示されるプロンプトを入力します。
Accepted Message	正常に認証されたときに表示されるメッセージを入力します。
Rejected Message	何らかの理由で認証が失敗したときに表示されるメッセージを入力します。
Rejected Message for Invalid Credentials	不明または無効なクレデンシャルを入力したために認証が失敗したときに表示されるメッセージを入力します。 FWSM 3.2 以降のデバイスでのみ使用できます。
Rejected Message for Expired Password	期限が切れたパスワードを入力したために認証が失敗したときに表示されるメッセージを入力します。 FWSM 3.2 以降のデバイスでのみ使用できます。
Maximum Local Authentication Failed Attempts	アカウントがロックされる前に、デバイスがローカルデータベースでユーザの認証を試行する回数を指定します。有効な値は 1 ～ 16 です。 ASA/PIX 7.01 以降と FWSM 3.11 以降のデバイスでのみ使用できます。
ログイン履歴	ログイン履歴レポート機能を有効にするには、このチェックボックスをオンにします。有効にすると、ログインに成功した直後に、すべての管理ログイン試行に関する情報が収集され、ASA に表示されます。これには次の情報が含まれます。 • 最後にログインが試行された日時 • 最後にログインした場所（端末または IP アドレス） • 最後に成功したログイン以降の失敗したログイン試行の回数。 • 組織が定義した期間中に発生した、成功したログイン試行の数。 （注） この機能はデフォルトでイネーブルになっています。

要素	説明
期間（Duration）（任意）	ログインイベントを保存する日数を入力します。ここで値を指定しない場合、ログイン履歴は無制限になります。 （注）　デフォルト値は 90 日です。

[Authorization] タブ

[Authorization] タブでは、ファイアウォール コマンドにアクセスするための認可を設定できます。

ナビゲーション パス

[Authorization] タブには [AAA] ページからアクセスできます。[AAA] の [Authentication] タブの設定 （2472 ページ）を参照してください。

関連項目

- セキュリティ デバイスでの AAA について （2467 ページ）
- [Accounting] タブ （2476 ページ）

フィールド リファレンス

表 587 : [Authorization] タブ

要素	説明
Enable Authorization for Command Access Server Group Use LOCAL when server group fails	ファイアウォール コマンドにアクセスするために認可を必要とします。 認可に使用するサーバ グループを指定します。 選択したサーバ グループで障害が発生した場合に、LOCAL サーバ グループを使用します。
execシェルアクセスの承認の有効化（Enable Authorization for exec shell access） (ASA 8.0(2) 以降のみ)	選択すると、管理許可が有効になります。 管理許可を有効にしたら、認証にリモートサーバーを使用するか、ローカルデータベースを使用するかを指定します。 • [ローカルサーバー（Local Server）]：ローカルユーザーのデータベースは、入力したユーザー名と割り当てられた Service-Type および Privilege-Level 属性のソースとなります。 • [リモートサーバー（Remote Server）]：認証と許可の両方に同じサーバーが使用されます。

要素	説明
execシェルアクセスの承認の自動有効化（Auto Enable Authorization for exec shell access） （ASA 9.1(5) 以降のみ）	十分な権限を有するユーザーは、ログイン認証サーバーから特権EXECモードに直接入れます。それ以外では、ユーザはユーザEXECモードになります。これらの特権は、各EXECモードに入るために必要なService-TypeおよびPrivilege-Level属性で決定されます。特権 EXEC モードを開始するには、ユーザは Administrative の Service-Type 属性およびそれらに割り当てられた 1 以上の Privilege Level 属性を有している必要があります。 このオプションは、システム コンテキストではサポートされていません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はスイッチからASASMへのセッションにも適用されます。
HTTP接続の承認の有効化（Enable Authorization for HTTP Connection） Server Group Use LOCAL when server group fails （ASA 9.4(1) 以降のみ）	選択すると、HTTP による認証が有効になります。ユーザー名の認証はデフォルトで無効になっています。 承認に使用するサーバーグループを選択します。 選択したサーバ グループで障害が発生した場合に、LOCAL サーバ グループを使用します。

[Accounting] タブ

[Accounting] タブを使用して、ファイアウォール デバイスへのアクセスおよびデバイス上のコマンドへのアクセスのアカウンティングをイネーブルにします。

ナビゲーション パス

[Accounting] タブには [AAA] ページからアクセスできます。 [AAA] の [Authentication] タブの設定 （2472 ページ）を参照してください。

関連項目

- セキュリティ デバイスでの AAA について （2467 ページ）
- [Authorization] タブ （2475 ページ）

フィールド リファレンス

表 588 : [Accounting] タブ

要素	説明
Require AAA Accounting for privileged commands	

要素	説明
有効	選択すると、コンソールによる管理アクセス用の特権モードの開始と終了を示すアカウンティング レコードの生成がイネーブルになります。
Server Group	アカウンティング レコードが送信されるサーバか、RADIUS または TACACS+ サーバのグループを指定します。
Require AAA Accounting for the following types of connections	
接続タイプ	アカウンティング レコードを生成する接続タイプを指定します。 • HTTP：HTTP で作成される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。 • シリアル：コンソールへのシリアルインターフェイス経由で確立される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。 • SSH：SSHで作成される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。 • Telnet：Telnet で作成される管理セッションの確立と終了を示すアカウンティングレコードの生成を有効または無効にします。有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。
Server Group	アカウンティング レコードが送信されるサーバか、RADIUS または TACACS+ サーバのグループを指定します。
Require Accounting for command access	
有効	選択すると、管理者/ユーザによって入力されたコマンドのアカウンティング レコードの生成がイネーブルになります。
Server Group	アカウンティング レコードが送信されるサーバか RADIUS または TACACS+ サーバのグループを選択できるドロップダウン メニューが表示されます。
特権レベル	アカウンティング レコードを生成するために、コマンドに関連付けられている必要がある最小権限レベル。デフォルトの特権レベルは 0 です。

バナーの設定

[バナー（Banner）] ページを使用して、セキュリティアプライアンスまたは共有ポリシーの [セッション（exec）（Session (exec)）]、[ログイン（Login）]、および [本日のメッセージ（motd）（Message-of-the-Day (motd)）] のバナーを指定できます。

（注） バナーでトークン $(hostname) または $(domain) を使用すると、これらはセキュリティ アプライアンスのホスト名またはドメイン名に置き換えられます。コンテキスト設定で $(system) トークンを入力した場合、コンテキストはシステム設定で設定されているバナーを使用します。

バナーテキストのスペースは保持されますが、タブは入力できません。複数行のバナーを作成するには、追加する行ごと個別のテキスト行を入力します。各行は既存のバナーの末尾に追加されます。行が空の場合は、Carriage Return（CR; 復帰）がバナーに追加されます。

メモリおよびフラッシュ メモリの制限以外に、バナーの長さに制限はありません。使用できるのは、改行（Enter キーを押す）を含む ASCII 文字だけです。改行は 2 文字としてカウントされます。Telnet または SSH を介してセキュリティ アプライアンスにアクセスしたときに、バナー メッセージを処理するのに十分なシステム メモリがなかった場合や、バナー メッセージの表示を試行して TCP 書き込みエラーが発生した場合には、セッションが閉じます。

ステップ 1 バナーを設定するには、[Banner] ページにアクセスします。

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [バナー（Banner）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [バナー（Banner）]** を選択しますポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 [セッション（exec）バナー（Session (exec) Banner）] フィールドに、イネーブルプロンプトを表示する前にバナーとして表示するテキストを入力します。

ステップ 3 Telnet を使用したセキュリティアプライアンスへのアクセス時に、パスワード ログイン プロンプトの前にバナーとして表示するテキストを [ログインバナー（Login Banner）] フィールドに入力します。

ステップ 4 [本日のメッセージ（motd）バナー（Message-of-the-Day (motd) Banner）] フィールドに、本日のメッセージバナーとして表示するテキストを入力します。

ステップ 5 バナーを置換するには、該当するボックスの内容を変更します。

ステップ 6 バナーを削除するには、該当するボックスの内容をクリアします。

[Boot Image/Configuration] の指定

[Boot Image/Configuration] ページを使用して、起動時にセキュリティ アプライアンスが使用する設定ファイルを指定します。Adaptive Security Device Manager（ASDM）の設定ファイルへのパスも指定できます。

ブートイメージの場所を指定しない場合、内部フラッシュ メモリ上にある最初の有効なイメージがシステムの起動に選択されます。

（注） このページは ASA および PIX 7.0 以降のデバイスでのみ使用できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブートイメージ/設定（Boot Image/Configuration）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [ブートイメージ/設定（Boot Image/Configuration）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 589 : [Boot Image/Configuration] ページ

要素	説明
Boot Config Location	システムがロードされるときに使用する設定ファイルのパスと名前を入力します。ASA では、次のいずれかの構文構成子を使用できます。 • **disk0:**/[*path/*]*filename* 値「disk0」は内部フラッシュカードを示します。「**disk0**」の代わりに「**flash**」を使用することもできます。これらはエイリアス関係にあります。 • **flash:**/[*path/*]*filename* • **disk1:**/[*path/*]*filename* 値「disk1」は外部フラッシュカードを示します。 PIX デバイスでは、次のような「flash」構文のみを使用できます。 • **flash:**/[*path/*]*filename*

要素	説明
ASDM Image Location	ASDM セッションの開始時に使用される ASDM ソフトウェア イメージの場所と名前（ASDM を使用して ASA と PIX の両方のデバイスをモニタできます）。 PIX デバイスでは、ブート設定のロケーションと同様、「flash」構文のみを使用できます。 ASA では、ブート設定のロケーションと同様、「disk0」、「flash」、「disk1」の構成子を使用できます。さらに、次のようにして TFTP サーバ上のイメージ ファイルを指定できます。 • **tftp:**//[*user* [*:password*]@]*server* [*:port*]/[*path/*]*filename*
[Boot Images] テーブル	このテーブルには、定義した代替の設定ファイルがすべて一覧で表示されます。設定ファイルは 4 個まで定義できます。[Boot Config Location] フィールドでプライマリ ファイルを指定しなかった場合や指定したファイルが使用できない場合、このリストで最初に使用できるイメージが使用されます。 これは Security Manager の標準のテーブルです。テーブルの使用 （64 ページ）で説明されているとおり、テーブルの下の上矢印ボタン、下矢印ボタン、[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] と [Edit Row] のボタンでは、[Images] ダイアログボックス （2480 ページ）を開きます。これは代替の設定ファイルへのパスを追加および編集するために使用します。 （注） ASA では、このテーブルの最初のエントリだけが TFTP サーバ上の ASDM 設定ファイルを参照できます。このデバイスが TFTP サーバに到達できない場合、リストにある次のイメージ ファイルをロードしようとします。

[Images] ダイアログボックス

[Images] ダイアログボックスを使用して、[Boot Image/Configuration] ページにある [Boot Images] テーブルの設定ファイルのエントリを追加または編集します。

ナビゲーション パス

[Images] ダイアログボックスには、[Boot Image/Configuration] ページからアクセスできます。詳細については、[Boot Image/Configuration] の指定 （2479 ページ）を参照してください。

フィールド リファレンス

[Images] ダイアログボックスにはフィールドが 1 つあります。このフィールドは、次のように、ブート イメージまたは設定ファイルへのパスを定義するために使用します。

表 *590 : [Images]* ダイアログボックス

要素	説明
Image File	順番に並べられた [Boot Images] リストに追加する設定ファイルのパスと名前を入力します。 PIX デバイスでは、次のような「flash」シンタックスのみを使用できます。 • **flash:**/[*path/*]*filename* ASA では、次のいずれかの構文構成子を使用できます。 • **disk0:**/[*path/*]*filename* 値「disk0」は内部フラッシュカードを示します。「**disk0**」の代わりに「**flash**」を使用することもできます。これらはエイリアス関係にあります。 • **flash:**/[*path/*]*filename* • **disk1:**/[*path/*]*filename* 値「disk1」は外部フラッシュカードを示します。 さらに、ASA では次のようにして TFTP サーバ上の ASDM イメージ ファイルを指定できます。 • **tftp:**//[*user* [*:password*]@]*server* [*:port*]/[*path/*]*filename* 指定できる TFTP の場所は 1 箇所だけです。また、この場所は [Boot Image/Configuration] ページにある [Boot Images] テーブルの一番上に表示されている必要があります。

CLI プロンプトの設定

[CLIプロンプト（CLI Prompt）] ページを使用して、CLI セッション中に ASA 7.2(1) 以降のデバイスによって使用されるプロンプトをカスタマイズできます。デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

（注） 使用可能な属性は、ASA のバージョンによって異なります。

cluster-unit （ASA 9.1.1以降のみ）	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。

domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
management-mode （ASA 9.2.1 以降のみ）	管理モードを表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。
state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、state に対して次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。この状況は、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 グループ化の場合、state に対して次の値が表示されます。 • コントロール • データ たとえば、プロンプト ciscoasa/cl2/slave では、ホスト名は ciscoasa、ユニット名は cl2、状態名は data です。

ステップ 1 次のいずれかを実行して、[CLIプロンプト（CLI Prompt）] ページにアクセスします。

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [CLIプロンプト（CLI Prompt）]** を選択します。

（注） マルチコンテキストモードのデバイスの場合、[CLIプロンプト（CLI Prompt）] ページはシステムコンテキストでのみ使用できます。管理コンテキストでは、[CLIプロンプト（CLI Prompt）] ページは使用できません。

- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [CLIプロンプト（CLI Prompt）]** を選択します。ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 CLI プロンプトをカスタマイズするには、次の操作を実行します。

- プロンプトに属性を追加する場合は、[使用可能なメンバー（Available Members）] リストで属性を選択して、[>>] をクリックします。属性が [使用可能なメンバー（Available Members）] リストから [選択済みのメンバー（Selected Members）] リストに移動します。

プロンプトには複数の属性を追加できます。[選択済みのメンバー（Selected Members）] リストに属性が追加された順序によって、CLI プロンプトに表示される順序が決まります。

（注） ASA 9.1.1 以降では、CLI プロンプトに最大 6 個の属性を設定できます。以前の ASA バージョンでは、最大 5 個の属性のみを設定できます。

- プロンプトから属性を削除する場合は、[選択済みのメンバー（Selected Members）] リストで属性をクリックし、[<<] をクリックします。属性が [選択済みのメンバー（Selected Members）] リストから [使用可能なメンバー（Available Members）] リストに移動します。

デバイス クロックの設定

[Clock] ページを使用して、選択したデバイスに日時を設定します。

（注） このページは Catalyst 6500 サービス モジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

NTP サーバを使用してダイナミックに時刻を設定するには、[NTP] ページ （2624 ページ）を参照してください。NTP サーバから取得された時刻は、[Clock] ページで手動で設定された時刻を上書きします。

（注） マルチコンテキスト モードの場合、時刻はシステム コンテキストでのみ設定します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *591 : [Clock]* ページ

要素	説明
Device Time Zone	デバイスのタイム ゾーンを選択します。これらのオプションは、Greenwich Mean Time（GMT; グリニッジ標準時）との時差に従って表されます。 （注） デバイスでタイム ゾーンを変更すると、取り付けられているいずれかの Security Services Module（SSM; セキュリティ サービス モジュール）への接続がドロップすることがあります。
Daylight Savings Time (Summer Time)	夏時間のオプションを選択します。また、必要に応じて、夏時間を適用するタイミングと方法を指定します。 [なし（None）]：夏時間を自動的に修正しない場合は、このオプションを選択します。 [日付により設定（Set by Date）]：特定の年の夏時間の開始日時と終了日時を指定する場合は、このオプションを選択します。このオプションを使用する場合、日付を毎年リセットする必要があります。 [日により設定（Set by Day）]：夏時間を開始および終了する月、週、日を使用して、夏時間の開始日および終了日を指定する場合、このオプションを選択します。このオプションを使用すると、日付の範囲が自動更新されるように設定できるため、毎年変更する必要はありません。
Set by Date [Start] セクションと [End] セクションには、次の 3 つのパラメータが表示されます。2 つのセットを使用して、夏時間を開始する日時と終了する日時を定義します。	
日付	夏時間を開始する日時と終了する日付を MMM DD YYYY 形式（Jul 15 2011 など）で入力します。カレンダーアイコンをクリックして、ポップアップ カレンダーから日付を選択することもできます。
時間（Hour）	夏時間の開始時間（時間）または終了時間（時間）を 00 ～ 23 から選択します。
毎分	夏時間の開始時間（分）または終了時間（分）を 00 ～ 59 から選択します。
Set by Day	

要素	説明
Specify Recurring Time	このチェックボックスをオンにすると、[Start] と [End] のパラメータがイネーブルになります。これらのパラメータは、夏時間の開始時間と終了時間の日付を毎年変更する必要がないように、自動更新するために使用します。
[Start] セクションと [End] セクションには、次の 5 つのパラメータが表示されます。2 つのセットを使用して、夏時間を開始する日時と終了する日時を定義します。	
月	夏時間が開始または終了する月を選択します。
週（Week）	夏時間が開始または終了する週を選択します。週に対応する数値を 1 ～ 4 の範囲で選択できます。または、[最初（first）] または [最後（last）] を選択して、月の最初の週または最後の週を指定できます。たとえば、日付が第 5 週の途中にあたる場合は、[last] を指定します。
Weekday	夏時間が開始または終了する曜日を選択します。
時間（Hour）	夏時間の開始時間（時間）または終了時間（時間）を 0 ～ 23 から選択します。
毎分	夏時間の開始時間（分）または終了時間（分）を 00 ～ 59 から選択します。

FIPS の有効化/無効化

4.15 以降、Cisco Security Manager には、ASA デバイスで連邦情報処理標準（FIPS）モードを有効化または無効化するオプションが用意されています。FOM で FIPS モードを有効にすると、Cisco SSL バージョンに実装されているレガシーメソッドの代わりに、FOM に実装されている FIPS 140-2 標準準拠の暗号化メソッドがシグネチャおよび検証の目的で使用されます。この機能は、ASA 9.8.2 以降のデバイスでのみサポートされています。

（注） デバイスで FIPS モードを設定するには、デバイスを手動で再起動する必要があります。

FIPS を有効にする前に、ASA で次の内容が設定されていることを確認してください。

1. DH グループが 14 に設定されている、または ECDH グループが 19、20、21 に設定されている。
2. デバイス ID 証明書のキータイプが RSA に設定されていて、キーサイズが 2048 以上である。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [FIPS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [FIPS]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *592 : [FIPS]* ページ

要素	説明
FIPS	チェックボックスをオンにして、デバイスでFIPSを有効にします。このオプションは、ASA 9.8.2 以降でのみ使用できます。 （注） 設定を有効にするには、FIPS を有効または無効にした後で、デバイスを再起動する必要があります。

Cisco Success Network の有効化

バージョン 4.20 以降、Cisco Security Manager には、カスタマー サクセス ネットワークを有効にするオプションが用意されています。これにより、ASAデバイスで有効になっている機能を利用し、Smart Call Home（SCH）の同じメカニズムを利用できます。SCHが収集するデータはほとんどが古く、SCH のリリース以降に追加された機能は正確なステータスを報告しないため、カスタマー サクセス ネットワークが導入されています。この機能は、ASA 9.13.1 以降のデバイスでサポートされています。

（注） 機能は、設定済みで、使用する準備ができている場合にのみ、「有効になっている」と見なされる必要があります。機能を設定しても動作しない場合、その機能を「有効になっている」と見なすことはできません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [カスタマー サクセス ネットワーク（Customer Success Network）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [カスタマー サクセス

ネットワーク ポリシー（Customer Success Network Policy）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *593 : [カスタマー サクセス ネットワーク（Customer Success Network）] ページ*

要素	説明
[カスタマー サクセス ネットワーク（Customer Success Network）]	[カスタマー サクセス ネットワークの有効化（Enable Customer Success Network）] チェックボックスをオンにして、デバイスで有効にします。このオプションは、ASA 9.13.1 以降のデバイスでのみ使用できます。

Umbrella グローバルポリシーの設定

バージョン 4.18 以降、Cisco Security Manager は Umbrella グローバルポリシーの設定をサポートしています。Cisco Umbrella Branch は、最初に DNS トラフィックを検査し、次に不審な HTTP/HTTPS トラフィックを検査するクラウドベースのセキュリティサービスです。Cisco Umbrella コネクタは、DNS パケットをインターセプトし、関心を引く DNS クエリを解決のために Cisco Umbrella リゾルバにリダイレクトします。DNS 応答を受信すると、その応答をホストに転送します。この機能は、ASA 9.10.1 以降のデバイスでのみサポートされています。

Cisco Umbrella サービスを設定したら、Cisco Umbrella DNS ポリシーマップも設定されていることを確認します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [Cisco Umbrella（Umbrella）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [Cisco Umbrella（Umbrella）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *594 : [Cisco Umbrella（Umbrella）] ページ*

要素	説明
Umbrella	選択したデバイス（ASA 9.10.1 以降）のグローバル Cisco Umbrella 設定を適用するには、チェックボックスをオンにします。

要素	説明
トークン	Cisco Umbrella サーバーへの登録時の ASA デバイスのトークン値。この値が 64 文字未満の場合、Cisco Security Manager からエラーメッセージがスローされます。
公開キー（3Public Key）	Cisco Umbrella サーバーへの登録時の ASA デバイスの公開キー値。この値は 64 桁の 16 進数で 80 文字未満である必要があります。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[EDNS フロータイムアウト（EDNS Flow Timeout）]	設定されている EDNS タイムアウト値。EDNS フローの Cisco Umbrella タイムアウトは、<0:0:0> ～ <1193:0:0> である必要があります。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[IPv4 リゾルバ（IPv4 Resolver）]	DNS 要求を解決するために使用するデフォルト以外の Cisco Umbrella DNS サーバーの IPv4 アドレス。有効な IPv4 であることを確認してください。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[IPv6 リゾルバ（IPv6 Resolver）]	DNS 要求を解決するために使用するデフォルト以外の Cisco Umbrella DNS サーバーの IPv6 アドレス。有効な IPv6 であることを確認してください。そうでない場合、Cisco Security Manager はエラーメッセージを表示します。
[正規表現クラス（Regular Expression Class）]	正規表現クラスを使用して、Cisco Umbrella をバイパスする必要があるローカルドメインバイパスを照合します。
正規表現	正規表現を使用して、Cisco Umbrella をバイパスする必要があるローカルドメインバイパスを照合します。

デバイス クレデンシャルの設定

[Credentials] ページを使用して、このデバイスに接続するときに Security Manager が使用するユーザ クレデンシャルを指定します。デバイスで [Enable Password] および [Telnet/SSH Password] を変更することもできます。

このユーザ名とパスワードの組み合わせを使用すると、HTTP、HTTPS、Telnet または SSH セッションを使用してセキュリティ アプライアンスに接続する場合に、EXEC モードでデバイスにログインできます。Telnet セッションおよび SSH セッション専用に個別のパスワードを指定することもできます（さらに、[Device Properties] ウィンドウの [Device Credentials] ページ （143 ページ）では、HTTP/HTTPS 接続用の個別のクレデンシャルを定義できます）。

[Enable Password] を使用すると、ログイン後に特権 EXEC モードにアクセスできます。

ヒント　このページの [Username]、[Password]、[Enable Password] は、[Device Properties] ウィンドウの [Credentials] 設定にリンクされています。これらのパラメータを更新して、その変更をデバイスに展開すると、Security Manager は [Device Properties] に定義されている既存のクレデンシャルを使用してデバイスにログインし、変更を展開します。変更が正常に展開されると、これらの設定に一致するように [Device Properties] のクレデンシャルが更新されます。[Device Properties] の [Credentials] の詳細については、[Device Credentials] ページ （143 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [クレデンシャル（Credentials）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [クレデンシャル（Credentials）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

危険　各デバイスには複数のユーザ アカウントが存在できるため、共有のクレデンシャル ポリシーを複数のデバイスに適用すると、各デバイスの [Enable Password] だけが更新されます。共有ポリシーに指定されている [Username] と [Password]（または [Telnet/SSH Password]）は適用されません。AAA や TACACS+ などの外部認証が設定されていない限り、PIX/ASA/FWSM デバイスには [Enable Password] だけでもアクセスできます。外部認証が設定されている場合は [Enable Password] だけでは不十分です。この場合、外部認証を使用する各デバイスで [Username]、[Password]、[Enable Password] を手動で更新する必要があります。

関連項目

- ユーザ アカウントの設定 （2588 ページ）

フィールド リファレンス

表 595 : [Credentials] ページ

要素	説明
[ユーザー名（Username）]	デバイスにログインするためのユーザ名を入力します。名前は 4 文字以上である必要があります。最大は 64 文字です。エントリは、大文字と小文字が区別されます。

要素	説明
パスワード 確認（Confirm）	指定した [Username] でデバイス（ユーザ EXEC モード）にログインするためのパスワードを指定します。このパスワードは 3 文字以上である必要があります。最大は 32 文字です。エントリは、大文字と小文字が区別されます。 [Confirm] フィールドにユーザ パスワードもう一度入力します。 （注） 8 文字以上の長さのパスワードを推奨します。
特権レベル	このユーザの特権レベルを選択します。使用可能な値は 1 ～ 15 です。レベル 1 では、EXEC モードのアクセスのみが許可されます。ログインのデフォルト レベルである 15 では、特権 EXEC モードのアクセスが許可されます。つまり、イネーブル モードにアクセスできます。他のレベルは、明示的にデバイスで定義する必要があります。
イネーブル パスワード	
暗号化されたパスワード（Password as encrypted）	[プレーンテキスト（Plain Text）] または [暗号化（Encrypted）] を選択します。
パスワード暗号化タイプ（Password encrypt type）	MD5 または PBKDF2 を選択します。
パスワードを有効にする（Enable Password） 確認（Confirm）	[パスワードの有効化（Enable Password）] を指定すると、このユーザーはログイン後に特権 EXEC モードにアクセスできます。入力は大文字と小文字が区別されます。 [Confirm] フィールドにイネーブル パスワードをもう一度入力します。 （注） プレーンテキストのパスワードの場合： • MD5 パスワードの長さは 3 ～ 32 文字にする必要があります。 • PBKDF2 パスワードの長さは、33 ～ 127 文字にする必要があります。展開の失敗を避けるために、PBKDF2 パスワードに正しい `sha` キー値が使用されていることを確認します。 （注） イネーブルアクセスのユーザ認証を設定する場合は、ユーザごとに専用のパスワードを指定します。このパスワードは使用しません）。詳細については、[AAA] の [Authentication] タブの設定 （2472 ページ）を参照してください。

要素	説明
Telnet/SSH パスワード 確認（Confirm）	Telnet セッションまたは SSH セッション経由でデバイスに接続するときに、EXEC モードにアクセスするためのパスワードを指定できます。このパスワードは 3 文字以上である必要があります。最大は 32 文字です。エントリは、大文字と小文字が区別されます。 [Confirm] フィールドに Telnet または SSH のパスワードもう一度入力します。 （注） Telnet または SSH アクセスのユーザ認証を設定する場合は、ユーザごとに専用のパスワードを指定します。このパスワードは使用しません。詳細については、[AAA] の [Authentication] タブの設定 （2472 ページ）を参照してください。

マウント ポイントの管理

[マウントポイント（Mount Points）] ページを使用して、Common Internet File System（CIFS）または File Transfer Protocol（FTP）ファイルシステムがセキュリティアプライアンスにアクセスできるようにします。

（注） FTP タイプのマウントポイントを作成する場合、FTP サーバーには UNIX のディレクトリ リストスタイルが必要です。Microsoft FTP サーバーには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

[ファイルマウントポイント設定（File Mount Point Configuration）] テーブルには、設定されたマウントポイントが一覧表示されます。[ファイルマウントポイント設定（File Mount Point Configuration）] テーブルは、Security Manager の標準のテーブルです。このテーブルには [行の追加（Add Row）]、[行の編集（Edit Row）]、[行の削除（Delete Row）] ボタンがあります（テーブルの使用 （64 ページ）に説明されているとおり、これらは標準のボタンです）。[行の追加（Add Row）] ボタンでは [DHCP リレーエージェント設定の追加（Add DHCP Relay Agent Configuration）] ダイアログボックスが開き、[行の編集（Edit Row）] では [DHCP リレーエージェント設定の編集（Edit DHCP Relay Agent Configuration）] ダイアログボックスが開きます。タイトルを除き、この 2 つのダイアログボックスは同じです。詳細については、[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス （2492 ページ）を参照してください。

（注） この機能は ASA 8.0(2)+ のデバイスでのみ使用できます。マウントポイントはルータモードでのみサポートされます。8.0(2) と 9.x の間の ASA バージョンの場合、マウントポイントはマルチコンテキストモードではサポートされません。マウントポイントは、マルチコンテキスト、ルーテッドモードの ASA 9.x+ デバイスの管理コンテキストでサポートされます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [マウントポイント（Mount Points）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [マウントポイント（Mount Points）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス

[マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックスを使用して、[マウントポイント（Mount Points）] ページの [ファイルマウントポイント設定（File Mount Point Configuration）] テーブルでマウントポイントエントリを追加または編集します。マウントポイントを使用して、Common Internet File System（CIFS）または File Transfer Protocol（FTP）ファイルシステムがセキュリティアプライアンスにアクセスできるようにします。

ナビゲーション パス

[マウントポイント（Mount Points）] ページから [マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックスにアクセスできます。詳細については、マウント ポイントの管理 （2491 ページ）を参照してください。

フィールド リファレンス

表 *596 : [マウントポイント設定の追加/編集（Add/Edit Mount Point Configuration）] ダイアログボックス*

要素	説明
[マウントポイントの有効化（Enable Mount Point）]	ファイルシステムをマウント対象または非マウント対象（使用可能または使用不能）に設定します。

要素	説明
接続タイプ	マウントするファイルシステムのタイプを選択します。 • [CIFS]：マウント対象のファイルシステムとして CIFS を指定します。CIFS は、CIFS 共有ディレクトリにボリュームマウント機能を提供するファイルシステムです。 • [FTP]：マウント対象のファイルシステムとして FTP を指定します。FTP は Linux カーネルモジュールであり、仮想ファイルシステム（VFS）を FTP ボリュームマウント機能で強化し、FTP 共有ディレクトリをマウントできるようにしたものです。 （注） FTP タイプのマウントポイントを作成する場合、FTP サーバーには UNIX のディレクトリ リストスタイルが必要です。Microsoft FTP サーバーには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。
[マウントポイント名（Mount Point Name）]	マウントの名前を指定します。マウントポイント名は、セキュリティアプライアンスにすでにマウントされているファイルシステムを他の CLI コマンドが参照するときに使用されます。マウントポイント名は 31 文字以下にする必要があります。
Server Name/IP Address	CIFS または FTP ファイルシステムサーバーの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
ユーザー名	ファイルシステムのマウントが認可されているユーザ名を指定します。
パスワード 確認（Confirm）	ファイルシステムのマウントのための認可されたパスワードを指定します。
パスワードの暗号化	選択すると、指定されたパスワードが暗号化された形式であることが示されます。
共有名 （CIFS のみ）	サーバ内のファイルデータにアクセスするために、特定のサーバ共有（フォルダ）を名前で明示的に識別します。
ドメイン名 （CIFS のみ）	CIFS ファイルシステムの場合のみ使用します。この引数には Windows NT ドメイン名を指定します。最大 63 文字が許可されます。
[モード（Mode）] （FTP のみ）	FTP 転送モードをアクティブまたはパッシブとして識別します。

要素	説明
パス（Path） （FTP のみ）	指定された FTP ファイル システム サーバーへのディレクトリ パス名を指定します。疑問符とスペースはパス名に使用できず、表示されません。

IP クライアント

[IPクライアント（IP Client）] ページには、インターフェイス名と IP バージョンが一覧表示されます。設定済みの IP クライアントを使用して、Firepower 2100 シリーズデバイスでの統合ルーティングおよびブリッジングサポートを使用できます。[IPクライアント（IP Client）] ページには、エントリを追加、編集、および削除するための標準オプションがあります。

（注） この機能は、ASA 9.8.2+ Firepower 2100 シリーズのシングル コンテキスト デバイスでのみ使用できます。IP クライアントのマルチコンテキストサポートはありません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [IPクライアント（IP Client）] を選択します。

（注） メニューは、Firepower 2100 シリーズデバイスでのみ表示されます。

- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [IPクライアント（IP Client）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックス

[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックスを使用して、[IPクライアント（ IP Client）] ページの [IPクライアント（IP Client）] テーブルの IP クライアントエントリを追加または編集します。IP クライアント設定を使用して、Firepower 2100 シリーズ デバイスで統合ルーティングとブリッジングをサポートします。

ナビゲーション パス

[IPクライアントの追加（Add IP Client）]/[IPクライアントの編集（Edit IP Client）] ダイアログボックスには、[IPクライアント（IP Client）]ページからアクセスできます。詳細については、IP クライアント （2494 ページ）を参照してください。

フィールド リファレンス

表 *597 : [IP*クライアントの追加（*Add IP Client***）*]/[IP*クライアントの編集（***Edit IP Client***）*]* ダイアログボックス**

要素	説明
IPバージョン	デバイスの IP アドレス。アドレスは IPv4 または IPv6 アドレスです。
インターフェイス	Firepower 2100 シリーズ デバイスに関連するインターフェイスを選択します。

設定のプレビューページには、IPv6 インターフェイスに IPv6 サフィックスが付いた IP クライアント設定が表示されます。IPv4 インターフェースの場合、インターフェース名のみが表示されます。

アプリケーション エージェント

[アプリケーションエージェント（App Agent）]ページを使用して、アプリケーションエージェント設定を行います。ハートビート間隔とリトライ回数を指定できます。

（注） App-Agent は、Firepower 2100 シリーズ、Firepower 4000 シリーズ、および Firepower 9000 シリーズデバイスでのみ使用できます。Cisco Security Manager では、Firepower 2100 シリーズデバイスの App-Agent は 9.8.2+ 以降でサポートされています。 Firepower 4000 シリーズおよび Firepower 9000 シリーズデバイスの App-Agent は、9.6.2+ 以降でサポートされています。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アプリケーションエージェント（App Agent）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [アプリケーションエージェント（App Agent）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *598 : [*アプリケーションエージェント（*App Agent*）*]* ページ

要素	説明
インターバル	アプリケーション エージェントのハートビート間隔を入力します。ASA 9.6.2 から ASA 9.8.1 では、App-Agent ハートビート値は 300 ～ 6000 ミリ秒にすることができます。 ASA 9.8.2+ デバイスの場合、App-Agent ハートビート間隔の値は 100 ～ 6000 ミリ秒です。 （注） 100 の倍数の値を入力しない場合、Cisco Security Manager はエラーメッセージを表示します。
再試行回数（Retry Count）	3 ～ 10 で再試行回数を入力します。
保存	クリックして、設定を保存します。

第 49 章

ファイアウォール デバイスでのデバイス アクセスの設定

ポリシーセレクタの [Device Admin] フォルダの下にある [Device Access] セクションには、ファイアウォール デバイスへのアクセスを定義するためのページがあります。

この章は次のトピックで構成されています。

- コンソール タイムアウトの設定 （2497 ページ）
- [HTTP] ページ （2498 ページ）
- ICMP の設定 （2502 ページ）
- 管理アクセスの設定 （2504 ページ）
- 管理セッションクォータの制限の設定 （2505 ページ）
- セキュア シェル アクセスの設定 （2506 ページ）
- SSL 設定：[基本（Basic）] タブと [詳細（Advanced）] タブ （2508 ページ）
- 参照 ID （2514 ページ）
- SNMP の設定 （2516 ページ）
- [Telnet] ページ （2537 ページ）

コンソール タイムアウトの設定

[Console] ページを使用して、非アクティブなコンソール セッションのタイムアウト値を指定します。指定した時間制限に達した場合は、コンソール セッションが終了します。

[コンソールタイムアウト（Console Timeout）] フィールドに、コンソールセッションがデバイスによって閉じられる前にアイドル状態でいられる時間（分単位）を入力します。有効値は、0 ～ 60 分です。コンソールセッションがタイムアウトにならないようにするには、0 を入力します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [コンソール（Console）] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [コンソール（Console）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[HTTP] ページ

[HTTP] ページのテーブルを使用して、デバイス上の HTTP サーバにアクセスするように設定されたインターフェイスと、それらのインターフェイスでの HTTP から HTTPS へのリダイレクトを管理します。このページから、デバイス上の HTTP サーバをイネーブルまたはディセーブルにすることもできます。特定のデバイス マネージャから管理者アクセスを行うには、HTTPS アクセスが必要です。

（注） HTTP をリダイレクトするには、インターフェイスに HTTP を許可するアクセス リストが必要です。このアクセスリストがないと、インターフェイスはポート 80、または HTTP 用に設定した他のポートをリッスンできません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 599 : [HTTP] ページ

要素	説明
[HTTP Interface] テーブル	このテーブルの [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、HTTP-to-HTTPS リダイレクトが設定されているデバイス インターフェイスを管理します。[Add Row] および [Edit Row] を使用すると、[HTTP Configuration] ダイアログボックス （2501 ページ）が開きます。

要素	説明
[証明書からユーザー名を取得（Fetch user name from certificate）] 設定	このオプションを選択して、証明書からユーザー名を抽出するためのルールを設定します。次を入力します。 • [証明書からのHTTPユーザー名を有効にする（Enable HTTP username from certificate）]：このボックスをオンにして、認証用に証明書からHTTP ユーザー名を取得します。 • [ユーザー名の事前入力（Prefill Username）]：認証に対するこの名前の使用をイネーブルにするには、[ユーザー名の事前入力（Prefill Username）] チェックボックスをオンにします。イネーブルの場合は、このユーザ名が、ユーザが入力したパスワードと一緒に認証に使用されます。 次のいずれかのオプションを選択します。 （注） この機能は、ASA ソフトウェア バージョン 9.4(1) 以降を実行しているデバイスでのみサポートされています。 • [DN全体をユーザー名として使用（Use the entire DN as the username）]：DN 全体をユーザー名として使用する場合、このオプションを選択します。このオプションはデフォルトでは無効になっています。

要素	説明
[証明書からユーザー名を取得（Fetch user name from certificate）] 設定（続き）	• [個々のDNフィールドをユーザー名として指定（Specify Individual DN fields as the Username）]：ユーザー名の抽出に使用する属性と追加の属性を指定する値を[プライマリDNフィールド（Primary DN Field）]ドロップダウンと[セカンダリDNフィールド（Secondary DN Field）]ドロップダウンから選択します。このオプションは、デフォルトで有効です。 • C：国：ISO 3166 国名コードに準拠する 2 文字の国名コード。 • CN：一般名：個人やシステムなどのエンティティの名前。セカンダリ属性としては使用できません。 • DNQ：ドメイン名修飾子。 • EA：電子メール アドレス。 • GENQ：世代修飾子。 • GN：名。 • I：イニシャル。 • L：地名：組織が所在する市または町。 • N：名前。 • O：組織：会社、団体、機関、協会などのエンティティの名前。 • OU：組織単位：組織（O）内のサブグループ。 • SER：シリアル番号。 • SN：姓。 • SP：州/都道府県：組織が所在する州または都道府県。 • T：肩書き。 • UID：ユーザ識別子。 • UPN：ユーザ プリンシパル名。 • [ASDMによって生成されたLUAスクリプトを使用（Use LUA Script generated by ASDM）]：ASDM によって生成された LUA スクリプトを使用する場合は、このオプションを選択します。このオプションはデフォルトでは無効になっています。
Enable HTTP Server	デバイス上で HTTP サーバをイネーブルまたはディセーブルにします。イネーブルになっている場合は、サーバーの通信用 [ポート（Port）] を指定できます。ポートの範囲は 1 ～ 65535 です。デフォルトは 443 です。

[HTTP Configuration] ダイアログボックス

[HTTP Configuration] ダイアログボックスを使用して、特定のインターフェイスを介してデバイス上のHTTPサーバへのアクセスを許可されるホストまたはネットワークを追加または編集します。HTTP リダイレクトをイネーブルおよびディセーブルにすることもできます。

ナビゲーション パス

[HTTP Configuration] ダイアログボックスには、[HTTP] ページ （2498 ページ）からアクセスできます。

フィールド リファレンス

表 *600 : [HTTP Configuration]* ダイアログボックス

要素	説明
Interface Name	デバイス上のHTTPサーバへのアクセスが許可されるインターフェイスを入力または選択します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9.2 デバイス以降でHTTPのBVIインターフェイスを設定できます。ただし、マルチコンテキストでは、「トランスペアレント」モードのセキュリティコンテキストは BVI インターフェイスのみをサポートします。
IP Address/Netmask	デバイスとのHTTP接続の確立を許可されるホストまたはネットワークのIPアドレスとネットマスクをスラッシュ（「/」）で区切って入力します。または、[Select] をクリックして、ネットワーク/ホストオブジェクトを選択できます。 （注） バージョン 4.13 以降、Cisco Security Manager は、IPv6 デバイスのポリシー（グループ、ホスト、アドレスの範囲、およびネットワーク）をサポートします。
Enable Authentication Certificate	このオプションは、HTTP 接続を確立するためにユーザ証明認証を要求する場合に選択します。ASA および PIX 8.0(2) 以降のデバイスでは、認証**ポート**を指定できます。
証明書マップ（Certificate Maps）	[リモートアクセスVPN（Remote Access VPN）]>[証明書から接続プロファイルへのマップ（Certificate to Connection Profile Maps）]>[ルール（Rules）] で設定した証明書マップ名を選択します。詳細については、[Map Rule] ダイアログボックス（上半分のテーブル） （1757 ページ）を参照してください。デフォルトでは [None] が選択されています。 この機能は、ASA 9.6(2) 以降のデバイスの Cisco Security Manager バージョン 4.12 以降で使用できます。このオプションは、ASA デバイスのシングル、マルチ、ルーテッド、およびトランスペアレント コンテキストでサポートされています。

要素	説明
Redirect port	セキュリティ アプライアンスが HTTPS にリダイレクトする HTTP 要求をリッスンするポート。HTTP リダイレクトをディセーブルにするには、このフィールドがブランクであることを確認します。

ICMP の設定

[ICMP] ページのテーブルを使用して、インターネット制御メッセージプロトコル（ICMP）規則を管理します。この規則では、セキュリティデバイス上の特定のインターフェイスへの ICMP アクセスを許可または拒否するすべてのホストまたはネットワークのアドレスを指定します。

（注） ASA 8.2(1) 以降、ICMP IPv6 はトランスペアレント ファイアウォール モードでサポートされるようになりました。

ICMP ルールでは、任意のデバイス インターフェイス上で終了する ICMP トラフィックを制御します。ICMP 制御リストが設定されていない場合、デバイスは、外部インターフェイスを含む任意のインターフェイスで終了するすべての ICMP トラフィックを受け入れます。ただし、デフォルトでは、デバイスはブロードキャストアドレスに送信された ICMP エコー要求に応答しません。

ICMP Unreachable メッセージ（タイプ 3）は常に許可することを推奨します。ICMP Unreachable メッセージを拒否すると、ICMP パス MTU ディスカバリがディセーブルになり、IPsec および PPTP トラフィックが停止することがあります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

ICMP 制御リストが設定されている場合、デバイスは ICMP トラフィックとの最初の一致を使用し、続いて暗黙的な deny all を使用します。つまり、最初に一致したエントリが許可エントリの場合は、ICMP パケットの処理を継続します。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しない場合、デバイスは ICMP パケットを廃棄し、syslog メッセージを生成します。ICMP 制御リストが設定されていない場合は、すべてのケースで許可ルールが想定されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ICMP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [ICMP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） ICMP IPv6 サポートは、PIX および FWSM デバイスでは使用できません。

フィールド リファレンス

表 *601 : [ICMP]* ページ

要素	説明
[ICMP Rules] テーブル	このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、ICMP ルールを管理します。[Add Row] を選択すると、[Add ICMP] ダイアログボックスが開きます。[Edit Row] を選択すると、[Edit ICMP] ダイアログボックスが開きます。これらのダイアログボックスについては、[Add ICMP]/[Edit ICMP] ダイアログボックス（2503 ページ）を参照してください。
ICMP Unreachable Parameters	
レート制限	このデバイス上のインターフェイスで終了する ICMP トラフィックについて、デバイスが 1 秒間に転送できる ICMP Unreachable メッセージの最大数です。この値は、1 ～ 100 メッセージ/秒です。デフォルトは 1 メッセージ/秒です。
バースト サイズ	ICMP Unreachable メッセージのバースト サイズ。1 ～ 10 の値を指定できます。 （注） このパラメータは、現在システムでは使用されていないため、任意の値を選択できます。

[Add ICMP]/[Edit ICMP] ダイアログボックス

[Add ICMP] ダイアログボックスを使用して、ICMP ルールを追加します。このルールでは、指定したデバイス インターフェイス上で指定した ICMP アクセスを許可または拒否されるホスト/ネットワークを指定します。

（注） [Edit ICMP] ダイアログボックスは、事実上 [Add ICMP] ダイアログボックスと同じであり、既存の ICMP ルールの修正に使用します。次の説明は、両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add ICMP]/[Edit ICMP] ダイアログボックスには、ICMP の設定 （2502 ページ）からアクセスできます。

（注） ICMP ポリシーを追加するときは、ネットワークとサービスが同じタイプであること、つまり、IPv6 ネットワークが IPv6 サービスをサポートしていることを確認してください。

フィールド リファレンス

表 *602 : [Add ICMP]/[Edit ICMP]* ダイアログボックス

要素	説明
操作	このルールによって、指定したインターフェイス上の指定したネットワークからの選択した ICMP サービス メッセージが許可されるか、または拒否されるか。次のどちらかを選択します。 • [許可（Permit）] : 指定したネットワーク/ホストからの ICMP メッセージは、指定したインターフェイスに対して許可されます。 • [拒否（Deny）] : 指定したネットワーク/ホストから指定したインターフェイスへの ICMP メッセージはドロップされます。
ICMP Service	ルールを適用する特定の ICMP サービス メッセージを入力または選択します。
インターフェイス	これらの ICMP メッセージの送信先のデバイス インターフェイスを入力または選択します。
ネットワーク（Network）	ホスト名、 IPv4 または IPv6 アドレスを入力するか、ネットワーク/ホストオブジェクトを選択して、指定した ICMP メッセージの送信元を定義します。

管理アクセスの設定

[Management Access] ページを使用して、高セキュリティ インターフェイスへのアクセスをイネーブルまたはディセーブルにして、デバイスに対して管理機能を実行できるようにします。内部インターフェイスでこの機能をイネーブルにして、IPsec VPN トンネル上のインターフェイスで管理機能を実行可能にできます。管理アクセス機能は、一度に 1 つのインターフェイスでだけイネーブルにすることができます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [管理アクセス（Management Access）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス**

（**Device Access**）] > **[管理アクセス（Management Access**）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

管理アクセスのイネーブル化とディセーブル化

[管理アクセスインターフェイス（Management Access Interface）] フィールドで、管理アクセス接続を許可するデバイスインターフェイスの名前を入力します。[Select] をクリックすると、インターフェイス オブジェクトのリストからインターフェイスを選択できます。

管理アクセス機能は、一度に 1 つのインターフェイスでだけイネーブルにすることができます。

管理アクセスをディセーブルにするには、[Management Access Interface] フィールドをクリアします。

管理セッションクォータの制限の設定

4.19 以降、Cisco Security Manager では、すべての接続タイプおよびユーザー名にわたる管理セッションの最大数とユーザー名ごとの同時セッションの最大数に加えて、ASA 9.12(1) 以降のデバイスでのプロトコルごとの制限の適用を設定できます。設定された同時セッション制限は、着信管理セッションを認証する前に適用されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [管理セッションクォータ（Management Session Quota）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [管理セッションクォータ（Management Session Quota）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） セッション制限の適用順序は、ユーザー制限、集約制限、プロトコルごとの制限の順です。

フィールド リファレンス

表 *603 : [Add ICMP]/[Edit ICMP]* ダイアログボックス

要素	説明
アグリゲート	すべての接続タイプにわたる管理セッションの最大数。デフォルトは 15 です。制限は 1 ～ 15 の範囲で設定できます。

要素	説明
HTTP	HTTP の管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。デフォルト値は 5 です。
SSH	SSH の管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。デフォルト値は 5 です。
Telnet	Telnet の管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。デフォルト値は 5 です。
ユーザー（User）	ユーザーの管理セッションクォータ制限を 1 ～ 5 の範囲で入力します。ユーザー制限のデフォルト値は指定されていません。

セキュア シェル アクセスの設定

[Secure Shell] ページを使用して、SSH プロトコルを使用したセキュリティ デバイスへの管理アクセスを許可するルールを設定します。ルールでは、特定の IP アドレスとネットマスクへの SSH アクセスが制限されます。これらのルールに準拠する任意の SSH 接続試行は、AAA サーバまたは Telnet パスワードによって認証される必要があります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 604 : [Secure Shell] ページ

要素	説明
SSH Version	デバイスによって受け入れられる SSH バージョンを指定します。**1**、**2**、または **1 と 2** を選択します。デフォルトでは、SSH バージョン 1 接続および SSH バージョン 2 接続が受け入れられます。
タイムアウト（Timeout）	セキュア シェル セッションがデバイスによって閉じられる前にアイドル状態でいられる時間（分単位）を 1 ～ 60 で入力します。デフォルト値は 5 分です。

要素	説明
[Allowed Hosts] テーブル	このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、SSH を介したセキュリティ デバイスへの接続を許可するホストを管理します。[Add Row] を選択すると、[Add Host] ダイアログボックスが開きます。[Edit Row] を選択すると、[Edit Host] ダイアログボックスが開きます。これらのダイアログボックスについては、[Add SSH Host]/[Edit SSH Host] ダイアログボックス （2507 ページ）を参照してください。
Enable Secure Copy	このボックスをオンにして、セキュリティ アプライアンス上の Secure Copy（SCP; セキュア コピー）サーバをイネーブルにします。これにより、アプライアンスはデバイスとの間でファイルを転送するための SCP サーバとして機能できます。SSH を使用したセキュリティ アプライアンスへのアクセスを許可されるクライアントだけが、セキュア コピー接続を確立できます。 セキュア コピー サーバのこの実装には、次の制限があります。 • サーバはセキュア コピーの接続を受け入れまたは終了できますが、開始はできません。 • サーバーにはディレクトリ サポートがありません。ディレクトリ サポートがないため、セキュリティ アプライアンスの内部ファイルへのリモート クライアント アクセスが制限されます。 • サーバではバナーがサポートされません。 • サーバではワイルドカードがサポートされません。 • セキュリティ アプライアンス ライセンスには、SSH バージョン 2 接続をサポートするための VPN-3DES-AES 機能が必要です。

[Add SSH Host]/[Edit SSH Host] ダイアログボックス

[Add SSH Host] ダイアログボックスを使用して、SSH アクセス ルールを追加します。

（注） [Edit Host] ダイアログは、事実上 [Add Host] ダイアログボックスと同じであり、既存の SSH アクセス ルールの修正に使用されます。次の説明は、両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add Host]/[Edit Host] ダイアログボックスには、セキュア シェル アクセスの設定 （2506 ページ）からアクセスできます。

フィールド リファレンス

表 605 : [Add Host]/[Edit Host] ダイアログボックス

要素	説明
インターフェイス（Interface）	SSH接続が許可されるデバイスインターフェイスの名前を入力または選択します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9.2 デバイス以降で SSH 接続の BVI インターフェイスを設定できます。ただし、マルチコンテキストでは、「トランスペアレント」モードのセキュリティコンテキストはBVIインターフェイスのみをサポートします。
IP Addresses	指定したインターフェイス上のセキュリティ デバイスとの SSH 接続の確立を許可される各ホストまたはネットワークの名前またはIPアドレスを入力します。複数のエントリを区切るにはカンマを使用します。[Select] をクリックして、リストからネットワーク/ホスト オブジェクトを選択することもできます。 （注） バージョン 4.13 以降、Cisco Security Manager は、IPv6 デバイスのポリシー（グループ、ホスト、アドレス範囲、およびネットワーク）をサポートします。

SSL 設定：[基本（Basic）] タブと [詳細（Advanced）] タブ

バージョン 4.8 以降、Security Manager は、セキュアソケットレイヤ（SSL）を使用して強化されたセキュリティ機能を提供します。

[デバイスアクセス（Device Access）] で SSL を設定するには、[CSM管理（CSM Admin）] > [ポリシー管理（Policy Management）] で SSL を有効にしてください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SSL] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SSL] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *606 : [SSL]* ページの *[基本（Basic）]* タブ

要素	説明
証明書認証	
[FCAタイムアウト（FCA Timeout）]	1 ～ 120 の範囲で値を入力します。 （注） FCA タイムアウトは、ASA ソフトウェアバージョン 9.1(2) 以降を実行しているデバイスに適用されます。
インターフェイス	[インターフェイス（Interface）] テーブルの下にある [行の追加（Add Row）]、[行の編集（Edit Row）]、および [行の削除（Delete Row）] ボタンを使用して、SSL を介したセキュリティデバイスへの接続を許可するインターフェイスとそのポート番号を管理します。[行の追加（Add Row）] を選択すると、[ホストの追加（Add Host）] ダイアログボックスが開きます。[行の編集（Edit Row）] を選択すると、[ホストの編集（Edit Host）] ダイアログボックスが開きます。[インターフェイスセレクタ（Interface Selector）] ダイアログボックスの利用可能なエントリからインターフェイスを選択できます。ポート番号は 1 ～ 65535 の範囲で入力してください。
クライアント バージョン（Client Version） [SSL/TLSプロトコルバージョン（SSL/TLS Protocol Version）]	[クライアントバージョン（Client Version）] は、デバイスがクライアントとして機能するときに使用する SSL/TLS プロトコルのバージョンです。次のオプションのいずれかを選択します。 • [任意（Any）]：このキーワードを選択すると、SSLv3 クライアントの hello が送信され、SSLv3 以降 がネゴシエートされます。これがデフォルトのキーワードです。 • [SSLV3]：このキーワードを入力すると、SSLv3 クライアントの hello が送信され、SSLv3 以降 がネゴシエートされます。 • [TLSV1]：このキーワードを入力すると、TLSv1 クライアントの hello が送信され、TLSv1 以降 がネゴシエートされます。 • [TLSV1.1]：このキーワードを入力すると、TLSv1.1 クライアントの hello が送信され、TLSv1.1 以降 がネゴシエートされます。 • [TLSV1.2]：このキーワードを入力すると、TLSv1.2 クライアントの hello が送信され、TLSv1.2 以降 がネゴシエートされます。 （注） TLSV1.1 および TLSV1.2 プロトコルバージョンは、ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスに適用できます。

要素	説明
サーバー バージョン [SSL/TLSプロトコルバージョン（SSL/TLS Protocol Version）]	[サーバーバージョン（Server Version）] は、デバイスがサーバーとして機能するときに使用する SSL/TLS プロトコルの最小バージョンです。次のオプションのいずれかを選択します。 • [任意（Any）]：このキーワードを選択すると、SSLv2 クライアントの hello が受け入れられ、共通の最新バージョンがネゴシエートされます。これがデフォルトのキーワードです。 • [SSLV3]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、SSLv3 以降 がネゴシエートされます。 • [SSLV3-Only]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、SSLv3 以降 がネゴシエートされます。 • [TLSV1]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1 以降 がネゴシエートされます。 • [TLSV1-Only]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1 以降 がネゴシエートされます。 • [TLSV1.1]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1.1 以降 がネゴシエートされます。 • [TLSV1.2]：このキーワードを入力すると、SSLv2 クライアントの hello が受け入れられ、TLSv1.2 以降 がネゴシエートされます。 **注**： • [任意（Any）] キーワードは、サーバーバージョンとクライアントバージョン両方のデフォルトであり、共通してサポートされている TLS の最新バージョンをデバイスがネゴシエートすることを意味します。 • TLSV1.1 および TLSV1.2 プロトコルバージョンは、ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスに適用できます。 • SSLV3-Only および TLSV1-Only プロトコルバージョンは、9.3(2) より前の ASA ソフトウェアバージョンを実行しているデバイスに適用できます。

表 *607 : [SSL]* ページの *[*詳細（*Advanced*）*]* タブ

要素	説明
9.3(2) より前の ASA ソフトウェアバージョンを実行しているデバイスの詳細な SSL 設定	

要素	説明
暗号化（Encryption）	使用可能なリストから暗号化アルゴリズムを選択します。暗号化アルゴリズムを追加するには、[使用可能なメンバー（Available Members）] リストで項目を選択してから、[>>] をクリックします。項目が [使用可能なメンバー（Available Members）] リストから [選択済みのメンバー（Selected Members）] リストに移動します。複数の暗号化アルゴリズムを追加できます。 使用可能な暗号化アルゴリズムは次のとおりです。 • 3DES-SHA1 • AES128-SHA1 • AES256-SHA1 • DES-SHA1 • RC4-MD5 • RC4-SHA1 • NULL-SHA1 • DHE-AES128-SHA1 • DHE-AES256-SHA1 （注） 4.19 以降、Cisco Security Manager は、ASA 9.12(1) 以降のデバイスの SSL 暗号で NULL SHA1 を使用した TLS プロキシの設定をサポートしていません。 暗号化アルゴリズムを削除するには、[選択済みのメンバー（Selected Members）] リストで項目を選択してから、[<<] をクリックします。項目が [選択済みのメンバー（Selected Members）] リストから [使用可能なメンバー（Available Members）] リストに移動します。 [Save] をクリックして設定を保存します。
ASA ソフトウェアバージョン 9.3(2) 以降を実行しているデバイスの詳細な SSL 設定	
SSL Cipher	[SSL暗号（SSL Cipher）] テーブル下の [行の追加（Add Row）]、[行の編集（Edit Row）]、および [行の削除（Delete Row）] ボタンを使用して、SSL 暗号のバージョンとレベルを管理します。[暗号の追加（Add Cipher）] ダイアログで、バージョンとレベルの組み合わせを選択します。

要素	説明
バージョン	次のいずれかのバージョンを選択します。 • DEFAULT • DTLSV1 • DTLSV1.2 • SSLV3 • TLSV1 • TLSV1.1 • TLSV1.2 （注） DEFAULT キーワードは、デバイスがクライアントとして動作し、サーバーへの接続を確立しているときに、アウトバウンド接続を設定するために使用されます。他のすべてのキーワードは、デバイスがサーバーとして機能し、クライアントからの接続を受け入れているときに使用されます。 （注） SSLV3 バージョンは、ASA バージョン 9.4(1) 以降廃止されています。そのため、バージョン 4.9 以降、Security Manager は検証を実行して、SSLV3 オプションがバージョン 9.4(1) 以降を実行している ASA デバイスに設定されているかどうかを確認します。
レベル	次のいずれかのバージョンを選択します。 • [All]：NULL-SHA を含むすべての暗号が含まれます。 • [LOW]：NULL-SHA を除くすべての暗号が含まれます。 • [MEDIUM]：NULL-SHA:DES-CBC-SHA:RC4-SHA:RC4-MD5 を除くすべての暗号が含まれます。 • [FIPS]：FIPS 準拠のすべての暗号が含まれます（つまり NULL-SHA:DES-CBC-SHA:RC4-MD5:RC4-SHA:DES-CBC3-SHA ではない暗号）。 • [HIGH]：SHA-2 暗号を使用する AES-256 のみが含まれます（TLSv1.2 にのみ適用）。

要素	説明
[カスタム文字列（Custom String）]	Security Manager の CUSTOM キーワードを使用し、OpenSSL 暗号定義文字列を使用して暗号スイートを全面的に制御します。 （注） バージョン 4.9 以降、Security Manager は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスに対して、次の新しい TLSV1.2 暗号のサポートを提供します。 • ECDHE_RSA_AES128_SHA256 • ECDHE_RSA_AES256_SHA384 • ECDHE_ECDSA_AES128_SHA256 • ECDHE_ECDSA_AES256_SHA384 （注） バージョン 4.16 以降、Security Manager は、ASA ソフトウェアバージョン 9.4(1) 以降を実行しているデバイスに対し、上記の暗号に加えて、次の新しい TLSV1.2 暗号のサポートを提供します。 • ECDHE-ECDSA-AES256-GCM-SHA384 • ECDHE-RSA-AES256-GCM-SHA384 • DHE-RSA-AES256-GCM-SHA384 • AES256-GCM-SHA384 • ECDHE-ECDSA-AES128-GCM-SHA256 • ECDHE-RSA-AES128-GCM-SHA256 • DHE-RSA-AES128-GCM-SHA256 • AES128-GCM-SHA256
[ECDH設定（ECDH Configuration）]	ECDH グループのオプション（19、20、21、なし）のいずれかから選択します。この機能は、ASA デバイスバージョン 9.4(1) 以降の Security Manager バージョン 4.9 以降で使用できます。

（注） 一部の国では輸入規制があるため、Oracle の展開では、暗号化アルゴリズムの強度を制限するデフォルトの暗号管轄ポリシーファイルが提供されています。より強力なアルゴリズムを設定する必要がある場合や、デバイスですでに設定されている場合（たとえば、256 ビットキーを使用する AES、5、14、24 を使用する DH グループなど）は、次の手順に従います。

1. Java 7 の無制限強度の暗号ポリシー .jar ファイルを http://www.oracle.com からダウンロードします。シスコは Oracle の Web サイトで次を検索することを推奨しています。

Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files Java 7

（ダウンロードボタンをクリックし、使用許諾契約に同意してファイルをダウンロードします）

1. Security Manager サーバーの CSCOpx\MDC\vms\jre\lib\security フォルダにある local_policy.jar および US_export_policy.jar を置き換えます。
2. Security Manager サーバーを再起動します。

参照 ID

バージョン 4.12 以降、Security Manager を使用すると、ASA ソフトウェアバージョン 9.6(2) 以降を実行しているデバイスでセキュアな Syslog サーバー接続用の参照 ID ポリシーオブジェクトを設定できます。このオブジェクトは、コモンクライテリア要件のサポートを有効にします。

参照 ID は、サーバー証明書で示された ID と比較される 1 つ以上の ID として設定されます。ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。

[参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックス

新しい参照 ID ポリシーオブジェクトを作成したり既存のポリシーオブジェクトを編集するには、[参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックスを使用します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [参照 ID（Reference Identity）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object] を選択するか [+] ボタンをクリックして新しいオブジェクトを追加するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *608 : [参照 ID の追加/編集（Add/Edit Reference Identity）] ダイアログボックス*

要素	説明
名前	参照 ID ポリシーオブジェクトの名前。各参照 ID は複数の行の値を持つことができることに注意してください。
説明	参照 ID ポリシーオブジェクトの説明。

要素	説明
[共通名 ID（Common Name ID）]	証明書のサブジェクトフィールドに設定される、共通名（CN）タイプの 1 つの属性タイプと値のペアだけが含まれる相対識別名（RDN）。この値は、完全な形のドメイン名と一致します。CN 値は自由形式のテキストにできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
[ドメイン名 ID（Domain Name ID）]	タイプ dNSName の subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
[サービス名 ID（Service Name ID）]	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。
[ユニフォーム リソース識別子 ID（Uniform Resource Identifier ID）]	タイプ uniformResourceIdentifier の subjectAltName エントリです。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。
カテゴリ	（任意）CAT-A ～ CAT-J の間でカテゴリを選択します。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[Edit] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[Overrides] フィールドは、このオブジェクトに対するオーバーライドを持つデバイスの数を示します。

（注） 参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

SNMP の設定

簡易ネットワーク管理プロトコル（SNMP）は、PC またはワークステーションで実行されているネットワーク管理ステーションが、スイッチ、ルータ、セキュリティアプライアンスなどのさまざまなタイプのデバイスのヘルスとステータスをモニターするための標準的な方法を定義します。[SNMP] ページを使用して、SNMP 管理ステーションによってモニタされるようにファイアウォール デバイスを設定できます。

簡易ネットワーク管理プロトコル（SNMP）は、集中管理する場所からのネットワーク デバイスのモニタリングをイネーブルにします。Cisco セキュリティ アプライアンスでは、SNMP バージョン 1、2c、および 3 を使用したネットワーク モニタリングに加えて、トラップおよび SNMP 読み取りアクセスがサポートされます。SNMP 書き込みアクセスはサポートされません。

ネットワーク管理ステーション（NMS）に「トラップ」（イベント通知）を送信するようにセキュリティアプライアンスを設定したり、NMS を使用してセキュリティアプライアンス上の Management Information Base（MIB）を参照したりできます。CiscoWorks for Windows またはその他の任意の SNMP MIB-II 対応ブラウザを使用して、SNMP トラップを受信し、MIB を参照します。

セキュリティアプライアンスには、指定したイベントが発生した場合（たとえばネットワーク上のリンクが起動またはダウンした場合）に指定した管理ステーションに通知する SNMP エージェントがあります。通知には、管理ステーションに対してデバイスを識別する SNMP システム Object ID（OID; オブジェクト ID）が含まれます。セキュリティ アプライアンス SNMP エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP MIB および OID

SNMP トラップは、ネットワーク デバイスで発生した重要イベント（ほとんどの場合はエラーまたは障害）をレポートします。SNMP トラップは、標準またはエンタープライズ固有の管理情報ベース（MIB）で定義されています。

標準トラップと MIB は、Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）によって作成され、各種 RFC に文書化されています。標準トラップは、セキュリティ アプライアンス ソフトウェアにコンパイルされます。必要に応じて、RFC、標準 MIB、および標準トラップを IETF Web サイト http://www.ietf.org/ からダウンロードできます。

Cisco MIB ファイルおよび OID については、http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml を参照してください。OID は、FTP サイト ftp://ftp.cisco.com/pub/mibs/oid/oid.tar.gz からダウンロードできます。

ここでは、次の内容について説明します。

- SNMP の用語 （2517 ページ）
- SNMP バージョン 3 （2517 ページ）
- [SNMP] ページ （2519 ページ）

SNMP の用語

一般的な SNMP 用語の定義をいくつか示します。

- **エージェント**：セキュリティアプライアンス上で実行されている SNMP サーバー。エージェントは情報の要求と管理ステーションからのアクションに応答します。エージェントは、管理情報ベース（MIB）（SNMP マネージャから表示または変更できるデータ オブジェクトの集合）へのアクセスも制御します。
- **管理ステーション**：SNMPイベントをモニターし、セキュリティアプライアンスなどのデバイスを管理するように設定されたPCまたはワークステーション。管理ステーションは、ハードウェア障害など、対処する必要のあるイベントに関するメッセージも受信できます。
- **MIB**：エージェントは、Management Information Base（MIB）と呼ばれる標準化されたデータ構造をメンテナンスします。MIBは、パケット、接続カウンタ、エラーカウンタ、バッファ使用状況、フェールオーバーステータスなどの情報の収集に使用されます。MIBの番号は、特定の製品、およびほとんどのネットワーク デバイスで使用される共通プロトコルとハードウェア規格に対して定義されています。SNMP管理ステーションでは、MIBを参照したり、特定のフィールドだけを要求したりできます。一部のアプリケーションでは、管理の目的で MIB データを修正できます。
- **OID**：SNMP 標準ではシステムオブジェクト ID（OID）が割り当てられるため、管理ステーションがSNMPエージェントでネットワークデバイスを一意に識別したり、監視および表示される情報のソースをユーザーに示したりできます。
- **トラップ**：SNMPエージェントから管理ステーションへのメッセージを生成する指定されたイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog イベントなどのアラーム条件が含まれます。

SNMP バージョン 3

SNMP バージョン 3 は SNMP バージョン 1 または SNMP バージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバーと SNMP エージェント間でデータをクリア テキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザーベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA およびASASM は、SNMP グループとユーザーの作成、およびセキュアなSNMP通信の転送の認証と暗号化をイネーブルにするために必要なホストの作成もサポートします。

（注） SNMP バージョン 3 は、8.2(1) 以降を実行している ASA デバイスおよび 8.5(1) 以降を実行している ASASM デバイスでサポートされています。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティ モデルにまとめられます。セキュリティ モデルはユーザーとグループに適用され、次の 3 つのタイプに分けられます。

- NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。
- Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザーは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザー

SNMP ユーザーは、指定されたユーザー名、ユーザーが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは MD5 と SHA です。暗号化アルゴリズムのオプションは DES、3DES、および AES（128、192、および 256 バージョンで使用可能）です。ユーザーを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザーはグループのセキュリティ モデルを継承します。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザーだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザー名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA および ASA サービスモジュールで一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、SNMP NMS を設定し、NMS のユーザー クレデンシャルが ASA および ASASM のユーザー クレデンシャルと一致するように設定してください。

ASA、ASA サービスモジュールと Cisco IOS ソフトウェアの導入の相違点

ASA および ASASM での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装と次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカル エンジン ID は、ASA または ASASM が起動されたとき、あるいはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザーとグループを作成する必要があります。
- 正しい順序でユーザー、グループ、およびホストを削除する必要があります。
- **snmp-server host** コマンドを使用すると、着信 SNMP トラフィックを許可する ASA または ASASM のルールが作成されます。

[SNMP] ページ

[SNMP] ページを使用して、簡易ネットワーク管理プロトコル（SNMP）管理ステーションによってモニタされるようにセキュリティ アプライアンスを設定します。

（注） SNMP バージョン 3 の設定は、グループ、ユーザー、ホストの順に行う必要があります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP（SNMP）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP（SNMP）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMP Trap Configuration] ダイアログボックス （2522 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527 ページ）
- [SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス （2529 ページ）

- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス（2531 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （2533 ページ）
- [SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス （2537 ページ）

フィールド リファレンス

表 *609 : [SNMP]* ページ

要素	説明
Enable SNMP Servers	このオプションを選択すると、指定したインターフェイスの SNMP 情報がセキュリティ デバイスから提供されます。このオプションの選択を解除すると、設定情報を保持したまま、SNMP モニタリングをディセーブルにできます。
[Read コミュニティ ストリング（Read Community Strin）] 確認（Confirm）	要求をこのデバイスに送信するときに SNMP 管理ステーションで使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。セキュリティデバイスでは、このパスワードを使用して、着信 SNMP 要求が有効かどうかを判断します。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。 [確認（Confirm）] フィールドにパスワードを再度入力し、パスワードが正しく入力されたことを確認します。
System Administrator Name	デバイス管理者またはその他の担当者の名前を入力します。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
参照先	このセキュリティデバイスの場所を記します（**Building 42, Sector 54** など）。この文字列は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。
Port（PIX 7.x、ASA、FWSM 3.x のみ）	着信要求が受け入れられるポートを指定します。デフォルトは 161 です。
SNMP トラップの設定	[SNMP Trap Configuration] ダイアログボックス （2522 ページ）で SNMP トラップを設定するには、このボタンをクリックします。

要素	説明
SNMP エンジン ID	デバイスに設定されている SNMP エンジンの ID を表示します。[SNMP エンジンIDの取得（Get SNMP Engine ID）] をクリックして、デバイスからエンジン ID を取得します。
[SNMP Hosts] テーブル	このテーブルには、セキュリティ アプライアンスにアクセスできる SNMP 管理ステーションが一覧表示されます。これは Security Manager の標準のテーブルです。テーブルの使用 （64 ページ）で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 [Add Row] と [Edit Row] のボタンでは、[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527ページ）が開きます。これは管理ステーションのホストエントリを追加および編集するために使用します。 （注） 9.1(5) 以降を実行している ASA デバイスの場合、最大 129 の SNMP ホストを設定できます。他のデバイスおよび以前の ASA バージョンでは、最大 32 の SNMP ホストのみを設定できます。
SNMP ホストグループテーブル	バージョン 4.12 以降、Security Manager では、SNMP ユーザのホストグループエントリを追加および編集できます。詳細については、[SNMP ホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス （2529 ページ）を参照してください。
SNMPv3 の設定	
SNMP グループタブ	設定されている SNMP グループを一覧表示します。これは Security Manager の標準のテーブルです。テーブルの使用 （64 ページ）で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 [行の追加（Add Row）] と [行の編集（Edit Row）] ボタンでは、[SNMP グループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （2531 ページ）が開きます。これは SNMP グループを追加および編集するために使用します。
SNMP ユーザタブ	設定されている SNMP ユーザをリストします。これは Security Manager の標準のテーブルです。テーブルの使用 （64 ページ）で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 [行の追加（Add Row）] と [行の編集（Edit Row）] ボタンでは、[SNMP ユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （2533 ページ）が開きます。これは SNMP ユーザを追加および編集するために使用します。

要素	説明
SNMPユーザリストタブ	バージョン 4.12 以降、Security Manager では、複数の SNMP ユーザを含むユーザリストを追加できます。詳細については、[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス （2537 ページ）を参照してください。

[SNMP Trap Configuration] ダイアログボックス

[SNMP Trap Configuration] ダイアログボックスを使用して、選択したセキュリティ デバイスの SNMP トラップ（イベント通知）を設定します。

トラップは参照とは異なります。トラップは、生成される**リンクアップイベント**、**リンクダウンイベント**、**Syslog イベント**など、特定のイベントに対する管理対象デバイスから管理ステーションへの割り込み「コメント」です。

デバイスの SNMP オブジェクト ID（OID）は、デバイスから送信される SNMP イベント トラップに表示されます。セキュリティデバイスで実行されている SNMP サービスは、2 つの機能を実行します。

- 管理ステーションからの SNMP 要求に応答します。
- セキュリティ アプライアンスからのトラップを受信するように登録されている管理ステーションまたはその他のデバイスにトラップを送信します。

Cisco セキュリティ デバイスでは、3 種類のトラップがサポートされます。

- ファイアウォール
- generic
- syslog

[SNMP Trap Configuration] ダイアログボックスでは、使用できるトラップが、[Standard]、[Entity MIB]、[Resource]、[Other] の 4 つのタブ付きパネルに表示されます。

ナビゲーション パス

[SNMP Trap Configuration] ダイアログボックスには、[SNMP] ページ （2519 ページ）からアクセスできます。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527 ページ）

フィールド リファレンス

表 *610 : [SNMP Trap Configuration]* ダイアログボックス

要素	説明
Enable All SNMP Traps	4 つすべてのタブ付きパネルをすばやく選択するには、このチェックボックスをオンにします。
Enable Syslog Traps	トラップ関連の Syslog メッセージの送信をイネーブルにするには、このチェックボックスをオンにします。 トラップされる Syslog メッセージの重大度は、[Logging Filters] ページ （2651 ページ）で設定されます。
次の 4 つのタブ付きパネルで、目的のイベント通知トラップを選択します。選択したデバイスに適用できるトラップだけがダイアログボックスに表示されます。	
標準	• [認証（Authentication）] : 未認可の SNMP アクセス。この認証エラーは、間違ったコミュニティ ストリングが付いたパケットによって発生します。 • [リンクアップ（Link Up）] : 通知に示されているとおり、デバイスの通信リンクの 1 つが使用可能になりました。 • [リンクダウン（Link Down）] : 通知に示されているとおり、デバイスの通信リンクの 1 つにエラーが発生しました。 • [コールドスタート（Cold Start）] : デバイスが自動で再初期化しているときに、その設定またはプロトコルエンティティの実装が変更されることがあります。 • [ウォームスタート（Warm Start）] : デバイスが自動で再初期化しているときに、その設定またはプロトコルエンティティの実装が変更されることはありません。

要素	説明
Entity MIB	• [現場交換可能ユニット挿入（Field Replaceable Unit Insert）]：示されているとおり、現場交換可能ユニット（FRU）が挿入されました（FRUには電源装置、ファン、プロセッサ モジュール、インターフェイス モジュールなどの組み立て部品が含まれます）。 • [現場交換可能ユニット除外（Field Replaceable Unit Remove）]：通知に示されているとおり、現場交換可能ユニット（FRU）が取り外されました。 • [設定変更（Configuration Change）]：通知に示されているとおり、ハードウェアに変更がありました。 • [ファン障害（Fan Failure）]：通知に示されているとおり、デバイスの冷却ファンに障害が発生しました。 • [CPU温度（CPU Temperature）]：中央処理装置の温度が、設定した制限に達しました。 • [電源装置障害（Power-Supply Failure）]：通知に示されているとおり、デバイスの電源装置に障害が発生しました。 • [冗長スイッチオーバー（Redundancy Switchover）]：通知に示されているとおり、冗長コンポーネントでスイッチオーバーが発生しました。 • [アラームがアサートされた（Alarm Asserted）]：アラームで示されている状態が存在します。 • [アラームがクリアされた（Alarm Cleared）]：アラームで示されている状態は存在しません。
リソース（Resource）	• [接続制限到達（Connection Limit Reached）]：このトラップは、設定した接続制限に達したため、接続試行が拒否されたことを示します。 • [リソース制限到達（Resource Limit Reached）]：通知に示されているとおり、この通知は設定したリソース制限に達すると生成されます。 • [リソースレート制限到達（Resource Rate Limit Reached）]：通知に示されているとおり、この通知は設定したリソースのレート制限に達すると生成されます。

要素	説明
その他	

要素	説明
	• [IKEv2 開始（IKEv2 Start）]：インターネット キー エクスチェンジ バージョン 2（IKEv2）の交換が起動しました。 • [IKEv2 停止（IKEv2 Stop）]：インターネット キー エクスチェンジ バージョン 2（IKEv2）の交換が停止しました。 • [メモリしきい値（Memory Threshold）]：通知に示されているとおり、使用可能な空きメモリが、設定したしきい値を下回りました。 • [ASA の CPU 上昇しきい値（ASA CPU Rising Threshold）]：CPU リソースの使用率が、[期間（Period）] で指定した期間に [パーセンテージ（Percentage）] の値を超過すると、この通知が起動します。 [パーセンテージ（Percentage）]：CPU リソースの使用率の上限を、使用可能なリソース全体のパーセンテージとして入力します。有効な値の範囲は 10 ～ 94 です。デフォルトは 70 % です。 [期間（Period）]：時間の長さを分単位で入力します。この期間内に [パーセンテージ（Percentage）] で指定した使用可能なパーセンテージを超過すると通知が発行されます。有効値の範囲は 1 ～ 60 です。 • [インターフェイスしきい値（Interface Threshold）]：物理インターフェイスの使用率が、[パーセンテージ（Percentage）] で指定した、帯域幅全体のパーセンテージを超過すると、この通知が発行されます。 [パーセンテージ（Percentage）]：インターフェイスの使用率の上限を、使用可能な帯域幅全体のパーセンテージとして入力します。有効な値の範囲は 30 ～ 99 です。デフォルトは 70 % です。 • [IPSec 開始（IPSec Start）]：通知に示されているとおり、IPSec が起動しました。 • [IPSec 停止（IPSec Stop）]：通知に示されているとおり、IPSec が停止しました。 • [リモートアクセスセッションのしきい値を超過（Remote Access Session Threshold Exceeded）]：通知に示されているとおり、リモートアクセスセッションの数が、定義した制限に達しました。 • [NAT パケット破棄（NAT Packet Discard）]：IP パケットが NAT 機能により廃棄されると、この通知が生成されます。ネットワーク アドレス変換の使用可能なアドレスまたはポートが、設定したしきい値を下回りました。 • [CPU 上昇しきい値（CPU Rising Threshold）]：CPU リソースの使用率が、[期間（Period）] で指定した期間に [パーセンテージ（Percentage）] の値を超過すると、この通知が起動します。

要素	説明
	[パーセンテージ（Percentage）]：CPU リソースの使用率の上限を、使用可能なリソース全体のパーセンテージとして入力します。有効な値の範囲は 10 ～ 100 です。デフォルトは 70 % です。 [期間（Period）]：時間の長さを秒単位で入力します。この期間内に [パーセンテージ（Percentage）] で指定した使用可能なパーセンテージを超過すると通知が発行されます。有効な値の範囲は、60 ～ 3600 です。

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスを使用して、[SNMP] ページにある [SNMPホスト（SNMP Hosts）] テーブルのエントリを追加および編集します。これらのエントリは、セキュリティデバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

9.1(5) から 9.3(2) までのソフトウェアバージョンを実行している ASA デバイスの場合、129 の SNMP ホストを設定できます。9.1(5) より前のソフトウェアバージョンを実行している ASA デバイスの場合、設定できる SNMP ホストは 32 だけです。

バージョン 4.9 以降、Cisco Security Manager では、ソフトウェアバージョン 9.4(1) 以降を実行している ASA デバイスに最大 4096 の SNMP ホストを設定できます。ただし、この数の 129 のみがトラップに使用できます。129 を超えるトラップ設定の SNMP ホストを設定することはできません。

ナビゲーション パス

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスには、 [SNMP] ページ （2519 ページ）からアクセスできます。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMP Trap Configuration] ダイアログボックス （2522 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （2531 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （2533 ページ）

フィールド リファレンス

表 *611 : [SNMP*ホストアクセスエントリの追加/編集（*Add/Edit SNMP Host Access Entry*）*]* ダイアログボックス

要素	説明
Interface Name	このSNMP管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。
IPアドレス	IPアドレスを入力するか、またはSNMP管理ステーションを表すネットワークまたはホストのオブジェクトを選択します。 （注） Cisco Security Manager バージョン4.17以降、SNMP ポリシーの IPv6 アドレスは ASA 9.9.2 デバイス以降でサポートされます。 （注） IPv6 アドレスのネットワークまたは範囲を設定できるようになりました。
UDP ポート（UDP Port）	（任意）SNMP ホストからの要求用の UDP ポートを入力します。このフィールドを使用して、[SNMP] ページの指定したグローバル値を上書きできます。
コミュニティストリング（Community String） 確認（Confirm）	要求をセキュリティデバイスに送信するときにSNMP管理ステーションで使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。そのため、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。 [確認（Confirm）] フィールドにパスワードをもう一度入力します。
SNMP バージョン（SNMP Version）	管理ステーションで使用する SNMP のバージョン（**1**、**2c**、または **3**）を選択します。
SNMP ユーザ名	SNMPバージョン3を選択した場合は、SNMPユーザを選択します。SNMP ユーザについては、[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （2533 ページ）を参照してください。
Server Poll/Trap Specification	この管理ステーションとの通信タイプを指定します（ポーリングのみ、トラップのみ、またはトラップとポーリングの両方）。次のいずれかまたは両方をオンにします。 • [Poll]：セキュリティ デバイスは、管理ステーションからの定期的な要求を待機します。 • [Trap]：トラップイベントが発生すると、デバイスはトラップイベントを送信します。

[SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックス

Cisco Security Manager バージョン 4.12 以降では、[SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ダイアログボックスを使用して、[SNMP] ページの [SNMPホストグループ（SNMP Host Group）] テーブルのエントリを追加および編集できます。これらのエントリは、セキュリティ デバイスへのアクセスが許可されている SNMP 管理ステーションを示します。

9.1(5) から 9.4 までのソフトウェアバージョンを実行している ASA デバイスの場合、129 の SNMP ホストを設定できます。9.1(5) より前のソフトウェアバージョンを実行している ASA デバイスの場合、設定できる SNMP ホストは 32 だけです。

バージョン 4.9 以降、Cisco Security Manager では、ソフトウェアバージョン 9.4(1) 以降を実行している ASA デバイスに最大 4096 の SNMP ホストを設定できます。ただし、トラップに使用できるのは 129 ホストのみです。129 を超えるトラップ設定の SNMP ホストを設定することはできません。

（注） [SNMPホストグループエントリの追加/編集（Add/Edit SNMP Host Group Entry）] ページで [SNMPホスト（SNMP Host）] または [ホストグループ（Host Group ）] エントリを追加または編集した後に、Networks/Host Policy Object Manager で使用されているアドレスの範囲またはネットワークオブジェクトを編集すると、Cisco Security Manager では SNMP トラップの総数が検証されません。したがって、トラップエントリ数が 129 を超えると、展開が失敗します。

ナビゲーション パス

[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスには、[SNMP] ページ （2519 ページ）からアクセスできます。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMP Trap Configuration] ダイアログボックス （2522 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （2531 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （2533 ページ）

フィールド リファレンス

表 *612 : [SNMP*ホストアクセスエントリの追加/編集（*Add/Edit SNMP Host Access Entry*）*]* ダイアログボックス

要素	説明
Interface Name	この SNMP 管理ステーションがデバイスにアクセスするインターフェイスを入力または選択します。
IPアドレス	IP アドレスを入力するか、または SNMP 管理ステーションを表すネットワークまたはホストのオブジェクトを選択します。 （注） SNMP ホストグループエントリは、ASA 9.17(1) 以降のデバイスの IPV6 グループ化をサポートします。[SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックスで、IPV6 ネットワークまたは範囲を設定できます。 [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス（2527 ページ）
UDP ポート（UDP Port）	（任意）SNMP ホストからの要求用の UDP ポートを入力します。このフィールドを使用して、[SNMP] ページの指定したグローバル値を上書きできます。
コミュニティ ストリング（Community String） 確認（Confirm）	要求をセキュリティ デバイスに送信するときに SNMP 管理ステーションで使用されるパスワードを入力します。SNMP コミュニティ ストリングは、SNMP 管理ステーションと管理対象のネットワーク ノード間の共有秘密キーです。そのため、着信 SNMP 要求が有効かどうかを判断するためにパスワードが使用されます。パスワードは大文字小文字が区別される、最大 32 文字の英数字の文字列です。スペースは使用できません。 [確認（Confirm）] フィールドにパスワードをもう一度入力します。
SNMP バージョン（SNMP Version）	管理ステーションで使用する SNMP のバージョン（**1**、**2c**、または **3**）を選択します。

要素	説明
Server Poll/Trap Specification	この管理ステーションとの通信タイプを指定します（ポーリングのみ、トラップのみ、またはトラップとポーリングの両方）。次のいずれかまたは両方をオンにします。 • [Poll]：セキュリティデバイスは、管理ステーションからの定期的な要求を待機します。 • [Trap]：トラップ イベントが発生すると、デバイスはトラップ イベントを送信します。 （注） 同じSNMPホストグループに対して、トラップとポーリングの両方を有効にすることはできません。両方有効にする必要がある場合は、該当するホストに対してsnmp-server hostコマンドを使用することを推奨します。

[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス

[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックスを使用して、[SNMP] ページにある [SNMPグループ（SNMP Groups）] テーブルのエントリを追加または編集します。SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMPグループ内のユーザーは、SNMPグループのセキュリティモデルに一致する必要があります。これらのパラメータは、SNMPグループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

設定上の目的のために、認証とプライバシーのオプションはセキュリティモデルにまとめられます。セキュリティモデルはユーザーとグループに適用され、次の3つのタイプに分けられます。

- NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。
- Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

注記

- グループを削除する前に、そのグループに関連付けられているすべてのユーザーが削除されていることを確認する必要があります。削除する必要があるユーザーに関連付けられて

いるホストがある場合は、ユーザーを削除する前にそれらのホストを削除する必要があります。

- 特定のセキュリティモデルを使用して特定のグループに属するようにユーザーが設定されている場合、そのグループのセキュリティレベルを変更するには、次の手順を実行する必要があります。

  1. グループに属するユーザーに関連付けられているすべてのホストエントリを削除します。
  2. そのグループからユーザーを削除します。
  3. 変更をデバイスに展開します。
  4. グループのセキュリティ レベルを変更します。
  5. そのグループに属するユーザーを追加します。
  6. グループに追加したユーザーに属するホストを追加します。
  7. 変更をデバイスに展開します。

ナビゲーション パス

[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックスには、[SNMP] ページ （2519 ページ）からアクセスできます。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMP Trap Configuration] ダイアログボックス （2522 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527 ページ）
- [SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス （2533 ページ）

フィールド リファレンス

表 *613 : [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス*

要素	説明
グループ名（Group Name）	SNMP グループの名前を入力します。グループ名は 32 文字以下にする必要があります。

要素	説明
セキュリティ レベル（Security Level）	グループのセキュリティレベルを指定します。 • NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。 • Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。 • Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックス

[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックスを使用して、ユーザを SNMP グループに追加するか、[SNMP] ページの [SNMPユーザ（SNMP User）] テーブルのエントリを編集します。SNMP ユーザは、割り当てられたグループのセキュリティモデルを継承します。

注記

- ユーザーが作成された後は、そのユーザーが属するグループは変更できません。
- ユーザを削除するには、そのユーザ名に関連付けられているホストが設定されていないことを確認する必要があります。

ナビゲーション パス

[SNMPユーザエントリの追加/編集（Add/Edit SNMP User Entry）] ダイアログボックスには、[SNMP] ページ （2519 ページ）からアクセスできます。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMP Trap Configuration] ダイアログボックス （2522 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス（2531 ページ）

フィールド リファレンス

表 *614 : [SNMP*ユーザエントリの追加/編集（*Add/Edit SNMP User Entry*）*]* ダイアログボックス

要素	説明
グループ名（Group Name）	このユーザが所属する SNMP グループを選択します。SNMP グループについては、[SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （2531 ページ）を参照してください。
セキュリティ レベル（Security Level）	選択したグループのセキュリティレベルを表示します。 • NoAuth：認証もプライバシーもありません。メッセージにセキュリティが適用されないことを意味します。 • Auth：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。 • Priv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。
ユーザー名	SNMP ユーザの名前を入力します。ユーザ名は 32 文字以下で、選択した SNMP サーバー グループで一意である必要があります。

要素	説明

エンジンID（Engine ID）
 	
（SNMP バージョン v3 のみ）
	v3 で認証に使用される SNMP EngineID 識別子。
	
	複数のエンジン ID をカンマで区切って入力できます。エンジン ID 識別子は有効である必要があり、各エンジン ID は 1 ～ 257 文字の範囲内である必要があります。
	
	• MD5 アルゴリズムを使用して SNMP ユーザの EngineID を構成する場合、EngineID は有効なものである必要があります。EngineID が有効でない場合、設定のプレビューは「未処理の設定の生成に失敗しました（failed to generate raw config）」というエラーで失敗します。たとえば、入力された EngineID が 111 の場合、設定のプレビューは失敗します。
	
	• セキュリティレベルが NoAuth の SNMP グループの場合は、EngineID 識別子を指定しないでください。展開時に、ASA はこのエンジン ID を無視し、デフォルトのローカルエンジン ID を使用するためです。
	
	• デバイスの次のダイナミック動作は、Security Manager では処理できません。
	
	  • フェールオーバー ASA デバイスをバージョン 8.x または 9.x からバージョン 9.6(2) にアップグレードすると、デバイスは複数の SNMP エンジン ID に対して複数の SNMP ユーザコマンドを自動的に作成します。デバイスからエンジン ID を取得して、この [エンジン ID（Engine ID）] テキストボックスにコピーする必要があります。デバイスからエンジン ID を取得する方法については、[SNMP] ページ （2519 ページ）を参照してください。
	
	  • ASA デバイスをフェールオーバー構成に追加する、またはフェールオーバー構成から削除する場合、ASA デバイスは既存のエンジン ID に対して新しい SNMP ユーザコマンドを自動的に削除または作成するため、エンジン ID を手動で入力する必要があります。

パスワード暗号化タイプ（Encrypt Password Type）	使用するパスワードのタイプを指定します（[クリアテキスト（Clear Text）] または [暗号化（Encrypted）]）。 パスワードタイプが [クリアテキスト（Clear Text）] の場合、Security Manager はデバイスへの展開時にパスワードを暗号化します。パスワードタイプが [暗号化（Encrypted）] の場合、Security Manager は暗号化されたパスワードを直接展開します。Security Manager がクリアテキストのパスワードをデバイスに直接展開することはありません。

要素	説明
認証アルゴリズムタイプ（Auth Algorithm Type）	使用する認証のタイプを指定します（MD5、SHA、または SHA256）。 （注） バージョン 4.21 以降、Cisco Security Manager は ASA 9.14(1) 以降のデバイスに対して SHA256 認証タイプをサポートします。MD5 認証タイプは、今後の ASA バージョンで廃止されます。
認証パスワード（Authentication Password） 確認（Confirm）	認証に使用するパスワードを入力します。パスワード暗号化タイプに [暗号化（Encrypted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。 （注） パスワードの長さは、選択した認証アルゴリズムによって異なります。すべてのパスワードの長さを 256 文字以下とする必要があります。 暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。
暗号化タイプ（Encryption Type）	使用する暗号化のタイプを指定します（AES128、AES192、AES256、3DES、DES）。 （注） AES または 3DES 暗号化を使用するには、デバイスに適切なライセンスをインストールしておく必要があります。
Encryption Password 確認（Confirm）	暗号化に使用するパスワードを入力します。パスワード暗号化タイプに [暗号化（Encrypted）] を選択した場合、パスワードは xx:xx:xx... という形式にフォーマットされます。ここで、xx は 16 進数の値です。 暗号化を行う場合のパスワードの長さは選択された暗号化のタイプにより異なります。パスワードの長さは次のとおりです（各 xx は 1 つのオクテットを示します）。 • AES 128 では 16 オクテットとする必要があります • AES 192 では 24 オクテットとする必要があります • AES 256 では 32 オクテットとする必要があります • 3DES では 32 オクテットとする必要があります • DES の長さはさまざまです。 （注） すべてのパスワードの長さを 256 文字以下とする必要があります。 暗号化パスワードタイプに [クリア テキスト（Clear Text）] を選択した場合、[確認（Confirm）] フィールドにパスワードをもう一度入力してください。

[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックス

バージョン4.12以降、Security Managerでは、[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックスを使用して、複数の SNMP ユーザを含むユーザリストを追加できます。

注記

- 特定のホストグループで使用されているユーザリストは削除できません。
- 特定のユーザリストで参照されている SNMP ユーザを削除することはできません。

ナビゲーション パス

[SNMPユーザリストエントリの追加/編集（Add/Edit SNMP User List Entry）] ダイアログボックスには、[SNMP] ページ （2519 ページ）からアクセスできます。

フィールド リファレンス

表 *615 : [SNMP*ユーザリストエントリの追加/編集（*Add/Edit SNMP User List Entry*）*]* ダイアログボックス

要素	説明
ユーザリスト名	ユーザリストの名前を入力します。ユーザリスト名の長さは 1 ～ 33 文字にする必要があります。
ユーザ名	ドロップダウンリストからユーザ名を選択します。

関連項目

- SNMP の設定 （2516 ページ）
- [SNMP Trap Configuration] ダイアログボックス （2522 ページ）
- [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527 ページ）
- [SNMPグループエントリの追加/編集（Add/Edit SNMP Group Entry）] ダイアログボックス （2531 ページ）

[Telnet] ページ

[Telnet] ページを使用して、Telnet プロトコルを使用したファイアウォール デバイスへの接続を、特定のホストまたはネットワークにだけ許可するルールを設定します。

このルールにより、ファイアウォール デバイス インターフェイスを介した管理 Telnet アクセスが特定の IP アドレスおよびネットマスクに制限されます。このルールに準拠する接続試行

は、設定済みの AAA サーバまたは Telnet パスワードによって認証される必要があります。Telnet セッションは、[Monitoring] > [Telnet Sessions] を使用してモニタできます。

（注） シングルコンテキスト モードでは一度に 5 つの Telnet セッションだけアクティブにできます。ASA 上のマルチコンテキスト モードでは、コンテキストあたり 5 つの Telnet だけをアクティブにでき、ブレードあたり 100 個の Telnet セッションをアクティブにできます。リソース クラスでは、管理者がこのパラメータをさらに調整できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Telnet]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Telnet]** を選択します。[Telnet] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Telnet Configuration] ダイアログボックス （2538 ページ）

フィールド リファレンス

表 616 : [Telnet] ページ

要素	説明
タイムアウト（Timeout）	Telnet セッションがファイアウォール デバイスによって閉じられる前にアイドル状態でいられる時間（分単位）。値の範囲は 1 ～ 1440 分です。
Telnet Access Table	
インターフェイス	クライアントから Telnet パケットを受信するインターフェイス。
IP Addresses	指定されたインターフェイスを通じて Telnet コンソールにアクセスできる各ホストまたはネットワークの IP アドレスおよびネットワーク マスク。

[Telnet Configuration] ダイアログボックス

[Telnet Configuration] ダイアログボックスを使用して、インターフェイスの Telnet オプションを設定します。

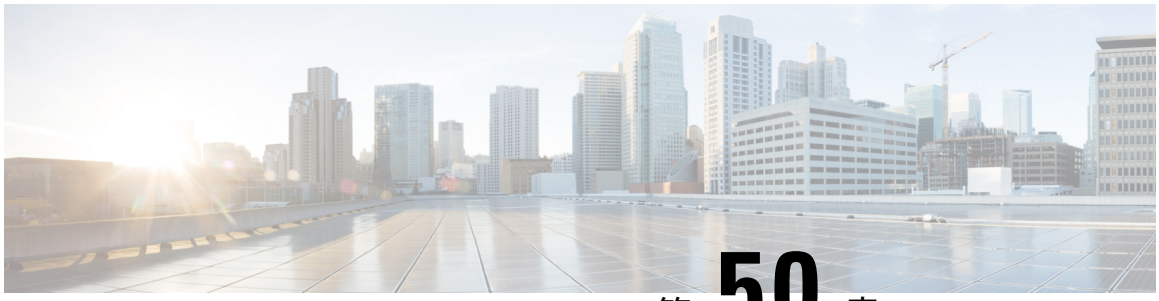
ナビゲーション パス

[Telnet Configuration] ダイアログボックスには、[Telnet] ページ （2537 ページ）からアクセスできます。

フィールド リファレンス

表 *617 : [Telnet Configuration]* ダイアログボックス

要素	説明
Interface Name	クライアントからの Telnet パケットを受信できるインターフェイスを入力または選択します。 （注） Cisco Security Manager バージョン 4.17 以降、ASA 9.9.2 以降のデバイスで Telnet の BVI インターフェイスを設定できます。ただし、マルチコンテキストでは、「トランスペアレント」モードのセキュリティコンテキストはBVIインターフェイスのみをサポートします。
IP Addresses/Netmask	指定したインターフェイスを通じてファイアウォールデバイスの Telnet コンソールへのアクセスを許可される各ホストまたはネットワークの IP アドレスとネットマスクを「/」で区切って入力または選択します。複数のエントリを指定する場合は、カンマで区切ります。 （注） アクセスを単一IPアドレスに制限するには、ネットマスクとして 255.255.255.255 または 32 を使用します。内部ネットワークのサブネットワーク マスクは使用しないでください。 （注） バージョン 4.13 以降、Cisco Security Manager は、IPv6 デバイスのポリシー（グループ、ホスト、アドレスの範囲、およびネットワーク）をサポートします。



第 50 章

フェールオーバーの設定

[Failover] ページで、選択したセキュリティ アプライアンスのフェールオーバーを設定できます。[Failover] ページで設定できる内容およびページ全体の外観は、選択したデバイスのタイプ、動作モード（ルーテッドまたはトランスペアレント）、およびコンテキスト モード（シングルまたはマルチ）によって若干異なる場合があります。

つまり、フェールオーバーの設定方法は、セキュリティ アプライアンスの動作モードとセキュリティ コンテキストの両方に応じて異なります。

インターフェイスをフェールオーバー リンクとして割り当てる場合は、次の警告に注意してください。

- [AddInterface] と [Edit Interface] ダイアログボックスでインターフェイスを定義できますが、設定しないでください。特に、インターフェイス名は指定しないでください。このパラメータを指定すると、インターフェイスをフェールオーバー リンクとして使用できなくなります。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください。
- IPv6 アドレスはフェールオーバー リンクではサポートされていません。
- ASA 5505 では、別のインターフェイスのバックアップとして割り当てられたインターフェイスは、フェールオーバー リンクとして使用できません（ただし、これを防ぐためのチェックは実行されません）。
- PPPoE 対応のインターフェイスをフェールオーバー リンクとして割り当てないでください。PPPoE とフェールオーバーを同じデバイス インターフェイスに設定しないでください（ただし、これを防ぐためのチェックは実行されません）。
- フェールオーバー インターフェイスでは、別のインターフェイスと同じ IP アドレス（特に、管理 IP アドレス）は使用できません（ただし、これを防ぐためのチェックは実行されません）。

また、インターフェイスをフェールオーバー リンクとして割り当てると、そのインターフェイスは [Interfaces] ページに表示されますが、[Interfaces] ページでそのインターフェイスを編集および削除することはできません。ただし、唯一の例外として、物理インターフェイスをステートフル フェールオーバー リンクとして設定している場合は、その速度とデュプレックスを設定できます。

この章は次のトピックで構成されています。

• フェールオーバーについて （2542 ページ）
• 基本的なフェールオーバー設定 （2547 ページ）
• アクティブ/スタンバイ フェールオーバー設定の追加手順 （2552 ページ）
• フェールオーバー ポリシー （2553 ページ）

フェールオーバーについて

フェールオーバーを使用すると、同一の2台のセキュリティアプライアンスで、一方に障害が発生した場合にもう一方がファイアウォール動作を引き継げるように設定できます。セキュリティ アプライアンスのペアを使用すると、オペレータの介入なしに、システムのハイ アベイラビリティが実現されます。

リンクされたこれらのセキュリティアプライアンスは、専用リンクを介してフェールオーバー情報をやり取りします。このフェールオーバー リンクは、LAN ベースの接続であるか、または PIX セキュリティ アプライアンスの場合は専用シリアル フェールオーバー ケーブルです。次の情報がフェールオーバー リンク経由で伝達されています。

- 現在のフェールオーバー状態（アクティブまたはスタンバイ）
- 「Hello」メッセージ（「キープアライブ」とも呼ばれる）
- ネットワーク リンクの状態
- MAC アドレス交換
- 設定の複製
- 接続ごとの状態情報（ステートフル フェールオーバーの場合）

注意 フェールオーバー リンクを介して送信されたすべての情報は、フェールオーバー キーで通信を保護しないかぎり、クリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用している場合、この情報には、トンネルの確立に使用されたユーザ名、パスワード、および事前共有キーが含まれます。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。特に、VPN トンネルの終端にセキュリティ アプライアンスを使用している場合は、フェールオーバー キーを使用してフェールオーバー通信を保護することを推奨します。

Cisco セキュリティ アプライアンスは、次の 2 つのタイプのフェールオーバーをサポートします。

- **アクティブ/スタンバイ**：アクティブ セキュリティ アプライアンスは、すべてのネットワークトラフィックを検査し、一方スタンバイ セキュリティ アプライアンスは、アクティブアプライアンスで障害が発生するまでアイドル状態のままとなります。アクティブ セ

キュリティ アプライアンスの設定に加えた変更は、フェールオーバー リンクを介してスタンバイ セキュリティ アプライアンスに送信されます。

フェールオーバーが発生すると、スタンバイ セキュリティ アプライアンスがアクティブ装置になり、前にアクティブであった装置の IP アドレスと MAC アドレスを引き継ぎます。IP アドレスまたは MAC アドレスのこの変更はネットワーク上の他のデバイスには認識されないため、ARP エントリがネットワーク上で変更されたりタイムアウトしたりすることはありません。

アクティブ/スタンバイ フェールオーバーを使用できるのは、シングル コンテキスト モードまたはマルチ コンテキスト モードで動作しているセキュリティ アプライアンスです。シングル コンテキスト モードでは、アクティブ/スタンバイ フェールオーバーだけを使用でき、すべてのフェールオーバー設定が [Failover] ページを使用して行われます。

（注） アクティブ/スタンバイ フェールオーバーを使用する場合、設定の変更はすべてアクティブ装置に対して行う必要があります。アクティブ装置は、これらの変更内容をスタンバイ装置に自動的に複製します。スタンバイ装置は、Security Manager デバイス リストにインポートまたは追加されません。また、認証証明書をアクティブ デバイスからスタンバイ デバイスに手動でコピーする必要があります。詳細については、アクティブ/スタンバイ フェールオーバー設定の追加手順 （2552 ページ）を参照してください。

- **アクティブ/アクティブ**：両方のセキュリティアプライアンスが、一方がアクティブでもう一方がスタンバイになるようにそれぞれのロールを切り替えて、ネットワークトラフィックをコンテキストベースで検査します。これは、アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードで動作するセキュリティ アプライアンスだけで使用できることを意味します。

ただし、アクティブ/アクティブ フェールオーバーが、マルチ コンテキスト モードでの必須のフェールオーバーというわけではありません。つまり、マルチ コンテキスト モードで動作しているデバイスでは、アクティブ/スタンバイ フェールオーバーまたはアクティブ/アクティブ フェールオーバーを設定できます。いずれの場合も、システム コンテキストでシステム レベルのフェールオーバー設定を指定し、個々のセキュリティ コンテキストでコンテキスト レベルのフェールオーバー設定を指定します。

この項目の詳細については、アクティブ/アクティブ フェールオーバー （2544 ページ）を参照してください。

さらに、フェールオーバーは、ステートレスまたはステートフルにすることができます。

- **ステートレス**：「通常」フェールオーバーとも呼ばれます。ステートレス フェールオーバーでは、フェールオーバーが発生すると、アクティブな接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。
- **ステートフル**：フェールオーバーペアのアクティブ装置は、接続ごとの状態情報をスタンバイ装置に継続的に渡します。フェールオーバーの発生後も、新しいアクティブ装置で同

じ接続情報を使用できます。サポートされるエンドユーザアプリケーションは、現在の通信セッションを保持するために再接続する必要はありません。

詳細については、ステートフル フェールオーバー （2546 ページ）を参照してください。

関連項目

- 基本的なフェールオーバー設定 （2547 ページ）
- フェールオーバー ポリシー （2553 ページ）

アクティブ/アクティブ フェールオーバー

アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードで動作するセキュリティ アプライアンスだけで使用できます。アクティブ/アクティブ フェールオーバー設定では、両方のセキュリティ アプライアンスがコンテキストごとにネットワーク トラフィックを検査します。つまり、各コンテキストで、一方のアプライアンスがアクティブデバイスで、もう一方のアプライアンスがスタンバイ デバイスとなります。

アクティブロールとスタンバイロールは、セキュリティコンテキストのセット全体でほぼ任意で割り当てられます。

セキュリティ アプライアンスでアクティブ/アクティブ フェールオーバーをイネーブルにするには、2 つのフェールオーバー グループのいずれかにセキュリティ コンテキストを割り当てる必要があります。フェールオーバー グループは、単に 1 つ以上のセキュリティ コンテキストの論理グループです。フェールオーバー グループ 1 がアクティブ状態になる装置にフェールオーバー グループ割り当てを指定する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの各装置には、プライマリまたはセカンダリのどちらかが指定されます。アクティブ/スタンバイ フェールオーバーとは異なり、両方の装置が同時に起動した場合にどちらの装置がアクティブになるかは指示されていません。設定の各フェールオーバー グループには、プライマリまたはセカンダリ ロール プリファレンスが設定されます。このプリファレンスにより、両方の装置が同時に起動したときに、フェールオーバー グループのコンテキストがアクティブ状態で表示される装置が決まります。ペアの一方の装置にアクティブ状態の両方のフェールオーバー グループを含めて、もう一方の装置にスタンバイ状態のフェールオーバー グループを含めることができます。ただし、一般的な設定では、各フェールオーバー グループに別々のロール プリファレンスを割り当てて、それぞれを別の装置上でアクティブにすることでデバイスにトラフィックを分散させます。

（注） Cisco Security Manager は、アクティブ/アクティブ フェールオーバー モードのセキュリティ コンテキストを確実に管理するために、各コンテキストの管理インターフェイス用の IP アドレスを要求して、フェールオーバー ペアのアクティブなセキュリティ コンテキストと直接通信できるようにします。

初期設定同期は、一方または両方の装置が起動すると実行されます。この同期は、次のように実行されます。

- 両方の装置が同時に起動した場合、設定はプライマリ装置からセカンダリ装置に同期されます。
- 一方の装置がすでにアクティブであるときに、もう一方の装置が起動した場合は、起動した装置が、すでにアクティブな装置から設定を受信します。

両方の装置が動作中になった後で、次のように、コマンドが一方の装置からもう一方の装置に複製されます。

- セキュリティ コンテキスト内で入力されたコマンドは、そのセキュリティ コンテキストがアクティブ状態で表示される装置からピア装置に複製されます。

（注） あるコンテキストがある装置でアクティブ状態と見なされるのは、そのコンテキストが属するフェールオーバー グループがその装置上でアクティブ状態である場合です。

- システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から、フェールオーバー グループ 1 がスタンバイ状態である装置に複製されます。
- 管理コンテキストで入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から、フェールオーバー グループ 1 がスタンバイ状態である装置に複製されます。

コマンドの複製の実行に適切な装置上でコマンドを入力しなかった場合は、設定が非同期になります。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

（注） アクティブ/アクティブ フェールオーバー設定のピア デバイスをブートストラップすると、そのブートストラップ設定は、それぞれのフェールオーバー ピア デバイスのシステム コンテキストにだけ適用されます。

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリ装置で両方のフェールオーバー グループをアクティブと指定した場合にフェー

ルオーバー グループ 1 で障害が発生すると、フェールオーバー グループ 2 はプライマリ装置でアクティブのままですが、フェールオーバー グループ 1 はセカンダリ装置でアクティブになります。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

ステートフル フェールオーバー

（注） ステートフル フェールオーバーは、ASA 5505 アプライアンスではサポートされていません。

ステートフル フェールオーバーがイネーブルになっている場合、フェールオーバー ペアのアクティブ装置は、引き続きスタンバイ装置上の現在の接続状態情報を更新します。フェールオーバーの発生時、サポートされるエンドユーザアプリケーションは、現在の通信セッションを保持するために再接続する必要がありません。

（注） ステート リンクおよび LAN フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

ステートフル フェールオーバーを使用するには、すべての状態情報をスタンバイ装置に渡すようにリンクを設定する必要があります。シリアル フェールオーバー インターフェイス（PIX プラットフォームでだけ使用可能）ではなく、LAN フェールオーバー接続を使用している場合、ステート リンクおよびフェールオーバー リンクに同じインターフェイスを使用できます。ただし、スタンバイ装置に状態情報を渡すときは、専用のインターフェイスを使用することを推奨します。

ステートフル フェールオーバーがイネーブルになっている場合、次の情報がスタンバイ装置に渡されます。

- NAT 変換テーブル
- タイムアウト接続を含む、TCP 接続テーブル（HTTP を除く）
- HTTP 接続状態（HTTP レプリケーションがイネーブルの場合）
- H.323、SIP、および MGCP UDP メディア接続
- システム クロック
- ISAKMP および IPSec SA テーブル

ステートフル フェールオーバーがイネーブルになっている場合、次の情報はスタンバイ装置にコピーされません。

- HTTP 接続テーブル（HTTP レプリケーションがイネーブルでない場合）
- ユーザ認証（UAUTH）テーブル
- ARP テーブル
- ルーティング テーブル

基本的なフェールオーバー設定

次の手順では、基本的なフェールオーバー設定について説明します。インターフェイスをフェールオーバー リンクとして割り当てる場合は、次の警告に注意してください。

- [AddInterface] と [Edit Interface] ダイアログボックスでインターフェイスを定義できますが、設定しないでください。特に、インターフェイス名は指定しないでください。このパラメータを指定すると、インターフェイスをフェールオーバーリンクとして使用できなくなります。
- ASA 5505 では、別のインターフェイスのバックアップとして割り当てられたインターフェイスは、フェールオーバー リンクとして使用できません（ただし、これを防ぐためのチェックは実行されません）。
- PPPoE 対応のインターフェイスをフェールオーバー リンクとして割り当てないでください。PPPoE とフェールオーバーを同じデバイス インターフェイスに設定しないでください（ただし、これを防ぐためのチェックは実行されません）。
- フェールオーバー インターフェイスでは、別のインターフェイスと同じ IP アドレス（特に、管理 IP アドレス）は使用できません（ただし、これを防ぐためのチェックは実行されません）。

（注） フェールオーバー設定を保存すると、その設定はセキュリティ アプライアンスとフェールオーバー ピアの両方に適用されます。

はじめる前に

フェールオーバー設定が許可されたライセンスがデバイスにインストールされている必要があります。ASA 5505 と 5510 デバイスでは、このフェールオーバー ライセンスはオプションのライセンスです。フェールオーバーライセンスは、ASDM またはデバイスの CLI を使用して、Security Manager の外部にインストールする必要があります。また、デバイスプロパティの（デバイスを右クリックして [デバイスプロパティ（Device Properties）] を選択）の [全般（General）] ページで [ライセンスはフェールオーバーをサポート（License Supports Failover）] オプションを必ず選択します。デバイスをインベントリに追加するときにライセンスをインストールする

場合や、ライセンスをインストールしてからデバイス ポリシーを再検出する場合、Security Manager はライセンスを識別して、このオプションを適切に設定します。

このオプションを選択しても、ライセンスがインストールされていない場合、展開は失敗します。このオプションを選択しないと、ポリシーを設定しても、Security Manager によってデバイスにフェールオーバー ポリシーが展開されません。

関連項目

- デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）
- フェールオーバーについて （2542 ページ）
- アクティブ/スタンバイ フェールオーバー設定の追加手順 （2552 ページ）
- フェールオーバー ポリシー （2553 ページ）

ステップ 1 デバイスビューが現在のアプリケーションビューであることを確認します。必要に応じて、ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

（注） デバイス ビューを使用したデバイス ポリシーの設定の詳細については、デバイス ビューおよび Site-to-Site VPN Manager におけるポリシーの管理 （247 ページ）を参照してください。

ステップ 2 設定するアプライアンスを選択します。

ステップ 3 デバイスポリシーセレクタで [プラットフォーム（Platform）] エントリを展開し、次に [デバイス管理（Device Admin）] を展開して、[フェールオーバー（Failover）] を選択します。

[Failover] ページが表示されます。

ステップ 4 （PIX のみ）[フェールオーバー方式（Failover Method）]（[シリアルケーブル（Serial Cable）] または [LANベース（LAN Based）]）を選択します。[Serial Cable] を選択する場合、[LAN Failover] 設定はディセーブルになります。2 台のデバイスを接続するケーブルが正しく接続されていることを確認します。

ステップ 5 [フェールオーバーの有効化（Enable Failover）] を選択して、このアプライアンス上でのフェールオーバーをイネーブルにします。

ステップ 6 （任意）[Settings] ボタンをクリックして、選択したデバイスの [Settings] ダイアログボックスを開きます。[Settings] ダイアログボックスの内容は、デバイスのタイプ、およびデバイスがシングル モードまたはマルチ モードのどちらで動作しているかによって異なります。一部のオプションが使用できない場合があります。次の項を参照してください。

- [Settings] ダイアログボックス （2570 ページ）（ASA/PIX 7+）
- [Advanced Settings] ダイアログボックス （2562 ページ）（FWSM）

ステップ 7 [ブートストラップ（Bootstrap）] ボタンをクリックして、[LANフェールオーバー用のブートストラップ設定（Bootstrap configuration for LAN failover）] ダイアログボックスを開きます。このダイアログボックスでは、LAN フェールオーバー設定内のプライマリデバイスとセカンダリデバイスに適用できるブートストラップ設定が示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）を参照してください。

ステップ 8 （マルチコンテキストデバイスのみ）[設定（Configuration）] セクションで、フェールオーバーモード（[アクティブ/アクティブ（Active/Active）] または [アクティブ/スタンバイ（Active/Standby）]）を選択します。

ステップ 9 （任意）次の手順を実行して、2 台のデバイス間の LAN フェールオーバー通信用のインターフェイスを設定します。

a) LAN ベースの通信用のデバイスインターフェイスを割り当て、次にキーボードの Tab キーを押してページを更新します。

PIX デバイスおよび ASA デバイスでは、このドロップダウン リストに、デバイスで定義されているインターフェイスが表示されます。ポート ID（gigabitethernet1 など）を入力するか、またはインターフェイスをすでに定義している場合はポートを選択できます。

FWSM では、このインターフェイス リストには VLAN ID は読み込まれません。ユーザは、使用する必要がある VLAN の数値 ID を入力する必要があります。

（注） いずれの場合も、名前付きインターフェイスは指定できず、PPPoE にはインターフェイスを設定できません。

b) [論理名（Logical Name）] にこのフェールオーバー インターフェイスの論理名を指定します。
c) [アクティブIP（Active IP）] にフェールオーバー通信用のアクティブ IP アドレスを入力します。
d) [スタンバイIP（Standby IP）] にフェールオーバー通信用のスタンバイ IP アドレスを入力します。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティ アプライアンスで使用されます。
e) [サブネットマスク（Subnet Mask）] に両方の IP アドレスのサブネットマスクを入力します。両方が同じサブネット上にある必要があります。

ステップ 10 （任意）次の手順を実行して、2 台のデバイス間のステートフルフェールオーバー通信用のインターフェイスを設定します。

a) 更新通信用のデバイスインターフェイスを割り当て、次にキーボード上の Tab キーを押してページを更新します。

ポート ID（gigabitethernet1 など）を入力するか、またはインターフェイスをすでに定義している場合は、ポートを選択できます。ただし、名前付きインターフェイスは指定できません。

（注） FWSM では、これは VLAN インターフェイスです。

b) [論理名（Logical Name）] にこのインターフェイスの論理名を指定します。
c) [アクティブIP（Active IP）] に接続更新用のアクティブ IP アドレスを入力します。
d) [スタンバイIP（Standby IP）] に更新通信用のスタンバイ IP アドレスを入力します。
e) [サブネットマスク（Subnet Mask）] に両方の IP アドレスのサブネットマスクを入力します。両方が同じサブネット上にある必要があります。
f) HTTP 接続情報を保持するには、[HTTPレプリケーションの有効化（Enable HTTP Replication）] を選択します。

HTTP を除くすべての TCP プロトコルに関する接続情報が、スタンバイ装置に伝達されます。HTTP 接続は一般に存続期間が短いため除かれます。フェールオーバー中に HTTP 接続を保持するには、このオプションを選択します。

ステップ 11 通信の暗号化キーを指定します。共有キーを入力し、次に[確認（Confirm）]フィールドに再度入力します。両方のデバイスで同じキーを必ず入力してください（3.1 よりも前のバージョンの FWSM では使用できません）。

共有キーには、最大 63 の英数字の任意の文字列を使用できます。[HEX] オプションが選択されている場合、共有キーは、厳密に 32 の 16 進数文字からなる任意の文字列となります（[HEX] オプションは、PIX/ASA バージョン 7.0.5 以降、および FWSM バージョン 3.1.3 以降でだけ使用できます）。

（注） この手順の実行は任意ですが、フェールオーバー通信を暗号化することを強く推奨します。

ステップ 12 非対称ルーテッドセッションのフェールオーバーの再接続タイムアウト値を指定するには、時間を hh:mm:ss（分と秒の値は省略可能）形式で[タイムアウト（Timeout）]フィールドに入力します。このフィールドが空白（デフォルト）または 0 の場合、再接続は行われません。この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも接続を再開できます。

ステップ 13 (オプション)フェールオーバーペアと通信するように双方向フォワーディング検出（BFD）を設定でき、これを使用してフェールオーバーユニットの正常性を監視できます。[ヘルスチェックモニタリング（Health-Check Monitoring）] セクションから BFD テンプレートを作成または選択します。

（注） これは、ASA 9.7.1 以降を実行している Firepower フェールオーバーデバイスにのみ適用されます。

ヒント BFD フェールオーバーコマンドは、アクティブ/スタンバイモードでのみサポートされます。マルチコンテキストデバイスでは、BFD フェールオーバーコマンドはシステムコンテキストでのみサポートされます。BFD フェールオーバーコマンドは、透過モードではサポートされません。

ステップ 14 （FWSM だけ）設定されているインターフェイスが、[Interface Configuration] テーブルにリストされます。リストされているインターフェイスのフェールオーバー設定を編集するには、そのフェールオーバー設定を選択し、[Edit Row] ボタンをクリックして [Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）を開きます。

フェールオーバー グループ 2 へのセキュリティコンテキストの追加

新しいセキュリティコンテキストを既存のフェールオーバーグループ 2 に追加するには、新しいコンテキストコンフィギュレーションを展開ファイルに保存してから、適切なデバイスに手動で追加する必要があります。それ以外の場合、最初に展開が成功するまで、Security Manager はデバイスの管理コンテキストを介して新しいコンテキストとの通信を試みます。（グループ 1 と 2 の両方が同じデバイスでアクティブでない限り、）管理コンテキストを介してグループ 2 に到達できないため、これは失敗します。

次に、新しいセキュリティコンテキストを作成し、それをフェールオーバーグループ 2 に追加する手順を示します。

1. 新規セキュリティコンテキストを作成します。

   必ず、コンテキスト名、設定 URL を定義し、インターフェイスを割り当て、フェールオーバーグループ 2 を選択し、管理 IP アドレスを指定してください。詳細については、セキュリティ コンテキストの管理 （2984 ページ）を参照してください。

2. これらの変更を保存して送信します。
3. 次のコンテキスト設定情報を提供し、各変更を保存します。
   - 新しいコンテキストの [デバイスプロパティ（Device Properties）] ウィンドウの [ログイン情報（Credentials）]ページで、ユーザー名とパスワードを入力します。詳細については、デバイス プロパティの表示または変更 （136 ページ）を参照してください。
   - コンテキストの [インターフェイス（Interfaces）]ページで、割り当てられたインターフェイスを編集して、名前、IP アドレス、およびサブネットマスクを指定します。詳細については、デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照してください。
   - コンテキストの [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）で、インターフェイス設定を編集して、スタンバイ IP アドレスを提供します。
   - [HTTP] ページ （2498 ページ）で、[HTTPサーバーを有効にする（Enable HTTP Server）] をオンにして、HTTP アクセスを定義します。
   - ログイン情報（Credentials）]ページで、コンテキストに接続するときに使用するユーザー名とパスワードを入力します。詳細については、デバイス クレデンシャルの設定 （2488 ページ）を参照してください。
4. Configuration Manager の [ファイル（File）] メニューから [展開（Deploy）] を選択します。変更を送信し、[保存した変更の展開（Deploy Saved Changes）] ダイアログ ボックスで、この新しいコンテキストのみが選択されていることを確認してから、[展開メソッドの編集（Edit Deploy method）] をクリックします。[展開メソッドの編集（Edit Deploy method）] ダイアログ ボックスで、[メソッド（Method）] を [ファイル（File）] に変更し、[接続先（Destination）] と [ファイル名（file name）] を指定します。[OK] をクリックして [展開メソッドの編集（Edit Deploy method）] ダイアログボックスを閉じ、[保存した変更の展開（Deploy Saved Changes）] ダイアログボックスの [展開（Deploy）] をクリックします。
5. 設定ファイルをデバイスにアップロードした後、CLI を使用してコンテキストの HTTP アクセスを有効にします。次に例を示します。
6. コンテキストの設定成が指定したファイルに保存されます。この手順の詳細については、ファイルへの展開 （493 ページ）を参照してください。

```
ciscoasa/group2(config-if)#  int g3/0
ciscoasa/group2(config-if)# nameif man
ciscoasa/group2(config-if)# security-level 100
ciscoasa/group2(config-if)# ip add 203.0.113.176 255.255.254.0 st 203.0.113.177
ciscoasa/group2(config-if)# exit
ciscoasa/group2(config)# http serv ena
ciscoasa/group2(config)# http 0.0.0.0 0.0.0.0 man
ciscoasa/group2(config)# username cisco pass cisco
ciscoasa/group2(config)#wr
```

このプロセスに従って、Security Manager を使用して、コンテキストへの新しい変更をコンテキストに正常に展開できます（コンテキストに到達しようとした場合、管理コンテキストの管理 IP アドレスを経由しません）。

代替方法

この問題に対する別のアプローチは、最初に新しいコンテキストをフェールオーバーグループ 1 に追加してから、Security Manager を介して設定を実行することです。ただし、このコンテキストをフェールオーバーグループ 2 に移動するには、両方のグループ（1 と 2）が同じデバイスでアクティブになっている必要があります。そうでない場合、次のエラーが報告されます。

```
"join-failover-group 2
ERROR: Command requires failover-group 2 and 1 to be in the same state or no nameif
comand for all interfaces in this context"
```

アクティブ/スタンバイ フェールオーバー設定の追加手順

Cisco Security Manager を使用すると、PIX/ASA/FWSM デバイスにインストールされている証明書を検証して、そのデバイスを認証できます。アクティブ/スタンバイ フェールオーバー設定でファイアウォールを設定する場合は、証明書をアクティブ デバイスからスタンバイ デバイスに手動でコピーして、フェールオーバーの発生後に Security Manager がスタンバイ デバイスと通信できるようにする必要があります。

次の手順では、ASDM を使用して、ネットワーク内のセキュリティ アプライアンスのアイデンティティ証明書、CA 証明書、およびキーをエクスポートまたは表示し、次に ASDM を使用してその情報をスタンバイ デバイスにインポートする方法について説明します。

- ファイルまたは PKCS12 データへの証明書のエクスポート （2552 ページ）
- スタンバイ デバイスへの証明書のインポート （2553 ページ）

ファイルまたは PKCS12 データへの証明書のエクスポート

トラストポイント設定をエクスポートするには、ASDM を使用して次の手順を実行します。

ステップ 1 **[設定（Configuration）] > [機能（Features）] > [デバイス管理（Device Administration）] > [証明書（Certificate）] > [トラストポイント（Trustpoint）] > [エクスポート（Export）]** に移動します。

ステップ 2 [Trustpoint Name]、[Encryption Passphrase]、および [Confirm Passphrase] の各フィールドに入力します。これらのフィールドの詳細については、[Help] をクリックしてください。

ステップ 3 トラストポイント設定をエクスポートするための方法を選択します。

- [Export to a File]：ファイル名を入力するか、またはファイルを参照します。
- [Display the trustpoint configuration in PKCS12 format]：トラストポイント設定全体をテキスト ボックスに表示してから、インポートするためにコピーします。詳細については、[Help] をクリックしてください。

ステップ 4 [エクスポート（Export）] をクリックします。

スタンバイ デバイスへの証明書のインポート

トラストポイント設定をインポートするには、ASDM を使用して次の手順を実行します。

ステップ 1 [設定（Configuration）]>[機能（Features）]>[デバイス管理（Device Administration）]>[証明書（Certificate）]>[トラストポイント（Trustpoint）]>[インポート（Import）] に移動します。

ステップ 2 [Trustpoint Name]、[Decryption Passphrase]、および [Confirm Passphrase] の各フィールドに入力します。これらのフィールドの詳細については、[Help] をクリックしてください。この復号化パスフレーズは、このトラストポイントがエクスポートされたときに使用された暗号化パスフレーズと同じです。

ステップ 3 トラストポイント設定をインポートするための方法を選択します。

- [Import from a File]：ファイル名を入力するか、またはファイルを参照します。
- [Enter the trustpoint configuration in PKCS12 format]：エクスポート元からのトラストポイント設定全体をテキスト ボックスに貼り付けます。詳細については、[Help] をクリックしてください。

フェールオーバー ポリシー

この項では、さまざまなタイプのセキュリティアプライアンスにおけるフェールオーバー設定を説明しているページを示します。ページは、デバイス タイプ別に整理されています。

PIX 6.x ファイアウォール

- [Failover] ページ（PIX 6.3） （2554 ページ）
  - [Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3） （2556 ページ）
  - [Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）

ファイアウォール サービス モジュール

- [Failover] ページ（FWSM） （2557 ページ）
  - [Advanced Settings] ダイアログボックス （2562 ページ）
  - [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （2573 ページ）
  - [Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）
  - [Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）

適応型セキュリティ アプライアンスおよび PIX 7.0 ファイアウォール

- [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）

- [Settings] ダイアログボックス （2570 ページ）
- [Edit Failover Group] ダイアログボックス （2576 ページ）
- [Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）
- [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （2573 ページ）
- [Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）

[Failover] ページ（PIX 6.3）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

[Failover] ページは、PIX 6.3.x ファイアウォールのフェールオーバー値を設定するために使用します。

ナビゲーション パス

デバイスビューで PIX 6.3.x デバイスを選択してから、デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）] を選択します。

関連項目

- フェールオーバーについて （2542 ページ）
- フェールオーバー ポリシー （2553 ページ）

フィールド リファレンス

表 *618 : [Failover]* ページ（*PIX 6.3*）

要素	説明
フェールオーバー	
Failover Method	フェールオーバーリンクのタイプを [シリアルケーブル（Serial Cable）] または [LANベース（LAN Based）] から選択します。[Serial Cable] を選択する場合、物理ケーブルが両方のデバイスに接続されていることを確認します。

要素	説明
Enable Failover	このデバイスでフェールオーバーをイネーブルにするには、このチェックボックスをオンにします。両方のデバイスのソフトウェア バージョン、アクティベーション キー タイプ、フラッシュ メモリ、およびメモリが同じであることを確認します。 PIX デバイスで [Failover Method] に [LAN Based] を選択している場合、次に論理 LAN フェールオーバー インターフェイスを設定する必要があります。また、任意でステートフル フェールオーバー インターフェイスを設定します。
[Bootstrap] ボタン	クリックすると、[Bootstrap Configuration for LAN Failover] ダイアログボックスが表示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）を参照してください。
Failover Poll Time	装置間での hello メッセージの間隔を指定します。値の範囲は 3 ～ 15 秒です。デフォルトは 15 です。
LAN-Based Failover これらのフィールドは [Failover Method] に [LAN Based] が選択されているときに使用できます。	
インターフェイス	LANベースのフェールオーバーに使用するインターフェイスを選択します。[未選択（Not Selected）] を選択すると、LANベースのフェールオーバーが無効になります。
共有キー 確認（Confirm）	プライマリ デバイスとスタンバイ デバイス間の通信を暗号化するために使用します。値には任意の英数文字列を指定できます。 [Confirm] フィールドに [Shared Key] をもう一度入力します。
Stateful Failover （任意）ステートフル フェールオーバー （2546ページ）を設定するには、次のパラメータを指定します。	
インターフェイス	ステートフル フェールオーバーに使用するインターフェイスを選択します。[未選択（Not Selected）] を選択すると、ステートフル フェールオーバーが無効になります。 （注） リストから高速 LAN リンクを選択する必要があります（100full、1000full、1000sxfull など）。

要素	説明
Enable HTTP Replication	選択すると、アクティブなHTTPセッションがスタンバイ ファイアウォールにコピーされます。選択しないと、HTTP 接続はフェールオーバー時に切断されます。HTTP レプリケーションをディセーブルにすると、ステートリンク上のトラフィックの量が少なくなります。
インターフェイス コンフィギュレーション このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスの [Standby IP Address] および [Active MAC Address] と [Standby MAC Address] を定義するには、リストからそれらを選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3） （2556 ページ）を開きます。	

[Edit Failover Interface Configuration] ダイアログボックス（PIX 6.3）

（注） バージョン4.17以降、Cisco Security Managerは引き続きPIXの機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[Edit Failover Interface Configuration] ダイアログボックスを使用して、選択したPIX 6.3.xデバイスのフェールオーバー インターフェイスを設定します。

（注） PPPoE にはフェールオーバー インターフェイスを設定できません。

ナビゲーション パス

[Edit Failover Interface Configuration] ダイアログボックスには、[Failover] ページ（PIX 6.3）（2554 ページ）の [Interface Configuration] テーブルからアクセスできます。

関連項目

- フェールオーバー ポリシー （2553 ページ）

フィールド リファレンス

表 *619 : [Edit Failover Interface Configuration]* ダイアログボックス（*PIX 6.3*）

要素	説明
インターフェイス（Interface）	インターフェイスの名前。読み取り専用です。

要素	説明
Active IP Address	アクティブ インターフェイスの IP アドレスを表示します。このアドレスは、アクティブ デバイスと通信するためにスタンバイ デバイスによって使用されます。アドレスは、システムの IP アドレスと同じネットワーク上にある必要があります。 このインターフェイスのアクティブ IP アドレス。読み取り専用です。このアドレスは、アクティブデバイスと通信するためにスタンバイ デバイスによって使用されます。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドはブランクです。 **ヒント** この IP アドレスを ping ツールで使用して、アクティブ デバイスのステータスを確認できます。
ネットマスク	アクティブ IP アドレスのサブネット マスク。読み取り専用です。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドはブランクです。
Standby IP Address	スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。このアドレスは、スタンバイ デバイスと通信するためにアクティブデバイスによって使用されます。アドレスは、システムの IP アドレスと同じネットワーク上にある必要があります。 インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。 **ヒント** この IP アドレスを ping ツールで使用して、スタンバイ デバイスのステータスを確認できます。
フェールオーバー MAC アドレス これらのパラメータでは、フェールオーバー用に設定する物理インターフェイスの仮想MAC アドレスを定義できます。これらのアドレスはオプションです。	
Active MAC Address	アクティブ インターフェイスの MAC アドレスを 16 進数形式で指定します（0123.4567.89ab など）。
Standby MAC Address	スタンバイ インターフェイスの MAC アドレスを 16 進数形式で指定します（0123.4567.89ab など）。

[Failover] ページ（FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[フェールオーバー（Failover）] ページを使用して、選択した Firewall Services Module の基本的なフェールオーバー値を設定します。

ナビゲーション パス

この機能にアクセスするには、デバイスビューで FWSM を選択し、次に、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）]** を選択します。

関連項目

- フェールオーバー ポリシー （2553 ページ）
- アクティブ/スタンバイ フェールオーバー設定の追加手順 （2552 ページ）
- [Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）

フィールド リファレンス

表 *620 : [Failover]* ページ（*FWSM*）

要素	説明
Enable Failover	このデバイスでフェールオーバーをイネーブルにするには、このチェックボックスをオンにします。両方のデバイスのソフトウェア バージョン、アクティベーション キー、フラッシュ メモリ、およびメモリが同じであることを確認します。 次に論理 LAN フェールオーバー インターフェイスを設定する必要があります。また、任意でステートフル フェールオーバー インターフェイスを設定します。
設定ボタン	クリックすると、[Advanced Settings] ダイアログボックス （2562 ページ）が表示されます。これは、フェールオーバーを実行するタイミングを定義します。
Configuration このセクションは、マルチコンテキスト モードで動作している FWSM 3.1.1 以降のデバイスでのみ表示されます。	

要素	説明
アクティブ/アクティブ	アクティブ/アクティブ フェールオーバー設定では、両方のセキュリティ アプライアンスがコンテキストごとにネットワーク トラフィックを検査します。つまり、各コンテキストで、一方のアプライアンスがアクティブ デバイスで、もう一方のアプライアンスがスタンバイ デバイスとなります。 デバイスでアクティブ/アクティブ フェールオーバーをイネーブルにするには、2 つのフェールオーバー グループのいずれかにセキュリティ コンテキストを割り当てる必要があります。フェールオーバー グループは、単に 1 つ以上のセキュリティ コンテキストの論理グループです。フェールオーバー グループ 1 がアクティブ状態になる装置にフェールオーバー グループ割り当てを指定する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。フェールオーバーグループへのコンテキストの割り当てについては、[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986ページ）を参照してください。
アクティブ/スタンバイ	アクティブ/スタンバイ設定では、アクティブ セキュリティ アプライアンスがフェールオーバー ペアを通過するすべてのネットワーク トラフィックを処理します。スタンバイ セキュリティ アプライアンスは、アクティブ セキュリティ アプライアンスで障害が発生するまではネットワーク トラフィックを処理しません。アクティブ セキュリティ アプライアンスの設定が変更されるたびに、設定情報がフェールオーバー リンクを介してスタンバイ セキュリティ アプライアンスに送信されます。 フェールオーバーが発生すると、スタンバイ セキュリティ アプライアンスがアクティブ装置になります。前のアクティブ装置の IP アドレスと MAC アドレスが使用されます。IP アドレスまたは MAC アドレスの変更はネットワーク上の他のデバイスには認識されないため、ARP エントリが変更されたりタイムアウトしたりすることはありません。
LAN Failover	

要素	説明
VLAN	フェールオーバー リンクに使用している VLAN インターフェイスの数値 ID（11 など）を入力します。このリストには、VLAN ID は自動的に読み込まれません。[未選択（Not Selected）] を強調表示して、目的の VLAN ID 番号を入力し、キーボードの Tab キーを押して関連フィールドをアクティブ化する必要があります。 フェールオーバー用に設定する場合、インターフェイスはスタンバイ デバイスに直接接続されます。
論理名（Logical Name）	フェールオーバー VLAN インターフェイスの論理名を入力します。
Active IP Address	このインターフェイスのアクティブ IP アドレスを指定します。
Standby IP Address	このインターフェイスのスタンバイ IP アドレスを指定します。 フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティ アプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
[Bootstrap] ボタン	クリックすると、[Bootstrap Configuration for LAN Failover] ダイアログボックスが表示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）を参照してください。
Stateful Failover （任意）ステートフル フェールオーバー （2546 ページ）を設定するには、次のパラメータを指定します。	
VLAN	フェールオーバー リンクに使用している VLAN インターフェイスの数値 ID（12 など）を入力します。このリストには、VLAN ID は自動的に読み込まれません。[未選択（Not Selected）] を強調表示して、目的の VLAN ID 番号を入力し、キーボードの Tab キーを押して関連フィールドをアクティブ化する必要があります。 フェールオーバー用に設定する場合、インターフェイスはスタンバイ デバイスに直接接続されます。
論理名（Logical Name）	ステートフル フェールオーバー VLAN インターフェイスの論理名を入力します。

要素	説明
Active IP Address	このインターフェイスのアクティブ IP アドレスを指定します。
Standby IP Address	このインターフェイスのスタンバイ IP アドレスを指定します。 フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティ アプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
Enable HTTP Replication	選択すると、ステートフル フェールオーバーで、アクティブ HTTP セッションをスタンバイ ファイアウォールにコピーできるようになります。選択しないと、HTTP 接続はフェールオーバー時に切断されます。HTTP レプリケーションをディセーブルにすると、ステートリンク上のトラフィックの量が少なくなります。
共有キー（Shared Key）（FWSM 3.1.1 以降のみ） このセクションのオプションを使用すると、共有暗号キーを提供して、アクティブ デバイスとスタンバイ デバイス間の通信を暗号化できます。 **注意** フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。このデバイスを VPN トンネルの終端に使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。共有キーを使用して、フェールオーバー通信のセキュリティを確保することを推奨します。	
共有キー 確認（Confirm）	最大 63 文字の数字、文字、句読点の文字列を入力します。この文字列は暗号キーを生成するために使用されます。 [確認（Confirm）] フィールドにこの文字列をもう一度入力します。 [HEX] を選択する場合、[共有キー（Shared Key）] と [確認（Confirm）] のフィールドには、正確に 32 文字の 16 進数（0 ～ 9、a ～ f）を入力する必要があります。

要素	説明
インターフェイス コンフィギュレーション このテーブルは、シングルコンテキストモードで動作しているデバイスまたは個々のセキュリティ コンテキストだけの [Failover] ページに表示されます。 このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスのモニタリングをイネーブルまたはディセーブルにするには、インターフェイスをリストから選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）を開きます。[このインターフェイスの障害をモニターする（Monitor this interface for failure）] をオンまたはオフにします。	

[Advanced Settings] ダイアログボックス

[Advanced Settings] ダイアログボックスでは、選択した FWSM 用に追加のフェールオーバーを設定できます。

（注） 次のリファレンス テーブルは、[Advanced Settings] ダイアログボックスに表示される可能性があるすべてのフィールドを示しています。実際に表示されるフィールドは、動作モード（ルーテッドまたはトランスペアレント）とデバイスがシングル コンテキストとマルチ コンテキストのどちらをホストしているかによって異なります。

ナビゲーション パス

[Failover] ページ（FWSM） （2557 ページ）の [Settings] ボタンをクリックして、[Advanced Settings] ダイアログボックスにアクセスできます。

関連項目

- フェールオーバー ポリシー （2553 ページ）

フィールド リファレンス

表 621 : [Advanced Settings] ダイアログボックス

要素	説明
Interface Policy 障害が発生したインターフェイス オプションを選択して、適切な値を指定します。	
Number of failed interfaces	障害が発生したモニタ対象インターフェイスの数がこの値を超えると、セキュリティ アプライアンスはフェールオーバーします。有効な値の範囲は 1 ～ 250 です。

要素	説明
障害が発生したインターフェイスのパーセンテージ（Percentage of failed interfaces）	障害が発生したモニタ対象インターフェイスの数がこのパーセンテージを超えると、セキュリティアプライアンスはフェールオーバーします。
Failover Poll Time これらのフィールドは、フェールオーバー リンクに送信される hello メッセージの頻度、およびhello メッセージを受信していないときにピアの障害テストを実行するまでに待機する時間を定義します。	
Unit Failover	フェールオーバー装置間での hello メッセージの間隔。秒単位で 1 ～ 15 の値を入力するか、[msec] をオンにする場合は、ミリ秒単位で 500 ～ 999 の値を入力します。
Unit Hold Time	フェールオーバー リンク上で hello メッセージを待機する時間。この時間を過ぎると、装置はピアの障害テストを開始します。秒単位で 3 ～ 45 の値を入力します。この値は少なくとも [Unit Failover] 値の 3 倍である必要があります。
Monitored Interface	インターフェイス間でのポーリングの間隔。秒単位で 3 ～ 15 の値を入力します。
MAC Address Mapping アクティブ/スタンバイ モードでは、このテーブルにはインターフェイスと仮想 MAC アドレスのマッピングが一覧表示されます。これは Security Manager の標準のテーブルです。 テーブルの使用 （64 ページ）で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 インターフェイス マッピングを追加または編集するには、[Add Row] または [Edit Row] ボタンをクリックして、 [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （2573 ページ）を開きます。	
フェールオーバー グループ アクティブ/アクティブ モードでは、このテーブルには両方のフェールオーバー グループが一覧表示されます。いずれかのグループのフェールオーバー パラメータを編集するには、グループをリストで選択して、[Edit Row] ボタンをクリックして、 [Edit Failover Group] ダイアログボックス （2576 ページ）を開きます。	

要素	説明
Bridge Group Configuration シングルコンテキスト トランスペアレント モードでは、このテーブルには現在定義されているすべてのブリッジ グループが一覧表示されます（デバイス インターフェイス、ハードウェア ポート、ブリッジ グループの管理 （2373 ページ）を参照）。スタンバイ IP アドレスをブリッジ グループに追加するには、グループをリストで選択して、[Edit Row] ボタンをクリックして、 [Edit Failover Bridge Group Configuration] ダイアログボックス （2564 ページ）を開きます。	

[Edit Failover Bridge Group Configuration] ダイアログボックス

このダイアログボックスを使用して、スタンバイ IP アドレスをフェールオーバー ブリッジ グループに追加します。

ナビゲーション パス

[Edit Failover Bridge Group Configuration] ダイアログボックスには、次の場所からアクセスできます。

- ASA 上のトランスペアレント モードの個々のセキュリティ コンテキストに表示される [Failover] ページ。
- トランスペアレント モードの FWSM で表示される [Advanced Settings] ダイアログボックス （2562 ページ）の [Bridge Group Configuration] テーブル。

関連項目

- フェールオーバー ポリシー （2553 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）
- [Failover] ページ（FWSM） （2557 ページ）

フィールド リファレンス

表 622 : [Edit Failover Bridge Group Configuration] ダイアログボックス

要素	説明
名前	ブリッジ グループを示します。編集はできません。
IPアドレス	ブリッジ グループに割り当てられている IP アドレスを示します。編集はできません。
ネットワーク マスク（Network Mask）	IP アドレスのサブネット マスクを示します。編集はできません。

要素	説明
Standby Address	スタンバイ ブリッジ グループの IP アドレスを入力します。このアドレスはプライマリ アドレスと同じサブネットにある必要があります。

[Failover] ページ（ASA/PIX 7.0 以降）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

[Failover] ページを使用して、ASA および PIX 7.0 以降のセキュリティ デバイスの基本的なフェールオーバー値を設定します。

（注） [Failover]ページに表示される機能とオプションは、選択したデバイスのタイプ、オペレーティング システムのバージョン、ファイアウォール モード（ルーテッドまたはトランスペアレント）、およびセキュリティ コンテキスト（シングルまたはマルチ）によって異なります。したがって、次の表で説明されている要素によっては、現在選択しているデバイスの [Failover] ページに表示されないものもあります。

ナビゲーション パス

デバイスビューで ASA または PIX 7.0 以降を選択してから、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）]** を選択します。

関連項目

- フェールオーバーについて （2542 ページ）
- フェールオーバー ポリシー （2553 ページ）
- アクティブ/スタンバイ フェールオーバー設定の追加手順 （2552 ページ）

フィールド リファレンス

表 *623 : [Failover]* ページ（*ASA/PIX 7.0* 以降）

要素	説明
Failover Method	フェールオーバーリンクのタイプを [シリアルケーブル（Serial Cable）] または [LANベース（LAN Based）] から選択します。[Serial Cable] を選択する場合、物理ケーブルが両方のデバイスに接続されていることを確認します。 （注） このオプションは PIX デバイスでのみ使用できます。
Enable Failover	このデバイスでフェールオーバーをイネーブルにするには、このチェックボックスをオンにします。両方のデバイスのソフトウェア バージョン、アクティベーション キー タイプ、フラッシュ メモリ、およびメモリが同じであることを確認します。 PIX デバイスで [Failover Method] に [LAN Based] を選択している場合およびすべての ASA では、次に論理 LAN フェールオーバー インターフェイスを設定する必要があります。また、任意でステートフル フェールオーバー インターフェイスを設定します。
[Bootstrap] ボタン	クリックすると、[Bootstrap Configuration for LAN Failover] ダイアログボックスが表示されます。詳細については、[Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）を参照してください。
設定ボタン	クリックすると、[Settings] ダイアログボックス （2570 ページ）が表示されます。これは、フェールオーバーを実行するタイミングを定義します。
タイムアウト（Timeout）	フェールオーバーの [タイムアウト（Timeout）] では、システムが起動したときまたはアクティブになったときを起点として、、固定されたセッションが受け入れられる期間を指定します。これは、スタティック トランスレーション ルールとともに使用されます（詳細については、[Static Rules] タブ （1342 ページ）を参照してください）。 非対称ルーテッドセッションのフェールオーバーの再接続タイムアウト値を指定するには、このフィールドに値を入力します。値は hh:mm:ss（時間:分:秒）の形式で入力します。分と秒は両方ともオプションです。 時間の有効な値 -1 ～ 1193 です。デフォルト値は 0 です。0 に設定すると、接続は再確立されません。この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも再接続できます。

要素	説明
Configuration このセクションは、マルチコンテキスト モードで動作しているデバイスでのみ表示されます。	
アクティブ/アクティブ	アクティブ/アクティブ フェールオーバー設定では、両方のセキュリティ アプライアンスがコンテキストごとにネットワーク トラフィックを検査します。つまり、各コンテキストで、一方のアプライアンスがアクティブ デバイスで、もう一方のアプライアンスがスタンバイ デバイスとなります。 セキュリティ アプライアンスでアクティブ/アクティブ フェールオーバーをイネーブルにするには、2つのフェールオーバー グループのいずれかにセキュリティ コンテキストを割り当てる必要があります。フェールオーバー グループは、単に 1 つ以上のセキュリティ コンテキストの論理グループです。フェールオーバー グループ 1 がアクティブ状態になる装置にフェールオーバー グループ割り当てを指定する必要があります。管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。フェールオーバー グループへのコンテキストの割り当てについては、[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） （2988 ページ）を参照してください。
アクティブ/スタンバイ	アクティブ/スタンバイ設定では、アクティブ セキュリティ アプライアンスがフェールオーバー ペアを通過するすべてのネットワーク トラフィックを処理します。スタンバイ セキュリティ アプライアンスは、アクティブセキュリティアプライアンスで障害が発生するまではネットワーク トラフィックを処理しません。アクティブ セキュリティ アプライアンスの設定が変更されるたびに、設定情報がフェールオーバー リンクを介してスタンバイ セキュリティ アプライアンスに送信されます。 フェールオーバーが発生すると、スタンバイ セキュリティ アプライアンスがアクティブ装置になります。前のアクティブ装置の IP アドレスと MAC アドレスが使用されます。IP アドレスまたは MACアドレスの変更はネットワーク上の他のデバイスには認識されないため、ARP エントリが変更されたりタイムアウトしたりすることはありません。
LAN Failover	

要素	説明
インターフェイス	フェールオーバー リンクとして使用するインターフェイスを選択します。デバイス上の使用可能なすべてのインターフェイスが一覧表示されます。 フェールオーバー用に設定する場合、インターフェイスはスタンバイ デバイスに直接接続されます。 （注） フェールオーバー リンクとして EtherChannel インターフェイスを選択できます。フェールオーバーリンクとして割り当てられた他のタイプのインターフェイスと同様、EtherChannel インターフェイスに名前を付けることはできません。また、EtherChannel のメンバインターフェイスに名前を付けることもできません。さらに、アクティブ フェールオーバー リンクとして使用されている最中は、インターフェイス設定を変更することはできません。詳細については、EtherChannel の設定 （2343 ページ）を参照してください。
論理名（Logical Name）	フェールオーバー インターフェイスの論理名を入力します。
Active IP Address	このインターフェイスのアクティブ IP アドレスを指定します。
Standby IP Address	このインターフェイスのスタンバイ IP アドレスを指定します。 フェールオーバー ペアの両方の装置からパケットを受信するには、すべてのインターフェイスにスタンバイ IP アドレスを設定する必要があります。スタンバイ IP アドレスは、現在スタンバイ装置であるセキュリティ アプライアンスで使用され、アクティブ IP アドレスと同じサブネットに存在する必要があります。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
Stateful Failover （任意）ステートフル フェールオーバー （2546 ページ）を設定するには、次のパラメータを指定します。	

要素	説明
インターフェイス	ステートフル フェールオーバー リンクに使用するインターフェイスを選択します。デバイス上の使用可能なすべてのインターフェイスが一覧表示されます。 （注） ステートフル フェールオーバー リンクとして EtherChannel インターフェイスを選択できます。フェールオーバーリンクとして割り当てられた他のタイプのインターフェイスと同様、EtherChannel インターフェイスに名前を付けることはできません。また、EtherChannel のメンバインターフェイスに名前を付けることもできません。さらに、アクティブ フェールオーバー リンクとして使用されている最中は、インターフェイス設定を変更することはできません。詳細については、EtherChannel の設定 （2343 ページ）を参照してください。
論理名 （Logical Name）	アクティブ ファイアウォール デバイス上のインターフェイスの論理名を入力します。このインターフェイスは、フェールオーバー時にスタンバイ デバイスと通信します。ステートフル フェールオーバー用に設定されたインターフェイスは、スタンバイ デバイスに直接接続します。
Active IP Address	アクティブ インターフェイスの IP アドレスを指定します。
Standby IP Address	スタンバイ インターフェイスの IP アドレスを指定します。
サブネットマスク	アクティブ IP アドレスおよびスタンバイ IP アドレスのサブネット マスクを入力します。
Enable HTTP Replication	選択すると、アクティブな HTTP セッションがスタンバイ ファイアウォールにコピーされます。選択しないと、HTTP接続はフェールオーバー時に切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。
キー（Key） このセクションのオプションを使用すると、アクティブ デバイスとスタンバイ デバイス間の通信を暗号化できます。タイプを選択して、共有暗号キーを生成する文字列を指定します。 **注意** フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。このデバイスを VPN トンネルの終端に使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。共有キーを使用して、フェールオーバー通信のセキュリティを確保することを推奨します。	

要素	説明
Any string 16 進数	[任意の文字列（Any string）] を選択すると、[共有キー（Shared Key）] フィールドには、最大 63 文字の数字、文字、句読点の任意の組み合わせを入力できます。この文字列は暗号キーを生成するために使用されます。 [HEX] を選択する場合、[共有キー（Shared Key）] と [確認（Confirm）] のフィールドには、正確に 32 文字の 16 進数（0 ～ 9、a ～ f）を入力する必要があります。この文字列は暗号キーとして使用されます。
共有キー 確認（Confirm）	キー タイプとして選択した [Any string] または [HEX] のいずれかに適した文字列を入力します。 [確認（Confirm）] フィールドに文字列をもう一度入力します。
インターフェイスコンフィギュレーション（Interface Configuration）（場合によっては [Monitor Interface Configuration] と表示） このテーブルは、シングルコンテキスト、トランスペアレント モードで動作している ASA 8.4.1 以降のデバイスおよび PIX/ASA デバイスの個々のコンテキストの [Failover] ページに表示されます。これらに表示されない場合は、[Settings] ダイアログボックス （2570 ページ）に表示されます。 このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスのモニタリングをイネーブルまたはディセーブルにするには、インターフェイスをリストから選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）を開きます。[このインターフェイスの障害をモニターする（Monitor this interface for failure）] をオンまたはオフにします。	

[Settings] ダイアログボックス

[Settings] ダイアログボックスでは、選択した ASA または PIX 7.x アプライアンスでフェールオーバーが発生するタイミングの基準を定義できます。

ナビゲーション パス

[Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）の [Settings] ボタンをクリックすると、[Settings] ダイアログボックスにアクセスできます。

（注） 次のリファレンス テーブルは、[Settings] ダイアログボックスに表示される可能性があるすべてのフィールドを示しています。実際に表示されるフィールドは、動作モード（ルーテッドまたはトランスペアレント）とデバイスがシングル コンテキストとマルチ コンテキストのどちらをホストしているかによって異なります。

関連項目

- フェールオーバー ポリシー （2553 ページ）
- [Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）
- [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （2573 ページ）
- [Bootstrap Configuration for LAN Failover] ダイアログボックス （2579 ページ）

フィールド リファレンス

表 *624 : [Settings]* ダイアログボックス

要素	説明
Interface Policy	
Number of failed interfaces	障害が発生したモニタ対象インターフェイスの数がこの値を超えると、セキュリティ アプライアンスはフェールオーバーします。値の範囲は 1 ～ 250 です。
障害が発生したインターフェイスのパーセンテージ（Percentage of failed interfaces）	障害が発生したモニタ対象インターフェイスの数がこのパーセンテージを超えると、セキュリティ アプライアンスはフェールオーバーします。
Failover Poll Time	
Unit Failover	装置間での hello メッセージの間隔。値の範囲は 1 ～ 15 秒です。[単位をミリ秒に変更（Change units to msec）] オプションをオンにしている場合は 200 ～ 999 ミリ秒です。
Unit Hold Time	装置がフェールオーバー リンク上で hello メッセージを受信する必要がある時間を設定します。設定した時間内に受信しない場合、装置はピアの障害のテスト プロセスを開始します。値の範囲は 3 ～ 45 秒です。[msec] オプションをオンにしている場合は 800 ～ 999 ミリ秒です。[Unit Failover] の値の 3 倍より少ない値は入力できません。
Monitored Interface	インターフェイス間でのポーリングの間隔。値の範囲は 3～15 秒、またはミリ秒のオプションが選択されている場合は 500 ～ 999 ミリ秒です。

要素	説明
Interface Hold Time	データ インターフェイスが hello メッセージを受信する必要がある時間を設定します。この時間が過ぎると、ピアの障害が宣言されます。有効な値は 5 ～ 75 秒です。この値は少なくとも [Unit Failover] 値の 5 倍である必要があります。
リンクステート間隔（Link State Interval）	フェールオーバーペアの各 ASA がインターフェイスのリンクステートをチェックする間隔を設定します。デフォルトでは、リンクステート間隔の値は 500 ミリ秒です。polltime はカスタマイズできます。たとえば、polltime を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。有効な範囲は 300 ～ 799 ミリ秒です。 （注） [リンクステート間隔（Link State Interval）] は、ASA 9.7.1 以降で使用できます。
フェールオーバー グループ アクティブ/アクティブ モードでは、このテーブルには両方のフェールオーバー グループが一覧表示されます。いずれかのグループのフェールオーバー パラメータを編集するには、グループをリストで選択して、[Edit Row] ボタンをクリックして、[Edit Failover Group] ダイアログボックス （2576 ページ）を開きます。	
MAC Address Mapping アクティブ/スタンバイ モードでは、このテーブルにはインターフェイスと仮想 MAC アドレスのマッピングが一覧表示されます。これは Security Manager の標準のテーブルです。 テーブルの使用 （64 ページ）で説明されているとおり、このテーブルには [Add Row]、[Edit Row]、[Delete Row] ボタンがあります。 インターフェイス マッピングを追加または編集するには、[Add Row] または [Edit Row] ボタンをクリックして、[Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス （2573 ページ）を開きます。	
Monitor Interface Configuration シングルコンテキスト モードでは、このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。インターフェイスのモニタリング用のスタンバイ IP アドレスを定義したり、インターフェイスのモニタリングをイネーブルまたはディセーブルにしたりするには、インターフェイスをリストから選択して、[Edit Row] ボタンをクリックして、[Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）を開きます。	

要素	説明
管理 IP アドレス（Management IP Address） シングルコンテキストのトランスペアレントモードでは、このセクションには（[Management IP] ページ （2461 ページ）で）デバイスに定義されている管理 IP アドレスとネットマスクが表示されます。これらの値は変更できません。	
スタンバイ（Standby）	スタンバイ装置の管理 IP アドレスを入力します。このアドレスはプライマリ アドレスと同じサブネットにある必要があります。

[Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス

[Add Interface MAC Address] と [Edit Interface MAC Address] ダイアログボックスでは、フェールオーバー用に設定されている ASA、FWSM 3.x、PIX 7.x セキュリティ アプライアンス上の物理インターフェイスの仮想 MAC アドレスを定義できます（ASA 5505 デバイスでは使用できません）。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置の MAC アドレスは常にアクティブ IP アドレスに関連付けられています。セカンダリ装置は、最初にブートされてアクティブになると、そのインターフェイスの焼き付け済み MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更によりネットワーク トラフィックが中断される可能性があります。各インターフェイスに仮想 MAC アドレスを設定して、セカンダリ装置がプライマリ装置よりも前にオンラインになっても、セカンダリ装置がアクティブ装置である場合、正しい MAC アドレスを使用するようにします。仮想 MAC アドレスを指定しない場合、フェールオーバー ペアはバーンドイン MAC アドレスを使用します。

（注） フェールオーバーまたはステートフル フェールオーバー リンクには、仮想 MAC アドレスは設定できません。これらのリンクの MAC アドレスおよび IP アドレスは、フェールオーバー中に変更されません。

ナビゲーション パス

[Add Interface MAC Address] と [Edit Interface MAC Address] ダイアログボックスは、[Settings] ダイアログボックス （2570 ページ）から開けます。

関連項目

- フェールオーバー ポリシー （2553 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）
- [Edit Failover Group] ダイアログボックス （2576 ページ）

フィールド リファレンス

表 625 : [Add Interface MAC Address]/[Edit Interface MAC Address] ダイアログボックス

要素	説明
Physical Interface	フェールオーバー仮想 MAC アドレスを設定する物理インターフェイスを選択します。
MAC アドレス	
アクティブ インターフェイス（Active Interface）	アクティブ インターフェイスの仮想 MAC アドレスを 16 進数形式で入力します（0023.4567.89ab など）。
Standby Interface	スタンバイ インターフェイスの仮想 MAC アドレスを 16 進数形式で入力します（0023.4567.89ab など）。

[Edit Failover Interface Configuration] ダイアログボックス

[Edit Failover Interface Configuration] ダイアログボックスを使用して、インターフェイスのスタンバイ IP アドレスを定義し、インターフェイスのステータスをモニタするかどうかを指定します。

（注） PPPoE にはフェールオーバー インターフェイスを設定できません。

ナビゲーション パス

[Edit Failover Interface Configuration] ダイアログボックスには、（ASA/PIX 7.0 以降では）[Settings] ダイアログボックス（2570 ページ）、（FWSM では）[Advanced Settings] ダイアログボックス（2562 ページ）からアクセスできます。また、シングルコンテキストのトランスペアレントモードで動作している ASA 8.4.1 以降のデバイスおよび個々の ASA/PIX セキュリティ コンテキストの [Failover] ページ自体からもアクセスできます。

関連項目

- フェールオーバー ポリシー （2553 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）
- [Failover] ページ（FWSM） （2557 ページ）
- [Edit Failover Group] ダイアログボックス （2576 ページ）

フィールド リファレンス

表 *626 : [Edit Failover Interface Configuration]* ダイアログボックス

要素	説明
Interface Name	インターフェイスの名前。読み取り専用です。
Active IP Address	このインターフェイスのアクティブ IP アドレス。読み取り専用です。IP アドレスがインターフェイスで割り当てられていない場合、このフィールドはブランクです。たとえば、DHCP がインターフェイスでイネーブルの場合です。
Mask	アクティブ IP アドレスのサブネット マスク。読み取り専用です。IP アドレスがインターフェイスで割り当てられていない場合、このフィールドはブランクです。たとえば、DHCP がインターフェイスでイネーブルの場合です。
Standby IP Address	スタンバイ フェールオーバー装置上の対応するインターフェイスの IP アドレスを指定します。インターフェイスに IP アドレスが割り当てられていない場合、このフィールドは表示されません。
このインターフェイスの障害をモニターする（Monitor this interface for failure）	このインターフェイスの障害をモニタするかどうかを指定します。モニタリングをイネーブルにするには、このチェックボックスをオンにします。セキュリティ アプライアンスのモニタ可能なインターフェイスの数は 250 です。 インターフェイスのポーリング時間中、セキュリティ アプライアンスのフェールオーバー ペア間で Hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。モニター対象のフェールオーバー インターフェイスには、次のステータスが設定されます。 • Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。 • Normal：インターフェイスはトラフィックを受信しています。 • Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。 • [Link Down]：インターフェイスは管理上ダウンしています。 • No Link：インターフェイスの物理リンクがダウンしています。 • Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

要素	説明
ASR Group Number	このインターフェイスが非対称ルーティング グループの一部である場合、その ASR グループ番号を指定します。ASR グループ番号の有効な値は 1 ～ 32 です。 フェールオーバー設定の装置間で非対象ルーティング サポートを適切に機能させるためには、ステートフル フェールオーバーをイネーブルにする必要があります。

[Edit Failover Group] ダイアログボックス

[Edit Failover Group] ダイアログボックスを使用して、アクティブ/アクティブ フェールオーバー設定でセキュリティ コンテキストのグループのフェールオーバー パラメータを設定します。フェールオーバー グループへのコンテキストの割り当てについては、[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） （2988 ページ）または [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）を参照してください。

ナビゲーション パス

[Add Failover Group] ダイアログボックスには、PIX/ASA の [Settings] ダイアログボックス （2570 ページ）または FWSM の [Advanced Settings] ダイアログボックス （2562 ページ）からアクセスできます。

関連項目

- フェールオーバー ポリシー （2553 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）
- [Failover] ページ（FWSM） （2557 ページ）

フィールド リファレンス

表 *627 : [Edit Failover Group]* ダイアログボックス

要素	説明
Preferred Role	[Preferred Role]：同時に起動した場合や、[Preempt] オプションが選択されている場合、このフェールオーバー グループがアクティブ状態として表示される、フェールオーバー ペアのプライマリ装置またはセカンダリ装置を指定します。[プライマリ（Primary）] または [セカンダリ（Secondary）] を選択します。 ペアの一方の装置にアクティブ状態の両方のフェールオーバー グループを含めることができます。ただし、一般的な設定では、各フェールオーバー グループに別々のロールを割り当てて、それぞれを別の装置上でアクティブにすることでデバイス間にトラフィックを分散させます。
Poll time interval for monitored interfaces	モニタされているインターフェイスのポーリング間隔を指定します。有効値の範囲は 3 ～ 15 秒（[msec] が選択されている場合は 500 ～ 999 ミリ秒）です。
保留時間（Hold Time）	グループが hello メッセージを受信する必要がある時間を指定します。この時間を経過すると、もう一方のグループの障害が宣言されます。有効な値は 5 ～ 75 秒です。
Preempt after Reboot	優先フェールオーバー デバイスがリブート後に引き継ぎを待機する秒数を指定します。この時間を経過すると、優先フェールオーバー デバイスは、このフェールオーバー グループのアクティブ装置として処理を引き継ぎます。有効な値は 0 ～ 1200 秒です。
Enable HTTP Replication	アクティブな HTTP セッションが、このフェールオーバー グループのスタンバイ デバイスにステートフル フェールオーバーの一部としてコピーされるかどうかを示します。HTTP レプリケーションを許可しない場合、HTTP 接続はフェールオーバー時に切断されます。HTTP レプリケーションをディセーブルにすると、ステート リンク上のトラフィックの量が少なくなります。この設定は、[Failover] ページの HTTP レプリケーションの設定を上書きします。

要素	説明
Failover Criteria	このグループに対して障害が発生したインターフェイス基準を選択して、適切な値を指定します。 • [障害が発生したインターフェイスの数（Number of failed interfaces）]：この数のインターフェイスで障害が発生すると、フェールオーバーがトリガーされます。有効な値は 1 ～ 250 です。 • [障害が発生したインターフェイスのパーセンテージ（Percentage of failed interfaces）]：インターフェイスの総数に対してこのパーセンテージのインターフェイスで障害が発生すると、フェールオーバーがトリガーされます。有効な値は 1 ～ 100 です。
MAC Address Mapping このテーブルには、アクティブ MAC アドレスとスタンバイ MAC アドレスがマッピングされるインターフェイスが表示されます。	

[Failover] ページ（セキュリティ コンテキスト）

個々の ASA および PIX 7.0 以降のセキュリティコンテキストの [フェールオーバー（Failover）] ページには [インターフェイス設定（Interface Configuration）] テーブルが表示されます。このテーブルには、使用可能なすべての名前付きインターフェイスが一覧表示されます。

テーブルでインターフェイスを選択して、[Edit Row] ボタンをクリックすると、[Edit Failover Interface Configuration] ダイアログボックス （2574 ページ）が開きます。ここでは、スタンバイ IP アドレスと ASR グループ番号を指定できます。また、インターフェイスのモニタリングをイネーブルまたはディセーブルにできます。

ASA 8.4.1 以降のデバイスにおける個々のトランスペアレントモード コンテキストの場合、[フェールオーバー（Failover）] ページには [ブリッジグループ設定（Bridge Group Configuration）] テーブルも表示されます。このテーブルには、現在定義されているすべてのフェールオーバー ブリッジ グループが一覧表示されます。

テーブルでエントリを選択して、[Edit Row] ボタンをクリックすると、[Edit Failover Bridge Group Configuration] ダイアログボックス （2564 ページ）が開きます。ここでは、選択したブリッジ グループのスタンバイ IP アドレスを指定できます。

ナビゲーション パス

デバイスビューでセキュリティコンテキストを選択してから、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [フェールオーバー（Failover）]** を選択します。

関連項目

- フェールオーバーについて （2542 ページ）

- フェールオーバー ポリシー （2553 ページ）
- ファイアウォール デバイスでのブリッジングについて （2449 ページ）

[Bootstrap Configuration for LAN Failover] ダイアログボックス

[Bootstrap Configuration for LAN Failover] ダイアログボックスでは、LAN フェールオーバー設定のプライマリおよびセカンダリ デバイスに適用できるブートストラップ設定が表示されます。

ナビゲーション パス

[Bootstrap Configuration for LAN Failover] ダイアログボックスには、[Failover] ページからアクセスできます。[Failover] ページの詳細については、次の項を参照してください。

- [Failover] ページ（PIX 6.3） （2554 ページ）
- [Failover] ページ（FWSM） （2557 ページ）
- [Failover] ページ（ASA/PIX 7.0 以降） （2565 ページ）

関連項目

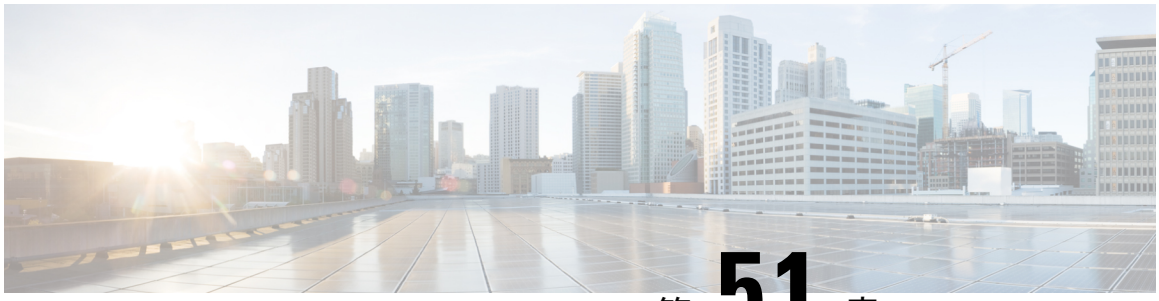
- フェールオーバー ポリシー （2553 ページ）
- アクティブ/スタンバイ フェールオーバー設定の追加手順 （2552 ページ）

フィールド リファレンス

表 *628 : [Bootstrap Configuration for LAN Failover]* ダイアログボックス

要素	説明
プライマリ	プライマリ デバイスのブートストラップ設定が含まれています。プライマリ デバイスへのコンソール接続を開き、この設定を貼り付けて、プライマリ デバイスでフェールオーバーをアクティブにします。
セカンダリ（Secondary）	セカンダリ デバイスのブートストラップ設定が含まれています。プライマリ デバイスがアクティブになったあとに、セカンダリ デバイスへのコンソール接続を開き、次に、この設定を貼り付けて、セカンダリ デバイスでフェールオーバーをアクティブにします。

（注） アクティブ/アクティブ フェールオーバーの場合、ブートストラップ設定は、各フェールオーバー ピア デバイスのシステム コンテキストにだけ適用されます。



第 51 章

ホスト名、リソース、ユーザ アカウントおよび SLA の設定

ここでは、セキュリティ アプライアンス上のホスト名の設定、マルチコンテキスト モードの Firewall Services Module（FWSM; ファイアウォール サービス モジュール）でのリソース クラスの定義と管理、ローカル ユーザ データベースでのユーザ アカウントの管理、およびルートトラッキングを実行するための Service Level Agreement（SLA; サービス レベル契約）のモニタリングについて説明します。

この章は次のトピックで構成されています。

- [Hostname] ページ （2581 ページ）
- マルチコンテキスト FWSM でのリソース管理 （2582 ページ）
- ユーザ アカウントの設定 （2588 ページ）
- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）

[Hostname] ページ

[Hostname] ページを使用して、セキュリティ デバイスのホスト名を指定し、デフォルト ドメインを指定します。設定ファイルが展開されたあとで、他のコマンドで完全修飾ドメインを入力しない場合、デバイスではこのドメイン名が使用されます。RSA キーの生成でもこのドメイン名が使用されます。

デバイスは、このドメイン名を非修飾名に追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバーとして非修飾名「jupiter」を指定した場合は、セキュリティアプライアンス が名前に「jupiter.example.com」と入力します。

セキュリティ アプライアンスのホスト名を設定した場合は、その名前がコマンド ライン プロンプトに表示されます。複数のデバイスへのセッションを確立する場合、ホスト名はコマンドを入力する場所の追跡に役立ちます。デフォルトのホスト名はプラットフォームによって異なります。

マルチコンテキスト モードでは、各コンテキストのドメイン名と、システム実行スペースを指定できます。システム実行スペースで指定するホスト名は、すべてのコンテキストのコマンド

ラインプロンプトに表示されます。オプションでコンテキストに設定されているホスト名はコマンドラインに表示されませんが、バナー コマンド $(hostname) トークンでは使用できます。

ナビゲーション パス

デバイスビューでセキュリティデバイスを選択し、次にデバイスポリシーセレクタから[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）] を選択します。

フィールド リファレンス

表 *629 : [Hostname]* ページ

要素	説明
ホスト名	デバイスの区別に役立つ一意のデバイス名（ *PIX-510-A* など）を入力します。 （注） 管理するデバイスごとに一意のホスト名を使用することを推奨します。デバイス名には最大 63 文字の英数字（米国英語）を使用でき、次の特殊文字をすべて使用できます。` ( ) + - , . / : =
ドメイン名	オプションで、デバイスの有効なドメインネームシステム（DNS）のドメイン名（*cisco.com* など）を入力します。

マルチコンテキスト FWSM でのリソース管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

デフォルトでは、マルチコンテキスト Firewall Services Module（FWSM; ファイアウォール サービス モジュール）のすべてのセキュリティ コンテキストは、コンテキストごとの最大制限が設定されている場合を除き、FWSM のリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

（注） FWSM はコンテキストあたりの帯域幅を制限しませんが、FWSM が含まれているスイッチは VLAN あたりの帯域幅を制限できます。詳細については、スイッチのマニュアルを参照してください。

FWSM は、リソース クラスにコンテキストを割り当てることでリソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスを作成する場合、FWSM はクラスに割り当てられている各コンテキストのリソースの一部を確保しませ

ん。代わりに、FWSMはコンテキストの最大制限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。

すべてのリソースの制限は、デバイスで使用可能な合計に対するパーセンテージとして設定できます。また、個々のリソースの制限をパーセンテージまたは絶対値として設定できます。

すべてのコンテキストにリソースの100%を超えて割り当てることで、FWSMをオーバーサブスクライブできます。たとえば、接続をコンテキストあたり20%に制限するクラスを設定してから、10個のコンテキストをクラスに割り当てて、合計が200%になるようにできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した20%を下回ります。

FWSMでは、パーセンテージや絶対値の代わりに、クラス内の1つ以上のリソースへの無制限アクセスを割り当てることもできます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキストA、B、およびCがクラス「Onepercent」に割り当てられているとします。このクラスでは、各クラスメンバーを1秒あたりのシステム検査の1%に制限すると、合計で3%になりますが、現在3つのコンテキストで合計2%しか使用していません。一方、クラス「Nolimit」では、検査へのアクセスが制限されていません。Nolimitのコンテキストは、「未割り当て」検査の97%より多くを使用できます。コンテキストA、B、およびCが合計限度である3%に到達しないことになるとしても、コンテキストA、B、およびCが現在使用していない1%を合わせて使用できるからです。無制限アクセスの設定はFWSMのオーバーサブスクライブと同様ですが、システムをどの程度オーバーサブスクライブできるかを詳細には制御できません。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に対して2%の制限があり、その他の制限はないクラスを作成する場合、他のすべての制限はデフォルトクラスから継承されます。反対に、すべてのリソースに対して2%の制限があるクラスを作成する場合、クラスはデフォルト クラスの設定を使用しません。

初期設定時に、デフォルトクラスは、デフォルトでコンテキストあたり許可される最大値に設定される次の制限を除き、すべてのコンテキストに対してリソースへの無制限アクセスを提供します。

- Telnetセッション：5セッション
- SSHセッション：5セッション
- IPSecセッション：5セッション
- MACアドレス：65,535エントリ

デフォルト クラスは編集できます。

関連項目

- [Resources] ページ （2584 ページ）
- [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）

[Resources] ページ

[Resources] ページを使用して、リソース管理クラスを設定および管理します。

このページのテーブルには、現在定義されているすべてのリソースクラスがリストされます。テーブルの下のボタンを使用して、このリストを管理します。

- [Add Row]：新規クラスを定義してセキュリティ コンテキストに割り当てることのできる [Add Resource] ダイアログボックスを開きます。詳細については、[Add Resource]/[Edit Resource] ダイアログボックス （2584 ページ）を参照してください。
- [Edit Row]：現在選択されている行で [Edit Resource] ダイアログボックスを開いて、クラスとそのコンテキスト割り当てを編集できるようにします。詳細については、[Add Resource]/[Edit Resource] ダイアログボックス （2584 ページ）を参照してください。
- [Delete Row]：現在選択されている行を削除します。確認が必要な場合があります。

ナビゲーション パス

デバイスビューで、マルチコンテキストモードの ASA または FWSM のシステムコンテキストを選択し、デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [リソース（Resources）]** を選択します。

関連項目

- マルチコンテキスト FWSM でのリソース管理 （2582 ページ）

[Add Resource]/[Edit Resource] ダイアログボックス

[リソースの追加（Add Resources）]/[リソースの編集（Edit Resource）] ダイアログボックスを使用して、FWSM セキュリティコンテキストのリソースクラスと割り当てを追加または編集します。

タイトルを除き、両方のダイアログボックスは同じです。次の説明は両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add Resource]/[Edit Resource] ダイアログボックスには、[Resources] ページ （2584 ページ）からアクセスできます。

関連項目

- マルチコンテキスト FWSM でのリソース管理 （2582 ページ）

フィールド リファレンス

表 *630 : [Add Resource]/[Edit Resource]* ダイアログボックス

要素	説明
クラス名（Class Name）	このクラスの名前を入力します。最大 20 文字の英数字を入力でき、次の特殊文字をすべて使用できます。` ( ) + - , . / : =
[Limits] タブ	
（注） 次の制限については、特定の制限に値を指定しない場合に、制限がデフォルト クラスから継承されます。デフォルト クラスでその制限が設定されていない場合、制限はシステム制限を継承します。また、入力した値は、関連する [パーセント（percent）] ボックスもオンになっていない限り *1* 秒あたりのレートと見なされます（オンになっている場合、値は合計リソースに対するパーセンテージです）。	
TCP or UDP Connections	1 つのホストと他の複数のホスト間の接続を含め、任意の 2 つのホスト間の TCP または UDP 接続に対するレート制限を設定します。0（システム制限）～ 102400 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
Inspections (Fixups)	アプリケーション インスペクションのレート制限を設定します。1 秒あたり 0（システム制限）～ 10000 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
Syslog メッセージ	システム ログ メッセージのレート制限を設定します。制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。 FWSM では、FWSM 端末またはバッファに送信されるメッセージに対して 1 秒あたり 30,000 メッセージをサポートできます。メッセージを syslog サーバに送信する場合、FWSM では 1 秒あたり 25,000 がサポートされます。

要素	説明
接続（Connections）	同時の TCP または UDP 接続の絶対制限を設定します。0（システム制限）～ 999900 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。 （注） 同時接続に対して、FWSM は接続を受け入れる 2 つの Network Processor（NP; ネットワーク プロセッサ）それぞれに制限の半分を割り当てます。通常、接続は NP 間に均等に分割されます。ただし、状況によっては、接続が均等に分割されず、一方の NP で最大制限に達する前にもう一方の NP で最大接続制限に達することがあります。この場合、許可される最大接続数は設定した制限を下回ります。NP 分散は、分散アルゴリズムに基づいてスイッチによって制御されます。このアルゴリズムは、スイッチ上で調整することも、不均衡の原因となった接続限度を引き上げて調整することもできます。
ホスト（Hosts）	FWSM を介して同時に接続できるホストの制限を設定します。0（システム制限）～262144 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
IPsec Sessions	IPsec セッションの制限を設定します。1 ～ 5 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。同時セッションの最大数は 10 で、すべてのコンテキスト間で分割されます。
SSH セッション	SSH セッションの制限を設定します。1 ～ 5 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。同時セッションの最大数は 100 で、すべてのコンテキスト間で分割されます。
Telnet セッション	同時 Telnet セッションの制限を設定します。1 ～ 5 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。同時セッションの最大数は 100 で、すべてのコンテキスト間で分割されます。
NAT Translations	同時アドレス変換の制限を設定します。0（システム制限）～ 266144 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100 % を超える値を割り当てることができます。

要素	説明
MAC アドレス	（トランスペアレントモードのみ）MAC アドレステーブルで許可される同時 MAC アドレス エントリの制限を設定します。0（システム制限）～65535 の整数を入力して制限を絶対値で設定するか、またはデバイスをオーバーサブスクライブする場合は 100% を超える値を割り当てることができます。
ASDM	ASDM 管理セッションの制限を設定します（デフォルトは 5 です）。1 ～ 5 の整数を入力して制限を絶対値で設定するか、3.0 ～ 15.0 のパーセンテージを入力できます。同時セッションの最大数は 80 で、すべてのコンテキスト間で分割されます。 ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、80 ASDM セッションのシステム制限は、すべてのコンテキスト間で分割される 160 HTTPS セッションの制限を表します。
Other VPN	サイトツーサイト VPN セッションに対する制限を設定します。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
Other VPN Burst	vpn other でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数を設定します。たとえば、使用するモデルで 5000 セッションがサポートされており、vpn other で割り当てたセッション数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが other vpn burst に使用可能です。other vpn ではセッション数がコンテキストに対して保証されますが、対照的に other vpn burst ではオーバーサブスクライブが可能です。すべてのコンテキストがバーストプールを先着順に使用できます。
（注） AnyConnect VPN および AnyConnect VPN Burst の最大値は、ASA ライセンスによって異なります。Cisco Security Manager は、AnyConnect VPN および AnyConnect VPN Burst に入力された値を検証できません。そのため、ユーザーは、AnyConnect VPN および AnyConnect VPN Burst の値が最大値以内であることを確認する必要があります。そうでない場合、展開エラーが発生します。最大値を把握するには、ASA に Telnet 接続して、show version コマンドを実行します。合計 VPN ピアの値は、最大値に対応します。	
AnyConnect VPN	AnyConnect ピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。

要素	説明
AnyConnect VPN Burst	AnyConnect でコンテキストに割り当てられた数を超えて許可される AnyConnect セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、AnyConnect で割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが AnyConnect Burst に使用可能です。AnyConnect ではセッション数がコンテキストに対して保証されますが、対照的に AnyConnect Burst ではオーバーサブスクライブが可能です。すべてのコンテキストがバーストプールを先着順に使用できます。
ストレージ	バージョン 4.12 以降、Security Manager では、ストレージサイズを入力するか、デフォルトを選択できます。この機能は、ASA バージョン 9.6(2) 以降で使用できます。制限は MB 単位で設定されます。このストレージに複数のディスクを含めることはできないため、デフォルトの上限は設定されたディスクの 100% です。
All Resources Limit	すべてのリソースの制限を設定します。特定のリソースの制限も設定した場合は、その制限によって、すべてのリソースに対してここで設定した制限が上書きされます。制限をパーセンテージで設定できます。または値を **0** に設定することで無制限として設定できます（[パーセント（percent）] がオンになっていない場合）。他の絶対値は設定できません。デバイスをオーバーサブスクライブする場合は、100% を超えて割り当てることができます。
[Contexts] タブ	
Available Contexts	クラス割り当てに使用可能なすべてのコンテキストがリストされます。クラスがすでに割り当てられているコンテキストは表示されません。 1 つ以上のコンテキストを選択し、[>>] ボタンをクリックしてコンテキストを [Selected Contexts] リストに追加します。
Selected Contexts	このクラスに割り当てられているすべてのコンテキストがリストされます。 1 つ以上のコンテキストを選択し、[<<] ボタンをクリックしてコンテキストを [Available Contexts] リストに戻します。

ユーザ アカウントの設定

[User Accounts] ページを使用すると、ローカル ユーザ データベースを管理できます。ローカルデータベースのユーザーアカウントを認証、許可、およびアカウンティング（AAA）機能とともに使用して、デバイス上で「どのユーザーが何を実行できるか」を指定できます。詳細については、セキュリティ デバイスでの AAA について （2467 ページ）を参照してください。

このページのテーブルには、現在定義されているすべてのローカル ユーザ アカウントがリストされ、それぞれのユーザに関して、名前および割り当てられている権限レベルが示されます。これらのフィールドの詳細については、[Add User Account]/[Edit User Account] ダイアログボックス （2589 ページ）を参照してください。

重要 Cisco Security Manager 管理対象デバイスの場合、[デバイスのプロパティ（Device Properties）] ページでパスワードを変更する場合は、[ユーザーアカウント（User Accounts）] ページでも同じように更新してください。同じように更新しないと、Cisco Security Manager とデバイス間の通信の初期フェーズは成功し、[接続のテスト（Test Connectivity）] も正常に検証されますが、展開は失敗します。これは、[ユーザーアカウント（User Accounts）] ページで設定されたパスワードが [デバイスのプロパティ（Device Properties）] ページで更新されるためです。したがって、ログイン情報の更新が [デバイスのプロパティ（Device Properties）] ページと [ユーザーアカウント（User Accounts）] ページで並行して実行されるようにすることを推奨します。

- ユーザ アカウントを追加するには、[Add Row] ボタンをクリックします。
- アカウントの設定を編集するには、そのアカウント設定を選択し、[Edit Row] ボタンをクリックします。
- ユーザ アカウントを削除するには、そのアカウントを選択して [Delete Row] ボタンをクリックします。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [ユーザーアカウント（User Accounts）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ローカル データベース （2470 ページ）
- AAA の準備 （2468 ページ）

[Add User Account]/[Edit User Account] ダイアログボックス

[Add User Account] および [Edit User Account] ダイアログボックスを使用して、ローカル ユーザ アカウントを追加するか、または既存のユーザ アカウントを編集します。

ナビゲーション パス

[Add User Account] および [Edit User Account] ダイアログボックスには、ユーザ アカウントの設定 （2588 ページ）で説明しているように、[User Accounts] ページからアクセスできます。

フィールド リファレンス

表 *631 : [Add User Account]/[Edit User Account]* ダイアログボックス

要素	説明
[ユーザー名 （Username）]	ユーザアカウントの名前を入力します。4 文字以上である必要があります。最大値は 64 文字です。エントリは、大文字と小文字が区別されます。
パスワード	
[暗号化されたパスワード （Password as encrypted）]	[プレーンテキスト （Plain Text）] または [暗号化 （Encrypted）] を選択します。
[パスワード暗号化タイプ （Password encrypt type）]	[MD5] または [PBKDF2] を選択します。
パスワード	このユーザーアカウント固有のパスワードを入力します。エントリは、大文字と小文字が区別されます。 （注） セキュリティを確保するために、パスワードの長さは 8 文字以上にすることを推奨します。 （注） プレーンテキストパスワードの場合： • MD5 パスワードの長さは 3 ～ 32 文字にする必要があります。 • PBKDF2 パスワードの長さは、33 ～ 127 文字にする必要があります。展開の失敗を避けるために、PBKDF2 パスワードに正しい `sha` キー値が使用されていることを確認します。
確認 （Confirm）	確認のためにユーザ パスワードを再入力します。
特権レベル	ユーザの権限レベルを選択します。ローカル コマンド認可を定義します。範囲は、0（最低）～15（最高）です。デフォルトの特権レベルは 2 です。

接続を維持するためのサービス レベル契約（SLA）のモニタリング

サービスレベル契約をモニタリングしてルートトラッキングを実行するように、バージョン 7.2 以降を実行している ASA または PIX デバイスを設定できます。別のネットワーク上のデバイスへの接続性をモニタリングすることによって、プライマリ ルートの可用性をトラッキングし、プライマリ ルートに障害が発生した場合のバックアップ ルートを準備することができます。たとえば、インターネット サービス プロバイダー（ISP）ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。この方法はデュアル ISP と呼ばれ、セキュリティ アプライアンスにハイ アベイラビリティをもたらします。ハイ アベイラビリティは、カスタマーに必要なサービスを提供するための重要な要素となります。

ルートが有効かどうかを本質的に判断するメカニズムは、ルート トラッキング以外には存在しません。ネクスト ホップ ゲートウェイが使用できなくなった場合にも、スタティック ルートはルーティング テーブル内に残ります。セキュリティ アプライアンス上の関連付けられたインターフェイスがダウンした場合にのみ削除されます。

セキュリティ アプライアンスは、SLA モニタのポリシー オブジェクトで定義したモニタリング対象にルートを関連付けることによって、ルート トラッキングを実行します。対象のモニタリングは、オブジェクトで設定されたパラメータに従い、ICMP エコー要求を使用して行われます。指定された時間内にエコー応答が受信されない場合、SLA モニタはダウンしていると見なされ、関連付けられたルートがルーティング テーブルから削除されます。削除されたルートに代わって、すでに定義されているバックアップ ルートが使用されます。

SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージング アウトしません）。

関連項目

- スタティック ルートの設定 （2891 ページ）
- ファイアウォール デバイスのインターフェイスの設定 （2333 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

ここでは、次の内容について説明します。

- サービス レベル契約の作成 （2591 ページ）

サービス レベル契約の作成

次の手順では、SLA モニタ オブジェクトを設定し、ASA または PIX の設定で、それらのオブジェクトをルートおよびインターフェイスに関連付ける方法について説明します。

関連項目

- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）
- スタティック ルートの設定 （2891 ページ）
- ファイアウォール デバイスのインターフェイスの設定 （2333 ページ）
- ポリシー オブジェクトの作成 （299 ページ）

ステップ 1 SLA モニタ ポリシー オブジェクトを作成します。

a) **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] を開き（ Policy Object Manager （290 ページ）を参照）、コンテンツテーブルから [SLAモニター（SLA Monitors）] を選択します。

ヒント SLA モニタ オブジェクトは、このオブジェクト タイプを使用するポリシーを定義する際に作成することもできます。詳細については、ポリシーのオブジェクトの選択 （288 ページ）を参照してください。

b) 作業領域を右クリックして [新しいオブジェクト（New Object）] を選択し、[SLAモニターを追加（Add SLA Monitor）] ダイアログボックスを開きます。詳細については、 SLA モニタ オブジェクトの設定 （2593 ページ）を参照してください。

c) モニタリング オプションはほとんどの接続に適しているため、設定する必要があるのは次の項目のみです。

- [Name]：オブジェクトの名前。
- [SLA Monitor ID]：モニタリング プロセスを識別する番号。この番号は 1 つのデバイス設定内で一意である必要があります。
- [Monitored Address]：モニタリング対象のアドレス。モニタリング対象を選択する場合は、その対象が ICMP エコー要求（ping）に応答できることを確認してください。対象には任意のネットワーク アドレスを選択できますが、次のどれを使用するか検討する必要があります。
- ISP ゲートウェイ アドレス。
- ネクスト ホップ ゲートウェイ アドレス（ISP ゲートウェイの可用性を確認する場合）。
- セキュリティ アプライアンスが通信する必要のある、AAA サーバなどのターゲット ネットワーク上のサーバ。
- 宛先ネットワーク上の永続的なネットワーク デバイス（夜間にシャットダウンされるデスクトップ コンピュータやノートブック コンピュータは適切ではありません）。
- [Interface]：ICMP メッセージのソースとなるインターフェイスを識別する、インターフェイス名またはインターフェイス ロール。デバイスでは、監視対象のアドレスに対して、このインターフェイスの IP アドレスから ping が行われます。

d) [OK] をクリックしてオブジェクトを保存します。

ステップ 2 このオブジェクトを使用してルートをモニタリングするように、ASA/PIX ポリシーを設定します。SLA をモニタリングするために、次のポリシーを設定できます。

- **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [静的ルート（Static Route）]**：スタティックルートを定義するとき、そのルートに対するルートトラッキングを実行する SLA モニタオブジェクトを選択できます。詳細については、スタティック ルートの設定 （2891 ページ）および[Add Static Route]/[Edit Static Route] ダイアログボックス （2893 ページ）を参照してください。
- [インターフェイス（Interfaces）]：DHCP または PPPoE を使用するインターフェイスを定義するとき、DHCP または PPPoE の学習されたデフォルトルートがトラッキングされるように設定できます。詳細については、デバイス インターフェイス：IP タイプ（PIX/ASA 7.0 以降） （2424 ページ）を参照してください。

SLA モニタ オブジェクトの設定

[Add SLA Monitor] と [Edit SLA Monitor] ダイアログボックスを使用すると、SLA モニタ オブジェクトを作成、編集およびコピーできます。各 SLA モニタでは、モニタリング対象のアドレスへの接続ポリシーを定義し、そのアドレスへのルートの可用性をトラッキングします。ルートの可用性は、ICMP エコー要求を送信し、応答を待機することによって、定期的にチェックされます。要求がタイムアウトすると、そのルートはルーティング テーブルから削除され、バックアップ ルートに置き換えられます。

SLA モニターは、PIX/ASA バージョン 7.2 以降を実行するセキュリティアプライアンスにのみ設定できます。SLA モニタリング ジョブは、デバイス設定から SLA モニタを削除していない限り、展開後すぐに開始して実行し続けます（つまり、ジョブはエージングアウトしません）。

SLA モニタ オブジェクトの設定と使用の詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [SLAモニター（SLA Monitors）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

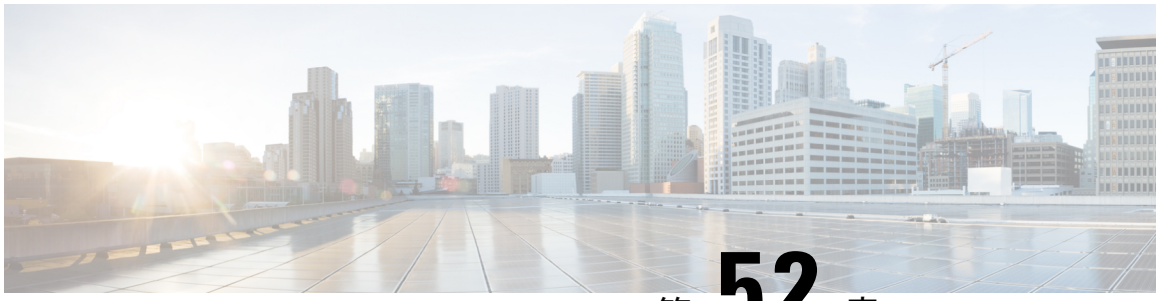
- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）
- Policy Object Manager （290 ページ）

フィールド リファレンス

表 *632 : [SLA Monitor]* ダイアログボックス

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
SLA Monitor ID	SLA 操作の ID 番号。値の範囲は 1 ～ 2147483647 です。1 つのデバイスには最大で 2000 個の SLA 操作を作成できます。各 ID 番号はポリシーとデバイス設定に対して一意である必要があります。
Monitored Address	SLA 操作によって可用性をモニタリングされる IP アドレス。モニタリングするアドレスの選択に関する推奨事項については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）を参照してください。
インターフェイス	可用性をテストするためにモニタリング対象のアドレスに対して送信される、すべての ICMP エコー要求の送信元インターフェイス。インターフェイスやインターフェイス ロールの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択するか新しいインターフェイス ロールを作成します。
周波数（Frequency）	ICMP エコー要求の送信頻度（秒単位）。値の範囲は 1 ～ 604800 秒（7 日）です。デフォルトは 60 秒です。 （注） 頻度はタイムアウト値未満にできません。これらの値を比較するには、頻度をミリ秒に換算する必要があります。
[しきい値（Threshold）]	上昇しきい値が宣言されるまでに、ICMP エコー要求のあとに経過する必要のある時間（ミリ秒単位）。値の範囲は 0 ～ 2147483647 ミリ秒です。デフォルトは 5000 ミリ秒です。 しきい値は、定義された値を超過したイベントを示すためだけに使用されます。これらのイベントは、タイムアウト値が適切であるかどうかを評価するために使用できます。このイベントは、モニタリング対象のアドレスへの到達可能性を直接的に示すものではありません。 （注） しきい値はタイムアウト値を超過しないようにします。

要素	説明
時間切れ（Time out）	SLA 操作が ICMP エコー要求への応答を待機する時間（ミリ秒単位）。値の範囲は 0 ～ 604800000 ミリ秒（7 日）です。デフォルトは 5000 ミリ秒です。 モニタリング対象のアドレスからの応答がこのフィールドに定義された時間内に受信されない場合、スタティック ルートがルーティング テーブルから削除され、バックアップ ルートに置き換えられます。 （注） タイムアウト値は頻度値を超過できません。2つの数値を比較するには、頻度値をミリ秒に換算してください。
Request Data Size	ICMP 要求パケット ペイロードのサイズ（バイト単位）。値の範囲は 0 ～ 16384 バイトです。デフォルトは 28 バイトです。この場合、全体の ICMP パケットは 64 バイトとなります。この値には、プロトコルまたは Path Maximum Transmission Unit（PMTU）で許可される最大値を超える値を設定しないでください。 場合によっては、到達可能性を確保するために、デフォルトのデータ サイズを大きくして、ソースとターゲットの間での PMTU の違いを検出できるようにすることが必要となります。PMTUが小さいと、セッションのパフォーマンスに影響を及ぼすことがあります。セッションのパフォーマンスへの影響が検出されると、セカンダリ パスが使用されます。
ToS	ICMP 要求パケットの IP ヘッダー内に定義されたタイプ オブ サービス（ToS）。値の範囲は 0 ～ 255 です。デフォルトは 0 です。 このフィールドには、遅延、優先順位、信頼性などの情報が含まれます。この情報は、ポリシー ルーティングのためにネットワーク上の他のデバイスが使用する場合もあれば、専用アクセス レートなどの機能によって使用される場合もあります。
パケット数	送信されたパケットの数。値の範囲は 1 ～ 100 です。デフォルトは 1 パケットです。 ヒント パケット損失によって、セキュリティ アプライアンスがモニタリング対象のアドレスに到達できないと誤って認識することが懸念される場合は、デフォルトのパケット数を大きくしてください。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用（304 ページ） を参照してください。



第 52 章

ファイアウォール デバイスでのサーバ アクセスの設定

[Server Access] セクションには、ファイアウォールデバイスでサーバアクセスを設定するためのページが含まれています。[Server Access] は、デバイス セレクタまたはポリシー セレクタの [Device Admin] の下にあります。

この章は次のトピックで構成されています。

- [AUS] ページ （2597 ページ）
- [DHCP Relay] ページ （2602 ページ）
- [DHCPリレーIPv6（DHCP Relay IPv6）] ページ （2606 ページ）
- DHCP サーバーの設定 （2610 ページ）
- [DNS] ページ （2616 ページ）
- DDNS の設定 （2620 ページ）
- [NTP] ページ （2624 ページ）
- [SMTP Server] ページ （2627 ページ）
- [TFTP Server] ページ （2627 ページ）

[AUS] ページ

[AUS] ページでは、[Auto Update] 指定をサポートするサーバからのセキュリティ アプライアンスのリモート更新を設定できます。[Auto Update] によって、設定変更およびソフトウェア更新が、リモート サーバからアプライアンスに自動的に適用されます。

（注） このページで指定するサーバと、（[Tools] メニューから [Device Properties] を選択して表示される）[Device Properties] の [Auto Update] セクションで指定するサーバは、同じである必要があります。[Device Properties] 情報は、Security Manager が設定更新を送信する宛先の AUS サーバを指定します。これに対し、このページの情報は、デバイスが更新のために接続するサーバを定義します。また、[Device Properties] で指定する [Device Identity] と、このページの [Device ID] とが一致している必要もあります。

AUSサーバを変更した場合、デバイスは、新しい設定を受け取るまで現在の設定内に定義されている AUS サーバを引き続き使用することに注意してください。したがって、AUS ポリシーは変更しますが、設定の展開には前の AUS サーバを使用する必要があります。展開が正常に完了したあとで、新しいサーバを指し示すように [Device Properties] を変更します。AUS への展開の詳細については、Auto Update Server または CNS Configuration Engine を使用した設定の展開 （532 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [AUS] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス （2601 ページ）

フィールド リファレンス

表 *633 : [AUS]* ページ

要素	説明
自動更新サーバーテーブル	このテーブルには、現在設定されている Auto Update Server が一覧表示されます。テーブルの下のボタンを使用して、これらのエントリを管理します。 エントリは、AUSサーバに接続するための優先順位の高いものから一覧表示されます。リストの順序を変更するには、上下の矢印ボタンを使用して、選択したエントリを上下に移動します。 [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、エントリを追加、編集、または削除します。[Add Row] を選択すると、[Add Auto Update Server] ダイアログボックスが開きます。[Edit Row] を選択すると、選択した行の [Edit Auto Update Server] ダイアログボックスが開きます。これらのダイアログボックスについては、[Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス （2601 ページ）を参照してください。 （注） この AUS サーバーに接続するための URL は、[自動更新サーバーの追加（Add Client Update）]/[自動更新サーバーの編集（Edit Client Update）] ダイアログボックスで指定される *Protocol* ://*Username* :*Password* @*IP IP Address* (:*Port*)/*Path* を連結して生成されます。ポートは、デフォルトの443以外のポート番号を入力した場合にかぎり含まれます。

要素	説明
デバイス ID タイプ（Device ID Type）	AUS サーバでこのデバイスを識別するために使用する方式を選択します。 • [ホスト名（Host Name）]：[デバイスプロパティ（Device Properties）] ウィンドウ（[ツール（Tools）] > [デバイスプロパティ（Device Properties）]）で指定されている、このデバイスのホスト名。 • [シリアル番号（Serial Number）]：このデバイスのシリアル番号。 • [IPアドレス（IP Address）]：指定されたインターフェイスの IP アドレス。このオプションを選択すると、[Interface] フィールドが表示されます。目的のデバイス インターフェイスを入力するか、または選択します。 • [MACアドレス（MAC Address）]：指定されたインターフェイスの MAC アドレス。このオプションを選択すると、[Interface] フィールドが表示されます。目的のデバイスインターフェイスを入力するか、または選択します。 • [定義されたユーザ（User Defined）]：ユーザ指定の一意の ID が使用されます。このオプションを選択すると、[User Defined] フィールドが表示されます。このフィールドに英数字文字列を入力します。この文字列は、[Device Properties] ウィンドウ（[Tools] > [Device Properties]）の [Device Identity] フィールドにも表示されている必要があります。

要素	説明
Poll Type	更新のためにAUSサーバをポーリングする頻度を定義する方式を選択します。 • [指定した頻度で（At Specified Frequency）]：このオプションを選択すると、[ポーリング期間（Poll Period）] フィールドが表示されます。 • [ポーリング期間（Poll Period）]：デバイスが AUS サーバーのポーリングと次のポーリングの間待機する時間を分で指定します。有効な値は 1 ～ 35791 です。 • [スケジュールした時間に（At Scheduled Time）]：このオプションを選択すると、次のフィールドが表示されます（バージョン 7.2 以降を実行している ASA/PIX デバイスにかぎり使用可能）。 • [曜日（Days of the week）]：デバイスが AUS サーバーをポーリングする 1 日以上の日を選択します。 • [ポーリング開始時間（Polling Start Time in Hours）]：選択した日にポーリングを開始する時間（24 時間形式に基づく）。 • [ポーリング開始時間（分）（Polling Start Time in Mins）]：ポーリングを開始する時間の分の値。 • [開始時間のランダム化を有効にする（Enable Randomization of the Start Time）]：ランダムなポーリング時間枠を指定する場合は、このオプションを選択します。[時間枠のランダム化（Randomization Window）] フィールドが有効になります。 [時間枠のランダム化（Randomization Window）]：デバイスが指定のポーリング時間をランダム化するために使用できる最大分数。有効な値は 1 ～ 1439 です。
再試行回数（Retry Count）	デバイスが新しい情報のために AUS サーバへのポーリングを試行する回数。任意。このフィールドに 0 を入力した場合、またはこのフィールドをブランクのままにした場合、デバイスはポーリング試行の失敗後に再試行しません。
Retry Period	[Retry Count] が 0 でもブランクでもない場合に、デバイスがポーリング試行の失敗後に AUS サーバへの再ポーリングを待機する時間（分）。有効な値は 1 ～ 35791 です。[Retry Count] が 0 でもブランクでもないのに、このフィールドをブランクのままにした場合、値はデフォルトで 5 分に設定されます。
Disable Device After:	このオプションを選択すると、指定されたタイムアウト期間中に AUS サーバからの応答がない場合、セキュリティ アプライアンスによって通過中のトラフィックが停止されます。 • [タイムアウト（Timeout）]：AUS サーバーからの応答がない場合にファイアウォールデバイスがタイムアウトを待機する時間（分）。

[Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス

[Add Auto Update Server] ダイアログボックスを使用して、新しい AUS サーバ定義を設定します。セキュリティアプライアンスは、このサーバを自動的にポーリングして、イメージおよび設定の更新がないかどうかを確認します。

[Auto Update] 指定では、Auto Update Server が設定情報をプッシュしてセキュリティ アプライアンスに情報の要求を送信するか、または Auto Update Server に対する定期的なポーリングをセキュリティアプライアンスで行うように設定することによって設定情報をプルするかを選択できます。また、Auto Update Server は、セキュリティアプライアンスにコマンドを送信して、いつでも即時ポーリング要求を送信できます。Auto Update Server とセキュリティ アプライアンスが互いに通信を行うには、各セキュリティ アプライアンス上に通信パスとローカル CLI 設定が必要です。

（注） この AUS サーバーに接続するための URL は、これらのダイアログボックスで指定されている Protocol://Username:Password@IP IP Address(:Port)/Path を連結して生成します。ポートは、デフォルトの 443 以外のポート番号を入力した場合にかぎり含まれます。

[Edit Auto Update Server] ダイアログボックスと [Add Auto Update Server] ダイアログボックスは、タイトルを除けば同じです。次の説明は両方に適用されます。

ナビゲーション パス

[Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックスには、[AUS] ページ （2597 ページ）からアクセスできます。

フィールド リファレンス

表 634 : [Add Auto Update Server]/[Edit Auto Update Server] ダイアログボックス

要素	説明
プロトコル	AUS サーバーとの通信に使用されるプロトコル。[http] または [https] を選択します。 （注） Auto Update Server と通信するためのプロトコルとして [https] を選択した場合、セキュリティアプライアンスでは SSL が使用されます。この場合、セキュリティアプライアンスには DES、3DES、AES ライセンスが必要です。
IPアドレス	IP アドレスを入力するか、またはこの AUS サーバを表すネットワーク/ホスト オブジェクトを選択します。

要素	説明
[ポート（Port）]	AUS サーバとの通信が行われるポートの番号を入力します。[Protocol] に [http] を選択した場合は、デフォルトで 80 に設定されます。[https] を選択した場合は、443 に設定されます。任意のポート番号を入力した場合、AUS サーバが同じポートを使用するように設定されていることを確認してください。
パス（Path）	サーバ上の AUS サービスへのパス。標準のパスは autoupdate/AutoUpdateServlet です。AUS サーバーホストが ASA の場合にのみ、admin/auto-update に変更します。
AUS Interface	Auto Update Server のポーリングに使用するインターフェイスを入力または選択します。
Verify Certificate	このオプションを選択すると、AUS サーバからの SSL 検証が必要になります。サーバから返された証明書は、Certification Authority（CA; 証明局）ルート証明書に基づいてチェックされます。これには、AUS サーバとこのデバイスが同じ認証局を使用している必要があります。
ユーザー名	AUS 認証に使用するユーザ名を入力します（任意）。
パスワード	AUS 認証に使用するパスワードを入力します（任意）。
確認（Confirm）	パスワードを再入力します（任意）。

[DHCP Relay] ページ

[DHCP Relay] ページを使用して、セキュリティ デバイスの DHCP リレー サービスを設定します。Dynamic Host Configuration Protocol（DHCP）リレーでは、あるインターフェイス上で受信された DHCP 要求が、別のインターフェイスの背後にある外部 DHCP サーバに渡されます。DHCP リレーを設定するには、少なくとも 1 つの DHCP リレー サーバを指定してから、DHCP 要求を受信するインターフェイスで DHCP リレー エージェントをイネーブルにする必要があります。

（注） DHCP リレー サーバが設定されているインターフェイスでは、DHCP リレー エージェントをイネーブルにできません。DHCP リレー エージェントは外部 DHCP サーバでだけ動作します。DHCP 要求は、DHCP サーバとして設定されているセキュリティ アプライアンス インターフェイスには転送されません。

Security Manager バージョン 4.9 以降、DHCP リレー IPv4 は、ソフトウェアバージョン 9.4.0 以降を実行している ASA クラスタデバイスでサポートされています。

ASA-SM 9.1.2+ では、DHCP リレーサーバーをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサー

バーに対してのみリレーされます。インターフェイス固有のサーバーが設定されていないインターフェイスにDHCP要求が届くと、ASAはその要求をすべてのグローバルサーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバル サーバーは使用されません。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。詳細については、[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （2396 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCPリレー（DHCP Relay）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCPリレー（DHCP Relay）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 635 : [DHCP Relay] ページ

要素	説明
[DHCP Relay Agent] テーブル	このテーブルには、DHCP リレーが設定されているインターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] ボタンでは [Add DHCP Relay Agent Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Relay Agent Configuration] ダイアログボックスが開きます。詳細については、[Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス （2604 ページ）を参照してください。
[DHCP Servers] テーブル	このテーブルには、DHCP 要求がリレーされるグローバル DHCP サーバーが一覧表示されています。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] ボタンでは [Add DHCP Relay Server Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Relay Server Configuration] ダイアログボックスが開きます。詳細については、[Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス （2605 ページ）を参照してください。
タイムアウト（秒）	DHCP アドレス ネゴシエーションに許可される時間を秒単位で指定します。有効値の範囲は 1 ～ 3600 秒で、デフォルト値は 60 秒です。

要素	説明
信頼情報（Option 82）	信頼するすべての DHCP クライアント インターフェイスを指定します。DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。 （注） 信頼するインターフェイスを個別に指定することもできます。詳細については、[Add Interface]/[Edit Interface] ダイアログボックス - [Advanced] タブ（ASA/PIX 7.0 以降） （2396 ページ）を参照してください。 DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレーエージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレーエージェントアドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。

[Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス

[Add DHCP Relay Agent Configuration] ダイアログボックスを使用して、インターフェイスで DHCP リレーエージェントを設定してイネーブルにします。[Edit DHCP Relay Agent Configuration] ダイアログボックスを使用して、既存のインターフェイス リレーエージェントを更新します。

（注） DHCP リレー サーバが設定されているインターフェイスでは、DHCP リレー エージェントをイネーブルにできません。DHCP リレー エージェントは外部 DHCP サーバでだけ動作します。DHCP 要求は、DHCP サーバとして設定されているセキュリティ アプライアンス インターフェイスには転送されません。

[Add DHCP Relay Agent Configuration] ダイアログボックスと [Edit DHCP Relay Agent Configuration] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

ナビゲーション パス

[Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックスには、[DHCP Relay] ページ （2602 ページ）からアクセスできます。

関連項目

- [Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス （2605 ページ）

フィールド リファレンス

表 636 : [Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	DHCP リレー エージェントを設定するインターフェイスの名前を入力または選択します。
Enable DHCP Relay	このチェックボックスをオンにすると、指定したインターフェイスで DHCP リレーがイネーブルになります。
Set Route	このチェックボックスをオンにして、DHCP サーバから返された情報内のデフォルト ルータ アドレスが変更されるように DHCP リレー エージェントを設定します。このオプションを選択した場合、DHCP リレー エージェントは、DHCP サーバから返された情報内のデフォルト ルータ アドレスを、選択されたインターフェイスで置き換えます。

[Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス

新しい DHCP リレー サーバを定義する場合は、[Add DHCP Relay Server Configuration] ダイアログボックスを使用します。既存のサーバ情報を更新する場合は、[Edit DHCP Relay Server Configuration] ダイアログボックスを使用します。シングル モードおよびコンテキストごとに、グローバルおよびインターフェイス固有のサーバを合わせて 10 台までの DHCPv4 リレー サーバを設定できます。インターフェイスごとには、4 台まで設定できます。

（注） 7.2 より前の OS を実行している PIX ファイアウォールは、4 つの DHCP リレー サーバーのみをサポートします。

[Add DHCP Relay Server Configuration] ダイアログボックスと [Edit DHCP Relay Server Configuration] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

ナビゲーション パス

[Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックスには、[DHCP Relay] ページ （2602 ページ）からアクセスできます。

関連項目

- [Add DHCP Relay Agent Configuration]/[Edit DHCP Relay Agent Configuration] ダイアログボックス （2604 ページ）

フィールド リファレンス

表 637 : [Add DHCP Relay Server Configuration]/[Edit DHCP Relay Server Configuration] ダイアログボックス

要素	説明
サーバ	IP アドレスを入力するか、または DHCP 要求の転送先の外部 DHCP サーバを表すネットワーク/ホスト オブジェクトを選択します。
インターフェイス	DHCP 要求の外部 DHCP サーバへの転送に使用されるインターフェイスを入力または選択します。

[DHCPリレーIPv6（DHCP Relay IPv6）] ページ

[DHCPリレーIPv6（DHCP Relay IPv6）] ページを使用して、セキュリティデバイスの DHCP リレーサービスを設定します。Dynamic Host Configuration Protocol v6（DHCPv6）リレーは、あるインターフェイスで受信したDHCPv6要求を、別のインターフェイスの背後にある外部DHCPv6サーバーに渡します。DHCPv6 リレーを構成するには、少なくとも 1 つの DHCPv6 リレーサーバーを指定してから、DHCPv6要求を受信するインターフェイスでDHCPv6リレーエージェントをイネーブルにする必要があります。

（注） DHCPv6 リレーサーバーが構成されているインターフェイスでは、DHCPv6 リレーエージェントは有効にできません。DHCPv6 リレーエージェントは、外部 DHCPv6 サーバーでのみ機能しますが、DHCPv6 サーバーとして設定されたセキュリティ アプライアンス インターフェイスには DHCPv6 要求を転送しません。Security Manager バージョン 4.9 以降、DHCP リレー IPv6 は、ソフトウェアバージョン 9.4.0 以降を実行している ASA クラスタデバイスでサポートされています。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCPリレーIPv6（DHCP Relay IPv6）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCPリレーIPv6（DHCP Relay IPv6）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

（注） DHCPv6 には、「managed-config-flag」と「other-config-flag」という 2 つの新しいインターフェイス設定が導入されました。詳細については、IPv6 インターフェイスの設定（ASA/FWSM） （2409 ページ）を参照してください。

フィールド リファレンス

表 *638 : [DHCPリレーIPv6（DHCP Relay IPv6）] ページ*

要素	説明
[DHCPリレーIPv6エージェント（DHCP Relay IPv6 Agent）] テーブル	このテーブルには、DHCP リレー IPv6 が設定されているインターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [行の追加（Add Row）] ボタンでは [DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay Agent Configuration）] ダイアログボックスが開き、[行の編集（Edit Row）] では [DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay Agent Configuration）] ダイアログボックスが開きます。詳細については、[DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）]/[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックス （2608 ページ）を参照してください。
[DHCP Servers] テーブル	このテーブルには、DHCP リレー IPv6 が設定されているインターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [行の追加（Add Row）] ボタンでは [DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay Agent Configuration）] ダイアログボックスが開き、[行の編集（Edit Row）] では [DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay Agent Configuration）] ダイアログボックスが開きます。詳細については、[DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）]/[DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックス （2609 ページ）を参照してください。
タイムアウト（秒）	DHCPv6 アドレスネゴシエーションに許可される時間を秒単位で指定します。有効値の範囲は 1 ～ 3600 秒で、デフォルト値は 60 秒です。

[DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）]/[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックス

[DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）] ダイアログボックスを使用して、インターフェイスでDHCPv6 リレーエージェントを設定して有効にします。[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックスを使用して、既存のインターフェイス リレーエージェントを更新します。

（注） DHCPv6 リレーサーバーが構成されているインターフェイスでは、DHCPv6 リレーエージェントは有効にできません。DHCPv6 リレーエージェントは、外部 DHCPv6 サーバーでのみ機能しますが、DHCPv6 サーバーとして設定されたセキュリティ アプライアンス インターフェイスには DHCPv6 要求を転送しません。

[DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）] ダイアログボックスと [DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

ナビゲーション パス

[DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）]/[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックスには、[DHCPリレーIPv6（DHCP Relay IPv6）] ページ （2606 ページ）からアクセスできます。

関連項目

- [DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）]/[DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックス （2609 ページ）

フィールド リファレンス

表 *639 : [DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）]/[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックス*

要素	説明
インターフェイス（Interface）	DHCPv6 リレーエージェントを設定するインターフェイスの名前を入力または選択します。
DHCPv6リレーの有効化（Enable DHCPv6 Relay）	オンにすると、指定したインターフェイスでDHCPv6リレーが有効になります。

要素	説明
Set Route	このチェックボックスをオンにして、DHCPv6 サーバーから返された情報内のデフォルトルータアドレスが変更されるように DHCPv6 リレーエージェントを設定します。このオプションを選択した場合、DHCPv6 リレーエージェントは、DHCPv6 サーバーから返された情報内のデフォルトルータアドレスを、選択されたインターフェイスのアドレスで置き換えます。

[DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）]/[DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックス

新しい DHCP リレーサーバーを定義する場合は、[DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）] ダイアログボックスを使用します。既存のサーバー情報を更新する場合は、[DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックスを使用します。最大 10 台の DHCPv6 リレーサーバーを定義できます。

（注） [DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）] ダイアログボックスと [DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックスは実質的には同じです。次の説明は両方に適用されます。

ナビゲーション パス

[DHCPリレーIPv6サーバー設定の追加（Add DHCP Relay IPv6 Server Configuration）]/[DHCPリレーIPv6サーバー設定の編集（Edit DHCP Relay IPv6 Server Configuration）] ダイアログボックスには、[DHCPリレーIPv6（DHCP Relay IPv6）] ページ （2606 ページ）からアクセスできます。

関連項目

- [DHCPリレーIPv6エージェント構成の追加（Add DHCP Relay IPv6 Agent Configuration）]/[DHCPリレーIPv6エージェント構成の編集（Edit DHCP Relay IPv6 Agent Configuration）] ダイアログボックス （2608 ページ）

フィールド リファレンス

表 *640 : [DHCP*リレー*IPv6*サーバー設定の追加（*Add DHCP Relay IPv6 Server Configuration*）*]/[DHCP*リレー*IPv6*サーバー設定の編集（*Edit DHCP Relay IPv6 Server Configuration*）*]*

要素	説明
サーバ	IP アドレスを入力するか、または DHCPv6 要求の転送先の外部 DHCPv6 サーバーを表すネットワーク/ホストオブジェクトを選択します。
インターフェイス	DHCPv6 要求が外部 DHCPv6 サーバーに転送されるインターフェイスを入力または選択します。

DHCP サーバーの設定

Dynamic Host Configuration Protocol（DHCP）サーバは、IP アドレスなどのネットワーク設定パラメータを DHCP クライアントに提供します。セキュリティアプライアンスは、セキュリティアプライアンスのインターフェイスに接続された DHCP クライアントに、DHCP サーバまたは DHCP リレーサービスを提供できます。DHCP サーバは、ネットワーク設定パラメータを DHCP クライアントに直接提供します。一方、DHCP リレーでは、あるインターフェイスで受信された DHCP 要求が、別のインターフェイスの背後にある外部 DHCP サーバに渡されます。DHCP リレーの詳細については、[DHCP Relay] ページ （2602 ページ）を参照してください。

（注） セキュリティアプライアンスの DHCP サーバーは BOOTP 要求をサポートしません。マルチコンテキストモードの場合、複数のコンテキストが使用するインターフェイス上で DHCP サーバーまたは DHCP リレーをイネーブルにすることはできません。

セキュリティアプライアンスの各インターフェイスで、DHCP サーバを設定できます。各インターフェイスは、アドレスの導出元としてそれぞれのアドレスプールを持つことができます。ただし、その他の DHCP 設定（DNS サーバ、ドメイン名、オプション、ping タイムアウト、WINS サーバなど）は、グローバルに設定され、すべてのインターフェイスの DHCP サーバによって使用されます。

DHCP サーバがイネーブルになっているインターフェイスで、DHCP クライアントまたは DHCP リレーサービスを設定することはできません。また、DHCP クライアントは、サーバがイネーブルになっているインターフェイスに直接接続する必要があります。

外部インターフェイスでファイアウォールも DHCP クライアントとして動作している場合は、IP 設定のオートネゴシエーションをイネーブルにできます。これにより、ファイアウォールは、（DHCP クライアントとして）外部インターフェイスから取得した DNS、WINS、およびドメイン名のパラメータを、内部ネットワークのホストに渡すことができます。あるいは、DNS、WINS、およびドメイン名のパラメータを手動で指定することもできます。これらのパラメータを手動で指定したが、自動設定も有効になっている場合、自動設定よりも手動で指定した値が優先されます。

DHCP サーバ定義を管理するには、 [DHCP Server] ページ （2611 ページ）を使用します。

[DHCP Server] ページ

[DHCP Server] ページを使用して、グローバル DHCP サーバおよび Dynamic DNS（DDNS）での更新オプションの設定、1 つ以上のデバイス インターフェイスでの DHCP サーバの設定、および拡張サーバ オプションの設定を行います。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCPサーバー（DHCP Server）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCPサーバー（DHCP Server）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- DHCP サーバーの設定 （2610 ページ）

フィールド リファレンス

表 641 : [DHCP Server] ページ

要素	説明
Ping Timeout	ファイアウォールデバイスが DHCP ping 試行のタイムアウトを待つ時間をミリ秒単位で入力します。アドレス競合を回避するために、ファイアウォール デバイスは 2 つの ICMP ping パケットをアドレスに送信してから、そのアドレスを DHCP クライアントに割り当てます。有効値の範囲は 10 ～ 10000 ミリ秒です。
Lease Length	リースが期限切れになる前に、クライアントが割り当てられた IP アドレスを使用できる時間を秒単位で指定します。有効な値の範囲は、300 ～ 1048575 秒です。デフォルト値は 3600 秒（1 時間）です。

要素	説明
自動設定有効（Enable auto-configuration）（PIX および ASA 限定）	このオプションを選択すると、DHCP 自動設定がイネーブルになります。 DHCP 自動設定では、指定したインターフェイスで動作している DHCP クライアントから取得した DNS サーバ、ドメイン名、および WINS サーバの情報が、DHCP サーバから DHCP クライアントに提供されます。自動設定によって取得された情報のいずれかが手動でも指定されている場合は、手動で指定された情報の方が、検出された情報よりも優先されます。
インターフェイス	[Enable auto-configuration] チェックボックスがオンになっている場合、このフィールドが使用可能になります。DNS、WINS、およびドメイン名のパラメータを提供する DHCP クライアントを実行しているインターフェイスを入力または選択します。
[設定の定義（Define settings）]（任意）	
ドメイン名	DHCP クライアントの DNS ドメイン名を指定します。有効な DNS ドメイン名（example.com など）を入力します。
プライマリ DNS サーバ（Primary DNS Server）	IP アドレスを入力するか、または DHCP クライアントのプライマリ DNS サーバを表すネットワーク/ホスト オブジェクトを選択します。
プライマリ WINS サーバ（Primary WINS Server）	IP アドレスを入力するか、または DHCP クライアントのプライマリ WINS サーバを表すネットワーク/ホスト オブジェクトを選択します。
セカンダリ DNS サーバ（Secondary DNS Server）	IP アドレスを入力するか、または DHCP クライアントの代替 DNS サーバを表すネットワーク/ホスト オブジェクトを選択します。
セカンダリ WINS サーバ（Secondary WINS Server）	IP アドレスを入力するか、または DHCP クライアントの代替 WINS サーバを表すネットワーク/ホスト オブジェクトを選択します。
Dynamic DNS Update	

要素	説明
ダイナミック DNS 更新有効（Enable Dynamic DNS Update）	グローバルな DDNS 更新オプションを定義する場合は、このチェックボックスをオンにします。 • リソースレコード更新のタイプとして、[PTR レコードのみ（PTR Record only）] または [A および PTR レコード（A Record and PTR Record）] を選択します。 • [Override DHCP Client Request] も選択できます。選択した場合、DHCP クライアントによって要求されたすべての更新が、DHCP サーバ更新によって上書きされます。 これらのオプションは、ASA/PIX 7.2 以降でのみ使用可能です。
[DHCP Server Interface Configuration] テーブル	
Interface table	このテーブルには、DHCP サーバ、DDNS 更新、またはその両方が設定されているデバイス インターフェイスが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] ボタンでは [Add DHCP Server Interface Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Server Interface Configuration] ダイアログボックスが開きます。詳細については、[Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス （2613 ページ）を参照してください。
詳細オプション	
[Advanced] ボタン	[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス （2614 ページ）が開きます。

[Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス

これらのダイアログボックスを使用すると、DHCP をイネーブルにして、指定したインターフェイスに DHCP アドレス プールを指定したり、インターフェイスで Dynamic DNS（DDNS）更新をイネーブルにしたりすることができます。

（注） タイトルを除き、この 2 つのダイアログボックスは同じです。

ナビゲーション パス

[DHCPサーバーインターフェイス設定の追加（Add DHCP Server Interface Configuration）]/[DHCPサーバーインターフェイス設定の編集（Edit DHCP Server Interface Configuration）] ダイアログボックスには、[DHCP Server] ページ （2611 ページ）からアクセスできます。

関連項目

- DHCP サーバーの設定 （2610 ページ）

フィールド リファレンス

表 642 : [Add DHCP Server Interface Configuration]/[Edit DHCP Server Interface Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	DHCP サーバを設定するインターフェイスを識別します。インターフェイス名を入力するか、またはインターフェイス オブジェクトを選択します。
DHCP Address Pool	DHCP サーバが IP アドレスの割り当て時に使用する IP アドレスまたは（ハイフンで区切った）アドレス範囲を入力します。範囲の開始アドレスと終了アドレスは同じサブネット内にある必要があり、開始アドレスを終了アドレスより大きくすることはできません。
Enable DHCP Server	このインターフェイスで DHCP サーバーをイネーブルにするには、このチェックボックスをオンにします。
ダイナミック DNS 更新有効（Enable Dynamic DNS Update）	この DHCP サーバによる DDNS 更新をイネーブルにするには、このチェックボックスをオンにします。更新するレコードを指定します。 • PTR レコードのみ（PTR Record only） • **A Record and PTR Record** [DHCPクライアントリクエストのオーバーライド（Override DHCP Client Request）] も選択できます。選択した場合、DHCP クライアントによって要求されたすべての更新が、DHCP サーバ更新によって上書きされます。

[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス

[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックスでは、DHCP サーバに設定されている DHCP オプションを管理できます。DHCP オプションで、DHCP クライアントに追加情報を提供します。たとえば、DHCP オプション 150 お

よび DHCP オプション 66 は、Cisco IP Phone および Cisco IOS ルータに TFTP サーバ情報を提供します。

ナビゲーション パス

[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックスにアクセスするには、[DHCP Server] ページ （2611 ページ）で [Advanced] ボタンをクリックします。

関連項目

- DHCP サーバーの設定 （2610 ページ）

フィールド リファレンス

表 643 : [Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス

要素	説明
[Options] テーブル	このテーブルには、設定されている DHCP サーバ オプションが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] ボタンでは [Add DHCP Server Interface Configuration] ダイアログボックスが開き、[Edit Row] では [Edit DHCP Server Interface Configuration] ダイアログボックスが開きます。詳細については、[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックス （2615 ページ）を参照してください。

[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックス

[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックスでは、DHCP クライアントに追加情報を提供する DHCP サーバ オプション パラメータを設定できます。たとえば、DHCP オプション 150 および DHCP オプション 66 は、Cisco IP Phone および Cisco IOS ルータに TFTP サーバ情報を提供します。

ナビゲーション パス

[Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックスには、[Add DHCP Server Advanced Configuration]/[Edit DHCP Server Advanced Configuration] ダイアログボックス （2614 ページ）からアクセスできます。

関連項目

- DHCP サーバーの設定 （2610 ページ）
- [DHCP Server] ページ （2611 ページ）

フィールド リファレンス

表 644 : [Add DHCP Server Option]/[Edit DHCP Server Option] ダイアログボックス

要素	説明
オプション コード	使用可能なオプション コードのリストから、オプションを選択します。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（オプション 1 ～ 255）がサポートされています。 DHCP オプションコードの詳細情報については、cisco.com の『DHCP Options Reference』を参照してください。
タイプ（Type）	オプションが DHCP クライアントに返す情報のタイプを選択します。 • **IP**：このタイプを選択すると、1 つまたは 2 つの IP アドレスが DHCP クライアントに返されるように指定されます。最大 2 つの IP アドレスを指定します。 • **ASCII**：このタイプを選択すると、ASCII 値が DHCP クライアントに返されるように指定されます。ASCII 文字列を指定します。スペースを含めることはできません。 • **HEX**：このタイプを選択すると、16 進数値が DHCP クライアントに返されるように指定されます。桁数が偶数の HEX 文字列を、スペースを含めずに指定します。0x プレフィックスを使用する必要はありません。

[DNS] ページ

DNS ページを使用して、DNS サーバーグループを設定します。ファイアウォールデバイスは、これらの DNS サーバを使用して、完全修飾ドメイン名（ホスト名）を、ID 認証ファイアウォール ポリシーで使用する SSL VPN、証明書、および FQDN ネットワーク/ホスト オブジェクトの IP アドレスに解決します。サーバー名を定義するその他の機能（AAA など）は DNS 解決をサポートしていません。IP アドレスを入力するか、IP アドレスへの名前を手動で解決する必要があります。

ヒント　DefaultDNS サーバーグループは ASA で事前定義されており、FQDN ネットワーク/ホストオブジェクトの解決に使用されます。FQDN オブジェクトを使用する場合は、このグループの DNS サーバーを設定していることを確認してください。そうでない場合、名前を解決できません。セキュリティを強化するため、できればネットワーク内にある、信頼できる DNS サーバーを指定してください。詳細については、ID 認証ファイアウォール ポリシーの要件 （811 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DNS]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add DNS Server] ダイアログボックス （2619 ページ）

フィールド リファレンス

表 645 : [DNS] ページ

要素	説明
[DNS Server Groups] テーブル	このテーブルには、現在定義されている DNS サーバーグループが一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのグループ エントリを管理します。 [Add Row] ボタンでは [Add DNS Server Group] ダイアログボックスが開き、[Edit Row] ボタンでは [Edit DNS Server Group] ダイアログボックスが開きます。タイトルを除き、これらのダイアログボックスは同じです。詳細については、[Add DNS Server Group] ダイアログボックス （2618 ページ）を参照してください。
DNS Lookup Interfaces	DNS ルックアップをイネーブルにするインターフェイスが一覧表示されます。1 つ以上のインターフェイスまたはインターフェイス ロールを入力または選択します。
Enable DNS Guard（ASA/PIX 7.0(5)、7.2(x)、および 8.x のみ）	このチェックボックスをオンにすると、選択したデバイスまたは共有ポリシーで DNS Guard がイネーブルになります。DNS Guard は、セキュリティアプライアンスによって DNS 応答が転送されるとすぐに、DNS クエリーと関連付けられた DNS セッションをティアダウンします。また、DNS Guard は、メッセージ交換をモニタして、DNS 応答の ID が DNS クエリーの ID と一致することを確認します。 このコマンドは、DNS 検査が無効のインターフェイス上でのみ有効です。DNS インスペクションがイネーブルになっている場合、DNS Guard 機能は常に実行されます。 （注） 7.0(5) よりも前のリリースでは、DNS インスペクションの設定に関係なく、DNS Guard 機能は常にイネーブルになります。

要素	説明
DefaultDNS Server Group（ASA 8.4(2)+）	DefaultDNS サーバーグループのみに適用される追加設定。これらの設定は、FQDN ネットワーク/ホストオブジェクトを IP アドレスに解決するときに使用されます。 • [ポーリングタイマー（Poll Timer）]：FQDN ネットワーク/ホストオブジェクトを IP アドレスに解決するために使用するポーリングサイクルの時間（分単位）。FQDN オブジェクトはファイアウォール ポリシーで使用される場合にのみ解決されます。タイマーによって解決間隔の最大時間が決まります。IP アドレス解決に対して更新するタイミングの決定には DNS エントリの存続可能時間（TTL）値も使用されるため、個々の FQDN がポーリングサイクルよりも頻繁に解決される場合があります。 デフォルトは 240（4 時間）です。指定できる範囲は 1 ～ 65535 分です。 • [エントリの有効期限切れタイマー（Expire Entry Timer）]：DNS エントリの期限が切れた（TTL が経過した）後、そのエントリが DNS ルックアップテーブルから削除されるまでの分数。エントリを削除するとテーブルの再コンパイルが必要になります。このため、頻繁に削除するとデバイスの処理負荷が大きくなる可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。 デフォルトは 1 分です（つまり、TTL が経過してから 1 分後にエントリが削除されます）。指定できる範囲は 1 ～ 65535 分です。

[Add DNS Server Group] ダイアログボックス

[DNSサーバーグループの追加（Add DNS Server Group）] ダイアログボックスを使用して、セキュリティデバイスが、名前解決をサポートするポリシーの IP アドレスにサーバー名を解決するときに使用する、DNS サーバーグループの DNS サーバーおよび設定を定義します。

（注） このダイアログボックスと [Edit DNS Server Group] ダイアログボックスは、タイトルを除けば同じです。次の説明は両方に適用されます。

ナビゲーション パス

[Add DNS Server Group] および [Edit DNS Server Group] ダイアログボックスには、[DNS] ページ（2616 ページ）からアクセスできます。

フィールド リファレンス

表 646 : [Add DNS Server Group]/[Edit DNS Server Group] ダイアログボックス

要素	説明
名前	DNS サーバ グループの名前を指定します。 ヒント　DefaultDNS という名前は ASA で事前定義されており、FQDN ネットワーク/ホストオブジェクトの解決など、特定のグループの選択を許可しないポリシーに使用されるサーバーが含まれています。
DNS サーバ	このグループの DNS サーバーを一覧表示します。DNS 要求を転送可能な宛先のサーバを最大 6 台指定できます。セキュリティ アプライアンスは、応答を受け取るまで、各 DNS サーバを上から順に試行します。 （注）　また、[DNS] ページ （2616 ページ）の [DNS Lookup] セクションで、DNS がイネーブルになっているインターフェイスを少なくとも 1 つ指定する必要があります。 このリストの隣の各ボタンを使用して、エントリを管理します。上から順に次の機能があります。 • DNS サーバをリストに追加する。 [Add DNS Server] ダイアログボックス （2619 ページ）が開きます。 • リストから、選択されている DNS サーバ エントリを削除する。 • 現在選択されているエントリを 1 つ上の行に移動する。 • 現在選択されているエントリを 1 つ下の行に移動する。
タイムアウト（Timeout）	次の DNS サーバの試行を待機する秒数を 1 ～ 30 の範囲で指定します。デフォルトは 2 秒です。セキュリティ デバイスがサーバのリストを再試行するたびに、このタイムアウトは 2 倍に増えます。
Retries	セキュリティ デバイスが応答を受信しない場合に DNS サーバのリストを再試行する回数を、0 ～ 10 の範囲で指定します。
ドメイン名	任意で、サーバーの有効な DNS ドメイン名を指定します（**dnsexample.com** など）。

[Add DNS Server] ダイアログボックス

[Add DNS Server] ダイアログボックスを使用して、[Add DNS Server Group] または [Edit DNS Server Group] ダイアログボックス内の DNS サーバ リストに DNS サーバを追加します。

ナビゲーション パス

[Add DNS Server] ダイアログボックスには、[Add DNS Server Group] または [Edit DNS Server Group] ダイアログボックスからアクセスできます。これらのダイアログボックスの詳細については、[Add DNS Server Group] ダイアログボックス （2618 ページ）を参照してください。

関連項目

- [DNS] ページ （2616 ページ）

フィールド リファレンス

表 *647 : [Add DNS Server]* ダイアログボックス

要素	説明
DNS サーバー	DNS サーバーの IP アドレス、または DNS サーバーのアドレスを定義するホストネットワーク/ホストオブジェクト。アドレスを入力します。または、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成します。
[インターフェイス（Interface）]（ASA 9.5(1) 以降）	[選択（Select）] をクリックして、インターフェイスを選択します。[インターフェイス（Interface）] セレクタダイアログボックスには、インターフェイスロールのみが一覧表示され、物理インターフェイスは表示されません。そのため、送信元インターフェイスを選択する前に、インターフェイスロールに物理インターフェイスを追加する必要があります。インターフェイスにデフォルト値はありません。 この機能は、ASA バージョン 9.5(1) 以降を実行しているデバイスの Security Manager バージョン 4.9 以降で使用できます。

DDNS の設定

Dynamic DNS（DDNS）は、DHCP で割り当てられた IP アドレスが頻繁に変更されても各ホストが互いを検出できるように、IP アドレスとドメイン名のマッピングの更新を行います。また、バージョン 7.2(3) 以降では、Cisco セキュリティ アプライアンスは DDNS 更新を生成できます。この機能は、[DDNS] ページで設定します。

DDNS マッピングは、DHCP サーバーで 2 種類の Resource Record（RR）内で管理されます。アドレス（A）レコードには、名前から IP アドレスへのマッピングが含まれ、ポインタ（PTR）レコードはアドレスをホスト名にマップします。

DDNS は、定義した間隔で割り当て済みのアドレスとホスト名の間のアソシエーションを自動的に記録するため、アドレスとホスト名のアソシエーションを頻繁に変更することができます。これにより、たとえばモバイルホストは、ユーザまたは管理者が操作することなく、ネットワーク内を自由に移動できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DDNS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DDNS]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 648 : [DDNS] ページ

要素	説明
Dynamic DNS Interface Settings	このテーブルには、現在定義されている DDNS インターフェイス更新方式が一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらの方式を管理します。[Add Row] および [Edit Row] ボタンを使用すると、[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス （2621 ページ）が開きます。
DHCP Client requests DHCP Server to update records	DHCP クライアント更新要求のための、アプライアンスでのグローバル設定。このオプションでは、クライアントが DHCP サーバを介して DDNS 更新を送信できるようにし、更新するレコード（PTR リソース レコード、A リソース レコードと PTR リソース レコードの両方、またはどちらも更新しない）を指定します。[Not Selected]、[Only PTR Record]、[Both A and PTR Record]、または [No Update] を選択します。
DHCP Client ID Interface	グローバル DHCP クライアントの更新要求で使用するインターフェイスを指定します。インターフェイス名または IP アドレスを入力するか、インターフェイス オブジェクトを選択します。
DHCPクライアントブロードキャストの有効化（Enable DHCP Client Broadcast）	このオプションを選択すると、デバイス上の DHCP クライアントが DDNS 更新をブロードキャストできます。ASA/PIX 7.2(3)+デバイスだけで選択可能です。

[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス

[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックスを使用して、Dynamic DNS 更新のルールを管理します。これらのルールは、インターフェイスごとに定義します。

ナビゲーション パス

[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックスには、 DDNS の設定（2620 ページ）からアクセスします。

関連項目

- [DDNS Update Methods] ダイアログボックス （2622 ページ）
- [Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックス （2623 ページ）

フィールド リファレンス

表 *649 : [Add DDNS Interface Rule]/[Edit DDNS Interface Rule]* ダイアログボックス

要素	説明
インターフェイス（Interface）	DDNS を設定するインターフェイスの名前を入力または選択します。 （注） 指定したインターフェイスでは、DHCP がイネーブルになっている必要があります。
メソッド名	以前に定義されている DDNS 更新方式を選択するか、または [更新方式の追加（Add Update Method）]/[更新方式の編集（Edit Update Method）] を選択して新しい方式を定義します。 [DDNS Update Methods] ダイアログボックス （2622 ページ）ダイアログボックスが開きます。
ホストネーム	更新の送信先の DDNS サーバ ホストの名前を入力します。
DHCP Client requests DHCP Server to update records	インターフェイスでの DHCP クライアントの更新要求の設定。DHCP サーバが、PTR リソース レコードだけを更新するか、A リソース レコードと PTR リソース レコードの両方を更新するか、またはどちらも更新しないかを指定します。 [Not Selected]、[Only PTR Record]、[Both A and PTR Record]、または [No Update] を選択します。[Not Selected] 以外の項目を選択すると、DDNS の設定 （2620 ページ）のグローバル設定が上書きされます。

[DDNS Update Methods] ダイアログボックス

[DDNS Update Methods] ダイアログボックスを使用して、Dynamic DNS 更新の方式を管理します。定義済みの方式ではそれぞれ、更新間隔と、更新対象のリソース レコードが指定されています。

ナビゲーション パス

[DDNS 更新方式（DDNS Update Methods）] ダイアログボックスにアクセスするには、[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス （2621 ページ）の [方式名（Method Name）] ドロップダウンリストから [更新方式の追加（Add Update Method）]/[更新方式の編集（Edit Update Method）] を選択します。

関連項目

- DDNS の設定 （2620 ページ）

フィールド リファレンス

表 *650 : [DDNS Update Methods]* ダイアログボックス

要素	説明
Update Methods	このテーブルには、現在定義されている更新方式が一覧表示されます。テーブルの下のボタンを使用して、これらのエントリを管理します。
[Add Row] ボタン	新しい更新方式を定義できる [Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックス （2623 ページ）が開きます。
[Edit Row] ボタン	テーブルで現在選択されている方式を編集できる [Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックス （2623 ページ）が開きます。
[Delete Row] ボタン	[更新方式（Update Methods）] テーブルで現在選択されている方式を削除します。確認が必要な場合があります。

[Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックス

[Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックスを使用して、DDNS 更新方式を定義または編集します。現在定義されている方式は、[DDNS Update Methods] ダイアログボックス （2622 ページ）に一覧表示されます。

ナビゲーション パス

[Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックスにアクセスするには、[DDNS Update Methods] ダイアログボックス （2622 ページ）で [Add Row] または [Edit Row] ボタンをクリックします。

関連項目

- DDNS の設定 （2620 ページ）

フィールド リファレンス

表 651 : [Add DDNS Update Methods]/[Edit DDNS Update Methods] ダイアログボックス

要素	説明
メソッド名	この方式の識別子を指定します。
[アップデート間隔（Update Interval）]	この方式でのレコードの更新頻度を指定します。日数、時間数、分数、および秒数を指定します。時間、分、および秒のデフォルト値は 0 ですが、[Day] のデフォルト値はないため、[Day] には数字を入力する必要があります。
Update Records	更新するリソースレコードを指定します。[定義なし（Not Defined）]、[A レコード（A Records）]、または [A および PTR レコードの両方（Both A and PTR Records）] を選択してください。[A Records] または [Both A and PTR Records] を選択すると、[Add DDNS Interface Rule]/[Edit DDNS Interface Rule] ダイアログボックス （2621 ページ）の設定が上書きされます。

[NTP] ページ

正確に同期された時刻をネットワーク システムに提供するサーバの階層システムを実装するには、ネットワーク タイム プロトコル（NTP）を使用します。正確なタイム スタンプが関連する時間依存操作（Certificate Revocation List（CRL; 証明書失効リスト）など）では、時刻が正確である必要があります。複数の NTP サーバーを設定できます。セキュリティ デバイスは、（データの信頼度を測る手段として）最下層のサーバを選択します。

（注） このページは Catalyst 6500 サービス モジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

[NTP]ページを使用して、NTPをイネーブルにし、セキュリティデバイスの時刻を動的に設定するために使用する NTP サーバを管理します。

（注） NTP サーバーから取得された時刻によって、[クロック（Clock）] ページで手動で設定した時刻がオーバーライドされます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 652 : [NTP] ページ

要素	説明
Enable NTP Authentication	NTP サーバでの認証をイネーブルまたはディセーブルにします。認証をディセーブルにしても、設定されているサーバのリストは変更されません。 認証をイネーブルにした場合、セキュリティ アプライアンスは、パケット内で適切な trusted key を使用している場合にだけ、NTP サーバと通信します。また、セキュリティ アプライアンスは、認証キーを使用して NTP サーバと同期します。
NTP Server Table	現在設定されている NTP サーバが一覧表示されます。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、このリストを管理します。[Add Row] および [Edit Row] ボタンを使用すると、[NTP Server Configuration] ダイアログボックス （2625 ページ）が開きます。

[NTP Server Configuration] ダイアログボックス

[NTP Server Configuration] ダイアログボックスを使用して、NTP サーバ定義を追加または編集します。

ナビゲーション パス

[NTP Server Configuration] ダイアログボックスには、[NTP] ページ （2624 ページ）からアクセスできます。

（注） [NTP] ページは Catalyst 6500 サービスモジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

フィールド リファレンス

表 653 : [NTP Server Configuration] ダイアログボックス

要素	説明
IPアドレス	NTP サーバの IP アドレスを入力または選択します。
優先（Preferred）	このチェックボックスをオンにした場合、複数のサーバの精度が同程度であれば、この NTP サーバが優先サーバとなります。 NTP では、どのサーバーの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバーに同期します。複数のサーバの精度が同程度であれば、このオプションで指定されたサーバが使用されます。ただし、優先サーバよりもはるかに精度の高いサーバがある場合、セキュリティアプライアンスによって精度の高い方のサーバが使用されます。たとえば、セキュリティ アプライアンスでは、第 3 層の優先サーバではなく第2層のサーバが使用されます。複数のサーバの層が同じである可能性が高い場合にだけ、NTP サーバを優先サーバとして設定することを推奨します。
インターフェイス	ルーティング テーブル内のデフォルト インターフェイスを上書きする場合は、NTP トラフィックに使用するインターフェイスを入力または選択します。
認証タイプ（Authentication Type）	MD5 に追加すると、ASA 9.13(1) 以降のデバイスでは、バージョン 4.20 以降の Cisco Security Manager で次の認証タイプもサポートされます。 • sha1 • sha256 • sha512 • cmac
Key Number	この認証キーの ID を入力します。NTP サーバーのパケットも、常にこのキー ID を使用する必要があります。以前に別のサーバに対してキー ID を設定した場合は、そのキー ID をリストから選択できます。それ以外の場合は、1 ～ 4294967295 の数字を入力します。
信頼できる	このキーを trusted key として設定します。認証を正常に行うには、このオプションを選択する必要があります。
Key Value	認証キーを最大 32 文字の文字列として入力します。
確認（Confirm）	認証キーを再入力して、それが正しいことを確認します。

[SMTP Server] ページ

[SMTPサーバー（SMTP Server）]ページを使用して、SMTP サーバーの IP アドレスを指定し、必要に応じて、バックアップサーバーの IP アドレスを指定します。バックアップサーバーの IP アドレスには、特定のイベントへの応答として電子メールアラートと通知が送信されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [SMTPサーバー（SMTP Server）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [SMTPサーバー（SMTP Server）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 654 : [SMTP Server] ページ

要素	説明
Primary Server IP Address	SMTP サーバーの IP アドレスを入力または選択します。
セカンダリサーバーのIPアドレス（Secondary Server IP Address）	バックアップ SMTP サーバの IP アドレスを入力または選択します。

[TFTP Server] ページ

簡易ファイル転送プロトコル（TFTP）は、単純なクライアント/サーバーファイル転送プロトコルで、RFC783 および RFC1350 Rev. 2 で規定されています。[TFTP Server] ページを使用して、セキュリティアプライアンスが実行設定のコピーを TFTP サーバに転送できるように、セキュリティアプライアンスを TFTP クライアントとして設定できます。この方法で、設定ファイルをバックアップして、複数のセキュリティアプライアンスに伝播できます。1 台のサーバだけがサポートされます。

ナビゲーション パス

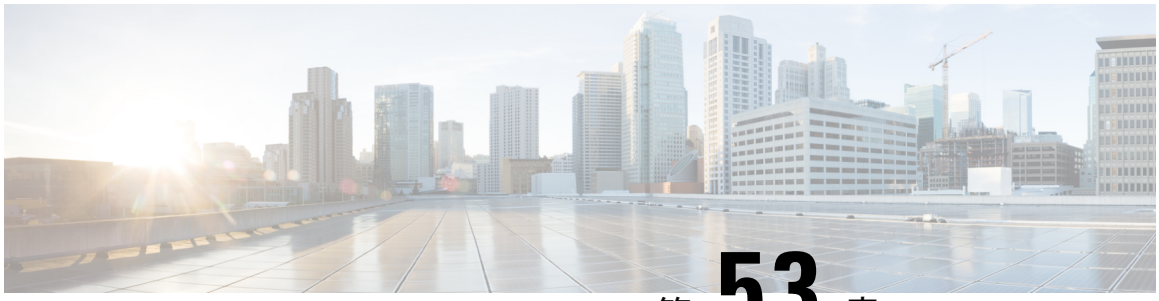
- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [TFTPサーバー（TFTP Server）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [TFTPサーバー（TFTP Server）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 655 : [TFTP Server] ページ

要素	説明
インターフェイス（Interface）	TFTP サーバへのアクセスに使用するインターフェイスの名前を入力または選択します。
IPアドレス	TFTP サーバーの IP アドレスを入力または選択します。
ディレクトリ	スラッシュ（/）で始まり、構成ファイルが書き込まれるファイル名で終わる TFTP サーバー上のパスを入力します（例：**/tftpboot/asa/config3**）。 （注）　パスの先頭には必ずスラッシュ（/）を付けます。



第 53 章

Firepower 2100 シリーズ デバイスでの FXOS サーバーアクセス設定の構成

[FXOSサーバーアクセス（FXOS Server Access）] セクションには、Firepower 2100 デバイスで FXOS サーバーアクセスを設定するためのページが含まれています。[FXOS サーバーアクセス（FXOS Server Access）] は、デバイスセレクタまたはポリシーセレクタの [デバイス管理（Device Admin）] の下にあります。

ASA および Cisco Security Manager でサポートされる Firepower 2100 シリーズ デバイスは次のとおりです。

- Cisco FPR-2110 適応型セキュリティアプライアンス
- Cisco FPR-2120 適応型セキュリティアプライアンス
- Cisco FPR-2130 適応型セキュリティアプライアンス
- Cisco FPR-2140 適応型セキュリティアプライアンス

この章は次のトピックで構成されています。

- [HTTPS] ページ （2629 ページ）
- SSH ページ（SSH Page） （2631 ページ）
- [SNMP] ページ （2633 ページ）

[HTTPS] ページ

[HTTPS] ページでは、HTTPS を介して FXOS サーバーにアクセスするようにデバイスを設定できます。このプロトコルを使用して設定を展開すると、Cisco Security Manager では設定ファイルが暗号化されてからデバイスに送信されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [FXOS サーバーアクセス（FXOS Server Access）] > [HTTPS] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [FXOS サーバーアクセス（FXOS Server Access）] > [HTTPS] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [HTTPSの追加（Add HTTPS）]/[HTTPSの編集（Edit HTTPS）] ダイアログボックス （2630 ページ）

フィールド リファレンス

表 *656 : [HTTPS]* ページ

要素	説明
操作	許可アクションにより、IP アドレスとポートを使用して Firepower 2100 シリーズ デバイスを設定できます。IPv4 および IPv6 アドレスをサポートします。
インターフェイス	HTTPS が設定されているデバイスインターフェイスの名前。ブリッジグループ（BG）インターフェイスでは HTTPS を設定できません。
IPアドレス	デバイスの IP アドレス。アドレスは IPv4 または IPv6 アドレスです。
[ポート（Port）]	FXOS サーバーとの通信が行われるポート。

[HTTPSの追加（Add HTTPS）]/[HTTPSの編集（Edit HTTPS）] ダイアログボックス

[HTTPS構成の追加（Add HTTPS Configuration）] ダイアログボックスを使用して、HTTPS ルールを作成します。セキュリティアプライアンスは、このサーバを自動的にポーリングして、イメージおよび設定の更新がないかどうかを確認します。

[HTTPS構成の編集（Edit HTTPS Configuration）] ダイアログボックスは、[HTTPS構成の追加（Add HTTPS Configuration）] ダイアログボックスと同じです。次の説明は両方に適用されます。

ナビゲーション パス

[HTTPS構成の追加（Add HTTPS Configuration）] および [HTTPS構成の編集（Edit HTTPS Configuration）] ダイアログボックスには、[HTTPS] ページ （2629 ページ）からアクセスできます。

フィールド リファレンス

表 *657 : [HTTPS*構成の追加（*Add HTTPS Configuration*）*]/[HTTPS*構成の編集（*Edit HTTPS Configuration*）*]* ダイアログボックス

要素	説明
操作	[許可（Permit）] を選択します。
インターフェイス	[選択（Select）] をクリックし、インターフェイスを選択します。ブリッジグループ（BG）インターフェイスは HTTPS では設定できません。
IPアドレス	[選択（Select）] をクリックして、FXOS サーバーにアクセスできるデバイスの IP アドレスを選択します。アドレスは IPv4 または IPv6 アドレスです。
[ポート（Port）]	ページを保存すると、この値はデフォルトで 3443 に設定されます。FXOS サーバーとの通信が行われるポートも入力できます。

SSH ページ（SSH Page）

[Secure Shell] ページを使用して、SSH プロトコルを使用した Firepower 2100 シリーズ デバイスへの FXOS サーバーアクセスを許可するポートを設定します。ルールでは、特定の IP アドレスとネットマスクへの SSH アクセスが許可されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [FXOSサーバーアクセス（FXOS Server Access）] > [SSH] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [FXOSサーバーアクセス（FXOS Server Access）] > [SSH] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [HTTPSの追加（Add HTTPS）]/[HTTPSの編集（Edit HTTPS）] ダイアログボックス （2630 ページ）

フィールド リファレンス

表 *658 : SSH* ページ（*SSH Page*）

要素	説明
操作	許可アクションにより、FXOS サーバーにアクセスするための IP アドレスとポートを使用して Firepower 2100 シリーズ デバイスを設定できます。IPv4 および IPv6 アドレスをサポートします。
インターフェイス	SSH が設定されているデバイスインターフェイスの名前。ブリッジグループ（BG）インターフェイスでは SSH を設定できません。
IPアドレス	デバイスの IP アドレス。アドレスは IPv4 または IPv6 アドレスです。
[ポート（Port）]	FXOS サーバーとの通信が行われるポート。

[SSHホストの追加（AddSSHHost）]/[SSHホストの編集（EditSSHHost）] ダイアログボックス

[SSH構成の追加（Add SSH Configuration）] ダイアログボックスを使用して、SSH ルールを作成します。セキュリティアプライアンスは、このサーバを自動的にポーリングして、イメージおよび設定の更新がないかどうかを確認します。

[SSH構成の編集（Edit SSH Configuration）] ダイアログボックスは、[SSH構成の追加（Add SSH Configuration）] ダイアログボックスと同じです。次の説明は両方に適用されます。

ナビゲーション パス

[SSH構成の追加（Add SSH Configuration）] および [SSH構成の編集（Edit SSH Configuration）] ダイアログボックスには、[HTTPS] ページ （2629 ページ）からアクセスできます。

フィールド リファレンス

表 *659 : [SSH*構成の追加（*Add SSH Configuration*）*]/[SSH*構成の編集（*Edit SSH Configuration*）*]* ダイアログボックス

要素	説明
操作	[許可（Permit）] を選択します。
インターフェイス	[選択（Select）] をクリックし、インターフェイスを選択します。ブリッジグループ（BG）インターフェイスは SSH では設定できません。
IPアドレス	[選択（Select）] をクリックして、FXOS サーバーにアクセスできるデバイスの IP アドレスを選択します。アドレスは IPv4 または IPv6 アドレスです。

要素	説明
[ポート（Port）]	ページを保存すると、この値はデフォルトで 3022 に設定されます。FXOS サーバーとの通信に使用されるポートも入力できます。

[SNMP] ページ

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP ページを使用して、SNMP による監視のために Firepower 2100 シリーズ デバイスを設定できます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [FXOSサーバーアクセス（FXOS Server Access）] > [SNMP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [デバイス管理（Device Admin）] > [FXOSサーバーアクセス（FXOS Server Access）] > [SNMP] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [SNMPの追加（Add SNMP）]/[SNMPの編集（Edit SNMP）] ダイアログボッス （2634 ページ）

フィールド リファレンス

表 *660 : [SNMP]* ページ

要素	説明
操作	許可アクションにより、FXOS サーバーにアクセスするための IP アドレスとポートを使用して Firepower 2100 シリーズ デバイスを設定できます。IPv4 および IPv6 アドレスをサポートします。
インターフェイス	SNMP が設定されているデバイスインターフェイスの名前。ブリッジグループ（BG）インターフェイスでは SSH を設定できません。
IPアドレス	デバイスの IP アドレス。アドレスは IPv4 または IPv6 アドレスです。
[ポート（Port）]	FXOS サーバーとの通信が行われるポート。

[SNMPの追加（Add SNMP）]/[SNMPの編集（Edit SNMP）] ダイアログボックス

[SNMP 構成の追加（Add SNMP Configuration）] ダイアログボックスを使用して、SNMP ルールを作成します。セキュリティアプライアンスは、このサーバを自動的にポーリングして、イメージおよび設定の更新がないかどうかを確認します。

[SNMP 構成の編集（Edit SNMP Configuration）] ダイアログボックスは、[SNMP 構成の追加（Add SNMP Configuration）] ダイアログボックスと同じです。次の説明は両方に適用されます。

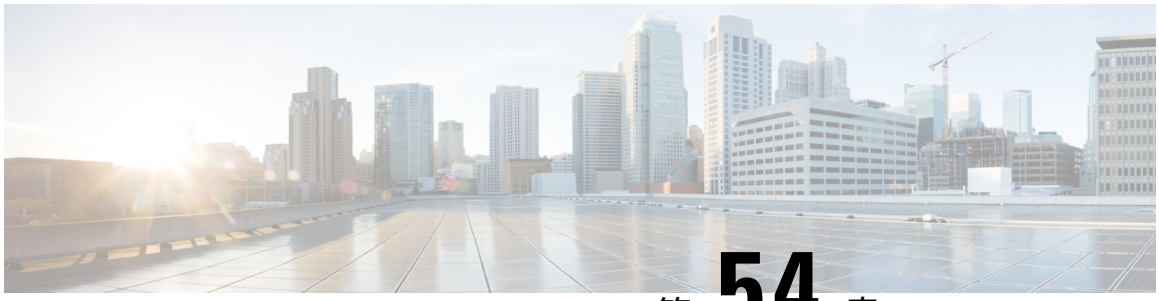
ナビゲーション パス

[SNMP構成の追加（Add SNMP Configuration）] および [SNMP構成の編集（Edit SNMP Configuration）] ダイアログボックスには、[SNMP] ページ（2633 ページ）からアクセスできます。

フィールド リファレンス

表 *661 : [SNMP*構成の追加（*Add SNMP Configuration*）*]/[SNMP*構成の編集（*Edit SNMP Configuration*）*]* ダイアログボックス

要素	説明
操作	[許可（Permit）] を選択します。
インターフェイス	[選択（Select）] をクリックし、インターフェイスを選択します。ブリッジグループ（BG）インターフェイスは、SNMP で構成できません。
IPアドレス	[選択（Select）] をクリックして、FXOS サーバーにアクセスできるデバイスの IP アドレスを選択します。アドレスは IPv4 または IPv6 アドレスです。
[ポート（Port）]	ページを保存すると、この値はデフォルトで 3161 に設定されます。FXOS サーバーとの通信が行われるポートも入力できます。



第 54 章

ファイアウォール デバイスでのロギング ポリシーの設定

ロギング機能では、NetFlow「コレクタ」のイネーブル化と管理、システムロギングのイネーブル化、ロギングパラメータの設定、イベントリスト（syslog フィルタ）の設定、宛先へのフィルタの適用、syslog メッセージの設定、syslog サーバーの設定、および電子メール通知パラメータの指定を行います。

[Logging Setup] ページを使用してロギングをイネーブルにし、ロギング パラメータを設定したあとで、[Event Lists] ページで（syslog のセットに対して）フィルタを設定します。このフィルタをロギング先に送信できます。[Logging Filters] ページでは、送信する syslog のロギング先を指定します。最後に、[Syslog] ページと [E-Mail] ページで syslog と電子メールを設定します。

この章は次のトピックで構成されています。

- [NetFlow] ページ （2635 ページ）
- 組み込まれている Event Manager （2638 ページ）
- [E-Mail Setup] ページ （2645 ページ）
- [Event Lists] ページ （2647 ページ）
- [Logging Filters] ページ （2651 ページ）
- ロギング設定の設定 （2655 ページ）
- レート制限レベルの設定 （2658 ページ）
- Syslog サーバ設定の設定 （2662 ページ）
- Syslog サーバの定義 （2669 ページ）

[NetFlow] ページ

NetFlowデータ エクスポート用に設定されているデバイスは、そのデバイスのフローベースのトラフィック統計をキャプチャします。この情報は、デバイスからNetFlow コレクション サーバにユーザ データグラム プロトコル（UDP）データグラムの形式で定期的に送信されます。

[NetFlow] ページでは、選択したデバイスで NetFlow エクスポートをイネーブルにし、収集したフロー情報を送信する NetFlow「コレクタ」を定義および管理します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）]>[ロギング（Logging）] > [NetFlow]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [NetFlow]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ルール テーブルの使用 （764 ページ）
- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

フィールド リファレンス

表 662 : [NetFlow] ページ

要素	説明
Enable Flow Export	オンになっている場合は、NetFlowデータエクスポートがイネーブルになります。
Template Export Interval	フロー情報がコレクタに送信される間隔（分単位）。この値は、1 ～ 3600 分で、デフォルトは 30 です。
アクティブ更新間隔（Active Refresh Interval）	アクティブ接続では、flow-updateイベント間の間隔を分単位で指定します。有効な値は、1 ～ 60 分です。デフォルト値は 1 分です。
遅延フロー作成（Delay Flow Create）	flow-create イベントの送信を指定した秒数遅らせます。値は 1 ～ 180 秒です。 この値が入力されていない場合は、遅延はなく、flow-create イベントはフローが作成された時点でエクスポートされます。設定されている遅延よりも前にフローが切断された場合は、flow-create イベントは送信されません。その代わりに拡張フロー ティアダウン イベントが送信されます。

要素	説明
Collectors table	現在定義されているNetFlowコレクタがリストされます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。 [Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、[Add Collector]/[Edit Collector] ダイアログボックス（NetFlow） （2637 ページ）が開きます。 （注） Cisco Security Manager では、ASA 9.6(4) から 9.7.0、および 9.8(2) 以降のデバイスに対する重複するNetflowコレクタは許可されません。デバイスの現在の設定を変更するか、重複している構成を削除します（**[プラットフォーム（Platform）] > [ロギング（Logging）] > [Netflow]**）。

[Add Collector]/[Edit Collector] ダイアログボックス（NetFlow）

[コレクタの追加（Add Collector）] および [コレクタの編集（Edit Collector）] ダイアログボックスを使用して、NetFlowの「コレクタ」を定義および編集します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[Add Collector]/[Edit Collector] ダイアログボックスは、[NetFlow] ページ （2635 ページ）から開くことができます。

フィールド リファレンス

表 663 : [Add Collector]/[Edit Collector] ダイアログボックス

要素	説明
インターフェイス（Interface）	コレクタのアクセスに使用するデバイス インターフェイスの名前を入力または選択します。
コレクタ	NetFlow パケットの送信先のサーバの IP アドレスまたはネットワーク名を入力します。ネットワーク/ホストオブジェクトも選択できます。
UDP ポート（UDP Port）	NetFlow パケットの送信先の指定済みコレクタ上の UDP ポートを指定します。値の範囲は 1 ～ 65535 で、デフォルトは 2055 です。

組み込まれている Event Manager

Embedded Event Manager（EEM; 組み込みイベントマネージャ）を利用することで、問題をデバッグすることが可能になり、トラブルシューティング用に汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。

（注） Embedded Event Manager は、ASA 9.2(1) 以降でのみサポートされます。

サポートされるイベント

EEM は次のイベントをサポートします。

- Syslog：ASA は、syslog メッセージの ID を使用して、イベント マネージャ アプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベント マネージャ アプレット内で syslog メッセージの ID が重複することはできません。
- タイマー：タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベント マネージャ アプレットに対して一度だけ設定できます。各イベント マネージャ アプレットには最大で 3 つのタイマーがあります。3 種類のタイマーは次のとおりです。
  - ウォッチドッグ（定期的）タイマーは、アプレットアクションの完了後に指定された期間が経過するとイベント マネージャ アプレットをトリガーし、自動的にリスタートします。
  - カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベント マネージャアプレットを1回トリガーします。削除および再追加されない限りはリスタートしません。
  - 絶対（1 日 1 回）タイマーは、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は hh:mm:ss です。

各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを 1 つだけ設定できます。

- [なし（None）]：イベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。output コマンドの値に関係なく、action コマンドはクラッシュ情報ファイルを対象とします。出力は、show tech コマンドの前に生成されます。

（注） Syslog ID の範囲を使用するとき、およびタイマーを使用するときは注意が必要です。設定が正しくないと、ASA ループが発生し、アプレットが正常に実行されなくなる可能性があります。

アクションの設定

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先の設定

次の 3 つの場所のいずれかに action CLI コマンドの出力を送信できます。

- なし：デフォルトの設定です。出力を破棄します。
- コンソール：出力を ASA コンソールに送信します。
- ファイル：出力をファイルに送信します。次の 4 つのファイル オプションを使用できます。
  - 新規：イベント マネージャ アプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
  - 上書き：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。
  - 付加：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
  - ローテート：連のファイルを作成する：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

注意事項と制約事項

- シングル モードでだけサポートされています。マルチ コンテキスト モードではサポートされません。
- ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。
- EEM は、デバイスでロギング機能がイネーブルになっているかどうかに関係なくイネーブルになります。
- ASA の EEM 機能には、Cisco ルータにある EEM 機能のサブセットのみが含まれています。

- 通常、クラッシュ時は、ASA の状態は不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。
- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は none です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

Embedded Event Manager テーブルには、現在定義されているイベント マネージャ アプレットが一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。[Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス （2640 ページ）が開きます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Embedded Event Manager]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Embedded Event Manager]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス （2640 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログ ボックスを使用して、イベントマネージャアプレットを定義および編集します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックスは、 組み込まれている Event Manager （2638 ページ）から開くことができます。

フィールド リファレンス

表 *664 : [アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス*

要素	説明
名前	イベント マネージャ アプレットの一意の名前を入力します。名前にスペースを含めることはできず、32 文字未満にする必要があります。
説明	イベント マネージャ アプレットの説明を入力します。説明の長さは最大 256 文字です。
[構成] タブ	
クラッシュ情報	選択すると、ASA がクラッシュしたときにイベント マネージャ アプレットがトリガーされます。Output コマンドの値に関係なく、action コマンドはクラッシュ情報ファイルを対象とします。出力は、show tech コマンドの前に生成されます。 （注） ASA がクラッシュした場合、その状態は通常は不明です。一部の CLI コマンドは、この状態のときに実行するのは安全でない場合があります。
なし（None）	選択すると、イベント マネージャ アプレットを手動でトリガーできます。 （注） EEM アプレットの手動トリガーは、Cisco Security Manager ではサポートされていません。アプレットを手動でトリガーするには、FlexConfig を使用する必要があります。詳細については、FlexConfig の管理 （431 ページ）を参照してください。
Syslog テーブル	Syslog テーブルには、選択したアプレットに現在定義されている Syslog メッセージ ID が一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。[Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、[Syslog 設定の追加（Add Syslog Configuration）]/[Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックス （2644 ページ）が開きます。
Absolute	絶対（1 日 1 回）タイマーイベントの設定。絶対タイマーが、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。 提供されたフィールドを使用して、時間、分、秒で時刻を入力します。時刻の範囲は 00:00:00（真夜中）から 23:59:59 です。

要素	説明
カウントダウン	カウントダウン（ワンショット）タイマーイベントを設定します。カウントダウンタイマーは、指定された期間が経過するとイベント マネージャ アプレットを 1 回トリガーします。削除および再追加されない限りはリスタートしません。 期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
ウォッチドッグ	ウォッチドッグ（定期的）タイマーイベントを設定します。ウォッチドッグタイマーは、アプレットアクションの完了後に指定された期間が経過するとイベントマネージャアプレットをトリガーし、自動的にリスタートします。 期間を秒単位で入力します。秒数は、1 ～ 604800 の範囲で設定してください。
出力	アクションからの出力を送信するための特定の宛先を設定するには、使用可能な出力宛先オプションのいずれかを選択します。 • なし：（デフォルト）出力を破棄します。 • コンソール：出力を ASA コンソールに送信します。 • ファイル：出力をファイルに送信します。[アクション（Action）] リストでファイルオプションを選択します。

要素	説明
操作	次の 4 つのファイル オプションを使用できます。 • 新規：イベントマネージャアプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。ファイル名は eem-applet-timestamp.log というフォーマットで、applet はイベントマネージャ アプレットの名前、timestamp は YYYYMMDD-hhmmss 形式の日付型タイムスタンプです。 • 上書き：イベントマネージャアプレットが呼び出されるたびに、指定されたファイルを上書きします。[ファイルの場所（File Location）] および [ファイル名（File Name）] フィールドを使用して、ファイルの詳細を指定します。 • 付加：イベントマネージャアプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。[ファイルの場所（File Location）] および [ファイル名（File Name）] フィールドを使用して、ファイルの詳細を指定します。 • ローテート：イベントマネージャアプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。[ファイル数（File Count）] フィールドでローテーションするファイルの数を指定します（有効な値の範囲は 2 から 100）。 新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数で示されます。ファイル名の形式は、eem-applet-x.log です。ここで、applet はアプレットの名前、x はファイル番号を示しています。
ファイルの場所（File Location）	出力ファイルの場所を指定します。ローテーションは、FTP、TFTP、および SMB のターゲットファイルを使用する場合もあります。
ファイル名	出力ファイルのファイル名を指定します。
ファイル数	「ローテート」が選択されたアクションの場合、ローテーションするファイル数を指定します。 新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数で示されます。有効なローテーションの値の範囲は 2 ～ 100 です。ファイル名の形式は、eem-applet-x.log です。ここで、applet はアプレットの名前、x はファイル番号を示しています。
[Action] タブ	

要素	説明
アクション テーブル	アクションテーブルには、選択したアプレットに現在定義されているアクションが一覧表示されます。テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、これらのエントリを管理します。[Add Row] ボタンおよび [Edit Row] ボタンをクリックすると、アクション構成の追加および編集ダイアログボックス （2645 ページ）が開きます。

[Syslog 設定の追加（Add Syslog Configuration）]/[Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックス

[Syslog 設定の追加（Add Syslog Configuration）] および [Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックスを使用して、イベントマネージャアプレットの Syslog メッセージ ID を設定します。タイトルを除き、2 つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[Syslog 設定の追加（Add Syslog Configuration）] および [Syslog 設定の編集（Edit Syslog Configuration）] ダイアログボックスには、[アプレットの追加（Add Applet）] および [アプレットの編集（Edit Applet）] ダイアログボックス （2640 ページ）からアクセスできます。

フィールド リファレンス

表 *665 : [Syslog* 設定の追加（*Add Syslog Configuration*）*]/[Syslog* 設定の編集（*Edit Syslog Configuration*）*]* ダイアログボックス

要素	説明
ID	単一の syslog メッセージまたは syslog メッセージの範囲を入力します。指定された個々の syslog メッセージまたは syslog メッセージの範囲に一致する syslog メッセージが発生すると、イベント マネージャ アプレットがトリガーされます。 （注） syslog メッセージ ID を 2 回入力したり、1 つのイベント マネージャ アプレット内で重複させることはできません。
発生回数	（任意）[発生回数（Occurrences）] フィールドに、イベント マネージャ アプレットを呼び出すために syslog メッセージが発生する必要がある回数を入力します。デフォルトの発生回数は 0 秒ごとに 1 回です。有効な値は、1 ～ 4294967295 です。
Period	（任意）[期間（Period）] フィールドに、アクションを呼び出すために syslog メッセージが発生しなければならない許容時間（秒数）を入力します。この値によって、イベント マネージャ アプレットが設定された期間に 1 回呼び出される際の最大の間隔が制限されます。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

アクション構成の追加および編集ダイアログボックス

[アクション設定の追加（Add Action Configuration）]および[アクション設定の編集（Edit Action Configuration）]ダイアログボックスを使用して、イベントマネージャアプレットのアクションを設定します。タイトルを除き、2つのダイアログボックスは同じです。次の情報が両方のダイアログボックスに適用されます。

ナビゲーション パス

[アクション設定の追加（Add Action Configuration）]および[アクション設定の編集（Edit Action Configuration）]ダイアログボックスには、[アプレットの追加（Add Applet）]および[アプレットの編集（Edit Applet）] ダイアログボックス （2640 ページ）からアクセスできます。

フィールド リファレンス

表 *666*：アクション構成の追加および編集ダイアログボックス

要素	説明
序数 ID（Ordinal ID）	[序数ID（Ordinal ID）]フィールドに一意のシーケンス番号を入力します。有効なシーケンス番号の範囲は 0 ～ 4294967295 です。アクション設定を追加する場合、デフォルトで、序数 ID は使用されている最大序数 ID より 1 つ大きくなります。
CLI	CLI コマンドを [CLI] フィールドに入力します。このコマンドは、特権レベル 15（最高）を持つユーザーとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。

[E-Mail Setup] ページ

[E-Mail Setup] ページ（PIX 7.0/ASA のみ）では、送信元電子メールアドレスと、電子メールとして送信する指定済み syslog メッセージの受信者のリストを設定します。宛先電子メール アドレスに送信される syslog メッセージを重大度でフィルタできます。テーブルには、どのエントリが設定されているかが表示されます。

宛先電子メール アドレスに使用される syslog 重大度フィルタは、このセクションで選択した重大度と [Logging Filters] ページですべての電子メール受信者に対して設定したグローバル フィルタのうち、より高い方になります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから**[プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslog]>[電子メールセットアップ（E-Mail Setup）]**を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）]>[ロギング（Logging）]>[Syslog]>[電子メールセット**

アップ（**E-Mail Setup**）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *667 : [E-Mail Setup]* ページ

要素	説明
Source Email Address	syslog が電子メールとして送信されるときに送信元アドレスとして使用される電子メール アドレスを入力します。
[Destination Address] テーブル	現在定義されている、syslog メッセージの電子メール受信者がリストされます。 [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、このリストを管理します。[Add Row] ボタンおよび [Edit Row] ボタンを使用すると、[Add Email Recipient]/[Edit Email Recipient] ダイアログボックス （2646 ページ）が開きます。

[Add Email Recipient]/[Edit Email Recipient] ダイアログボックス

[Add Email Recipient]/[Edit Email Recipient] ダイアログボックスでは、syslog メッセージを含む電子メールを送信する宛先アドレスを設定します。重大度に応じて送信するメッセージを制限できます。

宛先電子メール アドレスに使用される syslog 重大度フィルタは、このセクションで選択した重大度と [Logging Filters] ページ （2651 ページ）ですべての電子メール受信者に対して設定したグローバル フィルタのうち、より高い方になります。

ナビゲーション パス

[Add Email Recipient]/[Edit Email Recipient] ダイアログボックスには、[E-Mail Setup] ページ（2645 ページ）からアクセスできます。

フィールド リファレンス

表 *668 : [Add Email Recipient]/[Edit Email Recipient]* ダイアログボックス

要素	説明
Destination Email Address	選択したタイプの syslog メッセージの受信電子メール アドレスを入力します。

要素	説明
[Syslog Severity] リスト	この受信者に電子メールで送信する syslog の重大度を選択します。選択した重大度以上のメッセージが送信されます。メッセージの重大度レベルについては、ログ レベル （2667ページ）を参照してください。

[Event Lists] ページ

[Event Lists] ページ（PIX 7.0+/ASA のみ）では、ロギングに対する syslog メッセージ フィルタのセットを定義します。[Logging Setup] ページでロギングをイネーブルにし、グローバル ロギング パラメータを設定したあとで、このページを使用して、さまざまなロギング先に送信される syslog メッセージのフィルタに使用するイベント リストを設定します（[Logging Filters] ページ （2651 ページ）で、イベント リストのロギング先を指定します）。

[Event Lists] テーブルの下の [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、エントリを管理します。[Add Row] および [Edit Row] を使用すると、[Add Event List]/[Edit Event List] ダイアログボックス （2649 ページ）が開きます。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [イベント リスト（Event Lists）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [イベント リスト（Event Lists）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Logging Setup] ページ （2656 ページ）
- ロギング設定の設定 （2655 ページ）

セージ クラスおよび関連するメッセージ ID 番号

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *669* : セージ クラスおよび関連するメッセージ *ID* 番号

クラス	定義（Definition）	メッセージ ID 番号
auth	ユーザ認証	109、113

クラス	定義（Definition）	メッセージ ID 番号
ブリッジ	トランスペアレントファイアウォール	110、220
ca	PKI 証明機関	717
config	コマンド インターフェイス	111、112、208、308
電子メール（e-mail）	電子メール プロキシ	719
ha	フェールオーバー（ハイアベイラビリティ）	101、102、103、104、210、311、709
ids	侵入検知システム	400、401、415
ip	IP スタック	209、215、313、317、408
np	ネットワーク プロセッサ	319
ospf	OSPF ルーティング	318、409、503、613
rip	RIP ルーティング	107、312
rm	Resource Manager	321
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
webvpn	Web ベースの VPN	716

[Add Event List]/[Edit Event List] ダイアログボックス

[Add Event List]/[Edit Event List] ダイアログボックスでは、イベント リストを作成または編集し、イベント リスト フィルタに含める syslog メッセージを指定します。

次の基準を使用して、イベント リストを定義できます。

- クラスと重大度
- メッセージ ID

クラスは、関連する syslog メッセージの特定のタイプを表します。たとえば、クラス auth は、ユーザ認証に関連するすべての syslog メッセージを表します。

重大度は、ネットワークの通常機能におけるイベントの相対的な重要性に基づいて syslog を分類します。最も高い重大度は [緊急（Emergency）] で、利用可能なリソースがないことを意味します。最も低い重大度は [デバッグ（Debugging）] で、すべてのネットワーク イベントに関する詳細情報を提供します。

メッセージ ID は、個々のメッセージを一意に識別する数値です。単一のメッセージ ID または ID の範囲をイベント リストで指定できます。

ナビゲーション パス

[Add Event List]/[Edit Event List] ダイアログボックスには、[Event Lists] ページ （2647 ページ）からアクセスできます。

フィールド リファレンス

表 *670 : [Add Event List]/[Edit Event List]* ダイアログボックス

要素	説明
Event List Name	このイベント リストを一意に識別する名前を入力します。
Event Class/Severity Filters	このテーブルには、このイベント リストに対して定義されているイベント クラスと重大度レベル フィルタがリストされます。 エントリを管理するには、このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用します。[Add Row] および [Edit Row] を使用すると、[Add/Edit Syslog Class] ダイアログボックス （2650 ページ）が開きます。
Message ID Filters	このテーブルには、このイベント リストに対して定義されているメッセージ ID フィルタがリストされます。 エントリを管理するには、このテーブルの下にある [Add Row]、[Edit Row]、および [Delete Row] ボタンを使用します。[Add Row] および [Edit Row] を使用すると、[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス （2650 ページ）が開きます。

[Add/Edit Syslog Class] ダイアログボックス

[Add Syslog Class]/[Edit Syslog Class] ダイアログボックスでは、イベント クラスおよび関連する重大度レベルをイベント リスト フィルタとして指定します。

クラスによって、関連する特定のタイプの syslog メッセージが表されるため、syslog を個別に選択する必要はありません。たとえば、クラス auth は、ユーザ認証に関連するすべての syslog メッセージを表します。

重大度は、ネットワークの通常機能におけるイベントの相対的な重要性に基づいて syslog を分類します。最も高い重大度は [緊急（Emergency）] で、利用可能なリソースがないことを意味します。最も低い重大度は [デバッグ（Debugging）] で、すべてのネットワーク イベントに関する詳細情報を提供します。

ナビゲーション パス

[Add Syslog Class]/[Edit Syslog Class] ダイアログボックスには、[Add Event List]/[Edit Event List] ダイアログボックス （2649 ページ）からアクセスします。

関連項目

- [Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス （2650 ページ）
- [Event Lists] ページ （2647 ページ）

フィールド リファレンス

表 *671 : [Add/Edit Syslog Class]* ダイアログボックス

要素	説明
イベント クラス	目的のイベント クラスを選択します。イベント クラスについては、セージ クラスおよび関連するメッセージID番号 （2647ページ）を参照してください。
重大度	目的のメッセージ重大度レベルを選択します。重大度レベルについては、ログ レベル （2667 ページ）を参照してください。

[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックス

[Syslog メッセージ ID フィルタの追加（Add Syslog Message ID Filter）]/[Syslog メッセージ ID フィルタの編集（Edit Syslog Message ID Filter）] ダイアログボックスでは、Syslog メッセージ ID、または ID の範囲をイベントリストフィルタとして指定します。

ナビゲーション パス

[Add Syslog Message ID Filter]/[Edit Syslog Message ID Filter] ダイアログボックスには、[Add Event List]/[Edit Event List] ダイアログボックス （2649 ページ）からアクセスできます。

関連項目

- [Add/Edit Syslog Class] ダイアログボックス　（2650 ページ）
- [Event Lists] ページ　（2647 ページ）

フィールド リファレンス

[メッセージ ID（Message IDs）]：Syslog メッセージ ID または ID の範囲を入力します。範囲を指定するには、ハイフンを使用します（101001-101010 など）。メッセージ ID は、100000 ～ 999999 である必要があります。

メッセージ ID および対応するメッセージは、適切な製品の『System Log Message』ガイドにリストされています。これらのガイドには、cisco.com からアクセスできます。

PIX ファイアウォール

- http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html

ASA

- http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html

FWSM

- http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html

[Logging Filters] ページ

[Logging Filters] ページでは、[Event Lists] ページを使用して設定されているイベント リスト（syslog フィルタ）、または [Edit Logging Filters] ページを使用して指定する syslog メッセージだけのためのロギング先を設定します。特定のイベント クラスまたはすべてのイベント クラスからの syslog メッセージは、[Edit Logging Filters] ページを使用して選択できます。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング フィルタ（Logging Filters）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング フィルタ（Logging Filters）] を選択します。[ロギング フィルタ（Logging Filters）] を右クリックしてポリシーを作成するか、または共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- ロギング設定の設定　（2655 ページ）

- [Edit Logging Filters] ダイアログボックス （2653 ページ）

フィールド リファレンス

表 *672 : [Logging Filters]* ページ

要素	説明
Logging Destination	このフィルタに一致するメッセージが送信されるロギング先の名前がリストされます。ロギング先は次のとおりです。 • [内部バッファ（Internal Buffer）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスの内部バッファにパブリッシュされます。 • [コンソール（Console）]。このフィルタと一致するメッセージは、コンソール ポート接続にパブリッシュされます。 • [Telnetセッション（Telnet Sessions）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスに接続されている Telnet セッションにパブリッシュされます。 • [Syslogサーバー（Syslog Servers）]。このフィルタと一致するメッセージは、**[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog サーバー（Syslog Servers）]** ページで指定された syslog サーバーにパブリッシュされます。 • [電子メール（E-Mail）]。このフィルタと一致するメッセージは、**[プラットフォーム（Platform）] > [ロギング（Logging）] > [電子メール設定（E-mail Setup）]**（PIX7.0/ASA のみ）ページで指定された受信者にパブリッシュされます。 • [SNMPトラップ（SNMP Trap）]。このフィルタと一致するメッセージは、**[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP]** ページで指定された SNMP 管理ステーションにパブリッシュされます。 • [ASDM]。このフィルタと一致するメッセージは、いずれかの ASDM セッションにパブリッシュされます。
Syslogs From All Event Classes	フィルタする重大度、使用するイベント リスト、またはロギングがすべてのイベント クラスからディセーブルにされているかどうかがリストされます。イベント クラスについては、セージ クラスおよび関連するメッセージ ID 番号 （2647 ページ）を参照してください。
Syslogs From Specific Event Classes	フィルタとして設定されているイベント クラスと重大度がリストされます。イベント クラスについては、セージ クラスおよび関連するメッセージ ID 番号 （2647ページ）を参照してください。重大度レベルについては、ログ レベル （2667 ページ）を参照してください。

[Edit Logging Filters] ダイアログボックス

[Edit Logging Filters] ダイアログボックスでは、ロギング先のフィルタを編集します。syslog は、すべてまたは特定のイベント クラスから設定するか、特定のロギング先に対してディセーブルにできます。

ナビゲーション パス

[Edit Logging Filters] ダイアログボックスには [Logging Filters] ページからアクセスできます。[Logging Filters] ページの詳細については、[Logging Filters] ページ （2651 ページ）を参照してください。

関連項目

- ロギング設定の設定 （2655 ページ）
- [Logging Filters] ページ （2651 ページ）

フィールド リファレンス

表 673 : [Edit Logging Filters] ダイアログボックス

要素	説明
Logging Destination list	このフィルタのロギング先を指定します。 • [内部バッファ（Internal Buffer）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスの内部バッファにパブリッシュされます。 • [コンソール（Console）]。このフィルタと一致するメッセージは、コンソール ポート接続にパブリッシュされます。 • [Telnetセッション（Telnet Sessions）]。このフィルタと一致するメッセージは、セキュリティ アプライアンスに接続されている Telnet セッションにパブリッシュされます。 • [Syslogサーバー（Syslog Servers）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslogサーバー（Syslog Servers）] ページで指定された syslog サーバーにパブリッシュされます。 • [電子メール（E-Mail）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）]>[ロギング（Logging）]>[電子メール設定（E-mail Setup）]（PIX7.0/ASA のみ）ページで指定された受信者にパブリッシュされます。 • [SNMPトラップ（SNMP Trap）]。このフィルタと一致するメッセージは、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）]>[SNMP] ページで指定された SNMP 管理ステーションにパブリッシュされます。 • [ASDM]。このフィルタと一致するメッセージは、いずれかの ASDM セッションにパブリッシュされます。
Syslog from All Event Classes	
Filter on severity option	ロギング メッセージの重大度をフィルタします。
Filter on severity list	フィルタするロギング メッセージのレベルを指定します。
Use event list option	イベント リストを使用することを指定します。
Use event list	使用するイベント リストを指定します。イベント リストは [Event Lists] ページ （2647 ページ）で定義されています。
Disable logging option	選択した宛先へのすべてのロギングをディセーブルにします。

要素	説明
Syslog from Specific Event Classes (PIX7.0)	
イベント クラス	イベント クラスと重大度を指定します。イベント クラスには、1 つまたはすべての使用可能なアイテムが含まれます。イベント クラスについては、セージ クラスおよび関連するメッセージ ID 番号 （2647 ページ）を参照してください。
重大度	ロギング メッセージのレベルを指定します。重大度レベルについては、ログ レベル （2667 ページ）を参照してください。

ロギング設定の設定

[Logging Setup] ページでは、セキュリティ アプライアンスでのシステム ロギングをイネーブルにしたり、他のロギング オプションを設定したりできます。これらのオプションには、セキュリティ アプライアンスおよびフェールオーバー装置に関するロギングのイネーブル化、基本的なログ フォーマットと詳細、および内部バッファをパージする前の長期保管デバイス、FTP サーバ、またはフラッシュへのロギングが含まれます。

関連項目

- [Logging Setup] ページ （2656 ページ）

ステップ 1 [プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslog]>[ロギングの設定（Logging Setup）] を選択して、[ロギングの設定（Logging Setup）] ページを表示します。

ステップ 2 [ロギングの有効化（Enable Logging）] をオンにします。

このオプションは、セキュリティ アプライアンスでのロギングをイネーブルにします。

ステップ 3 このセキュリティアプライアンスとペアになっているフェールオーバー装置上でロギングをイネーブルにするには、[スタンバイフェールオーバー装置でのロギングを有効にする（Enable logging on the standby failover unit）] チェックボックスをオンにします。

ステップ 4 EMBLEM フォーマットをイネーブルにするには、またはデバッグ メッセージを syslog メッセージの一部として送信するには、対応するチェックボックスをオンにします。

EMBLEM をイネーブルにする場合は、UDP プロトコルを使用して syslog メッセージをパブリッシュする必要があります。TCP とは互換性がありません。

ステップ 5 内部バッファをクリアする前に、あとで処理するために内部バッファ データを FTP サーバに書き込むには、次の手順を実行します。

a) [FTPサーバーバッファラップ（FTP Server Buffer wrap）] をオンにします。
b) FTP サーバーの IP アドレスを [IPアドレス（IP Address）] フィールドに入力します。
c) FTP サーバーへのログインに使用するアカウントのユーザー名を [ユーザー名（User Name）] フィールドに入力します。

d) ファイルを保存するパスを、FTP ルートに関連した [パス（Path）] フィールドに入力します。
e) ユーザ名の認証に使用されるパスワードを入力および確認します。

ステップ 6 内部バッファをクリアする前に、あとで処理するために内部バッファ データをフラッシュに書き込むには、次の手順を実行します。

a) [フラッシュ（Flash）] をオンにします。
b) 内部バッファ データのストレージに割り当てる最大メモリ量を指定します。
c) フラッシュ ドライブに残す必要のある最小空きメモリを指定します。内部バッファからのデータを書き込むとき、この最小値を維持できないと、容量要件を満たすためにメッセージが切り詰められます。

ステップ 7 ASDM クライアントで表示するためにアプライアンス上に維持する最大キューサイズを指定するには、[メッセージキューのサイズ（メッセージ数）（Message Queue Size (Messages)）] フィールドにその値を入力します。

[Logging Setup] ページ

[Logging Setup] ページでは、セキュリティ アプライアンスでのシステム ロギングをイネーブルにしたり、他のロギング オプションを設定したりできます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング設定（Logging Setup）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング設定（Logging Setup）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 674 : [Logging Setup] ページ

要素	説明
Enable Logging	メイン セキュリティ アプライアンスのロギングをオンにします。
Enable Logging on the Failover Standby Unit	スタンバイ セキュリティ アプライアンスが使用可能な場合は、そのロギングをオンにします。

要素	説明
Send syslogs in EMBLEM format（PIX7.x+、ASA、FWSM 3.x+）	すべてのロギング先に対する EMBLEM フォーマット ロギングをイネーブルにします。EMBLEM を有効にする場合は、UDP プロトコルを使用して syslog メッセージをパブリッシュする必要があります。EMBLEM は TCP と互換性がありません。 （注） この設定は、CS-MARS と互換性がありません。
Send debug messages as syslogs（PIX7.x+、ASA、FWSM 3.x+）	すべてのデバッグ トレース出力を syslog にリダイレクトします。このオプションが有効になっている場合、syslog メッセージはコンソールに表示されません。したがって、デバッグ メッセージを表示するには、コンソールでロギングを有効にし、デバッグ syslog メッセージ番号とログ レベルの宛先として設定する必要があります。使用される syslog メッセージ番号は 711011 です。この syslog のデフォルトロギングレベルは [デバッグ（debug）] です。
Memory Size of Internal Buffer (bytes)	ロギング バッファがイネーブルになっている場合に syslog が保存される内部バッファのサイズを指定します。バッファが一杯になった場合は上書きされます。デフォルトは 4096 バイトです。有効な範囲は 4096 ～ 1048576 です。
Specify FTP Server Information（PIX7.x+、ASA、FWSM 3.x+）	
FTP Server Buffer Wrap	バッファの内容を上書きする前に FTP サーバに保存するには、このボックスをオンにし、次のフィールドに必要な宛先情報を入力します。FTP 設定を削除するには、このオプションを選択解除します。
IPアドレス	FTP サーバの IP アドレスを入力します。
ユーザー名	FTP サーバに接続するときに使用するユーザ名を入力します。
パス（Path）	バッファの内容を保存するパスを FTP ルートからの相対で入力します。
Password/Confirm	FTP サーバへのユーザ名の認証に使用されるパスワードを入力および確認します。
Specify flash size	
フラッシュ	バッファの内容を上書きする前にフラッシュ メモリに保存するには、このチェックボックスをオンにします。このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。

要素	説明
Maximum flash to be used by logging (KB)	ロギング用のフラッシュ メモリで使用する最大容量を指定します（KB 単位）。このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。
Minimum free space to be preserved (KB)	フラッシュ メモリに保持する最小空き容量を指定します（KB 単位）。このオプションは、ルーテッドまたはトランスペアレント シングル モードだけで使用できます。
ASDM Logging（PIX7.x+、ASA、FWSM 3.x+）	
Message Queue Size	ASDM で表示する syslog のキュー サイズを指定します。

レート制限レベルの設定

[レート制限（Rate Limit）]ページでは、特定のタイプ（「アラート」または「クリティカル」）のログメッセージの最大数、および特定の期間内に生成できる特定の Syslog ID のメッセージを指定します。ロギング レベルごと、および Syslog メッセージ ID ごとに個別の制限を指定できます。設定が競合する場合は、Syslog メッセージ ID の制限が優先されます。

特定の期間内の特定の Syslog メッセージ ID に対して生成できるメッセージの最大数を指定するには、[Add/Edit Rate Limited Syslog Message] ダイアログボックス （2661 ページ）を使用します。

特定の期間内の特定の Syslog ロギング レベルに対して生成できるメッセージの最大数を指定するには、[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （2660 ページ）を使用します。

関連項目

- [Rate Limit] ページ （2659 ページ）

次の手順に従って、メッセージ ロギングのレート制限を管理します。

ステップ 1 [Rate Limit] ページにアクセスするには、次のいずれかを実行します。

- （デバイス ビュー）デバイス ポリシー セレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 Syslog ロギング レベルのレート制限を追加、編集、および削除します。

- 一定の期間内に特定のロギング レベルに対して生成できるメッセージの最大数を指定するには、[Syslog ロギング レベルのレート制限（Rate Limits for Syslog Logging Levels）] テーブルの下にある [行の追加

（Add Row）] ボタンをクリックして、[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （2660 ページ）を開きます。ロギング レベルを選択し、レート制限を定義します。

- 特定のロギングレベルのレート制限を編集するには、[Syslogロギングレベルのレート制限（Rate Limits for Syslog Logging Levels）] テーブルの適切なエントリを選択し、テーブルの下にある [行の編集（Edit Row）] ボタンをクリックして、[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス（2660 ページ）を開きます。必要に応じてレート制限を変更します。
- [Syslogロギングレベルのレート制限（Rate Limits for Syslog Logging Levels）] テーブルからレート制限エントリを削除するには、そのエントリを選択し、テーブルの下にある [行の削除（Delete Row）] ボタンをクリックします。確認ダイアログボックスが表示される場合があります。[OK] をクリックしてエントリを削除します。

ステップ 3 メッセージ ID に従ってログ メッセージの制限を追加、編集、および削除します。

- 特定の期間内に特定メッセージ ID に対して生成できるメッセージの最大数を指定するには、[個別にレート制限されたSyslogメッセージ（Individually Rate Limited Syslog Messages）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックして、[Add/Edit Rate Limited Syslog Message] ダイアログボックス （2661 ページ）を開きます。Syslog メッセージ ID を選択し、レート制限を定義します。
- 特定の Syslog メッセージ ID のレート制限を編集するには、[個別にレート制限されたSyslogメッセージ（Individually Rate Limited Syslog Messages）] テーブルの適切なエントリを選択し、テーブルの下にある [Edit Row] ボタンをクリックして、[Add/Edit Rate Limited Syslog Message] ダイアログボックス（2661 ページ）を開きます。必要に応じてレート制限を変更します。
- [個別にレート制限されたSyslogメッセージ（Individually Rate Limited Syslog Messages）] テーブルからメッセージ制限エントリを削除するには、そのエントリを選択し、テーブルの下にある [行の削除（Delete Row）] ボタンをクリックします。確認ダイアログボックスが表示される場合があります。[OK] をクリックしてエントリを削除します。

[Rate Limit] ページ

[Rate Limit] ページでは、特定の期間内に生成する必要のある特定のタイプ（たとえば、アラートやクリティカル）のログ メッセージの最大数を指定できます。ロギング レベルごと、および Syslog メッセージ ID ごとに制限を指定できます。設定が異なる場合は、Syslog メッセージ ID の制限が優先されます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [レート制限（Rate Limit）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- ロギング設定の設定　（2655 ページ）
- [Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス　（2660 ページ）
- [Add/Edit Rate Limited Syslog Message] ダイアログボックス　（2661 ページ）

フィールド リファレンス

表 675 : [Rate Limit] ページ

要素	説明
[Rate Limits for Syslog Logging Levels] テーブル	
ログ レベル（Logging Level）	レート制限を指定する Syslog ロギング レベル。
No. of Messages	指定された時間に送信できる、指定されたタイプのメッセージの最大数。
Interval (seconds)	レート制限カウンタがリセットされるまでの秒数。
[Individually Rate Limited Syslog Messages] テーブル	
syslog ID	レート制限を指定する Syslog メッセージの識別番号。
No. of Messages	指定された時間に送信できる、指定された ID を持つメッセージの最大数。
Interval (seconds)	レート制限カウンタがリセットされるまでの秒数。

[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス

[Add Rate Limit for Syslog Logging Levels]/[Edit Rate Limit for Syslog Logging Levels] ダイアログボックスを使用して、特定の期間内に生成する必要のある特定のログ レベルのログ メッセージの最大数を指定できます。ロギング レベルごと、または syslog メッセージ ID ごとに制限を指定できます（[Add/Edit Rate Limited Syslog Message] ダイアログボックス　（2661 ページ）を参照）。設定が異なる場合、レート制限された syslog メッセージレベルの設定がレート制限のロギング レベルの設定を上書きします。

ナビゲーション パス

[Add Rate Limit for Syslog Logging Levels]/[Edit Rate Limit for Syslog Logging Levels] ダイアログボックスには、[Rate Limit] ページからアクセスできます。詳細については、[Rate Limit] ページ　（2659 ページ）を参照してください。

関連項目

- ロギング設定の設定　（2655 ページ）

- [Add/Edit Rate Limited Syslog Message] ダイアログボックス （2661 ページ）
- [Rate Limit] ページ （2659 ページ）

フィールド リファレンス

表 676 : [Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス

要素	説明
ログ レベル（Logging Level）	レート制限を指定する syslog ロギング レベル。
メッセージ数（Number of Messages）	指定された時間に送信できる、指定されたタイプのメッセージの最大数。
間隔（秒）	レート制限カウンタがリセットされるまでの秒数。

[Add/Edit Rate Limited Syslog Message] ダイアログボックス

[Add Rate Limited Syslog Message]/[Edit Rate Limited Syslog Message] ダイアログボックスを使用して、特定の期間内に生成できる特定の Syslog ID のログ メッセージの最大数を指定できます。syslog メッセージ ID ごと、またはロギング レベルごとに制限を指定できます（[Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （2660 ページ）を参照）。設定が異なる場合、レート制限された syslog メッセージレベルの設定がレート制限のロギング レベルの設定を上書きします。

ナビゲーション パス

[Add Rate Limited Syslog Message]/[Edit Rate Limited Syslog Message] ダイアログボックスには、[Rate Limit] ページからアクセスできます。詳細については、[Rate Limit] ページ （2659 ページ）を参照してください。

関連項目

- ロギング設定の設定 （2655 ページ）
- [Rate Limit] ページ （2659 ページ）
- [Add/Edit Rate Limit for Syslog Logging Levels] ダイアログボックス （2660 ページ）

フィールド リファレンス

表 677 : [Add/Edit Rate Limited Syslog Message] ダイアログボックス

要素	説明
syslog ID	レート制限を指定する syslog メッセージの識別番号。

要素	説明
メッセージ数（Number of Messages）	指定された時間に送信できる、指定された ID を持つメッセージの最大数。
間隔（秒）	レート制限カウンタがリセットされるまでの秒数。

Syslog サーバ設定の設定

一般的な Syslog サーバ設定を設定して、Syslog サーバに送信される Syslog メッセージに含めるファシリティ コードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

関連項目

- Syslog サーバの定義 （2669 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）**[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）]** を選択して、[Server Setup] ページ （2664 ページ）を開きます。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [電子メールセットアップ（E-Mail Setup）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ステップ 2 必要に応じて基本的なメッセージ設定を変更します。

- syslog サーバーでデフォルトとは異なるファシリティが必要な場合は、[ファシリティ（Facility）] リストで必要なファシリティを選択します。
- メッセージが生成された日時をメッセージに含める場合は、[タイムスタンプを各 Syslog メッセージで有効にする（Enable Timestamp on Each Syslog Message）] を選択します。
  - ロギングタイムスタンプを rfc5424 形式で設定する場合は、[タイムスタンプ形式の有効化（rfc5424）（Enable Timestamp Format(rfc5424)）] を選択します。このオプションは、ASA 9.12.1 デバイス以降に適用されます。タイムスタンプの出力例：

例：

```
2003-08-24T05:14:15.000003-07:00
```

- デバイス識別子を syslog メッセージに追加する場合は（これはメッセージの先頭に配置されます）、[Syslogデバイス IDを有効にする（Enable Syslog Device ID）] を選択し、ID のタイプを選択します。

（注） ASA クラスタの場合、クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタブートストラップ設定で割り当てられたローカルユニット名をデバイス ID（クラスタ ID オプション） として使用するようにロギングを設定した場合は、syslog メッセージはそれぞれ別のユニットからのように見えます。コントロールユニットのインターフェイス IP アドレスをすべてのクラスタデバイスに使用するかどうかも指定できます。

- [インターフェイス（Interface）]：アプライアンスがメッセージの送信に使用するインターフェイスに関係なく、指定されたインターフェイスの IP アドレスを使用します。[選択（Select）] をクリックして、インターフェイスを識別するインターフェイスまたはインターフェイス ロールを選択します。インターフェイス ロールは、単一のインターフェイスにマッピングされる必要があります。

ASA クラスタの場合、コントロールユニットのインターフェイス IP アドレスをすべてのクラスタデバイスに使用するように指定するには、[インターフェイス名（Interface Name）] フィールドで対応するオプションを選択します。

- [ユーザ定義ID（User Defined ID）]：選択したテキスト文字列を使用します（最大 16 文字）。
- [ホスト名（Host Name）]：デバイスのホスト名を使用します。
- [クラスタID（Cluster ID）]：デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

ステップ 3 [Syslog Message] テーブルを使用して、特定の Syslog メッセージのデフォルト設定を変更します。デフォルト設定を変更する場合にだけ、このテーブルでルールを設定する必要があります。メッセージに割り当てられている重大度を変更したり、メッセージが生成されてないように（ディセーブル化）したりできます。

- ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add/Edit Syslog Message] ダイアログボックス （2668 ページ）に入力します。

設定を変更するメッセージ番号を選択してから、新しいシビラティ（重大度）レベルを選択するか、[抑制（Suppressed）] を選択してメッセージの生成をディセーブルにします。通常は、重大度レベルの変更やメッセージのディセーブル化は行いませんが、必要に応じて両方のフィールドを変更できます。[OK] をクリックしてテーブルにルールを追加します。

メッセージ重大度レベルの詳細については、ログ レベル （2667 ページ）を参照してください。

- ルールを編集するには、ルールを選択して [行の編集（Edit Row）] ボタンをクリックし、目的の変更を加えて [OK] をクリックします。
- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）] ボタンをクリックします。
- NetFlow を使用している場合は、[NetFlowと同等のsyslogを無効化（Disable NetFlow Equivalent Syslogs）] ボタンをクリックして、NetFlow と同等の syslog メッセージの生成を簡単にディセーブルにできます。

これにより、メッセージが抑止されたメッセージとしてテーブルに追加されます。これらの同等の syslog メッセージがすでにテーブルにある場合、既存のルールは上書きされません。

Syslog リレー構成

Cisco Security Manager サーバーで受信したイベントに加えて、最大 2 台の外部/リモートコントローラ（syslog ホスト）にイベントを転送できます。syslog リレーは、UDP syslog プロトコルを使用して受信したメッセージを別の syslog ホストに転送します。

Cisco Security Manager サーバーから転送された syslog メッセージに、syslog メッセージの送信元 IP アドレスとして Cisco Security Manager サーバーの IP アドレスを含めるには、CLI コマンドでそのアドレスを有効にする必要があります。

1. CSCOpx\MDC\logrelay に移動し、logrelay.properties ファイルを開きます。
2. 次のように、ext1 と ext2 の値を false に設定します。

```
## Source Preservation
#logrelay.dp.txring.ext0.preserve.source=true logrelay.dp.txring.ext1.preserve.source=false
logrelay.dp.txring.ext2.preserve.source=false
```

（注） デフォルトでは、ext1 と ext2 を false に設定することにより、値はすべてのコレクタに対して true になります。Cisco Security Manager は、Cisco Security Manager IP を使用して syslog メッセージを送信します。この変更は、リモートコレクタに対してのみ実行でき、ローカルコレクタ（ext0）に対しては実行できません。

[Server Setup] ページ

[Server Setup] ページでは、syslog サーバに送信される syslog メッセージに含めるファシリティコードの設定、各メッセージにタイムスタンプが含まれるかどうかの指定、メッセージに含めるデバイス ID の指定、メッセージの重大度レベルの表示と変更、および特定のメッセージの生成のディセーブル化を行うことができます。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [サーバー設定（Server Setup）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- Syslog サーバ設定の設定 （2662 ページ）
- Syslog サーバの定義 （2669 ページ）
- ロギング設定の設定 （2655 ページ）
- ログ レベル （2667 ページ）

フィールド リファレンス

表 *678 : [Server Setup]* ページ

要素	説明
Facility	アプライアンスが syslog サーバで定義されているメッセージに含める syslog ファシリティ コード。デフォルトは LOCAL4(20) です。これは UNIX システムで最も可能性の高いコードです。LOCAL0(16) ～ LOCAL7(23) のファシリティを選択できます。 Syslog ファシリティは、syslog データ ストリームを生成する各種ネットワーク デバイスを識別する必要のある集中 syslog モニタリング システムがある場合に役立ちます。ネットワーク デバイスは使用可能な 8 つのファシリティを共有するため、この値の変更が必要な場合があります。
Enable Timestamp on Each Syslog Message	メッセージが生成された日時を syslog メッセージに含めるかどうか。デフォルトでは、タイム スタンプは含められません。

要素	説明
Enable Syslog Device ID	EMBLEM 以外のフォーマットの syslog メッセージでデバイス ID を設定するかどうか。このオプションをオンにした場合は、次のいずれかをデバイス ID として使用することを選択します。これはすべての syslog メッセージの先頭に配置されます。 （注） ASA クラスタの場合、クラスタの各ユニットは自身の syslog メッセージを生成します。各ユニットの syslog メッセージ ヘッダー フィールドで使用されるデバイス ID を同一にするか、別にするかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのユニットに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合は、どのユニットで生成された syslog メッセージも 1 つのユニットからのように見えます。クラスタブートストラップ設定で割り当てられたローカルユニット名をデバイス ID（クラスタ ID オプション） として使用するようにロギングを設定した場合は、syslogメッセージはそれぞれ別のユニットからのように見えます。コントロールユニットのインターフェイス IP アドレスをすべてのクラスタデバイスに使用するかどうかも指定できます。 • [Interface]：選択したインターフェイスの IP アドレス。インターフェイスの名前を入力するか、あるいは [選択（Select）] をクリックしてリストから選択します（またはインターフェイスを指定するインターフェイスロールを選択します）。適応型セキュリティ アプライアンスが外部サーバへのログ データの送信に使用するインターフェイスに関係なく、メッセージには、指定したインターフェイスの IP アドレスが含まれます。 インターフェイス ロールを選択する場合、そのロールはデバイス上の単一インターフェイスにマッピングされる必要があります。 ASA クラスタの場合、コントロールユニットのインターフェイス IP アドレスをすべてのクラスタデバイスに使用するように指定するには、[インターフェイス名（Interface Name）] フィールドで対応するオプションを選択します。 • [User Defined ID]：デバイス ID として定義するテキスト文字列。この文字列は最大 16 文字にできますが、次の特殊文字を含めることはできません。 & ’ " < > ? • [Host Name]：セキュリティ アプライアンスのホスト名。 • [Cluster ID]：デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。

要素	説明
[Syslog Message] テーブル	このテーブルを使用して、特定の syslog メッセージの生成をイネーブルまたはディセーブルにしたり、メッセージの重大度レベルを変更したりします。生成されるメッセージ タイプが競合しないようにする場合、またはメッセージの重大度レベルを変更する場合は、このテーブルで何も設定する必要はありません。テーブルには、メッセージレベルを設定したメッセージ、および生成が抑止されているかどうか（テーブルの [true]）が表示されます。 • ルールを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add/Edit Syslog Message] ダイアログボックス （2668 ページ）に入力します。 • ルールを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • ルールを削除するには、ルールを選択し、[Delete Row] ボタンをクリックします。
[Disable NetFlow Equivalent Syslogs]/[Enable NetFlow Equivalent Syslogs]	NetFlow ロギングを使用している場合は、NetFlow メッセージと重複する syslog メッセージの生成をディセーブルにできます。[Disable] ボタンをクリックした場合、これらの重複する syslog メッセージが [Syslog Message] テーブルに抑止されたメッセージとして追加され、ボタンの名前が [Enable NetFlow Equivalent Syslogs] に変更されます。 [Enable] ボタンをクリックすると、重複する syslog メッセージがテーブルから削除され、抑止されなくなり、デバイスはこれらのメッセージの送信を再開します。ただし、[Disable] ボタンでリストに追加されたメッセージを手動で編集した場合、そのメッセージは [Enable] ボタンで削除されません。

ログ レベル

次の表で、ロギング レベルについて説明します。

表 *679* : ログ レベル

ログ レベル（**Logging Level**）	タイプ	説明
[0]	Emergency	システムが使用不能です。システムが不安定であることを示すメッセージを生成します。
1	アラート	即時のアクションが必要です。即時の管理アクションを必要とするシステム整合性の問題を示すメッセージを生成します。
2	クリティカル	危険な状態です。クリティカルなシステムの問題を示すメッセージを生成します。

ログ レベル（Logging Level）	タイプ	説明
3	エラー	エラー条件。操作中のシステム エラーを示すメッセージを生成します。
4	警告	警告条件。システム警告を示すメッセージを生成します。たとえば、デバイスが正しく設定されていない可能性があります。
5	通知	正常だが注意を要する状態。通常は重大なイベントと見なされる正常な操作を示すメッセージを生成します。
6	Information	情報のみ。ネットワーク セッション レコードなど、通常の日常的なアクティビティであるシステム情報を示すメッセージを生成します。
7	Debugging	デバッグに役立つ syslog メッセージを生成します。また、FTP セッション中に発行されたコマンドおよび HTTP セッション中に要求された URL を示すログも生成します。すべての緊急事態、アラート、クリティカル、エラー、警告、通知、および情報メッセージを含みます。
-	無効	ロギングを行いません。

[Add/Edit Syslog Message] ダイアログボックス

[Add Syslog Message]/[Edit Syslog Message] ダイアログボックスでは、syslog メッセージのロギング レベルまたは抑止設定を変更します。

ナビゲーション パス

[Add Syslog Message]/[Edit Syslog Message] ダイアログボックスには、[Server Setup] ページ （2664 ページ）からアクセスできます。

フィールド リファレンス

表 *680 : [Add/Edit Syslog Message]* ダイアログボックス

要素	説明
Syslog ID list	重大度レベルまたは抑止設定を変更するメッセージのメッセージ ログ ID。これらの値および対応するメッセージは、適切な製品の『System Log Message』ガイドに示されています。 **PIX ファイアウォール** http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_system_message_guides_list.html **ASA** http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html **FWSM** http://www.cisco.com/en/US/products/hw/modules/ps2706/ps4452/tsd_products_support_model_home.html （注） Cisco Security Manager 4.10 以降では、[Syslog ID] フィールドに syslog メッセージを入力できます。デバイスに対応する有効な syslog ID を入力してください。そうしないと、展開が失敗する可能性があります。
Logging Level list	メッセージに割り当てるロギング レベル。ロギング レベルと説明については、ログ レベル （2667 ページ）を参照してください。 メッセージに割り当てるデフォルト レベルの使用を選択します（デフォルト）。
Suppressed	syslog メッセージの生成を抑止するかどうか。メッセージを抑止するとその生成がディセーブルになり、syslogs に表示されなくなります。
スタンバイでの Syslog の無効化（Disable Syslogs on Standby）	特定の syslog メッセージがスタンバイ ASA デバイスで生成されないようにするかどうか。この機能は ASA バージョン 9.4(1) から利用でき、Security Manager はバージョン 4.9 からこの機能をサポートします。

Syslog サーバの定義

[Syslog Servers] ページでは、セキュリティ アプライアンスが syslog メッセージを送信する syslog サーバを指定します。定義した syslog サーバを利用するには、[Logging Setup] ページを使用してロギングをイネーブルにし、[Logging Filters] ページを使用して宛先に適切なフィルタを設定する必要があります。

ヒント Security Manager Event Viewer を使用して ASA デバイスからイベントを表示する場合は、Security Manager サーバが syslog サーバとして定義されていることを確認してください。CS-MARS またはその他のアプリケーションを使用して syslog イベントを管理する場合はそれらのサーバをこのポリシーに含めてください。

セキュリティ アプライアンスで生成される syslog レコードを指示することで、レコードを処理および調査できます。

はじめる前に

ロギングをイネーブルにします。ロギング設定の設定 （2655 ページ） を参照してください。

関連項目

- [Syslog Servers] ページ （2671 ページ）
- [Add/Edit Syslog Server] ダイアログボックス （2672 ページ）

ステップ 1 Select **Platform** > **Logging** > **Syslog** > **Syslog Servers** to display the Syslog Servers page.

ステップ 2 次のいずれかを実行します。

- 新しい syslog ターゲットを追加するには、[行の追加（Add Row）] ボタンをクリックします。
- 既存の syslog ターゲットを編集するには、その行のチェックボックスをオンにし、[行の編集（Edit Row）] ボタンをクリックします。

ステップ 3 [インタフェース（Interface）] フィールドで、インターフェイス名を入力または選択します。

リストには、現在のスコープに定義されているすべてのインターフェイスが表示されます。

ステップ 4 syslog サーバーの IP アドレスを [IPアドレス（IP Address）] フィールドで入力または選択します。

ステップ 5 UDP と TCP のいずれを使用するかを決定し、[Protocol] の下の適切なオプション ボタンをクリックします。

ステップ 6 セキュリティ アプライアンスが UDP または TCP syslog メッセージを送信するポートを入力します。ポートは、syslog サーバが受信するポートと同じである必要があります。

- TCP：1470（デフォルト）。TCP ポートは、セキュリティ アプライアンスの syslog サーバとだけ連携します。
- UDP：514（デフォルト）。

ステップ 7 EMBLEM フォーマットを使用して syslog メッセージを生成するには、[Cisco EMBLEMフォーマットのログメッセージ（Log messages in Cisco EMBLEM format）] チェックボックスをオンにします。

このオプションをイネーブルにするには、UDP プロトコルを選択してメッセージをこの syslog サーバにパブリッシュする必要があります。

ステップ 8 [OK] をクリック

定義が [Syslog Servers] テーブルに表示されます。

[Syslog Servers] ページ

[Syslog Servers] ページでは、セキュリティアプライアンスが syslog メッセージを送信する syslog サーバを指定します。定義した syslog サーバを利用するには、[Logging Setup] ページを使用してロギングをイネーブルにし、[Logging Filters] ページを使用して宛先に適切なフィルタを設定する必要があります。

ヒント　Security Manager Event Viewer を使用して ASA デバイスからイベントを表示する場合は、Security Manager サーバが syslog サーバとして定義されていることを確認してください。CS-MARS またはその他のアプリケーションを使用して syslog イベントを管理する場合はそれらのサーバをこのポリシーに含めてください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [Syslogサーバー（Syslog Servers）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ロギング（Logging）] > [Syslog] > [Syslogサーバー（Syslog Servers）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- Syslog サーバの定義　（2669 ページ）
- ロギング設定の設定　（2655 ページ）

フィールド リファレンス

表 681 : [Syslog Servers] ページ

要素	説明
[Syslog Servers] テーブル	このデバイスが syslog メッセージを送信する syslog サーバ。テーブルには、サーバーにメッセージをパブリッシュするデバイスインターフェイス、サーバーの IP アドレス、syslog プロトコルとポート番号、およびメッセージが Cisco EMBLEM syslog フォーマットかどうかが表示されます。 コンテキストごとに設定できる syslog サーバは 4 つに制限されています。 • サーバーを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Add/Edit Syslog Server] ダイアログボックス （2672 ページ）に入力します。 • サーバーを編集するには、サーバーを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • サーバーを削除するには、サーバーを選択し、[行の削除（Delete Row）] ボタンをクリックします。
キュー サイズ	syslog サーバがビジーな場合にセキュリティ アプライアンスに syslog メッセージを格納するためのキューのサイズを指定します。最小は 1 メッセージです。デフォルトは 512 です。無制限の数のメッセージをキューに入れる場合は、0 を指定します（使用可能なブロック メモリによって制限されます）。
Allow user traffic to pass when TCP syslog server is down	TCP プロトコルを使用している syslog サーバがダウンした場合にすべてのトラフィックを制限するかどうか。

[Add/Edit Syslog Server] ダイアログボックス

[Add Syslog Servers]/[Edit Syslog Servers] ダイアログボックスでは、セキュリティ アプライアンスが syslog メッセージを送信する syslog サーバを追加または編集します。定義した syslog サーバを利用するには、[Logging Setup] ページを使用してロギングをイネーブルにし、[Logging Filters] ページを使用して宛先に適切なフィルタを設定する必要があります。

（注） コンテキストごとに設定できる syslog サーバは 4 つに制限されています。

ナビゲーション パス

[Add Syslog Servers] ダイアログボックスには、[Syslog Servers] ページからアクセスできます。[Syslog Servers] ページの詳細については、[Syslog Servers] ページ （2671 ページ）を参照してください。

関連項目

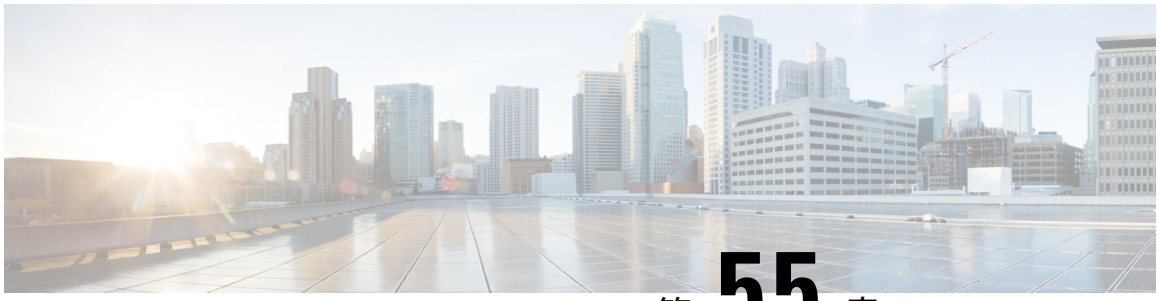
- Syslog サーバの定義 （2669 ページ）
- ロギング設定の設定 （2655 ページ）

フィールド リファレンス

表 *682 : [Add/Edit Syslog Server]* ダイアログボックス

要素	説明
インターフェイス（Interface）	syslog サーバとの通信に使用するインターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、または [選択（Select）] をクリックして、リストからオブジェクトを選択するか、新しいオブジェクトを作成します。
IPアドレス	syslog サーバの IP アドレス。アドレスを定義するネットワーク/ホストポリシーオブジェクトの IP アドレスまたは名前を入力するか、[選択（Select）] をクリックしてネットワーク/ホストオブジェクトを選択します。 （注） Cisco Security Manager 4.13 以降、syslog サーバーで IPv6 アドレスがサポートされています。
プロトコル	syslog サーバで使用されるプロトコル（TCP または UDP）。UDP がデフォルトです。TCP ポートは、セキュリティ アプライアンスの syslog サーバとだけ連携します。 （注） EMBLEM フォーマットを使用する場合は、UDP を選択する必要があります。

要素	説明
[ポート（Port）]	セキュリティ アプライアンスが syslog メッセージを送信し、syslog サーバがそれらのメッセージを受信する TCP または UDP ポート。各プロトコルのデフォルト ポートは次のとおりです。 • TCP：1470 • UDP：514 ヒント Security Manager サーバを syslog サーバとして定義している場合は、Security Manager Administration の [Event Management] ページ （677 ページ）にポート番号が表示されます。 （注） Security Manager のインストールまたはアップグレード時に、Common Services syslog サービス ポートが 514 から 49514 に変更されます。あとで Security Manager がアンインストールされた場合、ポートは 514 に戻されません。
Log messages in Cisco EMBLEM format（UDP のみ）	メッセージを Cisco EMBLEM フォーマットでロギングするかどうか。syslog サーバでは UDP を使用する必要があります。 （注） syslog サーバが Cisco Security MARS アプライアンスの場合は、このオプションを選択しないでください。Cisco Security MARS では、EMBLEM フォーマットが処理されません。
参照ID（Reference Identity）	バージョン 4.12 以降、Cisco Security Manager を使用すると、ポリシーオブジェクト セレクタから参照 ID ポリシーオブジェクト名を選択できます。 参照 ID は、ポートが TCP の場合にのみ有効になり、ポートが UDP の場合は無効になります。 詳細については、 参照 ID （2514 ページ）を参照してください。



第 55 章

ファイアウォールデバイスでのマルチキャスト ポリシーの設定

マルチキャストのセクションには、セキュリティ デバイスに IP マルチキャスト ルーティングを定義するためのページが含まれています。マルチキャスト ルーティングは、シングルコンテキストのルーテッド モードでだけサポートされます。

マルチキャスト ルーティングがイネーブルになれば、デフォルトですべてのインターフェイス上の IGMP と PIM がイネーブルになります。インターネット グループ管理プロトコル（IGMP）は、直接接続されたサブネットにグループのメンバーが存在するかどうかを学習するために使用します。ホストは、IGMP レポート メッセージを送信することにより、マルチキャスト グループに参加します。Protocol Independent Multicast（PIM）は、マルチキャスト データグラムの転送テーブルを維持するために使用します。

（注） マルチキャスト ルーティングでは、UDP トランスポート レイヤだけがサポートされています。

この章は次のトピックで構成されています。

- PIM および IGMP のイネーブル化 （2675 ページ）
- IGMP の設定 （2676 ページ）
- マルチキャスト ルートの設定 （2684 ページ）
- マルチキャスト境界フィルタの設定 （2686 ページ）
- PIM の設定 （2688 ページ）

PIM および IGMP のイネーブル化

[Enable PIM and IGMP] ページを使用すると、セキュリティ アプライアンスのすべてのインターフェイスでインターネット グループ管理プロトコル（IGMP）および Protocol Independent Multicast（PIM）をイネーブルまたはディセーブルにできます。IGMP は、直接接続されているサブネット上にグループのメンバーが存在するかどうか学習するために使用されます。ホストは、IGMP

レポート メッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

このページで [PIM と IGM のイネーブル化（PEnable PIM and IGMP）] をオンにすると、セキュリティ アプライアンスのすべてのインターフェイスで PIM および IGMP がイネーブルになります。このオプションをオフにすると、すべてのインターフェイスで PIM および IGMP がディセーブルになります。

（注） インターフェイスごとに PIM および IGMP をディセーブルにできます。詳細については、[IGMP] ページ - [Protocol] タブ （2678 ページ）および [PIM] ページ - [Protocol] タブ （2689 ページ）を参照してください。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから [プラットフォーム（Platform）] > [マルチキャスト（Multicast）] > [PIM と IGM のイネーブル化（PEnable PIM and IGMP）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [マルチキャスト（Multicast）] > [PIM と IGM のイネーブル化（PEnable PIM and IGMP）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- IGMP の設定 （2676 ページ）
- マルチキャスト ルートの設定 （2684 ページ）
- マルチキャスト境界フィルタの設定 （2686 ページ）
- PIM の設定 （2688 ページ）

IGMP の設定

インターネット プロトコル ホストは、IGMP を使用して、グループ メンバーシップを直接接続されたマルチキャスト ルータにレポートします。インターネット グループ管理プロトコル（IGMP）は、グループ アドレス（クラス D）の IP アドレスを使用します。

ホスト グループ アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。アドレス 224.0.0.0 がグループに割り当てられることはありません。アドレス 224.0.0.1 は、サブネットのシステムすべてに割り当てられます。アドレス 224.0.0.2 は、サブネットのルータすべてに割り当てられます。

[IGMP] ページには、タブ付きのパネルが 4 つあり、Security Manager で IGMP を設定および管理するのに使用できます。

- [IGMP] ページ - [Protocol] タブ （2678 ページ）：このパネルには、インターフェイス固有の IGMP パラメータが表示されます。IGMP をディセーブルにしたり、IGMP パラメータを変更したりできます。
- [IGMP] ページ - [Access Group] タブ （2680 ページ）：インターフェイスで許可されるマルチキャスト送信元を制限するアクセス グループを管理できます。
- [IGMP] ページ - [Static Group] タブ （2682 ページ）：ネットワーク上のホストの中には、IGMP クエリーに応答しないように設定されているものもあります。ただし、その場合でもそのネットワーク セグメントにマルチキャスト トラフィックを転送できます。マルチキャスト トラフィックをネットワーク セグメントにプルする方法が 2 つあります。
  - [Join Group] タブは、マルチキャスト グループのメンバーとしてインターフェイスを設定するために使用します。この方法では、セキュリティ アプライアンスがマルチキャストパケットを受け付けて、そのパケットを指定のインターフェイスに転送します。
  - [Static Group] タブは、スタティックに接続されたグループ メンバーになるようにセキュリティ アプライアンスを設定するために使用します。この方法では、セキュリティアプライアンスはパケット自体は受け付けず、パケットの転送だけを行います。そのため、スイッチングが高速に実施されます。発信インターフェイスはIGMPキャッシュに表示されますが、インターフェイス自体はマルチキャスト グループのメンバーではありません。

このタブでは、マルチキャスト グループをインターフェイスにスタティックに割り当てたり、既存のスタティックなグループ割り当てを変更したりできます。

- [IGMP] ページ - [Join Group] タブ （2683 ページ）：このタブは、セキュリティ アプライアンスが所属するマルチキャスト グループを管理するために使用します。

（注） 単にインターフェイスに特定のグループのマルチキャスト パケットを転送するだけで、セキュリティ アプライアンスではそのパケットをグループの一部として受け付けないようにする場合は、[IGMP] ページ - [Static Group] タブ （2682 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [マルチキャスト（Multicast）] > [IGMP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [IGMP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[IGMP] ページ - [Protocol] タブ

[Protocol] タブは、セキュリティ アプライアンス上のインターフェイスに IGMP パラメータを設定するために使用します。

ナビゲーション パス

[Protocol] タブには、[IGMP] ページからアクセスできます。[IGMP] ページの詳細については、IGMP の設定 （2676 ページ）を参照してください。

関連項目

- [Configure IGMP Parameters] ダイアログボックス （2679 ページ）
- PIM および IGMP のイネーブル化 （2675 ページ）
- PIM の設定 （2688 ページ）
- マルチキャスト ルートの設定 （2684 ページ）

フィールド リファレンス

表 683 : [Protocol] タブ

要素	説明
[Protocol] テーブル	
インターフェイス	IGMP 設定を適用するインターフェイスの名前。
[有効（Enabled）]	インターフェイスで IGMP がイネーブルになっているかどうかを示します。
バージョン	インターフェイスでイネーブルになっている IGMP のバージョン。
Query Interval	指定ルータが IGMP ホストクエリー メッセージを送信する間隔（秒数）。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。
クエリー タイムアウト（Query Timeout）	前のセキュリティ アプライアンスがインターフェイスに対するクエリーを停止してから、セキュリティ アプライアンスがその処理を引き継ぐまでの時間（秒数）。有効な値の範囲は 60 ～ 300 秒です。デフォルト値は 255 秒です。

要素	説明
応答時間（Response Time）	IGMP クエリーでアドバタイズされる最大応答時間（秒数）。セキュリティ アプライアンスが指定された応答時間内にホスト レポートを受信しない場合、IGMP グループは排除されます。この値を小さくすると、セキュリティ アプライアンスによるグループの排除が早くなります。有効な値の範囲は 1 ～ 12 秒です。デフォルト値は 10 秒です。この値の変更は、IGMP Version 2 の場合にだけ有効です。
Group Limit	インターフェイス上で参加できるホストの最大数。有効な値の範囲は 1 ～ 500 です。デフォルト値は 500 です。
Maximum Groups (PIX 6.3)	マルチキャストがイネーブルになっているグループの最大数。有効な値の範囲は 0 ～ 2000 です。
Forward Interface	IGMP 転送がイネーブルになっている場合に、選択したインターフェイスが IGMP ホスト レポートを転送するインターフェイスの名前。

[Configure IGMP Parameters] ダイアログボックス

[Configure IGMP Parameters] ダイアログボックスは、セキュリティ アプライアンス上のインターフェイスに IGMP パラメータを設定するために使用します。

ナビゲーション パス

[Configure IGMP Parameters] ダイアログボックスには、[IGMP] ページ - [Protocol] タブからアクセスできます。詳細については、[IGMP] ページ - [Protocol] タブ （2678 ページ）を参照してください。

関連項目

- [IGMP] ページ - [Protocol] タブ （2678 ページ）
- IGMP の設定 （2676 ページ）

フィールド リファレンス

表 684 : [Configure IGMP Parameters] ダイアログボックス

要素	説明
インターフェイス（Interface）	IGMP 設定を適用するインターフェイスの名前。
Forward Interface	IGMP 転送がイネーブルになっている場合に、IGMP ホスト レポートが転送されるインターフェイスの名前。

要素	説明
バージョン	インターフェイスでイネーブルになっている IGMP のバージョン。IGMP バージョン 1 をイネーブルにするには 1 を選択し、IGMP バージョン 2 をイネーブルにするには 2 を選択します。機能によっては、IGMP バージョン 2 にする必要があります。デフォルトでは、セキュリティ アプライアンスは IGMP バージョン 2 を使用します。
Query Interval	指定ルータが IGMP ホストクエリー メッセージを送信する間隔（秒数）。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 125 秒です。
応答時間（Response Time）	IGMP クエリーでアドバタイズされる最大応答時間（秒数）。セキュリティアプライアンスが指定された応答時間内にホスト レポートを受信しない場合、IGMP グループは排除されます。この値を小さくすると、セキュリティアプライアンスによるグループの排除が早くなります。有効な値の範囲は 1 ～ 12 秒です。デフォルト値は 10 秒です。この値の変更は、IGMP Version 2 の場合にだけ有効です。
Maximum Groups (PIX 6.3)	マルチキャストがイネーブルになっているグループの最大数。有効な値の範囲は 0 ～ 2000 です。
PIX 7.x、 ASA だけ	
Enable IGMP	このチェックボックスをオンにすると、指定したインターフェイスで IGMP がイネーブルになります。
Group Limit	インターフェイス上で参加できるホストの最大数。有効な値の範囲は 1 ～ 500 です。デフォルト値は 500 です。
クエリー タイムアウト（Query Timeout）	前のセキュリティアプライアンスがインターフェイスに対するクエリーを停止してから、セキュリティアプライアンスがその処理を引き継ぐまでの時間（秒数）。有効な値の範囲は 60 ～ 300 秒です。デフォルト値は 255 秒です。

[IGMP] ページ - [Access Group] タブ

[Access Group] タブは、インターフェイスで許可されるマルチキャスト グループを制御するために使用します。

このページのテーブルには、現在定義されているすべてのマルチキャスト アクセス グループがリストされ、グループごとに、グループが定義されているインターフェイスまたはインターフェイス ロールの名前、グループ ネットワーク、およびグループが許可されるか拒否されるかが表示されます。これらのフィールドの詳細については、[Configure IGMP Access Group Parameters] ダイアログボックス （2681 ページ）を参照してください。

- マルチキャスト アクセス グループをテーブルに追加するには、[Add Row] ボタンをクリックします。

- グループの設定を編集するには、そのグループを選択して [Edit Row] ボタンをクリックします。
- グループを削除するには、そのグループを選択して [Delete Row] ボタンをクリックします。

ナビゲーション パス

[Access Group] タブには、 IGMP の設定 （2676 ページ）からアクセスできます。

関連項目

- PIM および IGMP のイネーブル化 （2675 ページ）
- マルチキャスト ルートの設定 （2684 ページ）

[Configure IGMP Access Group Parameters] ダイアログボックス

[Configure IGMP Access Group Parameters] ダイアログボックスは、アクセス グループ エントリを追加または変更するために使用します。

ナビゲーション パス

[Configure IGMP Access Group Parameters] ダイアログボックスには、 [IGMP] ページ - [Protocol] タブ （2678 ページ）からアクセスできます。

関連項目

- [IGMP] ページ - [Protocol] タブ （2678 ページ）
- IGMP の設定 （2676 ページ）

フィールド リファレンス

表 *685 : [Configure IGMP Access Group Parameters]* ダイアログボックス

要素	説明
インターフェイス（Interface）	アクセス グループを割り当てるインターフェイスの名前を入力するか、または選択します。
Multicast Group Network	指定したインターフェイスに割り当てるマルチキャスト グループ アドレスを入力するか、または選択します。1 つ以上の IP アドレス/ネットマスク エントリ、1 つ以上のネットワーク/ホスト オブジェクト、または両方の組み合わせを指定できます。エントリはカンマで区切ります。 グループ ネットワーク アドレスの範囲は、224.0.0.0 ～ 239.255.255.255 です。

要素	説明
操作	インターフェイスでマルチキャストグループを許可する場合は、[許可（permit）] を選択します。マルチキャストグループを許可しない場合は、[拒否（deny）] を選択します。

[IGMP] ページ - [Static Group] タブ

[Static Group] タブは、マルチキャスト グループをインターフェイスにスタティックに割り当てるために使用します。

ナビゲーション パス

[Static Group] タブには、[IGMP] ページからアクセスできます。[IGMP] ページの詳細については、 IGMP の設定 （2676 ページ）を参照してください。

関連項目

- PIM および IGMP のイネーブル化 （2675 ページ）
- マルチキャスト ルートの設定 （2684 ページ）
- PIM の設定 （2688 ページ）

フィールド リファレンス

表 686 : [Static Group] タブ

要素	説明
インターフェイス（Interface）	スタティック グループを関連付けるインターフェイスの名前。
[マルチキャスト グループ アドレス（Multicast Group Address）]	このルールを適用するマルチキャスト グループ アドレス。

[Configure IGMP Static Group Parameters] ダイアログボックス

[Configure IGMP Static Group Parameters] ダイアログボックスは、マルチキャスト グループをインターフェイスにスタティックに割り当てるため、または既存のスタティックなグループ割り当てを変更するために使用します。

ナビゲーション パス

[Configure IGMP Static Group Parameters] ダイアログボックスには、[IGMP] ページ - [Static Group] タブからアクセスできます。詳細については、 [IGMP] ページ - [Static Group] タブ （2682 ページ）を参照してください。

関連項目

- [IGMP] ページ - [Static Group] タブ （2682 ページ）
- IGMP の設定 （2676 ページ）

フィールド リファレンス

表 *687 : [Configure IGMP Static Group Parameters]* ダイアログボックス

要素	説明
インターフェイス（Interface）	スタティック グループを関連付けるインターフェイスの名前。
マルチキャスト グループ	このルールを適用するマルチキャスト グループ アドレス。グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の値である必要があります。

[IGMP] ページ - [Join Group] タブ

[Join Group] タブは、マルチキャスト グループのメンバーになるようにインターフェイスを設定するために使用します。

ナビゲーション パス

[Join Group] タブには、[IGMP] ページからアクセスできます。[IGMP] ページの詳細については、 IGMP の設定 （2676 ページ）を参照してください。

関連項目

- PIM および IGMP のイネーブル化 （2675 ページ）
- PIM の設定 （2688 ページ）
- マルチキャスト ルートの設定 （2684 ページ）

フィールド リファレンス

表 *688 : [Join Group]* タブ

要素	説明
インターフェイス（Interface）	マルチキャスト グループ メンバーシップを設定するインターフェイスの名前。
[マルチキャスト グループ アドレス（Multicast Group Address）]	このルールを適用するマルチキャスト グループ アドレス。

[Configure IGMP Join Group Parameters] ダイアログボックス

[Configure IGMP Join Group Parameters] ダイアログボックスは、マルチキャスト グループのメンバーになるようにインターフェイスを設定するため、または既存のメンバーシップ情報を変更するために使用します。

ナビゲーション パス

[Configure IGMP Join Group Parameters] ダイアログボックスには、[IGMP] ページ - [Join Group] タブからアクセスできます。詳細については、[IGMP] ページ - [Join Group] タブ （2683 ページ）を参照してください。

関連項目

- [IGMP] ページ - [Join Group] タブ （2683 ページ）
- IGMP の設定 （2676 ページ）

フィールド リファレンス

表 689 : [Configure IGMP Join Group Parameters] ダイアログボックス

要素	説明
インターフェイス（Interface）	マルチキャスト グループ メンバーシップを設定するインターフェイスの名前。
Join Group	このルールを適用するマルチキャスト グループ アドレス。グループ アドレスは、224.0.0.0 ～ 239.255.255.255 の値である必要があります。

マルチキャスト ルートの設定

スタティックなマルチキャスト ルートを使用すると、マルチキャスト トラフィックとユニキャスト トラフィックとを区別できます。たとえば、送信元と宛先間のパスでマルチキャスト ルーティングがサポートされていない場合、このことを解決するには、マルチキャスト デバイスを 2 つ用意して両者間に GRE トンネルを設定し、そのトンネルでマルチキャスト パケットを送信します。

スタティックなマルチキャスト ルートは、セキュリティ アプライアンスにローカルであり、アドバタイズも再配布もされません。

[Multicast Routes] ページは、スタティックなマルチキャスト ルートを管理するために使用します。現時点で定義されているルートが表示され、スタティックなマルチキャスト ルートを追加、編集、および削除できます。

このページのこのテーブルに表示されているフィールドの詳細については、[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックス （2685 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [マルチキャスト（Multicast）] > [マルチキャストルート（Multicast Routes）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [マルチキャスト（Multicast）] > [マルチキャストルート（Multicast Routes）]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- PIM および IGMP のイネーブル化 （2675 ページ）
- IGMP の設定 （2676 ページ）
- PIM の設定 （2688 ページ）

[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックス

[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックスは、スタティックなマルチキャスト ルートをセキュリティ アプライアンスに追加するため、または既存のルートを変更するために使用します。

ナビゲーション パス

[Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックスには、[Multicast Routing] ページからアクセスできます。詳細については、マルチキャスト ルートの設定 （2684 ページ）を参照してください。

フィールド リファレンス

表 690 : [Add MRoute Configuration]/[Edit MRoute Configuration] ダイアログボックス

要素	説明
送信元インターフェイス（Source Interface）	マルチキャスト ルートの着信インターフェイスを入力するか、または選択します。
送信元ネットワーク	マルチキャスト送信元の IP アドレスおよびマスクを入力するか、またはネットワーク/ホスト オブジェクトを選択します。

要素	説明
Output Interface/Dense	（任意）マルチキャスト ルートの発信インターフェイスを入力するか、または選択します。宛先インターフェイスを指定した場合、ルートは選択したインターフェイス経由で転送されます。宛先インターフェイスを指定しない場合、RPF を使用してルートが転送されます。インターフェイスまたは RPF ネイバーを指定できますが、同時に両方は指定できません。
マルチキャスト ネットワーク（PIX 6.3）	マルチキャスト パケットを受信するグループを入力するか、または選択します。これは、範囲が 224.0.1.0 ～ 239.255.255.255 のマルチキャスト IP アドレスである必要があります。
Distance（PIX 7.x、ASA、FWSM）	スタティックなマルチキャスト ルートのアドミニストレーティブ ディスタンスを入力します。スタティックなマルチキャスト ルートにユニキャスト ルートと同じアドミニストレーティブ ディスタンスがある場合は、スタティックなマルチキャスト ルートが優先されます。

マルチキャスト境界フィルタの設定

バージョン 7.2(1) 以降が稼働する ASA では、[Multicast Boundary Filter] ページを使用して、マルチキャスト ドメイン間の境界として機能するようにアプライアンスを設定できます。ASA は、マルチキャスト グループ アドレスをアクセス リストと比較して、リストで特に許可したものを除いてすべてのマルチキャスト トラフィックをブロックします。

[Multicast Boundary Filter] ページには、現在定義されているインターフェイス境界フィルタがすべて表示されます。このページから、フィルタ リストを追加、編集、および削除できます。

このページのフィールドの詳細については、[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックス （2687 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、**[プラットフォーム（Platform）] > [マルチキャスト（Multicast）] > [マルチキャストバウンダリフィルタ（Multicast Boundary Filter）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [マルチキャスト（Multicast）] > [マルチキャストバウンダリフィルタ（Multicast Routes）]** を選択します。Multicast Boundary Filter 共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス （2687 ページ）

[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックス

[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックスは、個々のインターフェイスのマルチキャスト境界フィルタ リストを追加、編集、および削除するために使用します。

ナビゲーション パス

[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックスには、マルチキャスト境界フィルタの設定 （2686 ページ）からアクセスできます。

関連項目

- [Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス （2687 ページ）
- マルチキャスト境界フィルタの設定 （2686 ページ）

フィールド リファレンス

表 *691 : [Add MBoundary Configuration]/[Edit MBoundary Configuration]* ダイアログボックス

要素	説明
インターフェイス（Interface）	このマルチキャスト境界のインターフェイスを入力するか、または選択します。
すべてのAuto_RPグループ範囲のアナウンスメントの削除（any Auto_RP group range announcements）	このボックスをオンにすると、このインターフェイスの境界アクセス コントロール リストによって拒否されたAuto-RPメッセージがドロップされます。これは、自動フィルタリングと呼ばれます。
Multicast boundary filter configuration list	指定したインターフェイス用に特に許可または拒否されたマルチキャスト グループ アドレスを表示します。このリストは、[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス （2687 ページ）（[Add Row or Edit Row] をクリックします）で管理されます。

[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス

このダイアログボックスは、[Add MBoundary Configuration]/[Edit MBoundary Configuration] ダイアログボックスのリストに対する許可または拒否を示すマルチキャスト グループ エントリを定義するために使用します。

ナビゲーション パス

[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックスには、[Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス （2687 ページ）からアクセスできます。

関連項目

- マルチキャスト境界フィルタの設定 （2686 ページ）

フィールド リファレンス

表 692 : [Add MBoundary Interface Configuration]/[Edit MBoundary Interface Configuration] ダイアログボックス

要素	説明
操作	[許可（permit）] または [拒否（deny）] を選択して、このマルチキャスト グループに対して実行するアクションを指定します。
マルチキャスト グループ	このアクションが適用される単一のマルチキャスト アドレス、またはマルチキャスト グループ アドレスを入力します。アドレスは、0.0.0.0 であるか、または 224.0.0.0 ～ 239.255.255.255 である必要があります。グループ アドレス範囲は、標準サブネット マスク（239.0.0.0 255.0.0.0 など）または CIDR プレフィックス表記法（239.0.0.0/8 など）を使用して入力できます。 また、指定済みのネットワーク/ホスト オブジェクトも選択できます。

PIM の設定

IGMP を使用してマルチキャスト送信を受信するように登録された各ホストに特定のマルチキャスト送信を配布する場合、Protocol Independent Multicast（PIM）を使用すると、ネットワークの最良パスを柔軟に決定できます。ルータおよびセキュリティ デバイスは、PIM を使用して、マルチキャスト データグラムを転送するためのテーブルを維持します。

Cisco ルータのデフォルトである PIM Sparse Mode（PIM SM; PIM スパース モード）では、マルチキャスト送信の送信元がブロードキャストを開始すると、登録されたすべてのホストにパケットが到達するまで、トラフィックがマルチキャスト ルータ間を転送されます。トラフィック送信元により直接的に到達できるパスが存在する場合は、ラスト ホップ ルータが Join メッセージを送信元に送信します。これにより、より適切なパスを経由して、トラフィックが再ルーティングされます。

（注） PIM は PAT ではサポートされていません。これは、PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルでだけ機能するためです。

セキュリティ アプライアンスでマルチキャスト ルーティングをイネーブルにすると、デフォルトではすべてのインターフェイスで PIM および IGMP がイネーブルになります。インターフェイスごとに PIM をディセーブルにできます。

[PIM] ページには、最大 6 個のタブ付きパネルが表示されます。

- [PIM] ページ - [Protocol] タブ （2689 ページ）：インターフェイス固有の PIM プロパティを管理できます。
- [PIM] ページ - [Neighbor Filter] タブ （2691 ページ）：個々のインターフェイスのネイバー フィルタを管理できます。ただし、ASA 7.2(1)+ のデバイスでだけ使用できます。
- [PIM] ページ - [Bidirectional Neighbor Filter] タブ （2692 ページ）：個々のインターフェイスの双方向ネイバー フィルタを管理できます。ただし、ASA 7.2(1)+ のデバイスでだけ使用できます。
- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）：PIM を設定するときは、ランデブー ポイント（RP）として動作するデバイスを 1 つ以上選択する必要があります。RP は、共用配布ツリーの単一の共通ルートであり、デバイスごとにスタティックに設定されます。第 1 ホップ ルータは、RP を使用して、送信元のマルチキャスト ホストに代わって登録パケットを送信します。
- [PIM] ページ - [Route Tree] タブ （2697 ページ）：デフォルトでは、新規送信元から最初のパケットが届くと、PIM リーフ ルータはただちに最短パス ツリーに参加します。これにより、遅延が短縮されます。ただし、共有ツリーよりも多くのメモリが必要になります。セキュリティ アプライアンスが最短パス ツリーに参加するか、または共有ツリーを使用するかについて、すべてのマルチキャスト グループまたは特定のマルチキャスト アドレスだけを対象に設定できます。
- [PIM] ページ - [Request Filter] タブ （2698 ページ）：セキュリティ アプライアンスが RP として機能する場合は、登録できるマルチキャスト送信元を制限できます。これにより、未認可の送信元が RP に登録されることを回避できます。[Request Filter] パネルでは、セキュリティ アプライアンスが PIM 登録メッセージを受け付けるマルチキャスト送信元を定義できます。

[PIM] ページ - [Protocol] タブ

[Protocol] タブは、セキュリティ アプライアンスでインターフェイスの PIM プロパティを設定するために使用します（ただし、PIX 6.3 デバイスにはありません）。現在設定されているすべてのインターフェイスが表示されます。このパネルでは、エントリを追加、編集、および削除できます。

このパネルのフィールドの詳細については、 [Add PIM Protocol]/[Edit PIM Protocol] ダイアログ ボックス （2690 ページ）を参照してください。

ナビゲーション パス

[PIM] ページから [Protocol] タブにアクセスします。詳細については、 PIM の設定 （2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）
- [PIM] ページ - [Route Tree] タブ （2697 ページ）
- [PIM] ページ - [Request Filter] タブ （2698 ページ）

[Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックス

[Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックスは、PIX 7.x 以降が稼働するセキュリティ アプライアンスでインターフェイスの PIM プロパティを設定するために使用します。

指定ルータについて

代表ルータは、PIM Register、Join、Prune の各メッセージをランデブー ポイント（RP）に送信します。ネットワーク セグメントに複数のマルチキャスト ルーティング デバイスがあるときは、DR プライオリティに基づいて指定ルータを選択する選択プロセスがあります。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。デフォルトでは、セキュリティ アプライアンスの DR プライオリティは 1 です。

ナビゲーション パス

[Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックスには、 [PIM] ページ - [Protocol] タブ（2689 ページ）からアクセスできます。

フィールド リファレンス

表 693 : [Add PIM Protocol]/[Edit PIM Protocol] ダイアログボックス

要素	説明
インターフェイス（Interface）	PIM を設定するインターフェイスを入力するか、または選択します。
Protocol-Independent Multicast（PIM）のイネーブル化	このチェックボックスをオンにすると、選択したインターフェイスで PIM がイネーブルになります。このチェックボックスをオフにすると、テーブルからこの PIM プロトコル エントリを削除せずに、インターフェイスで PIM をディセーブルにできます。
DR Priority	このインターフェイスの Designated Router（DR; 指定ルータ）プライオリティ。サブネットで DR プライオリティが最も高いルータが指定ルータになります。有効な値の範囲は 0 ～ 4294967294 です。デフォルトの DR プライオリティは 1 です。この値をゼロに設定すると、セキュリティ アプライアンス インターフェイスは、デフォルト ルータになる資格がなくなります。
Hello Interval (seconds)	インターフェイスが PIM hello メッセージを送信する頻度（秒）。有効な値の範囲は 1 ～ 3600 秒で、デフォルト値は 30 秒です。

要素	説明
Join-Prune Interval (seconds)	インターフェイスが PIM Join および Prune アドバタイズメントを送信する頻度（秒）。有効な値の範囲は 10 ～ 600 秒で、デフォルト値は 60 秒です。

[PIM] ページ - [Neighbor Filter] タブ

PIM ネイバー フィルタは、PIM に参加できるネイバー デバイスを定義するアクセス コントロール リスト（ACL）です。インターフェイスのネイバー フィルタが設定されていない場合、制限はありません。PIM ネイバー フィルタが設定されている場合は、フィルタ リストで許可されるネイバーだけが、セキュリティ アプライアンスとともに、PIM に参加できます。

バージョン 7.2(1) 以降が稼働する ASA では、[Neighbor Filter] タブを使用して、PIM ネイバーになることができるデバイスを制御できます。このパネルは、インターフェイスごとのネイバー フィルタ リストを定義および管理するために使用します。このパネルのフィールドの詳細については、[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックス （2691 ページ）を参照してください。

ナビゲーション パス

[PIM] ページから [Protocol] タブにアクセスします。詳細については、PIM の設定 （2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Protocol] タブ （2689 ページ）
- [PIM] ページ - [Bidirectional Neighbor Filter] タブ （2692 ページ）
- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）
- [PIM] ページ - [Route Tree] タブ （2697 ページ）
- [PIM] ページ - [Request Filter] タブ （2698 ページ）

[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックス

[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックスは、[PIM] ページの [Neighbor Filter] パネルに表示される PIM ネイバー フィルタ ACL でエントリを追加および編集するために使用します。

ナビゲーション パス

[Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックスには、[PIM] ページ - [Neighbor Filter] タブ （2691 ページ）からアクセスできます。

フィールド リファレンス

表 694 : [Add PIM Neighbor Filter]/[Edit PIM Neighbor Filter] ダイアログボックス

要素	説明
インターフェイス（Interface）	この PIM ネイバー フィルタ エントリが適用されるインターフェイスを入力するか、または選択します。
Neighbor Filter Group	選択したアクションが適用される単一のマルチキャスト アドレス、またはマルチキャスト グループ アドレスを入力します。グループ アドレス範囲は、標準サブネット マスク（239.0.0.0 255.0.0.0 など）または CIDR プレフィックス表記法（239.0.0.0/8 など）を使用して入力できます。 また、指定済みのネットワーク/ホスト オブジェクトも選択できます。
操作	指定したネイバーを PIM に参加させるには [許可（permit）] を選択し、指定したネイバーを PIM に参加させないためには [拒否（deny）] を選択します。

[PIM] ページ - [Bidirectional Neighbor Filter] タブ

PIM 双方向ネイバーフィルタは、双方向ツリーおよび Designated Forwarder（DF; 代表フォワーダ）選択に参加できるネイバーデバイスを定義するアクセス制御リスト（ACL）です。PIM 双方向ネイバーフィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバーフィルタを使用すると、DF 選択に参加するデバイスを指定し、その一方で、引き続きすべてのデバイスがスパースモードのドメインに参加できるようにして、スパースモード専用ネットワークから「双方向」ネットワークに移行できます。双方向対応デバイスは、セグメントに双方向でないデバイスがあっても、数ある双方向対応デバイスの中から DF を選択できます。双方向でないデバイス上にマルチキャスト境界があるため、双方向グループからの PIM メッセージおよびデータが双方向サブセット クラウドの内外に漏れることを回避できます。

双方向 PIM を使用すると、マルチキャスト デバイスが保持する状態情報を削減できます。セグメント内のすべてのマルチキャスト デバイスが、DF を選択できるように双方向対応である必要があります。

PIM 双方向ネイバー フィルタがイネーブルになっていると、ACL で許可されるルータおよび他のデバイスは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。

- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

双方向ネイバー フィルタ リストの管理

バージョン 7.2(1) 以降が稼働する ASA では、このパネルでインターフェイスごとの双方向ネイバー フィルタ リストを定義および管理して、特定のインターフェイスのマルチキャスト送信元アドレスを許可または拒否できます。このパネルのフィールドの詳細については、[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックス （2693 ページ）を参照してください。

ナビゲーション パス

[Bidirectional Neighbor Filter] タブには、[PIM] ページからアクセスします。詳細については、PIM の設定 （2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Protocol] タブ （2689 ページ）
- [PIM] ページ - [Neighbor Filter] タブ （2691 ページ）
- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）
- [PIM] ページ - [Route Tree] タブ （2697 ページ）
- [PIM] ページ - [Request Filter] タブ （2698 ページ）

[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックス

[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックスは、[PIM] ページ - [Bidirectional Neighbor Filter] タブ （2692 ページ）に表示される双方向ネイバー アクセス コントロール リストでエントリを追加または編集するために使用します。

ナビゲーション パス

[Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックスには、[PIM] ページ - [Bidirectional Neighbor Filter] タブ （2692 ページ）からアクセスできます。

フィールド リファレンス

表 695 : [Add PIM Bidirectional Neighbor Filter]/[Edit PIM Bidirectional Neighbor Filter] ダイアログボックス

要素	説明
インターフェイス（Interface）	この PIM 双方向ネイバー フィルタ エントリが適用されるインターフェイスを入力するか、または選択します。

要素	説明
Neighbor Filter Group	選択したアクションが適用される単一のマルチキャスト アドレス、またはマルチキャスト グループ アドレスを入力します。グループ アドレス範囲は、標準サブネット マスク（239.0.0.0 255.0.0.0 など）または CIDR プレフィックス表記法（239.0.0.0/8 など）を使用して入力できます。 また、指定済みのネットワーク/ホスト オブジェクトも選択できます。
操作	指定したネイバーを DF 選択プロセスに参加させるには [許可（permit）] を選択し、指定したネイバーを DF 選択プロセスに参加させないためには [拒否（deny）] を選択します。

[PIM] ページ - [Rendezvous Points] タブ

PIM を設定するときは、RP として動作するルータまたはルーティング デバイスを 1 つ以上選択する必要があります。RP は、共用配布ツリーの単一の共通ルートであり、デバイスごとにスタティックに設定されます。第 1 ホップ ルータは、RP を使用して、送信元のマルチキャスト ホストに代わって登録パケットを送信します。

複数のグループにサービスを提供するように単一の RP を設定できます。特定のグループを指定していない場合、そのグループの RP は IP マルチキャスト グループ範囲（224.0.0.0/4）全体に適用されます。

[Rendezvous Points] パネルは、ランデブー ポイントを定義するために使用します。複数の RP を設定できますが、同じ RP に複数のエントリは設定できません。

ナビゲーション パス

[Rendezvous Points] タブには、[PIM] ページからアクセスします。詳細については、PIM の設定 （2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Protocol] タブ （2689 ページ）
- [PIM] ページ - [Route Tree] タブ （2697 ページ）
- [PIM] ページ - [Request Filter] タブ （2698 ページ）

フィールド リファレンス

表 696 : [Rendezvous Points] タブ

要素	説明
Generate older IOS compatible register messages	ランデブー ポイントが Cisco IOS ルータである場合には、このボックスをオンにします。セキュリティ アプライアンス ソフトウェアが PIM ヘッダーと後続の 4 バイトだけに基づいて計算されたチェックサムを持つ Register メッセージを受け付けるのに対して、Cisco IOS ソフトウェアはすべての PIM メッセージ タイプについて、PIM メッセージ全体に基づいて計算されたチェックサムを持つ Register メッセージを受け付けます。
Rendezvous Points table	セキュリティ アプライアンスに現在設定されているランデブー ポイントを表示します。[Add Row]、[Edit Row]、および [Delete Row] ボタンを使用して、このリストを管理します。[Add Row] および [Edit Row] ボタンを使用すると、[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス （2695 ページ）が開きます。

[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス

[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックスは、[Rendezvous Points] テーブルにエントリを追加するため、または既存のランデブー ポイント エントリを編集するために使用します。次の点に注意してください。

- 同じランデブー ポイント アドレスは 2 回使用できません。
- 複数のランデブーポイントに「全グループ」を指定することはできません。

ナビゲーション パス

[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックスには、[PIM] ページ - [Rendezvous Points] タブ （2694 ページ）からアクセスできます。

フィールド リファレンス

表 697 : [Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス

要素	説明
Rendezvous Point IP Address	ランデブー ポイントの IP アドレスを入力します。これはユニキャスト アドレスです。また、[Select] をクリックして、ネットワーク/ホスト オブジェクトを選択することもできます。 ランデブー ポイント エントリを編集するときには、この値を変更できません。

要素	説明
Use bi-directional forwarding	指定したマルチキャスト グループを双方向モードで動作させる場合には、このボックスをオンにします。双方向モードでは、セキュリティ アプライアンスはマルチキャスト パケットを受信し、自らに直接接続されたメンバーまたは PIM ネイバーが存在しない場合、送信元に Prune メッセージを返します。指定したマルチキャスト グループをスパース モードで動作させる場合には、このボックスをオフにします。 （注） セキュリティ アプライアンスは、実際の双方向設定に関係なく常に PIM hello メッセージで双方向機能をアドバタイズします。
この RP をすべてのマルチキャスト グループに使用する（Use this RP for All Multicast Groups）	インターフェイスのすべてのマルチキャスト グループに、指定されたランデブー ポイントを使用するには、このオプションを選択します。
Use this RP for the Multicast Groups as specified below	指定のランデブー ポイントを使用するマルチキャスト グループを定義するには、このオプションを選択します。[Multicast Groups] テーブルがアクティブになります。
[Multicast Groups] テーブル	指定のランデブー ポイントに現在関連付けられているマルチキャスト グループが表示されます。 テーブル エントリは上から順に処理されます。たとえば、マルチキャスト グループの範囲を含むエントリを作成してから、その範囲内の特定グループに対する拒否ルールをテーブルの一番上に配置することによって、その特定グループを除外できます。つまり、マルチキャスト グループの範囲に対する許可ルールを、個々の拒否ステートメントの後ろに続けます。 テーブルの下部にあるボタンを使用して [Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス （2696 ページ）を開き、エントリの追加または編集、エントリの削除、およびテーブル内でのエントリの上下移動を行います。

[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス

[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックスは、[Add/Edit Rendezvous Point] ダイアログボックスに表示される [Multicast Groups] テーブルのマルチキャスト グループ ルールを作成するため、またはマルチキャスト グループ ルールを変更するために使用します。また、このダイアログボックスは、[Route Tree] タブで [Shared Tree] ルート フィルタリングを使用するマルチキャスト グループを個別に指定する場合にも使用します。

ナビゲーション パス

ランデブー ポイントを定義するときは、[Add Rendezvous Point]/[Edit Rendezvous Point] ダイアログボックス （2695 ページ）から [Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックスにアクセスします。詳細については、[PIM] ページ - [Rendezvous Points] タブ （2694 ページ）を参照してください。

PIM Register メッセージのフィルタリング方法を指定するときは、[PIM] ページ - [Route Tree] タブ （2697 ページ）の [Multicast Groups] テーブルの下にある [Add Row] ボタンまたは [Edit Row] ボタンをクリックして、このダイアログボックスを開きます。

フィールド リファレンス

表 *698 : [Add Multicast Group Rules]/[Edit Multicast Group Rules]* ダイアログボックス

要素	説明
操作	指定したマルチキャストアドレスを許可するグループルールを作成するには、[許可（permit）] を選択します。指定したマルチキャストアドレスを拒否するグループルールを作成するには、[拒否（deny）] を選択します。
Multicast Group Network	グループに関連付けられたマルチキャスト アドレスおよびネットワーク マスクを入力するか、または目的のネットワーク/ホスト オブジェクトを選択します。

[PIM] ページ - [Route Tree] タブ

セキュリティ アプライアンスがランデブー ポイントとして機能している場合は、[Route Tree] タブを使用して、さまざまな送信元からの PIM Register メッセージをどのようにフィルタリングするかを指定します。具体的には、すべてのマルチキャスト グループまたは特定のマルチキャストアドレスだけを対象に、最短パス ツリーまたは共有ツリーのいずれかを指定します。

ナビゲーション パス

[Route Tree] タブには、[PIM] ページからアクセスできます。詳細については、PIM の設定 （2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Protocol] タブ （2689 ページ）
- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）
- [PIM] ページ - [Request Filter] タブ （2698 ページ）

フィールド リファレンス

表 699 : [Route Tree] タブ

要素	説明
If.., specify how the PIM register messages from various sources are filtered	ツリー/グループ オプションを選択します。 • [すべてのグループに最短パスツリーを使用（Use Shortest Path Tree for All Groups）]：セキュリティアプライアンスは、すべてのマルチキャストグループに最短パスツリーを使用します。 • [すべてのグループに共有ツリーを使用（Use Shared Tree for All Groups）]：セキュリティアプライアンスは、すべてのマルチキャストグループに共有ツリーを使用します。 • [以下に指定されているグループに共有ツリーを使用（Use Shared Tree for the Groups specified below）]：セキュリティアプライアンスは、[マルチキャストグループ（Multicast Groups）] テーブルの下で指定されているグループに共有ツリーを使用します。[Multicast Groups] テーブルに記載されていないグループには、最短パス ツリーが使用されます。
[Multicast Groups] テーブル	共有ツリーを使用するマルチキャスト グループが表示されます。 テーブル エントリは上から順に処理されます。たとえば、マルチキャスト グループの範囲を含むエントリを作成してから、その範囲内の特定グループに対する拒否ルールをテーブルの一番上に配置することによって、その特定グループを除外できます。つまり、マルチキャスト グループの範囲に対する許可ルールを、個々の拒否ステートメントの後ろに続けます。 テーブルの下部にあるボタンを使用して [Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス （2696 ページ）を開き、エントリの追加または編集、エントリの削除、およびテーブル内でのエントリの上下移動を行います。

[PIM] ページ - [Request Filter] タブ

セキュリティ アプライアンスがランデブー ポイントとして機能しているときには、ランデブー ポイントに登録されるマルチキャスト送信元を制限できます。これにより、未認可の送信元がランデブー ポイントに登録されることを回避できます。[Request Filter] タブでは、セキュリティ アプライアンスが PIM Register メッセージを受け付けるマルチキャスト送信元と、拒否するマルチキャスト送信元を定義できます。

ナビゲーション パス

[Request Filter] タブには、[PIM] ページからアクセスできます。詳細については、 PIM の設定（2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Protocol] タブ （2689 ページ）
- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）
- [PIM] ページ - [Route Tree] タブ （2697 ページ）

フィールド リファレンス

表 700 : [Request Filter] タブ

要素	説明
次を使用して PIM Registerメッセージをフィルタリング（Filter PIM register messages using）	さまざまなマルチキャスト グループを対象に、PIM Register メッセージのフィルタリング方法を選択します。 • [なし（None）] : PIM Register メッセージをフィルタリングしません。 • [ルートマップ（route-map）] : 指定のルートマップを使用して、PIM Register メッセージをフィルタリングします。[ルートマップ（Route Map）] フィールドがアクティブになります。ルート マップで許可される PIM Register メッセージだけが、ランデブー ポイントに到達できます。 • [アクセスリスト（access-list）] : アクセスリストを使用して、PIM Register メッセージをフィルタリングします。[マルチキャストグループ（Multicast Groups）] テーブルがアクティブになります。アクセスリストで許可される PIM Register メッセージだけが、ランデブー ポイントに到達できます。
ルート マップ	フィルタとして [ルートマップ（route-map）] を選択したときは、ルートマップ名を入力します。参照先のルート マップで標準のホスト ACL を使用します。拡張 ACL はサポートされません。 （注） このフィールドにはルートマップ名だけが含まれます。ルートマップは、FlexConfig 内で作成および格納されます。

要素	説明
[Multicast Groups] テーブル	マルチキャスト グループとして現在定義されている要求フィルタ ルールを表示します。 テーブル エントリは上から順に処理されます。たとえば、マルチキャスト グループの範囲を含むエントリを作成してから、その範囲内の特定グループに対する拒否ルールをテーブルの一番上に配置することによって、その特定グループを除外できます。つまり、マルチキャスト グループの範囲に対する許可ルールを、個々の拒否ステートメントの後ろに続けます。 テーブルの下部にあるボタンを使用して [Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス （2696 ページ）を開き、エントリの追加または編集、エントリの削除、およびテーブル内でのエントリの上下移動を行います。

[Add Multicast Group Rules]/[Edit Multicast Group Rules] ダイアログボックス

[Add/Edit Multicast Group Rules] ダイアログボックスは、アプライアンスがランデブー ポイントとして機能するときに、セキュリティ アプライアンスへの登録を拒否または許可するマルチキャスト送信元を定義するために使用します。送信元 IP アドレスおよび宛先マルチキャスト アドレスに基づいて、フィルタ ルールを作成します。

ナビゲーション パス

[Add/Edit Multicast Group Rules] ダイアログボックスには、 [PIM] ページ - [Request Filter] タブ（2698 ページ）からアクセスできます。

フィールド リファレンス

表 *701 : [Add Multicast Group Rules]/[Edit Multicast Group Rules]* ダイアログボックス

要素	説明
操作	指定した宛先マルチキャスト トラフィックの指定した送信元に対してセキュリティ アプライアンスへの登録を許可するルールを作成するには、[許可（permit）] を選択します。指定した送信元/宛先マルチキャスト トラフィックへの登録を拒否するルールを作成するには、[拒否（deny）] を選択します。
送信元ネットワーク	Register メッセージ送信元の IP アドレスおよびネットワーク マスクを入力するか、または適切なネットワーク/ホスト オブジェクトを選択します。
宛先ネットワーク	マルチキャスト宛先の IP アドレスおよびネットワーク マスクを入力するか、または適切なネットワーク/ホスト オブジェクトを選択します。

PIM ページ - ブートストラップ ルータ タブ

PIM ブートストラップ ルータ（BSR）は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント（RP）セレクションモデルです。RP 機能にはRPの検出が含まれており、RPにデフォルトルートを提供します。これは、一連のデバイスを BSR の選択プロセスに参加する候補の BSR（C-BSR）として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブーポイント（C-RP）として設定されたデバイスは、選定された BSR にグループマッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経由で、マルチキャストツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

[ブートストラップルータ（Boot Strap Router）] タブを使用して、デバイスを PIM ブートストラップルータとして設定できます。

ナビゲーション パス

[PIM] ページから [ブートストラップルータ（Boot Strap Router）] タブにアクセスできます。詳細については、 PIM の設定 （2688 ページ）を参照してください。

関連項目

- [PIM] ページ - [Protocol] タブ （2689 ページ）
- [PIM] ページ - [Rendezvous Points] タブ （2694 ページ）
- [PIM] ページ - [Route Tree] タブ （2697 ページ）

フィールド リファレンス

表 *702 : [*ブートストラップルータ（***Boot Strap Router***）*]* タブ

要素	説明
インターフェイス（Interface）	BSR アドレスを候補の BSRにするため、アドレスの派生元のインターフェイスを選択します。
ハッシュマスク長	ハッシュ関数が呼び出される前にグループアドレスと AND 演算されるマスクの長さを入力します。ハッシュ元が同じであるすべてのグループは、同じランデブー ポイント（RP）に対応します。 たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。これにより、複数のグループについて 1 つの RP を取得できます。
プライオリティ	BSR 候補の優先順位を入力します。プライオリティが大きな BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。

[ブートストラップルータの追加/編集（Add/Edit Bootstrap Router）] ダイアログボックス

[ブートストラップルータの追加/編集（Add/Edit Bootstrap Router）] ダイアログボックスを使用して、ブートストラップルータをボーダー BSR として設定します。BSR メッセージを異なるドメイン間で交換しないでください。そのようにすると、一方のドメインにあるルータが他方のドメインにあるランデブーポイント（RP）を選択し、結果としてドメイン間でプロトコルが誤動作したり分離が行われなかったりする可能性があるためです。

PIM スパースモード（PIM-SM）のドメインの境界インターフェイスは、特にそのインターフェイスによって到達可能な隣接ドメインも PIM-SM を実行している場合、該当するドメインとの特定のトラフィックのやりとりを回避するように設定されています。そのため、該当するインターフェイスでの BSR メッセージの送受信を防ぐ目的で、そのインターフェイスをボーダー BSR として設定します。

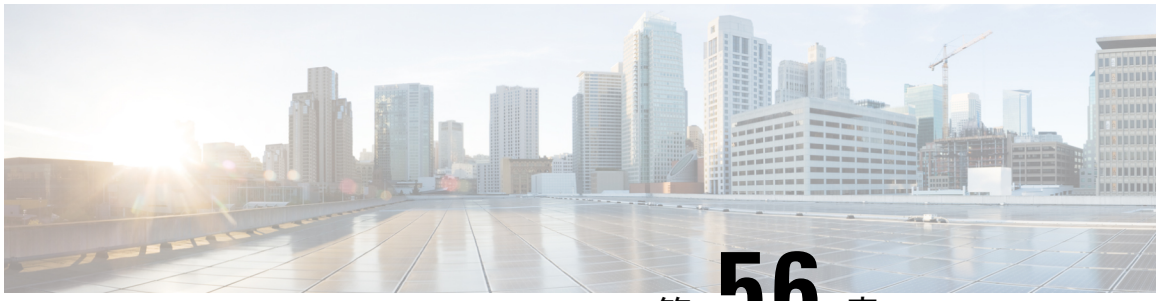
ナビゲーション パス

[ブートストラップルータの追加/編集（Add/Edit Bootstrap Router）] ダイアログボックスには、PIM ページ - ブートストラップ ルータ タブ （2701 ページ）からアクセスできます。

フィールド リファレンス

表 *703 : [ブートストラップ ルータの追加/編集] ダイアログボックス*

要素	説明
（任意）[BSRボーダー（BSR Border）] テーブルの [追加（Add）]	インターフェイスを追加し、ボーダー BSR として設定します。インターフェイスがボーダー BSR として設定されている場合、PIM BSR メッセージは送受信されません。



第 56 章

ファイアウォール デバイスでのルーティング ポリシーの設定

Security Manager のルーティング セクションには、セキュリティ アプライアンスのルーティング設定を定義および管理するためのページがあります。

この章は次のトピックで構成されています。

- [No Proxy ARP] の設定 （2703 ページ）
- BGP の設定 （2704 ページ）
- EIGRP の設定 （2751 ページ）
- ISIS の設定 （2772 ページ）
- BFD ルーティングの設定 （2803 ページ）
- OSPF の設定 （2812 ページ）
- キーチェーンの設定 （2849 ページ）
- OSPFv3 の設定 （2853 ページ）
- RIP の設定 （2879 ページ）
- スタティック ルートの設定 （2891 ページ）
- ASA ルーティング ポリシーのポリシーオブジェクトの設定 （2896 ページ）

[No Proxy ARP] の設定

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。Address Resolution Protocol（ARP）は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは、「この IP アドレスはだれですか」と質問する ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP を使用すると、デバイスは IP アドレスを持っていない場合でも、ARP 要求に対して MAC アドレスを返信します。別のホストの ARP プロキシとして機能することにより、ネットワーク トラフィックをプロキシ（この場合は、セキュリティ アプライアンス）に転送できます。アプライアンスを通過するトラフィックは、適切な宛先にルーティングされます。

たとえば、NAT を設定し、同じネットワーク上のグローバル アドレスをアプライアンスのインターフェイスとして指定すると、セキュリティ アプライアンスではプロキシ ARP が使用されます。アプライアンスがトラフィックを要求してから宛先グローバル アドレスにルーティングする場合にだけ、トラフィックは宛先ホストに到達できます。

デフォルトでは、プロキシ ARP はすべてのインターフェイスに対してイネーブルです。グローバル アドレスに対してプロキシ ARP をディセーブルにするには、[No Proxy ARP] ページを使用します。

- 1 つ以上のインターフェイスに対してプロキシ ARP をディセーブルにするには、[Interfaces] フィールドに名前を入力します。複数のインターフェイスを指定する場合は、カンマで区切ります。[Select] をクリックして、デバイス上に定義されているインターフェイスおよび Security Manager で定義されているインターフェイス ロールのリストから、インターフェイスを選択できます。

（注） ルーテッド モードで動作する ASA 8.4.2 以降のデバイスでは、手動 NAT ルールの出力インターフェイスで Proxy ARP をディセーブルできます。詳細については、テーブル 24-15 の「宛先インターフェイスで*ARP*をプロキシしない」を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから、[プラットフォーム（Platform）] > [ルーティング（Routing）] > [プロキシARPなし（No Proxy ARP）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [プロキシARPなし（No Proxy ARP）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- スタティック ルートの設定 （2891 ページ）
- RIP の設定 （2879 ページ）
- OSPF の設定 （2812 ページ）

BGP の設定

Border Gateway Protocol（BGP）は相互自律システム ルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

（注） BGP 設定は、ASA 9.2(1)+ でのみサポートされています。また、ASA 9.3(1) 以降、BGP は L2（EtherChannel タイプ）および L3（個別インターフェイスタイプ）クラスタリングモードでのみサポートされています。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [BGP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [BGP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

[BGP] ページには、ファイアウォールデバイス上の BGP ルーティングを設定するための 2 つのタブ付きパネルがあります。次に、BGP プロセスを設定するための基本的な手順を示します。

1. [BGP] ページの [GBPの有効化（Enable BGP）] チェックボックスをオンにして、BGP ルーティングプロセスをイネーブルにします。
2. [AS Number] フィールドに、BGP プロセスの自律システム（AS）番号を入力します。AS 番号内部には、複数の自律番号が含まれます。AS 番号には、1 ～ 4294967295 または 1.0 ～ 65535.65535 を指定できます。
3. [General] タブ （2709 ページ） で、次の手順を実行します。
   - （オプション）[受信されたルートのAS_PATH属性に含まれるAS番号の数を制限する（Limit the number of AS numbers in the AS_PATH attribute of received routes）] チェックボックスをオンにして、AS_PATH 属性の AS 番号の数を特定数に制限します。有効値は 1 ～ 254 です。
   - （オプション）[ネイバーの変更の記録（Log Neighbor Changes）] チェックボックスをオンにして、BGP ネイバーの変更（アップ状態またはダウン状態）およびリセットのロギングをイネーブルにします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
   - （オプション）[TCPパスMTUディスカバリを使用する（Use TCP path MTU discovery）] チェックボックスをオンにし、パス MTU ディスカバリ手法を使用して 2 つの IP ホスト間のネットワークパスにおける最大伝送単位（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。
   - （オプション）[Enable fast external failover] チェックボックスをオンにして、リンク障害の発生時に外部 BGP セッションをただちにリセットします。
   - （オプション）[最初のASをEBGPルートのピアのASとして実行（Enforce that first AS is peer's AS for EBGP routes）] チェックボックスをオンにして、その AS 番号を AS_path

属性の 1 つ目のセグメントとしてリストしていない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。

- （オプション）[Use dot notation for AS numbers] チェックボックスをオンにして、完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。
- BGPルーティングの最適なパスの選択プロセスに関連する設定を定義します（[General] タブ （2709 ページ）を参照）。
- [ネイバータイマー（Neighbor timers）] 領域でタイマー情報を指定します（ [General] タブ （2709 ページ）を参照）。
- （オプション）グレースフルリスタートを設定します（[General] タブ （2709ページ）を参照）。

4. [IPv4ファミリ（IPv4 Family）] タブで、[IPv4ファミリの有効化（Enable IPv4 Family）] チェックボックスをオンにし、提供されているタブを使用してIPv4アドレスファミリを設定します。詳細については、[IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）を参照してください。
5. [IPv6ファミリ（IPv6 Family）] タブで、[IPv6ファミリの有効化（Enable IPv6 Family）] チェックボックスをオンにし、提供されているタブを使用してIPv6アドレスファミリを設定します。詳細については、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）を参照してください。

関連項目

- BGP について （2706 ページ）

BGP について

BGP は相互自律システム ルーティング プロトコルです。自律システムとは、共通の管理下にあり、共通のルーティング ポリシーを使用するネットワークまたはネットワーク グループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

BGP を使用する状況

大学や企業などの顧客ネットワークでは、そのネットワーク内でルーティング情報を交換するために OSPF などの内部ゲートウェイ プロトコル（IGP）を通常使用しています。顧客は ISP に接続し、ISP は BGP を使用して顧客のルートと ISP のルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サー

ビス プロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGP ルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

BGP により学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。これらのプロパティは BGP 属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight：これは、シスコ定義の属性で、ルータに対してローカルです。[重要度（Weight）] 属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重要度（Weight）] 属性値が最も大きいルートが優先されます。
- Local preference：Local preference 属性は、ローカル AS からの出力点を選択するために使用されます。[重要度（Weight）] 属性とは異なり、[ローカル プリファレンス（Local preference）] 属性は、ローカル AS 全体に伝搬されます。AS からの出力点が複数ある場合は、[ローカル プリファレンス（Local preference）] 属性値が最も高い出力点が特定のルートの出力点として使用されます。
- Multi-exit discriminator：メトリック属性である Multi-exit discriminator（MED）は、メトリックをアドバタイズしている AS への優先ルートに関して、外部 AS への提案として使用されます。これが提案と呼ばれるのは、MED を受信している外部 AS がルート選択の際に他の BGP 属性も使用している可能性があるためです。MED メトリックが小さい方のルートが優先されます。
- Origin：Origin 属性は、BGP が特定のルートについてどのように学習したかを示します。Origin 属性は、次の 3 つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP：ルートは発信側 AS の内部にあります。この値は、ネットワーク ルータ コンフィギュレーション コマンドを使用して BGP にルートを挿入する場合に設定されます。
  - EGP：ルートは Exterior Border Gateway Protocol（EBGP）を使用して学習されます。
  - Incomplete：ルートの送信元が不明であるか、他の方法で学習されています。Incomplete の Origin は、ルートが BGP に再配布されるときに発生します。
- AS_path：ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティング テーブルにインストールされます。
- Next hop：EBGP の Next-hop 属性は、アドバタイズしているルータに到達するために使用される IP アドレスです。EBGP ピアの場合、ネクスト ホップ アドレスは、ピア間の接続

の IP アドレスです。IBGP の場合、EBGP のネクスト ホップ アドレスがローカル AS に伝送されます。

- Community：Community 属性は、ルーティングの決定（承認、優先度、再配布など）を適用できる宛先をグループ化する方法、つまりコミュニティを提供します。ルート マップは、[コミュニティ（Community）] 属性を設定するために使用されます。定義済みの [コミュニティ（Community）] 属性は次のとおりです。
  - no-export：EBGP ピアにこのルートをアドバタイズしません。
  - no-advertise：どのピアにもこのルートをアドバイタイズしません。
  - internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGP は、異なる送信元から同じルートの複数のアドバタイズメントを受信する場合があります。BGP はベスト パスとして 1 つのパスだけを選択します。このパスを選択すると、BGP は IP ルーティング テーブルに選択したパスを格納し、そのネイバーにパスを伝搬します。BGP は次の基準を使用して（示されている順序で）、宛先へのパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、この更新はドロップされます。
- ウェイトが最大のパスが優先されます。
- ウェイトが同じである場合、ローカルの優先順位が最大のパスが優先されます。
- ローカルの優先順位が同じである場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_path が最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じである場合、起点タイプが最下位のパス（[IGP] は [EGP] よりも低く、[EGP] は [不完全（Incomplete）] よりも低い）が優先されます。
- 起点コードが同じである場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じである場合、内部パスより外部パスが優先されます。
- それでもパスが同じである場合、最も近い IGP ネイバーを経由するパスが優先されます。
- 両方のパスが外部の場合、最初に受信したパス（最も古いパス）が優先されます。
- BGP ルータ ID で指定された、IP アドレスが最も小さいパスが優先されます。
- 送信元またはルータ ID が複数のパスで同じである場合、クラスタ リストの長さが最小のパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

[General] タブ

[全般（General）] タブを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの BGP 設定を構成します。

ナビゲーション パス

[ネイバー（Neighbors）] タブには、[OSPF] ページからアクセスできます（BGP の設定 （2704 ページ）を参照）。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）

フィールド リファレンス

表 *704 : [General] タブ*

要素	説明
[受信されたルートのAS_PATH属性に含まれるAS番号の数（Limit the number of AS numbers in AS_PATH attribute of received routes）]	AS_PATH 属性に含まれる AS 番号の数を特定の数に制限します。有効値は 1 ～ 254 です。
ネイバーの変更を記録（Log Neighbor Changes）	BGP ネイバーの変更（アップまたはダウン）のロギングを有効にします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
[TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）]	パス MTU ディスカバリ手法を使用して、2 つの IP ホスト間のネットワークパスにおける最大伝送ユニット（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。
[高速外部フェールオーバーの有効化（Enable fast external failover）]	リンク障害の発生時、外部 BGP セッションを即時にリセットします。

要素	説明
[最初のASをEBGPルートのピアのASとして実行（Enforce that the first AS is peer's AS for EBGP routes）]	AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストに表示していない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。
[AS番号にドット表記を使用（Use dot notation for AS numbers）]	完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。
[ベストパスの選択（Best Path Selection）]	
Default local preference	0 ～ 4294967295 の数値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバーに送信されます。
[異なるネイバーのMEDの比較を許可（Allow comparing MED from different neighbors）]	異なる自律システムにあるネイバーからのパスの Multi-Exit 識別子（MED）の比較を許可します。
[同一のBGPパスのルータIDを比較（Compare Router-id for identical EBGP paths）]	ベストパスの選択プロセス中に外部 BGP ピアから受信した類似パスを比較し、ベストパスをルータ ID が最も小さいルートに切り替えます。
[隣接ASからアドバタイズされたパスの間で最適なMEDパスを選択（Pick the best MED path among paths advertised from the neighboring AS）]	コンフェデレーション ピアから学習した複数のパスの間で MED 比較をイネーブルにします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。
[欠落MEDを最低優先度として処理（Treat missing MED as the least preferred one）]	欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。
[ネイバータイマー（Neighbor Timers）]	
[キープアライブ間隔（Keepalive Interval）]	キープアライブメッセージを送信しなかった場合に、その後 BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。

要素	説明
保留時間（Hold Time）	BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。デフォルト値は 180 秒です。
Min Hold Time	（任意）BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する最小時間間隔を入力します。0 ～ 65535 の値を指定します。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタモードで使用） （ASA 9.3.1 以降のみ）	
グレースフル リスタートをイネーブルにします。	スイッチオーバー後のルーティングフラップを ASA ピアが回避できるようにします。
再起動時間	BGP オープンメッセージが受信される前に、ASA ピアが古いルートを削除するまでの待機時間を指定します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。
[Stalepath時間（Stalepath Time）]	再起動する ASA から End Of Record（EOR）メッセージを受信した後、ASA が古いルートを削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

[IPv4ファミリ（IPv4 Family）] タブ

[BGP] ページの [IPv4ファミリ（IPv4 Family）] タブを使用して、BGP の IPv4 設定を有効にして構成します。

ナビゲーション パス

[BGP] ページから [IPv4ファミリ（IPv4 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2704 ページ）を参照してください。

関連項目

- BGP について （2706 ページ）
- [General] タブ （2709 ページ）

フィールド リファレンス

表 *705 : IPv4* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
IPv4ファミリの有効化（Enable IPv4 Family）	標準の IPv4 アドレスプレフィックスを使用するルーティングセッションの設定を有効にします。
一般	このパネルを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの一般的な IPv4 設定を設定します。これらの定義の詳細については、IPv4 Family - [全般（General）] タブ （2713 ページ）を参照してください。
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）を参照してください。
フィルタリング	このパネルを使用して、着信 BGP アップデートで受信したルータまたはネットワークをフィルタ処理します。これらの定義の詳細については、[Add Filter]/[Edit Filter] ダイアログボックス （2717 ページ）を参照してください。
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）を参照してください。
ネットワーク	このパネルを使用して、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2728 ページ）を参照してください。
再配布	Use this panel to define the conditions for redistributing routes from another routing domain into BGP. これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （2729 ページ）を参照してください。
ルートの挿入	このパネルを使用して、条件に応じて BGP ルーティングテーブルに注入されるルートを定義します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2730 ページ）を参照してください。

IPv4 Family - [全般（General）] タブ

[IPv4 ファミリ] - [全般（General）] タブを使用して、全般的な IPv4 設定を行います。

ナビゲーション パス

[全般（General）] タブには、[BGP] ページの [IPv4ファミリ（IPv4 Family）] タブからアクセスできます。[IPv4ファミリ（IPv4 Family）] タブの詳細については、[IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）を参照してください。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）

フィールド リファレンス

表 *706 : IPv4 Family - [全般（General）] タブ*

要素	説明
ルータ ID（Router ID）	単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（IP アドレスを選択すると、[アドレス（address）] フィールドが表示されます。） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルートID（Router ID）] フィールドに IPv4 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）] または [クラスタプール（Cluster Pool）] を選択します。（[クラスタプール（ Cluster Pool）] を選択すると、[IPv4プールオブジェクトID（ IPv4 Pool object ID）] フィールドが表示されます）。 [クラスタプール（Cluster Pool）] を選択した場合は、ルータの ID アドレスを提供する IPv4 プールオブジェクトの名前を入力または選択します。詳細については、[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス （407 ページ）を参照してください。

要素	説明
学習したルートマップ	ルートマップオブジェクトの名前を入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
スキャン間隔	ネクストホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。
ルートと同期	
デフォルトルートの生成	（任意）デフォルトルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティングプロセスを設定します。
サブネットルートをネットワークレベルのルートに集約します。	（任意）サブネットルートのネットワークレベルルートへの自動集約を設定します。
非アクティブのルートのアドバタイズ	（任意）ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。
BGP と内部ゲートウェイプロトコル（IGP）システム間の同期	BGP と内部ゲートウェイプロトコル（IGP）システム間の同期をイネーブルにします。Cisco IOS ソフトウェアが IGP を待機せずにネットワークルートをアドバタイズできるようにするには、このオプションの選択を解除します。 通常、ルートがローカルであるか IGP に存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。デフォルトでは BGP と IGP 間の同期はオフになっており、Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようになっています。この機能により、自律システム内のルータおよびアクセス サーバーは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。自律システム内のルータが BGP を実行していない場合は、synchronization を使用します。
IBGPのIGPへの再配布	（任意）IS-IS や OSPF などの内部ゲートウェイプロトコル（IGP）への iBGP の再配布を設定します。
Administrative Route Distances	

要素	説明
外部	外部 BGP ルートのアドミニストレーティブ ディスタンスを指定します。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 20 です。
内線	内部 BGP ルートのアドミニストレーティブ ディスタンスを指定します。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。
ローカル（Local）	ローカルの BGP ルートのアドミニストレーティブ ディスタンスを指定します。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。
ネクスト ホップ	
アドレストラッキングの有効化	（任意）BGP ネクストホップ アドレス トラッキングをイネーブルにします。
遅延間隔	ルーティングテーブルにインストールされている更新済みのネクストホップルートのチェック間の遅延間隔を指定します。
マルチパス上のフォワードパケット	
パス数	（任意）ルーティングテーブルにインストールできる外部 BGP ルートの最大数を指定します。
IBGP のパス数	（任意）ルーティングテーブルにインストールできる内部 BGP ルートの最大数を指定します。

[集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

ナビゲーション パス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）からアクセスできます。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）

- IPv4 Family - [全般（General）] タブ （2713 ページ）
- [Add Filter]/[Edit Filter] ダイアログボックス （2717 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2728 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2729 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2730 ページ）

フィールド リファレンス

表 *707 : [*集約アドレスの追加/編集（***Add/Edit Summary Address***）*]* ダイアログボックス

要素	説明
ネットワーク	IP アドレスを入力するか、目的のネットワーク/ホストオブジェクトを入力または選択します。
属性マップ	（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
アドバタイズマップ（Advertise Map）	（オプション）AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルートマップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

要素	説明
抑制マップ（Suppress Map）	（オプション）抑制するルートの選択に使用されるルートマップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
AS 設定パス情報の生成（Generate AS Set Path Information）	自律システム設定パス情報の生成を有効にします。
アップデートからのすべてのより具体的なルートをフィルタ処理（Filter all more-specific routes from updates）	アップデートからのすべてのより具体的なルートをフィルタ処理します。

[Add Filter]/[Edit Filter] ダイアログボックス

[フィルタの追加（Add Filter）]/[フィルタの編集（Edit Filter）] ダイアログボックスを使用して、着信 BGP アップデートで受信したルータまたはネットワークをフィルタ処理します。

ナビゲーション パス

[フィルタの追加（Add Filter）]/[フィルタの編集（Edit Filter）] ダイアログボックスには、[IPv4 ファミリ（IPv4 Family）] タブ （2711 ページ）からアクセスできます。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv4ファミリ（IPv4 Family）] タブ：[全般（General）]タブ （2777 ページ）
- [集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）

- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス（2749 ページ）

フィールド リファレンス

表 *708 : [Add Filter]/[Edit Filter]* ダイアログボックス

要素	説明
ACL	受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。
方向	[Direction] ドロップダウン リストから方向を選択します。方向は、フィルタを着信アップデートに適用するか、または発信アップデートに適用するかを指定します。
プロトコル	[なし（None）]、[BGP]、[接続（Connected）]、[EIGRP]、[OSPF]、[RIP]、または [静的（Static）] のルーティングプロセスのうち、フィルタ処理するものを選択します。
AS 番号（AS Number）	BGP ルーティングプロセスの自律システム番号を表示します。この値は、BGP ページで指定されます（ BGP の設定 （2704 ページ）を参照）。
プロセス ID（Process ID）	ルーティングプロセスの識別子を入力します。EIGRP および OSPF ルーティングプロトコルに適用されます。

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスを使用して、BGP ネイバーとネイバーの設定を定義します。

ナビゲーション パス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスには、 [IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）からアクセスできます。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- IPv4 Family - [全般（General）] タブ （2713 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （2715 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2728 ページ）

- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2729 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス（2730 ページ）

フィールド リファレンス

表 *709 : [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス*

要素	説明
一般	
[IPアドレス（IP Address）]	BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。
リモート AS	BGP ネイバーが属する自律システムを入力します。
アドレスファミリの有効化（Enable Address Family）	（任意）BGP ネイバーとの通信を有効にします。
ネイバーを管理的にシャットダウンする（Shutdown neighbor administratively）	（任意）ネイバーまたはピアグループを無効にします。
ネイバーごとのBGPグレースフルリスタートの設定（Configure Graceful Restart per neighbor） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能の設定を有効にします。このオプションを選択した後、[グレースフルリスタート（フェールオーバーまたはスパンドクラスタモードで使用）（Graceful Restart (Use in failover or spanned cluster mode) ）] オプションを使用して、このネイバーに対してグレースフルリスタートを有効にするか、無効にするかを指定する必要があります。
グレースフルリスタート（フェールオーバーまたはスパンドクラスタモードで使用）（Graceful Restart (Use in failover or spanned cluster mode) ） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能を有効にします。
説明	（任意）BGP ネイバーの説明を入力します。
フォールオーバーBFD（fall-over BFD）	（任意）BGP ネイバーのフォールオーバーに対する BFD サポートを有効にします。
BFDホップ（BFD-Hop）	（任意）BFD の送信元と宛先の間に単一の IP ホップがあるか、複数の IP ホップがあるかを指定します。

要素	説明
フィルタリング	
アクセスリストを使用してルートをフィルタ処理する（Filter routes using an access list）	（任意）適切な着信または発信アクセス制御リストを入力または選択して、BGP ネイバー情報を配布します。
ルートマップを使用してルートをフィルタ処理する（Filter routes using route map）	（任意）適切な着信または発信ルートマップを入力または選択して、着信または発信ルートにルートマップを適用します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
プレフィックスリストを使用してルートをフィルタ処理する（Filter routes using a Prefix list）	（任意）適切な着信または発信プレフィックスリストを入力または選択して、BGP ネイバー情報を配布します。 ヒント [選択（Select）] をクリックして、プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト セレクタを開きます。プレフィックス リスト オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
ASパスフィルタを使用してルートをフィルタ処理する（Filter routes using AS Path filter）	（任意）適切な着信または発信 AS パスフィルタを入力または選択して、BGP ネイバー情報を配布します。 ヒント [選択（Select）] をクリックして、AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。AS パスオブジェクトセレクタから新しい AS パスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924 ページ）を参照してください。

要素	説明

ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）	（任意）選択して、ネイバーから受信できるプレフィックスの数を制御します。
	• [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
	• [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。
	• （任意）[ピアから受信したプレフィックスの制御（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
	  • プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] を選択します。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
	  • 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning message when prefix limit is exceeded）] を選択します。この場合、BGP ネイバーは終了しません。

ルート	
アドバタイズメント間隔	BGP ルーティング更新が送信される最小間隔（秒単位）を入力します。有効な値は、1 ～ 600 です。
アウトバウンドルーティング更新からプライベート AS 番号を削除します。	（任意）プライベート AS 番号をアウトバウンドルートでアドバタイズしないようにします。

要素	説明
デフォルトルートの生成（Generate Default route）	（任意）選択して、ネイバーへのデフォルトルート 0.0.0.0 の送信をローカルルータに許可して、デフォルトルートとして使用します。[ルート マップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

ルートの条件付きアドバタイズ（Conditionally Advertised Routes）	（任意）条件付きでアドバタイズされるルートを追加または編集するには、[行の追加（Add Row）]（+）ボタンをクリックするか、テーブル内の行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。
	[アドバタイズ対象ルートの追加/編集（Add/Edit Advertised Route）] ダイアログボックスで、次の手順を実行します。
	• [選択（Select）] をクリックして [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。このセレクタから、存在マップまたは非存在マップの条件が満たされた場合にアドバタイズされるルートマップを選択できます。ルートマップの詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
	• 次のいずれかを実行します。
	  • [存在マップの設定（Set Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からルートマップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。
	  • [非存在マップ（Non-Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からルートマップを選択します。このルート マップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

要素	説明
タイマー	
BGPピアにタイマーを設定する（Set timers for the BGP peer）	（任意）選択して、キープアライブ頻度、ホールド時間、最小ホールド時間を設定します。
キープアライブ間隔（Keepalive Interval）	ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
保留時間（Hold Time）	キープアライブメッセージを受信できない状態が継続して、ピアがデッドであるとASAが宣言するまでの間隔（秒単位）を入力します。有効な値は、0～65535 です。デフォルト値は180秒です。
Min Hold Time	（任意）キープアライブメッセージを受信できずに、ピアがデッドであるとASAが宣言するまでの最小間隔（秒単位）を入力します。有効な値は、0～65535 です。デフォルト値は0秒です。
詳細設定（Advanced）	
Enable Authentication	（任意）選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。 • [暗号化を有効にする（Enable Encryption）] ドロップダウンリストから暗号化タイプを選択します。 • パスワードを [Password] フィールドに入力します。[Confirm] フィールドにパスワードを再入力します。 パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字まで指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。 （注） 数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。
コミュニティ属性をこのネイバーに送信します	（任意）コミュニティ属性をBGPネイバーに送信する必要があることを指定します。
ネイバーのネクストホップとしてASAを使用する（Use ASA as next hop for neighbor）	（任意）選択して、BGPスピーキングネイバーまたはピアグループのネクストホップとしてルータを設定します。

要素	説明
接続検証の無効化（Disable connection verification）	（任意）選択して、シングルホップで到達可能だが、ループバックインターフェイス上に設定されている、あるいは直接接続されない IP アドレスで設定されている eBGP ピアリングセッションの接続検証プロセスを無効にします。 このコマンドが必要になるのは、neighbor ebgp-multihop コマンドで TTL 値を 1 に設定している場合だけです。シングル ホップ eBGP ピアのアドレスに到達できる必要があります。neighbor update-source コマンドを使用して、BGP ルーティングプロセスでピアリングセッションにループバック インターフェイスを使用できるように設定する必要があります。 オフ（デフォルト）にすると、シングルホップ eBGP ピアリング セッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリングセッションは確立されません。
直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）	選択して、直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、そのピアへの BGP 接続を試みます。 （オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。 （注） この機能は、シスコ テクニカル サポート担当者の指示のもとでのみ使用してください。ルートが一定でないことによるループの発生を回避するために、マルチホップピアのルートがデフォルトルート（0.0.0.0）だけの場合はマルチホップは確立されません。

要素	説明
ネイバーへのTTLホップ数を制限する（Limit number of TTL hops to neighbor）	

要素	説明
	BGP ピアリングセッションを保護するには、このオプションを選択します。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。 この機能は、CPU利用率に基づく攻撃からBGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケット ヘッダーの送信元と宛先のIPアドレスを偽造した大量のIPパケットでネットワークをあふれさせてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。 この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。 この機能は、参加している各ルータで設定する必要があります。この機能では、eBGPセッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。この機能がイネーブルの場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能はBGP ピアリング セッションには影響しません。この機能がイネーブルの場合でも、キープアライブ パケットを受信しなければピアリング セッションは期限切れになります。受信パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージプロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。 この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するようにhop-countの値を正確に設定する必要があります。また、この機能をマルチホップ ピアリング セッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。 このコマンドの設定には、次の制限が適用されます。 • この機能は、内部BGP（iBGP）ピアではサポートされません。 • 大きい直径のマルチホップ ピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定されたBGPルータに対するCPU利用率に基づく攻撃の場合は、影

要素	説明
	響を受けたピアリング セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。 • この機能は、ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、送信元ネットワークと宛先ネットワークの間のネットワーク セグメント上のピアも含まれます。
TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）	（任意）選択して、BGP セッションの TCP トランスポートセッションを有効にします。
TCPトランスポートモード（TCP transport mode）	ドロップダウンリストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。
重量	（任意）BGP ネイバー接続の重みを入力します。
BGPバージョン（BGP Version）	ドロップダウンリストから、ASA が受け入れる BGP バージョンを選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン 4 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。
移行 （注） このカスタマイズは、AS 移行にのみ使用し、移行完了後に削除する必要があります。この手順は、経験豊富なネットワークオペレータのみ実行する必要があります。不適切な設定によってルーティング ループが作成される可能性があります。	
ネイバーから受信したルートのAS番号をカスタマイズする（Customize the AS number for routes received from the neighbor）	（任意）選択して、eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズします。
ローカルAS番号（Local AS Number）	ローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。
ネイバーから受信したルートの先頭にローカルAS番号を追加しない（Do not prepend local AS number to routes received from neighbor）	（任意）選択して、ローカル AS 番号が eBGP ピアから受信したルートの先頭に追加されないようにします。

要素	説明
実際のAS番号をネイバーから受信したルート内のローカルAS番号と置き換える（Replace real AS number with local AS number in routes received from neighbor）	（任意）選択して、実際の自律システム番号をeBGPアップデートのローカル自律システム番号で置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。
ネイバーから学習したルートで実際のAS番号かローカルAS番号を受け入れる（Accept either real AS number or local AS number in routes received from neighbor）	（任意）（ローカル BGP ルーティングプロセスの）実際の自律システム番号を使用するか、ローカル自律システム番号を使用してピアリングセッションを確立するように eBGP ネイバーを設定します。

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスを使用して、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義します。

ナビゲーション パス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）からアクセスできます。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- IPv4 Family - [全般（General）] タブ （2713 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （2715 ページ）
- [Add Filter]/[Edit Filter] ダイアログボックス （2717 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2729 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2730 ページ）

フィールド リファレンス

表 *710 : [*ネットワークの追加/編集（*Add/Edit Network*）*]* ダイアログボックス

要素	説明
ネットワーク	BGP ルーティングプロセスでアドバタイズするネットワークを指定します。
ルート マップ	（任意）アドバタイズされるネットワークをフィルタ処理するために調べる必要があるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

[Add Redistribution]/[Edit Redistribution] ダイアログボックス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスを使用して、別のルーティングドメインから BGP にルートを再配布する条件を定義します。

ナビゲーション パス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）からアクセスできます。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- IPv4 Family - [全般（General）] タブ （2713 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （2715 ページ）
- [集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2728 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2730 ページ）

フィールド リファレンス

表 711 : [Add Redistribution]/[Edit Redistribution] ダイアログボックス

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。
プロセス ID（Process ID）	ルーティングプロセスの識別子を入力します。EIGRP および OSPF ルーティングプロトコルに適用されます。
メトリック（Metric）	（オプション）：再配布されているルートのメトリックを入力します。
ルート マップ	再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
一致（Match）	1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。 • 内線 • 外部 1 • 外部 2 • NSSA 外部 1 • NSSA 外部 2

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスを使用して、条件に応じて BGP ルーティングテーブルに挿入されるルートを定義できます。

ナビゲーション パス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスには、[IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）からアクセスできます。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- IPv4 Family - [全般（General）] タブ （2713 ページ）
- [集約アドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （2715 ページ）
- [Add Filter]/[Edit Filter] ダイアログボックス （2717 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2728 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2729 ページ）

フィールド リファレンス

表 *712 : [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス*

要素	説明
インジェクトマップ	ローカル BGP ルーティングテーブルに挿入するプレフィックスを指定するルートマップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
存在マップ	BGP スピーカーが追跡するプレフィックスを含むルートマップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

要素	説明
挿入されたルートは、集約ルートの属性を継承します。	挿入されたルートが集約ルートの属性を継承するように設定します。

[IPv6ファミリ（IPv6 Family）] タブ

[BGP] ページの [IPv6 ファミリ（IPv6 Family）] タブを使用して、BGP の IPv6 設定を有効にして設定します。

ナビゲーション パス

[BGP] ページから [IPv6 ファミリ（IPv6 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2704 ページ）を参照してください。

関連項目

- BGP について （2706 ページ）
- [General] タブ （2709 ページ）

フィールド リファレンス

表 *713 : IPv6* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
[IPv6 ファミリの有効化（Enable IPv6 Family）]	標準の IPv6 アドレスプレフィックスを使用するルーティングセッションの設定を有効にします。
一般	このパネルを使用して、一般的な IPv6 設定を指定します。これらの定義の詳細については、[IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブ （2733 ページ）を参照してください。
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）を参照してください。

要素	説明
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）を参照してください。
ネットワーク	このパネルを使用して、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）を参照してください。
再配布	このパネルを使用して、別のルーティングドメインから BGP にルートを再配布する条件を定義します。これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）を参照してください。
ルートの挿入	このパネルを使用して、条件に応じて BGP ルーティングテーブルに注入されるルートを定義します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2749 ページ）を参照してください。

[IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブ

全般的な IPv6 設定を指定するには、[IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブを使用します。

ナビゲーション パス

[全般（General）] タブには、[BGP] ページの [IPv6ファミリ（IPv6 Family）] タブからアクセスできます。[IPv6ファミリ（IPv6 Family）] タブの詳細については、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）を参照してください。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）

フィールド リファレンス

表 *714 : [IPv6* ファミリ（*IPv6 Family*）*]*：*[*全般（*General*）*]* タブ

要素	説明
スキャン間隔	ネクストホップの検証用に BGP ルータのスキャン間隔（秒）を入力します。有効な値は 5 ～ 60 秒です。デフォルト値は 60 です。
ルートと同期	

要素	説明
デフォルトルートの生成	（オプション）デフォルトルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティングプロセスを設定します。
非アクティブのルートのアドバタイズ	（任意）ルーティング情報ベース（RIB）にインストールされていないルートをアドバタイズします。
BGP と内部ゲートウェイプロトコル（IGP）システム間の同期	BGP と内部ゲートウェイプロトコル（IGP）システム間の同期をイネーブルにします。Cisco IOS ソフトウェアが IGP を待機せずにネットワークルートをアドバタイズできるようにするには、このオプションの選択を解除します。 通常、ルートがローカルであるかIGPに存在する場合を除き、BGP スピーカーは外部ネイバーにルートをアドバタイズしません。デフォルトでは BGP と IGP 間の同期はオフになっており、Cisco IOS ソフトウェアが IGP を待機せずにネットワーク ルートをアドバタイズできるようになっています。この機能により、自律システム内のルータおよびアクセス サーバーは、BGP が他の自律システムでルートを使用可能にする前にルートを確保できるようになります。自律システム内のルータが BGP を実行していない場合は、synchronization を使用します。
[iBGP の IGP への再配布（Redistribute iBGP into an IGP）]（再配布されるプレフィックスの数を制限するため、フィルタリングを使用します）	（任意）IS-IS や OSPF などの内部ゲートウェイプロトコル（IGP）への iBGP の再配布を設定します。
Administrative Route Distances	
外部	外部 BGP ルートのアドミニストレーティブディスタンスを指定します。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 20 です。
内線	内部 BGP ルートのアドミニストレーティブディスタンスを指定します。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。
ローカル（Local）	ローカルの BGP ルートのアドミニストレーティブディスタンスを指定します。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。デフォルト値は 200 です。

要素	説明
マルチパス上のフォワードパケット	
パス数	（任意）ルーティングテーブルにインストール可能な Border Gateway Protocol ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。
IBGP のパス数	（任意）ルーティングテーブルにインストール可能な並行内部ボーダー ゲート ウェイプロトコル（IBGP）ルートの最大数を指定します。値の範囲は 1 ～ 8 です。デフォルト値は 1 です。

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスで、特定のルートの 1 つのルートへの集約を定義します。

ナビゲーション パス

[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （2733 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2749 ページ）

フィールド リファレンス

表 *715 : [*集約アドレスの追加/編集（*Add/Edit Aggregate Address*）*]* ダイアログボックス

要素	説明
ネットワーク	IP アドレスを入力するか、目的のネットワーク/ホストオブジェクトを入力または選択します。

要素	説明
属性マップ	（オプション）集約ルートの属性の設定に使用されるルート マップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
アドバタイズマップ（Advertise Map）	（オプション）AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルートマップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
抑制マップ（Suppress Map）	（オプション）抑制するルートの選択に使用されるルートマップを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
AS 設定パス情報の生成（Generate AS Set Path Information）	自律システム設定パス情報の生成を有効にします。
アップデートからのすべてのより具体的なルートをフィルタ処理（Filter all more-specific routes from updates）	アップデートからのすべてのより具体的なルートをフィルタ処理します。

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスを使用して、BGP ネイバーとネイバーの設定を定義します。

ナビゲーション パス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （2733 ページ）
- [集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2749 ページ）

フィールド リファレンス

表 *716 : [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス*

要素	説明
一般	
[IPアドレス（IP Address）]	BGP ネイバーの IP アドレスを入力します。この IP アドレスは、BGP ネイバー テーブルに追加されます。
リモート AS	BGP ネイバーが属する自律システムを入力します。
アドレスファミリの有効化（Enable Address Family）	（任意）BGP ネイバーとの通信を有効にします。
ネイバーを管理的にシャットダウンする（Shutdown neighbor administratively）	（任意）ネイバーまたはピアグループを無効にします。

要素	説明
ネイバーごとのBGPグレースフルリスタートの設定（Configure Graceful Restart per neighbor） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能の設定を有効にします。このオプションを選択した後、[グレースフルリスタート（フェールオーバーまたはスパンドクラスタモードで使用）（Graceful Restart (Use in failover or spanned cluster mode)）] オプションを使用して、このネイバーに対してグレースフルリスタートを有効にするか、無効にするかを指定する必要があります。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタモードで使用） （ASA 9.3.1 以降のみ）	（任意）ネイバーのボーダー ゲートウェイ プロトコル（BGP）グレースフルリスタート機能を有効にします。
説明	（任意）BGP ネイバーの説明を入力します。
フォールオーバーBFD（fall-over BFD）	(オプション) BGP ネイバーのフォールオーバーに対する BFD サポートを有効にします。
BFDホップ（BFD-Hop）	（任意）BFD の送信元と宛先の間に単一の IP ホップがあるか、複数の IP ホップがあるかを指定します。
フィルタリング	
アクセスリストを使用してルートをフィルタ処理する（Filter routes using an access list）	（任意）適切な着信または発信アクセス制御リストを入力または選択して、BGP ネイバー情報を配布します。
ルートマップを使用してルートをフィルタ処理する（Filter routes using route map）	（任意）適切な着信または発信ルートマップを入力または選択して、着信または発信ルートにルートマップを適用します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

要素	説明
プレフィックスリストを使用してルートをフィルタ処理する（Filter routes using a Prefix list）	（任意）適切な着信または発信プレフィックスリストを入力または選択して、BGP ネイバー情報を配布します。 ヒント [選択（Select）] をクリックして、プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト セレクタを開きます。オブジェクト プレフィックス リスト オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
ASパスフィルタを使用してルートをフィルタ処理する（Filter routes using AS Path filter）	（任意）適切な着信または発信ASパスフィルタを入力または選択して、BGP ネイバー情報を配布します。 ヒント [選択（Select）] をクリックして、AS パスオブジェクトを選択できる AS パスオブジェクト セレクタを開きます。AS パスオブジェクト セレクタから新しい AS パスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924 ページ）を参照してください。

要素	説明

ネイバーから許可されるプレフィックスの数を制限する（Limit the number of prefixes allowed from the neighbor）	（任意）選択して、ネイバーから受信できるプレフィックスの数を制御ます。
	• [最大プレフィックス数（Maximum Prefixes）] フィールドに、特定のネイバーからの許可される最大プレフィックス数を入力します。
	• [しきい値レベル（Threshold Level）] フィールドに、ルータが警告メッセージの生成を開始するパーセンテージ（最大数に対する割合）を入力します。有効な値は 1 ～ 100 の整数です。デフォルト値は 75 です。
	• （任意）[ピアから受信したプレフィックスの制御（Control prefixes received from the peer）] チェックボックスをオンにし、ピアから受信したプレフィックスに対する追加の制御を指定します。次のいずれかを実行します。
	  • プレフィックス数の制限値に到達したときに BGP ネイバーを停止するには、[プレフィックス数の制限値を超えたときにピアリングを停止する（Terminate peering when prefix limit is exceeded）] を選択します。[Restart interval] フィールドで、BGP ネイバーが再起動するまでの時間を指定します。
	  • 最大プレフィックス数の制限値を超えたときにログメッセージを生成するには、[プレフィックス数の制限値を超えたときに警告メッセージのみを表示する（Give only warning message when prefix limit is exceeded）] を選択します。この場合、BGP ネイバーは終了しません。

ルート	
アドバタイズメント間隔	BGP ルーティング更新が送信される最小間隔（秒単位）を入力します。有効な値は、1 ～ 600 です。
アウトバウンドルーティング更新からプライベート AS 番号を削除します。	（任意）プライベート AS 番号をアウトバウンドルートでアドバタイズしないようにします。

要素	説明
デフォルトルートの生成（Generate Default route）	（任意）選択して、ネイバーへのデフォルトルート 0.0.0.0 の送信をローカルルータに許可して、デフォルトルートとして使用します。[ルート マップ（Route map）] フィールドで、ルート 0.0.0.0 が条件に応じて注入されるように許可するルート マップを入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897ページ）を参照してください。
ルートの条件付きアドバタイズ（Conditionally Advertised Routes）	（任意）条件付きでアドバタイズされるルートを追加または編集するには、[行の追加（Add Row）]（+）ボタンをクリックするか、テーブル内の行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。 [アドバタイズ対象ルートの追加/編集（Add/Edit Advertised Route）] ダイアログボックスで、次の手順を実行します。 • [選択（Select）] をクリックして [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。このセレクタから、存在マップまたは非存在マップの条件が満たされた場合にアドバタイズされるルートマップを選択できます。ルートマップの詳細については、ルートマップオブジェクトについて （2897ページ）を参照してください。 • 次のいずれかを実行します。 • [存在マップの設定（Set Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）]からルートマップを選択します。このルートマップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。 • [非存在マップ（Non-Exist Map）] を選択し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）]からルートマップを選択します。このルートマップは、advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較されます。

要素	説明
タイマー	
BGPピアにタイマーを設定する（Set timers for the BGP peer）	（任意）選択して、キープアライブ頻度、ホールド時間、最小ホールド時間を設定します。
キープアライブ間隔（Keepalive Interval）	ASA がキープアライブ メッセージをネイバーに送信する頻度（秒）を有効な値は、0 ～ 65535 です。デフォルト値は 60 秒です。
保留時間（Hold Time）	キープアライブメッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの間隔（秒単位）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 180 秒です。
Min Hold Time	（任意）キープアライブメッセージを受信できずに、ピアがデッドであると ASA が宣言するまでの最小間隔（秒単位）を入力します。有効な値は、0 ～ 65535 です。デフォルト値は 0 秒です。
詳細設定（Advanced）	
Enable Authentication	（任意）選択して、2 つの BGP ピア間の TCP 接続で MD5 認証を有効にします。 • [暗号化を有効にする（Enable Encryption）] ドロップダウンリストから暗号化タイプを選択します。 • パスワードを [Password] フィールドに入力します。[Confirm] フィールドにパスワードを再入力します。 パスワードは大文字と小文字を区別し、service password-encryption コマンドが有効な場合は最大 25 文字、service password-encryption コマンドが有効でない場合は最大 81 文字まで指定できます。最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。 （注） 数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。
コミュニティ属性をこのネイバーに送信します	（任意）コミュニティ属性を BGP ネイバーに送信する必要があることを指定します。
ネイバーのネクストホップとしてASAを使用する（Use ASA as next hop for neighbor）	（任意）選択して、BGP スピーキングネイバーまたはピアグループのネクストホップとしてルータを設定します。

要素	説明
接続検証の無効化（Disable connection verification）	（任意）選択して、シングルホップで到達可能だが、ループバックインターフェイス上に設定されている、あるいは直接接続されない IP アドレスで設定されている eBGP ピアリングセッションの接続検証プロセスを無効にします。 このコマンドが必要になるのは、neighbor ebgp-multihop コマンドで TTL 値を 1 に設定している場合だけです。シングル ホップ eBGP ピアのアドレスに到達できる必要があります。neighbor update-source コマンドを使用して、BGP ルーティングプロセスでピアリングセッションにループバック インターフェイスを使用できるように設定する必要があります。 オフ（デフォルト）にすると、シングルホップ eBGP ピアリング セッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリングセッションは確立されません。
直接接続されていないネイバーとの接続を許可する（Allow connections with neighbor that is not directly connected）	選択して、直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、そのピアへの BGP 接続を試みます。 （オプション）[TTL hops] フィールドに存続可能時間を入力します。有効な値は、1 ～ 255 です。 （注） この機能は、シスコテクニカルサポート担当者の指示のもとでのみ使用してください。ルートが一定でないことによるループの発生を回避するために、マルチホップピアのルートがデフォルトルート（0.0.0.0）だけの場合はマルチホップは確立されません。

要素	説明
ネイバーへのTTLホップ数を制限する（Limit number of TTL hops to neighbor）	

要素	説明
	BGP ピアリングセッションを保護するには、このオプションを選択します。[TTL hops] フィールドに、eBGP ピアを区切るホップの最大数を入力します。有効な値は、1 ～ 254 です。 この機能は、CPU利用率に基づく攻撃からBGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケット ヘッダーの送信元と宛先のIPアドレスを偽造した大量のIPパケットでネットワークをあふれさせてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。 この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。 この機能は、参加している各ルータで設定する必要があります。この機能では、eBGPセッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。この機能がイネーブルの場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能は BGP ピアリング セッションには影響しません。この機能がイネーブルの場合でも、キープアライブ パケットを受信しなければピアリング セッションは期限切れになります。受信パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージプロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。 この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するようにhop-countの値を正確に設定する必要があります。また、この機能をマルチホップ ピアリング セッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。 このコマンドの設定には、次の制限が適用されます。 • この機能は、内部 BGP（iBGP）ピアではサポートされません。 • 大きい直径のマルチホップ ピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定されたBGPルータに対するCPU利用率に基づく攻撃の場合は、影

要素	説明
	響を受けたピアリング セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。 • この機能は、ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、送信元ネットワークと宛先ネットワークの間のネットワーク セグメント上のピアも含まれます。
TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）	（任意）選択して、BGP セッションの TCP トランスポートセッションを有効にします。
TCPトランスポートモード（TCP transport mode）	ドロップダウンリストから TCP 接続モードを選択します。オプションは [デフォルト（Default）]、[アクティブ（Active）]、または [パッシブ（Passive）] です。
重量	（任意）BGP ネイバー接続の重みを入力します。
BGPバージョン（BGP Version）	ドロップダウンリストから、ASA が受け入れる BGP バージョンを選択します。[4 のみ（4-Only）] に設定すると、指定されたネイバーとの間でバージョン 4 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。
移行 （注） このカスタマイズは、AS 移行にのみ使用し、移行完了後に削除する必要があります。この手順は、経験豊富なネットワーク オペレータのみ実行する必要があります。不適切な設定によってルーティング ループが作成される可能性があります。	
ネイバーから受信したルートのAS番号をカスタマイズする（Customize the AS number for routes received from the neighbor）	（任意）選択して、eBGP ネイバーから受信したルートの AS_PATH 属性をカスタマイズします。
ローカルAS番号（Local AS Number）	ローカル自律システム番号を入力します。有効な値は、1 ～ 4294967295 または 1.0 ～ 65535.65535 の有効な自律システム番号です。
ネイバーから受信したルートの先頭にローカルAS番号を追加しない（Do not prepend local AS number to routes received from neighbor）	（任意）選択して、ローカル AS 番号が eBGP ピアから受信したルートの先頭に追加されないようにします。

要素	説明
実際のAS番号をネイバーから受信したルート内のローカルAS番号と置き換える（Replace real AS number with local AS number in routes received from neighbor）	（任意）選択して、実際の自律システム番号をeBGPアップデートのローカル自律システム番号で置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。
ネイバーから学習したルートで実際のAS番号かローカルAS番号を受け入れる（Accept either real AS number or local AS number in routes received from neighbor）	（任意）（ローカル BGP ルーティングプロセスの）実際の自律システム番号を使用するか、ローカル自律システム番号を使用してピアリングセッションを確立するように eBGP ネイバーを設定します。

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスを使用して、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義します。

ナビゲーション パス

[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （2733 ページ）
- [集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2749 ページ）

フィールド リファレンス

表 *717 : [*ネットワークの追加/編集（*Add/Edit Network*）*]* ダイアログボックス

要素	説明
ネットワーク	BGP ルーティングプロセスでアドバタイズするネットワークを指定します。
ルート マップ	（任意）アドバタイズされるネットワークをフィルタ処理するために調べる必要があるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

[Add Redistribution]/[Edit Redistribution] ダイアログボックス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスを使用して、別のルーティングドメインから BGP にルートを再配布する条件を定義します。

ナビゲーション パス

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv6 ファミリ（IPv6 Family）] : [全般（General）] タブ （2733 ページ）
- [集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）
- [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2749 ページ）

フィールド リファレンス

表 *718 : [Add Redistribution]/[Edit Redistribution]* ダイアログボックス

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウンリストから、どのプロトコルからルートを BGP ドメインに再配布するかを選択します。
プロセス ID（Process ID）	ルーティングプロセスの識別子を入力します。EIGRP および OSPF ルーティングプロトコルに適用されます。
メトリック（Metric）	（オプション）：再配布されているルートのメトリックを入力します。
ルート マップ	再配布されるネットワークをフィルタ処理するために調べる必要のあるルートマップを入力または選択します。この値を指定しない場合、すべてのネットワークが再配布されます。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
一致（Match）	1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。 • 内線 • 外部 1 • 外部 2 • NSSA 外部 1 • NSSA 外部 2

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスを使用して、条件に応じて BGP ルーティングテーブルに挿入されるルートを定義できます。

ナビゲーション パス

[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックスには、[IPv6ファミリ（IPv6 Family）] タブ （2732 ページ）からアクセスできます。[行の追加（Add Row）]（+）ボタンをクリックするか、テーブルから行を選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブ （2733 ページ）
- [集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）
- [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）
- [ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）
- [Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）

フィールド リファレンス

表 *719 : [ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス*

要素	説明
インジェクトマップ	ローカル BGP ルーティングテーブルに挿入するプレフィックスを指定するルートマップを入力または選択します。 **ヒント** [選択] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897ページ）を参照してください。

要素	説明
存在マップ	BGP スピーカーが追跡するプレフィックスを含むルートマップを入力または選択します。 ヒント [選択] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897ページ）を参照してください。
挿入されたルートは、集約ルートの属性を継承します。	挿入されたルートが集約ルートの属性を継承するように設定します。

EIGRP の設定

[EIGRP] ページには、ファイアウォールデバイスで Enhanced Interior Gateway Routing Protocol（EIGRP）ルーティングを設定するための 6 つのタブ付きパネルがあります。以下のトピックでは、EIGRP の有効化および設定について詳しく説明します。

- EIGRP について （2753 ページ）
- EIGRP 詳細ダイアログボックス （2754 ページ）
- [Setup] タブ （2757 ページ）
- [フィルタルール（Filter Rules）] タブ （2760 ページ）
- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interfaces] タブ （2770 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *720 : [EIGRP]* ページ

要素	説明
EIGRP のイネーブル化	EIGRP ルーティングプロセスを有効にするには、このチェックボックスをオンにします。
AS 番号（AS Number）	EIGRP プロセスの自律システム（AS）番号を入力します。指定できる AS 番号の範囲は 1 ～ 65535 です。
[Advanced] ボタン	EIGRP 詳細ダイアログボックス （2754 ページ）を開きます。ここでは、ルータ ID、スタブルーティング、隣接関係の変更など、追加の EIGRP プロセス設定を設定できます。
[Setup] タブ	[セットアップ（Setup）] タブを使用して、EIGRP ルーティングプロセスで使用されるネットワーク、パッシブインターフェイス、デフォルトルート情報、アドミニストレーティブ ディスタンス、およびデフォルトメトリックを設定します。 詳細については、[Setup] タブ （2757 ページ）を参照してください。
[フィルタルール（Filter Rules）] タブ	[フィルタルール（Filter Rules）] タブを使用してフィルタルールを定義すると、EIGRP ルーティングプロセスで受け入れ、またはアドバタイズされるルートを制御することができます。 詳細については、[フィルタルール（Filter Rules）] タブ （2760 ページ）を参照してください。
[ネイバー（Neighbors）] タブ	[ネイバー（Neighbors）] タブを使用して、EIGRP ネイバーを手動で定義します。 詳細については、[Neighbors] タブ （2762 ページ）を参照してください。
[再配布（Redistribution）] タブ	[再配布（Redistribution）] タブを使用して、他のルーティングプロトコルから EIGRP ルーティングプロセスにルートを再配布するためのルールを定義します。 詳細については、[Redistribution] タブ （2764 ページ）を参照してください。
[サマリーアドレス（Summary Address）] タブ	[サマリーアドレス（Summary Address）] タブを使用して、スタティックに定義された EIGRP サマリーアドレスを作成します。 詳細については、[サマリーアドレス（Summary Address）] タブ （2768 ページ）を参照してください。

要素	説明
[インターフェイス（Interfaces）] タブ	[インターフェイス（Interfaces）] タブを使用して、EIGRP のインターフェイスを設定します。 詳細については、[Interfaces] タブ （2770 ページ）を参照してください。

EIGRP について

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネット マスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネット マスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイバーから hello パケットを受信すると、トポロジ テーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジ テーブルを ASA に返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。ネイバーを手動で設定した場合、そのネイバーに送信される hello メッセージはユニキャストメッセージとして送信されます。ルーティングアップデートと確認応答が、ユニキャストメッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルは、ネイバーの検出、ネイバーの回復、Reliable Transport Protocol（RTP）、およびルート計算に重要な DUAL を含む、4 の主要なアルゴリズム テクノロジーと 4 つの主要なテクノロジーを使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジ テーブルに保存します。最小コストのルートはルーティング テーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブル サクセサから別のルートが選択されます。サクセサとは、宛先への最小コスト パスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティング ループを形成しないことが保証されます。

フィジブル サクセサがトポロジ テーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブル サクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

（注） EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

関連項目

- EIGRP の設定 （2751 ページ）

EIGRP 詳細ダイアログボックス

EIGRP 詳細ダイアログボックスを使用して、ルータ ID、スタブ ルーティング、隣接関係の変更などの設定を行います。

ナビゲーション パス

[EIGRP] ページから [EIGRP詳細（EIGRP Advanced）] ダイアログボックスにアクセスできます（EIGRP の設定 （2751 ページ）を参照）。

関連項目

- EIGRP の設定 （2751 ページ）

フィールド リファレンス

表 *721 : EIGRP* 詳細ダイアログボックス

要素	説明
ルータ ID（Router ID）	ルータ IDは、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。これを回避するには、ルータ ID のグローバルアドレスを指定します。各 EIGRP ルータには、一意の値を設定する必要があります。 単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（IPアドレスを選択すると、[アドレス（address）]フィールドが表示されます。） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルータID（Router ID）] フィールドに IPv4 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）]または[クラスタプール（Cluster Pool）]を選択します。（[クラスタプール（ Cluster Pool）] を選択すると、[IPv4プールオブジェクトID（ IPv4 Pool object ID）] フィールドが表示されます）。 [クラスタプール（Cluster Pool）] を選択した場合は、ルータの ID アドレスを提供する IPv4 プールオブジェクトの名前を入力または選択します。詳細については、を参照してください。

要素	説明
Stub	ASA を EIGRP スタブ ルータとしてイネーブル化し、設定することができます。スタブルーティングは、ASA でメモリと [IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス （407 ページ）の処理要件を減らす場合があります。ASA をスタブ ルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティング テーブルを維持する必要がなくなります。一般に、配布ルータからスタブ ルートに送信する必要があるのは、デフォルト ルートだけです。 スタブ ルータから配布ルータには、指定されたルートだけが伝搬されます。スタブ ルータである ASA は、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブ ルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブ ルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブ ルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。 ASA を EIGRP スタブルーティングプロセスとして有効にするには、次の EIGRP スタブルーティングプロセスから 1 つ以上を選択します。 • Receive only：隣接ルータからルート情報を受信しても、その隣接ルータにルート情報を送信しないために、EIGRP スタブルーティングプロセスを設定します。このオプションを選択する場合は、他のスタブ ルーティング オプションを選択できません。 • [接続済み（Connected）]：接続済みルートをアドバタイズします。 • [再配布済み（Redistributed）]：再配布済みルートをアドバタイズします。 • [スタティック（Static）]：スタティックルートをアドバタイズします。 • [サマリ - （Summary）]：サマリールートをアドバタイズします。

要素	説明
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [ログネイバーの変更（Log Neighbor Changes）]：EIGRP ネイバーの隣接関係に関する変更のロギングを有効にします。このオプションは、デフォルトで選択されます。 • [ログネイバーの警告（Log Neighbor Warnings）]：EIGRP ネイバーの警告メッセージのロギングを有効にします。このオプションは、デフォルトで選択されます。 （任意）ネイバー警告メッセージの反復間隔（秒数）。有効値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

[Setup] タブ

[EIGRP] ページの [セットアップ（Setup）] タブを使用して、EIGRP ルーティングプロセスで使用されるネットワーク、パッシブインターフェイス、デフォルトルート情報、アドミニストレーティブ ディスタンス、およびデフォルトメトリックを設定します。

ナビゲーション パス

[EIGRP] ページから [セットアップ（Setup）] タブにアクセスできます。詳細については、EIGRP の設定 （2751 ページ）を参照してください。

関連項目

- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [Setup] タブ （2757 ページ）
- [フィルタルール（Filter Rules）] タブ （2760 ページ）
- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interfaces] タブ （2770 ページ）

フィールド リファレンス

表 *722 : EIGRP* : *[*セットアップ（*Setup***）*]* タブ**

要素	説明
自動サマリー	自動ルート集約を有効にするには、このチェックボックスをオンにします。自動サマリーは、9.2.1 より前の ASA バージョンではデフォルトで有効になっており、ASA 9.2(1) 以降ではデフォルトで無効になっています。 有効になっている場合、EIGRP ルーティングプロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。 たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加しているとすると、EIGRP ルーティング プロセスはそれらのルートに対しサマリー アドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリー アドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。
ネットワーク	EIGRP ルーティングプロセスに参加するネットワークの IP アドレスを入力します。 **ヒント** [選択（Select）] をクリックすると、ネットワーク/ホストオブジェクトのリストからネットワークを選択できます。
パッシブ インターフェイス	1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。 デフォルトでは、そのインターフェイスでルーティングが有効になると、アクティブルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスが有効になります。 パッシブインターフェイスを設定するには、次のいずれかを実行します。 • そのインターフェイスに対してルーティングが有効な場合、アクティブルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスを有効にするには、[なし（None）] を選択します。 • すべてのインターフェイスをパッシブとして設定するには、[すべてのインターフェイス（All Interfaces）] を選択します。 • 特定のインターフェイスをパッシブとして設定するには、[指定されたインターフェイス（Specified Interfaces）] を選択し、パッシブにするインターフェイスを入力または選択します。

要素	説明
デフォルトのルート情報	EIGRP アップデート内のデフォルト ルート情報の送受信を制御できます。デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルト ルート ビット設定が無効になります。 • デフォルトのルート情報を受け入れる：外部のデフォルトルーティング情報を受け入れるように EIGRP を設定します。任意で、デフォルトルート情報を受信するときに許可するネットワークと許可しないネットワークを定義する標準アクセスリストを指定できます。 • デフォルトのルート情報を送信する：外部ルーティング情報をアドバタイズするように EIGRP を設定します。任意で、デフォルトルート情報を送信するときに許可するネットワークと許可しないネットワークを定義する標準アクセスリストを指定できます。
アドミニストレーティブ ディスタンス（Administrative Distance）	各ルーティング プロトコルには、他のルーティング プロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティング プロトコルによって生成された同じ宛先への 2 つのルートのいずれが「最適パス」であるかは、必ずしも判別できません。アドミニストレーティブ ディスタンスは、2 つの異なるルーティング プロトコルから同じ宛先への異なるルートが複数存在する場合に、ASA がベスト パスの選択に使用するルート パラメータです。 ASA で複数のルーティング プロトコルが実行されている場合、distance eigrp コマンドを使用して、EIGRP ルーティング プロトコルが検出するルートのデフォルト アドミニストレーティブ ディスタンスを、他のルーティング プロトコルと関連付けて調整できます。 [Internal Distance]：EIGRP 内部ルートのアドミニストレーティブ ディスタンスです。内部ルートとは、同じ自律システム内の別のエンティティから学習されるルートです。有効な値は、1 ～ 255 です。デフォルトは 90 です。 [External Distance]：EIGRP 外部ルートのアドミニストレーティブ ディスタンスです。外部ルートとは、最適パスを自律システムの外部にあるネイバーから学習するルートです。有効値の範囲は 1 ～ 255 で、デフォルト値は 170 です。

要素	説明
デフォルトメトリック	EIGRP ルーティングプロセスに再配布されるルートのデフォルトのメトリックを定義できます。 • [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。 • [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。 • [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。 • [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。

[フィルタルール（Filter Rules）] タブ

[フィルタルール（Filter Rules）] タブには、EIGRP ルーティングプロセスに設定されているルート フィルタリング ルールを表示する [フィルタルール（Filter Rules）] テーブルが含まれています。フィルタ ルールによって、EIGRP ルーティング プロセスで受け入れまたはアドバタイズされるルートを制御できます。

ナビゲーション パス

[EIGRP] ページから [フィルタルール（Filter Rules）] タブにアクセスできます。詳細については、EIGRP の設定 （2751 ページ）を参照してください。

関連項目

• [EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックス （2761 ページ）
• EIGRP の設定 （2751 ページ）
• EIGRP について （2753 ページ）
• [Setup] タブ （2757 ページ）
• [Neighbors] タブ （2762 ページ）
• [Redistribution] タブ （2764 ページ）
• [サマリーアドレス（Summary Address）] タブ （2768 ページ）

- [Interfaces] タブ （2770 ページ）

フィールド リファレンス

表 *723 : EIGRP* : *[フィルタルール（Filter Rules）]* タブ

要素	説明
方向（Direction）	フィルタルールの方向： • [Inbound]：このルールは、着信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [Outbound]：このルールは、着信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
インターフェイス	（オプション）フィルタルールが適用されるインターフェース。
プロトコル	フィルタリングされるルーティングプロトコル：[BGP]、[接続（Connected）]、[OSPF]、[RIP]、または [スタティック（Static）]。
ACL	標準 IP アクセスリスト名。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。

[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックス

[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックスを使用して、既存のフィルタルールテーブルに新しいフィルタルールを追加するか、または既存のフィルタルールを変更します。

ナビゲーション パス

[EIGRPフィルタルールの追加（Add EIGRP Filter Rule）]/[EIGRPフィルタルールの編集（Edit EIGRP Filter Rule）] ダイアログボックスには、[フィルタルール（Filter Rules）] タブ （2760 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [フィルタルール（Filter Rules）] タブ （2760 ページ）

フィールド リファレンス

表 *724 : [EIGRP*フィルタルールの追加（*Add EIGRP Filter Rule*）*]/[EIGRP*フィルタルールの編集（*Edit EIGRP Filter Rule*）*]* ダイアログボックス

要素	説明
EIGRP フィルタの方向	フィルタルールの方向を指定します。 • [インバウンド（Inbound）]：このルールは、着信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [アウトバウンド（Outbound）]：このルールは、発信 EIGRP ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
タイプ（Type）	フィルタルールのタイプを指定します。 • （任意）インターフェイス：ルーティングアップデートを適用するインターフェイスを指定します。インターフェイスを指定すると、アクセスリストはそのインターフェイスのルーティングアップデートにのみ適用されます。インターフェイスが指定されていない場合、アクセスリストはすべてのアップデートに適用されます。 • （任意）ルーティングプロトコル：アウトバウンド EIGRP ルーティングアップデートでは、フィルタリングするルーティングプロトコル（BGP、接続済み、OSPF、RIP またはスタティック）を選択します。 ルーティングプロトコル ID：ルーティングプロセスの識別子を入力します。BGP および OSPF ルーティングプロトコルに適用されます。
ACL	受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。

[Neighbors] タブ

[ネイバー（Neighbors）]タブには、スタティックネイバーを定義できるネイバーテーブルが含まれています。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

ナビゲーション パス

[EIGRP] ページから [ネイバー（Neighbors）] タブにアクセスできます。詳細については、EIGRP の設定 （2751 ページ）を参照してください。

関連項目

- [EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス （2763 ページ）

- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [Setup] タブ （2757 ページ）
- [フィルタルール（Filter Rules）] タブ （2760 ページ）
- [Redistribution] タブ （2764 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interfaces] タブ （2770 ページ）

フィールド リファレンス

表 *725 : EIGRP* : *[ネイバー（Neighbors）]* タブ

要素	説明
インターフェイス（Interface）	ネイバーが使用可能なインターフェイス。
ネイバー	スタティック ネイバーの IP アドレス。

[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックス

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

（注） インターフェイスに対して passive-interface コマンドを設定すると、そのインターフェイスではすべての発着信ルーティング更新および hello メッセージが表示されなくなります。EIGRP ネイバーとの隣接関係は、パッシブとして設定されるインターフェイス経由で確立および維持できません。

スタティックネイバーを定義するか、または既存のスタティックネイバーの情報を変更するには、[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックスを使用します。

ナビゲーション パス

[EIGRPネイバーの追加/編集（Add/Edit EIGRP Neighbor）] ダイアログボックスには、[Neighbors] タブ （2762 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （2751 ページ）

- EIGRP について （2753 ページ）
- [Neighbors] タブ （2762 ページ）

フィールド リファレンス

表 *726 : [EIGRP*ネイバーの追加/編集（*Add/Edit EIGRP Neighbor*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	ネイバーが使用可能なインターフェイス。 ヒント [選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。
ネイバー	スタティック ネイバーの IP アドレス。 ヒント [選択（Select）] をクリックすると、ホストオブジェクトのリストからネイバーを選択できます。

[Redistribution] タブ

[再配布（Redistribution）] タブを使用して、他のルーティングプロトコルから EIGRP ルーティングプロセスにルートを再配布するためのルールを定義します。

ナビゲーション パス

[EIGRP] ページから [再配布（Redistribution）] タブにアクセスできます。詳細については、EIGRP の設定 （2751 ページ）を参照してください。

関連項目

- [EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックス （2766 ページ）
- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [Setup] タブ （2757 ページ）
- [フィルタルール（Filter Rules）] タブ （2760 ページ）
- [Neighbors] タブ （2762 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interfaces] タブ （2770 ページ）

フィールド リファレンス

表 *727 : EIGRP* : *[*再配布（*Redistribution*）*]* タブ

要素	説明
プロトコル	ルートの再配布元の送信元プロトコル。 • [BGP]：BGP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [RIP]：RIP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [Static]：スタティックルートを EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [OSPF]：OSPF ルーティングプロセスで検出されたルートを EIGRP に再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または BGP ルートを再配布するときには使用できません。
ID	BGP または OSPF ルーティングプロセスの自律システム（AS）番号。
Bandwidth	ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。
遅延時間	ルート遅延（10 マイクロ秒単位）。有効値の範囲は、0 ～ 4294967295 です。
信頼性	正常なパケット伝送の可能性。0 ～ 255 の数値で表されます。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。
読み込み中	ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。
[MTU]	パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。
ルート マップ	再配布エントリに適用されるルートマップオブジェクトの名前。

[EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックス

[再配布の追加/編集（Add/Edit Redistribution）] ダイアログボックスを使用して、再配布ルールを追加するか、[再配布（Redistribution）] テーブルの既存の再配布ルールを編集します。

ナビゲーション パス

[EIGRP再配布の追加/編集（Add/Edit EIGRP Redistribution）] ダイアログボックスには、[Redistribution] タブ （2764 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [Redistribution] タブ （2764 ページ）

フィールド リファレンス

表 *728 : [EIGRP*再配布の追加/編集（*Add/Edit EIGRP Redistribution*）*]* ダイアログボックス

要素	説明
プロトコル	ルートが再配布されているソース プロトコルを選択します。次のいずれかのオプションを選択できます。 • [BGP]：BGP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [RIP]：RIP ルーティングプロセスによって検出されたルートを EIGRP に再配布します。 • [Static]：スタティックルートを EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にあるスタティック ルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を EIGRP ルーティングプロセスに再配布します。ネットワーク設定の範囲内にある接続済みルートは EIGRP に自動的に再配布されるため、それらのルートの再配布ルールを定義する必要はありません。 • [OSPF]：OSPF ルーティングプロセスで検出されたルートを EIGRP に再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、または BGP ルートを再配布するときには使用できません。

要素	説明
ルーティングプロセス ID	BGP または OSPF ルーティングプロセスの自律システム（AS）番号。
オプションメトリック	EIGRP ルーティングプロセスに再配布されるルートの次のメトリックを定義できます。 • [帯域幅（Bandwidth）]：ルートの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [遅延時間（Delay Time）]：ルートの遅延（10 マイクロ秒）。有効値の範囲は、0 ～ 4294967295 です。 • [信頼性（Reliability）]：0 ～ 255 の数値で表現した、パケットが正常に伝送される見込み。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを表します。 • [ローディング（Loading）]：ルートの実効帯域幅。有効値の範囲は 1 ～ 255 で、255 は負荷が 100 % であることを示します。 • [MTU]：パスの最大伝送単位の最小許容値。有効値の範囲は 1 ～ 65535 です。
ルートマップ	EIGRP ルーティングプロセスに再配布されるルートを定義するには、ルートマップオブジェクトを選択または入力します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。

要素	説明
オプションの OSPF 再配布	ルートタイプとして OSPF を選択した場合、1 つのルーティングプロトコルから別のルーティングプロトコルへのルート再配布に使用される条件を選択します。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。 • [Internal]：ルートは特定の AS の内部です。 • [External 1]：自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External 2]：自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。 • [NSSA External 1]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。 • [NSSA External 2]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

[サマリーアドレス（Summary Address）] タブ

[サマリーアドレス（Summary Address）] タブを使用して、特定のインターフェイスの EIGRP のサマリーを設定します。サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリーアドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリーアドレスを使用する場合は、手動でサマリーアドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

ナビゲーション パス

[EIGRP] ページから [サマリーアドレス（Summary Address）] タブにアクセスできます。詳細については、EIGRP の設定 （2751 ページ）を参照してください。

関連項目

• [EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックス （2769 ページ）
• EIGRP の設定 （2751 ページ）
• EIGRP について （2753 ページ）
• [Setup] タブ （2757 ページ）
• [フィルタルール（Filter Rules）] タブ （2760 ページ）

- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [Interfaces] タブ （2770 ページ）

フィールド リファレンス

表 *729 : EIGRP* : *[サマリーアドレス（Summary Address）] タブ*

要素	説明
インターフェイス（Interface）	サマリーアドレスのアドバタイズ元となるインターフェイスです。
ネットワーク（Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。
アドミニストレーティブ ディスタンス（Administrative Distance）	サマリールートのアドミニストレーティブ ディスタンス。

[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックス

[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックスを使用して、新しいエントリを追加するか、サマリーアドレステーブルの既存のエントリを変更します。サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリーアドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

ナビゲーション パス

[EIGRPサマリーアドレスの追加/編集（Add/Edit EIGRP Summary Address）] ダイアログボックスには、[サマリーアドレス（Summary Address）] タブ （2768ページ）からアクセスできます。

関連項目

- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）

フィールド リファレンス

表 *730 : [EIGRP*サマリーアドレスの追加/編集（*Add/Edit EIGRP Summary Address*）*]* ダイアログボックス

要素	説明
インターフェイス（Interface）	サマリーアドレスのアドバタイズ元となるインターフェイスです。 ヒント　[選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。
ネットワーク	サマリーアドレスの IP アドレスおよびネットワークマスク。 ヒント　[選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
アドミニストレーティブディスタンス（Administrative Distance）	（任意）集約ルートのアドミニストレーティブディスタンス。有効な値は 1 ～ 255 です。デフォルト値は 5 です。

[Interfaces] タブ

[インターフェイス（Interface）] タブを使用して、インターフェイス固有の EIGRP ルーティングプロパティを設定します。

ナビゲーション パス

[EIGRP] ページから [インターフェイス（Interfaces）] タブにアクセスできます。詳細については、 EIGRP の設定 （2751 ページ）を参照してください。

関連項目

- [EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックス （2771 ページ）
- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [Setup] タブ （2757 ページ）
- [フィルタルール（Filter Rules）] タブ （2760 ページ）
- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）

フィールド リファレンス

表 *731 : [EIGRP]* : *[インターフェイス（Interfaces）]* タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
Hello 間隔（Hello Interval）	インターフェイス上で送信される EIGRP hello パケット間の間隔（秒数）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
保留時間（Hold Time）	EIGRP hello パケットで ASA によってアドバタイズされるホールドタイム。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。
Split Horizon	インターフェイスで EIGRP スプリットホライズンが有効になっているか（true）無効になっているか（false）を示します。
遅延	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。このオプションは、マルチコンテキストモードのデバイスではサポートされています。
Key ID	EIGRP 更新の認証に使用されるキーの ID。

[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックス

[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックスを使用して、インターフェイス固有の EIGRP ルーティングパラメータを設定します。

ナビゲーション パス

[EIGRPインターフェイスの追加/編集（Add/Edit EIGRP Interface）] ダイアログボックスには、[Interfaces] タブ （2770 ページ）からアクセスできます。

関連項目

- EIGRP の設定 （2751 ページ）
- EIGRP について （2753 ページ）
- [Interfaces] タブ （2770 ページ）

フィールド リファレンス

表 *732 : [EIGRP*インターフェイスの追加（*Add EIGRP Interface***）*]/[EIGRP*インターフェイスの編集（***Edit EIGRP Interface***）*]* ダイアログボックス**

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
Hello 間隔（Hello Interval）	インターフェイス上で送信される EIGRP hello パケット間の間隔（秒数）。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
保留時間（Hold Time）	EIGRP hello パケットで ASA によってアドバタイズされるホールドタイム。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 15 秒です。
Split Horizon	インターフェイスで EIGRP スプリットホライズンを有効または無効にします。
遅延時間	遅延時間（10 マイクロ秒単位）。有効な値は、1 ～ 16777215 です。このオプションは、マルチコンテキストモードのデバイスではサポートされていないため、無効になります。
MD5 認証の有効化（Enable MD5 Authentication）	EIGRP パケットの MD5 認証をイネーブルにします。
キー タイプ	入力するキーがクリアテキストであることを示すには、[クリアテキスト（Clear Text）] を選択します。入力するキーがすでに暗号化されていることを示すには、[暗号化（Encrypted）] を選択します。
キー ID とキー	EIGRP 更新を認証するキーを指定します。 • [Key ID]：数値のキー ID を入力します。有効な値の範囲は 0 ～ 255 です。 • [Key]：最大 16 バイトの英数字文字列。 • [確認（Confirm）]：キーを再入力します。

ISIS の設定

[ISIS] ページには、ファイアウォールデバイスでの ISIS（Intermediate System-to-Intermediate System）ルーティングを設定するための 9 つのタブ付きパネルがあります。ISIS ルーティングプロトコルは、Security Manager バージョン 4.11 以降で、ソフトウェアバージョン 9.6(1) 以降

を実行している ASA デバイスについてサポートされています。以下のトピックでは、ISIS の有効化および設定について詳しく説明します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [ISIS] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [ISIS] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

選択した ASA デバイスで Intermediate System-to-Intermediate System プロトコルを有効にするには、[ISIS の有効化（Enable ISIS）] をオンにします。

ISIS について

Intermediate System-to-Intermediate System（ISIS）ルーティングプロトコルはリンクステートの内部ゲートウェイプロトコル（IGP）です。リンクステートプロトコルは、各参加ルータで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。IOS ISIS の実装は、CLNP、IPv4、および IPv6 をサポートします。

ルーティングドメインは1つ以上のサブドメインに分けることができます。各サブドメインはエリアと呼ばれ、エリアアドレスが割り当てられます。エリア内のルーティングは、レベル 1 ルーティングと呼ばれます。レベル 1 エリア間のルーティングは、レベル 2 ルーティングと呼ばれます。OSI の用語では、ルータは中継システム（IS）と呼ばれます。IS はレベル 1 とレベル 2、またはその両方で稼働します。レベル 1 で稼働している IS は、同じエリア内にある他のレベル 1 の IS とルーティング情報を交換します。レベル 2 で稼働している IS は、他のレベル 2 のルータとルーティング情報を交換します。この場合はルータが同じレベル 1 エリアにあるかどうかは関係しません。レベル 2 にあるルータと、これらとインターコネクトしているリンクは、レベル 2 サブドメインを形成します。ルーティングが正しく機能するためには、これらをパーティション化してはなりません。

[General] タブ

[全般（General）] タブを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの BGP 設定を構成します。

ナビゲーション パス

[ネイバー（Neighbors）] タブには、[OSPF] ページからアクセスできます（BGP の設定 （2704 ページ）を参照）。

関連項目

- BGP の設定 （2704 ページ）
- BGP について （2706 ページ）
- [IPv4ファミリ（IPv4 Family）] タブ （2711 ページ）

フィールド リファレンス

表 733 : [General] タブ

要素	説明
[受信されたルートのAS_PATH属性に含まれるAS番号の数（Limit the number of AS numbers in AS_PATH attribute of received routes）]	AS_PATH 属性に含まれる AS 番号の数を特定の数に制限します。有効値は 1 ～ 254 です。
ネイバーの変更を記録（Log Neighbor Changes）	BGP ネイバーの変更（アップまたはダウン）のロギングを有効にします。これは、ネットワーク接続の問題をトラブルシューティングしたり、ネットワークの安定性を評価する際に役に立ちます。
[TCPパスMTUディスカバリを使用する（Use TCP Path MTU Discovery）]	パス MTU ディスカバリ手法を使用して、2 つの IP ホスト間のネットワークパスにおける最大伝送ユニット（MTU）のサイズを決定します。これにより、IP フラグメンテーションが回避されます。
[高速外部フェールオーバーの有効化（Enable fast external failover）]	リンク障害の発生時、外部 BGP セッションを即時にリセットします。
[最初のASをEBGPルートのピアのASとして実行（Enforce that the first AS is peer's AS for EBGP routes）]	AS 番号を AS_path 属性の 1 つ目のセグメントとしてリストに表示していない外部 BGP ピアから受信した着信アップデートを破棄します。これにより、誤って設定されたピアや許可されていないピアが、別の自律システムから送信されたかのようにルートをアドバイタイズしてトラフィックを誤った宛先に送信することがなくなります。
[AS番号にドット表記を使用（Use dot notation for AS numbers）]	完全なバイナリ 4 バイトの AS 番号を、ドットで区切られた 16 ビットの 2 文字ずつに分割します。0 ～ 65553 の AS 番号は 10 進数で表され、65535 を超える AS 番号はドット付き表記を使用して表されます。
[ベストパスの選択（Best Path Selection）]	

要素	説明
Default local preference	0 ～ 4294967295 の数値を指定します。デフォルト値は 100 です。値が大きいほど、優先度が高いことを示します。この優先度は、ローカル自律システム内のすべてのルータおよびアクセス サーバーに送信されます。
[異なるネイバーのMEDの比較を許可（Allow comparing MED from different neighbors）]	異なる自律システムにあるネイバーからのパスの Multi-Exit 識別子（MED）の比較を許可します。
[同一のBGPパスのルータIDを比較（Compare Router-id for identical EBGP paths）]	ベストパスの選択プロセス中に外部 BGP ピアから受信した類似パスを比較し、ベストパスをルータ ID が最も小さいルートに切り替えます。
[隣接ASからアドバタイズされたパスの間で最適なMEDパスを選択（Pick the best MED path among paths advertised from the neighboring AS）]	コンフェデレーション ピアから学習した複数のパスの間で MED 比較をイネーブルにします。MED 間の比較は、外部の自律システムがパスに存在しない場合にのみ行われます。
[欠落MEDを最低優先度として処理（Treat missing MED as the least preferred one）]	欠落している MED 属性は無限大の値を持つものとみなし、このパスを最も推奨度の低いパスにします。したがって、MED が欠落しているパスが最も優先度が低くなります。
[ネイバータイマー（Neighbor Timers）]	
[キープアライブ間隔（Keepalive Interval）]	キープアライブメッセージを送信しなかった場合に、その後 BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。このキープアライブ インターバルが終わると、メッセージが送信されない場合、BGP ピアはデッドとして宣言されます。デフォルト値は 60 秒です。
保留時間（Hold Time）	BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する時間間隔を入力します。デフォルト値は 180 秒です。
Min Hold Time	（任意）BGP 接続が開始され設定されている間、BGP ネイバーがアクティブな状態を継続する最小時間間隔を入力します。0 ～ 65535 の値を指定します。
[グレースフルリスタート（Graceful Restart）]（フェールオーバーまたはスパンドクラスタ モードで使用） （ASA 9.3.1 以降のみ）	
グレースフル リスタートをイネーブルにします。	スイッチオーバー後のルーティングフラップを ASA ピアが回避できるようにします。

要素	説明
再起動時間	BGP オープンメッセージが受信される前に、ASA ピアが古いルートを削除するまでの待機時間を指定します。デフォルト値は 120 秒です。有効な値は 1 ～ 3600 秒です。
[Stalepath時間（Stalepath Time）]	再起動する ASA から End Of Record（EOR）メッセージを受信した後、ASA が古いルートを削除するまでの待機時間を入力します。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

[IPv4ファミリ（IPv4 Family）] タブ

[BGP] ページの [IPv4ファミリ（IPv4 Family）] タブを使用して、BGP の IPv4 設定を有効にして構成します。

ナビゲーション パス

[BGP] ページから [IPv4ファミリ（IPv4 Family）] タブにアクセスできます。[BGP] ページの詳細については、BGP の設定 （2704 ページ）を参照してください。

関連項目

- BGP について （2706 ページ）
- [General] タブ （2709 ページ）

フィールド リファレンス

表 *734 : IPv4* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
IPv4ファミリの有効化（Enable IPv4 Family）	標準の IPv4 アドレスプレフィックスを使用するルーティングセッションの設定を有効にします。
一般	このパネルを使用して、[ベストパス選択（Best Path Selection）]、[ネイバータイマー（Neighbor Timers）]、[グレースフルリスタート（Graceful Restart）] などの一般的な IPv4 設定を設定します。これらの定義の詳細については、IPv4 Family - [全般（General）] タブ （2713 ページ）を参照してください。

要素	説明
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）を参照してください。
フィルタリング	このパネルを使用して、着信 BGP アップデートで受信したルータまたはネットワークをフィルタ処理します。これらの定義の詳細については、[Add Filter]/[Edit Filter] ダイアログボックス （2717 ページ）を参照してください。
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）を参照してください。
ネットワーク	このパネルを使用して、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2728 ページ）を参照してください。
再配布	Use this panel to define the conditions for redistributing routes from another routing domain into BGP. これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （2729 ページ）を参照してください。
ルートの挿入	このパネルを使用して、条件に応じて BGP ルーティングテーブルに注入されるルートを定義します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2730 ページ）を参照してください。

[IPv4ファミリ（IPv4 Family）] タブ：[全般（General）]タブ

フィールド リファレンス

表 *735 : [ISIS IPv4ファミリ（ISIS IPv4 Family）] タブ：[全般（General）]タブ*

要素	説明
隣接関係チェックの実行（Perform Adjacency Check）	[隣接関係チェックの実行（Perform Adjacency Check）] チェックボックスをオンにし、ルータが近隣の IS ルータをチェックするようにします。
距離	

要素	説明
アドミニストレーティブ ディスタンス（Administrative Distance）	[Administrative Distance] フィールドに、IS-IS プロトコルによって検出されたルートに割り当てるディスタンスを入力します。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブ ディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。
転送パスの最大数（Maximum No. of Forward Paths）	ルーティングテーブルにインストールできる IS ルートの最大数を入力します。指定できる範囲は 1 ～ 8 です。デフォルトは 4 です。
デフォルトルートの配布（Distribute Default Route）	[デフォルトルートの配布（Distribute Default Route）] チェックボックスをオンにしてデフォルトルートを配布するように IS ルーティングプロセスを設定し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からデフォルトルートを選択します。
ISISメトリック（ISIS Metrics）	
グローバル ISIS メトリック レベル 1	メトリックを指定する数値を入力します。 範囲は、選択した TLV スタイルによって異なります。デフォルトは 10 です。 • [狭いメトリックで古いスタイルのTLVを使用する（Use old style of TLVs with narrow metric）] を選択した場合、範囲は 1 ～ 63 です。 • [より広いメトリックに対応する新しいスタイルのTLVを使用する（Use new style of TLVs to carry wider metric）] を選択した場合、範囲は 1 ～ 16777214 です。 • [移行中に両方のスタイルのTLVを送信して受け入れる（Send and accept both styles of TLVs during transition）] を選択した場合、範囲は 1 ～ 16777214 です。

要素	説明
グローバル ISIS メトリック レベル 2	メトリックを指定する数値を入力します。 範囲は、選択した TLV スタイルによって異なります。デフォルトは 10 です。 • [狭いメトリックで古いスタイルのTLVを使用する（Use old style of TLVs with narrow metric）] を選択した場合、範囲は 1 ～ 63 です。 • [より広いメトリックに対応する新しいスタイルのTLVを使用する（Use new style of TLVs to carry wider metric）] を選択した場合、範囲は 1 ～ 16777214 です。 • [移行中に両方のスタイルのTLVを送信して受け入れる（Send and accept both styles of TLVs during transition）] を選択した場合、範囲は 1 ～ 16777214 です。
TLV スタイル（TLV Style）	次のタイプ、長さ、および値のいずれかを選択します。 • 狭いメトリックで古いスタイルの TLV を使用する（Use old style of TLVs with narrow metric） • より広いメトリックに対応する新しいスタイルの TLV を使用する（Use new style of TLVs to carry wider metric） • 移行中に両方のスタイルの TLV を送信して受け入れる（Send and accept both styles of TLVs during transition）
移行中に両方のスタイルの TLV を受け入れる（Accept both styles of TLVs during transition）	このオプションは、[TLVスタイル（TLV Style）] で最初の 2 つのオプションのいずれかを選択した場合に選択できます。
メトリックスタイルの適用先（Apply metric style to）	次のいずれかを選択します。 • レベル 1 • レベル 2 • 両方 デフォルトはレベル 1 です。

[IPv4ファミリ（IPv4 Family）] タブ：[SPF] タブ

フィールド リファレンス

表 *736 : [ISIS IPv4*ファミリ（*ISIS IPv4 Family*）*]* タブ：*[SPF]* タブ

要素	説明
[最短パス優先（Shortest Path First）]	
[SPF計算に外部メトリックを含める（Honour external metrics during SPF calculations）]	SPF 計算に外部メトリックを含めるには、このチェックボックスをオンにします。
[このルータをSPF計算の中間ホップとして使用しないように他のルータに通知する（Signal other routers to not use this router as an intermediate hop in their SPF calculations）]	このデバイスを除外する場合は、このチェックボックスをオンにして、以下を設定します。
[起動時の動作を指定（Specify on-startup behavior）]	このオプションを選択した場合は、次のいずれかのオプションを選択する必要があります。 • [BGP収束前に過負荷として自身をアドバタイズする（Advertise overself as overloaded until BGP has converged）] • [再起動後に過負荷として自身をアドバタイズする時間を指定する（Specify time to advertise overself as overloaded after reboot）]：5 ～ 86400 秒の範囲で時間を指定します。
[過負荷ビットが設定されている場合に他のプロトコルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from other protocols when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
[過負荷ビットが設定されている場合に別のISISレベルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from another ISIS level when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
部分ルート計算の最小間隔	
[PRC間隔（PRC Interval）]	ルータが部分ルート計算（PRC）間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。

要素	説明
[PRCの初期待機時間（Initial wait for PRC）]	トポロジ変更後の最初の PRC 計算遅延（ミリ秒単位）を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。
[1番目と2番目のPRC間の最小待機時間（Minimum wait between first and second PRC）]	ルータが PRC 間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒です。
SPF 計算の最小間隔	
レベル 1 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。
レベル 2 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。

IPv4 ファミリータブ：再配布タブ

[追加（Add）]/[編集（Edit）] ボタンを使用して、新しい再配布ルートを追加するか、既存の行を編集します。

フィールド リファレンス

表 *737 : ISIS IPv4* ファミリータブ：再配布タブ

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウン リストから、ISIS ドメインにルートを再配布するプロトコル（[BGP]、[Connected]、[EIGRP]、[OSPF]、[RIP]、または [Static]）を選択します。
プロセス ID（Process ID）	送信元プロトコルのプロセス ID を入力します。
ルートレベル	[Route Level] ドロップダウン リストから、[Level-1]、[Level- 2]、または [Level 1-2] を選択します。
メトリック（Metric）	[メトリック（Metric）] フィールドに、再配布されるルートのメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。
メトリック タイプ	[Metric Type] で、[internal] または [external] オプション ボタンをクリックします。
ISIS エリア間ルートレベル	
送信元 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
接続先 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
[同報リスト（Distribution List）]	利用可能なアクセス制御リストから選択するか、新規に追加します。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から、再配布するネットワークをフィルタ処理するために調べる必要があるルートマップを選択するか、[追加（Add）] をクリックして、新しいルートマップを追加するか、既存のルートマップを編集します。
一致（Match）	[Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

[IPv6ファミリ（IPv6 Family）] タブ

[BGP] ページの [IPv6 ファミリ（IPv6 Family）] タブを使用して、BGP の IPv6 設定を有効にして設定します。

ナビゲーション パス

[BGP] ページから [IPv6 ファミリ（IPv6 Family）] タブにアクセスできます。[BGP] ページの詳細については、 BGP の設定 （2704 ページ）を参照してください。

関連項目

- BGP について （2706 ページ）
- [General] タブ （2709 ページ）

フィールド リファレンス

表 *738 : IPv6* ファミリ：*[*集約アドレス（*Aggregate Address*）*]* タブ

要素	説明
[IPv6 ファミリの有効化（Enable IPv6 Family）]	標準の IPv6 アドレスプレフィックスを使用するルーティングセッションの設定を有効にします。
一般	このパネルを使用して、一般的な IPv6 設定を指定します。これらの定義の詳細については、[IPv6 ファミリ（IPv6 Family）]：[全般（General）] タブ （2733 ページ）を参照してください。
[Aggregate Address]	このパネルを使用して、特定のルートから 1 つのルートへの集約を定義します。 [Aggregate Timer] フィールドで、集約タイマーの値（秒）を指定します。有効な値は、0 または 6 ～ 60 の値です。デフォルト値は 30 です。 これらの定義の詳細については、[集約アドレスの追加/編集（Add/Edit Aggregate Address）] ダイアログボックス （2735 ページ）を参照してください。
ネイバー	このパネルを使用して、BGP ネイバーとネイバーの設定を定義します。これらの定義の詳細については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）を参照してください。
ネットワーク	このパネルを使用して、BGP ルーティングプロセスによってアドバタイズされるネットワークを定義します。これらの定義の詳細については、[ネットワークの追加/編集（Add/Edit Network）] ダイアログボックス （2747 ページ）を参照してください。
再配布	このパネルを使用して、別のルーティングドメインから BGP にルートを再配布する条件を定義します。これらの定義の詳細については、[Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）を参照してください。

要素	説明
ルートの挿入	このパネルを使用して、条件に応じてBGPルーティングテーブルに注入されるルートを定義します。これらの定義の詳細については、[ルートインジェクションの追加/編集（Add/Edit Route Injection）] ダイアログボックス （2749 ページ）を参照してください。

[IPv6ファミリ（IPv6 Family）] タブ：[全般（General）]タブ

フィールド リファレンス

表 *739 : [ISIS IPv6ファミリ（ISIS IPv6 Family）] タブ：[全般（General）]タブ*

要素	説明
隣接関係チェックの実行（Perform Adjacency Check）	[隣接関係チェックの実行（Perform Adjacency Check）] チェックボックスをオンにし、ルータが近隣のISルータをチェックするようにします。
距離	
アドミニストレーティブディスタンス（Administrative Distance）	[アドミニストレーティブディスタンス（Administrative Distance）] フィールドに、IS-ISプロトコルによって検出されたルートに割り当てるディスタンスを入力します。アドミニストレーティブディスタンスは、複数のルーティングプロトコル間でルートを比較するのに使用されるパラメータです。通常は、値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。
転送パスの最大数（Maximum No. of Forward Paths）	ルーティングテーブルにインストールできるISルートの最大数を入力します。指定できる範囲は 1 ～ 8 です。デフォルトは 4 です。
デフォルトルートの配布（Distribute Default Route）	[デフォルトルートの配布（Distribute Default Route）] チェックボックスをオンにしてデフォルトルートを配布するようにISルーティングプロセスを設定し、[ルートマップオブジェクトセレクタ（Route Map Object Selector）] からデフォルトルートを選択します。

[IPv6ファミリ（IPv6 Family）] タブ：[SPF] タブ

フィールド リファレンス

表 *740 : [ISIS IPv6*ファミリ（*ISIS IPv6 Family*）*]* タブ：*[SPF]* タブ

要素	説明
[最短パス優先（Shortest Path First）]	
[このルータをSPF計算の中間ホップとして使用しないように他のルータに通知する（Signal other routers to not use this router as an intermediate hop in their SPF calculations）]	このデバイスを除外する場合は、このチェックボックスをオンにして、以下を設定します。
[起動時の動作を指定（Specify on-startup behavior）]	このオプションを選択した場合は、次のいずれかのオプションを選択する必要があります。 • [BGP収束前に過負荷として自身をアドバタイズする（Advertise overself as overloaded until BGP has converged）] • [再起動後に過負荷として自身をアドバタイズする時間を指定する（Specify time to advertise overself as overloaded after reboot）]：5 ～ 86400 秒の範囲で時間を指定します。
過負荷ビットが設定されている場合、他のプロトコルから学習された IP プレフィックスをアドバタイズしないでください。	IP プレフィックスを除外するには、このチェックボックスをオンにします。
[過負荷ビットが設定されている場合に別のISISレベルから学習されたIPプレフィックスをアドバタイズしない（Don’t advertise IP prefixes learned from another ISIS level when overload bit is set）]	IP プレフィックスを除外するには、このチェックボックスをオンにします。
部分ルート計算の最小間隔	
[PRC間隔（PRC Interval）]	ルータが部分ルート計算（PRC）間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
[PRCの初期待機時間（Initial wait for PRC）]	トポロジ変更後の最初の PRC 計算遅延（ミリ秒単位）を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 2000 ミリ秒です。

要素	説明
[1番目と2番目のPRC間の最小待機時間（Minimum wait between first and second PRC）]	ルータが PRC 間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒です。
SPF 計算の最小間隔	
レベル 1 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。
レベル 2 のパラメータの設定	
[SPF計算の間隔（SPF calculation interval）]	ルータが部分 SPF 計算間で待機する時間を入力します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
[SPF計算の初期待機時間（Initial wait for SPF calculation）]	ルータが SPF 計算で待機する時間を入力します。有効値は 1 ～ 120.000 ミリ秒です。デフォルトは 5500 ミリ秒です。
[1番目と2番目のSPF計算間の最小待機時間（Minimum wait between first and second SPF calculation）]	ルータが SPF 計算間で待機する時間（ミリ秒単位）を入力します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒です。

IPv6 ファミリータブ：再配布タブ

[追加（Add）]/[編集（edit）] ボタンを使用して、再配布ルートを追加または編集します。

フィールド リファレンス

表 *741 : ISIS IPv6* ファミリータブ：再配布タブ

要素	説明
ソース プロトコル	[Source Protocol] ドロップダウン リストから、ISIS ドメインにルートを再配布するプロトコル（[BGP]、[Connected]、[EIGRP]、[OSPF]、[RIP]、または [Static]）を選択します。
プロセス ID（Process ID）	送信元プロトコルのプロセス ID を入力します。
ルートレベル	[Route Level] ドロップダウン リストから、[Level-1]、[Level- 2]、または [Level 1-2] を選択します。
メトリック（Metric）	[メトリック（Metric）] フィールドに、再配布されるルートのメトリックを入力します。指定できる範囲は 1 ～ 4294967295 です。
メトリック タイプ	[Metric Type] で、[internal] または [external] オプション ボタンをクリックします。
ISIS エリア間ルートレベル	
送信元 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
接続先 ISIS レベル	レベル 1 またはレベル 2 を選択します。デフォルトはレベル 1 です。
[同報リスト（Distribution List）]	利用可能なアクセス制御リストから選択するか、新規に追加します。
ルート マップ	[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から、再配布するネットワークをフィルタ処理するために調べる必要があるルートマップを選択するか、[追加（Add）] をクリックして、新しいルートマップを追加するか、既存のルートマップを編集します。
一致（Match）	[Match] チェックボックス（[Internal]、[External 1]、[External 2]、[NSSA External 1]、[NSSA External 2] チェックボックス）を 1 つ以上オンにして、OSPF ネットワークからルートを再配布します。

IPv6 Familyタブ：サマリープレフィックス

続行するには、少なくとも 1 つのネットワーク エンティティ タイトルのエントリを設定する必要があります。

詳細については、[ネットワーク エンティティ タイトル（Network Entity Title）] タブ （2793 ページ）を参照してください。

[追加/編集（Add/Edit）] ボタンを使用して、サマリープレフィックスを追加または編集します。

フィールド リファレンス

表 *742 : ISIS IPv6* ファミリタブ：サマリープレフィックスタブ

要素	説明
IPv6 Summary Prefix	X.X.X.X.::X/0-128 形式の IPv6 プレフィックス。
Apply Summary Prefix into	レベル 1、レベル 2、または両方を選択します。 レベル 1：設定済みアドレスとマスク値を使用して、レベル 1 に再配布されたルートのみが集約されます。 レベル 2：設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートがレベル 2 バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートも集約されます。 両方：ルートをレベル 1 およびレベル 2 IS-IS に再配布したとき、レベル 2 IS-IS がレベル 1 ルートをエリアで到達可能なものとしてアドバタイズするとき、集約経路が適用されます。

[Authentication] タブ

フィールド リファレンス

表 *743 : [ISIS*認証（*Authentication*）*]* タブ

要素	説明
レベル 1 の認証パラメータを設定します。	
タイプ（Type）	ドロップダウン リストから [タイプ（Type）] を選択します。
キー（Key）	ISIS 更新を認証するためのキーを入力します。このキーの最大長は 16 文字です。
確認（Confirm）	キーを確認します。
[送信のみ（Send Only）]	[送信のみ（Send Only）] を有効にするかどうかに応じて、[有効化（Enable）] または [無効化（Disable）] をクリックします。

要素	説明
[モード（Mode）]	認証モードを選択するため、[無効（Disabled）]、[MD5]、[プレーンテキスト（Plaintext）] オプションボタンのいずれかをオンにします。
[エリアパスワード（Area password）]	エリアパスワードを入力し、次のテキストボックスに同じパスワードを入力して確認します。
レベル 2 の認証パラメータを設定します。	
タイプ（Type）	ドロップダウン リストから [タイプ（Type）] を選択します。
キー（Key）	ISIS 更新を認証するためのキーを入力します。このキーの最大長は 16 文字です。
確認（Confirm）	キーを確認します。
[送信のみ（Send Only）]	[送信のみ（Send Only）] を有効にするかどうかに応じて、[有効化（Enable）] または [無効化（Disable）] をクリックします。
[モード（Mode）]	認証モードを選択するため、[無効（Disabled）]、[MD5]、[プレーンテキスト（Plaintext）] オプションボタンのいずれかをオンにします。
ドメイン パスワード	ドメインパスワードを入力し、入力したパスワードを確認します。

リンクステートパケット タブ

フィールド リファレンス

表 *744 : [ISIS*リンクステートパケット（*ISIS Link State Packet*）*]* タブ**

要素	説明
[LSPエラーを無視（Ignore LSP errors）]	[LSPエラーを無視（Ignore LSP errors）] チェックボックスをオンにすると、内部チェックサムエラーのある受信 LSP パケットを、ASA がパージするのではなく無視できるようになります。

要素	説明
[SPFを実行する前にLSPをフラッド（Flood LSPs before running SPF）]	SPF を実行する前に LSP を高速フラッディングおよびフィルするには、このボックスをオンにします。このオプションを選択した場合は、フラッディングする LSP の数を 1 ～ 15 の範囲で入力します。 このパラメータでは、指定した数の LSP が ASA から送信されます。LSP 数が指定されない場合、デフォルト設定は 5 となります。LSP は、SPF の実行前に SPF を呼び出します。高速フラッディングを有効にすることをお勧めします。それにより、LSP のフラッディングプロセスの速度が上げり、ネットワークコンバージェンス時間全体が改善されるからです。デフォルト値は 5 です。
[IPプレフィックスを抑制（Suppress IP prefixes）]	IP プレフィックスを抑制するには、[IPプレフィックスを抑制（Suppress IP prefixes）] チェックボックスをオンにし、以下の 1 つをオンにします。 IS-IS への再配布ルート数に制限がないネットワークでは、LSP がフルになってルートが破棄される可能性があります。これらのオプションを使用することにより、PDU がフルになった場合にどのルートが抑制されるかを制御してください。
[LSPフラグメントが不足した場合に別のISISレベルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from another ISIS level when ran out of LSP fragments）]	別のレベルから来るルートを抑制します。たとえば、レベル 2 の LSP がフルになると、レベル 1 からのルートが抑制されます。
[LSPフラグメントが不足した場合に他のプロトコルから学習されたIPプレフィックスをアドバタイズしない（Don't advertise IP prefixes learned from other protocols when ran out of LSP fragments）]	ASA 上にある再配布済みルートを抑制します。
[LSPの一般的な間隔（LSP General Interval）]	
レベル 1 の LSP 間隔パラメータ	

要素	説明
[LSP計算間隔（LSP Calculation Interval）]	各 LSP の伝送間の間隔を秒数で入力します。範囲は 1 ～ 120 秒です。デフォルトは 5 分です。 接続ネットワーク上の任意の 2 台の ASA 間で想定されるラウンドトリップ遅延より大きな数値にする必要があります。この数は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。再送信が発生するのは、LSP が廃棄される場合だけです。したがって、数を大きい値に設定すると、再コンバージェンスへの影響は小さくなります。ASA のネイバーが多くなるほど、LSP フラッディングの可能性のあるパスが多くなり、この値をより高く設定できます。
[LSP計算の初期待機時間（Initial wait for LSP calculation）]	最初の LSP が生成されるまでの初期待機時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルトは 50 です。
[1番目と2番目の間の最小待機時間（Minimum wait between first and second）]	最初と 2 番目の LSP 生成の間の時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルト値は 5000 です。
レベル 2 の LSP 間隔パラメータ	
[レベル2にもレベル1パラメータを使用する（Use level 1 parameter also for level 2）]	レベル 1 に設定した値をレベル 2 にも適用する場合は、[Use level 1 parameters also for level 2] チェック ボックスをオンにします。
[LSP計算間隔（LSP Calculation Interval）]	各 LSP の伝送間の間隔を秒数で入力します。範囲は 1 ～ 120 秒です。デフォルトは 5 分です。 接続ネットワーク上の任意の 2 台の ASA 間で想定されるラウンドトリップ遅延より大きな数値にする必要があります。この数は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。再送信が発生するのは、LSP が廃棄される場合だけです。したがって、数を大きい値に設定すると、再コンバージェンスへの影響は小さくなります。ASA のネイバーが多くなるほど、LSP フラッディングの可能性のあるパスが多くなり、この値をより高く設定できます。
[LSP計算の初期待機時間（Initial wait for LSP calculation）]	最初の LSP が生成されるまでの初期待機時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルトは 50 です。
[1番目と2番目の間の最小待機時間（Minimum wait between first and second）]	最初と 2 番目の LSP 生成の間の時間をミリ秒単位で入力します。指定できる範囲は 1 ～ 120,000 です。デフォルト値は 5000 です。

要素	説明
[最大LSPサイズ（Maximum LSP size）]	[最大LSPサイズ（Maximum LSP size）] フィールドに秒数を入力します。指定できる範囲は 128 ～ 4352 です。デフォルトは 1492 です。
LSP リフレッシュ インターバル	[LSP refresh interval] フィールドには、LSP 更新間隔の秒数を入力します。指定できる範囲は 1 ～ 65,5535 です。デフォルトは 900 です。 リフレッシュ間隔によって、ソフトウェアが定期的に LSP で発信元のルート トポロジ情報を送信するレートが決定されます。これは、データベース情報が古くなるのを避けるために実行されます。 リフレッシュ間隔を短くすると、増加したリンク利用率のコストで未検出のリンク ステート データベース破損が持続する可能性のある期間が短くなります（破損に対する他の予防措置があるため、これは発生する可能性は極めて低いイベントです）。間隔を長くすると、更新されたパケットのフラッディングによるリンク使用率が低下します（ただしこの使用率は非常に低いです）。
最大 LSP ライフタイム	[Maximum LSP lifetime] フィールドには、ルータのデータベース内に更新なしで LSP が保持される最大秒数を入力します。指定できる範囲は 1 ～ 65535 です。デフォルトは 1200（20 分）です。 LSP の更新間隔を変更した場合、このパラメータを調整する必要があるかもしれません。LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。LSP 更新間隔に設定する値は LSP 最大ライフタイムに設定する値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 更新間隔と比べて LSP ライフタイムを大幅に少なく設定すると、LSP 更新間隔が自動的に短くされて、LSP がタイムアウトしないようになります。

[サマリーアドレス（Summary Address）] タブ

[追加/編集（Add/Edit）] ボタンを使用して、サマリーアドレスを追加または編集します。

フィールド リファレンス

表 *745 : [ISIS*サマリーアドレス（*ISIS Summary Address*）*]* タブ

要素	説明
IP アドレス	サマリールートの IP アドレスを入力します。
ネット マスク（Net Mask）	IP アドレスに適用されるネットワークマスクを選択または入力します。
レベルの選択（Select level）	サマリーアドレスを受信するレベルに応じて、[Level 1]、[Level 2]、または [Level 1 and 2] オプション ボタンをオンにします。
タグ	[Tag] フィールドに、タグの番号を入力します。範囲は 1 ～ 4294967295 です。
メトリック（Metric）	[メトリック（Metric）] フィールドに、サマリールートに適用するメトリックを入力します。範囲は 1 ～ 4294967295 です。デフォルト値は 10 です。

[ネットワーク エンティティ タイトル（Network Entity Title）] タブ

[追加（Add）]/[編集（Edit）] ボタンを使用して、ネットワーク エンティティ タイトルを追加および編集します。

フィールド リファレンス

表 *746 : [ISIS* ネットワーク エンティティ タイトル（*ISIS Network Entity Title*）*]* タブ

要素	説明
[ネットワーク エンティティ タイトル（NET）（Network Entity Title (NET)）]	アドレス形式 48.0000.1111.2222.00 で値を入力します。NET アドレスの合計の長さは 16 ～ 40 文字である必要があります。

要素	説明
[NET プール（NET Pool）]	[選択（Select）] をクリックして、[NET プールオブジェクトセレクタ（NET Pool Object Selector）] ダイアログボックスを開きます。このダイアログボックスを使用すると、NET プールオブジェクトを追加および編集できます。NET プールオブジェクトを追加または編集する方法の詳細については、[NETプールオブジェクトの追加/編集（Add or Edit NET Pool Object）] ダイアログボックス （411 ページ）を参照してください。 NET プールは、個別モードのクラスタデバイスにのみ適用されます。 ネットワーク エンティティ タイトル（NET）は、個別モードのクラスタデバイスには適用されません。
[NET の許容最大数（Maximum allowed NET）]	NET 値を 3 ～ 254 の範囲で入力します。デフォルト値は 3 です。

[Interface] タブ

[Interface] タブを使用して、インターフェイス固有の OSPF 認証ルーティング プロパティを設定します。

ナビゲーション パス

[Interface] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [Add Interface]/[Edit Interface] ダイアログボックス （2846 ページ）

フィールド リファレンス

表 *747 : [Interface]* タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。

要素	説明
認証	インターフェイス上でイネーブルにするOSPF認証のタイプ。認証タイプには、次のいずれかの値を指定できます。 • [None]：OSPF 認証はディセーブルになります。 • [Password]：クリアテキストパスワード認証がイネーブルになります。 • [MD5]：MD5 認証がイネーブルになります。 • [Area]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。 • [キーチェーン（Key Chain）]：キーチェーン認証を許可します。
ポイントツーポイント	インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は「true」が表示されます。インターフェイスがブロードキャストに設定されている場合は、「false」が表示されます。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。
プライオリティ	インターフェイスに割り当てられる OSPF プライオリティ。
MTU Ignore	MTU不一致検出がイネーブルの場合は、「false」が表示されます。MTU不一致検出がディセーブルの場合は「true」が表示されます。
Database Filter	同期およびフラッディング中に発信 LSA がフィルタリングされる場合は、「true」が表示されます。フィルタリングがイネーブルではない場合は「false」を表示します。
Hello 間隔（Hello Interval）	インターフェイス上で送信されるhelloパケット間の間隔（秒数）。hello間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。

要素	説明
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
再送信間隔（Retransmit Interval）	インターフェイスに属する隣接関係へのLSA再送信間の時間（秒数）。ルータが自身のネイバーにLSAを送信する場合、ルータは確認応答メッセージを受信するまでそのLSAを保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
dead 間隔（Dead Interval）	hello パケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。有効値の範囲は1 ～ 65535 です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。
Hello Multiplier （ASA 9.2(1) 以降のみ）	1 秒あたりに送信される hello パケットの数。有効な値は、3 ～ 20 です。

[インターフェイス（Interface）] タブ：[全般（General）] タブ

フィールド リファレンス

表 *748 : [ISIS* インターフェイス（*ISIS Interface*）*]* タブ：*[*全般（*General*）*]* タブ

要素	説明
インターフェイス（Interface）	使用可能なインターフェイスからインターフェイスを選択します。
[このインターフェイスでのISISのシャットダウン（Shutdown ISIS on this interface）]	[Shutdown ISIS on this interface]：設定パラメータを削除することなく、このインターフェイスの IS-IS プロトコルを無効化できます。IS-IS プロトコルはこのインターフェイスの隣接関係（アジャセンシー）を形成しません。ASA が生成した LSP にインターフェイスの IP アドレスが設定されます。

要素	説明
[このインターフェイスで ISIS を有効化（Enable ISIS on this interface）]	選択したインターフェイスで IS-IS プロトコルを有効にします。
[このインターフェイスで IPv6 ISIS を有効化（Enable IPv6 ISIS on this interface）]	選択したインターフェイスで IPv6 IS-IS ルーティングを有効にします。
[レベル 1 のプライオリティ（Priority for level 1）]	レベル 1 のプライオリティを設定します。プライオリティ値は、LAN 上の指定ルータまたは Designated Intermediate System（DIS）を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つルータが DIS になります。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
[レベル 2 のプライオリティ（Priority for level 2）]	レベル 2 のプライオリティを設定します。プライオリティ値は、LAN 上の指定ルータまたは Designated Intermediate System（DIS）を決める際に使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つルータが DIS になります。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
タグ	この IP プレフィックスが ISIS LSP に設定されている場合に、インターフェイスに設定された IP アドレスにタグを設定します。
[レベル 1 の CSNP 間隔（CSNP Interval for level 1）]	レベル 1 のマルチアクセスネットワークにおける、CSNP の送信間隔の完全なシーケンス番号 PDU（CSNP）を秒数で設定します。このインターバルは指定ルータだけに適用されます。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
[レベル 2 の CSNP 間隔（CSNP Interval for level 2）]	レベル 2 のマルチアクセスネットワークにおける、CSNP の送信間隔の完全なシーケンス番号 PDU（CSNP）を秒数で設定します。このインターバルは指定ルータだけに適用されます。範囲は 0 ～ 65535 です。デフォルトは 10 秒です。
[隣接関係のフィルタ処理（Adjacency filter）]	IS-IS 隣接関係の確立をフィルタ処理します。
[すべてのエリアアドレスに一致（Match all area addresses）]	隣接関係（アジャセンシー）を受け入れるには、すべての NSAP アドレスがフィルタと一致する必要があります。 指定しない場合（デフォルト）、受け入れる隣接関係（アジャセンシー）に関するフィルタに一致する必要があるのは 1 つのアドレスだけです。

[インターフェイス（Interface）] タブ : [認証（Authentication）] タブ

フィールド リファレンス

表 *749 : [ISIS*インターフェイス（*ISIS Interfaces***）*]* タブ *- [*認証（***ISIS Interfaces***）*]* タブ**

要素	説明
レベル 1 パラメータ	
キー タイプ	[クリアテキスト（Clear Text）] または [暗号化（Encrypted）] を選択します。
キー（Key）	IS-IS 更新を認証するためのキーを入力します。範囲は 0 ～ 8 文字です。 [Key] オプションで設定されたパスワードが存在しない場合、キー認証は行われません。 （注） [キータイプ（Key Type）] を [クリアテキスト（Clear Text）] として選択した場合は、[キー（Key）] フィールドに最大 17 文字を入力できます。[キー タイプ（Key Type）] を [暗号化（Encrypted）] として選択した場合は、[キー（Key）] フィールドに最大 50 文字を入力できます。
送信のみ（Send only）	[Send only] については、[Enable] または [Disable] のオプション ボタンをクリックします。 [Send only] を選択すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。デフォルトではディセーブルになっています。
[モード（Mode）]	[モード（Mode）] チェックボックスをオンにし、ドロップダウンリストから [MD5] または [テキスト（Text）] を選択します。
[パスワード（Password）]	パスワードを入力します。 （注） いずれかのモードを選択するか、パスワード値を入力できます。
レベル 2 パラメータ	
キー タイプ	[クリアテキスト（Clear Text）] または [暗号化（Encrypted）] を選択します。

要素	説明
キー（Key）	IS-IS 更新を認証するためのキーを入力します。範囲は 0 ～ 8 文字です。 [Key] オプションで設定されたパスワードが存在しない場合、キー認証は行われません。 （注） [キータイプ（Key Type）] を [クリアテキスト（Clear Text）] として選択した場合は、[キー（Key）] フィールドに最大 17 文字を入力できます。[キー タイプ（Key Type）] を [暗号化（Encrypted）] として選択した場合は、[キー（Key）] フィールドに最大 50 文字を入力できます。
送信のみ（Send only）	[Send only] については、[Enable] または [Disable] のオプション ボタンをクリックします。 [Send only] を選択すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。デフォルトではディセーブルになっています。
[モード（Mode）]	[モード（Mode）] チェックボックスをオンにし、ドロップダウンリストから [MD5] または [テキスト（Text）] を選択します。
[パスワード（Password）]	パスワードを入力します。 （注） いずれかのモードを選択するか、パスワード値を入力できます。

[インターフェイス（Interface）] タブ：[Helloパディング（Hello Padding）] タブ

フィールド リファレンス

表 *750 : [ISISインターフェイス（ISIS Interfaces）] タブ：[Helloパディング（Hello Padding）] タブ*

要素	説明
Hello Padding	Hello パディングを有効にします。 最大伝送ユニット（MTU）サイズになるまで IS-IS hello がパディングされます。IS-IS hello をフル MTU に埋め込むことにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。
レベル 1 の最小保留時間 1 秒（Minimal holdtime 1 second for level 1）	LSP がレベル 1 で有効であり続ける保留時間（秒数）を有効にします。

要素	説明
レベル 1 の Hello 間隔（Hello interval for level 1）	レベル 1 の hello パケット間の時間の長さを秒数で指定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。
レベル 2 の最小保留時間 1 秒（Minimal holdtime 1 second for level 2）	LSP がレベル 2 で有効であり続ける保留時間（秒数）を有効にします。
レベル 2 の Hello インターバル（Hello interval for level 2）	レベル 2 の hello パケット間の時間の長さを秒数で指定します。指定できる範囲は 1 ～ 65535 です。デフォルトは 10 です。
レベル 1 のHello 乗数（Hello multiplier for level 1）	ネイバーにおいて欠落できる IS-IS hello パケット数の最大値を指定します。欠落したパケット数がこの値を超えると、ASA は隣接がレベル 1 でダウンしていると宣言します。 IS-IS hello パケットでアドバタイズされる保持時間は、hello インターバルに hello 乗数を掛けた値に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、このルータへの隣接がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内のルータごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。
レベル 2 のHello 乗数（Hello multiplier for level 2）	ネイバーにおいて欠落できる IS-IS hello パケット数の最大値を指定します。欠落したパケット数がこの値を超えると、ASA は隣接がレベル 2 でダウンしていると宣言します。 IS-IS hello パケットでアドバタイズされる保持時間は、hello インターバルに hello 乗数を掛けた値に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、このルータへの隣接がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello インターバル）はインターフェイス単位で設定できます。また、1 つのエリア内のルータごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。
回線タイプの設定（Configure Circuit Type）	ローカルルーティング（レベル 1）、エリアルーティング（レベル 2）、またはローカルとエリアの両方のルーティング（レベル 1-2）のどれについてインターフェイスが設定されているかを指定します。

[インターフェイス（Interface）] タブ：[LSP設定（LSP Settings）] タブ

フィールド リファレンス

表 *751 : [ISIS*インターフェイス（*ISIS Interfaces*）*]* タブ *- [LSP*設定（*LSP Settings*）*]* タブ

要素	説明
ISISプレフィックスのアドバタイズ（Advertise ISIS Prefix）	IS-IS インターフェイスごとの LSP アドバタイズメントで、接続されたネットワークの IP プレフィックスのアドバタイズを許可します。 このオプションを無効にすることは、LSP アドバタイズメントから、接続されたネットワークの IP プレフィックスを除外し、IS-IS コンバージェンス時間を削減するための IS-IS メカニズムです。
再送信間隔（Retransmit Interval）	ポイントツーポイントリンク上にある各 IS-IS LSP の再送信間隔を秒単位で指定します。 接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな数値にする必要があります。指定できる範囲は 0 ～ 65535 です。デフォルトは 5 分です。
Retransmit Throttle Interval	ポイントツーポイント インターフェイス上にある各 IS-IS LSP の再送信間隔をミリ秒単位で指定します。 このオプションは、LSP 再送信トラフィックの制御方法として、多くの LSP およびインターフェイスを持つ大規模なネットワークで役立つ場合があります。このオプションは、インターフェイスで LSP を再送信できるレートを制御します。指定できる範囲は 0 ～ 65535 です。デフォルトは 33 です。
LSP Interval	連続した IS-IS LSP 伝送間の遅延時間をミリ秒単位で指定します。 多数の IS-IS ネイバーやインターフェイスが存在するトポロジでは、LSP 送信および受信を原因とする CPU 負荷が、ルータの障害となる可能性があります。このオプションにより、LSP の送信率（および、暗黙のうちにその他のシステムの受信率）を下げることができます。指定できる範囲は 1 ～ 4294967295 です。デフォルトは 33 です。

[インターフェイス（Interface）] タブ：[メトリック（Metrics）] タブ

フィールド リファレンス

表 *752 : [ISIS*インターフェイス（*ISIS Interface*）*]* タブ：*[*メトリック（*Metrics*）*]* タブ

要素	説明
レベル 1 の指標	

要素	説明
最大メトリック値を使用（Use maximum metric value）	リンクに割り当てるメトリックを指定します。このメトリックは、このリンクを通じてネットワーク内の他の各ルータからその他の宛先へのコストの計算に使用されます。この設定はデフォルトでイネーブルになっています。
デフォルト メトリック	メトリックの番号を入力します。指定できる範囲は 1 ～ 16777214 です。
レベル 2 の指標	
最大メトリック値を使用（Use maximum metric value）	リンクに割り当てるメトリックを指定します。このメトリックは、このリンクを通じてネットワーク内の他の各ルータからその他の宛先へのコストの計算に使用されます。この設定はデフォルトでイネーブルになっています。
デフォルト メトリック	メトリックの番号を入力します。指定できる範囲は 1 ～ 16777214 です。

[パッシブインターフェイス（Passive Interfaces）] タブ

[パッシブインターフェイス（Passive Interfaces）] タブでは、インターフェイスでのルーティングの更新を許可または抑制できます。名前が設定されているインターフェイスのみ、ルーティング更新の送信を抑制できます。

フィールド リファレンス

表 *753 : [ISIS* ネットワーク エンティティ タイトル（*ISIS Network Entity Title*）*]* タブ

要素	説明
パッシブ インターフェイス	次のオプションから選択します。 • [なし（None）] : インターフェイスは選択されません。 • [デフォルト（Default）] : [インターフェイスセレクタ（Interfaces Selector）] ダイアログを開き、除外するインターフェイスを選択します。デフォルトでは、すべてのインターフェイスが選択されます。 • [指定されたインターフェイス（Specified Interfaces）] : [インターフェイスセレクタ（Interfaces Selector）] ダイアログを開き、含めるインターフェイスを選択します。

BFD ルーティングの設定

[BFD] ページには、ファイアウォールデバイスで BFD（Bidirectional Forwarding Detection）ルーティングを設定するための2つのタブがあります。以下のトピックでは、BFDの設定について詳しく説明します。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [BFD]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [BFD]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- BFD について （2803 ページ）
- BFD テンプレートの作成 （2808 ページ）
- [BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックス （2810 ページ）
- [BFDインターフェイスの追加/編集（Add/Edit BFD Interface）] ダイアログボックス （2811 ページ）

BFD について

双方向フォワーディング検出（BFD）は、すべてのメディアタイプ、カプセル化、トポロジ、およびルーティングプロトコルのために短時間での転送パス障害検出を提供するために設計された検出プロトコルです。BFD は、2 つのシステム間の転送データ プロトコルすべてに加えて、ユニキャストのポイントツーポイントモードで動作します。パケットは、メディアやネットワークに対して適切なカプセル化プロトコルのペイロードで送信されます。

BFDは高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD 非同期モードおよびエコー機能

BFD は、エコー機能が有効であるかどうかに関わらず非同期モードで動作できます。

非同期モード

非同期モードでは、システムが相互に BFD 制御パケットを定期的に送信します。一方のシステムがこれらのパケットの多くを連続して受信しない場合、セッションはダウンしているものと宣言されます。純粋な非同期モード（エコー機能なし）では、エコー機能に必要な特定の検出時間を達成するのに必要なパケットの数が半分で済むため、便利です。

BFD エコー機能

BFD エコー機能は、フォワーディング エンジンから、直接接続シングル ホップ BFD ネイバーへエコー パケットを送信します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために同じパスに沿って返信されます。もう一方の BFD セッションは、エコーパケットの実際のフォワーディングに参加しません。エコー機能およびフォワーディングエンジンが検出プロセスを処理するため、BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディングエンジンがリモート ネイバー システムでフォワーディング パスをテストする際にリモート システムが関与しないため、パケット間の遅延のばらつきが改善します。この結果、障害検出にかかる時間が短くなります。

エコー機能が有効な場合、BFD はスロー タイマーを使用して、非同期セッションの時間を長くし、BFD ネイバー間で送信される BFD 制御パケットの数を減らすことができます。これにより、処理オーバーヘッドが削減し、同時に障害検出時間が短くなります。

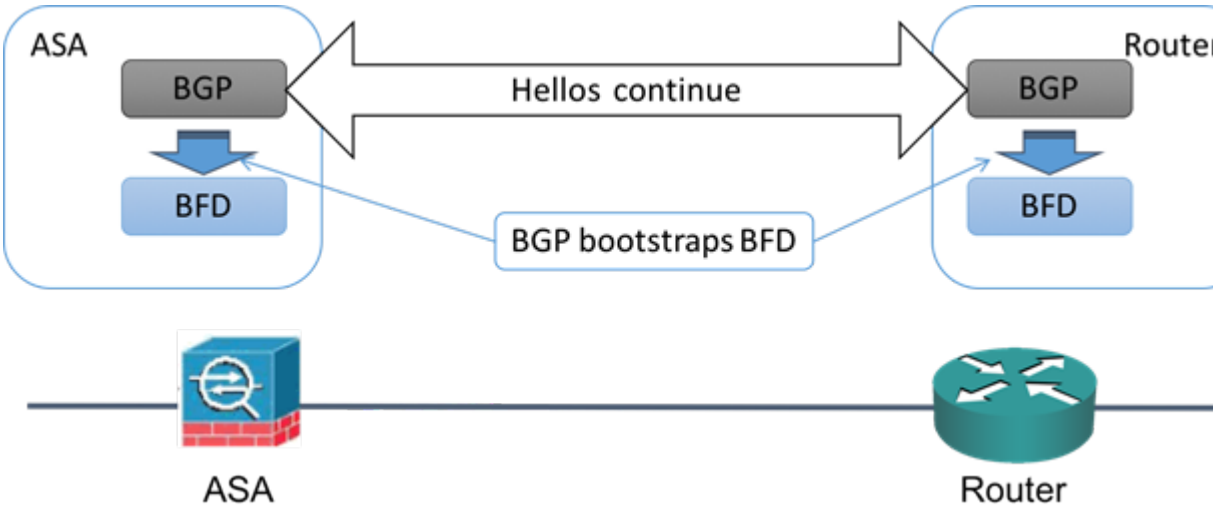
（注） IPv4 マルチホップまたは IPv6 シングルホップ BFD ネイバーでは、エコー機能はサポートされていません。

BFD はインターフェイス レベルとルーティング プロトコル レベルで有効にできます。両方のシステム（BFD ピア）で BFD を設定する必要があります。インターフェイスと、該当するルーティング プロトコルのルータ レベルで BFD を有効にすると、BFD セッションが作成され、BFD タイマーがネゴシエートされ、BFD ピアが BFD コントロール パケットをネゴシエートされたレベルで相互に送信し始めます。

BFD セッション確立

次の例は、ボーダー ゲートウェイ プロトコル（BGP）を実行している ASA とネイバールータを示しています。両方のデバイスが起動した時点では、デバイス間に BFD セッションは確立されていません。

図 *44 : BFD* セッションの開始



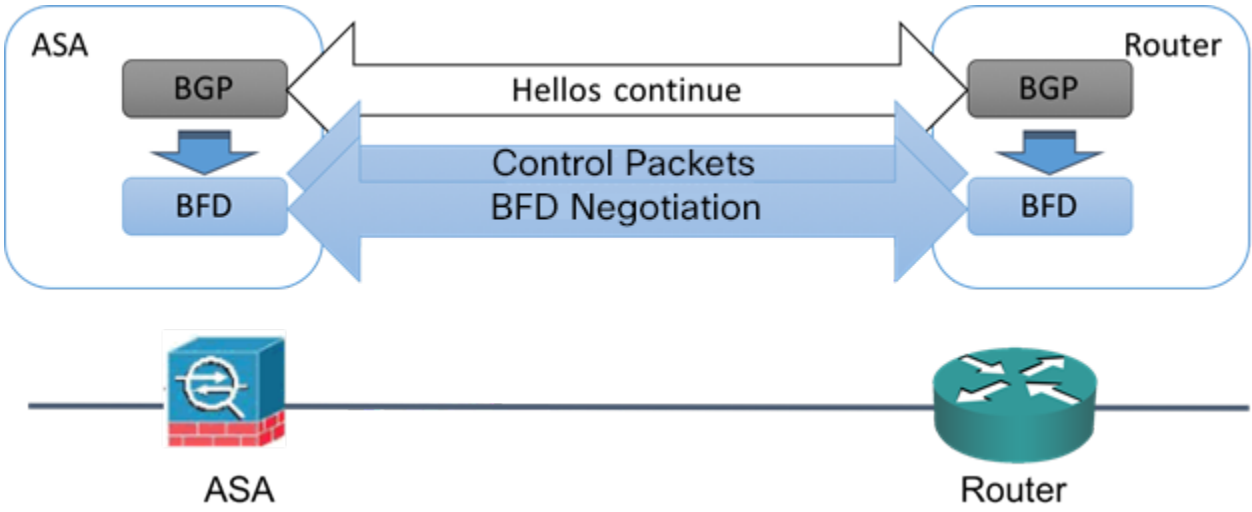
BGP は、BGP ネイバーの特定後に、そのネイバーの IP アドレスを使用して BFD プロセスをブートストラップします。BFD はそのピアを動的に検出しません。BFD は、設定されているルーティング プロトコルから、使用する IP アドレスと形成するピア関係を把握します。

ルータの BFD と ASA の BFD により BFD 制御パケットが形成され、BFD セッションが確立されるまで 1 秒間隔でこのパケットが相互に送信されます。両方のシステムの最初の制御パケットは非常によく似ています。たとえば、Vers、Diag、H、D、P、および F ビットはすべてゼロに設定され、State は Down に設定されます。[My Discriminator] フィールドには、送信デバイスで一意の値が設定されます。[Your Discriminator] フィールドにはゼロが設定されます。これは、BFD セッションがまだ確立されていないためです。TX タイマーと RX タイマーには、デバイスの設定で検出された値が設定されます。

リモート BFD デバイスは、セッション開始フェーズで BFD 制御パケットを受信すると、[My Discriminator] フィールドの値をデバイス自体の [Your Discriminator] フィールドに設定し、[Down] 状態から [Init] 状態、そして最終的には [Up] 状態に移行します。両方のシステムが、相互の制御パケットで各自の Discriminator を検出すると、セッションが正式に確立されます。

次の図は、確立された BFD 接続を示します。

図 *45 : BFD* セッションの確立



BFD タイマー ネゴシエーション

BFD デバイスは、BFD 制御パケットの送信速度を制御および同期するため、BFD タイマーをネゴシエートする必要があります。

BFD タイマーをネゴシエートする前に、デバイスは以下の点を確認する必要があります。

- そのピア デバイスが、ローカル デイバスの提示されるタイマーを含むパケットを確認している。
- ピアで設定されている BFD 制御パケットの受信速度を上回る速度でデバイスが BFD 制御パケットを送信することがない。
- ローカル システムで設定されている BFD 制御パケットの受信速度を上回る速度でピアが BFD 制御パケットを送信することがない。

[Your Discriminator] フィールドと H ビットの設定は、初期タイマーの期間中にリモート デバイスがそのパケットを確認するローカルデバイスを交換できるようにするのに十分です。各システムは BFD 制御パケットを受信すると、Required Min RX Interval をシステム自体の Desired Min TX Interval と比較し、2 つの値のうち大きい方の値（低速な値）を、BDF パケットの転送速度として使用します。2 つのシステムのうち低速なシステムによって、転送速度が決定します。

これらのタイマーがネゴシエートされていない場合、セッション中の任意の時点で、セッションをリセットすることなく再ネゴシエートできます。タイマーを変更するデバイスは、F ビットがセットされている BFD 制御パケットをリモート システムから受信するまで、後続のすべての BFD 制御パケットの P ビットをセットします。このビット交換により、転送中に失われる可能性があるパケットが保護されます。

（注） リモートシステムによってFビットがセットされている場合、新たに提示されるタイマーをリモート システムが受け入れることを意味しているわけではありません。これは、タイマーが変更されたパケットをリモート システムが確認したことを意味します。

BFD 障害検出

BFD セッションとタイマーがネゴシエートすると、BFD のピアは、ネゴシエートされた間隔で BFD 制御パケットを相互に送信します。これらの制御パケットはハートビートの役割を果たします。これは、IGP Hello プロトコルとよく似ていますが、レートはさらに速くなっています。

設定されている検出間隔（必要な最小 RX 間隔）内の BFD 制御パケットを各 BFD ピアが受信する限り、BFD セッションは有効であり、BFD と関連付けられたルーティング プロトコルは隣接関係を維持します。BFD ピアがこの間隔内に制御パケットを受信しない場合、その BFD セッションに参加しているクライアントに障害発生を通知します。ルーティングプロトコルにより、その情報に対する適切な応答が決定されます。標準的な応答は、ルーティングプロトコル ピア セッションを終了し、再コンバージェンスの後、障害の発生したピアをバイパスすることです。

BFD セッション中に BFD ピアが正常に BFD 制御パケットを受信するたびに、このセッションの検出タイマーがゼロにリセットされます。したがって、障害検出は、受信側が最後にパケットを送信した時点ではなく、パケット受信に依存しています。

BFD 導入シナリオ

具体的なシナリオで BFD がどのように動作するかについて、以下に説明します。

フェールオーバー

フェールオーバー シナリオでは、アクティブ ユニットとネイバー ユニット間で BFD セッションが確立、維持されます。スタンバイ ユニットはネイバーとの BFD セッションを維持しません。フェールオーバーが発生すると、新しいアクティブユニットがネイバーとのセッション確立を開始する必要があります。これは、アクティブ ユニットとスタンバイ ユニットの間ではセッション情報が同期されないためです。

グレースフル リスタート/NSF シナリオでは、クライアント（BGP IPv4/IPv6）がそのネイバーに対してイベントを通知します。ネイバーはこの情報を受信すると、フェールオーバーが完了するまで RIB テーブルを維持します。フェールオーバー中に、デバイスで BFD と BGP セッションがダウンします。フェールオーバーが完了し、BGPセッションがアップになると、ネイバー間で新しい BFD セッションが確立されます。

スパンド EtherChannel および L2 クラスタ

スパンド EtherChannel クラスタ シナリオでは、プライマリ ユニットとそのネイバー間で BFD セッションが確立、維持されます。従属ユニットはネイバーとの BFD セッションを維持しません。スイッチでのロードバランシングが原因で BFD パケットが従属ユニットにルーティン

グされる場合、従属ユニットはこのパケットをクラスタリンク経由でプライマリユニットに転送する必要があります。クラスタ スイッチオーバーが発生すると、新しいプライマリ ユニットがネイバーとのセッション確立を開始します。これは、プライマリ ユニットと従属ユニットの間でセッション情報が同期されていないためです。

個別インターフェイス モードと L3 クラスタ

個別インターフェイス モード クラスタのシナリオでは、個々のユニットが各自のネイバーとの BFD セッションを維持します。

BFD テンプレートの作成

このセクションでは、BFD テンプレート ポリシー オブジェクトを作成するために必要な手順を説明します。BFD テンプレートは、一連の BFD 間隔値を指定します。BFD テンプレートで指定された BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。また、シングルホップ セッションとマルチホップ セッションの認証も設定できます。エコーをイネーブルにできるのは、シングルホップのみです。

ナビゲーション パス

[管理（Manage）]> [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [BFDテンプレート（BFD Template）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。

フィールド リファレンス

表 *754 : BFD* テンプレートの追加/編集

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。
設定モード	インターフェイスに関連付けられた BFD の送信元と宛先の間に単一の IP ホップがあるか、複数の IP ホップがあるかを指定します。
エコーの有効化（Enable Echo）	（オプション）選択するとエコーが有効になります。有効にすると、エコーパケットはフォワーディングエンジンによって送信され、検出を実行するために同じパスに沿って返信されます。 （注） これは、単一ホップのコンフィギュレーション モードにのみ適用されます。
[間隔（Interval）]タブ（オプション）	

要素	説明
間隔タイプ（Interval Type）	間隔タイプをマイクロ秒またはミリ秒のどちらで定義するかを指定します。デフォルトの間隔タイプは「なし」です。
送受信の値（間隔値はマイクロ秒単位）（Transmit and Receive Values Interval Values in Microseconds）	このセクションは、間隔タイプがマイクロ秒の場合に有効になります。有効な値は 50000 ～ 999000 マイクロ秒です。 [最小伝送値（Minimum Transmit Values）]：最小伝送間隔機能をマイクロ秒単位で入力します。 [最小受信値（Minimum Receive Values）]：最小受信間隔機能をマイクロ秒単位で入力します。
送受信の値（間隔値はミリ秒単位）（Transmit and Receive Values Interval Values in Milliseconds）	このセクションは、間隔タイプがミリ秒の場合に有効になります。有効値の範囲は、50 ～ 999 ミリ秒です。 [最小伝送値（Minimum Transmit Values）]：最小伝送間隔機能をミリ秒単位で入力します。 [最小受信値（Minimum Receive Values）]：最小受信間隔機能をミリ秒単位で入力します。
乗算値（Multiplier Value）	連続して紛失してよいBFD制御パケットの数を入力します。この数に達すると、BFDはそのピアが利用不可になっていることを宣言します。デフォルト値は 3 です。有効な値は、3 ～ 50 です。
[認証（Authentication）] タブ（オプション）	
認証タイプ（Authentication Type）	BFDテンプレートの認証を設定する場合に選択します。認証に暗号化されたパスワードを使用するか、暗号化されていないパスワードを使用するかを指定します。
Key Value	BFD パスワードを入力して確認します。 • 暗号化された BFD テンプレートの場合、キー値の長さは 17 ～ 66 文字です。 • sha-1 または meticulous-sha-1 認証タイプの暗号化されていない BFD テンプレートの場合、キー値の長さは 29 文字未満でなければなりません。 • md5 または meticulous-md5 認証タイプの暗号化されていない BFD テンプレートの場合、キー値の長さは 25 文字未満である必要があります。
Key ID	認証キー ID を入力します。これは、キー文字列に一致する共有キー ID です。

要素	説明
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可（311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックス

[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックスでは、マルチホップテンプレートに関連付けることができる宛先が含まれているBFDマップを作成できます。マルチホップ BFD テンプレートがすでに設定されている必要があります。詳細については、BFD テンプレートの作成 （2808 ページ）を参照してください。

ナビゲーション パス

[BFDマップの追加/編集（Add/Edit BFD Map）] ダイアログボックスには、[BFD] ページの [マップ（Map）] タブからアクセスできます。新しいBFDマップを追加するには、[行の追加（Add Row）] ボタンをクリックします。既存の BFD マップを編集するには、そのマップを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- BFD テンプレートの作成 （2808 ページ）

フィールド リファレンス

表 *755 : [BFDマップ（BFD Map）] タブ*

要素	説明
BFDテンプレート（BFD Template）	マルチホップ BFD テンプレートを選択するか、マルチホップ BFD テンプレートを追加します。詳細については、BFDテンプレートの作成（2808ページ）を参照してください。

要素	説明
IP バージョン（IP version）	送信元と宛先の適切なアドレス形式（IPv4 または IPv6）を選択します。
IPv4 宛先/プレフィックス、IPv4 送信元/プレフィックス（IPv4 Destination/Prefix, IPv4 Source/Prefix）	宛先と送信元の IPv4 アドレスを、xxxx/プレフィックス形式で適切なフィールドに入力します。
IPv6 宛先/プレフィックス、IPv6 送信元/プレフィックス（IPv6 Destination/ Prefix, IPv6 Source/prefix）	宛先と送信元の IPv6 アドレスを、x:x:x:x:x:x:x:x/プレフィックス形式で適切なフィールドに入力します。
低速タイマー（Slow Timers）	これにより、BFD ネイバー間で送信される BFD 制御パケットの数が削減されます。これにより、非同期セッションの速度が低下し、処理のオーバーヘッドが削減され、障害検出が迅速になります。 低速タイマーのデフォルト値は 1000 で、有効な値は 1000 から 30000 です。

[BFDインターフェイスの追加/編集（Add/Edit BFD Interface）] ダイアログボックス

[BFDインターフェイスの追加（Add BFD Interface）]/[BFDインターフェイスの編集（Edit BFD Interface）] ダイアログボックスを使用すると、BFD テンプレートをインターフェイスにバインドすることで、基準 BFD セッションパラメータの設定およびエコーモードのイネーブル化をインターフェイスごとに行うことができるようになります。

ナビゲーション パス

[BFDインターフェイスの追加（Add BFD Interface）]/[BFDインターフェイスの編集（Edit BFD Interface）] ダイアログボックスには、[インターフェイス（Interfaces）] ページからアクセスできます。新しい BFD インターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックします。既存の BFD インターフェイスを編集するには、そのインターフェイスを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- BFD テンプレートの作成 （2808 ページ）

フィールド リファレンス

表 *756 : [BFD* インターフェイス（*BFD Interface*）*]* タブ

要素	説明
インターフェイス（Interface）	インターフェイス名を入力するか、インターフェイスを選択するか、インターフェイスロールを追加します。
BFDの設定（BFD Configuration）	BFDテンプレートを選択して既存のシングルホップBFDテンプレートを選択するか、シングルホップBFDテンプレートを追加します。または、BFD 間隔を選択します。 詳細については、BFDテンプレートの作成（2808ページ）を参照してください。
BFD間隔（BFD Interval）	
最小伝送間隔値（Minimum Transmit Value）	許容される最小伝送間隔をミリ秒単位で入力します。有効な値は 50 ～ 999 ミリ秒です。
最小受信間隔値（Minimum Receive Value）	許容される最小受信間隔をミリ秒単位で入力します。有効な値は 50 ～ 999 ミリ秒です。
Multiplier（乗数）	連続して紛失してよいBFD制御パケットの数を入力します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言します。デフォルト値は 3 です。有効な値は、3 ～ 50 です。
Echo	（オプション）選択するとエコーが有効になります。有効にすると、エコーパケットはフォワーディングエンジンによって送信され、検出を実行するために同じパスに沿って返信されます。

OSPF の設定

[OSPF] ページには、ファイアウォールデバイス上の Open Shortest Path First（OSPF）ルーティングを設定するための10のタブ付きパネルがあります。ここでは、OSPF のイネーブル化および設定について詳しく説明します。

（注） 設定しているデバイスのバージョンによっては、一部のタブが使用できない場合があります。

（注） ASA バージョン 9.2(1) 以降、特定の OSPF 設定が変更されました。ASA 9.2(1)+ に固有の設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1) より前のバージョンのデバイスに割り当てられていると、検証エラーが発生します。同様に、ASA 9.2(1)+ に適用されなくなった設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1)+ デバイスに割り当てられていると、検証エラーが発生します。

- OSPF について （2813 ページ）
- [General] タブ （2709 ページ）
- [Area] タブ （2823 ページ）
- [Range] タブ （2826 ページ）
- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [Virtual Link] タブ （2833 ページ）
- [Filtering] タブ （2837 ページ）
- [フィルタルール（Filter Rule）] タブ （2840 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interface] タブ （2794 ページ）
- キーチェーンの設定 （2849 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [OSPF] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [OSPF] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

OSPF について

Open Shortest Path First（OSPF）は、パス選択に距離ベクトルではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく Link-State Advertisement（LSA; リンクステート アドバタイズメント）を伝播します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。攻撃者は潜在的に OSPF と他のプロトコル（RIP など）間のルート再配布を使用してルーティング情報を操作できるため、可能なかぎり、すべてのルーティング プロトコルで認証を使用する必要があります。

OSPF がパブリック エリアおよびプライベート エリアで動作しているときに NAT が使用される場合で、アドレス フィルタリングが必要な場合は、2 つの OSPF プロセスを実行する必要があります。パブリック エリア用のプロセスとプライベート エリア用のプロセスです。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータ間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルータに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、セキュリティ アプライアンスが ABR として動作している別々のプライベート エリアとパブリック エリアを持つことができます。タイプ 3 LSA（エリア間ルート）を 1 つのエリアから他のエリアにフィルタリングできます。このことにより、プライベート ネットワークをアドバタイズしなくても、NAT と OSPF を一緒に使用できます。

（注） タイプ 3 LSA だけをフィルタリングできます。プライベート ネットワークでセキュリティ アプライアンスを ASBR として設定すると、セキュリティ アプライアンスはプライベート ネットワークを記述するタイプ 5 LSA を送信します。これは、パブリック エリアを含む自律システム（AS）全体にブロードキャストされます。

NAT が使用されるが、OSPF がパブリック エリアだけで実行されている場合、パブリック ネットワークへのルートは、プライベート ネットワーク内でデフォルトまたはタイプ 5 AS External LSA として再配布できます。ただし、セキュリティ アプライアンスによって保護されているプライベート ネットワークのスタティック ルートを設定する必要があります。また、同じセキュリティ アプライアンス インターフェイスで、パブリック ネットワークとプライベート ネットワークを混在させないでください。

関連項目

- OSPF の設定 （2812 ページ）

[General] タブ

[OSPF] ページの [General] パネルを使用して、最大 2 つの OSPF プロセス インスタンスをイネーブルにします。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。

（注） RIP をイネーブルにしている場合は、OSPF をイネーブルにすることはできません。

ナビゲーション パス

[全般（General）] パネルには、[OSPF] ページからアクセスできます。詳しくは、 OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [Area] タブ （2823 ページ）
- [Range] タブ （2826 ページ）
- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [Virtual Link] タブ （2833 ページ）
- [Filtering] タブ （2837 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interface] タブ （2794 ページ）

フィールド リファレンス

表 *757 : OSPF* の *[General]* タブ

要素	説明
[General] タブには 2 つの同一のセクションがあり、それぞれ 1 つの OSPF プロセスをイネーブルにするために使用されます。各セクションで次のオプションを使用できます。	
Enable this OSPF Process	OSPF プロセスをイネーブルにするには、このチェックボックスをオンにします。セキュリティ アプライアンスで RIP をイネーブルにしている場合は、OSPF プロセスをイネーブルにすることはできません。OSPF プロセスを削除するには、このオプションの選択を解除します。
OSPF プロセス ID（OSPF Process ID）	OSPF プロセスの一意の数値 ID を入力します。このプロセス ID は内部的に使用され、他の OSPF デバイスの OSPF プロセス ID と一致している必要はありません。有効値は 1 ～ 65535 です。

要素	説明
[Advanced] ボタン	[OSPF Advanced] ダイアログボックス （2816 ページ）が開き、[ルータID（Router ID）]、[隣接関係の変更（Adjacency Changes）]、[ルートのアドミニストレーティブディスタンス（Administrative Route Distances）]、[タイマー（Timers）]、[デフォルトの情報送信元（Default Information Originate）] 設定など、その他のプロセス関連パラメータを設定できます。

[OSPF Advanced] ダイアログボックス

[OSPF Advanced] ダイアログボックスを使用して、OSPF プロセスの [Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers]、[Default Information Originate] などの設定を行うことができます。

（注） ASA バージョン 9.2(1) 以降、特定の OSPF 設定が変更されました。ASA 9.2(1)+ に固有の設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1) より前のバージョンのデバイスに割り当てられていると、検証エラーが発生します。同様に、ASA 9.2(1)+ に適用されなくなった設定を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1)+ デバイスに割り当てられていると、検証エラーが発生します。

ナビゲーション パス

[OSPF Advanced] ダイアログボックスには、[General] タブ （2814 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *758 : [OSPF Advanced]* ダイアログボックス

要素	説明
OSPF Process	設定している OSPF プロセスの ID が表示されます。このダイアログボックスでこの値を変更することはできません。
[General] タブ	

要素	説明
ルータ ID（Router ID）	固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択してから、[ルータID（Router ID）] フィールドにルータ ID を IP アドレス形式で入力します。ルータ IDが自動的に生成されるようにするには（セキュリティアプライアンスの最高レベルのIPアドレスがルータ ID として使用されます）、[自動（Automatic）] を選択します。
Ignore LSA MOSPF	このオプションを選択すると、セキュリティ アプライアンスがタイプ 6（MOSPF）LSA パケットを受信したときに、syslog メッセージの送信が抑止されます。
RFC 1583 Compatible	このオプションを選択すると、RFC 1583 に基づいてサマリー ルートのコストが計算されます。このオプションを選択解除すると、RFC 2328 に基づいてサマリー ルートのコストが計算されます。ルーティング ループの可能性を最小限に抑えるには、OSPF ルーティング ドメイン内のすべての OSPF デバイスに同じように RFC 互換性が設定されている必要があります。このオプションは、デフォルトで選択されます。
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [Log Adjacency Changes]：選択すると、OSPF ネイバーの起動またはダウン時に常に、セキュリティ アプライアンスによって syslog メッセージが送信されます。このオプションは、デフォルトで選択されます。 • [Log Adjacency Changes Detail]：選択すると、OSPF ネイバーの起動またはダウン時だけでなく、状態の変更が発生したときに常に、セキュリティ アプライアンスによって syslog メッセージが送信されます。このオプションは、デフォルトでは選択されません。
Administrative Route Distances	ルート タイプに基づく管理ルート ディスタンスの設定。 • [Inter Area]：1 つのエリアから別のエリアへのすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 255 で、デフォルト値は 110 です。 • [Intra Area]：エリア内のすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 255 で、デフォルト値は 110 です。 • [External]：再配布によって学習された他のルーティング ドメインからのすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 255 で、デフォルト値は 110 です。

要素	説明
タイマー	

要素	説明

	ASA 9.2(1)+ デバイスの LSA 着信、LSA ペーシング、およびスロットリングの設定に使用される設定：
	• [LSA着信（LSA Arrival）]：ネイバーから同じ LSA が着信する場合に、同じLSAの着信と着信の間に経過する最小遅延（ミリ秒単位）。有効な範囲は 0 ～ 600,000 ミリ秒です。デフォルトは 1000 ミリ秒です。
	• [LSAフラッドペーシング（LSA Flood Pacing）]：フラッディングキュー内のLSAが更新と更新の間にペーシング処理される時間（ミリ秒単位）。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。
	• [LSA Group Pacing]：LSA がグループにまとめられ、リフレッシュ、チェックサム、およびエージングされる間隔。有効値の範囲は 10 ～ 1800 で、デフォルト値は 240 秒です。
	• [LSA再送信ペーシング（LSA Retransmission Pacing）]：再送信キュー内のLSAがペーシングされる時間（ミリ秒単位）。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は、66 ミリ秒です。
	• [LSAスロットル（LSA Throttle）]：LSA の最初の発信を引き起こす遅延（ミリ秒単位）。有効な値の範囲は、0 ～ 600000 ミリ秒です。このフィールドに値を入力すると、[最小（Min）]および [最大（Max）] フィールドが有効になります。
	  • [最小（Min）]：同じ LSA を発信するための最小遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。
	  • [最大（Max）]：同じ LSA を発信するための最大遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。
	（注） LSAスロットリングの場合、最初に発生する値は最小値以下である必要があり、最小値は最大値以下である必要があります。
	• [SPFスロットル（SPF Throttle）]：SPF 計算への変更を受信する遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。このフィールドに値を入力すると、[最小（Min）] および [最大（Max）] フィールドが有効になります。
	  • [最小（Min）]：1 番目と 2 番目の SPF 計算間の遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。
	  • [最大（Max）]：SPF 計算の最大待機時間。有効値の範囲は、1 ～ 600000 ミリ秒です。

要素	説明
	（注） SPF スロットリングの場合、最初に発生する値は最小値以下である必要があり、最小値は最大値以下である必要があります。 9.2(1) よりも前のデバイスバージョンで、LSA ペーシングおよび SPF 計算タイマーを設定するために使用される設定。 • [SPF Delay]：トポロジ変更の受信と Shortest Path First（SPF）計算の開始の間の時間。有効値の範囲は 0 ～ 65535 で、デフォルト値は 5 秒です。 • [SPF Hold]：連続する SPF 計算間のホールド時間。有効値の範囲は 1 ～ 65534 で、デフォルト値は 10 秒です。 • [LSA Group Pacing]：LSA がグループにまとめられ、リフレッシュ、チェックサム、およびエージングされる間隔。有効値の範囲は 10 ～ 1800 で、デフォルト値は 240 秒です。

要素	説明
デフォルトの情報発信元	OSPF ルーティング ドメインへのデフォルトの外部ルートを生成するために ASBR によって使用される設定。 • [Enable Default Information Originate]：OSPF ルーティング ドメインへのデフォルト ルートの生成をイネーブルにするには、このチェックボックスをオンにします。次のオプションが使用可能になります。 • [Always advertise the default route]：デフォルト ルートを常にアドバタイズするには、このチェックボックスをオンにします。 • [Metric Value]：デフォルト ルートの OSPF メトリックを入力します。有効値の範囲は 0 ～ 16777214 で、デフォルト値は 1 です。 • [Metric Type]：OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプを選択します。選択肢は [1] または [2] で、タイプ 1 またはタイプ 2 外部ルートを示します。デフォルト値は 2 です。 • [ルートマップ（Route Map）]：（任意）適用するルートマップオブジェクトを入力または選択します。ルート マップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて（2897 ページ）を参照してください。
[Nontop Forwarding] タブ （注） Nonstop Forwarding（NSF）は、スパンクラスタモードまたはフェールオーバーモードの ASA 9.3(1)+ デバイスでのみサポートされます。	
[Cisco Nonstop Forwarding機能を有効にする（Enable Cisco Nonstop Forwarding Capability）]	Cisco Nonstop Forwarding（NSF）操作の設定を有効にします。

要素	説明
[Cisco Nonstop Forwarding（NSF）ヘルパーモードの有効化（Enable Cisco Nonstop Forwarding Helper mode）]	Cisco Nonstop Forwarding（NSF）ヘルパーモードを有効にします。 ASA が NSF を有効にしている場合、ASA は NSF 対応であると見なされ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルートプロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパーモードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーのASAはそのノンストップフォワーディングの復帰プロセスを支援します。 再起動するネイバーのノンストップフォワーディングの復帰をASAが支援しないようにする場合は、Cisco Nonstop Forwarding ヘルパーの有効化オプションを解除します。
[Cisco Nonstop Forwardingの有効化（Enable Cisco Nonstop Forwarding）]	Cisco Nonstop Forwarding（NSF）を有効にします。
[非NSF対応のネイバーネットワーキングデバイスが検出されたときにNSF再起動をキャンセルする（Enforce Global）（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected (Enforce Global)）]	NSFグレースフルリスタートの実行時にネットワークインターフェイスで NSF 認識でないネイバーが検出された場合、そのインターフェイスでのみ再起動が中止され、他のインターフェイスではグレースフル リスタートが続行されます。再起動中に非 NSF 対応のネイバーが検出されたときに OSPF プロセス全体の再起動をキャンセルするには、[非NSF対応のネイバーネットワーキングデバイスが検出されたときにNSF再起動をキャンセルする（Enforce Global）（Cancel NSF restart when non-NSF-aware neighboring networking devices are detected (Enforce Global)）] オプションを選択します。 （注） ネイバーとの隣接関係のリセットが任意のインターフェイスで検出された場合、または、OSPF インターフェイスがダウンした場合も、プロセス全体でNSFの再起動がキャンセルされます。
[IETFノンストップフォワーディング機能を有効にする（Enable IETF Non Stop Forwarding Capability）]	Internet Engineering Task Force（IETF）NSF 操作の設定を有効にします。

要素	説明
[IETFノンストップフォワーディングヘルパーモードの有効化（Enable IETF Non Stop Forwarding Helper mode）]	IETF ノンストップ フォワーディング（NSF）ヘルパーモードを有効にします。 ASA が NSF を有効にしている場合、ASA は NSF 対応であると見なされ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルートプロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパーモードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。 再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、IETF ノンストップ フォワーディング ヘルパーの有効化オプションを解除します。
[リンクステートアドバタイズメント（LSA）の厳密なチェックの有効化（Enable Strict Link State advertisement checking）]	IETF NSF ヘルパーモードの厳密なリンクステート アドバタイズメント（LSA）を有効にします。
[IETFノンストップフォワーディングの有効化（Enable IETF Non Stop Forwarding）]	IETF ノンストップ フォワーディング（NSF）を有効にします。
グレースフルリスタート間隔の長さ	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

[Area] タブ

[OSPF] ページの [Area] タブを使用して、OSPF エリアおよびネットワークを設定します。

ナビゲーション パス

[Area] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス （2824 ページ）

- OSPF の設定 （2812 ページ）
- [General] タブ （2814 ページ）
- [Range] タブ （2826 ページ）
- [Neighbors] タブ （2762 ページ）
- [Redistribution] タブ （2764 ページ）
- [Virtual Link] タブ （2833 ページ）
- [Filtering] タブ （2837 ページ）
- [サマリーアドレス（Summary Address）] タブ （2768 ページ）
- [Interface] タブ （2794 ページ）

フィールド リファレンス

表 *759 : [Area]* タブ

要素	説明
OSPF Process	エリアが適用される OSPF プロセス。
エリア ID（Area ID）	エリア ID。
エリア タイプ	エリア タイプ（[Normal]、[Stub]、または [NSSA]）。
ネットワーク	エリア ネットワーク。
オプション	エリア タイプに対して設定するオプション（ある場合）。
認証	エリアに対して設定する認証のタイプ（[None]、[Password]、または [MD5]）。
コスト（Cost）	エリアのデフォルト コスト。

[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス

[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックスを使用して、エリア パラメータ、エリアによって含まれるネットワーク、およびエリアに関連付けられる OSPF プロセスを定義します。

ナビゲーション パス

[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックスには、[Area] タブ （2823 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *760 : [Add Area/Area Networks]/[Edit Area/Area Networks]* ダイアログボックス

要素	説明
OSPF Process	新しいエリアを追加する場合、エリアが追加される OSPF プロセスの OSPF プロセス ID を選択します。セキュリティ アプライアンスでイネーブルにされている OSPF プロセスが 1 つだけの場合、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID を変更することはできません。
エリア ID（Area ID）	新しいエリアを追加する場合、そのエリア ID を入力します。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。
エリア タイプ	
標準	エリアを標準 OSPF エリアにするには、このオプションを選択します。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。
Stub	このオプションを選択すると、エリアはスタブ エリアになります。スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッドされないようにします。スタブエリアを作成すると、[Summary] チェックボックスをオフにすることによって、集約 LSA（タイプ 3 および 4）がそのエリアにフラッドされるのを防ぐことができます。
[サマリー（LSA のスタブエリアへの送信を許可）（Summary (allows sending LSAs into the stub area)）]	定義しているエリアがスタブ エリアである場合、このチェックボックスをオフにすると、LSA はスタブ エリアに送信されません。スタブ エリアの場合、このチェックボックスはデフォルトでオンになっています。
NSSA	エリアを Not-So-Stubby Area にするには、このオプションを選択します。NSSA は、タイプ 7 LSA を受け入れます。NSSA を作成すると、[Summary] チェックボックスをオフにすることによって、集約 LSA がそのエリアにフラッドされるのを防ぐことができます。また、[Redistribute] チェックボックスをオフにし、[Default Information Originate] をイネーブルにすることによって、ルート再配布をディセーブルにすることができます。

要素	説明
Redistribute (imports routes to normal and NSSA areas)	ルートが NSSA にインポートされないようにするには、このチェックボックスをオフにします。このチェックボックスは、デフォルトでオンになっています。
Summary (allows sending LSAs into the NSSA area)	定義しているエリアが NSSA である場合、このチェックボックスをオフにすると、LSA はスタブ エリアに送信されません。NSSA の場合、このチェックボックスはデフォルトでオンになっています。
Default Information Originate (generate a Type 7 default)	タイプ 7 デフォルトを NSSA 内に生成するには、このチェックボックスをオンにします。このチェックボックスは、デフォルトでオフになっています。
メトリック値	デフォルト ルートの OSPF メトリック値を指定します。有効値の範囲は 0 ～ 16777214 です。デフォルト値は 1 です。
メトリック タイプ	デフォルト ルートの OSPF メトリック タイプ。選択肢は、1（タイプ 1）または 2（タイプ 2）です。デフォルト値は 2 です。
ネットワーク（Network）	エリアに追加するネットワークまたはホストの IP アドレスおよびネットワークマスク。デフォルト エリアを作成するには、0.0.0.0 およびネットマスク 0.0.0.0 を使用します。0.0.0.0 は 1 つのエリア内だけで使用できます。 **ヒント** [選択（Select）] をクリックすると、インターフェイス オブジェクトのリストからインターフェイスを選択できます。
認証	OSPF エリア認証の設定が含まれます。 • [None]：OSPF エリア認証をディセーブルにするには、このオプションを選択します。これがデフォルトの設定です。 • [Password]：エリア認証にクリア テキスト パスワードを使用するには、このオプションを選択します。セキュリティ面が懸念される場合、このオプションは推奨しません。 • [MD5]：MD5 認証を使用するには、このオプションを選択します。
デフォルト コスト（Default Cost）	エリアのデフォルト コストを指定します。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 0 ～ 65535、ASA 9.2(1) 以降の場合は 0 ～ 16777214 です。デフォルト値は 1 です。

[Range] タブ

[Range] タブを使用して、エリア間のルートをサマライズします。

ナビゲーション パス

[Range] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [エリア範囲ネットワークの追加/編集（Add/Edit Area Range Network）] ダイアログボックス （2827 ページ）

フィールド リファレンス

表 *761 : [Range]* タブ

要素	説明
プロセス ID（Process ID）	ルート要約と関連付ける OSPF プロセスの ID。
エリア ID（Area ID）	ルート要約と関連付けるエリアの ID。
ネットワーク （Network）	サマリー IP アドレスおよびネットワーク マスク。
[アドバタイズ（Advertise）]	ルート要約がアドレス/マスクペアと一致したときにアドバタイズされる場合は、「true」が表示されます。または、ルート要約がアドレス/マスク ペアと一致したときに抑止される場合は、「false」が表示されます。

[エリア範囲ネットワークの追加/編集（Add/Edit Area Range Network）] ダイアログボックス

[Add Area Range Network]/[Edit Area Range Network] ダイアログボックスを使用して、[Route Summarization] テーブルに新しいエントリを追加するか、既存のエントリを変更します。

ナビゲーション パス

[Add Area Range Network]/[Edit Area Range Network] ダイアログボックスには、[Range] タブ（2826 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *762 : [*エリア範囲ネットワークの追加/編集（*Add/Edit Area Range Network*）*]* ダイアログボックス

要素	説明
OSPF Process	ルート要約が適用される OSPF プロセスを選択します。既存のルート要約エントリを編集する場合、この値は変更できません。
領域	ルート要約が適用されるエリアのエリア ID を選択します。既存のルート要約エントリを編集する場合、この値は変更できません。
ネットワーク（Network）	サマライズされているルートのネットワークの IP アドレスおよびマスク。 ヒント　[選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
[アドバタイズ（Advertise）]	アドレスの範囲ステータスを「アドバタイズ」に設定するには、このチェックボックスをオンにします。これにより、タイプ 3 集約 LSA が生成されます。指定したネットワークのタイプ 3 集約 LSA を抑止するには、このチェックボックスをオフにします。

[Neighbors] タブ

[ネイバー（Neighbors）] タブを使用して、静的ネイバーを手動で定義します。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを定義する必要があります。また、[Neighbors] テーブルのスタティック ネイバーごとに、スタティック ルートを定義する必要があります。

ナビゲーション パス

[Neighbors] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定　（2812 ページ）を参照してください。

関連項目

- [Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックス　（2829 ページ）

フィールド リファレンス

表 *763 : [Neighbors]* タブ

要素	説明
OSPF Process	スタティック ネイバーと関連付ける OSPF プロセス。
ネイバー	スタティック ネイバーの IP アドレス。

要素	説明
インターフェイス	スタティック ネイバーと関連付けるインターフェイス。

[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックス

スタティック ネイバーを定義するか、または既存のスタティック ネイバーの情報を変更するには、[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックスを使用します。ポイントツーポイントの非ブロードキャスト インターフェイスごとに、スタティック ネイバーを定義する必要があります。

ナビゲーション パス

[Add Static Neighbor]/[Edit Static Neighbor] ダイアログボックスには、[Neighbors] タブ （2828 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *764 : [Add Static Neighbor]/[Edit Static Neighbor]* ダイアログボックス

要素	説明
OSPF Process	スタティック ネイバーと関連付ける OSPF プロセス。
ネイバー	スタティック ネイバーの IP アドレス。 **ヒント** [選択（Select）] をクリックすると、ホストオブジェクトのリストからネイバーを選択できます。
インターフェイス	スタティック ネイバーと関連付けるインターフェイス。 **ヒント** [選択（Select）] をクリックして、インターフェイスオブジェクトのリストからインターフェイスを選択できます。

[Redistribution] タブ

1 つのルーティング ドメインから別のドメインへのルートの再配布ルールを定義するには、[Redistribution] タブを使用します。

ナビゲーション パス

[再配布（Redistribution）] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [Redistribution] ダイアログボックス （2831 ページ）

フィールド リファレンス

表 *765 : [Redistribution]* タブ

要素	説明
OSPF Process	ルート再配布エントリに関連付けられた OSPF プロセス。
ルート タイプ（Route Type）	ルートの再配布元であるソース プロトコル。有効なエントリは次のとおりです。 • [BGP]：BGP ルーティング プロセスからルートを再配布します。 • [Connected]：接続されたルート（インターフェイス上で IP アドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。 • [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。 • [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。 • [RIP]：RIP ルーティング プロセスからルートを再配布します。 • [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
一致（Match）	1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。これらのオプションは、スタティック、接続済み、RIP、BGP、または EIGRP ルートを再配布するときに選択できます。
サブネット	サブネット化されたルートが再配布される場合は、「true」と表示されます。サブネット化されていないルートだけが再配布される場合は、何も表示されません。
メトリック値	ルートに使用されるメトリック。デフォルトのメトリックが使用される場合、このカラムは再配布エントリに対してブランクです。
メトリック タイプ	メトリックがタイプ 1 外部ルートの場合は「1」が表示され、メトリックがタイプ 2 外部ルートの場合は「2」が表示されます。

要素	説明
[タグ値（Tag Value）]	各外部ルートに付加される 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。
ルート マップ	再配布エントリに適用されるルートマップオブジェクトの名前。

[Redistribution] ダイアログボックス

[Redistribution] ダイアログボックスを使用して、再配布ルールを追加するか、[Redistribution] テーブルの既存の再配布ルールを編集します。

ナビゲーション パス

[Redistribution] ダイアログボックスには、[Redistribution] タブ （2829 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *766 : [OSPF Redistribution Settings]* ダイアログボックス

要素	説明
OSPF Process	ルート再配布エントリと関連付ける OSPF プロセスを選択します。

要素	説明
ルート タイプ（Route Type）	ルートが再配布されているソースプロトコルを選択します。次のいずれかのオプションを選択できます。 • [BGP]：BGP ルーティング プロセスからルートを再配布します。 • [Connected]：接続されたルート（インターフェイス上でIPアドレスをイネーブルにすることによって自動的に確立されるルート）を OSPF ルーティング プロセスに再配布します。接続済みルートは、AS の外部として再配布されます。 • [EIGRP]：EIGRP ルーティング プロセスからルートを再配布します。リストから EIGRP ルーティング プロセスの自律システム番号を選択してください。 • [OSPF]：別の OSPF ルーティング プロセスからのルートを再配布します。このプロトコルを選択すると、このダイアログボックスの [Match] のオプションが表示されます。これらのオプションは、スタティック、接続済み、RIP、BGP、または EIGRP ルートを再配布するときに選択できます。 • [RIP]：RIP ルーティング プロセスからルートを再配布します。 • [Static]：スタティック ルートを OSPF ルーティング プロセスに再配布します。
ルーティングプロセス ID（Routing Process ID）	BGP または EIGRP ルーティングプロセスの自律システム（AS）番号です。
一致（Match）	ルートタイプとして OSPF を選択した場合、1 つのルーティングプロトコルから別のルーティングプロトコルへのルート再配布に使用される条件を選択します。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。 • [Internal]：ルートは特定の AS の内部です。 • [External 1]：自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External 2]：自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。 • [NSSA External 1]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。 • [NSSA External 2]：自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

要素	説明
メトリック値	再配布されるルートのメトリック値。有効値の範囲は1～16777214です。同じデバイス上で1つのOSPFプロセスから別のOSPFプロセスに再配布する場合、メトリック値を指定しないと、メトリックは1つのプロセスから他のプロセスへ存続します。他のプロセスをOSPFプロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは20です。
メトリック タイプ	メトリックがタイプ1外部ルートの場合は「1」を選択し、メトリックがタイプ2外部ルートの場合は「2」を選択します。
[タグ値（Tag Value）]	タグ値は、各外部ルートに付加される32ビットの10進値です。これはOSPF自体には使用されません。ASBR間での情報通信に使用されることはあります。有効値の範囲は、0～4294967295です。
Use Subnets	選択すると、サブネット化されたルートの再配布がイネーブルになります。サブネット化されていないルートだけを再配布するには、このチェックボックスをオフにします。
ルート マップ	再配布エントリに適用するルートマップオブジェクトを入力または選択します。 **ヒント** [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897ページ）を参照してください。

[Virtual Link] タブ

[Virtual Link] タブを使用して、仮想リンクを作成します。OSPFネットワークにエリアを追加し、そのエリアをバックボーンエリアに直接接続できない場合、仮想リンクを作成する必要があります。仮想リンクは、通過エリアと呼ばれる共通エリアを持つ2つのOSPFデバイスを接続します。OSPFデバイスのいずれかは、バックボーン エリアに接続されている必要があります。

ナビゲーション パス

[Virtual Link] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPFの設定 （2812ページ）を参照してください。

関連項目

- [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス （2834ページ）

フィールド リファレンス

表 767 : [Virtual Link] タブ

要素	説明
OSPF Process	仮想リンクと関連付ける OSPF プロセス。
エリア ID（Area ID）	通過エリアの ID。
Peer Router	仮想リンク ネイバーの IP アドレス。
認証	仮想リンクによって使用される認証のタイプを表示します。 • [None]：認証は使用されません。 • [Password]：クリアテキスト パスワード認証が使用されます。 • [MD5]：MD5 認証が使用されます。 • [キーチェーン（Key Chain）]：キーチェーン認証を有効にします。

[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス

[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックスを使用して、仮想リンクを定義するか、既存の仮想リンクのプロパティを変更します。

ナビゲーション パス

[Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックスには、[Virtual Link] タブ （2833 ページ）からアクセスできます。

関連項目

- [Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス （2837 ページ）
- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 768 : [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス

要素	説明
OSPF Process	仮想リンクと関連付ける OSPF プロセスを選択します。

要素	説明
エリア ID（Area ID）	ネイバー OSPF デバイスによって共有されるエリアを選択します。選択するエリアは、NSSA またはスタブ エリアであってはなりません。
Peer Router	仮想リンク ネイバーの IP アドレスを入力します。
Hello 間隔（Hello Interval）	インターフェイス上で送信される hello パケット間の間隔（秒数）。hello 間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。デフォルト値は 10 秒です。
再送信間隔（Retransmit Interval）	インターフェイスに属する隣接関係への LSA 再送信間の時間（秒数）。ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。ルータは、確認応答メッセージを受信しないと、LSA を再び送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。デフォルト値は 5 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。デフォルト値は 1 秒です。
dead 間隔（Dead Interval）	hello パケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。有効な値の範囲は、9.2(1) より前の ASA デバイスの場合は 1 ～ 65535 秒、ASA 9.2(1) 以降の場合は 1 ～ 8192 秒です。このフィールドのデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

要素	説明
認証	OSPF 認証オプションを含みます。 • [None]：OSPF 認証をディセーブルにするには、このオプションを選択します。 • [エリア（Area）]：エリアに対して指定された認証タイプを使用するには、このオプションを選択します。エリア認証の設定については、[Add Area/Area Networks]/[Edit Area/Area Networks] ダイアログボックス （2824 ページ）を参照してください。エリア認証はデフォルトでディセーブルになっています。したがって、それ以前にエリア認証タイプを指定していない限り、エリア認証を設定するインターフェイスでは、設定するまで認証がディセーブルになっています。 • [Password]：クリアテキストパスワード認証を使用するには、このオプションを選択します。セキュリティ面が懸念される場合は推奨しません。 • [MD5]：MD5 認証を使用するには、このオプションを選択します（推奨）。 • [キーチェーン（Key Chain）]：キーチェーン認証を使用するには、このオプションを選択します。
Key Chain	このフィールドは、キー チェーン認証がイネーブルになっている場合に表示されます。][選択（Select）]をクリックして、設定されたキーチェーンを選択します。設定手順については、 キーチェーンの設定 （2849 ページ）を参照してください。 （注） 隣接関係を正常に確立するには、ピアに対して同じ認証タイプとキー ID を使用します。
認証パスワード（Authentication Password）	パスワード認証をイネーブルにした場合のパスワード入力設定を指定します。 • [Password]：最大 8 文字のテキスト文字列を入力します。 • [Confirm]：パスワードを再入力します。

MD5のIDとキー（MD5 ID and Keys）	MD5 認証をイネーブルにした場合、MD5 キーおよびパラメータの入力設定を指定します。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。
	• [MD5キーIDとMD5キー（MD5 Key ID and MD5 Key）] テーブル
	  • [MD5 Key ID]：数値のキー ID。有効値の範囲は、1 ～ 255 です。
	  • [MD5キー（MD5 Key）]：最大 16 バイトの英数字文字列。

[Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス

仮想リンクの認証用の MD5 キーを定義するには、[OSPF 仮想リンク MD5 設定の追加（Add OSPF Virtual Link MD5 Configuration）]/[OSPF 仮想リンク MD5 設定の編集（Edit OSPF Virtual Link MD5 Configuration）] ダイアログボックスを使用します。

ナビゲーション パス

[Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックスには、 [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス （2834 ページ）からアクセスできます。

関連項目

- [Add OSPF Virtual Link Configuration]/[Edit OSPF Virtual Link Configuration] ダイアログボックス （2834 ページ）
- [Virtual Link] タブ （2833 ページ）
- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 769 : [Add OSPF Virtual Link MD5 Configuration]/[Edit OSPF Virtual Link MD5 Configuration] ダイアログボックス

要素	説明
MD5 キー ID（MD5 Key ID）	数値のキー ID。有効値の範囲は、1 ～ 255 です。
MD5 キー（MD5 Key）	最大 16 バイトの英数字文字列。
確認（Confirm）	MD5 キーを再入力します。

[Filtering] タブ

各 OSPF プロセスの ABR タイプ 3 LSA フィルタを設定するには、[Filtering] タブを使用します。ABR タイプ 3 LSA フィルタによって、指定したプレフィックスだけが 1 つのエリアから別のエリアに送信され、その他のプレフィックスはすべて制限されます。このタイプのエリアフィルタリングは、特定の OSPF エリアから、特定の OSPF エリアへ、または同じ OSPF エリアへ同時に適用できます。

利点

OSPF ABR タイプ 3 LSA フィルタリングによって、OSPF エリア間のルート再配布の制御が向上します。

制約事項

フィルタリングされるのは、ABR から送信されるタイプ 3 LSA だけです。

ナビゲーション パス

[Filtering] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [Add Filtering]/[Edit Filtering] ダイアログボックス （2838 ページ）

フィールド リファレンス

表 *770 : [Filtering]* タブ

要素	説明
OSPF Process	フィルタエントリと関連付ける OSPF プロセス。
エリア ID（Area ID）	フィルタ エントリと関連付けるエリアの ID。
プレフィックスリスト名（Prefix List Name）	プレフィックス リストの名前。
Filtered Network	フィルタリングするネットワークの IP アドレスおよびマスク。
トラフィックの方向	OSPF エリアに着信する LSA にフィルタエントリが適用される場合「Inbound」を、OSPF エリアから発信される LSA に適用される場合は「Outbound」を表示します。
シーケンス番号（Sequence #）	フィルタ エントリのシーケンス番号。複数のフィルタが LSA に適用されている場合、最もシーケンス番号の小さいフィルタが使用されます。
操作	フィルタに一致する LSA が許可される場合は「Permit」を、フィルタに一致する LSA が拒否される場合は「Deny」を表示します。
下限範囲（Lower Range）	照合される最小プレフィックス長。
Upper Range	照合される最大プレフィックス長。

[Add Filtering]/[Edit Filtering] ダイアログボックス

[Add Filtering]/[Edit Filtering] ダイアログボックスを使用して、[Filter] テーブルに新しいフィルタを追加するか、既存のフィルタを変更します。

ナビゲーション パス

[フィルタ処理の追加（Add Filtering）]/[フィルタ処理の編集（Edit Filtering）] ダイアログボックスには、[Filtering] タブ （2837 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *771 : [Add Filtering]/[Edit Filtering]* ダイアログボックス

要素	説明
OSPF Process	フィルタ エントリと関連付ける OSPF プロセスを選択します。
エリア ID（Area ID）	フィルタ エントリと関連付けるエリアの ID を選択します。
プレフィックスリスト名	適切なプレフィックス リスト オブジェクトを入力または選択します。 **ヒント** [選択（Select）] をクリックして、プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト セレクタを開きます。オブジェクト プレフィックス リスト オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
Filtered Network	フィルタリングするネットワークの IP アドレスおよびマスクを入力します。
トラフィックの方向	フィルタリングするトラフィックの方向を選択します。OSPF エリアへの LSA をフィルタリングするには [着信（Inbound）] を選択し、OSPF エリアからの LSA をフィルタリングするには [発信（Outbound）] を選択します。
シーケンス番号（Sequence Number）	フィルタのシーケンス番号を入力します。有効値の範囲は 1 ～ 4294967294 です。複数のフィルタが LSA に適用されている場合、最もシーケンス番号の小さいフィルタが使用されます。
操作	LSA トラフィックを許可するには [許可（Permit）] を選択し、LSA トラフィックをブロックするには [拒否（Deny）] を選択します。
下限範囲（Lower Range）	照合される最小プレフィックス長を指定します。この設定の値は、[Filtered Network] フィールドに入力するネットワーク マスクの長さよりも大きく、[Upper Range] フィールドに入力する値（ある場合）以下である必要があります。

要素	説明
Upper Range	照合される最大プレフィックス長を入力します。この設定の値は、[Lower Range] フィールドに入力する値（ある場合）以上である必要があります。または、[Lower Range] フィールドがブランクの場合は、[Filtered Network] フィールドに入力するネットワーク マスクの長さよりも大きい値である必要があります。

[フィルタルール（Filter Rule）] タブ

[フィルタルール（Filter Rule）] タブを使用して、Open Shortest Path First（OSPF）アップデートで送受信されるネットワークをフィルタリングするルールを設定します。

（注） フィルタルールは、ASA 9.2(1)+ でのみサポートされます。

ナビゲーション パス

[フィルタルール（Filter Rule）] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス （2841 ページ）

フィールド リファレンス

表 *772 : [フィルタルール（Filter Rule）] タブ*

要素	説明
プロセス ID（Process ID）	フィルタルールと関連付ける OSPF プロセス。
ACL	標準 IP アクセス リスト名。このリストは、受信されるネットワークとルーティング アップデートで抑制されるネットワークを定義します。
方向	フィルタルールの方向： • [in]：このルールは、着信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [out]：このルールは、発信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。

要素	説明
インターフェイス	（オプション）フィルタルールが適用されるインターフェース。
ルーティングプロセス（Routing Process）	ルーティングプロセス：[なし（None）]、[BGP]、[接続（Connected）]、[EIGRP]、[OSPF]、[RIP]、または [静的（Static）]。
ルーティングプロセス ID（Routing Process ID）	ルーティングプロセスの識別子。

[フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス

[フィルタルールの追加（Add Filter Rule）]/[フィルタルールの編集（Edit Filter Rule）] ダイアログボックスを使用して、既存のフィルタルールテーブルに新しいフィルタルールを追加するか、または既存のフィルタルールを変更します。

（注） フィルタ ルールは、ASA 9.2(1)+ でのみサポートされます。

ナビゲーション パス

[フィルタルールの追加（Add Filter Rule）]/[フィルタルールの編集（Edit Filter Rule）] ダイアログボックスには、[フィルタルール（Filter Rule）] タブ （2840 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *773 : [フィルタルールの追加/編集（Add/Edit Filter Rule）] ダイアログボックス*

要素	説明
OSPF Process	フィルタルールと関連付ける OSPF プロセスを選択します。
ACL	受信されるネットワークとルーティングアップデートで抑制されるネットワークを定義するアクセス制御リストを選択します。

要素	説明
方向	フィルタルールの方向を指定します。 • [in]：このルールは、着信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。 • [out]：このルールは、発信ルーティングアップデートからのデフォルトルート情報をフィルタリングします。
インターフェイス	（任意）ルーティングアップデートを適用するインターフェイスを指定します。インターフェイスを指定すると、アクセスリストは指定されたインターフェイスで受信されたルーティングアップデートにのみ適用されます。
ルーティングプロセス	[なし（None）]、[BGP]、[接続済み（Connected）]、[EIGRP]、[OSPF]、[RIP]、または [スタティック（Static）] のルーティングプロセスのうち、フィルタ処理するものを選択します。
ルーティングプロセス ID	ルーティングプロセスの識別子を入力します。BGP、EIGRP、EIGRP、および OSPF ルーティングプロトコルに適用されます。

[サマリーアドレス（Summary Address）] タブ

各 OSPF ルーティング プロセスのサマリー アドレスを設定するには、[Summary Address] タブを使用します。

他のルーティングプロトコルから学習したルートをサマライズできます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。集約ルートは、ルーティング テーブルのサイズを削減するのに役立ちます。

OSPF の集約ルートを使用すると、OSPF ASBR は、そのアドレスでカバーされるすべての再配布ルートの集約として、1 つの外部ルートをアドバタイズします。OSPF に再配布されている、他のルーティング プロトコルからのルートだけをサマライズできます。

ナビゲーション パス

[Summary Address] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス （2843 ページ）

フィールド リファレンス

表 *774 : [サマリーアドレス（**Summary Address**）] タブ*

要素	説明
プロセス ID（Process ID）	サマリーアドレスに関連付けられた OSPF プロセス。
ネットワーク（Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。
タグ	各外部ルートに付加される 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。
[アドバタイズ（Advertise）]	サマリールートがアドバタイズされる場合は「true」が表示されます。サマリールートがアドバタイズされない場合は「false」が表示されます。

[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックス

[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックスを使用して、新しいエントリを追加するか、サマリーアドレステーブルの既存のエントリを変更します。

ナビゲーション パス

[サマリーアドレスの追加/編集（Add/Edit Summary Address）] ダイアログボックスには、[サマリーアドレス（Summary Address）] タブ （2842 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *775 : [サマリーアドレスの追加/編集（**Add/Edit Summary Address**）] ダイアログボックス*

要素	説明
OSPF Process	サマリーアドレスに関連付けられた OSPF プロセスを選択します。既存のエントリを編集する場合、この情報は変更できません。
ネットワーク（Network）	サマリーアドレスの IP アドレスおよびネットワークマスク。
タグ	タグ値は、各外部ルートに付加される 32 ビットの 10 進値です。これは OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。有効値の範囲は、0 ～ 4294967295 です。

要素	説明
[アドバタイズ（Advertise）]	選択すると、サマリー ルートがアドバタイズされます。サマリー アドレスになるルートを抑止するには、このチェックボックスをオフにします。デフォルトでは、このチェックボックスはオンです。

[Interface] タブ

[Interface] タブを使用して、インターフェイス固有の OSPF 認証ルーティング プロパティを設定します。

ナビゲーション パス

[Interface] タブには、[OSPF] ページからアクセスできます。[OSPF] ページの詳細については、OSPF の設定 （2812 ページ）を参照してください。

関連項目

- [Add Interface]/[Edit Interface] ダイアログボックス （2846 ページ）

フィールド リファレンス

表 776 : [Interface] タブ

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。
認証	インターフェイス上でイネーブルにする OSPF 認証のタイプ。認証タイプには、次のいずれかの値を指定できます。 • [None]：OSPF 認証はディセーブルになります。 • [Password]：クリア テキスト パスワード認証がイネーブルになります。 • [MD5]：MD5 認証がイネーブルになります。 • [Area]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。 • [キーチェーン（Key Chain）]：キーチェーン認証を許可します。

要素	説明
ポイントツーポイント	インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は「true」が表示されます。インターフェイスがブロードキャストに設定されている場合は、「false」が表示されます。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。
プライオリティ	インターフェイスに割り当てられる OSPF プライオリティ。
MTU Ignore	MTU不一致検出がイネーブルの場合は、「false」が表示されます。MTU不一致検出がディセーブルの場合は「true」が表示されます。
Database Filter	同期およびフラッディング中に発信 LSA がフィルタリングされる場合は、「true」が表示されます。フィルタリングがイネーブルではない場合は「false」を表示します。
Hello 間隔（Hello Interval）	インターフェイス上で送信されるhelloパケット間の間隔（秒数）。hello間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 10 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。
再送信間隔（Retransmit Interval）	インターフェイスに属する隣接関係へのLSA再送信間の時間（秒数）。ルータが自身のネイバーにLSAを送信する場合、ルータは確認応答メッセージを受信するまでそのLSAを保持します。確認応答を受信しなかった場合、ルータでは LSA を再送します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。デフォルト値は 5 秒です。
dead 間隔（Dead Interval）	hello パケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。有効値の範囲は1～65535です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。

要素	説明
Hello Multiplier （ASA 9.2(1) 以降のみ）	1 秒あたりに送信される hello パケットの数。有効な値は、3 ～ 20 です。

[Add Interface]/[Edit Interface] ダイアログボックス

[Add Interface]/[Edit Interface] ダイアログボックスを使用して、インターフェイスの OSPF 認証ルーティング プロパティを追加するか、既存のエントリを変更します。

（注） ASA バージョン 9.2(1) 以降、Hello 間隔、送信遅延、再送信間隔、およびデッド間隔の許容エントリの上限が 65535 秒から 8192 秒に削減されました。8192 を超える値を使用する共有ポリシーを設定した場合、そのポリシーが 9.2(1) 以降のデバイスに割り当てられていると、検証エラーが送信されます。

ナビゲーション パス

[Add Interface]/[Edit Interface] ダイアログボックスには、[Interface] タブ （2794 ページ）からアクセスできます。

関連項目

- OSPF の設定 （2812 ページ）

フィールド リファレンス

表 *777 : [Add Interface]/[Edit Interface]* ダイアログボックス

要素	説明
インターフェイス（Interface）	設定が適用されるインターフェイスの名前。

要素	説明
認証	インターフェイス上でイネーブルにする OSPF 認証のタイプ。認証タイプには、次のいずれかの値を指定できます。 • [認証なし（No Authentication）]：OSPF 認証が無効になります。 • [Area Authentication]：エリアに対して指定された認証タイプがインターフェイスでイネーブルになります。エリア認証が、インターフェイスのデフォルト値です。ただし、エリア認証は、デフォルトではディセーブルになっています。そのため、あらかじめエリア認証タイプを指定してある場合を除いて、エリア認証を指定したインターフェイスでは認証がディセーブルになります。 • [パスワード認証（Password Authentication）]：クリアテキストパスワード認証を有効にします。 • [MD5 Authentication]：MD5 認証がイネーブルになります。 • [キーチェーン（Key Chain）]：キーチェーン認証を有効にします。
Key Chain	[選択（Select）] をクリックして、設定されたキーチェーンを選択します。設定手順については、キーチェーンの設定 （2849 ページ）を参照してください。 （注） 隣接関係を正常に確立するには、ピアに対して同じ認証タイプとキー ID を使用します。
認証パスワード（Authentication Password）	パスワード認証をイネーブルにした場合のパスワード入力設定を指定します。 • [Enter Password]：最大 8 文字のテキスト文字列を入力します。 • [Confirm]：パスワードを再入力します。
MD5 キー ID とキー（MD5 Key ID and Keys）	MD5 認証をイネーブルにした場合、MD5 キーおよびパラメータの入力設定を指定します。OSPF 認証を使用するインターフェイス上のすべてのデバイスで、同じ MD5 キーおよび ID を使用する必要があります。 • [Key ID]：数値のキー ID を入力します。有効値の範囲は、1 ～ 255 です。 • [Key]：最大 16 バイトの英数字文字列。 • [Confirm]：MD5 キーを再入力します。 上記の値を入力し、[>>] をクリックしてキー情報を [キー（Keys）] テーブルに追加します。キーエントリを選択し、[<<] をクリックして [キー（Keys）] テーブルから削除します。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。

要素	説明
プライオリティ	インターフェイスに割り当てられる OSPF プライオリティ。
MTU Ignore	選択すると、MTU 不一致検出がディセーブルになります。MTU 不一致検出をイネーブルにするには、このチェックボックスをオフにします。
データベースフィルタ All Out（Database Filter All Out）	選択すると、同期およびフラッディング中に発信 LSA がフィルタリングされます。フィルタリングをディセーブルにするには、このチェックボックスをオフにします。
Hello 間隔（秒）（Hello Interval (sec)）	インターフェイス上で送信される hello パケット間の間隔（秒数）。hello間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 10 秒です。
Transmit Delay (sec)	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 1 秒です。
再送信間隔（Retransmit Interval）（秒）	インターフェイスに属する隣接関係へのLSA再送信間の時間（秒数）。ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。ルータは、確認応答メッセージを受信しないと、LSA を再び送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。デフォルト値は 5 秒です。

要素	説明
デッド間隔（Dead Interval）（秒）	hello パケットが受信されないために、ネイバーがルータ ダウンを宣言するまでの時間間隔（秒数）。 ASA 9.2(1)+ デバイスでは、有効な値の範囲は 1 ～ 8192 秒です。その他すべてのデバイスでは、有効な値の範囲は 1 ～ 65535 秒です。この設定のデフォルト値は、[Hello Interval] フィールドに設定されている時間間隔の 4 倍です。
hello 乗数（Hello Multiplier）（Hello/秒） （ASA 9.2(1)+ のみ）	1 秒あたりに送信される hello パケットの数。有効な値は、3 ～ 20 です。 （注） Hello 乗数を指定すると、Hello 間隔とデッド間隔の値は無視されます。Hello 間隔またはデッド間隔の値を入力した場合、Hello 間隔およびデッド間隔の設定の代わりに Hello 乗数を使用するかどうかを確認するように求められます。
ポイントツーポイント	インターフェイスが非ブロードキャスト（ポイントツーポイント）に設定されている場合は「true」が表示されます。インターフェイスがブロードキャストに設定されている場合は、「false」が表示されます。

キーチェーンの設定

ネットワークデバイスは、データセキュリティと保護を向上させるため、IGP ピアを認証するために 180 日以下の期間の循環キーを使用して設定されます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。このように設定すると、アクティブなキーの不在によりキーで保護された通信が失われるのを防ぐことができます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

Cisco Security Manager のキーチェーン設定には、次の 2 つの制限があります。

- 設定されたキー ID は、[OOB (Out of Band) Changes] ダイアログボックス （541 ページ）では暗号化されていない形式で表示されます
- プロビジョニングをコピーするオプションは、キーチェーンでは利用できません。

関連項目

- キーのライフタイム （2850 ページ）
- キーチェーンの追加/編集 （2850 ページ）

キーのライフタイム

安定した通信を維持するためには、各デバイスがキー チェーンの認証キーを保存し、複数のキーを同時に機能に使用します。キーの送信と受け入れのライフタイムに基づき、キーのロールオーバーを処理するセキュアなメカニズムがキーチェーン管理によって提供されます。デバイスは、キーのライフタイムを使用してキーチェーン内でアクティブになっているキーを判断します。

キー チェーン内の各キーには 2 つのライフタイムがあります。

- 受け入れライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
- 送信ライフタイム：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイム中、デバイスはルーティング アップデート パケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

ライフタイムが設定されていない場合は、タイムラインなしで MD5 認証を設定するのと同じことになります。

キーの選択

- キー チェンに複数の有効なキーがある場合、OSPF はライフタイムが最大のキーを選択します。
- ライフタイムが無限のキーが優先されます。
- ライフタイムが同じキーが複数ある場合は、もっとも大きなキー ID を持つキーが優先されます。

関連項目

- キーチェーンの設定 （2849 ページ）
- キーチェーンの追加/編集 （2850 ページ）

キーチェーンの追加/編集

[キーチェーンの追加/編集（Add/Edit KeyChain）] ダイアログボックスを使用して、新しいエントリを追加するか、キーチェーンテーブルの既存のエントリを変更します。

ナビゲーション パス

- [キーチェーン（Key Chain）] ページタブには、[OSPF] ページの [インターフェイス（Interface）] からアクセスできます。[Interface] タブの詳細については、[Interface] タブ（2794 ページ）を参照してください。
- [管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]>[キーチェーン（Key Chain）] から、[キーチェーンの追加（Add Key Chain）] ページに直接アクセスできます。

ステップ 1 認証用のキーチェーンを含むキー チェーン ポリシー オブジェクトを作成します。

a) [管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択して [Policy Object Manager] ウィンドウを開きます（Policy Object Manager （290 ページ）を参照）。

b) コンテンツテーブルから [キーチェーン（Key Chain）] を選択します。

c) 右クリックし、[新規オブジェクト（New Object）] を選択します。

d) [キーチェーンの追加（Add Key Chain）] ダイアログボックスで、オブジェクトの名前を入力します（Chain 1 など）。

e) [追加（Add）] ボタンをクリックして、キーチェーンエントリを [キーチェーン（Key Chain）] リストに追加します。

ステップ 2 [キーチェーンエントリの追加（Add Key Chain Entry）] ダイアログボックスに関連する値を入力します。

フィールドリファレンス

表 *778 : [キーチェーンエントリの追加（Add Key Chain Entry）] ページ*

要素	説明
アルゴリズム	認証に使用されるデフォルトの暗号化アルゴリズムは MD5 です。
Key ID	0 ～ 255 の範囲の値を入力します。 （注） キー ID は、[OOB (Out of Band) Changes] ダイアログボックス（541 ページ） に暗号化された形式では表示されません。
認証タイプ（Authentication Type）	関連するオプションを選択します。 • [クリアテキスト（Clear Text）]：認証キーをテキスト形式で取得します。 • [暗号化（Encryption）]：認証キーを暗号化された形式にします。
Key String	キー文字列を入力します。
[キー文字列の確認（Confirm Key String）]	同じキー文字列を再入力します。
[受け入れライフタイムの設定（Accept Lifetime Settings）]：別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間を入力します。	
タイムゾーン（Timezone）	[UTC] または [ローカル（Local）] のいずれかを選択します。
[開始日時（Start Date/Time）]	開始日時を hh:mm:ss 形式で入力します。

要素	説明
[終了時間のタイプ（End Time Type）]	関連するオプションを選択します。 • [日時（Date Time）]：ライフタイムが終了する絶対時間。 • [期間（Duration）]：開始時からライフタイムが終了するまでの経過秒数。 • [無限（Infinite）]：無限のライフタイム（終了時間なし）
End Date	絶対的な日時を指定します。このオプションは、[終了時間のタイプ（End Time Type）] として [期間（Duration）] または [無限（Infinite）] を選択した場合は使用できません。
期間	開始時からライフタイムが終了するまでの経過秒数を入力します。許容範囲は 1 ～ 2147483646 です。このオプションは、[終了時間のタイプ（End Time Type）] として [日時（Date Time）] または [無限（Infinite）] を選択した場合は使用できません。
[送信ライフタイムの設定（Send Lifetime Settings）]：別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。	
タイムゾーン（Timezone）	[UTC] または [ローカル（Local）] のいずれかを選択します。
[開始日時（Start Date/Time）]	開始日時を hh:mm:ss 形式で入力します。
[終了時間のタイプ（End Time Type）]	関連するオプションを選択します。 • [日時（Date Time）]：ライフタイムが終了する絶対時間。 • [期間（Duration）]：開始時からライフタイムが終了するまでの経過秒数。 • [無限（Infinite）]：無限のライフタイム（終了時間なし）
End Date	絶対的な日時を指定します。このオプションは、[終了時間のタイプ（End Time Type）] として [期間（Duration）] または [無限（Infinite）] を選択した場合は使用できません。
期間	開始時からライフタイムが終了するまでの経過秒数を入力します。許容範囲は 1 ～ 2147483646 です。このオプションは、[終了時間のタイプ（End Time Type）] として [日時（Date Time）] または [無限（Infinite）] を選択した場合は使用できません。

ステップ 3 [OK] をクリックします。データベースに変更を送信することを忘れないでください。

次のタスク

関連項目

- キーチェーンの設定 （2849 ページ）
- キーのライフタイム （2850 ページ）

OSPFv3 の設定

[OSPFv3] ページには、ファイアウォールデバイスで OSPF（Open Shortest Path First）バージョン 3 ルーティングを設定するための 2 つのタブ付きパネルがあります。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFv3] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [OSPFv3] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

これは、OSPFv3 プロセスを設定して [OSPFv3] ページでインターフェイスに割り当てるための基本的な手順です。

1. [プロセス（Process）] タブ （2856 ページ） で、次の手順を実行します。
   - [OSPFv3プロセス（OSPFv3 Process）] ドロップダウンリストから [プロセス1（Process 1）] または [プロセス2（Process 2）] を選択して、2 つのプロセスのどちらを設定するかを指定します。
   - [OSPFv3プロセスの有効化（Enable OSPFv3 Process）] をオンにします。
   - [プロセスID（Process ID）] を割り当てます。1 ～ 65535 の任意の正の整数を使用できます。
   - プロセスを定義するには、必要に応じて次の機能を使用します。
   - [詳細（Advanced）] ボタン。 [OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス （2857 ページ）が開きます。
   - [エリア（Area）] タブ（OSPFv3） （2863 ページ）。 Add/Edit Area Dialog Box（OSPFv3） （2864 ページ）、 範囲の追加/編集ダイアログボックス（OSPFv3） （2866 ページ）、 Add/Edit Virtual Link Dialog Box（OSPFv3） （2867 ページ）を使用して、エリア、範囲、および仮想リンクの定義を管理します。
   - [再配布（Redistribution）] パネル。 Add/Edit Redistribution Dialog Box（OSPFv3） （2869 ページ）を使用して、ルート再配布の定義を管理します。

- [サマリープレフィックス（Summary Prefix）] パネル。[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3） （2871 ページ）を使用してサマリープレフィックス定義のを管理します。

2. [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （2872 ページ） で、次の手順を実行します。
   1. [インターフェイス（Interface）] パネルと [ネイバー（Neighbor）] パネルで、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3） （2872 ページ）および[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3） （2877 ページ）を使用してプロセスを特定のインターフェイスに割り当てます。

関連項目

- OSPFv3 について （2854 ページ）

OSPFv3 について

Open Shortest Path First（OSPF）は、パス選択に距離ベクトルではなくリンク ステートを使用する Interior Gateway Routing Protocol です。バージョン 3 は、基本的に IPv6 向けに拡張された OSPFv2 です。OSPFv2 に似ていますが（OSPF について （2813 ページ）を参照）、下位互換性はありません。OSPF を使用して IPv4 パケットと IPv6 パケットの両方をルーティングするには、OSPFv2 と OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携しません。

（注） OSPFv3 は、シングルコンテキストのルーテッドモードでのみ動作する ASA 9.0 以降のデバイスでサポートされます。つまり、マルチコンテキストとトランスペアレントモードはサポートされていません。

リンクを、ネットワーキングデバイス上のインターフェイスとして考えます。リンクステートプロトコルは、送信元デバイスと宛先デバイスを接続するリンクの状態に基づいて、ルーティングの決定を行います。リンク ステートは、インターフェイスと、その隣接ネットワーキングデバイスとの関係を説明するものです。インターフェイス情報には、インターフェイスの IPv6 プレフィックス/長、接続先のネットワークのタイプ、そのネットワークに接続されているデバイスなどが含まれます。この情報は、さまざまなタイプのリンクステートアドバタイズメント（LSA）で伝播されます。ルーティングテーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

ASA は、OSPFv3 プロトコルのプロセスを 2 つ同時に異なるインターフェイスセット上で実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスが共存可能ですが、OSPFv3 ではアドレスは重複できません）がある場合に、2 つのプロセスを実行できます。あるいは、ルートのサブセットを 2 つのプロセス間で再配布して、一方のプロセスを内部インターフェイスで実行しながら別のプロセスを外部で実行できます。

同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

別の OSPFv3 ルーティングプロセス、RIP ルーティングプロセス、または OSPFv3 対応インターフェイスで設定されたスタティックルートおよび接続ルートから、ルートを OSPFv3 ルーティングプロセスに再配布できます。

NAT が使用されるが、OSPFv3 がパブリックエリアだけで実行されている場合、パブリックネットワークへのルートは、プライベートネットワーク内でデフォルトまたはタイプ 5 AS External LSA として再配布できます。ただし、セキュリティ アプライアンスによって保護されているプライベート ネットワークのスタティック ルートを設定する必要があります。また、同じセキュリティ アプライアンス インターフェイスで、パブリック ネットワークとプライベート ネットワークを混在させないでください。

OSPFv2 と OSPFv3 の相違点

OSPFv3 では、OSPFv2 の機能に次の機能が追加されます。

- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。
- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。
- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPSec ESP 標準を使用する認証サポート。

設定の制約事項

ASA OSPFv3 設定の制限は次のとおりです。

- 特定のインターフェイスで OSPFv3 をイネーブルにするには、そのインターフェイスで IPv6 を有効にし、名前を付ける必要があります。
- インターフェイスに割り当てることができるのは、1 つのエリアと 1 つのインスタンスを持つ 1 つの OSPFv3 プロセスだけです。
- インターフェイス ネイバーエントリは、OSPFv3 がイネーブルになっている場合にのみ有効であり、ネットワークタイプは指定されたインターフェイスでポイントツーポイントである必要があります。
- インターフェイス ネイバーアドレスは、リンクローカルアドレスである必要があります。

- エリア範囲テーブルの範囲値は、エリア全体で一意である必要があります。
- エリアがNSSAまたはスタブに設定されている場合、同じエリアを仮想リンクに設定することはできません。
- OSPFv3 再配布は、同じ OSPFv3 プロセスには適用されません。
- ASA クラスタで使用する場合は、OSPFv3 暗号化を無効にする必要があります。
- レイヤ 3 クラスタプールは、OSPFv3 とインターフェイスの間で共有されません。

関連項目

- OSPFv3 の設定 （2853 ページ）
- [プロセス（Process）] タブ （2856 ページ）
- [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （2872 ページ）

[プロセス（Process）] タブ

[OSPFv3] ページの [プロセス（Process）] タブを使用して、最大 2 つの OSPFv3 ルーティングプロセスを有効にして設定します。各 OSPF プロセスには、独自のエリアとネットワークが関連付けられます。それぞれについて、最低でも OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスを有効にする必要があります。その後、ターゲットの OSPFv3 ルーティングプロセスにルートを再配布する必要があります。シングルコンテキストモードのみがサポートされていることに注意してください。

ナビゲーション パス

[プロセス（Process）] タブは [OSPFv3] ページにあります。

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFv3] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [OSPFv3] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）
- [エリア（Area）] タブ（OSPFv3） （2863 ページ）
- [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （2872 ページ）

フィールド リファレンス

表 *779 : [プロセス（Process）] タブ*

要素	説明
OSPFv3 Process	設定している OSPFv3 プロセスを識別します。[プロセス1（Process 1）] または [プロセス2（Process 2）] を選択します。1 つまたは両方を有効にすることができます。
OSPFv3 プロセスを有効化	選択した OSPFv3 プロセスを有効にするには、このボックスをオンにします。OSPFv3 プロセスを無効にするには、このオプションの選択を解除します。プロセス設定情報は、後で再度有効にする場合に備えて保持されます。
プロセス ID（Process ID）	このプロセスの一意の数値 ID を入力します。ID には、1 から 65535 までの任意の正の整数を指定できます。 このプロセス ID は内部で使用され、他の OSPFv3 デバイスの OSPFv3 プロセス ID と一致する必要はありません。
詳細設定（Advanced）	[OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス （2857ページ）が開き、[ルータID（Router ID）]、[隣接関係の変更（Adjacency Changes）]、[ルートのアドミニストレーティブディスタンス（Administrative Route Distances）]、[タイマー（Timers）]、[デフォルトの情報送信元（Default Information Originate）]、[パッシブインターフェイス（Passive Interface）] 設定など、その他のプロセス関連パラメータを設定できます。
領域	このパネルのタブとテーブルを使用して、エリア、範囲、および仮想リンクの定義を管理します。これらの定義の詳細については、[エリア（Area）] タブ（OSPFv3） （2863 ページ）を参照してください。
再配布	このパネルを使用して、再配布定義を管理します。これらの定義の詳細については、 Add/Edit Redistribution Dialog Box（OSPFv3） （2869 ページ）を参照してください。
サマリープレフィックス	このパネルを使用して、サマリープレフィックスの定義を管理します。これらの定義の詳細については、[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3） （2871 ページ）を参照してください。

[OSPFv3の詳細プロパティ（OSPFv3 Advanced Properties）] ダイアログボックス

[OSPF Advanced] ダイアログボックスを使用して、OSPF プロセスの [Router ID]、[Adjacency Changes]、[Administrative Route Distances]、[Timers]、[Default Information Originate] などの設定を行うことができます。

ナビゲーション パス

[OSPF Advanced] ダイアログボックスには、[プロセス（Process）] タブ （2856 ページ）からアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）

フィールド リファレンス

表 *780 : [OSPF Advanced]* ダイアログボックス

要素	説明
OSPF Process	この読み取り専用フィールドには、設定している OSPF プロセスの ID が表示されます。
ルータ ID（Router ID）	単一のデバイスで、[自動（Automatic）] または [IPアドレス（IP Address）] を選択します。（[IPアドレス（IP Address）] を選択すると、アドレスフィールドが表示されます） [自動（Automatic）] を選択すると、セキュリティアプライアンス上で最上位の IP アドレスがルータ ID として使用されます。固定ルータ ID を使用するには、[IPアドレス（IP Address）] を選択して、[ルートID（Router ID）] フィールドに IPv4 アドレスを入力します。 デバイスクラスタで、[自動（Automatic）] または [クラスタプール（Cluster Pool）] を選択します。（[クラスタプール（Cluster Pool）] を選択すると、[IPv4プールオブジェクトID（IPv4 Pool object ID）] フィールドが表示されます） [クラスタプール（Cluster Pool）] を選択した場合は、ルータ ID アドレスを提供する IPv4 プールオブジェクトの名前を入力または選択します。詳細については、[IPv4プールの追加または編集（Add or Edit IPv4 Pool）] ダイアログボックス （407 ページ）を参照してください。
Ignore LSA MOSPF	このオプションを選択すると、セキュリティ アプライアンスがタイプ 6（MOSPF）LSA パケットを受信したときに、syslog メッセージの送信が抑止されます。

要素	説明
隣接関係の変更	これらのオプションでは、隣接関係の変更が発生したときに送信される syslog メッセージを指定します。 • [Log Adjacency Changes]：選択すると、OSPF ネイバーの起動またはダウン時に常に、セキュリティ アプライアンスによって syslog メッセージが送信されます。このボックスをチェックすると、[詳細を含める（Include Details）] オプションが有効になります。 • [詳細を含める（Include Details）]：選択すると、ネイバーの起動またはダウン時だけでなく、状態の変更が発生したときにはいつでも、セキュリティアプライアンスによって syslog メッセージが送信されます。このオプションは、[隣接関係の変更を記録（Log Adjacency Changes）] がチェックされている場合にのみ使用できます。
Administrative Route Distances	ルート タイプに基づく管理ルート ディスタンスの設定。 • [Inter Area]：1 つのエリアから別のエリアへのすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 254 で、デフォルト値は 110 です。 • [Intra Area]：エリア内のすべてのルートのアドミニストレーティブ ディスタンス。有効値の範囲は 1 ～ 254 で、デフォルト値は 110 です。 • [External]：再配布によって学習された他のルーティング ドメインからのすべてのルートのアドミニストレーティブディスタンス。有効値の範囲は 1 ～ 254 で、デフォルト値は 110 です。

要素	説明
タイマー（ミリ秒）	

要素	説明
	LSA および SPF スロットリングは、ネットワークが不安定になっている間に OSPFv3 の LSA 更新速度を低下させ、LSA レート制限を提供することにより、より高速な OSPFv3 変換を可能にするダイナミックメカニズムを提供します。LSA ペーシングおよび SPF 計算タイマーを設定するために使用される設定。 • [LSA着信（LSA Arrival）]：ネイバーから着信する同一 LSA の最短受信間隔を指定します。有効な値の範囲は、0 ～ 600000 ミリ秒です。デフォルトは 1000 です。 • [LSAフラッドペーシング（LSA Flood Pacing）]：フラッディングキュー内の LSA が更新と更新の間でペーシングされる時間の長さ。有効値の範囲は、5 ～ 100 ミリ秒です。デフォルト値は 33 です。 • [LSAグループのペーシング（LSA Group Pacing）]：LSA がグループにまとめられ、更新、チェックサム、およびエージングされる間隔。有効値の範囲は 10 ～ 1800 で、デフォルト値は 240 ミリ秒です。 • [LSA再送信のペーシング（LSA Retransmission Pacing）]：再送信キュー内の LSA がペーシングされる時間の長さ。有効値の範囲は、5 ～ 200 ミリ秒です。デフォルト値は 66 です。 • [LSAスロットル（LSA Throttle）]：LSA の最初の発信を引き起こす遅延（ミリ秒単位）。有効な値の範囲は、0 ～ 600000 ミリ秒です。このフィールドに値を入力すると、[最小（min）] および [最大（max）] フィールドが有効になります。 • [最小（min）]：同じ LSA を発信するための最小遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。 • [最大（max）]：同じ LSA を発信するための最大遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。 • [SPFスロットル（SPF Throttle）]：SPF 計算への変更を受信する遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。このフィールドに値を入力すると、[最小（min）] および [最大（max）] フィールドが有効になります。 • [最小（min）]：1 番目と 2 番目の SPF 計算間の遅延。有効値の範囲は、1 ～ 600000 ミリ秒です。 • [最大（max）]：SPF 計算の最大待機時間。有効値の範囲は、1 ～ 600000 ミリ秒です。 （注） LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よ

要素	説明
	りも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。
デフォルトの情報発信元	OSPFv3 ルーティングドメインへのデフォルトの外部ルートを生成するために ASBR によって使用される設定。 • [デフォルトの情報発信元の有効化（Enable Default Information Originate）]：OSPFv3 ルーティングドメインへのデフォルトルートの生成を有効にするには、このチェックボックスをオンにします。次のオプションが使用可能になります。 • [Always advertise the default route]：デフォルト ルートを常にアドバタイズするには、このチェックボックスをオンにします。 • [メトリック値（Metric Value）]：デフォルトルートの生成に使用する OSPFv3 メトリック。有効値の範囲は 0 ～ 16777214 です。 • [メトリックタイプ（Metric Type）]：OSPFv3 ルーティングドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンクタイプ。タイプ 1 外部ルートまたはタイプ 2 外部ルートを示す [1] か [2] を選択します。デフォルト値は 1 です。 • [ルートマップ（Route Map）]：（任意）適用するルートマップオブジェクトの名前を入力または選択します。ルートマップが一致すると、ルーティング プロセスによってデフォルト ルートが生成されます。 ヒント [選択] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて （2897 ページ）を参照してください。
パッシブ インターフェイス	パッシブルーティングは、OSPFv3 ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの OSPFv3 ルーティング更新の送受信を無効にします。 1 つ以上のインターフェイスまたはインターフェイス オブジェクトを入力または選択して、それらのインターフェイスでパッシブ OSPFv3 ルーティングを有効にします。IPv4 および IPv6 アドレスがサポートされます。
[Non Stop Forwarding] タブ （注） Non Stop Forwarding（NSF）は、ASA 9.3(1)+ でのみサポートされています。	

要素	説明
グレースフル リスタート ヘルパーの有効化	グレースフル リスタート ヘルパー モードを有効にします。 ASA で NSF が有効になっている場合、ASA は NSF 対応であると見なされ、グレースフル リスタート モードで動作します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。 再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、グレースフル リスタート ヘルパーの有効化オプションをクリアします。
リンク ステート アドバタイズメントの有効化	リンク ステート アドバタイズメント（LSA）の厳密なチェックを有効にします。 （注） イネーブルにすると、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。
グレースフルリスタートの有効化（スパンドクラスタまたはフェールオーバーが設定されている場合に使用）	ASA でグレースフルリスタートを有効にします。
グレースフルリスタート間隔の長さ	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

[エリア（Area）] タブ（OSPFv3）

[OSPFv3] ページの [プロセス（Process）] タブ （2856 ページ）の [エリア（Area）] パネルを使用して、OSPFv3 エリア、範囲、および仮想リンクを設定します。[エリア（Area）] は、[エリア（Area）]、[範囲（Range）]、および [仮想リンク（Virtual Link）] の 3 つの定義テーブルで構成されています。

- [エリア（Area）] テーブルエントリの追加と編集については、 Add/Edit Area Dialog Box （OSPFv3） （2864 ページ）を参照してください。

- [範囲（Range）]テーブルエントリの追加と編集については、範囲の追加/編集ダイアログボックス（OSPFv3） （2866 ページ）を参照してください。
- [仮想リンク（Virtual Link）] テーブルエントリの追加と編集については、Add/Edit Virtual Link Dialog Box（OSPFv3） （2867 ページ）を参照してください。

Cisco Security Manager テーブルの操作に関する基本情報については、テーブルの使用 （64 ページ）を参照してください。

ナビゲーション パス

[エリア（Area）] タブには、[OSPFv3] ページの [プロセス（Process）] タブ （2856 ページ）からアクセスできます。[OSPFv3] ページの詳細については、OSPFv3 の設定 （2853 ページ）を参照してください。

関連項目

- OSPFv3 について （2854 ページ）
- [OSPFv3インターフェイス（OSPFv3 Interface）] タブ （2872 ページ）

Add/Edit Area Dialog Box（OSPFv3）

[エリアの追加/編集（Add/Edit Area）] ダイアログボックスを使用して、エリアのパラメータを定義します。

ナビゲーション パス

[エリアの追加（Add Area）]/[エリアの編集（Edit Area）] ダイアログボックスには、[エリア（Area）] タブ（OSPFv3） （2863 ページ）からアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）
- [プロセス（Process）] タブ （2856 ページ）

フィールド リファレンス

表 *781 : [*エリアの追加/編集（*Add/Edit Area***）*]* ダイアログボックス**

要素	説明
エリア ID（Area ID）	10 進数または IP アドレスのいずれかを使用して、エリアの ID を入力します。有効な 10 進値の範囲は、0 ～ 4294967295 です。

要素	説明
コスト（Cost）	インターフェイス上でパケットを送信するコスト。有効値は、0 ～ 65535 です。 ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。
タイプ（Type）	次のいずれかを選択して、エリアタイプを定義します。 • [通常（Normal）]：このエリアは標準の OSPF エリアとなります。エリアを最初に作成するときは、このオプションがデフォルトで選択されています。 • [NSSA]：このエリアは「Not-So-Stubby Area」となります。NSSA は、タイプ 7 LSA を受け入れます。このオプションを選択すると、デフォルトの情報発信オプションが有効になります。 NSSA を作成するときに、[このエリアへのサマリーLSAの送信を許可する（Allow Sending summary LSA into this area）] チェックボックスをオフにすると、サマリー LSA がそのエリアにフラッドされるのを防ぐことができます。また、[再配布（Redistribute）] の選択を解除し、[デフォルトの情報送信元（Default Information Originate）] をイネーブルにすることによって、ルート再配布をディセーブルにすることができます。 • [スタブ（Stub）]：このエリアはスタブエリアとなります。スタブ エリアには、その向こう側にルータまたはエリアはありません。スタブ エリアは、AS External LSA（タイプ 5 LSA）がスタブ エリアにフラッドされないようにします。このオプションを選択すると、[このエリアへのサマリーLSAの送信を許可する（Allow Sending summary LSA into this area）] が有効になります。 スタブエリアを作成するときに、[このエリアへのサマリーLSAの送信を許可する（Allow Sending summary LSA into this area）] チェックボックスをオフにすると、サマリー LSA がそのエリアにフラッドされるのを防ぐことができます。
デフォルトの情報発信元（Default Information Originate） これらのオプションは、エリアタイプとして NSSA を選択すると有効になります。最初のオプションは、エリアタイプとして [Stub] を選択すると有効になります。	

要素	説明
このエリアへのサマリー LSA の送信を許可する（Allow sending summary LSA into this area）	エリアへのサマリー LSA のフラッディングを許可する場合に選択します。
Redistribute (imports routes to normal and NSSA areas)	ルートの再配布を許可する場合に選択します。
Default information originate	タイプ 7 デフォルトを NSSA 内に生成するには、このチェックボックスをオンにします。このオプションを選択すると、次のメトリックオプションが有効になります。 • [メトリック（Metric）]：デフォルトルートの OSPF メトリック値。有効値の範囲は 1 ～ 16777214 です。デフォルトは 1 です。 • [メトリックタイプ（Metric Type）]：デフォルトルートの OSPF メトリックタイプ。1（タイプ 1）または 2（タイプ 2）を選択します。デフォルトは 1 です。

範囲の追加/編集ダイアログボックス（OSPFv3）

[エリア範囲ネットワークの追加（Add Area Range Network）]/[エリア範囲ネットワークの編集（Edit Area Range Network）] ダイアログボックスを使用して、エリアテーブルで選択されたエリアに新しい範囲を追加するか、既存のエントリを変更します。

ナビゲーション パス

[範囲の追加（Add Range）]/[範囲の編集（Edit Range）] ダイアログボックスには、[エリア（Area）] タブ（OSPFv3） （2863 ページ）の [範囲（Range）] パネルからアクセスできます。

関連項目

• OSPFv3 の設定 （2853 ページ）
• OSPFv3 について （2854 ページ）
• [プロセス（Process）] タブ （2856 ページ）

フィールド リファレンス

表 *782 : [*範囲の追加（***Add Range***）*]/[*範囲の編集（***Edit Range***）*]* ダイアログボックス

要素	説明
エリア ID（Area ID）	この読み取り専用エントリは、この範囲が適用されるエリアの ID です。
IPv6 Prefix/Length	集約されるルートの IPv6 アドレス。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
コスト（Cost）	集約ルートのコスト。宛先への最短パスを決定するための OSPF SPF 計算で使用します。有効値の範囲は 0 ～ 16777215 です。 ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、宛先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。
[アドバタイズ（Advertise）]	アドレス範囲ステータスを「アドバタイズ」に設定するには、このオプションを選択します。これにより、タイプ 3 集約 LSA が生成されます（これがデフォルトです）。指定したネットワークのタイプ 3 集約 LSA を抑止するには、このオプションを選択解除します。

Add/Edit Virtual Link Dialog Box（OSPFv3）

[仮想リンクの追加（Add Virtual Link）]/[仮想リンクの編集（Edit Virtual Link）] ダイアログボックスを使用して、エリアテーブルで選択されたエリアの仮想リンクを定義するか、既存の仮想リンクのプロパティを変更します。

ナビゲーション パス

[仮想リンクの追加（Add Virtual Link）]/[仮想リンクの編集（Edit Virtual Link）] ダイアログボックスには、[エリア（Area）] タブ（OSPFv3） （2863 ページ）の下の [仮想リンク（Virtual Link）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）
- [プロセス（Process）] タブ （2856 ページ）

フィールド リファレンス

表 *783 : [*仮想リンクの追加（*Add Virtual Link*）*]/[*仮想リンクの編集（*Edit Virtual Link*）*]* ダイアログ ボックス

要素	説明
エリア ID（Area ID）	この読み取り専用エントリは、この仮想リンクが適用されるエリアの ID です。
ピア ルータ ID（Peer Router ID）	仮想リンク ネイバーの IP アドレスを入力します。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
TTL セキュリティ	仮想リンク上の存続可能時間（TTL）セキュリティホップ数。ホップ数の値は 1 ～ 254 の範囲で指定します。
dead 間隔（Dead Interval）	hello パケットが受信されない場合、ネイバーがデバイスダウンを宣言するまでの時間間隔（秒）。有効値の範囲は1～8192 です。このフィールドのデフォルト値は、hello 間隔の 4 倍です。
Hello 間隔（Hello Interval）	インターフェイス上で送信される hello パケット間の間隔（秒数）。hello 間隔を小さくすると、トポロジ変更はより高速に検出されますが、インターフェイス上で送信されるトラフィックはより多くなります。この値は、特定のインターフェイス上のすべてのルータおよびアクセス サーバーで同じである必要があります。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 10 秒です。
送信間隔	インターフェイスに属する隣接関係への LSA 再送信間の時間（秒数）。デバイスが自身のネイバーに LSA を送信する場合、デバイスは確認応答メッセージを受信するまでその LSA を保持します。デバイスは、確認応答メッセージを受信しないと、LSA を再び送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効な値の範囲は、1～8192 秒です。デフォルト値は 5 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効な値の範囲は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

Add/Edit Redistribution Dialog Box（OSPFv3）

[再配布の追加（Add Redistribution）]/[再配布の編集（Edit Redistribution）] ダイアログボックスを使用して、このプロセスに再配布ルールを追加するか、または既存の再配布ルールを編集します。

ナビゲーション パス

[プロセス（Process）] タブ （2856 ページ）の下の [再配布（Redistribution）] パネルから、[再配布（Redistribution）] ダイアログボックスにアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）

フィールド リファレンス

表 *784 : [Add Redistribution]/[Edit Redistribution]* ダイアログボックス

要素	説明
ソース プロトコル	ルート再配布の送信元プロトコルを選択します。 • [接続済み（Connected）]：接続済みルート（インターフェイス上で IP アドレスを有効にすることによって自動的に確立されるルート）を OSPFv3 ルーティングプロセスに再配布します。接続済みルートは、自律システムの外部として再配布されます。 • [OSPF]：別の OSPF ルーティングプロセスからのルートを再配布します。このオプションを選択すると、ルーティング PID と一致オプションが有効になります。 • [スタティック（Static）]：スタティックルートを OSPFv3 ルーティングプロセスに再配布します。
メトリック （Metric）	再配布されるルートのメトリック値。有効値の範囲は 0 ～ 16777214 で、デフォルトは 20 です。 同じデバイス上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。
メトリック タイプ	メトリックタイプは、OSPFv3 ルーティングドメインにアドバタイズされるデフォルトルートに関連付けられた外部リンクタイプです。 なし、1、または 2 を選択します。なしはデフォルトルートがないことを示し、1 はメトリックがタイプ 1 外部ルートであることを示し、2 はタイプ 2 外部ルートであることを示します。

要素	説明
Tag（任意）	このタグは、各外部ルートに付加される 32 ビットの 10 進値です。これは OSPF 自体には使用されません。これは、他の境界デバイス間で情報を通信するために使用される場合があります。有効値の範囲は、0 ～ 4294967295 です。
ルート マップ	再配布エントリに適用するルートマップオブジェクトの名前を入力または選択します。 ヒント [選択（Select）] をクリックして、ルートマップオブジェクトを選択できる [ルートマップオブジェクトセレクタ（Route Map Object Selector）] を開きます。[ルートマップオブジェクトセレクタ（Route Map Object Selector）] から新しいルートマップオブジェクトを作成することもできます。詳細については、ルートマップオブジェクトについて（2897 ページ）を参照してください。
ルーティング PID	再配布の対象となるプロセスの ID。（プロセス ID は [プロセス（Process）] タブ （2856 ページ）で定義されます。） このオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。
接続済みを含める	接続済みルートを再配布に含めるには、このチェックボックスをオンにします。
一致 1 つのルーティング プロトコルから別のルーティング プロトコルへのルート再配布に使用される条件。ルートが再配布されるには、選択した条件と一致している必要があります。次の一致条件から 1 つ以上を選択できます。これらのオプションは、OSPF が送信元プロトコルとして選択されているときにのみ有効になります。	
内線	特定の自律システムへの内部ルート。
外部 1	自律システムの外部だが、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
外部 2	自律システムの外部だが、OSPF にタイプ 2 外部ルートとしてインポートされるルート。
NSSA 外部 1	自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。
NSSA 外部 2	自律システムの外部だが、OSPF にタイプ 2 NSSA ルートとしてインポートされるルート。

[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス（OSPFv3）

[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックスを使用して、選択したプロセスに新しいルート要約エントリを追加するか、既存のエントリを変更します。

ナビゲーション パス

[サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックスには、[プロセス（Process）] タブ （2856 ページ）の下の [サマリープレフィックス（Summary Prefix）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）

フィールド リファレンス

表 *785 : [サマリープレフィックスの追加/編集（Add/Edit Summary Prefix）] ダイアログボックス*

要素	説明
プロセス ID（Process ID）	この読み取り専用の値は、このルールが適用されるプロセスを識別します。
IPv6 Prefix/Length	外部ルート集約の IPv6 プレフィックス/長さを入力します。 **ヒント** [選択（Select）] をクリックすると、ネットワークオブジェクトのリストからネットワークを選択できます。
[アドバタイズ（Advertise）]	選択した場合、指定したプレフィックスとマスクのペアに一致する集約ルートはアドバタイズされません。選択解除すると、指定したプレフィックスとマスクのペアに一致するルートは抑制されません。デフォルトでは、このチェックボックスはオンです。
Tag（任意）	このタグは、各外部ルートに付加される 32 ビットの 10 進値です。これは OSPF 自体には使用されません。これは、境界デバイス間で情報を通信するために使用される場合があります。有効値の範囲は、0 ～ 4294967295 です。 このフィールドは、[アドバタイズ（Advertise）] をオンにすると有効になります。

[OSPFv3インターフェイス（OSPFv3 Interface）] タブ

[インターフェイス（Interface）] パネルを使用して、インターフェイスおよびネイバー固有の OSPFv3 ルーティングプロパティを設定します。[インターフェイス（Interface）] パネルは、[インターフェイス（Interface）] と [ネイバー（Neighbor）] の 2 つの定義テーブルで構成されています。

- [インターフェイス（Interface）] テーブルエントリの追加と編集については、[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3） （2872 ページ）を参照してください。
- [ネイバー（Neighbor）] テーブルエントリの追加と編集については、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3） （2877 ページ）を参照してください。

Security Manager テーブルの操作に関する基本情報については、テーブルの使用 （64 ページ）を参照してください。

ナビゲーション パス

[OSPFv3] ページの [インターフェイス（Interface）] タブをクリックして、このパネルを表示します。[OSPFv3] ページの詳細については、OSPFv3 の設定 （2853 ページ）を参照してください。

関連項目

- OSPFv3 について （2854 ページ）
- [プロセス（Process）] タブ （2856 ページ）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックス（OSPFv3）

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックスを使用して、個別のインターフェイスの OSPFv3 認証ルーティングプロパティを追加するか、既存のエントリを変更します。

ナビゲーション パス

[インターフェイスの追加/編集（Add/Edit Interface）] ダイアログボックスには、[OSPFv3インターフェイス（OSPFv3 Interface）] タブ （2872 ページ）の [インターフェイス（Interfaces）] パネルからアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）
- [プロセス（Process）] タブ （2856 ページ）

フィールド リファレンス

表 *786 : [Add Interface]/[Edit Interface]* ダイアログボックス

要素	説明
インターフェイス（Interface）	このルーティング設定が適用されるインターフェイスの名前。 **ヒント** [選択（Select）] をクリックして、インター フェイスオブジェクトのリストからインターフェイスを選択できます。
[このインターフェイスでOSPFv3を有効にする（Enable OSPFv3 on this interface）]	指定されたインターフェイスでOSPFv3を有効にし、次のフィールドをアクティブにするには、このボックスをオンにします。 • [プロセスID（Process ID）]：このインターフェイスに適用するプロセスを選択します。 OSPFv3 [プロセス（Process）] タブ（2856 ページ）で定義されます。 • [エリアID（Area ID）]：割り当てられるエリアを識別します。エリアは OSPFv3 [プロセス（Process）] タブ （2856 ページ）でも定義されます。 • [インスタンスID（Instance ID）]：（任意）このプロセスインスタンスの ID を指定します。この設定の有効値の範囲は 0 ～ 255 です。 この機能により、1 つのリンク上に複数の OSPFv3 プロセスを設定できます。他のインスタンス ID を指定された受信パケットは、このプロセスによって無視されます。
Properties	
[発信リンクステートアドバタイズメントのフィルタリング（Filter outgoing link-state advertisements）]	発信LSAをフィルタリングするには、このボックスをオンにします。デフォルトでは、すべての発信LSAがインターフェイスにフラッディングされます。
[MTU不一致検出の無効化（Disable MTU mismatch detection）]	データベース記述子（DBD）パケットが受信された場合のOSPF MTU不一致検出を無効にするには、このボックスをオンにします。
[フラッドリダクション（Flood Reduction）]	安定したトポロジで LSA の不要なフラッディングを抑止するには、このボックスをオンにします。

要素	説明
[ポイントツーポイントネットワーク（Point-to-point Network）]	インターフェイスをポイントツーポイントネットワーク（2つのルーティングデバイス間のネットワーク）へのリンクとして定義するには、このボックスをオンにします。ポイントツーポイントネットワーク上の全ネイバーが隣接関係を確立します。代表ルータは存在しません。 [ブロードキャスト（Broadcast）] オプションが選択されている場合、このオプションは使用できません。
ブロードキャスト	インターフェイスを複数のルーティングデバイスを含むネットワークへのリンクとして定義するには、このボックスをオンにします。このようなネットワークは、代表ルータ（DR）とバックアップ代表ルータ（BDR）を確立し、ネットワークでの LSA フラッディングを制御します。 [ポイントツーポイントネットワーク（Point-to-point Network）] オプションが選択されている場合、このオプションは使用できません。
コスト（Cost）	インターフェイスを介したパケット送信のコスト。リンクコストは、最短パスの最初の計算で使用される任意の数値です。値を割り当てない場合、設定された参照帯域幅をインターフェイスポート速度で割った値が使用されます（デフォルトの参照帯域幅は 40 Gb/秒 です）。
プライオリティ	このインターフェイスにOSPFv3優先順位を割り当てます。この設定の有効値の範囲は 0 ～ 255 です。この設定に 0 を入力すると、適切でないルータが代表ルータまたはバックアップ代表ルータになります。この設定は、ポイントツーポイントの非ブロードキャスト インターフェイスとして設定されているインターフェイスには適用されません。 2つのルータがネットワークに接続している場合、両方が代表ルータになろうとします。優先順位の高いデバイスが代表ルータになります。ルータ優先順位が同じ場合は、ルータ ID が高い方が指定ルータになります。
dead 間隔（Dead Interval）	デバイスがこの間隔内にネイバーから hello パケットを受信しなかった場合、そのデバイスは非アクティブに指定されます。有効値の範囲は 1 ～ 65535 です。この設定のデフォルト値は、hello 間隔の 4 倍です。
Poll Interval	ネイバーデバイスが非アクティブな場合、そのネイバーに hello パケットを送信し続けることが必要な場合があります。hello パケットは短縮された間隔で送信されます。この間隔の値は hello 間隔よりも大きな値にする必要があります。

要素	説明
再送信間隔（Retransmit Interval）	隣接ネイバーへのLSA再送信間の時間（秒単位）。ルータがネイバーに LSA を送信する場合、ルータは確認応答を受信するまでその LSA を保持します。この間隔の間に確認応答が受信されなかった場合、ルータは LSA を再送信します。この値は控えめに設定する必要があります。そうしないと、不要な再送信が発生する可能性があります。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。有効値の範囲は、1 ～ 65535 秒です。
送信遅延（Transmit Delay）	インターフェイス上で LSA パケットを送信するために必要と推定される時間（秒数）。更新パケット内の LSA には、送信前に、このフィールドで指定した値によって増分された経過時間が格納されます。リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。この設定は、非常に低速のリンクでより重要な意味を持ちます。有効値の範囲は、1 ～ 65535 秒です。
認証	
タイプ（Type）	インターフェイス上で有効にする認証のタイプ。次のいずれかを実行します。 • [エリア（Area）]：OSPFv3 は「組み込み」認証を提供せず、代わりにIPv6/IPSecプロトコルに依存します。該当するプロトコルを使用して、エリア内のすべてのインターフェイスでOSPFv3トラフィックを認証するには、このオプションを選択します。これは、エリア内のすべてのルーティングデバイスがこのオプションを使用する必要があることを意味します。これがデフォルトです。 • [インターフェイス（Interface）]：このインターフェイスを安全な状態に保ち、OSPFv3 仮想リンクを保護するには、このオプションを選択します。このオプションを選択すると、このセクションで追加パラメータが有効になります。 • [なし（None）]：OSPFv3 認証は無効になります。
[セキュリティパラメータインデックス（Security Parameter Index）]	特定の OSPFv3 インターフェイスを区別するために使用される IPSec 識別タグを入力します。指定された認証および暗号化ルールと組み合わせて使用されます。有効値の範囲は、256 ～ 4294967295 です。

要素	説明
認証アルゴリズム（Authentication Algorithm）	使用する認証アルゴリズムのタイプを選択します。 • [md5]：Message Digest 5。128 ビットのハッシュ値を生成します。 • [sha1]：Secure Hash Algorithm バージョン 1。160 ビットのハッシュ値を生成します。
認証キー（Authentication Key）	認証キーを入力します。入力するキーの長さは、認証アルゴリズムとして選択した認証のタイプと、キーを暗号化するかどうかによって異なります（[認証キーの暗号化（Encrypt Authentication Key）] ボックスをオンにすると暗号化されます）。 • md5：32 文字。 • md5（暗号化）：66 文字。 • sha1：40 文字。 • sha1（暗号化）：82 文字。
[認証キーの暗号化（Encrypt Authentication Key）]	送信時に指定した認証キーの暗号化を要求するには、このボックスをオンにします。
[暗号化を含める（Include Encryption）]	OSPFv3 パケットの暗号化を要求するには、このボックスをオンにします。次のオプションが有効になります。
暗号化アルゴリズム（Encryption Algorithm）	使用する暗号化のタイプを選択します。 • [3des]：トリプル DES。Data Encryption Standard の暗号アルゴリズムが各パケットに 3 回適用されます。 • [aes-cbc]：暗号化が暗号ブロックチェーンを使用した Advanced Encryption Standard に基づいており、[キータイプ（Key Type）] パラメータで選択されたサイズのキーを生成します。 [キータイプ（Key Type）] リストは、この暗号化オプションを選択した場合にのみ有効になります。次のオプションのいずれかを選択します。 • [128]：128 ビットキーの場合。 • [192]：192 ビットキーの場合。 • [256]：256 ビットキーの場合。 • [des]：Data Encryption Standard に基づく暗号化で、56 ビットのキーを使用します。

要素	説明
暗号化キー（Encryption Key）	暗号キーを入力します。入力するキーの長さは、暗号化アルゴリズムとして選択した暗号化のタイプと、キーを暗号化するかどうかによって異なります（[キーの暗号化（Encrypt Key）] ボックスをオンにすると暗号化されます）。 • 3des：48 文字（192 ビット）。 • 3des（暗号化）：98 文字（192 ビット）。 • aes-cbc/128：32 文字（128 ビット）。 • aes-cbc/128（暗号化）：66 文字（128 ビット）。 • aes-cbc/192：48 文字（192 ビット）。 • aes-cbc/192（暗号化）：98 文字（192 ビット）。 • aes-cbc/256：64 文字（256 ビット）。 • aes-cbc/256（暗号化）：130 文字（256 ビット）。 • des：16 文字（64 ビット）。 • des（暗号化）：34 文字（64 ビット）。
暗号化キー	送信時に指定した暗号化キーの暗号化を要求するには、このボックスをオンにします。

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス（OSPFv3）

ポイントツーポイントの非ブロードキャストインターフェイスごとに、スタティック ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。次の制約事項に注意してください。

- 異なる 2 つの OSPFv3 プロセスに対して同じスタティック ネイバーを定義できません。
- 各スタティックネイバーにスタティックルートを定義する必要があります

インターフェイステーブルで選択したインターフェイスのスタティックネイバーを定義するか、または既存のスタティックネイバーの情報を変更するには、[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスを使用します。

ナビゲーション パス

[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックスには、[OSPFv3インターフェイス（OSPFv3 Interface）] タブ （2872 ページ）からアクセスできます。

関連項目

- OSPFv3 の設定 （2853 ページ）
- OSPFv3 について （2854 ページ）
- [プロセス（Process）] タブ （2856 ページ）

フィールド リファレンス

表 *787 : [ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス*

要素	説明
インターフェイス（Interface）	このネイバー定義に関連付けられたインターフェイス（読み取り専用）。
リンクローカルアドレス（Link-local Address）	スタティックネイバーの IPv6 アドレスを入力します。
コストおよびデータベースフィルタ（Cost and Database Filter）	同期およびフラッディング中にインターフェイス上の発信 LSA をフィルタリングを有効にするには、このボックスをオンにします。次のオプションを使用できます。 • [コスト（Cost）] : このフィールドを使用して、ネイバーに任意のコストを割り当てます。値が割り当てられていない場合、インターフェイスのコストが使用されます（この値はインターフェイスのポート速度に基づいており、基準帯域幅をインターフェイス速度で割って計算されます）。有効値の範囲は 1 ～ 65535 です。 • [発信リンクステートアドバタイズメントをフィルタ処理（Filter outgoing link-state advertisements）] : ネイバーへの発信 LSA の転送を無効にするには、このボックスをオンにします。 （注） [コストおよびデータベースフィルタ（Cost and Database Filter）] オプションと [ポーリング間隔（Poll-Interval）] オプションは相互に排他的です。

要素	説明
ポーリング間隔（Poll-Interval）	次のオプションを有効にするには、このボックスをオンにします。 • [ポーリング間隔（Poll Interval）] : 「デッド」ネイバーへの hello パケットの送信間隔（秒単位）。デフォルトは 120 です。 ネイバーデバイスが非アクティブになった（hello パケットがルータの dead 間隔期間に受信されなかった）場合でも、低いレートでデッドネイバーに hello パケットを送信し続ける必要がある場合があります。そのため、この値は、インターフェイスの hello 間隔より大きい値にする必要があります。 • [優先順位（Priority）] : ネイバーのルータの優先順位値。デフォルトは 0、有効値の範囲は 1 ～ 255 です。 優先順位値は、OSPFv3 リンクの代表ルータを決定するのに役立ちます。値がゼロの場合、デバイスが代表ルータまたはバックアップ代表ルータになれないことを意味します。 （注） [ポーリング間隔（Poll-Interval）] オプションと [コストおよびデータベースフィルタ（Cost and Database Filter）] オプションは相互に排他的です。また、各オプションの値はポイントツーマルチポイント インターフェイスには適用されません。

RIP の設定

Routing Information Protocol（RIP）は動的ルーティングプロトコルです。より正確には、ディスタンスベクターに基づく内部ゲートウェイプロトコルです。RIP は、パス選択のメトリックとしてホップ カウントを使用します。インターフェイスで RIP がイネーブルになっている場合、インターフェイスは RIP ブロードキャスト パケットをネイバー デバイスと交換し、動的にルートを学習してアドバタイズします。これらの RIP パケットには、ゲートウェイが到達可能な宛先ネットワークに関する情報、およびこれらの宛先に到達するためにパケットが通過しなければならないゲートウェイの数が含まれています。

Cisco Security Manager では、RIP バージョン 1 と RIP バージョン 2 の両方がサポートされます。バージョン 1 では、ルーティング更新でサブネット マスクは送信されません。RIP バージョン 2 では、ルーティング更新でサブネット マスクが送信され、可変長サブネット マスクがサポートされます。また、RIP バージョン 2 では、ルーティング更新の交換時にネイバー認証がサポートされます。この認証によって、セキュリティ アプライアンスは信頼できるソースから信頼できるルーティング情報を受信します。

（注） OSPF プロセスを実行している場合は、RIP をイネーブルにすることはできません。

制限事項

RIP には、次の制限事項があります。

- Cisco Security Manager は、インターフェイス間で RIP 更新を渡すことはできません。
- RIP バージョン 1 では、可変長サブネット マスクがサポートされていません。
- RIP の最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。
- RIP の収束は、他のルーティング プロトコルと比べて時間がかかります。

RIP バージョン 2 の注意事項

次の情報は、RIP バージョン 2 だけに適用されます。

- ネイバー認証を使用する場合、認証キーとキー ID は、RIP バージョン 2 更新をインターフェイスに提供するすべてのネイバー デバイスで同じである必要があります。
- RIP バージョン 2 では、セキュリティ アプライアンスは、マルチキャスト アドレス 224.0.0.9 を使用してデフォルトのルート更新を送受信します。パッシブ モードでは、そのアドレスでルート アップデートが受信されます。
- RIP バージョン 2 がインターフェイスで設定されている場合、マルチキャスト アドレス 224.0.0.9 がそのインターフェイス上に登録されます。RIP バージョン 2 構成がインターフェイスから削除されると、そのマルチキャスト アドレスは登録解除されます。

Security Manager を使用したセキュリティ アプライアンスでの RIP の設定

[RIP] ページを使用して、インターフェイスで Routing Information Protocol をイネーブルにします。RIP を設定するときに使用できる設定および機能は、設定しているデバイスのタイプおよび OS のバージョンによって異なります。

- OS バージョンが 7.2 よりも前の PIX ファイアウォールまたは ASA で、あるいは任意の FWSM で RIP を設定するには、PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （2881 ページ）を参照してください。
- OS バージョン 7.2 以降を実行している PIX ファイアウォールまたは ASA で RIP を設定するには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）を参照してください。

関連項目

- スタティック ルートの設定 （2891 ページ）
- OSPF の設定 （2812 ページ）
- [No Proxy ARP] の設定 （2703 ページ）
- 「Configuring Routing Information Protocol」：『Cisco IOS IP Configuration Guide, Release 12.2』の章。RIP の詳細情報が記載されています。

PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

この [RIP] ページを使用して、任意の FWSM、および 7.2 よりも前のバージョンのオペレーティング システムを実行している PIX/ASA のインターフェイスで Routing Information Protocol（RIP）をイネーブルにします。

このページの [RIP] テーブルには、現在 RIP が定義されているすべてのインターフェイスが一覧表示されます。[Add RIP Configuration]/[Edit RIP Configuration] ダイアログボックスを使用して、これらのエントリを作成および維持します。詳細については、PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （2881 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [RIP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [RIP] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

共有 RIP ポリシーの作成時には、[Create a Policy] ダイアログボックスで次のバージョンを選択する必要があります。

- **PIX/ASA 6.3-7.1 and FWSM**
- **PIX/ASA 7.2 and Later**

共有 RIP ポリシーの割り当て時には、必ずそのデバイスに適した RIP ポリシーを割り当ててください。たとえば、PIX/ASA 7.2+ RIP ポリシーを FWSM に割り当てることはできません。

関連項目

- スタティック ルートの設定 （2891 ページ）
- OSPF の設定 （2812 ページ）
- [No Proxy ARP] の設定 （2703 ページ）
- PIX/ASA 7.2 以降の RIP ページ （2883 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)]/[Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[Add RIP Configuration]/[Edit RIP Configuration] ダイアログボックスを使用して、RIP 設定をセキュリティ アプライアンスに追加するか、既存の RIP 設定を変更します。RIP 設定を追加することによって、指定したインターフェイスで RIP をイネーブルにします。タイトルを除き、2 つのダイアログボックスは同じです。

ナビゲーション パス

[Add RIP Configuration]/[Edit RIP Configuration] ダイアログボックスには、 PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （2881 ページ）からアクセスできます。

フィールド リファレンス

表 *788 : [RIP*設定の追加（*PIX/ASA 6.3–7.1***および***FWSM***）（***Add RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)***）***]/[RIP*設定の編集（***PIX/ASA 6.3–7.1***および***FWSM***）（***Edit RIP Configuration (PIX/ASA 6.3–7.1 and FWSM)***）***]*ダイアログボックス**

要素	説明
インターフェイス（Interface）	RIP 設定のインターフェイスを入力または選択します。同じインターフェイスで異なる RIP 設定を設定することはできません。
[モード（Mode）]	RIP 更新に関するインターフェイスの動作を選択します。 • [デフォルトルートの送信（Send default routes）]：インターフェイスは RIP ルーティング更新だけを送信します。 • [ルートの受信（Receive routes）]：インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルに読み込みますが、RIP ルーティング更新を送信しません。 • [デフォルトルートの送信とルートの受信（Send default routes and receive routes）]：インターフェイスは RIP ルーティング更新を送受信します。
バージョン	インターフェイスで有効にする RIP バージョンを選択します。 • [RIPバージョン1（RIP Version 1）]：インターフェイスで RIP バージョン 1 をイネーブルにします。 • [RIPバージョン2（RIP Version 2）]：インターフェイスで RIP バージョン2をイネーブルにします。RIP バージョン2を設定すると、マルチキャスト アドレス 224.0.0.9 がインターフェイス上に登録されます。

要素	説明
Version 2 Authentication	これらのオプションを使用すると、RIP バージョン 2 で使用される認証をイネーブルにし、そのタイプを選択できます。 • [認証の有効化（Enable Authentication）]：このオプションは、上記の [RIP バージョン2（RIP Version 2）] を選択した場合に使用できます。このチェックボックスをオンにすると、RIP ネイバー認証がイネーブルになり、次のオプションが使用可能になります。 • [タイプ（Type）]：認証に MD5 ハッシュアルゴリズムを使用する場合は [MD5] を選択し（推奨）、認証にクリアテキストを使用する場合は [クリア テキスト（Clear text）] を選択します。 • [キーID（Key ID）]：認証キーの識別番号。この番号は、セキュリティ アプライアンスに更新を送信し、セキュリティ アプライアンスから更新を受信する他のすべてのデバイスと共有される必要があります。有効値の範囲は、1 ～ 255 です。 • [キー（Key）]：認証に使用される共有キー。 このキーは、セキュリティ アプライアンスに更新を送信し、セキュリティ アプライアンスから更新を受信する他のすべてのデバイスと共有される必要があります。キーの文字数は最大 16 文字です。

PIX/ASA 7.2 以降の RIP ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX および FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

この RIP ページを使用して、オペレーティングシステム 7.2 以降を実行している PIX および ASA デバイスで Routing Information Protocol（RIP）を有効にし、設定します。[RIP] ページは、次のタブ付きパネルで構成されています。

- [RIP] - [Setup] タブ （2884 ページ）
- RIP の [再配布（Redistribution）] タブ （2886 ページ）
- [RIP] - [Filtering] タブ （2888 ページ）
- [RIP] - [Interface] タブ （2890 ページ）

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから、**[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [RIP]** を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

共有 RIP ポリシーの作成時には、[Create a Policy] ダイアログボックスで次のバージョンを選択する必要があります。

- **PIX/ASA 6.3-7.1 and FWSM**
- **PIX/ASA 7.2 and Later**

共有 RIP ポリシーの割り当て時には、必ずそのデバイスに適した RIP ポリシーを割り当ててください。たとえば、PIX/ASA 7.2+ RIP ポリシーを FWSM に割り当てることはできません。

関連項目

- スタティック ルートの設定 （2891 ページ）
- OSPF の設定 （2812 ページ）
- [No Proxy ARP] の設定 （2703 ページ）
- PIX/ASA 6.3 - 7.1 および FWSM の [RIP] ページ （2881 ページ）

[RIP] - [Setup] タブ

[Setup] パネルを使用して、セキュリティ アプライアンスで RIP を定義し、グローバル RIP プロトコル パラメータを設定します。セキュリティアプライアンスでは、RIP プロセスを 1 つだけイネーブルにできます。

ナビゲーション パス

[Setup] タブには、 PIX/ASA 7.2 以降の RIP ページ （2883 ページ）からアクセスできます。

関連項目

- RIP の [再配布（Redistribution）] タブ （2886 ページ）
- [RIP] - [Filtering] タブ （2888 ページ）
- [RIP] - [Interface] タブ （2890 ページ）

フィールド リファレンス

表 *789 : [Setup]* タブ

要素	説明
ネットワーク	RIP ルーティングに対して 1 つ以上のネットワークを定義します。IP アドレスを入力するか、目的のネットワーク/ホスト オブジェクトを入力または選択します（ネットワーク/ホストオブジェクトについて （391 ページ）を参照）。IP アドレスにはサブネット情報を含めないでください。セキュリティ アプライアンスの設定に追加できるネットワーク数に制限はありません。 RIP ルーティング更新は、指定したネットワークのインターフェイスだけを介して送受信されます。また、インターフェイスのネットワークを指定しない場合、インターフェイスは RIP 更新でアドバタイズされません。
パッシブ インターフェイス	このオプションを使用して、セキュリティ アプライアンスで受動インターフェイスを指定してから、アクティブ インターフェイスを指定します。デバイスは、そのルーティング テーブルを入力するための情報を使用して、パッシブ インターフェイスでの RIP ルートのブロードキャストをリッスンしますが、パッシブ インターフェイスでのルーティング更新はブロードキャストしません。パッシブとして指定されていないインターフェイスは、更新を送受信します。次のオプションのいずれかを選択します。 **1.** [なし（None）]：どのインターフェースもパッシブとして指定されません。 **2.** [すべてのインターフェース（All Interfaces）]：デバイス上のすべてのインターフェイスがパッシブとして指定されます。ただし、次の [除外されたインターフェース（Excluded Interfaces）] フィールドに入力したインターフェイスを除きます。 **3.** [指定されたインターフェース（Specified Interfaces）]：以下のインターフェイス フィールドで明示的に指定されたインターフェイスのみが、パッシブとして指定されます。

要素	説明
[Interfaces]/[Excluded Interfaces]	このフィールドを使用して、上記の [Passive Interface] リストからの選択に応じて、受動リストから除外するインターフェイス、または明示的に受動として指定するインターフェイスを指定します。 • [すべてのインターフェース（All Interfaces）] を選択した場合、このフィールドのラベルは [除外されたインターフェース（Excluded Interfaces）] になります。除外するインターフェイス（つまり、パッシブではなくアクティブにするインターフェイス）だけを入力または選択します。 • [Passive Interface] リストで [Specified Interfaces] を選択した場合、受動として指定するインターフェイスだけを入力または指定します。 （注） 同じインターフェイスに対して異なる RIP 設定を指定することはできません。
RIP Version	RIP 更新の送受信対象の RIP バージョンを選択します。 • Receive Version 1 and 2, Send Version 1 • Send and Receive Version 1 • Send and Receive Version 2
デフォルトルートの生成	選択すると、指定した [Route Map] に基づいて、配布のためのデフォルトルートが生成されます。
ルート マップ	デフォルト ルートの生成に使用するルート マップを指定します。 （注） このフィールドにはルートマップ名だけが含まれます。ルートマップは FlexConfig 内で作成および格納されます。詳細については、 FlexConfig ポリシーとポリシー オブジェクトについて（432 ページ） を参照してください。
Enable Auto-Summary	[RIP Version] として [Send and Receive Version 2] を選択した場合、このオプションが使用可能になります。オンにすると、自動ルート サマライズがイネーブルになります。切断されているサブネット間のルーティングを実行する必要がある場合は、自動サマライズを無効にします。自動サマライズを無効にすると、サブネットがアドバタイズされます。 （注） RIP バージョン 1 では、常に自動サマライズが使用されます。無効にすることはできません。

RIP の [再配布（Redistribution）] タブ

[Redistribution] パネルを使用して、再配布ルートを管理します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。詳細については、

[Add Redistribution]/[Edit Redistribution] ダイアログボックス （2748 ページ）を参照してください。

ナビゲーション パス

[Redistribution] タブには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）からアクセスできます。

関連項目

- [RIP] - [Setup] タブ （2884 ページ）
- [RIP] - [Filtering] タブ （2888 ページ）
- [RIP] - [Interface] タブ （2890 ページ）

[Add Redistribution]/[Edit Redistribution] ダイアログボックス

[Add Redistribution]/[Edit Redistribution] ダイアログボックスを使用して、RIP の [再配布（Redistribution）] タブ （2886 ページ）で再配布ルートを追加および編集します。これらは、他のルーティング プロセスから RIP ルーティング プロセスに再配布されているルートです。タイトルを除き、これら 2 つのダイアログボックスは同一です。

ナビゲーション パス

[Add Redistribution]/[Edit Redistribution] ダイアログボックスには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）の [Redistribution] タブからアクセスできます。

フィールド リファレンス

表 *790 : [Add Redistribution]/[Edit Redistribution]* ダイアログボックス

要素	説明
Protocol to Redistribute	RIP ルーティング プロセスに再配布するルーティング プロトコルを選択します。 • [Static]：スタティックルート。 • [Connected）]：直接接続されたネットワーク。 • [OSPF]：OSPF ルーティングプロセスによって検出されたルート。 [OSPF] を選択すると、OSPF の [Process ID]、および任意で [Match] 基準も入力する必要があります。
プロセス ID （Process ID）	OSPF プロトコルを選択した場合、プロセス ID を入力します。

要素	説明
一致（Match）	OSPF ルートを RIP ルーティング プロセスに再配布する場合、再配布する特定のタイプの OSPF ルートを選択できます。複数のタイプを選択するには、Ctrl を押しながらクリックします。 • [内部（Internal）]：自律システム（AS）の内部のルートが再配布されます。 • [外部 1（External 1）]：AS に対して外部のタイプ 1 ルートが再配布されます。 • [外部 2（External 2）]：AS に対して外部のタイプ 2 ルートが再配布されます。 • [NSSA 外部 1（NSSA External 1）]：Not-So-Stubby Area（NSSA）の外部のタイプ 1 ルートが再配布されます。 • [NSSA External 2]：NSSA の外部のタイプ 2 ルートが再配布されます。 [Match] 基準は任意です。デフォルトの一致は、[Internal]、[External 1]、および [External 2] です。
メトリック（Metric）	再配布されるルートに適用される RIP メトリック タイプ。選択肢は次の 2 つです。 • [トランスペアレント（Transparent）]：現在のルートメトリックを使用します。 • [指定値（Specified Value）]：特定のメトリック値を割り当てます。
ルート マップ	ルートが RIP ルーティング プロセスに再配布される前に満たす必要があるルートマップの名前。 （注） このフィールドにはルート マップ名だけが含まれます。ルートマップの内容は、FlexConfig 内で作成および格納されます。詳細については、FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

[RIP] - [Filtering] タブ

[Filtering] パネルを使用して、RIP ポリシーのフィルタを管理します。フィルタは、着信および発信 RIP アドバタイズメントでネットワーク情報を制限するために使用されます。詳細については、[Add Filter]/[Edit Filter] ダイアログボックス （2889 ページ）を参照してください。

ナビゲーション パス

[Filtering] タブには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）からアクセスできます。

関連項目

- [RIP] - [Setup] タブ （2884 ページ）
- RIP の [再配布（Redistribution）] タブ （2886 ページ）
- [RIP] - [Interface] タブ （2890 ページ）

[Add Filter]/[Edit Filter] ダイアログボックス

[Add Filter]/[Edit Filter] ダイアログボックスを使用して、[RIP] - [Filtering] タブ （2888 ページ）で RIP フィルタを追加および編集します。フィルタは、着信および発信 RIP アドバタイズメントでネットワーク情報を制限するために使用されます。タイトルを除き、これら 2 つのダイアログボックスは同一です。

ナビゲーション パス

[Add Filter]/[Edit Filter] ダイアログボックスには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）の [Filtering] タブからアクセスできます。

フィールド リファレンス

表 *791 : [Add Filter]/[Edit Filter]* ダイアログボックス

要素	説明
トラフィックの方向	フィルタリングするトラフィックのタイプを、[インバウンド（Inbound）] または [アウトバウンド（Outbound）] から選択します。 （注） [Traffic Direction] が [Inbound] の場合、インターフェイス フィルタだけを定義できます。
フィルタリングする	フィルタが [インターフェイス（Interface）] または [ルート（Route）] のどちらに基づいているかを指定します。 [インターフェイス（Interface）] を選択した場合、ルーティング更新がフィルタリングされるインターフェイスの名前を入力または選択します。 [ルート（Route）] を選択した場合、ルート タイプを選択します。 • [スタティック（Static）]：スタティックルートだけがフィルタリングされます。 • [接続済み（Connected）]：接続されたルートだけがフィルタリングされます。 • [OSPF]：指定した OSPF プロセスによって検出された OSPF ルートだけがフィルタリングされます。フィルタリングされる OSPF プロセスの [プロセス ID（Process ID）] を入力します。

要素	説明
Filter ACLs	許可されるネットワークまたは RIP ルート アドバタイズメントから削除されるネットワークを定義する 1 つ以上のアクセス コントロール リスト（ACL）の名前を入力または選択します。

[RIP] - [Interface] タブ

[Interface] パネルを使用して、RIP ブロードキャストを送受信するように設定されたインターフェイスを管理します。詳細については、[Add Interface]/[Edit Interface] ダイアログボックス（2890 ページ）を参照してください。

ナビゲーション パス

[Interface] タブには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）からアクセスできます。

関連項目

- [RIP] - [Setup] タブ （2884 ページ）
- RIP の [再配布（Redistribution）] タブ （2886 ページ）
- [RIP] - [Filtering] タブ （2888 ページ）

[Add Interface]/[Edit Interface] ダイアログボックス

[Add Interface]/[Edit Interface] ダイアログボックスを使用して、[RIP] - [Interface] タブ （2890 ページ）で RIP インターフェイス設定を追加および編集します。タイトルを除き、これら 2 つのダイアログボックスは同一です。

ナビゲーション パス

[Add Interface]/[Edit Interface] ダイアログボックスには、PIX/ASA 7.2 以降の RIP ページ （2883 ページ）の [Interface] タブからアクセスできます。

フィールド リファレンス

表 792 : [Add Interface]/[Edit Interface] ダイアログボックス

要素	説明
インターフェイス（Interface）	このアプライアンスで定義されるインターフェイスを入力または選択します。
Send (Version)	これらのオプションを使用して、このインターフェイスについて、[RIP] - [Setup] タブ （2884 ページ）で指定したグローバルな送信バージョンを上書きできます。該当するボックスを選択して、RIP バージョン 1、バージョン 2、または両方を使用して更新を送信するように指定します。

要素	説明
Receive (Version)	これらのオプションを使用して、グローバルな受信バージョンを上書きできます。該当するボックスを選択して、RIP バージョン 1 だけ、バージョン 2 だけ、または両方を使用して更新を受信するように指定します。
認証タイプ（Authentication Type）	RIP ブロードキャストに対してこのインターフェイスで使用される認証を選択します。 • [なし（None）]：認証されません。 • [MD5]：MD5 を使用します。 • [クリアテキスト（Clear Text）]：クリアテキスト認証を使用します。 [MD5] または [Clear Text] を選択した場合、次の認証パラメータも指定する必要があります。 • [キー ID（Key ID）]：認証キーの ID。有効な値は 0 ～ 255 です。 • [キー（Key）]：選択した認証方式で使用されるキー。最大 16 文字です。 • [確認（Confirm）]：確認のために、認証キーを再度入力します。

スタティック ルートの設定

スタティック ルートは、現在のデバイスで手動で定義されている特定の宛先ネットワークへの特定のパスです。スタティック ルートは、さまざまな状況で使用されます。宛先へのダイナミック ルートがない場合、またはダイナミック ルーティング プロトコルの使用が不可能な場合に、1 つのネットワークから別のネットワークにデータをルーティングする迅速で効果的な方法です。

すべてのルートに、その使用プライオリティを示す値または「メトリック」があります。（このメトリックは「アドミニストレーティブディスタンス」とも呼ばれます）。同じ接続先に対して 2 つ以上のルートが使用可能な場合、デバイスはアドミニストレーティブディスタンスを使って使用するルートを決定します。

スタティック ルートのデフォルトのメトリック値は 1 であり、ダイナミック ルーティング プロトコルによるルートよりも優先されます。ダイナミック ルートのメトリックよりも大きい値にメトリックを増やすと、スタティック ルートは、ダイナミック ルートに障害が発生した際のバックアップとして動作します。たとえば、Open Shortest Path First（OSPF）から取得されたルートには、100 というデフォルトのアドミニストレーティブディスタンスがあります。OSPF ルートが優先されるバックアップ スタティック ルートを設定するには、スタティック ルートに 100 よりも大きいメトリック値を指定します。これは、「フローティング」スタティック ルートと呼ばれます。

デフォルト ルートと呼ばれる特別な種類のスタティック ルートがあります。宛先アドレスとサブネット マスクの両方にすべて 0 が使用されるため、「0 - 0」ルートとも呼ばれます。デフォルトのスタティック ルートは、catch-all ゲートウェイとして機能します。デバイスのルーティング テーブルで特定の宛先について一致がない場合は、デフォルト ルートが使用されます。一般に、デフォルト ルートにはネクストホップ IP アドレスまたはローカル出口インターフェイスが含まれます。

[Static Route] ページを使用して、手動で定義したスタティック ルートを維持します。このページの [Static Route] テーブルには、現在定義されているすべてのスタティック ルートが一覧表示され、ルートごとに、ルートが定義されているインターフェイスまたはインターフェイス ロールの名前、宛先ネットワーク、ネクスト ホップ ゲートウェイ、ルート メトリック、ルートがトンネリングされるかどうか、ルートのサービス レベル契約トラッキングがあるかどうかが表示されます。これらのフィールドの詳細については、[Add Static Route]/[Edit Static Route] ダイアログボックス （2893 ページ）または [IPv6 スタティック ルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス （2895 ページ）を参照してください。

スタティック null0 ルートの設定

通常、トラフィックのフィルタリングには ACL が使用され、ヘッダーに含まれている情報に基づくパケットのフィルタが可能になります。パケット フィルタリングでは、ASA ファイアウォールがパケット ヘッダーを検査してフィルタリングを決定するため、パケット処理のオーバーヘッドが加わり、パフォーマンスに影響します。

スタティック null0 ルーティングは、フィルタリングを補完するソリューションです。スタティック null0 ルートは、不要なトラフィックや望ましくないトラフィックをブラック ホールに転送するために使用されます。ヌル インターフェイスである null0 が、ブラック ホールの作成に使用されます。望ましくない宛先用のスタティック ルートが作成され、そのスタティック ルート コンフィギュレーションで null インターフェイスを指すように設定されます。宛先アドレスに最も一致するルートがブラック ホールのスタティック ルートであるすべてのトラフィックが自動的にドロップされます。ACL の場合とは異なり、スタティック null0 ルートはまったくパフォーマンスを低下させません。

スタティック null0 ルート設定は、ルーティング ループの防止に使用されます。BGP では、Remotely Triggered Black Hole ルーティングのためにスタティック null0 設定を活用します。

ナビゲーション パス

- （デバイス ビュー）デバイス ポリシー セレクタから、[プラットフォーム（Platform）] > [ルーティング（Routing）] > [スタティック ルート（Static Route）] または [プラットフォーム（Platform）] > [ルーティング（Routing）] > [IPv6 スタティック ルート（IPv6 Static Route）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから、[PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [スタティック ルート（Static Route）] または [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ルーティング（Routing）] > [IPv6 スタティック ルート（IPv6 Static Route）] を選択します。共有ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add Static Route]/[Edit Static Route] ダイアログボックス （2893 ページ）
- [IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス（2895 ページ）
- 接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブル カラムおよびカラム見出しの機能 （66 ページ）

[Add Static Route]/[Edit Static Route] ダイアログボックス

[Add Static Route]/[Edit Static Route] ダイアログボックスを使用すると、スタティック ルートを追加または編集できます。

ナビゲーション パス

[Add Static Route]/[Edit Static Route] ダイアログボックスには、[Static Routes] ページからアクセスできます。新しいスタティック ルートを追加するには、[Add Row] ボタンをクリックします。既存のスタティック ルートを編集するには、そのルートを選択して [Edit Row] ボタンをクリックします。

関連項目

- スタティック ルートの設定 （2891 ページ）

フィールド リファレンス

表 793 : [Add Static Route]/[Edit Static Route] ダイアログボックス

要素	説明
インターフェイス（Interface）	このスタティック ルートが適用されるインターフェイスを入力または選択します。 トラフィックを Null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。詳細については、スタティック ルートの設定 （2891 ページ）を参照してください。 （注） インターフェイスとして Null0 が選択されている場合、[ゲートウェイ（Gateway）] と [トンネル化（Tunneled）] のオプションはディセーブルになります。

要素	説明
ネットワーク（Network）	宛先ネットワークを入力または選択します。1 つ以上の IP アドレス/ネットマスク エントリ、1 つ以上のネットワーク/ホスト オブジェクト、または両方の組み合わせを指定できます。エントリはカンマで区切ります。 デフォルトルートを指定するには、「0.0.0.0/0」または「any」を入力します。
ゲートウェイ	このルートのネクスト ホップであるゲートウェイ ルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。 （注） セキュリティアプライアンスのインターフェイスのいずれかの IP アドレスがゲートウェイ IP アドレスとして使用される場合、セキュリティアプライアンスはゲートウェイ IP アドレスを解決する代わりに、パケット内の指定された IP アドレスを解決します。
メトリック（Metric）	メトリックは、特定のホストが存在するネットワークへのホップ数（ホップ カウント）に基づくルートの「コスト」を示す測定値です。ホップ カウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。ホップ カウントには宛先ネットワークも含まれるため、直接接続されたすべてのネットワークのメトリックは 1 です。 宛先ネットワークへのホップ数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。 インスタンスごとに定義できる、コストが等しい（メトリックが等しい）ルートの最大数は、3 です。同じネットワーク上にある異なるインターフェイスで、同じメトリックのルートを追加することはできません。
Tunneled	これをトンネル ルートにするには、このオプションを選択します。デフォルト ルートだけに使用できます。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。[Tunneled] オプションは、トランスペアレント モードではサポートされません。PIX/ASA 7.0+ デバイスだけで使用できます。
Route Tracking	ルートの可用性をモニタするには、モニタリング ポリシーを定義する Service Level Agreement（SLA; サービス レベル契約）オブジェクトの名前を入力または選択します。PIX/ASA 7.2+ デバイスだけで使用できます。 ルート トラッキングの詳細については、接続を維持するためのサービス レベル契約（SLA）のモニタリング （2591 ページ）を参照してください。

[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス

[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックスを使用すると、IPv6 スタティックルートを追加または編集できます。IPv6 スタティックルートは、次のデバイスでのみサポートされています。

- ASA 7.0 以降（ルーテッドモード）
- ASA 8.2 以降（トランスペアレントモード）
- FWSM 3.1 以降（ルーテッドモード）

ナビゲーション パス

[IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックスには、[IPv6スタティックルート（IPv6 Static Route）] ページからアクセスできます。新しいスタティックルートを追加するには、[行の追加（Add Row）] ボタンをクリックします。既存のスタティックルートを編集するには、そのルートを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- スタティック ルートの設定 （2891 ページ）

フィールド リファレンス

表 *794 : [IPv6スタティックルートの追加/編集（Add/Edit IPv6 Static Route）] ダイアログボックス*

要素	説明
インターフェイス（Interface）	このスタティックルートが適用されるインターフェイスを入力または選択します。
IPv6ネットワーク（IPv6 Network）	宛先ネットワークを入力または選択します。1 つ以上の IP アドレスエントリ、1 つ以上のネットワーク/ホストオブジェクト、または両方の組み合わせを指定できます。エントリはカンマで区切ります。 2 つのコロン（::）を入力してデフォルトルートを指定します。

要素	説明
IPv6ゲートウェイ（IPv6 Gateway）	このルートのネクストホップであるゲートウェイ ルータを入力または選択します。IP アドレスまたはネットワーク/ホスト オブジェクトを指定できます。 （注） セキュリティアプライアンスのインターフェイスのいずれかの IP アドレスがゲートウェイ IP アドレスとして使用される場合、セキュリティアプライアンスはゲートウェイ IP アドレスを解決する代わりに、パケット内の指定された IP アドレスを解決します。
メトリック（Metric）	メトリックは、特定のホストが存在するネットワークへのホップ数（ホップカウント）に基づくルートの「コスト」を示す測定値です。ホップカウントは、ネットワーク パケットが最終的な宛先に到達するまでに通過する必要があるネットワークの数であり、宛先ネットワークも含まれます。ホップカウントには宛先ネットワークも含まれるため、直接接続されたすべてのネットワークのメトリックは 1 です。 宛先ネットワークへのホップ数を入力します。有効値の範囲は 1 ～ 255 で、デフォルト値は 1 です。 インスタンスごとに定義できる、コストが等しい（メトリックが等しい）ルートの最大数は、3 です。同じネットワーク上にある異なるインターフェイスで、同じメトリックのルートを追加することはできません。
Tunneled	ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定するには、このオプションを選択します。設定できるデフォルトのトンネル ゲートウェイは、デバイスごとに 1 つのみです。ルーテッド モードの ASA 7.0 以降のデバイスでのみ使用できます。

ASA ルーティング ポリシーのポリシーオブジェクトの設定

ASA ルーティングポリシーで使用するポリシーオブジェクトがいくつかあります。このリファレンスでは、これらのポリシー オブジェクトの設定について説明します。

ここでは、次の内容について説明します。

- ルートマップオブジェクトについて （2897 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）
- [プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）

- [プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （2920 ページ）
- [ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924 ページ）
- [コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （2926 ページ）
- BFD テンプレートの作成 （2808 ページ）

ルートマップオブジェクトについて

ルートマップを使用して、1 つのルーティングプロトコルから他のルーティングプロトコルへのルートを再配布するか、またはポリシールーティングを有効にするための条件を定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個々の文を一定の順序で並べたものです。ACL またはルートマップの評価は、事前に定義された順序でのリストのスキャンと、一致する各文の基準の評価で構成されています。リストのスキャンは、文の一致が初めて見つかり、その文に関連付けられたアクションが実行されると中断します。
- これらは汎用メカニズムです。基準の一致と一致の解釈は、その適用方法によって指定されます。異なるタスクに適用される同じルート マップの解釈が異なることがあります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップでは、一致基準として ACL を頻繁に使用します。

（注） ルートマップは、ユーザ、ユーザーグループ、セキュリティグループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

- ACL の評価の主な結果は、yes または no の答えとなります。つまり、ACL は入力データを許可するか拒否するかのいずれかです。再配布に適用された ACL は、特定のルートを再配布できるか（ルートが ACL の permit 文に一致）、再配布できないか（deny 文に一致）を判断します。一般的なルートマップでは、（一部の）再配布ルートを許可するだけではなく、別のプロトコルに再配布される場合は、ルートに関連付けられた情報も変更します。
- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルート タイプが内部であるかどうかを確認できます。

- 各 ACL は、設計の表記法により暗黙的な deny 文で終了しますが、ルートマップには同様の表記法はありません。一致試行の間にルートマップの終わりに達した場合は、そのルートマップの特定のアプリケーションによって結果が異なります。幸いなことに、再配布に適用されたルートマップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny 文が含まれている場合と同様にルートの再配布は拒否されます。

ルートマップは、再配布中にルート情報を変更する場合や、ACL よりも強力な照合機能が必要な場合に推奨します。プレフィックスまたはマスクに基づいて一部のルートを選択的に許可することだけが必要な場合は、ルートマップを使用して、ACL（または等価のプレフィックスリスト）に直接マップすることをお勧めします。

（注） 標準 ACL をルートマップの一致基準として使用する必要があります。拡張 ACL を使用しても機能しないため、ルートが再配布されなくなります。将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、10 単位で句に番号を指定することをお勧めします。

permit 句と deny 句

ルートマップでは permit 句と deny 句を使用できます。このルートマップの一致基準が満たされた場合、permit キーワードが指定されていると、設定アクションに従ってルートが再配布されます。一致基準が満たされなかった場合、permit キーワードが指定されていると、同じマップ タグを持つ次のルートマップがテストされます。あるルートが、同じ名前を共有するルートマップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。ルートマップの一致基準が満たされた場合でも、deny キーワードが指定されているとルートは再配布されません。

次のルールが適用されます。

- ルートマップの permit 句で ACL を使用する場合は、その ACL で許可されるルートが再配布されます。
- ルートマップの deny 句で ACL を使用すると、ACL で許可されるルートは再配布されません。
- ルートマップの permit 句または deny 句で ACL を使用する場合に、その ACL でルートが拒否されるときは、そのルートマップ句に一致するものは見つからないことになり、次のルートマップ句が評価されます。

match 句と set 句の値

ルートマップステートメントのエントリごとに、match 句と set 句の組み合わせが含まれています。match 句では、該当するパケットが特定のポリシーを満たす基準（つまり、満たすべき条件）を定義します。set 句は、一致基準を満たしたパケットをどのようにルーティングするかを説明します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは permit 句または deny 句の指示に従って再配布または拒否され、一部の属性は set 句で定義したように変更されることがあります。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の Match 句の値が句に存在する場合、指定したルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用されます）。
- 1 つのコマンド内で 1 つの Match 句の値が複数のオブジェクトを参照している場合、そのオブジェクトのいずれかが一致する必要があります（論理 OR アルゴリズムが適用されます）。
- Match 句の値が存在しない場合は、すべてのルートが句に一致します。
- ルートマップの permit 句に Set 値が存在しない場合、そのルートは現在の属性の変更なしに再配布されます。

（注） ルートマップの deny 句では Set 値を設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

Match または Set 値がないルートマップ句は、アクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。

BGP match 句および BGP set 句

前述の match および set の値に加えて、BGP ではルート マップに対して追加の match および set 機能が提供されています。

次のルートマップの match 句が BGP でサポートされています。

- match AS path access list
- match community
- match policy list

次のルートマップの set 句が BGP でサポートされています。

- set AS path
- set community

- set automatic tag
- set local preference
- set weight
- set origin
- set next hop
- set IP prefix list

ルートマップオブジェクトの作成と使用

ルートマップを識別する必要があるポリシーを設定する場合、[ルートマップ（Route Map）] フィールドの横にある [選択（Select）] ボタンをクリックして、ルートマップオブジェクトを選択または作成できます。[ルートマップオブジェクトセレクタ（Route Map Object Selector ）] ダイアログボックスから新しいルートマップを作成するには、ルートマップリストの下にある [作成（Create）] ボタンをクリックします。オブジェクトタイプセレクタから [ルートマップ（Route Map）] を選択し、[新規オブジェクト（New Object）] ボタンをクリックすることにより、 Policy Object Manager （290 ページ）からルートマップオブジェクトを作成することもできます。ルートマップオブジェクトを作成するときに使用できる特定のフィールドについては、[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （2901 ページ）を参照してください。

BGP ポリシーでのルートマップオブジェクトの使用に関する注意

ルートマップで使用される一致基準および設定基準の一部は、すべての BGP サブコマンドでサポートされていません。次に例を示します。

次のルートマップの一致基準：

- Match Clause tab > Match first hop interface of route、Match Next Hop (IPv4 and IPv6)、Match Route Source (IPv4 and IPv6)、Match Metric Route Value、および Match Tag
- BGP Match Clause tab > Match AS path access lists

および次のルートマップの設定基準：

- Set Clause tab > Metric Values (all fields) および Metric Type
- BGP Set Clause tab > Set AS path、Prepend AS path、および Prepend last AS to the AS path

は、次の場所ではサポートされていません。

- BGP policy > IPv4 Address Family:
  - Aggregate Address tab > Attribute Map、Advertise Map、および Suppress Map
  - Neighbor tab > Filtering tab
  - Route Injection tab > Inject Map および Exist Map

Security Manager では、ルートマップにサポートされていない一致基準または設定基準が含まれている場合でも、BGP 設定でルートマップを使用でき、検証中に警告やエラーを受け取ることはありません。このような場合、展開は失敗し、デバイスから次の形式のエラーを受け取ります：...%"My-Route-map" used as BGP inbound route-map, nexthop match not supported... 。

BGP 設定で使用されるルートマップでサポートされる一致/設定基準に関するガイドラインについては、ASA のドキュメントを参照してください。

関連項目

- [ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （2901 ページ）
- [ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （2903 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス

[ルートマップオブジェクトの追加または編集（Add/Edit Route Map Object）] ダイアログボックスを使用して、ルートマップポリシーオブジェクトを作成、コピー、および編集します。ルートマップを使用して、1つのルーティングプロトコルから他のルーティングプロトコルへのルートを再配布するか、またはポリシールーティングを有効にするための条件を定義できます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [ルートマップ（Route Map）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ルートマップオブジェクトについて （2897 ページ）
- [ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （2903 ページ）
- Policy Object Manager （290 ページ）

- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *795 : [*ルートマップオブジェクトの追加または編集（*Add/Edit Route Map Object*）*]* ダイアログボックス

要素	説明
名前	ルートマップオブジェクト用の意味のある名前を入力します。ルートマップオブジェクト名は 58 文字以下にする必要があります。 **注意** Cisco Security Manager では、オブジェクトの名前は、デバイスで変更できない場合でも変更できます。Cisco Security Manager でそれらのオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Cisco Security Manager では変更結果に関する警告メッセージは表示されません。
説明	（任意）オブジェクトの説明。
ルートマップテーブル（Route Map table）	オブジェクトで定義されているルートマップエントリ。 • ルートマップエントリを追加するには、[追加（Add）] ボタンをクリックして、[ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （2903 ページ）を開きます。 • ルートマップエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • ルートマップエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて（310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス

[ルートマップエントリの追加または編集（Add/Edit Route Map Entry）] ダイアログボックスを使用して、ルートマップオブジェクトの新しいルートマップエントリを作成したり、既存のルートマップエントリを編集したりします。

ナビゲーション パス

[ルートマップオブジェクトの追加または編集（Add or Edit Route Map Object）] ダイアログボックス （2901 ページ）で、[ルートマップ（Route Map）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

関連項目

- ルートマップオブジェクトについて （2897 ページ）
- [ルートマップエントリの追加または編集（Add or Edit Route Map Entry）] ダイアログボックス （2903 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *796 : [*ルートマップエントリの追加または編集（*Add/Edit Route Map Entry*）*]* ダイアログボックス

要素	説明
シーケンス番号（Sequence Number）	このルートマップオブジェクトにすでに設定されているルートマップエントリのリストでの新しいルートマップエントリの位置を示す 0 ～ 65535 の番号。 **ヒント** 将来的に句を挿入する必要性が生じたときの番号の間隔を確保するために、少なくとも 10 単位で句に番号を指定することをお勧めします。
再配布	ルートを再配布するかどうか。一致するルートの再配布を許可するには、[許可（Permit）] をクリックします。一致するルートの再配布を拒否するには、[拒否（Deny）] を選択します。 ルートマップの Permit 句で ACL を使用すると、その ACL で許可されるルートが再配布されます。ルート マップの Deny 句で ACL を使用すると、そのACLで許可されるルートは再配布されなくなります。さらに、ルートマップの Permit または Deny 句で ACL を使用する場合に、その ACL でルートが拒否されたときは、そのルート マップ句に一致するものは見つからなかったことになり、次のルート マップ句が評価されます。
[match 句（Match Clause）] タブ [match 句（Match Clause）] タブを選択して、この句を適用する必要のあるルートを選択し、次のパラメータを設定します。	
[ルートの最初のホップインターフェイスを照合（Match first hop interface of route）]	指定したいずれかのインターフェイスの外部にネクストホップを持つルートの照合を有効または無効にします。照合するインターフェースを入力または選択します。複数のエントリがある場合は、カンマで区切ります。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。 省略記号を使用して、1 つ以上のインターフェイスを選択できるインターフェイスセレクタを開きます。インターフェイスセレクタから新しいインターフェイスロールを作成することもできます。詳細については、インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
IPv4	

要素	説明
照合アドレス	指定したいずれかのアクセスリストによって渡されるルートアドレスまたは一致パケットがあるルートの照合を有効または無効にします。 IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
[ネクストホップの照合（Match Address）]	ルートのネクストホップアドレスの照合を有効または無効にします。 IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。

要素	説明
[ルートの送信元の照合（Match Route Source）]	ルートのアドバタイジング ソース アドレスの照合を有効または無効にします。 IPv4 アドレスに対して、照合にアクセス リストまたはプレフィックス リストを使用するかどうかをドロップダウン リストから選択し、照合に使用する ACL オブジェクトまたはプレフィックス リストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクト セレクタを開きます。オブジェクト セレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
IPv6	
[アドレスの照合（Match Address）]	指定した、いずれかのアクセスリストによって渡されるルートアドレスまたは一致パケットがあるルートの照合を有効または無効にします。 IPv6 アドレスに対して、照合にアクセスリストまたは IPv6 プレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたは IPv6 プレフィックスリストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたは IPv6 プレフィックスリストオブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （2920 ページ）を参照してください。

要素	説明
[ネクストホップの照合（Match Address）]	ルートのネクストホップアドレスの照合を有効または無効にします。 IPv6 アドレスに対して、照合にアクセスリストまたはプレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたは IPv6 プレフィックスリストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたは IPv6 プレフィックスリストオブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （2920 ページ）を参照してください。
[ルートの送信元の照合（Match Route Source）]	ルートのアドバタイジング ソースアドレスの照合を有効または無効にします。 IPv6 アドレスに対して、照合にアクセスリストまたは IPv6 プレフィックスリストを使用するかどうかをドロップダウンリストから選択し、照合に使用する ACL オブジェクトまたは IPv6 プレフィックスリストを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたは IPv6 プレフィックスリストオブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストIPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （2920 ページ）を参照してください。
[メトリックルート値の照合（Match Metric Route Value）]	ルートのメトリックの照合を有効または無効にします。[メトリックルート値の照合（Match Metric Route Value）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。

要素	説明
[タグの照合（Match Tag）]	ルートのセキュリティグループタグの照合を有効または無効にします。[タグの照合（Match Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティグループタグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
[ルートタイプの照合（Match Route Type）]	ルートタイプの照合を有効または無効にします。有効なルートタイプは、External1、External2、Internal、Local、NSSA-External1、NSSA-External2 です。イネーブルの場合、複数のルートタイプをリストから選択することができます。
[set 句（Set Clause）] タブ [set 句（Set Clause）] タブを選択して、ターゲットプロトコルに再配布される次の情報を変更します。 （注） 帯域幅の値のみまたはすべての値を指定するか、まったく指定しないこともできます。	
Bandwidth	メトリック値または帯域幅（K ビット/秒単位）。0 ～ 4294967295 の整数値です。
[EIGRP 遅延（EIGRP Delay）]	EIGRP ルート遅延（10 マイクロ秒単位）。有効値の範囲は 1 ～ 4294967295 です。
[EIGRP 信頼性（EIGRP Reliability）]	0 ～ 255 の数値で表される、EIGRP のパケット伝送の成功確率。値 255 は 100 % の信頼性を意味し、0 は信頼性がないことを意味します。
[EIGRP 有効（EIGRP Effective）]	1 ～ 255 の数値で表される、ルートの有効な EIGRP 帯域幅。値 255 は、100% のロードを意味します。
[EIGRP MTU]	EIGRP のルートの最小 MTU サイズ（バイト単位）。有効値の範囲は 1 ～ 4294967295 です。
メトリック タイプの設定	宛先ルーティングプロトコルのメトリックタイプを選択して指定し、ドロップダウンリストからメトリックタイプ（[内部（internal）]、[タイプ 1（type-1）]、または[タイプ 2（type-2）]）を選択します。
[BGP match 句（BGP Match Clause）] タブ	

要素	説明
[BGP AS パスアクセスリストの照合（Match AS path access lists）]	BGP 自律システムパスアクセスリストと指定されたパスアクセスリストの照合を有効にする場合は、オンにします。複数のパス アクセス リストを指定した場合、ルートはいずれかのパスアクセスリストと一致します。 省略記号を使用して、1 つ以上の AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。AS パスオブジェクトセレクタから新しい AS パスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924ページ）を参照してください。
[コミュニティの照合（Match community）]	BGP コミュニティと指定されたコミュニティの照合を有効にするために選択します。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。少なくとも 1 つの Match コミュニティと一致しないルートは、アウトバウンドルートマップにアドバタイズされません。 省略記号を使用して、1 つ以上のコミュニティ リスト オブジェクトを選択できるコミュニティ リスト オブジェクト セレクタを開きます。コミュニティ リスト オブジェクト セレクタから新しいコミュニティ リスト オブジェクトを作成することもできます。詳細については、[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （2926ページ）を参照してください。 BGP コミュニティと指定したコミュニティの完全一致を有効にするには、[指定したコミュニティと完全に一致（Match the specified community exactly）] チェックボックスをオンにします。
[ポリシーリストの照合（Match policy list）]	BGP ポリシーを評価および処理するためのルートマップを設定する場合は、オンにします。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。 省略記号を使用して、1 つ以上のポリシーリストオブジェクトを選択できるポリシー リスト オブジェクト セレクタを開きます。ポリシー リスト オブジェクト セレクタから新しいポリシーリストオブジェクトを作成することもできます。詳細については、[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913ページ）を参照してください。
[BGP set 句（BGP Set Clause）] タブ [BGP set 句（BGP Set Clause）] タブを選択して、BGP プロトコルに再配布される次の情報を変更します。	

要素	説明
[AS パス の設定（Set AS path）]	BGPルートの自律システムパスを変更する場合は、オンにします。 • BGP ルートの前に任意の自律システムパス文字列を付加するには、[AS パスプリペンド（Prepend AS path）] をオンにします。通常、ローカルな AS 番号が複数回追加され、自律システムパス長が増します。複数の AS パス番号を指定した場合、ルートはいずれかの AS 番号を付加できます。 • 最後の AS 番号を AS パスの前に付加するには、[最後の AS を AS パスの前に付加（Prepend last AS to the AS path）] をオンにします。AS 番号の値を 1 ～ 10 の範囲で入力します。 • ルートのタグを自律システムパスに変換するには、[ルートタグを AS パスに変換する（Convert route tag into AS path）] をオンにします。
[コミュニティの設定（Set community）]	BGP コミュニティ属性を設定する場合は、オンにします。 • ルートマップをパスするプレフィックスからコミュニティ属性を除去するには、[なし（None）] をオンにします。 • コミュニティ番号を入力するには、[コミュニティの指定（Specify community）] をオンにします（必要な場合）。有効な値は、1 ～ 4294967295 です。 既存のコミュニティにコミュニティを追加するには、[既存のコミュニティに追加する（Add to the existing communities）] をオンにします。 • 既知のコミュニティのいずれかを使用するには、[インターネット（Internet）]、[アドバタイズなし（no-advertise）]、または [エクスポートなし（no-export）] をオンにします。
[自動タグ設定（Set Automatic-tag）]	自動的にタグ値を計算する場合は、オンにします。
[ローカルプリファレンスの設定（Set local preference）]	自律システムパスのプリファレンス値を指定する場合は、オンにします。0 から 4294967295 までの値を入力してください。
[重みの設定（Set weight）]	ルーティングテーブルの BGP 重みを設定する場合は、オンにします。0 ～ 65535 の範囲で値を入力します。
[発信元の設定（Set origin）]	BGP の発信元コードを選択して指定します。有効な値は [Local IGP] および [Incomplete] です。
[ネクストホップ IPv4（Next hop IPv4）]	

要素	説明
[ネクストホップの設定（Set next hop）]	ルートマップの match 句を満たすパケットの出力アドレスを指定する場合は、オンにします。 • パケットが出力されるネクストホップの IPv4 アドレスを入力するには、[IPv4 アドレスを指定（Specify IPv4 address）] をオンにします。隣接ルータである必要はありません。複数の IPv4 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。 • BGP ピアアドレスにするネクストホップを設定するには、[ピアアドレスの使用（Use peer address）] をオンにします。
[ネクストホップ IPv6（Next hop IPv6）]	
[ネクストホップの設定（Set next hop）]	ルートマップの match 句を満たすパケットの出力アドレスを指定する場合は、オンにします。 • パケットが出力されるネクストホップの IPv6 アドレスを入力するには、[IPv6 アドレスを指定（Specify IPv6 address）] をオンにします。隣接ルータである必要はありません。複数の IPv6 アドレスを指定した場合、いずれかの IP アドレスでパケットを出力できます。複数の値をカンマで区切って入力することもできます。 • BGP ピアアドレスにするネクストホップを設定するには、[ピアアドレスの使用（Use peer address）] をオンにします。
プレフィックス リスト	
[IPv4 プレフィックスリストの設定（Set IPv4 prefix list）]	IPv4 プレフィックスリストを設定する場合は、オンにします。 省略記号を使用して、1 つ以上のプレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト セレクタを開きます。プレフィックス リスト オブジェクト セレクタから新しいプレフィックスリストオブジェクトを作成することもできます。詳細については、[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。

要素	説明
[IPv6 プレフィックスリストの設定（Set IPv6 prefix list）]	IPv6 プレフィックスリストを設定する場合は、オンにします。 省略記号を使用して、1 つ以上の IPv6 プレフィックス リスト オブジェクトを選択できるプレフィックス リスト オブジェクト IPv6 セレクタを開きます。プレフィックス リスト オブジェクト セレクタから新しい IPv6 プレフィックス リスト オブジェクトを作成することもできます。詳細については、[プレフィックスリスト IPv6オブジェクトの追加または編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックス （2920ページ）を参照してください。
[ポリシーベースルーティング（PBR）（Policy Based Routing（PBR））] タブ [Policy Based Routing] タブをクリックして、トラフィック フローにポリシーを設定し、ルーティング プロトコルから派生したルートへの依存を弱めることができます。PBR は、ルーティング プロトコルで提供される既存のメカニズムを拡張および補完することにより、ルーティングの制御を強化します。PBR を使用すると、IP プレジデンスを設定できます。高コスト リンク上のプライオリティ トラフィックなど、特定のトラフィックのパスを指定することもできます。	
[デフォルトのネクストホップ IPv4 アドレスの設定（Set Default Next-Hop IPv4 Address）]	ポリシールーティング用のルートマップの match 句を渡すパケットの出力先を指定するには、[デフォルトのネクストホップ IPv4 アドレスの設定（Set default next-hop IPv4 address）] チェックボックスをオンにします。[IPv4 Address] に、宛先アドレスを入力します。
[デフォルトのネクストホップ IPv6 アドレスの設定（Set Default Next-Hop IPv6 Address）]	ポリシールーティング用のルートマップの match 句を渡すパケットの出力先を指定するには、[デフォルトのネクストホップ IPv6 アドレスの設定（Set default next-hop IPv6 address）] チェックボックスをオンにします。[IPv6 アドレス（IPv6 Address）] に宛先アドレスを入力します。
[ネクストホップ IPv4 アドレスの再帰検索および設定（Recursively find and set Next-Hop IPv4 Address）]	[Recursively find and set next-hop IP address] チェック ボックスをオンにして、[IPv4 Address] フィールドで IP アドレスを指定します。この場合、ネクストホップ IP アドレスは直接接続されたサブネットにある必要はありません。
[インターフェイスの設定（Set Interfaces）]	[インターフェイスの設定（Set interfaces）] チェックボックスをオンにして、[インターフェイスセレクタ（Interfaces Selector）] ダイアログボックスから接続先インターフェイスを選択します。
[Null0 インターフェイスをデフォルトインターフェイスとして設定（Set Null0 Interfaces as Default Interface）]	一部のトラフィックを完全にブラック ホール化またはドロップする必要がある場合には、[Set null0 interface as the default interface] チェック ボックスをオンにします。

要素	説明
do-not-fragment ビットを 0 または 1 に設定します。	[Set do-not-fragment bit to either 1or 0] をオンにして、適切なオプション ボタンを選択します。
[IPv4 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set Differential Service Code Point (DSCP) value in QOS bits for IPv4 packets）]	[IPv4 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set differential service code point (DSCP) value in QoS bits for IPv4 packets）] チェックボックスをオンにして、0 ～ 63 の値を入力するか [値の選択（Select Value）] ドロップダウンリストから値を選択します。
[IPv6 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set Differential Service Code Point (DSCP) value in QOS bits for IPv6 packets）]	[IPv6 パケットの QoS ビットに DiffServ コードポイント（DSCP）を設定（Set differential service code point (DSCP) value in QoS bits for IPv6 packets）] チェックボックスをオンにして、0 ～ 63 の値を入力するか [値の選択（Select Value）] ドロップダウンリストから値を選択します。

[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス

[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックスを使用して、ポリシーリストのポリシーオブジェクトを作成、コピー、および編集します。ルートマップの設定時に使用するポリシーリストオブジェクトを作成できます（ルートマップオブジェクトについて （2897 ページ）を参照）。

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクト タイプセレクタから [ポリシーリスト（Policy List）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- ルートマップオブジェクトについて （2897 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *797 : [*ポリシーリストオブジェクトの追加/編集（*Add/Edit Policy List Object*）*]* ダイアログボックス

要素	説明
名前	オブジェクトの名前。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ） を参照してください。 **注意** Cisco Security Manager では、オブジェクトの名前は、デバイスで変更できない場合でも変更できます。Cisco Security Manager でオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Cisco Security Manager では変更結果に関する警告メッセージは表示されません。
説明	（任意）オブジェクトの説明。
[基本（Basic）] タブ	
操作	条件に一致するアクセスを許可するかどうかを指定します。 （注） ポリシーリストオブジェクトの [アクション（Action）] は、オブジェクトの作成後は変更できません。
インターフェイスの照合（Match Interface）	指定したいずれかのインターフェイスをネクストホップとするルートを配布する場合に選択します。照合するインターフェースを入力または選択します。複数のエントリがある場合は、カンマで区切ります。2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。 省略記号を使用して、1 つ以上のインターフェイスを選択できるインターフェイスセレクタを開きます。インターフェイスセレクタから新しいインターフェイスロールを作成することもできます。詳細については、 インターフェイス ロール オブジェクトについて （381 ページ） を参照してください。

要素	説明
アドレスの照合（Match Address）	標準アクセスリストまたはプレフィックスリストで許可された宛先アドレスを持つルートを再配布するために選択します。ドロップダウンリストから [アクセスリスト（Access List）] または [プレフィックスリスト（Prefix List）] を選択し、照合に使用する ACL オブジェクトまたはプレフィックス リスト オブジェクトを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
ネクストホップの照合（Match Next-Hop）	指定したアクセスリストまたはプレフィックスリストの 1 つから渡されたネクスト ホップ ルータ アドレスを持つルートを再配布するために選択します。ドロップダウンリストから [アクセスリスト（Access List）] または [プレフィックスリスト（Prefix List）] を選択し、照合に使用する ACL オブジェクトまたはプレフィックス リスト オブジェクトを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
ルートの送信元の照合（Match Route Source）	アクセスリストまたはプレフィックスリストで指定されたアドレスのルータおよびアクセスサーバーによってアドバタイズされたルートを再配布するために選択します。ドロップダウンリストから [アクセスリスト（Access List）] または [プレフィックスリスト（Prefix List）] を選択し、照合に使用する ACL オブジェクトまたはプレフィックス リスト オブジェクトを入力または選択します。 省略記号を使用して、1 つ以上のオブジェクトを選択できるアクセス制御リストオブジェクトセレクタまたはプレフィックス リスト オブジェクトセレクタを開きます。オブジェクトセレクタから新しいオブジェクトを作成することもできます。詳細については、[Add Access List]/[Edit Access List] ダイアログボックス （365 ページ）または[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）を参照してください。
[Advanced] タブ	

要素	説明
ASパスの照合（Match AS Path）	BGP 自律システムパスを照合するために選択します。複数の AS パスを指定した場合、ルートはいずれかの AS パスと一致します。 省略記号を使用して、1 つ以上の AS パスオブジェクトを選択できる AS パスオブジェクトセレクタを開きます。AS パスオブジェクトセレクタから新しい AS パスオブジェクトを作成することもできます。詳細については、[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924 ページ）を参照してください。
コミュニティルールの照合（Match Community Rules）	BGP コミュニティと指定されたコミュニティの照合を有効にするために選択します。複数のコミュニティを指定した場合、ルートはいずれかのコミュニティと一致します。 省略記号を使用して、1 つ以上のコミュニティ リスト オブジェクトを選択できるコミュニティ リスト オブジェクト セレクタを開きます。コミュニティ リスト オブジェクト セレクタから新しいコミュニティ リスト オブジェクトを作成することもできます。詳細については、[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （2926 ページ）を参照してください。 BGP コミュニティと指定したコミュニティの完全な照合を有効にするには、[exact-match] チェックボックスをオンにします。
メトリックの照合（Match Metric）	ルートのメトリックの照合を有効または無効にします。[メトリックの照合（Match Metric）] フィールドに、照合に使用するメトリック値を入力します。複数の値をカンマで区切って入力することもできます。設定したメトリックを持つ任意のルートを照合できます。メトリック値は、0 ～ 4294967295 の範囲で指定します。
タグの照合（Match Tag）	ルートのセキュリティグループタグの照合を有効または無効にします。[タグの照合（Match Tag）] フィールドに照合に使用するタグ値を入力します。複数の値をカンマで区切って入力することもできます。指定したセキュリティグループタグを持つ任意のルートを照合できます。タグ値は、0 ～ 4294967295 の範囲で指定します。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックスを使用して、プレフィックスリストのポリシーオブジェクトを作成、コピー、および編集します。ルートマップ（ルートマップオブジェクトについて （2897ページ）を参照）、ポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）を参照）、OSPF フィルタリング（[Add Filtering]/[Edit Filtering] ダイアログボックス （2838ページ）を参照）またはBGP ネイバーフィルタリング（[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）を参照）を設定するときに使用する、プレフィックス リスト オブジェクトを作成できます。

エリア境界ルータ（ABR）のタイプ3リンクステートアドバタイズメント（LSA）フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックス リストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクト タイプセレクタから [プレフィックスリスト（Prefix List）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス （2919 ページ）
- ルートマップオブジェクトについて （2897 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *798 : [プレフィックスリストオブジェクトの追加/編集（Add/Edit Prefix List Object）] ダイアログボックス*

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシーオブジェクトの作成 （299 ページ）を参照してください。 **注意** Cisco Security Manager では、デバイスで名前を変更できない場合でもオブジェクトの名前を変更できます。Cisco Security Manager でそれらのオブジェクトの名前を変更する場合、名前の変更は、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成および割り当てることで実現できます。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Security Manager はこれらの結果に関する警告メッセージを表示しません。
説明	（任意）オブジェクトの説明。

要素	説明
プレフィックスリストテーブル	オブジェクトで定義されているプレフィックス リスト エントリ。 • プレフィックス リスト エントリを追加するには、[追加（Add）] ボタンをクリックして、[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス （2919 ページ）を開きます。 • プレフィックス リスト エントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • プレフィックス リスト エントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。 カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、 ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス

[プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックスを使用して、新しいプレフィックス リスト エントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[プレフィックスリストオブジェクトの追加/編集（Add or Edit Prefix List Object）] ダイアログボックス （2917 ページ）で、[プレフィックスリスト（Prefix Listt）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *799 : [*プレフィックスリストエントリの追加または編集（*Add/Edit Prefix List Entry*）*]* ダイアログボックス

要素	説明
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
シーケンス No（Sequence No）	（任意）このオブジェクトですでに設定されているプレフィックス リスト エントリのリストにおける、新しいプレフィックス リストエントリの位置を示す固有の数字。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。
IPアドレス	プレフィックス番号をIPアドレス/マスク長の形式で指定します。
プレフィックスの最小長（Minimum Prefix Length）	（任意）プレフィックスの最小長を入力します。 値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。
プレフィックスの最大長（Maximum Prefix Length）	（任意）プレフィックスの最大長を入力します。 値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

[プレフィックスリストIPv6オブジェクトの追加または編集（AddorEdit Prefix List IPv6 Object）] ダイアログボックス

[プレフィックスリストIPv6オブジェクトの追加/編集（Add or Edit Prefix List IPv6 Object）] ダイアログボックスを使用して、IPv6 プレフィックスリスト のポリシーオブジェクトを作成、コピー、および編集します。ルートマップ（ルートマップオブジェクトについて （2897 ページ）を参照）、ポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）を参照）、OSPF フィルタリング（[Add Filtering]/[Edit Filtering] ダイアログボックス （2838 ページ）を参照）または BGP ネイバーフィルタリング（[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2737 ページ）を参照）を設定するときに使用する、IPv6 プレフィックス リスト オブジェクトを作成できます。

エリア境界ルータ（ABR）のタイプ 3 リンクステートアドバタイズメント（LSA）フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されているときは、指定されたプレフィックスのみが OSPF エリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを

出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックスリストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクトタイプセレクタから [プレフィックスリストIPv6（Prefix ListIPv6）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [プレフィックスリストエントリの追加または編集（Add or Edit Prefix List Entry）] ダイアログボックス （2919 ページ）
- ルートマップオブジェクトについて （2897 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *800 : [IPv6プレフィックスリストオブジェクトの追加/編集（Add/Edit IPv6 Prefix List Object）] ダイアログボックス*

要素	説明
名前	IPv6プレフィックス リスト オブジェクト名、最大 128 文字。オブジェクト名では、大文字と小文字が区別されません。詳細については、ポリシー オブジェクトの作成 （299 ページ）を参照してください。 **注意** Cisco Security Manager では、デバイスで名前を変更できない場合でもオブジェクトの名前を変更できます。Cisco Security Manager でこれらのオブジェクトの名前を変更する場合、既存の CLI を無効にして、新しい CLI を発行し、新しい名前を使用してオブジェクトを作成して割り当てることで名前を変更します。この最初の無効化により、環境内でルーティングやネットワークの問題を引き起こす可能性があります。オブジェクトの名前を変更しても、Security Manager はこれらの結果に関する警告メッセージを表示しません。
説明	（任意）オブジェクトの説明。
IPv6 プレフィックス リスト テーブル	オブジェクトで定義されている IPv6 プレフィックス リスト エントリ。 • IPv6プレフィックスリストエントリを追加するには、[追加（Add）] ボタンをクリックして[IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス （2923 ページ）を開きます。 • IPv6プレフィックスリストエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • IPv6プレフィックスリストエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス

[IPv6プレフィックスリストエントリの追加または編集（Add/Edit IPv6 Prefix List Entry）] ダイアログボックスを使用して、新しい IPv6 プレフィックス リスト エントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[IPv6プレフィックスリストエントリの追加または編集（Add or Edit IPv6 Prefix List Entry）] ダイアログボックス （2923 ページ）で、[プレフィックスリスト（Prefix Listt）] テーブルの下にある [追加（Add）] ボタンをクリックするか、またはテーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *801 : [プレフィックスリストエントリの追加または編集（Add/Edit Prefix List Entry）] ダイアログボックス*

要素	説明
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
シーケンス No（Sequence No）	（任意）このオブジェクトですでに設定されている IPv6 プレフィックス リスト エントリのリストにおける、新しい IPv6 プレフィックス リスト エントリの位置を示す固有の数字。空白にしておくと、現在使用されている最大シーケンス番号より 5 大きいシーケンス番号がデフォルトになります。 （注） シーケンス番号は 1 から 4294967295 の範囲で指定する必要があります。
IPv6 アドレス	プレフィックス番号は、IPv6 アドレス/マスク長の形式で指定します。マスク長は 128 以下です。
プレフィックスの最小長（Minimum Prefix Length）	（任意）プレフィックスの最小長を 1 ～ 128 の範囲で入力します。 値は、最大プレフィックス長の値が指定されている場合に、マスク長以上、最大プレフィックス長以下でなければなりません。
プレフィックスの最大長（Maximum Prefix Length）	（任意）プレフィックスの最大長を 1 ～ 128 の範囲で入力します。 値は、最小プレフィックス長の値が指定されている場合に、最小プレフィックス長以上、最小プレフィックス長の値が指定されていない場合に、マスク長以上でなければなりません。

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックスを使用して、自律システム（AS）パスのポリシーオブジェクトを作成、コピー、編集します。ルートマップ（ルートマップオブジェクトについて （2897 ページ）を参照）、ポリシーマップ（[ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）を参照）、またはBGPネイバーフィルタリング（[ネイバーの追加/編集（Add/Edit Neighbor）] ダイアログボックス （2718 ページ）を参照）を設定するときに使用する、AS パスオブジェクトを作成できます。

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。

（注） AS パスオブジェクト名は、1 ～ 500 の一意の整数である必要があります。既存の AS パスオブジェクトと同じ名前を使用するデバイスまたは構成ファイルからASパスオブジェクトが検出された場合、Security Managerの [検出されたポリシーオブジェクトに対するデバイスのオーバーライドを許可（Allow Device Override for Discovered Policy Objects）] 設定（[Security Manager管理（Security Manager Administration）] > [検出（Discovery）] ページ）に関係なく、Security Manager の AS パスオブジェクトは上書きされます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、オブジェクトタイプセレクタから [ASパス（AS Path）] を選択します。作業領域内を右クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [パス エントリとして追加または編集] ダイアログボックス （2926 ページ）
- ルートマップオブジェクトについて （2897 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）

- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *802 : [AS*パスオブジェクトの追加（（*Add AS Path Object*））*]/[AS*パスオブジェクトの編集（*Edit AS Path Object*）*]* ダイアログボックス

要素	説明
名前	AS パスフィルタの名前を入力します。1 ～ 500 の一意の値を指定します。
説明	（任意）オブジェクトの説明。
[ASパス（AS Path）] テーブル	オブジェクトで定義されている AS パスエントリ。 • AS パスエントリを追加するには、[追加（Add）] ボタンをクリックして、[パスエントリとして追加または編集] ダイアログボックス （2926 ページ）を開きます。 • AS パスエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • AS パスエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。 • エントリを並べ替えるには、エントリを選択してから、[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトをオーバーライドするデバイスの数が表示されます。

[パス エントリとして追加または編集] ダイアログボックス

[ASパスエントリの追加（Add As Path Entry）]/[ASパスエントリの編集（Edit As Path Entry）] ダイアログボックスを使用して、新しい自立システム（AS）パスエントリを作成するか、既存のエントリを編集します。

ナビゲーション パス

[ASパスオブジェクトの追加（（Add AS Path Object））]/[ASパスオブジェクトの編集（Edit AS Path Object）] ダイアログボックス （2924 ページ）で、[ASパス（As Path）] テーブルの下にある [行の追加（Add Row）] ボタンをクリックするか、エントリを選択して [行の編集（Edit Row）] ボタンをクリックします。

フィールド リファレンス

表 *803 : [AS*パスエントリの追加（*Add As Path Entry*）*]/[AS*パスエントリの編集（*Edit As Path Entry*）*]* ダイアログボックス

要素	説明
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
正規表現（Reg Exp）	AS パスフィルタを定義する正規表現を指定します。正規表現の作成に使用できるメタ文字の詳細については、 正規表現の作成に使用されるメタ文字 （1127 ページ）を参照してください。

[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス

[プレフィックスリストオブジェクトの追加/編集（Add/Edit Prefix List Object）] ダイアログボックスを使用して、プレフィックスリストのポリシーオブジェクトを作成、コピー、および編集します。ルートマップ（ルートマップオブジェクトについて （2897 ページ）を参照）またはポリシーマップ（ [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）を参照）を設定するときに使用する、コミュニティ リスト ポリシー オブジェクトを作成できます。

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次に、オブジェクト タイプセレクタから [コミュニティリスト（Community List）] を選択します。作業領域内を右

クリックして [新規オブジェクト（New Object）] を選択するか、行を右クリックして [オブジェクトの編集（Edit Object）] を選択します。

関連項目

- [コミュニティ リスト エントリの追加または編集] ダイアログボックス （2928 ページ）
- ルートマップオブジェクトについて （2897 ページ）
- [ポリシーリストオブジェクトの追加/編集（Add or Edit Policy List Object）] ダイアログボックス （2913 ページ）
- Policy Object Manager （290 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）
- ポリシー オブジェクトの作成 （299 ページ）
- オブジェクトの編集 （303 ページ）
- カテゴリ オブジェクトの使用 （304 ページ）
- オブジェクト オーバーライドの管理 （309 ページ）
- ポリシー オブジェクトの上書きの許可 （311 ページ）

フィールド リファレンス

表 *804 : [コミュニティリストオブジェクトの追加/編集（Add/Edit Community List Object）] ダイアログボックス*

要素	説明
名前	最大 128 文字のオブジェクト名。オブジェクト名では、大文字と小文字が区別されません。詳細については、 ポリシー オブジェクトの作成 （299 ページ）を参照してください。
説明	（任意）オブジェクトの説明。

要素	説明
[コミュニティリスト（Community List）] テーブル	オブジェクトで定義されているコミュニティリストエントリ。 • コミュニティリストエントリを追加するには、[追加（Add）] ボタンをクリックして、[コミュニティ リスト エントリの追加または編集] ダイアログボックス （2928 ページ）を開きます。 • コミュニティリストエントリを編集するには、エントリを選択し、[編集（Edit）] ボタンをクリックします。 • コミュニティリストエントリを削除するには、エントリを選択し、[削除（Delete）] ボタンをクリックします。 • エントリを並べ替えるには、エントリを選択し、[上へ移動（Move Up）] または [下へ移動（Move Down）] ボタンをクリックします。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可 （311 ページ）および 個々のデバイスのポリシー オブジェクト オーバーライドについて （310 ページ）を参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

[コミュニティ リスト エントリの追加または編集] ダイアログボックス

[コミュニティリストエントリの追加/編集（Add/Edit Community List Entry）] ダイアログボックスを使用して、新しいコミュニティ リスト エントリを作成するか、既存のエントリを編集します。

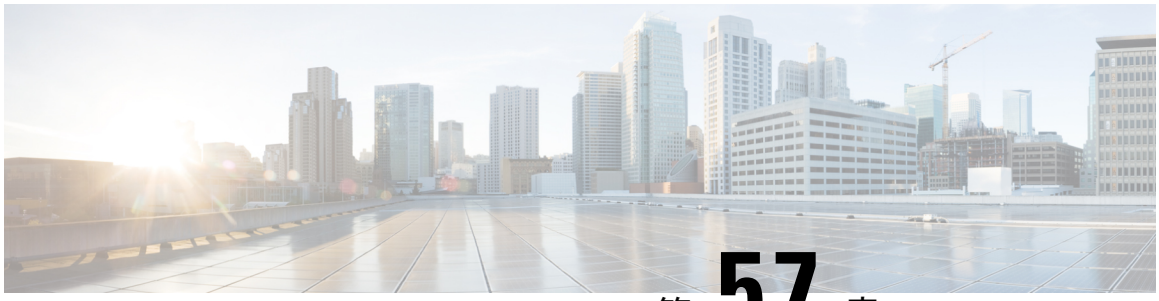
ナビゲーション パス

[コミュニティリストオブジェクトの追加または編集（Add or Edit Community List Object）] ダイアログボックス （2926 ページ）で、[コミュニティリスト（Community List）] テーブルの下にある [追加（Add）] ボタンをクリックするか、テーブル内のエントリを選択して [編集（Edit）] ボタンをクリックします。

フィールド リファレンス

表 *805 : [*コミュニティリストエントリの追加/編集（*Add/Edit Community List Entry***）*]* ダイアログボックス**

要素	説明
タイプ	[標準（Standard）] または [拡張（Expanded）] オプションボタンを選択して、コミュニティルールの種類を表示します。 （注） 標準を使用したエントリ、コミュニティ ルールの拡張種類を使用したエントリを、同じコミュニティ リスト オブジェクトに含めることはできません。
操作	[許可（Permit）] または [拒否（Deny）] オプションボタンをクリックして再配布アクセスを指定します。
コミュニティ（Communities）	コミュニティ番号を指定します。有効な値は 1 ～ 4294967295 または 0:1 ～ 65534:65535 です。
internet	インターネットのウェルノウンコミュニティを指定するには、これを選択します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
no-advertise	非アドバタイズのウェルノウンコミュニティを指定するには、これを選択します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。
no-export	非エクスポートのウェルノウンコミュニティを指定するには、これを選択します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。
式	拡張コミュニティリストの場合は、正規表現を指定します。正規表現の作成に使用できるメタ文字の詳細については、正規表現の作成に使用されるメタ文字 （1127 ページ）を参照してください。



第 57 章

ファイアウォールデバイスのセキュリティポリシーの設定

[Platform] > [Security] の [General] ページおよび [Timeouts] ページを使用して、デバイスの一般的なセキュリティ設定を行うことができます。インターフェイスでアンチスプーフィングをイネーブルにしたり、IP フラグメント設定を行ったり、デバイスのさまざまなタイムアウト値を設定したりできます。

この章は次のトピックで構成されています。

- [一般（General）] ページ （2931 ページ）
- タイムアウトの設定 （2935 ページ）

[一般（General）] ページ

[General] ページを使用して、悪意のあるパケット、スプーフィングされたパケット、フラグメント化されたパケット、および DoS 攻撃から保護するためのセキュリティ設定を行います。このページの設定の詳細については、 フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （2933 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [全般（General）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [セキュリティ（Security）] > [全般（General）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- [Add/Edit General Security Configuration] ダイアログボックス （2934 ページ）
- タイムアウトの設定 （2935 ページ）

フィールド リファレンス

表 *806 : [一般（General）] ページ*

要素	説明
Disable Floodguard（PIX 6.3 および FWSM 2.x だけ）	ファイアウォールデバイス上でフラッドガードをディセーブルにするには、このチェックボックスをオンにします。このオプションは、PIX 6.3 および FWSM 2.x デバイスでだけ使用できます。フラッドガード機能の詳細については、フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （2933ページ）を参照してください。
Global Fragment Settings 次のオプションを使用して、デバイスのグローバル フラグメント値を設定します。個々のインターフェイスに対するこれらの設定をオーバーライドできます。詳細については、[Add/Edit General Security Configuration] ダイアログボックス （2934 ページ）を参照してください。	
Enable Default Settings	デフォルトのフラグメント設定フィールドをイネーブルにするには、このチェックボックスをオンにします。
サイズ	再構成を待機する IP 再構成データベースに格納できる最大フラグメント数を指定します。デフォルトは200です。
Chain	完全な IP パケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは 24 パケットです。
タイムアウト（Timeout）	フラグメント化されたパケット全体が到着するのを待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。
Interface Configuration Table このテーブルには、個々のアンチ スプーフィング設定およびフラグメント設定が定義されているすべてのインターフェイスが示されます。これらの設定の詳細については、フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （2933 ページ）を参照してください。個々のインターフェイスにおけるこれらの値の設定の詳細については、[Add/Edit General Security Configuration] ダイアログボックス （2934 ページ）を参照してください。	

フラッドガード、アンチスプーフィング、およびフラグメント値の設定

[Platform] > [Security] の [General] ページを使用して、（PIX 6.3 または FWSM 2.x デバイスの）フラッドガードをイネーブルまたはディセーブルにし、個々のインターフェイスでユニキャスト リバース パス転送（アンチ スプーフィング）をイネーブルにし、デバイスおよびデバイスの各インターフェイスの IP フラグメント値を設定します。

フラッドガード

フラッドガードを使用すると、ユーザ認証サブシステムでリソースが不足した場合にファイアウォール リソースを再要求できます。インバウンドまたはアウトバウンドの uauth 接続が攻撃を受けている場合または過剰に使用されている場合、ファイアウォールは TCP ユーザ リソースをアクティブに再要求します。

ユーザ認証サブシステムのリソースが枯渇すると、緊急性に応じて、次の順序で、さまざまな状態の TCP ユーザ リソースが再要求されます。

1. Timewait
2. LastAck
3. FinWait
4. Embryonic
5. Idle

フラッドガードは、デフォルトでイネーブルになっています。このオプションは、PIX 6.3 または FWSM 2.x デバイスにだけ適用されます。

アンチ スプーフィング

ユニキャスト Reverse Path Forwarding（RPF; リバース パス転送）は、すべてのパケットの送信元 IP アドレスが、ルーティング テーブルに基づく正しい送信元インターフェイスに一致することを確認することによって、IP スプーフィング（本来の送信元を隠すために不正な送信元 IP アドレスを使用するパケット）を防止します。

通常、セキュリティ アプライアンスは、パケットの転送先を決めるときに、宛先アドレスだけを確認します。ユニキャスト RPF は、送信元アドレスも確認することをセキュリティ アプライアンスに指示します。これが、リバース パス転送と呼ばれる理由です。セキュリティアプライアンスの通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティアプライアンスのルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、セキュリティアプライアンスは、デフォルトのルートを使用してユニキャスト RPF 保護を実現できます。トラフィックが外部インターフェイスから入り、その送信元アドレスをルーティング テーブルが認識できない場合、セキュリティ アプライアンスはデフォルトのルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

トラフィックが、ルーティングテーブルにとって既知であるが、内部インターフェイスに関連付けられているアドレスから外部インターフェイスに入る場合、セキュリティアプライアンスはそのパケットをドロップします。同様に、トラフィックが未知の送信元アドレスから内部インターフェイスに入る場合、一致するルート（デフォルトルート）は外部インターフェイスを示しているため、セキュリティ アプライアンスはそのパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP および TCP にはセッションがあるため、初期パケットにはリバース ルート ルックアップが必要となります。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

フラグメント設定

フラグメント設定によって、パケット フラグメンテーションの管理が提供され、Network File System（NFS; ネットワーク ファイル システム）との互換性が向上します。デフォルトでは、セキュリティ アプライアンスは、IP パケットごとに最大 24 のフラグメント、および再構成を待機する最大200のフラグメントを許可します。定期的にパケットをフラグメント化するアプリケーション（NFS over UDP など）がある場合は、ネットワーク上でフラグメントを許可する必要がある場合があります。ただし、トラフィックをフラグメント化するアプリケーションがない場合は、セキュリティアプライアンス経由でのフラグメントを許可しないことを推奨します。フラグメント化されたパケットは、DoS 攻撃として使用されることがあるためです。

関連項目

- [一般（General）] ページ （2931 ページ）
- [Add/Edit General Security Configuration] ダイアログボックス （2934 ページ）

[Add/Edit General Security Configuration] ダイアログボックス

[Add/Edit General Security Configuration] ダイアログボックスを使用して、アンチ スプーフィングをイネーブルまたはディセーブルにし、フラグメント オーバーライド設定値をインターフェイスに設定します。

ナビゲーション パス

[Add/Edit General Security Configuration] ダイアログボックスには、[Platform] > [Security] > [一般（General）] ページ （2931 ページ） の [Anti-Spoofing and Fragment Interface Configuration] テーブルからアクセスできます。

関連項目

- フラッドガード、アンチ スプーフィング、およびフラグメント値の設定 （2933 ページ）

フィールド リファレンス

表 *807 : [Add/Edit General Security Configuration]* ダイアログボックス

要素	説明
インターフェイス（Interface）	アンチスプーフィングまたはフラグメント値を設定するインターフェイスの名前を入力または選択します。
Enable Anti-Spoofing	指定したインターフェイスでユニキャストRPF（アンチスプーフィング）をイネーブルにするには、このチェックボックスをオンにします。
Override Default Fragment Settings	指定したインターフェイスのデフォルトのフラグメント設定をオーバーライドするには、このチェックボックスをオンにして次のフィールドをイネーブルにしてから、新しい値を入力します。デバイスのデフォルトのグローバルフラグメント設定値については、[一般（General）] ページ （2931 ページ）を参照してください。
サイズ	指定したインターフェイスに関して、再構成を待機しているIP再構成データベースに格納できる最大フラグメント数を指定します。デフォルトは 200 です。
Chain	指定したインターフェイスに関して、完全なIPパケットをフラグメント化する場合の最大フラグメント数を指定します。デフォルトは24パケットです。
タイムアウト（Timeout）	フラグメント化されたパケット全体が、指定したインターフェイスに到着するのを待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントの到着後に開始されます。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。デフォルトは 5 秒です。

タイムアウトの設定

[Timeouts] ページを使用すると、セキュリティ アプライアンスでさまざまなタイムアウト値を設定できます。すべての時間が **hh:mm:ss** の形式になります。

これらの値は、さまざまなプロトコルの接続スロットと変換スロットのアイドルタイムアウトを表します。指定したアイドル時間中にスロットが使用されなかった場合、リソースはフリープールに戻されます。TCP 接続スロットは、通常の接続クローズ シーケンスの約 60 秒後に解放されます。

危険 これらの値は、カスタマー サポートに指示された場合を除き、変更しないことを推奨します。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから、[PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [セキュリティ（Security）] > [タイムアウト（Timeouts）] を選択します。ポリシー セレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

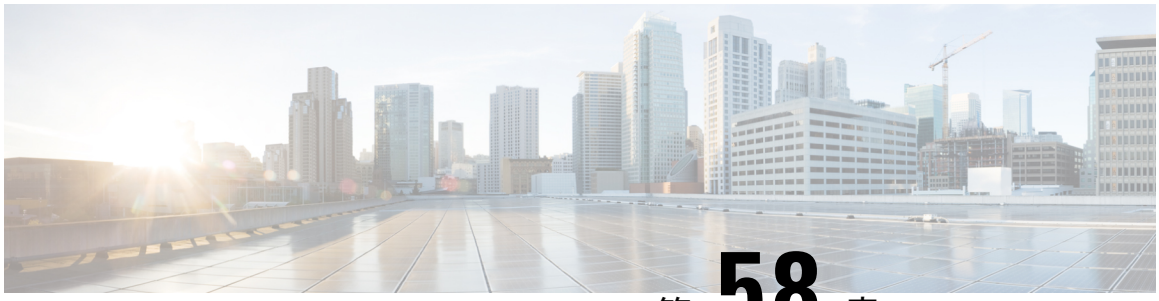
表 *808 : [Timeouts]* ページ

要素	説明
パラメータのタイムアウト値を変更するには、そのパラメータ エントリの左にあるオプション ボタンをクリックしてアクティブ化してから、そのパラメータ フィールドに新しい値を入力します。値をデフォルトにリセットするには、関連する [Default] ボタンをクリックします。 [Disable] ボタン（提供されている場合）をクリックすると、値が 0:00:00 に設定され、そのタイムアウトがディセーブルになります。前の段落のいずれかの手順を実行して、ディセーブルになっている値を再度イネーブルにします。	
Translation Slot (xlate)	変換スロットが解放されるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 3 時間です。このタイムアウトをディセーブルにするには、0:00:00 を入力します。
Connection (conn)	接続スロットが解放されるまでのアイドル時間。この値は 5 分以上である必要があります。デフォルトは 1 時間です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
Half-Closed	TCP ハーフクローズ接続が閉じられるまでのアイドル時間。ASA 9.1.2 以降のデバイスの場合、最小値は 30 秒です。他のすべてのデバイスの場合、最小値は 5 分です。デフォルトは 10 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
UDP	UDP プロトコル接続が閉じられるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 2 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。

要素	説明
SCTP	SCTP プロトコル接続が閉じられるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 2 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
接続ホールドダウン（Connection Holddown）	トラフィックが転送されるまでのアイドル時間。これは、ルートフラッピングを回避するために、トラフィックを転送する前に ASA が待機する時間です。この値は 1 秒以上にする必要があります。デフォルトは 15 秒です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
ICMP（PIX 7.x+、ASA、FWSM 3.x+）	全般的な ICMP 状態が終了するまでのアイドル時間。
RPC/Sun RPC	SunRPC スロットが解放されるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 10 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
H.225	H.225 シグナリング接続が閉じられるまでのアイドル時間。H.225 のデフォルトのタイムアウトは 1 時間（01:00:00）です。この値を 00:00:00 に設定すると、接続が閉じられなくなります。すべてのコールがクリアされた直後に接続を閉じるには、1 秒（0:00:01）を入力します。
H.323	H.323 メディア接続が閉じられるまでのアイドル時間。デフォルトは 5 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
MGCP	MGCP メディア ポートが閉じられるまでのアイドル時間。デフォルトは 5 分（0:05:00）です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
MGCP PAT（PIX 7.x+、ASA、FWSM 3.x+）	MGCP PAT 変換が削除されるまでのアイドル時間。最小時間は 30 秒です。デフォルトは 5 分（0:05:00）です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
SIP	SIP シグナリング ポート接続が閉じられるまでのアイドル時間。この値は 5 分以上である必要があります。デフォルトは 30 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。

要素	説明
SIP Media	SIP メディア ポート接続が閉じられるまでのアイドル時間。この値は 1 分以上である必要があります。デフォルトは 2 分です。このタイムアウトをディセーブルにするには、[無効（Disable）] をクリックするか 0:00:00 を入力します。
SIP Disconnect（PIX 6.3(5)、PIX/ASA 7.2+、FWSM 3.2+）	CANCEL または BYE メッセージに対する 200 OK を受信しなかった場合に、SIP セッションが削除されるまでのアイドル時間。最小値は 0:00:01 です。最大値は 0:10:00 です。デフォルト値は 0:02:00 です。
SIP Invite（PIX 6.3(5)、PIX/ASA 7.2 以降、FWSM 3.2 以降）	暫定応答のピンホールおよびメディア xlate が終了するまでのアイドル時間。最小値は 0:01:00 です。最大値は 0:30:00 です。デフォルト値は 0:03:00 です。
SIP Provisional Media（PIX/ASA 7.2(3)+）	SIP プロビジョニングメディア接続のタイムアウト値。値の範囲は 0:01:00 ～ 1193:00:00 である必要があります。デフォルトは 2 分です。
承認タイプ(uath) Absolute	認証キャッシュがタイムアウトし、新しい接続の再認証が必要となるまでの時間。システムは、ユーザが新しい接続を開始するまで待機してから、再認証を要求します。この時間は、変換スロット値よりも短い必要があります。キャッシングをディセーブルにし、すべての新しい接続に対して再認証を要求するには、[無効（Disable）] をクリックするか、0:00:00 を入力します。 （注） 接続でパッシブ FTP を使用する場合は、この値を 0:00:00 に設定しないでください。 （注） この値を 0:00:00 に設定すると、 HTTPS 認証が機能しない場合があります。HTTPS 認証後に、ブラウザが複数の TCP 接続を開始して Web ページをロードすると、最初の接続は許可されますが、その後の接続では認証がトリガーされます。このため、ユーザーには、認証の成功後も常に認証ページが表示されます。これを回避するには、認証の絶対タイムアウトを 1 秒に設定します。ただし、この回避策では、同じ送信元 IP アドレスからアクセスした認証されていないユーザがファイアウォールを通過できる期間が 1 秒間発生します。
承認タイプ(uath) Inactivity	認証キャッシュがタイムアウトし、ユーザによる新しい接続の再認証が必要となるまでのアイドル時間。この期間は、変換スロット値よりも短い必要があります。

要素	説明
IGP	Cisco ASA は、ダイナミック ルーティング プロトコル（ボーダー ゲートウェイ プロトコル（BGP）および Open Shortest Path First（OSPF））について、ソフトウェアバージョン 9.3.1 以降でノンストップ フォワーディングをサポートします。Open Shortest Path First（OSPF）のコンバージェンス時間は、デフォルトで 70 秒です。 このフィールドを使用して、コンバージェンス時間を変更できます。この値は、10 秒から 1 時間 40 秒の範囲内である必要があります。IGP のデフォルト値は 0:01:10 です。



第 58 章

ファイアウォール デバイスでのサービス ポリシールールの設定

ここでは、サービス ポリシールールを設定する方法について説明します。サービス ポリシーを使用すると、一貫した柔軟な方法で、プライオリティ キューイング、アプリケーション インスペクション、Quality of Service（QoS）など、特定のセキュリティ アプライアンス機能を設定できます。たとえば、サービス ポリシーを使用すると、すべての TCP アプリケーションに適用されるタイムアウト コンフィギュレーションではなく、特定の TCP アプリケーションに固有のタイムアウト コンフィギュレーションを作成できます。

- サービス ポリシールールについて （2941 ページ）
- TCP ステート バイパスについて （2943 ページ）
- [Priority Queues] ページ （2944 ページ）
- [サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）
- トラフィック フロー オブジェクトの設定 （2965 ページ）
- TCP マップの設定 （2971 ページ）

サービス ポリシールールについて

サービス ポリシールールには、次の機能が含まれています。

- TCP 接続設定および一般接続設定（TCP ステート バイパスを含む。 TCP ステート バイパスについて （2943 ページ）を参照）
- Content Security Control（CSC）
- アプリケーション インスペクション
- 侵入防御サービス
- QoS キューイングおよびポリシング
- ASA CX リダイレクション（ ASA CX について （2963 ページ）を参照）
- ASA FirePOWER リダイレクション

- アイデンティティベースのファイアウォール ポリシーのユーザ統計情報

これらの機能の設定オプションは、Cisco Security Manager の 2 つのページ（[プライオリティキュー（Priority Queues）] および [ルール（Rules）]）にあります。これらのページには、[プラットフォーム（Platform）] > [サービスポリシー（Service Policy）] に移動してアクセスできます。

プライオリティ キューイング

プライオリティキューイングでは、低遅延キューイング（LLQ）プライオリティキューおよび「ベストエフォート」キューの2つのキューがインターフェイスに設定されます。この機能により、音声およびビデオなど、遅延の影響を受けやすいトラフィックを優先して、他のトラフィックより先に送信できます。プライオリティキュー内のパケットは、常にベストエフォート キュー内のパケットより先に送信されます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューが一杯になると、それ以上はパケットをキューに格納することができなくなり、パケットはドロップされます。これは「テールドロップ」と呼ばれます。テールドロップを最小限に抑えるには、キューのバッファサイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションにより、プライオリティキューイングの遅延およびロバストネスを制御できます。

プライオリティ キューイングは Quality of Service（QoS）の機能です。Security Manager では、プライオリティ キュー サイズおよび送信キュー サイズを [Priority Queues] ページ （2944 ページ）で管理します。一方、トラフィック クラスのプライオリティ キューイングは、Service Policy (MPC) Rule ウィザードの [QoS] タブにあるオプションで設定します。このウィザードには、[サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）からアクセスします。

アプリケーション インスペクションおよび QoS

アプリケーションの中には、セキュリティ アプライアンスによる特別な処理を必要とするものがあります。このため、固有のアプリケーション インスペクション エンジンが用意されています。特に、ユーザ データ パケットに IP アドレス情報を埋め込むアプリケーション、または動的に割り当てられるポートでセカンダリ チャネルを開くアプリケーションなどでは特別な検査が必要です。

アプリケーションインスペクションは、デフォルトで多くのプロトコルに対してイネーブルになっていますが、ディセーブルになっているプロトコルもあります。多くの場合、アプリケーション インスペクション エンジンがトラフィックをモニタするポートは変更可能です。

アプリケーション インスペクション エンジンはネットワーク アドレス変換（NAT）と連動し、埋め込まれたアドレス情報の位置を特定できます。このことにより、これらの埋め込みアドレスを NAT で変換し、変換によって影響を受けるチェックサムまたはその他のフィールドを更新できるようになります。

サービス ポリシー ルールでは、セキュリティ アプライアンスで処理されるさまざまなタイプのトラフィックに、特定タイプのアプリケーションインスペクションを適用する方法を定義し

ます。ルールは、特定のインターフェイスに適用するか、またはすべてのインターフェイスにグローバルに適用できます。

これらのルールにより、Cisco IOS ソフトウェアの Quality of Service（QoS）CLI と同じ仕組みで、セキュリティ アプライアンスの機能を設定できます。たとえば、サービス ポリシールールを使用して、トラフィックを識別する基準の 1 つとして IP precedence を追加し、レートを制限できます。すべての TCP アプリケーションに適用されるタイムアウト設定を作成する一方で、特定の TCP アプリケーションに固有のタイムアウト設定を作成することもできます。

アプリケーション インスペクションを適用するトラフィックのタイプを定義するには、トラフィック一致基準を使用します。たとえば、ポート 23 の TCP トラフィックは Telnet トラフィック クラスに分類できます。すると、トラフィック クラスを使用して接続制限を適用できます。

トラフィック一致基準は、単一のインターフェイスに複数割り当てることができます。ただし、パケットが一致するのは、特定のサービス ポリシールール内の最初の基準だけです。

TCP ステート バイパスについて

デフォルトでは、ASA または FWSM を通過するすべてのトラフィックは、アダプティブ セキュリティ アルゴリズムを使用して検査され、セキュリティポリシーに基づいて、通過を許可されるか、またはドロップされます。デバイスは、各パケットの状態をチェックして（新規の接続か確立済み接続であるかを判定し）、そのパケットをセッション管理パス（新規接続の SYN パケットの場合）、高速パス（確立済みの接続の場合）、またはコントロールプレーンパス（高度なインスペクションの場合）に割り当てることによって、ファイアウォールのパフォーマンスを最大限に高めます。

（注） TCP ステート バイパスは、FWSM 3.2+ デバイスおよび ASA 8.2+ デバイスだけで使用可能です。

高速パスの既存の接続に一致する TCP パケットは、セキュリティ ポリシーをすべて再チェックしなくてもアプライアンスを通過できます。この機能によってパフォーマンスは最大になります。ただし、SYN パケットを使用して高速パスでセッションを確立する方式、および高速パス内で発生するチェック（TCP シーケンス番号など）は、接続のアウトバウンドおよびインバウンド フローが同じデバイスを通過する必要があり、非対称ルーティング環境に該当しません。

たとえば、新規接続がセキュリティ デバイス 1 に割り当てられるとします。SYN パケットはセッション管理パスを通過し、接続のエントリが高速パステーブルに追加されます。この接続の後続パケットがデバイス 1 を通過した場合、高速パス内のエントリに一致するのでこのパケットは送信されます。ただし、後続パケットがデバイス 2 に向かった場合、SYN パケットはこのデバイスのセッション管理パスを通過していないので、高速パス内に接続のエントリは存在せず、パケットはドロップされます。

したがって、アップストリームルータに非対称ルーティングが設定されていて、トラフィックが 2 つのセキュリティデバイスを通過することがある場合は、これらの特定のトラフィックフローの TCP ステートバイパスをイネーブルにします。TCP ステート バイパスは、高速パスで

のセッションの確立方法を変更し、高速パスのインスペクションをディセーブルにします。この場合、TCP トラフィックは UDP 接続を処理するときと同じように処理されます。つまり、指定されたネットワークに一致する SYN パケット以外のパケットがセキュリティ デバイスに送信され、高速パス エントリが存在しない場合、そのパケットは高速パス内で接続を確立するためにセッション管理パスを通過します。いったん高速パスに入ると、トラフィックは高速パスのインスペクションをバイパスします。

サポートされない機能

TCP ステート バイパスをイネーブルにする場合、次の機能はサポートされません。

- アプリケーション インスペクション：アプリケーション インスペクションでは、インバウンドおよびアウトバウンドのトラフィックが同じセキュリティデバイスを通過する必要があります。したがって、TCP ステート バイパスではアプリケーション インスペクションがサポートされていません。
- AAA 認証セッション：あるセキュリティ デバイスでユーザを認証した場合、トラフィックが他のセキュリティデバイスを経由すると、そのデバイスではユーザが認証されていないため、トラフィックは拒否されます。
- TCP 代行受信、最大初期接続の制限、TCP シーケンス番号のランダム化：TCP ステート バイパスをイネーブルにした場合、デバイスは接続の状態を追跡しません。したがって、これらの機能は適用できません。
- Cisco Content Security and Control Security Services Module（CSC SSM）：TCP ステート バイパスで SSM および SSC 機能は使用できません。

NAT との互換性

変換セッションはセキュリティ デバイスごとに独立して確立されるため、スタティック NAT は必ず TCP ステート バイパス トラフィックの両方のデバイスに設定します。ダイナミック NAT を使用する場合、デバイス 1 のセッションに選択されるアドレスと、デバイス 2 のセッションに選択されるアドレスは異なります。

関連項目

- サービス ポリシールールについて （2941 ページ）

[Priority Queues] ページ

プライオリティ キューにより、ネットワークのトラフィックにプライオリティを付ける方法を定義できます。パケットの特性に基づいてプライオリティの異なるキューにトラフィックを格納する、一連のフィルタを定義できます。プライオリティの最も高いキューが最初に処理され、そのキューが空になると、プライオリティが次に高いキューから低いキューへと順番に処理が進みます。

Security Manager では、このページでプライオリティ キュー サイズおよび送信キュー サイズを管理します。一方、トラフィック クラスのプライオリティ キューイングは、Service Policy (MPC) Rule ウィザードの [QoS] タブにあるオプションで設定します。このウィザードには、[サービスポリシールール（Service Policy Rules）]ページ （2946 ページ）からアクセスします。

これらのキューを追加および編集するには、[Priority Queue Configuration] ダイアログボックスを使用します。このページの [Priority Queues] テーブルに表示されるフィールドの詳細については、 [Priority Queue Configuration] ダイアログボックス （2945 ページ）を参照してください。

（注） プライオリティキューイングはCatalyst 6500 サービスモジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[サービスポリシールール（Service Policy Rules）] > [プライオリティキュー（Priority Queues）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [サービスポリシールール（Service Policy Rules）] > [プライオリティキュー（Priority Queues）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- Insert/Edit Service Policy (MPC) Rule ウィザード （2948 ページ）
- サービス ポリシールールについて （2941 ページ）
- キューイング パラメータについて （3293 ページ）

[Priority Queue Configuration] ダイアログボックス

[Priority Queues] ページでプライオリティ キューを定義および編集するには、[Priority Queue Configuration] ダイアログボックスを使用します。

（注） プライオリティキューイングはCatalyst 6500 サービスモジュール（ファイアウォール サービス モジュールおよび適応型セキュリティ アプライアンス サービス モジュール）では使用できません。

ナビゲーション パス

[Priority Queue Configuration] ダイアログボックスを開くには、[Priority Queues] ページ （2944 ページ）で [Add Row] ボタンまたは [Edit Row] ボタンをクリックします。

関連項目

- Insert/Edit Service Policy (MPC) Rule ウィザード （2948 ページ）
- サービス ポリシールールについて （2941 ページ）
- キューイング パラメータについて （3293 ページ）

フィールド リファレンス

表 809 : [Priority Queue Configuration] ダイアログボックス

要素	説明
Interface Name	このルールが適用されるインターフェイスを指定します。インターフェイス名を入力するか、または [Select] をクリックして使用可能なインターフェイスを選択できます。
キュー制限（Queue Limit）	プライオリティ キューに格納できるパケットの最大数を入力します。この最大数を超えると、データがドロップされます。この制限には、0 ～ 2048 パケットの範囲を指定する必要があります。
Transmission Ring Limit	送信キューに格納できるパケットの最大数を入力します。これで送信キューを微調整すると遅延を短縮でき、送信ドライバを介してパフォーマンスを向上できます。 PIX デバイスの場合、この値の範囲は 3 ～ 128 パケットです。バージョン 7.2 よりも前の ASA の場合は、この制限を 3 ～ 256 パケットの範囲で指定します。また、バージョン 7.2 以降を実行している ASA の場合は、3 ～ 512 パケットの範囲で指定します。

[サービスポリシールール（Service Policy Rules）] ページ

新しいサービスポリシールールを定義し、既存のサービスポリシールールを編集または削除するには、[サービスポリシールール（Service Policy Rules）] ページを使用します。

サービスポリシールールの設定は、次の 3 つのタスクで構成されています。

1. **サービスポリシーの設定**。サービス ポリシーを作成し、そのサービス ポリシーが適用されるインターフェイスを決定します。詳細については、手順 1：サービス ポリシーの設定 （2948 ページ）を参照してください。

2. **トラフィッククラスの設定**。サービス ポリシーが適用されるトラフィックを識別する基準を指定します。詳細については、手順2：トラフィック クラスの設定 （2949ページ）を参照してください。

3. **アクションの設定**。情報またはリソースを保護するために実行するアクション、またはこのサービス ポリシーで指定されたトラフィックの QoS 機能を実行するアクションを指定します。詳細については、手順3：MPCアクションの設定 （2950ページ）を参照してください。

この 3 つのタスクの実行には、Insert/Edit Service Policy (MPC) Rule ウィザード （2948 ページ）を使用します。このページの [サービスポリシールール（Service Policy Rules）] テーブルに表示されるフィールドの詳細については、個々のタスクのトピックを参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）]>[サービスポリシールール（Service Policy Rules）] > [プライオリティキュー（Priority Queues）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）] > [サービスポリシー（Service Policy）] > [ルール（Rules）] を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または新しいポリシーを作成します。

ASA CX 認証プロキシの設定

[サービスポリシールール（Service Policy Rules）] テーブルの下にある [CXSC認証プロキシ（CXSC Auth Proxy）] ボタンをクリックすると、ASA CX 認証プロキシの設定 （2964 ページ）で説明されている [CXSC認証プロキシ設定の追加/編集（Add/Edit CXSC Auth Proxy Configuration）] ダイアログボックスが開きます。

[CXSC認証プロキシ（CXSC Auth Proxy）] ボタンには、デバイスビューの [サービスポリシールール（Service Policy Rules）] テーブルの下でのみアクセスできます。ポリシービューには表示されません。

（注） Security Manager は、ASA CX セキュリティ サービス プロセッサ（SSP）を参照する場所の一部で「CXSC」を使用します。

関連項目

- サービス ポリシールールについて （2941 ページ）
- 標準のルール テーブルに関する内容：
  - ルール テーブルの使用 （764 ページ）
  - テーブルのフィルタリング （64 ページ）

• テーブル カラムおよびカラム見出しの機能 （66 ページ）

Insert/Edit Service Policy (MPC) Rule ウィザード

[サービスポリシールール（Service Policy Rules）]ページでサービスポリシールールを追加および編集するには、Insert/Edit Service Policy (MPC) Rule ウィザードを使用します。Insert/Edit Service Policy (MPC) Rule ウィザードにより、次の手順が示されます。

• 手順 1：サービス ポリシーの設定 （2948 ページ）
• 手順 2：トラフィック クラスの設定 （2949 ページ）
• 手順 3：MPC アクションの設定 （2950 ページ）

（注） 「MPC」は現在モジュラー ポリシー フレームワークを指します。詳細については、「モジュラ ポリシー フレームワークの使用」を参照してください。

ナビゲーション パス

[サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）で [Add Row or Edit Row] ボタンをクリックして、Insert/Edit Service Policy (MPC) Rule ウィザードを開きます。

手順 1：サービス ポリシーの設定

サービスポリシー（MPC）ルールの挿入/編集（Insert/Edit Service Policy (MPC) Rule）ウィザードを使用してサービスポリシールールを設定する最初の手順は、ルールのイネーブル化とルールを適用するインターフェイスの指定です。

ナビゲーション パス

[サービスポリシールール（Service Policy Rules）] ページ （2946 ページ）で [Add Row or Edit Row] ボタンをクリックして、Insert/Edit Service Policy (MPC) Rule ウィザードを開きます。

関連項目

• 手順 2：トラフィック クラスの設定 （2949 ページ）
• 手順 3：MPC アクションの設定 （2950 ページ）

表 *810 : Insert/Edit Service Policy (MPC) Rule* ウィザード - 手順 *1*：サービス ポリシーの設定

要素	説明
Enable The Current MPC Rule	このサービスポリシールールをイネーブルにするには、このチェックボックスをオンにします。現時点でルールを定義しておき、あとからデバイスに展開する場合は、このオプションの選択を解除します。
カテゴリ	ルールをカテゴリに割り当てるには、このリストからカテゴリを選択します。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。詳細については、カテゴリ オブジェクトの使用 （304 ページ）を参照してください。
説明	（任意）サービス ポリシールールの説明を入力します。
Global - Applies to All Interfaces	すべてのインターフェイスにグローバルにルールを適用するには、このオプションを選択します。このオプションは、アクセスリストを使用して、送信元または宛先IPアドレスに基づいてトラフィックを照合する機能とは互換性がありません。
インターフェイス	特定のインターフェイスまたはインターフェイスのグループ（あるいはインターフェイスロール）にルールを適用するには、このオプションを選択したあと、インターフェイスまたはインターフェイスオブジェクトの名前を入力または選択します。 この選択は、アクセス リストを使用して、送信元または宛先 IP アドレスに基づいてトラフィックを照合する場合は必須です。 （注） インターフェイス固有のルールは、指定した機能のグローバルサービスポリシーに優先します。たとえば、FTPインスペクションを行うグローバル ポリシーと、TCP 接続制限を行うインターフェイスポリシーが設定されている場合、インターフェイスには FTP インスペクションおよび TCP 接続制限がどちらも適用されます。これに対し、FTPインスペクションのグローバルポリシーと、FTPインスペクションのインターフェイスポリシーがある場合は、インターフェイス ポリシーの FTP インスペクションだけがインターフェイスに適用されます。

手順 2：トラフィック クラスの設定

Insert/Edit Service Policy (MPC) Rule ウィザードを使用してサービスポリシールールを設定する 2 番めの手順は、ルールを適用するトラフィッククラスの指定です。

このルールのトラフィックを照合するクラスを指定します。

- [class-defaultをトラフィッククラスとして使用（Use class-default As The Traffic Class）]：このサービスポリシーでトラフィッククラス class-default を使用するには、このオプションを選択します。class-default トラフィック クラスは、すべてのトラフィックを照合します。

- [トラフィッククラス（Traffic Class）]：特定のトラフィッククラスにこのルールを適用するには、このオプションを選択します。定義済みのトラフィッククラスの名前を入力するか、または [選択（Select）] をクリックしてトラフィックフローセレクタからトラフィッククラスを選択します。

また、トラフィックフローセレクタで [作成（Create）] または [編集（Edit）] ボタンをクリックし、「オンザフライ」でトラフィックフローを定義または編集できます（トラフィックフローは Policy Object Manager の [トラフィックフロー（Traffic Flows）] ページでも作成および編集できます）。詳細については、トラフィック フロー オブジェクトの設定 （2965 ページ）を参照してください。

関連項目

- 手順 1：サービス ポリシーの設定 （2948 ページ）
- 手順 3：MPC アクションの設定 （2950 ページ）

手順 3：MPC アクションの設定

Insert/Edit Service Policy (MPC) Rule ウィザードの 3 番めの手順は、ルールに関する IPS、CXSC、FirePOWER、接続設定、QoS、CSC、ユーザー統計情報、ScanSafe Web セキュリティ、および NetFlow のパラメータの指定です。各パラメータセットは、別々のタブ付きパネルに表示されます。

関連項目

- 手順 1：サービス ポリシーの設定 （2948 ページ）
- 手順 2：トラフィック クラスの設定 （2949 ページ）

フィールド リファレンス

表 *811 : Insert/Edit Service Policy (MPC) Rule* ウィザード - 手順 *3*：アクションの設定。

要素	説明
[Intrusion Prevention] タブ	
Enable IPS for this Traffic	このトラフィック フローの侵入防御をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このパネル上の他のパラメータが使用可能になります。 （注） これらのパラメータは、IPS モジュールが取り付けられている ASA 7.0 以降のデバイスにのみ適用できます。詳細については、ASA デバイスでの IPS モジュールについて （2961 ページ）を参照してください。

要素	説明
IPS Mode	侵入防御の動作モードを選択します。 • [インライン（Inline）]：このモードでは、IPS モジュールをトラフィックフローに直接配置します。IPS 検査対象と認識されたトラフィックは、最初に IPS モジュールに渡されて検査を受けないと、ASA を通過できません。インスペクションの対象と識別されたすべてのパケットが分析されてから通過を許可されるため、このモードが最も安全です。また、IPS モジュールはパケット単位でブロッキング ポリシーを実装できます。ただし、このモードはスループットに影響する可能性があります。 • [無差別（Promiscuous）]：このモードでは、トラフィックの重複ストリームが IPS モジュールに送信されます。このモードの安全性はインライン モードより低くなりますが、トラフィックのスループットにはほとんど影響しません。[Inline] モードとは異なり、[Promiscuous] モードでは IPS モジュールは元のパケットをドロップできません。トラフィックをブロックできるのは、ASA にトラフィックの排除を指示するか、またはアプライアンス上の接続をリセットした場合だけです。 また、IPS モジュールがトラフィックを分析している間、IPS モジュールがそのトラフィックを排除する前に少量のトラフィックが ASA を通過することがあります。
On IPS Card Failure	IPS モジュールが動作不能になった場合に実行するアクションを指定します。次のいずれかを選択します。 • [開く（Open）]：モジュールまたはカードで障害が発生した場合にトラフィックを許可します。 • [閉じる（Close）]：モジュールまたはカードで障害が発生した場合にトラフィックをブロックします。
仮想センサー	追加または編集しているサービスポリシー内の仮想センサーを表示、編集、または削除できるテキストボックス
[CXSC] タブ （注） Cisco Security Manager は、ASA CX セキュリティ サービス プロセッサ（SSP）を参照する場所で「CXSC」を使用します。	

要素	説明
このトラフィックのCXSCの有効化（Enable CXSC For This Traffic）	ASA にインストールされている ASA CX へのトラフィックフローのリダイレクトを有効にするには、このボックスをオンにします。このチェックボックスをオンにすると、このパネル上の他のパラメータが使用可能になります。 （注） これらのパラメータは、ASA CX SSP がインストールされている、バージョン 8.4(4) 以降を実行している ASA 5585-X デバイスおよびバージョン 9.1(1) 以降を実行している ASA 55xx-X デバイスにのみ適用されます。
コンテキストセキュリティカードの障害時（On Context Security Card Failure）	ASA CX が動作不能になった場合に実行するアクションを指定します。次のいずれかを選択します。 • [開く（Open）]：何らかの理由で ASA CX に障害が発生した場合、ASA は、本来なら ASA CX にリダイレクトされるトラフィックを引き続き通過させます。 • [閉じる（Close）]：ASA CX に障害が発生した場合、ASA は、本来なら ASA CX にリダイレクトされるトラフィックをドロップします。
認証プロキシの有効化（Enable Auth Proxy）	認証プロキシを有効にするには、このボックスをオンにします。認証プロキシは、アクティブ認証を ASA CX での ID ポリシーに使用する場合に必要です。オンになっていない場合、認証は実行されません。 （注） 認証プロキシに使用されるポートを変更できます。詳細については、ASA CX 認証プロキシの設定 （2964 ページ）を参照してください。
[FirePOWER] タブ	
このトラフィックに対するFirePOWERカードの有効化（Enable FirePOWER Card For This Traffic）	ASA にインストールされている ASA FirePOWER モジュールへのトラフィックフローのリダイレクトを有効にするには、このボックスをオンにします。このチェックボックスをオンにすると、このパネル上の他のパラメータが使用可能になります。 （注） これらのパラメータは、バージョン 9.2(1) 以降を実行している ASA 55xx-X デバイスにのみ適用されます。

要素	説明
FirePOWERカード障害時（On FirePOWER Card Failure）	ASA FirePOWER モジュールが動作不能になった場合に実行するアクションを指定します。次のいずれかを選択します。 • [開く（Open）]：何らかの理由で ASA FirePOWER モジュールに障害が発生した場合、ASA は、本来なら ASA FirePOWER にリダイレクトされるトラフィックを引き続き通過させます。 • [閉じる（Close）]：ASA FirePOWER モジュールに障害が発生した場合、ASA は、本来なら ASA FirePOWER モジュールにリダイレクトされるトラフィックをドロップします。
モニター専用の有効化（Enable Monitor Only）	モジュールをモニタ専用モードに設定します。モニタ専用モードでは、モジュールはデモンストレーションを目的としてトラフィックを処理できますが、その後トラフィックをドロップします。トラフィック転送インターフェイスまたはデバイスを実稼働用に使用することはできません。
[接続設定（Connection Settings）] タブ	
Enable Connection Settings For This Traffic	このトラフィック フローの接続設定をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、このパネル上の他のパラメータがアクティブになります。[Connection Settings] タブでは、最大接続、初期接続、タイムアウト、およびTCPのパラメータを設定できます。

要素	説明
最大接続数	TCP 接続と UDP 接続の最大数、およびこのトラフィック フローの初期接続の最大数を指定できます。 • [TCP接続とUDP接続の最大数（Maximum TCP & UDP Connections）]：サブネット全体の TCP および UDP の最大同時接続数を指定します。上限は、8.4(5) より前の ASA バージョンの場合は 65,535、ASA 8.4(5) 以降のバージョンの場合は 2,000,000 です。どちらのプロトコルもデフォルトは 0 で、この場合に許可される接続は無制限です。 • [クライアントごとのTCP接続とUDP接続の最大数（Maximum TCP & UDP Connections Per Client）]：ASA/PIX 7.1 以降の場合のみ、クライアント単位で TCP および UDP の最大同時接続数を指定します。ASA 8.4(5) 以降の場合、最大数は 2,000,000 です。 • [最大初期接続数（Maximum Embryonic Connections）]：ASA/PIX 7.0 以降の場合のみ、ホストごとの最大初期接続数を指定します。上限は、8.4(5) より前の ASA バージョンの場合は 65,535、ASA 8.4(5) 以降のバージョンの場合は 2,000,000 です。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。この制限により、TCP 代行受信機能がイネーブルになります。デフォルトは 0 で、この場合の初期接続数は無制限です。TCP 代行受信は、TCP SYN パケットを使用してインターフェイスをフラッディングすることによる DoS 攻撃から内部システムを保護します。初期接続制限を超えると、クライアントからセキュリティ レベルのより高いサーバに送信される TCP SYN パケットが、TCP 代行受信機能によって代行受信されます。検証プロセス中には SYN クッキーが使用され、有効なトラフィックのドロップ量を最小限に抑えることができます。したがって、到達不能なホストからの接続試行がサーバに到達することはありません。この機能は、TCP ステート バイパスがイネーブルになっている場合には適用されません。 • [クライアントごとの最大初期接続数（Maximum Embryonic Connections Per Client）]：ASA/PIX 7.1 以降の場合のみ、クライアント単位で最大初期接続数を指定します。ASA 8.4(5) 以降の場合、最大数は 2,000,000 です。この機能は、TCP ステート バイパスがイネーブルになっている場合には適用されません。

要素	説明
接続タイムアウト数	このトラフィック フローの次の接続タイムアウト設定を指定できます。 • [初期接続タイムアウト（Embryonic Connection Timeout）]：初期接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトを無効にするには、0:00:00 と入力します。デフォルトは FWSM で 20 秒、ASA/PIX デバイスで 30 秒です。 • [ハーフクローズ接続タイムアウト（Half Closed Connection Timeout）]：ハーフクローズ接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトを無効にするには、0:00:00 と入力します。 FWSM の場合、デフォルト値は 20 秒、最大値は 255 秒（4 分 15 秒）です。 ASA 9.1.2 以降のデバイスの場合、最小値は 30 秒です。他のすべての ASA/PIX デバイスの場合、最小値は 5 分です。すべての ASA/PIX デバイスのデフォルト値は 10 分です。 • [アイドル接続タイムアウト（Idle Connection Timeout）]：接続スロットが解放されるまでのアイドル時間を指定します。接続のタイムアウトを無効にするには、0:00:00 と入力します。この期間は 5 分以上にする必要があります。デフォルトは 1 時間です。
Reset Connection Upon Timeout	選択した場合、タイムアウト発生後に接続がリセットされます。ASA/PIX 7.0(4)+ だけで選択可能です。
Detect Dead Connections	デッド接続検出機能をイネーブルにします。ASA/PIX 7.2+ デバイスだけで選択可能です。このオプションを選択すると、次の 2 つのフィールドがイネーブルになります。 • [デッド接続検出タイムアウト（Dead Connection Detection Timeout）]：デッド接続が検出された場合の再試行間隔を指定します。デフォルトは 15 秒です。 • [デッド接続検出再試行数（Dead Connection Detection Retries）]：デッド接続の検出後に実行される再試行の回数を指定します。デフォルトは 5 です。
トラフィックフローアイドルタイムアウト（Traffic Flow Idle Timeout）	トラフィックフローがアイドルになってからフローが切断されるまでの期間を指定します。FWSM 3.2+ だけに適用できます。デフォルトは 1 時間です。

要素	説明
Enable TCP Normalization	TCP 正規化をイネーブルにし、TCP マップ選択オプションをアクティブにします。ASA/PIX 7.0+ だけに適用されます。ただし、TCP ステート バイパスがイネーブルになっている場合には適用されません。
TCP map	TCP 正規化に使用する TCP マップを指定します。TCP マップの名前を入力または選択します。詳細については、TCP マップの設定 （2971 ページ）を参照してください。
Randomize TCP Sequence Number	シーケンス番号のランダム化機能をイネーブルにします。別のインライン セキュリティ アプライアンスもシーケンス番号をランダム化していて、結果としてデータが混乱している場合にだけ、この機能をディセーブルにします。それぞれの TCP 接続には 2 つの初期シーケンス番号が割り当てられており、そのうちの 1 つはクライアントで生成され、もう 1 つはサーバで生成されます。セキュリティ アプライアンスは、ホスト/サーバから生成された ISN をセキュリティ レベルの高いインターフェイス上でランダム化します。攻撃者が次の ISN を予測してセッション ハイジャックを実行できないように、少なくとも 1 つの ISN をランダムに生成する必要があります。TCP ステートバイパスがイネーブルになっている場合には適用されません。
Enable TCP State Bypass	このトラフィック フローの TCP ステートバイパスをイネーブルにします。このオプションにより、接続のアウトバウンドおよびインバウンド フローが同じデバイスを通過しない場合に、非対称ルーティング環境で特定のトラフィック フローが許可されます。FWSM 3.2+ および ASA 8.2+ だけに適用できます。詳細については、TCP ステート バイパスについて （2943 ページ）を参照してください。
SCTPステートバイパスの有効化（Enable SCTP State Bypass）（ASA 9.5.2 以降のみ）	Stream Control Transmission Protocol（SCTP）プロトコル検証が不要な場合、SCTP ステートフル インスペクションをバイパスできます。
Enable Decrement TTL	このオプションを選択すると、セキュリティ アプライアンスから渡されるパケットの存続可能時間（TTL）値の減分が有効になります。PIX/ASA 7.2.2+ だけに適用できます。

要素	説明
フローオフロードの設定（Configure Flow Offload）（Firepower 9000/4000 シリーズ ASA 9.6(1) 以降）	（注） Cisco Security Manager の Service Policy ウィザードでフローオフロードを設定する前に、ASA でフローオフロードを手動で有効にしてデバイスを再起動する必要があります。フローオフロードとフローオフロードの統計情報は、シングルコンテキストモードとシステムコンテキストモードの ASA でのみサポートされます。管理コンテキストまたはユーザーコンテキストではサポートされていません。ASA ではバージョン 9.5.2(1) 以降からフローオフロードがサポートされていますが、Cisco Security Manager では ASA 9.6(1) からフローオフロードがサポートされてます。 特定のトラフィックを超高速パスにオフロードするには、このオプションを選択します。トラフィックは、ASA ではなく NIC でスイッチングおよび処理されます。オフロードによって、大容量ファイルの転送など、データ集約型アプリケーションのパフォーマンスを向上させることができます。 ヒント デバイスで TCP ステートバイパスと SCTP ステートバイパスが有効になっていない場合にのみ、フローオフロードを設定できます。
[QoS] タブ	
Enable QoS For This Traffic	このトラフィック フローの Quality of Service（QoS）オプションをイネーブルにします。選択すると、[Enable Priority For This Flow] オプションおよび [Traffic Policing] オプションがアクティブになります。 （注） このタブ上のオプションは、PIX/ASA 7.0 以降のデバイスにのみ適用できます。
Enable Priority For This Flow	このフローの厳密なスケジューリング プライオリティをイネーブルにします。[Priority Queues] ページ （2944 ページ）でプライオリティ キューを定義する必要があります。
トラフィック ポリシング	出力および入力のトラフィック ポリシングをイネーブルにします。トラフィック ポリシングにより、インターフェイス上で送受信されるトラフィックの最大レートを制御できます。

要素	説明
Output (Traffic Policing)	デバイスから出力されるトラフィックのポリシングをイネーブルにします。ポリシングをイネーブルにする場合は、次の値を指定できます。 • [認定レート（Committed Rate）]：このトラフィックフローのレート制限。8,000 ～ 2,000,000,000 の範囲の値で、許容最大速度（1 秒あたりのビット数）を指定します。 • [バーストレート（Burst Rate）]：1,000 ～ 512,000,000 の範囲の値で、適合レート値まで抑制するまでに、持続的バーストにおいて許可される最大瞬間バイト数を指定します。 • [適合アクション（Conform Action）]：レートが適合バースト値未満の場合に実行するアクション。選択肢は [Transmit] または [Drop] です。 • [超過アクション（Exceed Action）]：レートが適合レート値と適合バースト値の間である場合に、このアクションを実行します。選択肢は [Transmit] または [Drop] です。
Input (Traffic Policing)	デバイスに入力されるトラフィックのポリシングをイネーブルにします。これらのオプションは、ASA/PIX 7.2+ デバイスだけに適用されます。ポリシングをイネーブルにする場合は、次の値を指定できます。 • [認定レート（Committed Rate）]：このトラフィックフローのレート制限。8,000 ～ 2,000,000,000 の範囲の値で、許容最大速度（1 秒あたりのビット数）を指定します。 • [バーストレート（Burst Rate）]：1,000 ～ 512,000,000 の範囲の値で、適合レート値まで抑制するまでに、持続的バーストにおいて許可される最大瞬間バイト数を指定します。 • [適合アクション（Conform Action）]：レートが適合バースト値未満の場合に実行するアクション。選択肢は [Transmit] または [Drop] です。 • [超過アクション（Exceed Action）]：レートが適合レート値と適合バースト値の間である場合に、このアクションを実行します。選択肢は [Transmit] または [Drop] です。
[CSC] タブ	

要素	説明
Enable Content Security Control For This Traffic	このトラフィック フローで Cisco Content Security and Control Security Services Module（CSC SSM）の使用をイネーブルまたはディセーブルにします。このチェックボックスをオンにすると、[On CSC SSM Failure] オプションが使用可能になります。これらのオプションは、ASA 7.1+ デバイスだけに適用できます。ただし、TCP ステート バイパスがイネーブルになっている場合には適用されません。 CSC SSM では、FTP、HTTP、POP3、および SMTP のパケットをスキャンして、ウイルス、スパイウェア、スパム、およびその他の好ましくないトラフィックから保護します。
On CSC SSM Failure	CSC SSM が動作不能になった場合に実行する次のアクションを指定します。 • [開く（Open）]：CSC SSM で障害が発生した場合にトラフィックを許可します。 • [閉じる（Close）]：CSC SSM で障害が発生した場合にトラフィックをブロックします。
[User Statistics] タブ	
Enable user statistics accounting（ASA 8.4(2)+ のみ）	アイデンティティベースのファイアウォール ポリシーで、ユーザ統計情報アカウンティング情報を収集するかどうか。これらの統計情報は、ユーザー名またはユーザー グループ メンバーシップに基づいてファイアウォールポリシーが適用されるユーザーに対して保持されます。収集する情報のタイプを選択します。 • **Account for sent drop count** • **Account for sent packet, sent drop and received packet count**
[プロトコルインスペクション（Protocol Inspection）] タブ	
このトラフィックに対するScansafe Webセキュリティの有効化（Enable Scansafe Web Security for this traffic）（ASA 9.0 以降 のみ）	トラフィックフローに対する ScanSafe Web セキュリティの使用を有効または無効にします。このボックスをオンにすると、2 つのオプションが使用可能になり、それらのオプションは、ASA 9.0 以降のデバイスにのみ適用されます。 • [ScanSafeポリシーマップ（ScanSafe Policy Map）]：ポリシーマップの選択を有効にします。 • [ScanSafe Towerの通信障害時（On ScanSafe Tower Communication Failure）]：ScanSafe Tower の通信に障害が発生した場合にシステムが実行するアクションを指定します。

要素	説明
このトラフィックに対するSCTPの有効化（Enable SCTP for this traffic）（ASA 9.5.2 以降のみ）	トラフィックフローに対する SCTP の使用を有効または無効にします。 • [SCTPポリシーマップ（SCTP Policy Map）]：ポリシーマップの選択を有効にします。
このトラフィックに対するDiameterインスペクションの有効化（Enable Diameter Inspection for this traffic）（ASA 9.5.2 以降のみ）	トラフィックフローに対する Diameter インスペクションの使用を有効または無効にします。 • [Diameterポリシーマップ（Diameter Policy Map）]：ポリシーマップの選択を可能にします。 Diameter インスペクションが有効になっている場合は、[暗号化トラフィックインスペクションの有効化（Enable encrypted traffic inspection）]チェックボックスをオンにすると、暗号化トラフィックの検査を追加で有効にできます。この検査に使用する TLS プロキシを選択する必要があります。
このトラフィックに対するLISPの有効化（Enable LISP for this traffic）（ASA 9.5.2 以降のみ）	トラフィックフローに対する LISP インスペクションの使用を有効または無効にします。 • [LISPポリシーマップ（LISP Policy Map）]：ポリシーマップの選択を有効にします。
デバイスのフローLISPモビリティの有効化（Enable Flow LISP mobility for devices）（ASA 9.5.2 以降のみ）	クラスタリングのフローモビリティを有効にします。
デバイスのSTUNインスペクションサポートの有効化（Enable STUN Inspection support for devices）（ASA 9.6.2 以降のみ）	トラフィックフローに対する STUN インスペクションの使用を有効または無効にします。シングルコンテキストモードおよびマルチコンテキストモードの ASA 9.6.2 以降でサポートされています。 （注） デフォルトのインスペクション クラスで STUN インスペクションをイネーブルにすると、STUN トラフィックに関して TCP/UDP ポート 3478 が監視されます。このインスペクションは、IPv4 アドレスと TCP/UDP のみをサポートします。ピンホールの複製時、STUN インスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はユニット間で複製されません。あるユニットが STUN 要求を受信後に故障し、別のユニットがその STUN 応答を受信した場合、その STUN 応答はドロップされます。

要素	説明
このトラフィックのM3UAの有効化（Enable M3UA for this traffic）（ASA 9.6.2 以降のみ）	トラフィックフローに対する M3UA の使用を有効または無効にします。 • [M3UAポリシーマップ（M3UA Policy Map）]：ポリシーマップの選択を可能にします。
[NetFlow] タブ	
このトラフィックに対するNetFlowの有効化（Enable NetFlow for this traffic）	トラフィックフローに対する NetFlow の使用を有効または無効にします。このボックスをオンにすると、NetFlowオプションが使用可能になります。
[Collectors]	特定のイベントタイプの NetFlow イベントを送信するときに使用する必要があるコレクタを指定します。 （注） [NetFlow] ページ（[プラットフォーム（Platform）] > [ロギング（Logging）] > [NetFlow]）で設定されているコレクタのみを使用してください。 • フロー作成イベント • フロー拒否イベント • フローティアイベント • すべてのイベントタイプ （注） Cisco Security Manager では、ASA 9.6(4) から 9.7.0、および 9.8(2) 以降のデバイスに対する重複するネットフローコレクタは許可されません。重複するコレクタは必ず削除してください。

ASA デバイスでの IPS モジュールについて

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

一部の ASA デバイス モデルには、Advanced Inspection and Prevention Security Services Module（AIP-SSM）などのさまざまな IPS モジュールを取り付けることができます。サポートされている IPS モジュールは ASA モデルごとに異なります。IPS モジュールは、フル機能の予防的な侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワーク ウイルスなどの悪意のあるトラフィックがネットワークに影響を与える前にこれらを阻止します。

ASA IPS モジュールは適応型セキュリティ アプライアンスから独立して動作するため、個別のデバイスとしてデバイス インベントリに追加する必要があります。ただし、AIP SSM/SSC は ASA のトラフィック フローに統合されます。

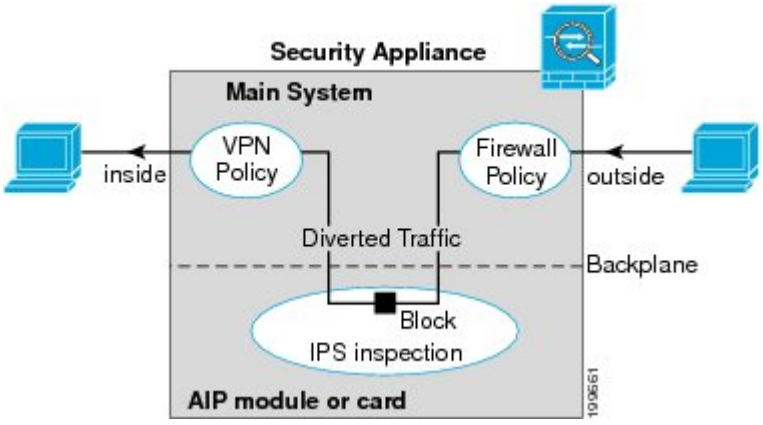
ASA IPS モジュールを設定する場合は、ホスト ASA 上にサービス ポリシールールを設定し、IPS モジュール上に IPS ポリシーを設定する必要があります。このサービス ポリシールールは、IPS モジュールで検査されるトラフィックを決定します。IPS ポリシー設定の概要については、IPS 設定の概要 （2088 ページ）を参照してください。

IPS 検査のトラフィックを識別する場合、トラフィックは次のように ASA および IPS モジュールを通過します。

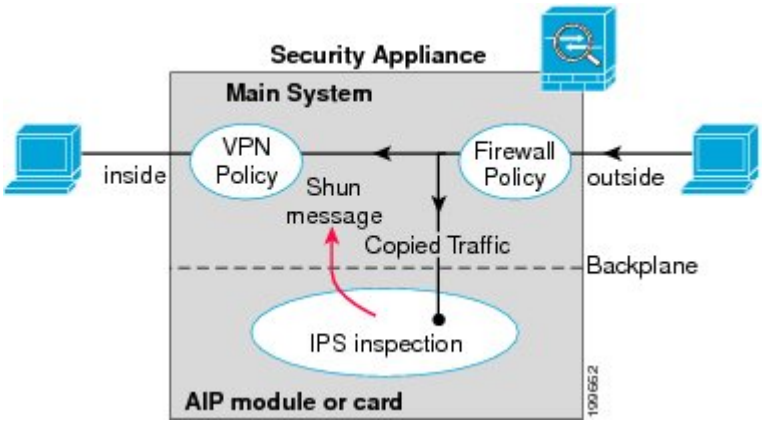
1. トラフィックが ASA に入ります。
2. インターフェイス アクセス ルールなどのファイアウォール ポリシーが適用されます。
3. インラインモードで操作する場合は、バックプレーンを介して IPS モジュールにトラフィックが送信されます。無差別モードを使用するようにシステムを設定する場合は、トラフィックのコピーが IPS モジュールに送信されます。

   インラインモードと無差別モードの詳細については、Insert/Edit Service Policy（MPC）Rule ウィザード（手順 3：MPC アクションの設定 （2950 ページ））の [侵入防御（Intrusion Prevention）] セクションで [IPS モード（IPS Mode）] を参照してください。
4. IPS モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 許可されたトラフィックがバックプレーンを介して適応型セキュリティ アプライアンスに返送されます。[Inline] モードでは、IPS モジュールはセキュリティ ポリシーに従ってトラフィックをブロックする場合があります。この場合、ブロックされたトラフィックは返送されません。
6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが ASA を出ます。

次の図に、IPS モジュールを [Inline] モードで実行する場合のトラフィック フローを示します。この例では、IPS モジュールが攻撃と見なしたトラフィックは、自動的にブロックされています。他のトラフィックはすべて ASA に戻されます。



次の図に、IPS モジュールを [Promiscuous] モードで実行する場合のトラフィック フローを示します。この例では、IPS モジュールは、脅威と見なしたトラフィックについての排除メッセージを ASA に送信します。



関連項目

- デバイス インベントリへのデバイスの追加 （94 ページ）

ASA CX について

ASA CX は、Cisco ASA-5585-X シリーズ適応型セキュリティアプライアンスにインストールできるセキュリティ サービス プロセッサ（SSP）です。トラフィックを ASA CX にリダイレクトするように親 ASA を設定すると、そのセキュリティポリシーが適用され、トラフィックがドロップされるか、さらに処理されて次の宛先にルーティングされるように ASA に戻されます。

ASA CX を追加する際に ASA で調整する必要がある 2 つの基本ポリシーとして、アクセスルールとインスペクションルールがあります。

- アクセスルールは、グローバルルールであっても、特定のインターフェイスに適用されるものであっても、トラフィックが ASA CX にリダイレクトされる前に必ず適用されます。そのため、セキュリティカードはすでに許可されているトラフィックのみを認識し、ASA

への入口でドロップされたトラフィックを処理しません。ASA CX で処理するすべてのトラフィックが許可されるように、ルールを調整することを検討してください。

- インスペクション ルールによって、トラフィックが検査されるかどうかを決定します。ASA CX は ASA で検査済みのトラフィックを検査しません。したがって、ASA CX で検査する予定のトラフィックを、自分で検査してはいけません。具体的には、HTTP トラフィックを検査しないでください。HTTP インスペクションは ASA CX の中核機能の 1 つであるためです。ASA のデフォルトのインスペクション ルールに HTTP インスペクションは含まれないため、HTTP ルールを追加した場合にのみお使いのインスペクション ルールを変更する必要があります。

インターフェイスにアクセスルールを作成する必要があるか、あるいはすべてのインターフェイスに適用するグローバルアクセスルールを作成する必要があるかを判断してください。ASA アクセスルールは、トラフィックを ASA CX にリダイレクトする前にフィルタリングするために使用します。絶対に渡さないトラフィッククラスがあるとわかっている場合は、ASA への入力時にすぐにドロップすると、より効率的です。

すでにアクセスルールを設定している場合、変更する必要はありません。ただし、アクセスルールを使用してドロップしている特定のタイプのトラフィックを ASA CX で処理するため、それらのアクセスルールを緩和することが必要かどうかを評価する必要があります。

インストールされている ASA CX へのトラフィック リダイレクションの有効化については、Insert/Edit Service Policy (MPC) Rule ウィザード （2948 ページ）の 手順 3：MPC アクションの設定 （2950 ページ）で説明されています。

関連項目

- サービス ポリシールールについて （2941 ページ）

ASA CX 認証プロキシの設定

ASA CX 認証プロキシを有効にした場合（サービスポリシー（MPC）Insert/Edit Service Policy（MPC）Rule ウィザードのステップ 3 の [CXSC] タブ。手順 3：MPC アクションの設定 （2950 ページ）を参照）：アクティブ認証にデフォルト以外のポートを使用する場合は、[CXSC認証プロキシ設定の追加/編集（Add/Edit CXSC Auth Proxy Configuration）] ダイアログボックスを使用して ASA CX 認証プロキシポート番号を変更します。

ユーザに認証クレデンシャルの入力を求める必要がある場合、プロンプト要求はこのポートを通じて行われます。

（注） Security Manager は、ASA CX セキュリティ サービス プロセッサ（SSP）を参照する場所の一部で「CXSC」を使用します。

ナビゲーション パス

[サービスポリシールール（Service Policy Rules）]ページ （2946ページ）のルールテーブルの下にある[CXSC認証プロキシ（CXSC Auth Proxy）]ボタンをクリックして、[CXSC認証プロキシ設定の追加/編集（Add/Edit CXSC Auth Proxy Configuration）]ダイアログボックスを開きます。

（注） [CXSC認証プロキシ（CXSC Auth Proxy）]ボタンには、デバイスビューの[IPS]、[QoS]、および[接続ルール（Connection Rules）]テーブルの下でのみアクセスできます。ポリシービューには表示されません。

関連項目

- [サービスポリシールール（Service Policy Rules）]ページ （2946 ページ）

フィールド リファレンス

表 *812 : [CXSC*認証プロキシ設定の追加/編集（*Add/Edit CXSC Auth Proxy Configuration*）]ダイアログボックス

要素	説明
[CXSC認証プロキシポート（CXSC Auth Proxy Port）]	デフォルトの認証プロキシの TCP ポートは 885 です。変更する場合は、1024 ～ 65535 のポート番号を入力する必要があります。

トラフィック フロー オブジェクトの設定

トラフィックの一致定義を設定するには、[Add Traffic Flow]/[Edit Traffic Flow] ダイアログボックスを使用します。これらのトラフィックフロー定義は、PIX 7.0 以降、ASA 7.0 以降、および FWSM 3.2 以降の各オペレーティングシステムが稼働するデバイスで、IPS、QoS、および接続ルールのサービスポリシーに含まれるクラスマップ（**class map** コマンド）に対応します。これらのルールの設定の詳細については、サービス ポリシールールについて （2941ページ）を参照してください。

ナビゲーション パス

[管理（Manage）]>[ポリシーオブジェクト（Policy Objects）]を選択し、次にオブジェクトタイプセレクタから[トラフィックフロー（Traffic Flows）]を選択します。作業領域内で右クリックして [New Object] を選択するか、または行を右クリックして [Edit Object] を選択します。

これらのダイアログボックスは、サービスポリシールールを定義しているときに、トラフィック フロー セレクタの [Create] または [Edit] ボタンをクリックして開くこともできます。トラフィック フロー クラスの選択の詳細については、手順 2：トラフィック クラスの設定 （2949ページ）を参照してください。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）

フィールド リファレンス

表 *813 : [Add Traffic Flow]/[Edit Traffic Flow]* ダイアログボックス

要素	説明
名前	トラフィック フロー オブジェクトの名前。最大 40 文字を使用できます。クラス マップのネーム スペースは、セキュリティ コンテキストに対してローカルです。したがって、複数のセキュリティ コンテキストで同じ名前を使用できます。セキュリティ コンテキストあたりのクラス マップの最大数は 255 です。
説明	トラフィック フローの説明（任意）。最大 1024 文字を使用できます。

要素	説明
Traffic Match Type	照合するトラフィックのタイプ。選択したオプションによって、ダイアログボックス内のフィールドが変更される場合があります。選択可能なすべてのフィールドについては、この表の後半を参照してください。[Traffic Match Type] のオプションは次のとおりです。 • [Any Traffic]：すべてのトラフィックを照合します。 • [Source and Destination IP Address (access-list)]：指定したアクセス コントロール リストに基づいて、パケットの送信元アドレスおよび宛先アドレスを照合します。 ASA 8.4(2) 以降のデバイスの場合、ACL に FQDN オブジェクトとユーザ指定を含めて、ID ベースのトラフィック照合を実行できます。 • [Default Inspection Traffic]：デフォルト インスペクション トラフィックを照合します。デフォルト設定のリストについては、デフォルト インスペクション トラフィック （2969 ページ）を参照してください。 • [Default Inspection Traffic with access list]：指定したアクセス コントロール リストで制限されたデフォルト インスペクション トラフィックを照合します。 • [TCP または UDP または SCTP 宛先ポート（TCP or UDP or SCTP Destination Port）]：トラフィックを、指定した TCP または UDP または SCTP 宛先ポートまたはポート範囲と照合します。ここで有効なポート番号は 0 ～ 65535 です。 • [RTP Range]：指定した UDP 宛先ポートの範囲に送信されるトラフィックを照合します。ここで有効なポート番号は 2000 ～ 65535 です。 • [Tunnel Group]：指定したトンネル グループに属する VPN トンネル内のフローに基づいて、宛先アドレスを照合します。 • [IP Precedence Bits]：トラフィック パケットに割り当てられた precedence 値を照合します。最大で 4 つの値を選択できます。 • [IP DiffServe Code Points (DSCP) Values]：トラフィック パケットに関連付けられた DSCP 値を照合します。最大で 8 つの値を選択できます。
可変フィールド [Add Traffic Flow]/[Edit Traffic Flow] ダイアログボックスには、[Traffic Match Type] フィールドで選択した内容に応じて次のフィールドが表示されます。次のリストに、選択可能なフィールド セットをすべて示します。	

要素	説明
Available ACLs	マップに選択可能なアクセス コントロール リスト（ACL）オブジェクトのリスト。ターゲット トラフィックを定義する ACL を選択するか、または [Create] ボタンをクリックして新しいオブジェクトを追加します。オブジェクトを選択して [Edit] をクリックし、定義を変更することもできます。オブジェクトのリストが大きい場合は、[Filter] フィールドを使用して表示を制限してください（セレクタ内の項目のフィルタリング （60 ページ））。
[TCP] または [UDP] または [SCTP] TCP/UDP/SCTP ポートまたはポート範囲（TCP/UDP/SCTP Port or Port Range）	プロトコル（TCP、UDP または SCTP）を指定するオプションボタン、および指定したプロトコル/ポートに基づいてトラフィックを照合するときに使用する、宛先ポート番号または番号の範囲を指定するテキスト フィールド。 単一のポート値またはポート番号の範囲（0-2000 など）を指定できます。有効なポート番号は 0 ～ 65535 です。
RTP Port Range	トラフィック フローに関連付けられた RTP 宛先ポートの範囲。有効な 2000 ～ 65535 の範囲内でポート範囲を入力する必要があります。 （注） ダイアログボックスを閉じると、入力したポート範囲は、終了値から開始値を引いた port-span 値に変換されます。たとえば、ダイアログボックスに範囲 2001-3000 を入力すると、[トラフィックフロー（Traffic Flows）] ポリシー オブジェクト テーブルの [照合値（Match Value）] 列に「RTPポート2001範囲999（RTP port 2001 range 999）」が表示されます。port-span 値はデバイスから要求されます。
Tunnel group name Match Flow IP Destination Address	使用可能な VPN トンネル グループが一覧表示されます。グループを選択するか、またはグループの名前を入力します。[Match Flow IP Destination Address] を選択して、宛先アドレスを一致タイプとして認識することもできます。 ヒント FlexConfig のオブジェクトおよびポリシーを使用して、PIX 7.0+ デバイスに VPN トンネル グループを定義できます。詳細については、FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。
Available IP Precedence Match on IP Precedence	IP precedence 番号。照合する値を選択し、[>>] をクリックして [一致（Match）] テーブルに追加します。複数の値を選択するには、Ctrl を押しながらクリックします。最大で 4 つの値を選択できます。 [一致（Match）] テーブルから値を削除するには、その値を選択して [<<] をクリックします。

要素	説明
Available DSCP Values Match on DSCP	IP DiffServe Code Point（DSCP）番号。照合する値を選択し、[>>] をクリックして [一致（Match）] テーブルに追加します。複数の値を選択するには、Ctrl を押しながらクリックします。最大で 8 つの値を選択できます。 [一致（Match）] テーブルから値を削除するには、その値を選択して [<<] をクリックします。
カテゴリ	トラフィック フロー オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ） を参照してください。

デフォルト インスペクション トラフィック

トラフィック フローポリシー オブジェクトを作成すると、デフォルト インスペクション トラフィックを照合できます。詳細については、トラフィック フロー オブジェクトの設定 （2965 ページ）を参照してください。次の表に、デフォルト インスペクション トラフィック カテゴリに含まれているトラフィックのタイプを示します。

表 *814*：デフォルト インスペクション トラフィック

値	[ポート（Port）]	NAT に関する制限事項	説明
CTIQBE	TCP/2748		
CuSeeMe	UDP/7648		
DNS over UDP	UDP/53	WINS 経由の名前解決では NAT は非サポート。	PTR レコードは変更されません。
FTP	TCP/21		
GTP	UDP/2123、3386		
H.323、H.225	TCP/1720、1718	同一セキュリティのインターフェイス上の NAT はサポートされません。スタティック PAT はサポートされません。	
RAS	UDP/1718、1719	同一セキュリティのインターフェイス上の NAT はサポートされません。スタティック PAT はサポートされません。	
HTTP	TCP/80		

値	[ポート（Port）]	NAT に関する制限事項	説明
ICMP	—		すべての ICMP トラフィックは、デフォルトのクラスマップで照合されます。
ILS（LDAP）	TCP/389	PAT なし。	
IP オプション	—		すべての IP オプション トラフィックは、デフォルトのクラス マップで照合されます。
MGCP	UDP/2427、2727		
NetBIOS ネームサーバ	UDP/137、138（送信元ポート）		NetBIOS は、NBNS UDP ポート 137 および NBDS UDP ポート 138 に対してパケットの NAT 処理を実行することでサポートされます。
RSH	TCP/514	PAT なし。	
RTSP	TCP/554	PAT なし。外部 NAT はサポートされません。	HTTP クローキングは処理しません。
SIP	TCP/5060、UDP/5060	外部 NAT はサポートされません。同一セキュリティのインターフェイス上の NAT はサポートされません。	
Skinny Client Control Protocol（SCCP）	TCP/2000	外部 NAT はサポートされません。同一セキュリティのインターフェイス上の NAT はサポートされません。	
SMTP および ESMTP	TCP/25		
SQL*Net	TCP/1521		バージョン 1 および 2。

値	[ポート（Port）]	NAT に関する制限事項	説明
Sun RPC over UDP	UDP/111	NAT および PAT はサポートされません。	デフォルトのルールには UDP ポート 111 が含まれています。TCP ポート 111 の Sun RPC インスペクションをイネーブルにする場合は、TCP ポート 111 を照合する新しいルールを作成し、Sun RPC インスペクションを実行する必要があります。
TFTP	UDP/69		ペイロード IP アドレスは変換されません。
XDMCP	UDP/177	NAT および PAT はサポートされません。	

TCP マップの設定

IPS、QoS、および接続ルールのサービス ポリシーで使用する TCP 正規化マップを定義するには、[Add TCP Map]/[Edit TCP Map] ダイアログボックスを使用します。TCP 正規化機能により、異常なパケットを識別する基準を指定できます。セキュリティアプライアンスは異常なパケットを検出すると、そのパケットをドロップします。このマップは、デバイスを通過する、またはデバイスに送信される TCP トラフィックに対して使用されます。

これらの TCP マップは、PIX 7.x+ デバイスおよび ASA デバイス上の TCP フローに適用できます。IPS、QoS、および接続ルールの設定の詳細については、サービス ポリシールールについて （2941 ページ）を参照してください。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] を選択し、次にオブジェクトタイプセレクタから [マップ（Maps）] > [TCPマップ（TCP Maps）] を選択します。作業領域内で右クリックして [New Object] を選択するか、または行を右クリックして [Edit Object] を選択します。

これらのダイアログボックスは、サービス ポリシールールを定義しているときに、TCP マップ セレクタの [Create] または [Edit] ボタンをクリックして開くこともできます。TCP 正規化の有効化および TCP マップの選択の詳細については、手順 3：MPC アクションの設定 （2950 ページ）の「接続の設定」セクションを参照してください。

関連項目

- マップ オブジェクトについて （388 ページ）

フィールド リファレンス

表 *815 : [Add TCP Map]/[Edit TCP Map]* ダイアログボックス

要素	説明
名前	TCP 正規化マップの名前。最大 128 文字を使用できます。
説明	マップ オブジェクトの説明。最大 1024 文字を使用できます。
キュー制限（Queue Limit） （ASA デバイス限定）	TCP 接続で、バッファに格納して順序を並べ替えることのできる out-of-order パケットの最大数。1 ～ 250 の間の値を入力します。0 を入力すると、この設定はディセーブルになり、デフォルトのシステム キュー制限が使用されます。この制限は、トラフィックのタイプによって次のように異なります。 • アプリケーション インスペクション、IPS、および TCP check-retransmission の接続のキュー制限は 3 パケットです。セキュリティ アプライアンスがウィンドウ サイズの異なる TCP パケットを受信した場合、キュー制限はアドバタイズされた設定に一致するように動的に変更されます。 • 他の TCP 接続の場合は、異常なパケットはそのまま通過します。 ただし、[Queue Limit] を 1 以上に設定した場合、すべての TCP トラフィックで許容される out-of-order パケットの数は、指定した値に一致します。アプリケーション インスペクション、IPS、および TCP check-retransmission のトラフィックの場合、アドバタイズされた設定はすべて無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。
タイムアウト（Time Out） （ASA 7.2(4)+ デバイス限定）	out-of-order パケットをバッファに格納しておくことのできる最大期間。この期間を超えると、パケットはドロップされます。1 ～ 20 秒の間の値を入力します。デフォルトは 4 秒です。 [Queue Limit] に 0 を入力した場合、この設定は無視されます。
Verify TCP Checksum	オンにすると、チェックサム検証がイネーブルになります。
Drop SYN Packets with Data	オンにすると、データを持つ TCP SYN パケットがドロップされます。
Drop Connection on Window Variation	オンにすると、ウィンドウ サイズが突然変更された接続がドロップされます。
Drop Packets that Exceed Maximum Segment Size	オンにすると、ピアに設定された Maximum Segment Size（MSS; 最大セグメント サイズ）を超えるパケットがドロップされます。

要素	説明
Check if Transmitted Data is the Same as Original	オンにすると、再送信データのチェックがイネーブルになります。
Clear Urgent Flag	オンにすると、セキュリティアプライアンスを介してURG（緊急）フラグがクリアされます。URGフラグは、ストリーム中の他のデータよりもプライオリティの高い情報がこのパケットに含まれていることを示すために使用します。TCPのRFCでは、URGフラグの厳密な解釈が定められていません。したがって、緊急オフセットの処理方法がエンドシステムによって異なり、エンドシステムが脆弱になる場合があります。
Enable TTL Evasion Protection	セキュリティアプライアンスから提供されるTTL回避保護をイネーブルにします。セキュリティポリシーを回避しようとする攻撃を防ぐ場合は、このオプションをイネーブルにしないでください。 たとえば、攻撃者はTTLを非常に短くしてポリシーを通過するパケットを送信できます。TTLが0になると、セキュリティアプライアンスとエンドポイントの間のルータは、パケットをドロップします。この時点で、攻撃者は長いTTLを設定した、悪意のあるパケットを送信できます。セキュリティアプライアンスはこのパケットを再送信と見なすため、パケットは通過します。一方、エンドポイントホストにとっては、このパケットが最初に受信するパケットになります。この場合、攻撃者はセキュリティによる攻撃の防止を受けず、攻撃に成功します。
選択的受信確認	
Clear Selective Ack	オンにすると、ウィンドウ選択的確認応答メカニズムオプションが選択解除され、パケットが許可されます。オフにすると、単一の選択的確認応答オプションを含むパケットが許可されます。
[複数の選択的確認応答を許可（Selective Ack Allow Multiple）]	複数の選択的確認応答メカニズム（SACK）を備えたパケットが許可されるかどうか。
（注） 選択的確認応答オプションが設定されていない場合、デフォルトでは、単一の選択的確認応答オプションを含むパケットは許可され、複数の選択的確認応答オプションを含むパケットはドロップされます。	
[TCPタイムスタンプ（TCP Timestamp）]	

要素	説明
Clear TCP Timestamp	オンにすると、TCP タイムスタンプオプションがクリアされ、パケットが許可されます。オフにすると、単一のTCPタイムスタンプオプションを含むパケットが許可されます。 （注） [TCPタイムスタンプのクリア（Clear TCP timestamp）] オプションを有効にすると、PAWS と RTT が無効になります。
[複数のTCPタイムスタンプを許可（TCP Timestamp Allow multiple）]	複数のTCPタイムスタンプオプションを含むパケットを許可するかどうか。
（注） TCP タイムスタンプオプションが設定されていない場合、デフォルトでは、単一の TCP タイムスタンプオプションを含むパケットは許可され、複数の TCP タイムスタンプオプションを含むパケットはドロップされます。	
ウィンドウ スケール（Window Scale）	
Clear Window Scale	オンにすると、ウィンドウ スケール タイムスタンプ オプションがクリアされ、パケットが許可されます。オフにすると、単一のウィンドウスケールオプションを含むパケットが許可されます。
[複数のウィンドウスケールを許可（Window Scale Allow Multiple）]	複数のウィンドウ スケール タイムスタンプ オプションを含むパケットを許可するかどうか。
（注） ウィンドウ スケール オプションが設定されていない場合、デフォルトでは、単一のウィンドウ スケール オプションを含むパケットは許可され、複数のウィンドウ スケール オプションを含むパケットはドロップされます。	
最大セグメント サイズ（MSS）（Maximum Segment Size (MSS)）	
[MSSのクリア（Clear MSS）]	オンにすると、MSSオプションがクリアされ、パケットが許可されます。オフにすると、単一のMSSオプションを含むパケットが許可されます。
[複数のMSSを許可（MSS Allow Multiple）]	複数の MSS オプションを含むパケットを許可するかどうか。
[最大MSS（Max. MSS）]	TCP MSS制限の値をバイト単位で入力します。有効な値は、68 ～ 65535 です。
（注） MSS オプションが設定されていない場合、デフォルトでは、単一の MSS オプションを含むパケットは許可され、複数の MSS オプションを含むパケットはドロップされます。	

要素	説明
[MD5オプションを含むパケットを許可（Allow packets with MD5 option）]	MD5 オプションを含むパケットを許可するかどうか。 [許可（Allow）]、[複数を許可（Allow Multiple）]、および [クリア（Clear）] チェックボックスは、MD5 オプションを含むパケットが許可されている場合に使用できます。 [許可（Allow）]：単一の MD5 オプションを含むパケットを許可します。 [複数を許可（Allow Multiple）]：複数の MD5 オプションを含むパケットを許可します。 [クリア（Clear）]：MD5 オプションをクリアして、パケットを許可します。
（注） MD5 オプションが設定されていない場合、デフォルトでは、単一の MD5 オプションを含むパケットは許可され、複数の MD5 オプションを含むパケットはドロップされます。	
Reserved Bits	TCP ヘッダーに予約済みビットが設定された TCP パケットの処理方法を指定します。TCP ヘッダーの 6 つの予約済みビットは今後の使用が想定されるもので、通常は値が 0 に設定されています。 • [Clear and Allow]：TCP ヘッダー内の予約済みビットをクリアし、パケットを許可します。 • [許可のみ（Allow only）]：TCP ヘッダーに予約済みビットが設定されたパケットを許可します。 • [Drop]：TCP ヘッダーに予約済みビットが設定されたパケットをドロップします。

要素	説明
[TCP Range Options] テーブル	[TCP Range Options] テーブルには、TCP マップに定義された TCP オプション範囲、およびそれらのオプションに実行するアクションが一覧表示されます。一般的な数値の範囲は 6 ～ 7、9 ～ 18 および 20 ～ 255 です。下限は上限以下とする必要があります。 • 範囲を追加するには、[Add] ボタンをクリックし、[Add TCP Option Range] ダイアログボックスを開きます（[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックス（2976 ページ）を参照）。 • 範囲を編集するには、範囲を選択し、[Edit] ボタンをクリックします。 • 範囲を削除するには、範囲を選択し、[Delete] ボタンをクリックします。 （注） ASA 9.6(2) より前のバージョンでは、TCP 値の範囲は 6 ～ 7 および 9 ～ 255 です。
カテゴリ	マップオブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用 （304 ページ）を参照してください。

[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックス

TCP 正規化マップで使用する TCP オプション範囲を定義または編集するには、[Add TCP Option Range]/[Edit TCP Option Range] ダイアログボックスを使用します。これらは、デバイスで明示的にサポートされていない TCP オプションです。この機能により、指定した TCP オプションセットを持つパケットを許可または廃棄できます。一般的な数値の範囲は 6 ～ 7、9 ～ 18、および 20 ～ 255 です。

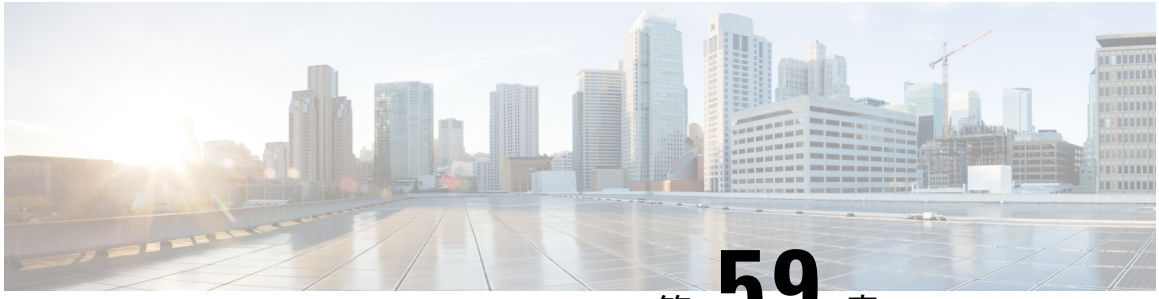
ナビゲーション パス

[Add TCP Map]/[Edit TCP Map] ダイアログボックスで、[TCP Range Options] テーブル内を右クリックして [Add Row] を選択するか、または既存の行を右クリックして [Edit Row] を選択します。 TCP マップの設定 （2971 ページ）を参照してください。

フィールド リファレンス

表 *816 : [Add TCP Option Range]/[Edit TCP Option Range]* ダイアログボックス

要素	説明
（注） ASA 9.6(2) より前では、範囲の下限と上限にそれぞれ 6 または 7、または 9 ～ 255 の整数を指定します。[下限（Lower）]の値は[上限（Upper）]の値以下とする必要があります。	
コストの	範囲の下限。6 または 7、または 9 ～ 18 の整数、または 20 ～ 255 の整数を入力します。
Upper	範囲の上限。6 または 7、または 9 ～ 18 の整数、または 20 ～ 255 の整数を入力します。
操作	指定したオプション セットを持つパケットに対して実行するアクションを選択します。 • [Allow]：指定したオプション セットを持つパケットをすべて許可します。 • [Clear]：指定したオプションが設定されたすべてのパケットからそのオプションをクリアし、パケットを許可します。 • [Drop]：指定したオプションセットを持つパケットをすべて廃棄します。



第 59 章

ファイアウォール デバイスでのセキュリティ コンテキストの設定

1 つのセキュリティ アプライアンスに対して複数のセキュリティ「コンテキスト」を定義できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立した仮想デバイスとして機能します。マルチ コンテキストとは、複数のスタンドアロン デバイスが存在するようなものです。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多数の機能がサポートされています。VPN、マルチキャスト、ダイナミック ルーティング プロトコルなど、サポートされていない機能もあります。セキュリティ コンテキストでは、スタティック ルートしかサポートしていないため、マルチ コンテキスト モードで OSPF または RIP をイネーブルにすることはできません。また、ASA デバイスおよび PIX デバイスの IPS フィーチャ セットなど、Cisco Security Manager によって直接管理されない機能もあります。

マルチ コンテキスト モードでは、セキュリティ アプライアンスに各コンテキストの設定が含まれます。この設定で、セキュリティ ポリシーやインターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションが指定されます。システム管理者は、システム設定でコンテキストを設定することにより、コンテキストを追加および管理します。これは、シングルモード設定と同様に起動設定です。システム設定には、セキュリティ アプライアンスの基本的な設定が指定されていますが、それ自身のネットワーク インターフェイスまたはネットワーク設定は含まれていません。システムがネットワーク リソースにアクセスする必要がある場合は（サーバからコンテキストをダウンロードする場合など）、管理コンテキストとして指定されたコンテキストが使用されます。システム設定は、基本的なコンテキスト設定の追加、削除、および編集に使用します（ネットワーク インターフェイスをさまざまなコンテキストに割り当てる場合など）。

管理コンテキストは他のコンテキストと似ていますが、ユーザが管理コンテキストにログインすると、そのユーザはシステム管理者権限を持ち、システム設定およびその他すべてのコンテキストにアクセスできるという点が異なります。

この章は次のトピックで構成されています。

- マルチ コンテキスト モードのイネーブル化とディセーブル化 （2980 ページ）
- マルチ セキュリティ コンテキストを設定するためのチェックリスト （2981 ページ）
- セキュリティ コンテキストの管理 （2984 ページ）

マルチコンテキストモードのイネーブル化とディセーブル化

Cisco Security Manager では、既存のデバイスでマルチ コンテキスト モードに切り替えることはサポートされていません。このタスクを実行するには、Security Manager からデバイスを削除し、デバイス マネージャまたは CLI 入力を使用してマルチコンテキスト モードをイネーブルにした後、再びデバイスを Security Manager に追加する必要があります。マルチ コンテキスト モードでデバイスを追加したあとは、セキュリティ コンテキストを追加、編集、および削除できます。

（注） マルチコンテキストデバイスを手動で定義する場合は、[新しいデバイス - デバイス情報（New Device - Device Information）] ダイアログボックスの [オペレーティングシステム（Operating System）] セクションで 、[コンテキスト（Contexts）] リストから [マルチ（Multi）] を選択します。

同様に、Cisco Security Manager では、既存のデバイスをシングルコンテキスト モードに復元することはサポートされていません。このタスクを実行するには、Security Manager からデバイスおよびその子コンテキストすべてを削除し、デバイス マネージャまたは CLI 入力を使用してシングルコンテキストの動作を復元した後、再びデバイスを Security Manager に追加する必要があります。

（注） シングルコンテキストデバイスを手動で定義する場合は、[新しいデバイス - デバイス情報（New Device - Device Information）] ダイアログボックスの [オペレーティングシステム（Operating System）] セクションで 、[コンテキスト（Contexts）] リストから [シングル（Single）] を選択します。

関連項目

- マルチ セキュリティ コンテキストを設定するためのチェックリスト （2981 ページ）
- セキュリティ コンテキストの管理 （2984 ページ）
  - [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） （2988 ページ）
  - [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）

マルチ セキュリティ コンテキストを設定するためのチェックリスト

セキュリティ コンテキストを使用すると、1つの物理デバイスを複数の独立したファイアウォールとして使用できます。各セキュリティ コンテキストは、独自の設定を持つ1つの仮想ファイアウォールを定義します。物理デバイスの場合と同様に、各セキュリティ コンテキストは適切に設定する必要があります。そうしない場合、全体的なセキュリティが低下するおそれがあります。このため、同じ物理アプライアンス上で複数のファイアウォールを定義して設定する際は、特に注意が必要です。

次のチェックリストに、複数のセキュリティ コンテキストを使用してファイアウォール デバイスを設定する際に必要な基本手順について概説します。これらの各手順の中にさらに複数の手順が含まれることがあります。すべての手順を、示されている順序どおりに実行してください。たとえば、さまざまなコンテキストを設定する前に、インターフェイスを定義する必要があります。

ステップ	タスク
ステップ 1	**物理アプライアンスで、インターフェイスとサブインターフェイス、またはVLANを定義します。** このタスクでは、FWSM でインターフェイスとサブインターフェイス、または VLAN を定義します。これらは、あとで作成するときに、さまざまなセキュリティ コンテキストに割り当てられます。物理インターフェイスのパラメータを指定します。たとえば、接続タイプ（イーサネット、ギガビットイーサネットなど）、ハードウェアポート ID、速度、デュプレックスモード、VLAN ID（サブインターフェイスを定義する場合）を指定します。 結果：すべてのインターフェイスおよびサブインターフェイスが定義されます。 詳細については、ファイアウォールデバイスのインターフェイスの設定 （2333ページ）を参照してください。

ステップ	タスク
ステップ 2	**基本セキュリティ アプライアンスを管理するための管理コンテキストを定義します。** セキュリティ アプライアンスの管理専用にコンテキストおよび IP アドレスを定義するために、このタスクは個別に呼び出されます。このプロセスは、セキュリティ コンテキストを定義するプロセスと同じです。ただし、プロセスの間は、これを管理コンテキストとして指定するために、必ず [管理コンテキスト（Admin Context）] をオンにしてください。 管理コンテキストは、アプライアンスの管理で使用される以外にも、追加の処理のために syslog および SNMP メッセージをモニタリング デバイス（Cisco Security Monitoring、Analysis and Response System（CS-MARS）など）に公開する場合にも使用されます。 特定の管理 IP アドレスを管理コンテキストに関連付けるまでは、デバイスを定義するときに指定した IP アドレスが、セキュリティ アプライアンスの管理に使用されます。管理 IP アドレスを管理コンテキストに関連付けて指定すると、この IP アドレスが [Device Properties] ページの IP アドレスよりも優先されます。 結果：管理コンテキストが定義され、物理インターフェイスに関連付けられます。 詳細については、以下を参照してください。 • [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）（2988 ページ） • [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）（2986 ページ）

ステップ	タスク
ステップ 3：	**基本アプライアンスで各セキュリティ コンテキスト（仮想ファイアウォール）を定義します。** このタスクでは、個々のセキュリティ コンテキストを定義します。それぞれに名前を付け、その設定ファイルのロケーションを割り当て、インターフェイスを割り当てます。各セキュリティ コンテキストは、仮想ファイアウォールを表します。また、その定義には、制御下にあるインターフェイスおよび関連付けられた VLAN ID の範囲が含まれます。 （注） 管理コンテキストはファイアウォール デバイスとして使用できますが、通常このように使用されるのは、シングルコンテキスト モードの場合だけです。このため、このチェックリストでは、セキュリティ コンテキストを個別のエンティティとして扱っています。 セキュリティ コンテキストを定義するときに、新しいインターフェイスを追加したり、ハードウェアのポート値を変更したりはできません。すでに定義されているインターフェイスを、コンテキストに割り当てるために選択するだけです。 結果：各セキュリティコンテキストが定義され、物理インターフェイスに関連付けられます。また、セキュリティコンテキストがトラフィックを調査する VLAN も指定されます。 詳細については、以下を参照してください。 • [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）（2988 ページ） • [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）

ステップ	タスク
ステップ 4：	**送信/展開を実行して、仮想ファイアウォールを基本アプライアンスの子として生成します。** 各コンテキストの個々の設定の定義を開始するには、セキュリティアプライアンスで必要なコンテキストを作成しておく必要があります。アプライアンスでコンテキストを作成するには、コンテキストを定義してから、Workflow モードでは変更を送信し、Workflow 以外のモードでは変更をセキュリティ アプライアンスに展開します。 セキュリティコンテキストを作成すると、デバイスビューで元のセキュリティアプライアンスの下に「仮想ファイアウォールデバイス」が表示されます。各仮想デバイスは、点線で縁取られた関連するデバイスアイコンで表されます。その名前は、基本セキュリティ アプライアンス名、アンダースコア（_）、コンテキスト名で構成されます。たとえば、仮想デバイス asaMultiRouted_admin は、「asaMultiRouted」という名前のセキュリティアプライアンスの管理コンテキスト（「admin」という名前）を表します。同様に、asaMultiRouted_security1 は、同じ基本アプライアンスのセキュリティコンテキスト「security1」を表します。 結果：変更が（Workflowモードに応じて）送信または展開されます。これにより、管理コンテキストおよびセキュリティコンテキストが基本セキュリティアプライアンスの子として作成されます。 詳細については、以下を参照してください。 • ワークフローおよびアクティビティの概要 （26 ページ） • 承認のためのアクティビティの送信（アクティビティ アプルーバを使用する Workflow モード） （202 ページ） • 展開および Configuration Archive の使用 （511 ページ）
ステップ 5	**セキュリティ コンテキストごとに追加の設定を定義します。** デバイスセレクタで仮想ファイアウォールデバイスを選択し、使用可能なポリシー（アクセスルールや変換オプションなど）を編集することにより、各セキュリティコンテキストの定義を完了できます。 結果：各セキュリティコンテキストが完全に定義され、仮想ファイアウォールとして使用できるようになります。

セキュリティ コンテキストの管理

[Security Contexts] ページに、選択したデバイスに設定されているセキュリティ コンテキストが一覧表示されます。このページから、マルチコンテキスト モードで実行されている ASA、PIX 7.0 以降、または FWSM デバイスのセキュリティ コンテキストを追加、編集、および削除できます。

ヒント FWSM デバイスからセキュリティ コンテキストを削除すると、デバイスの実行コンフィギュレーションからセキュリティ コンテキストが削除されますが、関連付けられた設定ファイルは削除されません。このため、すでに削除されたセキュリティ コンテキストと同じ名前で別のセキュリティ コンテキストをあとから追加すると、問題が発生することがあります。これは、FWSM の既知の問題であり、Security Manager の動作とは関連していません。この問題を回避するには、CLI を使用してデバイスから設定ファイルを削除します。

Security Manager を使用してコンテキストを設定するには、セキュリティ アプライアンスがマルチコンテキスト モードになっている必要があります。詳細については、マルチ コンテキスト モードのイネーブル化とディセーブル化 （2980 ページ）を参照してください。

セキュリティ コンテキストを管理するには、次の手順を実行します。

ステップ 1 デバイスビューが現在のアプリケーションビューであることを確認します。必要に応じて、ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

デバイス ビューを使用したデバイス ポリシーの設定の詳細については、デバイス ビューおよびSite-to-Site VPN Manager におけるポリシーの管理 （247 ページ）を参照してください。

ステップ 2 設定するアプライアンスを選択します。

ステップ 3 デバイスポリシーセレクタで [セキュリティコンテキスト（Security Contexts）] を選択して、[セキュリティコンテキスト（Security Contexts）] ページを表示します。

（注） マルチモード デバイスの子コンテキストは、シングル モードのファイアウォール デバイスとは別のアイコンを使用して表されます。

ステップ 4 必要に応じて、コンテキストを追加、編集、および削除します。

- 新しいコンテキストを定義するには、ページの一番下にある [行の追加（Add Row）] ボタンをクリックして、[セキュリティコンテキストの追加（Add Security Context）] ボックスを開きます。
- 既存のコンテキストを編集するには、[セキュリティコンテキスト（Security Contexts）] リストで目的のエントリを選択し、ページの一番下にある [行の編集（Edit Row）] ボタンをクリックして、[セキュリティコンテキストの編集（Edit Security Context）] ダイアログボックスを開きます。
- 既存のコンテキストを削除するには、リストから目的のエントリを選択し、[行の削除（Delete Row）] ボタンをクリックします。

（注） ここでセキュリティ コンテキストを削除すると、セキュリティ コンテキスト デバイスもデバイス インベントリから削除されます。

セキュリティ コンテキストおよび対応するセキュリティ コンテキスト デバイスを削除することを確認します。

（注） タイトルを除き、[Add Security Context] ダイアログボックスと [Edit Security Context] ダイアログボックスは同じです。PIX/ASA デバイスの場合、詳細については [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA） （2988 ページ）を参照してください。FWSM の場合、詳細については [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）を参照してください。

[AddSecurityContext]/[EditSecurityContext]ダイアログボックス（FWSM）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[Add Security Context]/[Edit Security Context] ダイアログボックスでは、現在選択されているファイアウォール サービス モジュールのコンテキストを定義および管理できます（タイトルを除き、2 つのダイアログボックスは同じです）。

少なくとも 1 つのセキュリティ コンテキストを管理コンテキストとして指定する必要があります。

注意 Security Manager は、FWSM に対してマッピングされた（つまり、「名前付き」または「エイリアス付き」の）インターフェイスをサポートしていません。名前付きインターフェイスを使用する FWSM を検出してから、関連する設定を変更した場合、再展開は失敗します。インターフェイス エイリアスを適切な VLAN ID で置き換えてください。

ナビゲーション パス

セキュリティ コンテキストの管理 （2984 ページ）で説明されているように、[Add Security Context]/[Edit Security Context] ダイアログボックスには [Security Contexts] ページからアクセスできます。

フィールド リファレンス

表 817 : [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）

要素	説明
名前	最大 32 文字のコンテキスト名を入力します。System と Null（大文字と小文字の区別なし）は予約済みであるため使用できません。 （注） コンテキスト名は、デバイス上では大文字と小文字が区別されますが、Security Manager では区別されません。つまり、Security Manager では、名前が同じで大文字と小文字が異なる 2 つのコンテキストを設定することはできません。

要素	説明
Mode（FWSM 3.1 以降）	このセキュリティ コンテキストのモード（[Router] または [Transparent]）を選択します。 （注） [Edit Security Context] ダイアログボックスでは、選択されているモードを変更できません。
管理コンテキスト	このコンテキストをこのデバイスの管理コンテキストにする場合、このチェックボックスをオンにします。 （注） デバイスの管理コンテキストの名前は、[Security Contexts] テーブルの下に表示されます。
VLAN IDs	このコンテキストに割り当てる VLAN を入力します。複数の VLAN エントリを区切るには、カンマを使用します。
Config URL	ファイルシステム プロトコルを選択し、アクセスするコンテキスト設定ファイルのパスと名前を入力して、コンテキスト設定の場所を URL タイプのアドレスとして指定します。 つまり、ドロップダウン リストからプロトコル タイプを選択し、サーバ名（リモート ファイル システムの場合）、パス、およびファイル名を関連するテキスト フィールドに入力します。たとえば、FTP の場合、組み合わせた URL は ftp://server.example.com/configs/admin.cfg の形式になります。 使用可能なプロトコルは次のとおりです。 • disk:/ • ftp:// • http:// • https:// • tftp://
フェールオーバー グループ	このコンテキストがアクティブ/アクティブ フェールオーバー設定の一部である場合は、このコンテキストが属するフェールオーバー グループを選択します。
説明	（任意）コンテキストの説明を入力します。

[Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

[セキュリティコンテキストの追加（Add Security Context）]/[セキュリティコンテキストの編集（Edit Security Context）] ダイアログボックスでは、現在選択されている PIX/ASA セキュリティアプライアンスのコンテキストを定義および管理できます（タイトルを除き、2 つのダイアログボックスは同じです）。

少なくとも 1 つのセキュリティ コンテキストを管理コンテキストとして指定する必要があります。

ナビゲーション パス

セキュリティ コンテキストの管理 （2984 ページ）で説明されているように、[Add Security Context]/[Edit Security Context] ダイアログボックスには [Security Contexts] ページからアクセスできます。

フィールド リファレンス

表 *818 : [Add Security Context]/[Edit Security Context] ダイアログボックス（PIX/ASA）*

要素	説明
名前	最大 32 文字のコンテキスト名を入力します。System と Null（大文字と小文字の区別なし）は予約済みであるため使用できません。 （注） コンテキスト名は、デバイス上では大文字と小文字が区別されますが、Security Manager では区別されません。つまり、Security Manager では、名前が同じで大文字と小文字が異なる 2 つのコンテキストを設定することはできません。
説明	（任意）コンテキストの説明を入力します。
モード（ASA 9.0+）	このセキュリティ コンテキストのモード（[Router] または [Transparent]）を選択します。 （注） [Edit Security Context] ダイアログボックスでは、選択されているモードを変更できません。

要素	説明
管理コンテキスト	このコンテキストをこのデバイスの管理コンテキストにする場合、このチェックボックスをオンにします。 （注） デバイスの管理コンテキストの名前は、[Security Contexts] テーブルの下に表示されます。 （注） このボックスをオンにすると、[IPv4アドレスプール（IPv4 Address Pool）] フィールドが無効になります。
Config URL	ファイルシステムプロトコルを選択し、アクセスするコンテキスト設定ファイルのパスと名前を入力して、コンテキスト設定の場所を URL タイプのアドレスとして指定します。 つまり、ドロップダウン リストからプロトコル タイプを選択し、サーバ名（リモート ファイル システムの場合）、パス、およびファイル名を関連するテキストフィールドに入力します。たとえば、FTP の場合、組み合わせた URL は ftp://server.example.com/configs/admin.cfg の形式になります。 使用可能なプロトコルは次のとおりです。 • disk0:/ • disk1:/ • flash:/ • ftp:// • http:// • https:// • tftp://
マルチコンテキストモードの VPN：ASA バージョン 9.6(2) デバイス用の Security Manager バージョン 4.12 以降、マルチコンテキストのリモートアクセス VPN はフラッシュの仮想化をサポートします。マルチコンテキスト構造内で、作成されたユーザコンテキストはそれぞれ、使用可能な合計フラッシュに基づき、プライベートなストレージスペースと共有ストレージの場所を設定できます。	

要素	説明
ストレージ URL：プライベート	[プライベート（Private）] チェックボックスをオンにすると、該当ユーザのみに関連付けられ、該当ユーザ対象コンテンツ固有のファイルを保存します。ドロップダウンメニューから、作成したプライベートディレクトリを選択し、設定 URL で指定したものにマップします。マルチコンテキスト ASA 9.6(2) 以降のデバイスのプライベートストレージ URL について、次のいずれかのオプションを選択します。 • disk0:/ • flash:/ ストレージ URL のデフォルト値：プライベートは **disk0:/** です。この値は変更できます。このコンテキストラベル名は、ASA 9.6(2) マルチコンテキストデバイスのファイル展開アクティビティの実行中にディレクトリとして使用されます。
ストレージ URL：共有済み	[共有済み（Shared）] チェックボックスをオンにすると、共有ストレージスペースにファイルをアップロードし、あらゆるユーザコンテキストに読み取り/書き込みアクセスできます。ドロップダウンメニューから。作成した共有ディレクトリを選択し、設定 URL で指定したものにマップします。マルチコンテキスト ASA 9.6(2) 以降のデバイスの共有ストレージ URL には、次のいずれかのオプションを選択します。 • disk0:/ • flash:/ ストレージ URL のデフォルト値：共有は **shared**。この値は変更できます。このコンテキストラベル名は、ASA 9.6(2) マルチコンテキストデバイスのファイル展開アクティビティの実行中にディレクトリとして使用されます。
ScanSafe 設定	このコンテキストで ScanSafe インスペクションを有効にするには、[ScanSafe Webセキュリティを有効にする（Enable ScanSafe Web Security）] を選択します。システム コンフィギュレーションに設定されたライセンスを上書きする場合は、[ライセンス（License）] フィールドにライセンス ID（32 桁の 16 進数でなければならない）を入力します。

要素	説明
インターフェイス	このテーブルには、このコンテキストに割り当てられているインターフェイスとサブインターフェイス、およびそれらに関連付けられた設定が一覧表示されます。これらのインターフェイスおよびサブインターフェイスについて、セキュリティ コンテキストはトラフィックを調査します。 インターフェイスおよびサブインターフェイスをこのコンテキストに追加するには、テーブルの下の [Add Row] ボタンをクリックして [Allocate Interfaces] ダイアログボックス（PIX/ASA だけ） （2991 ページ）を開きます。1 つ以上のインターフェイスを割り当てることができます。また任意で、各インターフェイスに 1 つまたは一定範囲のサブインターフェイスを割り当てることができます。 割り当てエントリを編集するには、エントリを選択し、テーブルの下の [Edit Row] ボタンをクリックして、[Edit Interface] ダイアログボックスを開きます。編集できるのは [Alias Name] と [Show hardware properties option] だけですので注意してください。インターフェイス/サブインターフェイスの割り当ては変更できません。これらのオプションの詳細については、 [Allocate Interfaces] ダイアログボックス（PIX/ASA だけ） （2991 ページ）を参照してください。 インターフェイス/サブインターフェイスの割り当てを削除するには、このテーブルから該当する行を選択し、テーブルの下の [Delete Row] ボタンをクリックします。
フェールオーバーグループ	このコンテキストがアクティブ/アクティブ フェールオーバー設定の一部である場合は、このコンテキストが属するフェールオーバー グループを選択します。

[Allocate Interfaces] ダイアログボックス（PIX/ASA だけ）

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

[Allocate Interfaces] ダイアログボックスでは、インターフェイスをコンテキストに割り当てることができます。また任意で、1 つまたは一定範囲の関連サブインターフェイスをコンテキストに割り当て、名前のエイリアス設定オプションを設定できます。

ナビゲーション パス

[Allocate Interfaces] ダイアログボックスには、[Add Security Context]/[Edit Security Context] ダイアログボックスからアクセスします。詳細については、を参照してください。

関連項目

- セキュリティ コンテキストの管理 （2984 ページ）

フィールド リファレンス

表 *819 : [Allocate Interfaces]* ダイアログボックス

要素	説明
Physical Interface	このコンテキストに割り当てる物理インターフェイスを選択します。 トランスペアレント ファイアウォール モードでは、別のコンテキストに割り当てられていないインターフェイスだけを割り当てることができます。すでに別のコンテキストに割り当てられているインターフェイスを選択した場合は、サブインターフェイスも指定する必要があります。
[Sub Interface ID From]/[Sub Interface ID To]	これらのドロップダウン リストを使用して、1 つまたは一定範囲のサブインターフェイスを指定します。どちらのリストにも、選択した物理インターフェイスに関連付けられているサブインターフェイス ID が表示されます。 1 つのサブインターフェイスを指定するには、最初のリストから目的の ID を選択します。範囲を指定するには、（使用可能な場合）2 番めのリストから最後の ID を選択します（トランスペアレント ファイアウォール モードでは、他のコンテキストに割り当てられていないサブインターフェイスだけが表示されます）。
[View Allocation] ボタン	このボタンをクリックすると、[View Interface Allocation] ダイアログボックスが開きます。このダイアログボックスに、このデバイスで定義されているすべての物理インターフェイスと、それぞれに関連付けられているセキュリティ コンテキストおよびフェールオーバー グループが読み取り専用のリストで表示されます。これを使用すると、[Allocate Interfaces] ダイアログボックスを開いたまま、現在の割り当てをすばやく確認できます。
[コンテキストでエイリアス名を使用する（Use aliased name in context）]	このインターフェイスやサブインターフェイスのエイリアス名設定をイネーブルにするには、[セキュリティコンテキストでエイリアス名を使用する（Use aliased names in the security context）] をオンにし、[エイリアス名（Alias Name）] フィールドにエイリアスを入力します。 この物理インターフェイスまたはサブインターフェイスの名前は、このコンテキストに表示されるあらゆる場所（[Interfaces Page] の [Hardware Port] カラムなど）で、この指定したエイリアスに置き換わります。
エイリアス名	目的のエイリアスを入力します。エイリアスは文字で始まり、文字または数字で終わる必要があります。また、内側には文字、数字、およびアンダースコアだけを使用できます。

要素	説明
[Suffix Range From]/[Suffix Range To]	サブインターフェイスの範囲を指定した場合、これらのフィールドが使用可能になって、エイリアス名に数字のサフィックスを指定できます。各サブインターフェイスのエイリアス名は、この範囲からのシーケンス番号に、直前のフィールドで指定した [Alias Name] を追加した名前になります。 これらの値は、デフォルトで最初のサブインターフェイス ID 番号および最後のサブインターフェイス ID 番号に設定されますが、任意の有効な数字範囲を入力できます。
Show hardware properties in context	このオプションを選択すると、エイリアスを定義した場合でも、**show interface** CLI コマンドにより、コンテキストの物理インターフェイスプロパティが表示されます。選択しない場合、show interface の出力にはエイリアス名が含まれます。

第 60 章

ユーザー設定

[ユーザー設定（User preferences）] セクションは、[展開（Deployment）] ページと [トランザクションコミット（Transactional Commit）] ページで構成されています。[展開（Deployment）] ページでは、[展開時にXLATEをクリア（Clear XLATE on deployment）] オプションにアクセスできます。[トランザクションコミット（Transactional Commit）] ページでは、アクセスルールまたは NAT ルールのトランザクション コミット モデルを有効または無効にすることができます。

- ファイアウォールデバイスでの展開設定の構成 （2995 ページ）
- ファイアウォールデバイスでのトランザクション コミットの設定の構成 （2996 ページ）

ファイアウォールデバイスでの展開設定の構成

[ユーザー設定の展開（User Preferences Deployment）] ページを使用して、特定のファイアウォールデバイスの展開オプションを指定します。使用する展開オプションでポリシーを作成し、それらの展開設定を使用して、必要なすべてのデバイスにそのポリシーを適用できます。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [ユーザー設定（User Preferences）] > [展開（Deployment）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSM プラットフォーム（PIX/ASA/FWSM Platform）] > [ユーザー設定（User Preferences）] > [展開（Deployment）] を選択します。[展開（Deployment）] を右クリックし、[新規展開ポリシー（New Deployment Policy）] を選択してポリシーを作成するか、またはポリシーセレクタから既存ポリシーを選択します。

。

[導入（Deployment）] ページが表示されます。

ステップ 2 設定がこのデバイスに展開されるときに変換テーブルをクリアする場合は、[展開時に XLATE をクリア（Clear XLATE on deployment）] をオンにします。

アクセスリストが変更される前に、**clear xlate** コマンドをファイアウォールに送信するには、このオプションをオンにします。このコマンドにより、すべてのNAT変換がクリアされます。デフォルトでは、このオプションはオフになっています。

（注） このオプションは、特定のコマンドを有効にする場合に必要です。これらのコマンドを変更する場合は、デバイスに対してこのオプションが有効になっていることを確認する必要があります。ただし、変換テーブルを消去すると、変換を使用している現在の接続がすべて切断されます。

ステップ 3 ページ下部の [**保存（Save）**]をクリックします。

ファイアウォールデバイスでのトランザクションコミットの設定の構成

デフォルトでは、ルール ベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性にはパフォーマンスにわずかなコストがかかります。パフォーマンス コストは、1秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しながら、25,000 個のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルールエンジンがルールをコンパイルするためです。デフォルトでは、新しいルールを適用できるように、接続試行を評価するときに未コンパイルのルールも検索されます。新しいルールはコンパイルされていないため、検索に時間がかかります。

ASA 9.1(5) 以降、この動作を変更して、ルールエンジンがトランザクションモデルを使用してルールの変更を展開し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクションモデルを使用すると、ルールのコンパイル中、パフォーマンスは低下しないはずです。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールと一致します。	新しいルールと照合します。 （接続数/秒が削減されます）	新しいルールと照合します。
トランザクション	古いルールと一致します。	古いルールと照合します。 （接続数/秒は影響を受けません）	新しいルールと照合します。

トランザクションモデルのメリットにはこのほか、インターフェイスでACLを置き換える際、古い ACL の削除と新しいポリシーの適用との間にギャップが生じないことがあります。これにより、動作中に許容可能な接続がドロップされる確率が減少します。

ヒント ルール タイプのトランザクション モデルをイネーブルにした場合、コンパイルの先頭と末尾をマークする syslog メッセージが存在します。これらのメッセージには、780001 以降の番号が付けられます。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [ユーザー設定（User Preferences）] > [トランザクションコミット（Transactional Commit）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから [PIX/ASA/FWSMプラットフォーム（PIX/ASA/FWSM Platform）][ユーザー設定（User Preferences）][トランザクションコミット（Transactional Commit）] を選択します。[トランザクションコミット（Transactional Commit）] を右クリックし [新しいトランザクションコミットポリシー（New Transactional Commit Policy）] を選択してポリシーを作成するか、ポリシーセレクタから既存ポリシーを選択します。

[トランザクションコミット（Transactional Commit）] ページが表示されます。

ステップ 2 目的の機能のトランザクション コミット モデルを有効にします。次のオプションがあります。

- アクセスグループ
- NAT

ステップ 3 ページ下部の [**保存（Save**）]をクリックします。

第 VI 部

ルータおよびスイッチ デバイスの設定

- ルータの管理 （3001 ページ）
- ルータインターフェイスの設定 （3005 ページ）
- ルータ デバイス管理 （3113 ページ）
- アイデンティティ ポリシーの設定 （3243 ページ）
- ロギング ポリシーの設定 （3269 ページ）
- Quality of Service の設定 （3289 ページ）
- ルーティング ポリシーの設定 （3331 ページ）
- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理 （3401 ページ）

第 61 章

ルータの管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Cisco Security Manager では、Cisco IOS アクセス セキュリティ ルータでの、セキュリティ機能およびその他のプラットフォーム固有の機能の管理および設定をサポートしています。これらの機能は、ポリシーの形式で設定します。各ポリシーでは、ルータの設定に関するさまざまな側面を定義します。Security Manager で使用するポリシーパラダイムの詳細については、ポリシーについて （209 ページ）

Cisco IOS ルータですでに定義されている設定を検出できます。この検出プロセスでは、デバイスの設定がポリシーまたはポリシー オブジェクトとして Security Manager にインポートされ、これらは必要に応じてあとで管理できます。詳細については、ルータ ポリシーの検出（3004 ページ）を参照してください。

（注） Security Manager では、Cisco IOS ソフトウェアリリース 12.3 以降がサポートされます。ただし、Cisco IOS ソフトウェア Release 12.1 または 12.2 を実行するルータに関しては、かぎられた数のポリシーだけがサポートされます。IOS ソフトウェア Release 12.1 および 12.2 を実行するルータの設定 （3003 ページ）を参照してください

いずれかのポリシー セレクタでポリシー タイプを右クリックして、単一ルータに 1 つのポリシーを割り当てたり、複数のルータ間でこのポリシーを共有したり、このポリシーの割り当てをデバイスから解除したりできます。

次の項では、Cisco IOS ルータでプラットフォーム ポリシーおよびインターフェイス ポリシーを設定する方法について説明します。

- インターフェイス ポリシー：
  - Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
  - Cisco IOS ルータでの高度なインターフェイス設定 （3021 ページ）

- [IPS Module Interface Settings] ページ （3033 ページ）
- Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）
- Cisco IOS ルータでの ADSL （3049 ページ）
- Cisco IOS ルータでの SHDSL （3057 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）
- Cisco IOS ルータでの PPP （3094 ページ）

- デバイス管理ポリシー：
  - Cisco IOS ルータにおける AAA （3114 ページ）
  - Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）
  - Cisco IOS ルータにおけるブリッジング （3135 ページ）
  - Cisco IOS ルータにおけるタイム ゾーン設定 （3141 ページ）
  - Cisco IOS ルータにおける CPU 使用率設定 （3145 ページ）
  - Cisco IOS ルータにおける HTTP と HTTPS （3149 ページ）
  - Cisco IOS ルータにおける回線アクセス （3157 ページ）
  - Cisco IOS ルータにおける任意の SSH 設定 （3194 ページ）
  - Cisco IOS ルータの SNMP （3198 ページ）
  - Cisco IOS ルータにおける DNS （3208 ページ）
  - Cisco IOS ルータにおけるホスト名とドメイン名 （3212 ページ）
  - Cisco IOS ルータにおけるメモリ設定 （3214 ページ）
  - Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）
  - [DHCP] ポリシー ページ （3230 ページ）
  - Cisco IOS ルータにおける NTP （3237 ページ）

- アイデンティティ ポリシー：
  - Cisco IOS ルータでの 802.1x （3244 ページ）
  - Cisco IOS ルータでの 802.1x （3244 ページ）
  - Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）

- ロギング ポリシー：
  - Cisco IOS ルータにおけるロギング （3269 ページ）
- Quality of Service：
  - Cisco IOS ルータにおける Quality of Service （3289 ページ）
- ルーティング ポリシー：
  - Cisco IOS ルータにおける BGP ルーティング （3331 ページ）
  - Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）
  - Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）
  - Cisco IOS ルータにおける RIP ルーティング （3384 ページ）
  - Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）

（注） [Security Manager Administration] ウィンドウの [Policy Management] ページでの設定によって、Security Manager で管理できるルータ プラットフォーム ポリシーが決まります。このウィンドウで選択していないポリシー タイプは、Security Manager の設定ページに表示されません。

- IOS ソフトウェア Release 12.1 および 12.2 を実行するルータの設定 （3003 ページ）
- ルータ ポリシーの検出 （3004 ページ）

IOS ソフトウェア Release 12.1 および 12.2 を実行するルータの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Security Manager は、Cisco IOS ソフトウェア Release 12.1 および 12.2 を実行するルータ（より多くの機能をサポートしている ASR 1000 シリーズは除く）に対して、限定的なサポートを提供します。これらのルータでは、次のポリシーを設定できます。

- アクセル ルール（レイヤ 3 だけ）。 アクセス ルールについて （913 ページ）を参照してください。
- アクセス ルール設定。 アクセス ルールについて （913 ページ）を参照してください。

- インターフェイス。Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。
- FlexConfig。FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

その他のすべてのポリシーでは、Cisco IOS ソフトウェアリリース 12.3 以降が必要です。サポートされているデバイスの詳細については、『Supported Devices and Software Versions for Cisco Security Manager』を参照してください。

ルータ ポリシーの検出

Cisco IOS ルータの設定を検出し、これらの設定をポリシーとして Security Manager にインポートできます。これにより、既存のデバイスを追加し、それらを Security Manager で管理できるようになり、各デバイスをポリシーごとに手動で設定する必要がなくなります。詳細については、デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。

Security Manager で設定できるすべての Cisco IOS コマンドを検出できます。サポートされていないコマンドは検出されません。つまり、これらのコマンドは、次に展開が行われたあともデバイスにそのまま残されています。さらに、Security Manager で検出できるコマンドの場合でも、そのコマンドに関連するサブコマンドとキーワードがすべて検出されるわけではなく、サポートされていない要素は、検出されずにデバイスにそのまま残されます。

また、Security Manager ですでに管理しているデバイスの設定をいつでも再検出できます。ただし、再検出の実行によって、Security Manager で定義したポリシーが上書きされるため、通常は推奨されていないことに注意してください。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

（注） Cisco IOS ルータでポリシーを検出したら、ポリシーに変更を加えたり、デバイスからポリシーを解除したりする前に、すぐ展開を実行することを推奨します。このようにしないと、Security Manager で設定した変更内容がデバイスに展開されない可能性があります。

（注） Security Manager で設定されていないポリシーが、最初の検出時から再検出の間にアウトオブバンド方式（CLI など）を使用してデバイス上で設定された場合は、再検出の直後に展開を実行することを推奨します。

関連項目

- ポリシーについて （209 ページ）
- ポリシーの検出 （223 ページ）
- 展開および Configuration Archive の使用 （511 ページ）

第 62 章

ルータインターフェイスの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

この章は次のトピックで構成されています。

- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- [Router Interfaces] ページ （3012 ページ）
- Cisco IOS ルータでの高度なインターフェイス設定 （3021 ページ）
- [Advanced Interface Settings] ページ （3024 ページ）
- Cisco IOS ルータでの IPS モジュール インターフェイス設定 （3032 ページ）
- [IPS Module Interface Settings] ページ （3033 ページ）
- Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）
- [CEF Interface Settings] ページ （3037 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）
- [Dialer Policy] ページ （3044 ページ）
- Cisco IOS ルータでの ADSL （3049 ページ）
- [ADSL] ポリシー ページ （3053 ページ）
- Cisco IOS ルータでの SHDSL （3057 ページ）
- [SHDSL] ポリシー ページ （3059 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）
- [PVC] ポリシー ページ （3075 ページ）
- Cisco IOS ルータでの PPP （3094 ページ）
- [PPP/MLP] ポリシー ページ （3100 ページ）

Cisco IOS ルータでの基本的なインターフェイス設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

一般に、Security Manager にインターフェイスを追加するには、ポリシーの検出 （223 ページ）の説明に従って検出を実行します。インターフェイスを検出したあと、各インターフェイスのプロパティを変更できます。

また、Security Manager を使用して、物理インターフェイスおよび仮想インターフェイスを手動で設定することもできます。これは既存のデバイスのインターフェイス設定を変更するときに便利であり、ネットワークにデバイスを物理的に追加する前にデバイスのすべてのインターフェイスを設定できるようになります。

関連項目

- 使用可能なインターフェイス タイプ （3006 ページ）
- 基本的なルータ インターフェイス設定の定義 （3009 ページ）
- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）

使用可能なインターフェイス タイプ

表 820 : ルータ インターフェイス タイプ （3006 ページ）では、Cisco IOS ルータで設定できるインターフェイスのタイプについて説明します。

表 *820 :* ルータ インターフェイス タイプ

タイプ	説明
Null	ヌル インターフェイス。
Analysis-module	Network Analysis Module（NAM; ネットワーク分析モジュール）の内部インターフェイスに接続するファスト イーサネット インターフェイス。 （注） このタイプのインターフェイスには、速度やデュプレックス モードなどのパラメータを設定できません。
Async	非同期インターフェイスとして使用されるポート回線。
ATM	ATM インターフェイス。

タイプ	説明
BRI	ISDN BRI インターフェイス。このインターフェイス設定は、各 B チャネルに伝播します。B チャネルは個別に設定できません。 （注） BRI インターフェイスでコールを発信するには、ダイヤラ インターフェイス ポリシーを設定する必要があります。詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）を参照してください。
BVI	ブリッジ グループ仮想インターフェイス。BVI インターフェイスは、レイヤ 3 でトラフィックをブリッジ グループのインターフェイスにルーティングする場合に使用します。
Content-engine	Content Engine（CE; コンテンツ エンジン）ネットワーク モジュール インターフェイス。 （注） このタイプのインターフェイスには、速度やデュプレックス モードなどのパラメータを設定できません。このタイプのインターフェイスのサブインターフェイスは作成できません。
Dialer	ダイヤラ インターフェイス。
Ethernet	イーサネット IEEE 802.3 インターフェイスです。
Fast Ethernet	100 Mbps イーサネット インターフェイスです。
FDDI	ファイバ分散データ インターフェイス。
Gigabit Ethernet	1000 Mbps イーサネット インターフェイス。
Group-Async	メイン非同期インターフェイス。このインターフェイス タイプは、1 つの非同期インターフェイスに他のインターフェイスを関連付けるためのものです。このように 1 対多の設定にすると、メインインターフェイスを設定することにより、関連付けられたすべてのメンバーインターフェイスを設定できるようになります。
HSSI	High-Speed Serial Interface（高速シリアル インターフェイス）の略。
Loopback	常時稼働しているインターフェイスをエミュレートする論理インターフェイス。たとえば、ルータにループバック インターフェイスがあると、ネイバー OSPF ルータの物理インターフェイスがダウンしても、そのルータとの隣接が失われません。 ループバック インターフェイスの名前は、0 ～ 2147483647 の数値で終了する必要があります。 （注） このインターフェイス タイプは、すべてのプラットフォームでサポートされます。作成できるループバック インターフェイスの数に制限はありません。

タイプ	説明
Multilink	マルチリンク インターフェイス。Multilink PPP（MLP; マルチリンク PPP）に使用される論理インターフェイスです。
Port channel	ポート チャネル インターフェイス。このインターフェイス タイプを使用すると、複数のポイントツーポイント ファスト イーサネット リンクを 1 つの論理リンクにバンドルできます。その結果、最大 800 Mbps の双方向の帯域幅を実現できます。
POS	Packet-over-SONET（POS）インターフェイス プロセッサ上のパケット OC-3 インターフェイス。
PRI	ISDN PRI インターフェイス。23/30 個の B チャネルと 1 個の D チャネルが含まれています。
Serial	シリアル インターフェイス。
Switch	スイッチ インターフェイス。
Ten Gigabit Ethernet	10000 Mbps イーサネット インターフェイス。
Token Ring	トークン リング インターフェイス。
Tunnel	トンネル インターフェイス。 （注） 作成できる仮想トンネル インターフェイスの数に制限はありません。有効値の範囲は 0 ～ 2147483647 です。
VG-AnyLAN	100VG-AnyLAN ポート アダプタ。
VLAN	仮想 LAN サブインターフェイス。
Virtual Template	仮想テンプレート インターフェイス。ユーザがダイヤルインすると、定義済みの設定テンプレートにより、仮想アクセス インターフェイスが設定されます。ユーザがダイヤルアウトすると、仮想アクセスインターフェイスがダウンし、他のダイヤルインに使用できるようにリソースが解放されます。

関連項目

- 基本的なルータ インターフェイス設定の定義 （3009 ページ）
- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）

基本的なルータ インターフェイス設定の定義

Cisco IOS ルータのインターフェイスまたはサブインターフェイスを定義するときは、インターフェイスに名前を付け、インターフェイスに IP アドレスを割り当てる方法を指定します。また任意で、速度、最大伝送単位（MTU）、カプセル化のタイプなど他のプロパティを定義することもできます。

（注） 基本的なインターフェイス設定は、常に設定先のデバイスにローカルなものとなります。このポリシーは他のデバイスと共有できません。ただし、高度なインターフェイス設定は共有できます。詳細については、Cisco IOS ルータでの高度なインターフェイス設定（3021 ページ）を参照してください。

関連項目

- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）

ステップ 1 デバイスビューで、ポリシーセレクタから [インターフェイス（Interfaces）] > [インターフェイス（Interfaces）] を選択します。

[Router Interfaces] ページ （3012 ページ）が表示されます。

ステップ 2 新規インターフェイスまたはサブインターフェイスを追加するには、[Add Row] ボタンをクリックして [Create Router Interface] ダイアログボックスを開きます。

既存のインターフェイスまたはサブインターフェイスを編集するには、[Interfaces] テーブルでそのインターフェイスを選択し、[Edit Row] ボタンをクリックして [Edit Router Interface] ダイアログボックスを開きます。これらのダイアログボックスのフィールドについては、[Create Router Interface] ダイアログボックス （3014 ページ）を参照してください。

ステップ 3 Security Manager でこのインターフェイスまたはサブインターフェイスをアクティブに管理するには、[有効（Enabled）] を選択します。このオプションを選択しないと、インターフェイス/サブインターフェイス定義は保持されますが、インターフェイス/サブインターフェイス自体は無効になります（または「シャットダウン」されます）。

ステップ 4 [タイプ（Type）] リストから [インターフェイス（Interface）] または [サブインターフェイス（Subinterface）] を選択します。

ステップ 5 インターフェイスを作成している場合は、インターフェイスの名前を入力します。[選択（Select）] をクリックするとダイアログボックスが開き、インターフェイスタイプ、およびインターフェイスの位置情報（カード、スロット、サブインターフェイスなど）に基づいて、標準の名前を生成できます。ダイアログボックスを使用してインターフェイス名を生成する方法については、[Interface Auto Name Generator] ダイアログボックス （3020 ページ）を参照してください。

（注） BVI インターフェイスに名前を付けるときには、カード番号としてブリッジ グループ番号を使用します。対応するブリッジ グループを設定せずに BVI インターフェイスを設定すると、展開が失敗します。

ステップ 6 サブインターフェイスを作成している場合は、次の項目を設定します。

a) [親（Parent）]：このサブインターフェイスの親インターフェイスを選択します。

b) [サブインターフェイス ID（Subinterface ID）]：サブインターフェイスを識別するための数値を入力します。

（注） Security Manager は、シリアル サブインターフェイスをマルチポイントではなくポイントツーポイントとして設定します。

ステップ 7 [レイヤタイプ（Layer Type）] を指定するには、このリストから [レベル 2（Level 2）]（データリンク）または [レベル 3（Level 3）]（ネットワーク）オプションを選択します。

ステップ 8 このインターフェイス/サブインターフェイスに **IP** アドレスを割り当てる方法を選択し、必要に応じて他にも情報を指定します。

- [スタティック IP（Static IP）]：[IP アドレス（IP Address）] および [サブネットマスク（Subnet Mask）] を指定します。
- [DHCP]：他に情報は必要ありません。
- [PPPoE]：他に情報は必要ありません。
- [アンナンバード（Unnumbered）]：IP アドレスを「借用する」インターフェイスの名前を指定します。

（注） レイヤ 2 インターフェイスでは IP アドレスはサポートされません。

ステップ 9 このほかに、インターフェイス/サブインターフェイスのプロパティをいくつか定義します。

- [ネゴシエーション（Negotiation）] チェックボックスを使用して、インターフェイスのオートネゴシエーションをイネーブルまたはディセーブルにします。

オートネゴシエーションでは、リモート デバイスの機能が検出され、2 つのデバイス間で可能な最大のパフォーマンスがネゴシエーションされます。ネゴシエーションがイネーブルであると、[Fast Ethernet Duplex] オプションおよび [Speed] オプションはディセーブルになります。

（注） オートネゴシエーションは、ASR デバイス上のファストイーサネットインターフェイスおよびギガビット イーサネット インターフェイスに対してだけ使用可能になります。

- [デュプレックス（Duplex）] リストから伝送モードを選択します。[Auto] を選択した場合は、伝送モードを自動的に検出するように、このインターフェイスの接続先となるネットワーク デバイスを設定してください（ASR では [Auto] を使用できません。代わりにオートネゴシエーションを使用してください）。

（注） デュプレックス値を定義するには、固定速度を設定する必要があります。トンネルインターフェイスおよびループバック インターフェイスは、この設定値をサポートしません。

- [速度（Speed）] リストから伝送速度を選択します。[Auto] を選択した場合は、伝送速度を自動的に検出するように、このインターフェイスの接続先となるネットワーク デバイスを設定してください（ASR では [Auto] を使用できません。代わりにオートネゴシエーションを使用してください）。

- 最大伝送単位（**MTU**）を入力して、このインターフェイスがサポートできる最大パケットサイズをバイト単位で定義します。

（注） インターフェイスプロパティには自動的に設定されるものもあれば、使用できないものもあり、インターフェイスタイプおよび基礎となるポートタイプによって決まります。たとえば、[Speed] オプションはファストイーサネットインターフェイスおよびギガビットイーサネットインターフェイスにだけ使用できます。

ステップ 10 [カプセル化（Encapsulation）] リストからカプセル化方法を選択します。

- [なし（None）]：カプセル化なし。他にパラメータは必要ありません。
- （イーサネット サブインターフェイス専用）[DOT1Q]：VLAN カプセル化。IEEE 802.1Q 標準の定義に従います。このサブインターフェイスには、次の VLAN パラメータを指定します。
  - このサブインターフェイスに関連付ける VLAN ID を入力します。

（注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。

- 802.1Q トランク インターフェイスを定義している場合は、[Native VLAN] を選択します。

ヒント VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを入力します。 FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。メイン インターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。

- （シリアルインターフェイス専用）[フレームリレー（Frame Relay）]：IETF フレームリレーのカプセル化。サブインターフェイスの Data-Link Connection Identifier（DLCI; データリンク接続識別子）を指定します。

（注） フレーム リレーは、親インターフェイスに設定する必要があります。

（注） IETF フレーム リレー カプセル化によって、Cisco IOS ルータと他のベンダーの機器との間に相互運用性が実現されます。Cisco フレーム リレー カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用します。

ステップ 11 （任意）インターフェイスの説明を最大 1024 文字で入力します。

ステップ 12 [OK] をクリックして、インターフェイス/サブインターフェイス定義を保存し、ダイアログボックスを閉じます。新規インターフェイスが [Router Interfaces] ページに表示されます。サブインターフェイスが親インターフェイスの下に表示されます。

Cisco IOS ルータ インターフェイスの削除

仮想インターフェイスの定義をいつでも削除できますが、このオプションの使用には最大限の注意を払ってください。インターフェイスがこのルータ向けのポリシー定義に含まれている場

合は、インターフェイスを削除すると、そのポリシー定義をデバイスに展開しようとしたときに失敗します。

（注） 基本的なインターフェイス定義を削除しても、**[インターフェイス（Interface）] > [設定（Settings）] > [詳細設定（Advanced Settings）]** に設定されている高度な設定は削除されません。このような高度な設定は個別に削除する必要があります。そうしないと、展開が失敗します。

（注） [Router Interfaces] ページから物理インターフェイスの定義を削除しても、そのインターフェイスはデバイスから削除されません。誤ってこの操作を実行した場合は、再検出を実行して Security Manager に定義を復元できます。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

関連項目

- 基本的なルータ インターフェイス設定の定義 （3009 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）

ステップ 1 ツールバーの [デバイスビュー（Device View）] ボタンをクリックします。

ステップ 2 デバイス セレクタからルータを選択します。

ステップ 3 ポリシーセレクタから **[インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** を選択します。[Router Interfaces] ページが表示されます。このページのフィールドの説明については、表 821 : [Router Interfaces] ページ （3013 ページ）を参照してください。

ステップ 4 テーブルからインターフェイスを選択し、[削除（Delete）] をクリックします。インターフェイスが削除されます。

[Router Interfaces] ページ

[Router Interfaces] ページは、選択した Cisco IOS ルータでインターフェイス定義（物理および仮想）を表示、作成、編集、および削除する場合に使用します。[Router Interfaces] ページには、Security Manager が検出したインターフェイスだけでなく、デバイスをシステムに追加したあとに手動で追加したインターフェイスも表示されます。

（注） [Interfaces] ポリシーは、他のルータ ポリシーと異なり、複数のデバイス間で共有できません。一方、[Advanced Settings] ポリシーは共有できます。ローカルポリシーと共有ポリシー （211 ページ）を参照してください。

詳細については、Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

ナビゲーション パス

デバイスセレクタから Cisco IOS ルータを選択し、ポリシーセレクタから **[インターフェイス（Interfaces）] > [インターフェイス（Interfaces）]** を選択します。

関連項目

- 使用可能なインターフェイス タイプ （3006 ページ）
- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 821 : [Router Interfaces] ページ

要素	説明
Interface Type	インターフェイス タイプ。サブインターフェイスが、親インターフェイスの下にインデントされて表示されます。
インターフェイス名	インターフェイスの名前。
[有効（Enabled）]	インターフェイスが現在イネーブルである（Security Manager で管理されている）のか、ディセーブルである（シャットダウン状態である）のかを示します。
IPアドレス	スタティック アドレスで定義されたインターフェイスの IP アドレス。
IP アドレス タイプ	インターフェイスに割り当てられた IP アドレスのタイプ。スタティック、DHCP、PPPoE、アンナンバードのいずれかになります（IP アドレスは、選択したインターフェイス ロールによって定義されます）。
インターフェイス ロール	選択したインターフェイスに割り当てられるインターフェイス ロール。
[追加（Add）] ボタン	[Create Router Interface] ダイアログボックス （3014 ページ）が開きます。ここから、選択したルータにインターフェイスを作成できます。
[編集（Edit）] ボタン	[Create Router Interface] ダイアログボックス （3014 ページ）が開きます。ここから、選択したインターフェイスを編集できます。

要素	説明
[削除（Delete）] ボタン	選択したインターフェイスをテーブルから削除します。インターフェイスを削除する前に、他のポリシーでそのインターフェイスが使用されていないことを確認してください。

[Create Router Interface] ダイアログボックス

[Create Router Interface] ダイアログボックスは、選択した Cisco IOS ルータで物理インターフェイスおよび仮想インターフェイスを作成または編集する場合に使用します。

ヒント　インターフェイス設定は、デバイスのタイプに固有のものです。デバイス タイプまたはインターフェイス タイプによっては、このページのオプションの多くがグレーになります。そのオプションが適用されないか、または設定できないためです。

ナビゲーション パス

[Router Interfaces] ページ （3012 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）
- Cisco IOS ルータでの高度なインターフェイス設定 （3021 ページ）

フィールド リファレンス

表 822 : [Create Router Interface] ダイアログボックス

要素	説明
有効	インターフェイスはイネーブルである（シャットダウン状態でない）かどうかを指定します。このオプションを選択しないと、インターフェイスは設定には作成されますが、シャットダウンされます。
タイプ（Type）	インターフェイスまたはサブインターフェイスを定義しているかどうかを指定します。

要素	説明
名前	インターフェイスにだけ適用されます。 インターフェイスの名前。名前を手動で入力するか、または [選択（Select）] をクリックして名前を自動的に生成するためのダイアログボックスを表示します。[Interface Auto Name Generator] ダイアログボックス （3020 ページ）を参照してください。 論理インターフェイスには、名前のあとに数値が必要です。 • ダイヤラ インターフェイスの範囲は 0 ～ 799 です。 • ループバック インターフェイスの範囲は 0 ～ 2147483647 です。 • BVI インターフェイスの範囲は 1 ～ 255 です。 • ヌル インターフェイスに唯一許可されている値は 0 です。
親	サブインターフェイスだけに適用されます。 サブインターフェイスの親インターフェイス。このリストから親インターフェイスを選択します。
Subinterface ID	サブインターフェイスだけに適用されます。 サブインターフェイスの ID 番号。

要素	説明
IP	インターフェイスに IP アドレスを割り当てる方法。 • [Static IP]：インターフェイスのスタティック IP アドレスおよびサブネットマスクを定義します。オプションの下に表示されるフィールドにこの情報を入力します。 （注） ドット付き 10 進（たとえば、255.255.255.255）または CIDR 表記（/32）を使用して、マスクを定義できます。連続および不連続ネットワークマスク（IPv4 アドレスに対応） （393 ページ）を参照してください。 • [DHCP]：インターフェイスは、DHCP サーバからダイナミックに IP アドレスを取得します。 • [PPPoE]：ルータは、（PPP/IPCP 経由で）中央のサーバから自身の登録済み IP アドレスを自動的にネゴシエートします。次のインターフェイス タイプが PPPoE をサポートしています。 • Async • シリアル • HSSI（High-Speed Serial Interface） • ダイヤラ • [BRI]、[PRI]（ISDN） • Virtual template • マルチリンク • [Unnumbered]：インターフェイスは、デバイス上の別のインターフェイスから IP アドレスを取得します。[Interface] リストからインターフェイスを選択します。このオプションは、ポイントツーポイント インターフェイスでだけ使用できます。 （注） レイヤ 2 インターフェイスでは IP アドレスはサポートされません。レイヤ 2 インターフェイスに IP アドレスを定義した場合には、展開が失敗します。

要素	説明
レイヤタイプ（Layer Type）	インターフェイスが定義されている OSI レイヤ。 • [Unknown]：レイヤは不明です。 • [Layer 2]：データ リンク層。物理層（レイヤ 1）を制御するプロトコルと、メディアに送信するデータを事前にフレーム化する方法が含まれています。レイヤ 2 は、ブリッジングおよびスイッチングに使用されます。レイヤ 2 インターフェイスには IP アドレスがありません。 • [Layer 3]：ネットワーク層。主として論理インターネットワーク パスでデータをパケット単位でルーティングします。このルーティングは、IP アドレスを使用して実現されます。
Negotiation	ASR で使用可能で、ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスにだけ適用されます。 オートネゴシエーションでは、リモート デバイスの機能が検出され、2 つのデバイス間で可能な最大のパフォーマンスがネゴシエーションされます。ネゴシエーションがイネーブルであると、[Duplex] オプションおよび [Speed] オプションはディセーブルになります。
デュプレックス	インターフェイス伝送モード。 • [None]：伝送モードが、デバイス固有のデフォルト設定に戻ります。 • [Full]：インターフェイスは同時に送受信します（全二重）。 • [Half]：インターフェイスは送信または受信できますが、送受信を同時に行うことはできません（半二重）。これがデフォルトです。 • [Auto]：ルータは、適切な伝送モード（全二重または半二重）を自動的に検出して設定します。ASR では使用できません。代わりにオートネゴシエーションを使用してください。 （注） [Auto] モードを使用している場合は、このインターフェイスの接続先となるアクティブなネットワーク デバイス上のポートも、伝送モードを自動的にネゴシエートするように設定されていることを確認してください。それ以外の場合は、適切な固定モードを選択します。 （注） デュプレックス値を設定できるのは、[Speed] を [Auto] ではなく固定速度に設定する場合だけです。 （注） この設定値は、シリアル、HSSI、ATM、PRI、DSL、トンネル、ループバックの各インターフェイスには適用されません。

要素	説明
速度	ファスト イーサネット インターフェイスおよびギガビット イーサネット インターフェイスにだけ適用されます。 インターフェイスの速度。 • [None]：設定はデバイスに設定できません。 • [10]：10 メガビット/秒（10Base-T ネットワーク）。 • [100]：100 メガビット/秒（100Base-T ネットワーク）。これは、ファスト イーサネット インターフェイスのデフォルトです。 • [1000]：1000 メガビット/秒（ギガビット イーサネット ネットワーク）。これは、ギガビット イーサネット インターフェイスのデフォルトです。 • [Auto]：ルータは適切なインターフェイス速度を自動的に検出して設定します。ASR では使用できません。オートネゴシエーションを使用してください。 （注） [Auto] モードを使用している場合は、このインターフェイスの接続先となるアクティブなネットワーク デバイス上のポートも、伝送速度を自動的にネゴシエートするように設定されていることを確認してください。それ以外の場合は、適切な固定速度を選択します。
[MTU]	最大伝送単位。このインターフェイスが処理できる最大パケット サイズ（バイト単位）です。 シリアル、イーサネット、ファスト イーサネットの各インターフェイスの有効値の範囲は、64 ～ 17940 バイトです。 ギガビット イーサネット インターフェイスの有効値の範囲は、1500 ～ 9216 バイトです。
カプセル化	インターフェイスによって実行されたカプセル化のタイプ。 • [None]：カプセル化なし。 • [DOT1Q]：VLAN カプセル化。IEEE 802.1Q 標準の定義に従います。イーサネット サブインターフェイスだけに適用されます。 • [Frame Relay]：IETF フレーム リレーのカプセル化。（シリアル サブインターフェイスではなく）シリアル インターフェイスにだけ適用されます。 （注） IETF フレーム リレー カプセル化によって、Cisco IOS ルータと他のベンダーの機器との間に相互運用性が実現されます。Cisco フレーム リレー カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用します。

要素	説明
VLAN ID（Admin. VLAN ID）	カプセル化のタイプが DOT1Q であるサブインターフェイスにだけ適用されます。 このサブインターフェイスに関連付けられた VLAN ID。VLAN ID は、このサブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。有効値の範囲は 1 ～ 4094 です。 （注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。メイン インターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。
ネイティブ VLAN	カプセル化のタイプが DOT1Q で、802.1Q トランク インターフェイスとして機能する物理インターフェイスを設定しているときにだけ適用します。トランキングは、2 つのデバイスをつなぐポイントツーポイント リンクに複数の VLAN を定義してトラフィックを伝送する方法です。 選択されている場合、[VLAN ID] フィールドで指定された ID を使用して、このインターフェイスにネイティブ VLAN が関連付けられます（ネイティブ VLAN に VLAN ID が指定されていない場合、デフォルト値は 1 です）。ネイティブ VLAN は、タグ付けされていないすべての VLAN パケットがデフォルトで論理的に割り当てられる VLAN です。これには、VLAN に関連付けられた管理トラフィックが含まれます。VLAN ID が定義されていない場合、デフォルトは 1 です。 たとえば、このインターフェイスの VLAN ID が 1 である場合、すべての着信非タグ付きパケットと VLAN ID が 1 であるパケットが、サブインターフェイスではなくメイン インターフェイスで受信されます。メインインターフェイスから送信されるパケットは、802.1Q タグが付与されずに送信されます。 オフにすると、ネイティブ VLAN はこのインターフェイスに関連付けられません。 （注） トランク インターフェイスのサブインターフェイスには、ネイティブ VLAN を設定できません。リンクの両端には必ず同じ [Native VLAN] 値を設定してください。同じ値を設定しないと、トラフィックが失われたり、間違った VLAN に送信される場合があります。

要素	説明
DLCI	フレーム リレーがカプセル化されるシリアル サブインターフェイスにだけ適用されます。 サブインターフェイスに関連付けるデータリンク接続識別子を入力します。有効値の範囲は 16 ～ 1007 です。 （注） Security Manager は、シリアル サブインターフェイスをマルチポイントではなくポイントツーポイントとして設定します。
説明	インターフェイスに関する追加の情報（最大 1024 文字）。
ロール（Roles）	このインターフェイスに割り当てられたインターフェイス ロール。ロールがまだ割り当てられていない場合は、メッセージが表示されます。

[Interface Auto Name Generator] ダイアログボックス

[Interface Auto Name Generator] ダイアログボックスは、インターフェイスのタイプとルータやスイッチでのインターフェイスの場所に基づいて、Security Manager でインターフェイスの名前を生成する場合に使用します。

ナビゲーション パス

[Create Router Interface] ダイアログボックス （3014 ページ）に移動し、[タイプ（Type）] リストから [インターフェイス（Interface）] を選択し、[名前（Name）] フィールドで [選択（Select）] をクリックします。

フィールド リファレンス

表 *823 : [Interface Auto Name Generator]* ダイアログボックス

要素	説明
タイプ	インターフェイスのタイプ。このリストで選択した内容が、生成した名前の先頭部分となり、[Result] フィールドに表示されます。詳細については、使用可能なインターフェイス タイプ （3006 ページ）を参照してください。
カード	インターフェイスに関連するカード。 （注） BVI インターフェイスを定義している場合は、対応するブリッジ グループの番号を入力します。
スロット	インターフェイスに関連するスロット。
[ポート（Port）]	インターフェイスに関連するポート。 （注） これらのフィールドに入力した情報によって、[Result] フィールドに表示される、生成される名前の残りの部分が形成されます。

要素	説明
結果	入力したインターフェイス タイプおよび場所の情報を基に Security Manager が生成した名前。このフィールドに表示される名前は読み取り専用です。 **ヒント** このダイアログボックスを閉じたあと、必要に応じて [Create Router Interface] ダイアログボックスで生成した名前を編集できます。

Cisco IOS ルータでの高度なインターフェイス設定

Security Manager では、[Interfaces] ページに定義できる基本的なインターフェイス定義に加えて、高度な設定も、インターフェイスでサポートされていれば定義できます。

[Interfaces] ページに定義されている基本的なインターフェイス設定と異なり、[Advanced Settings] ポリシーは複数のデバイスで共有できます。これにより、同じ設定の複数のデバイスを簡単に設定できます。 デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用（256 ページ）を参照してください。

選択したインターフェイス、サブインターフェイス、またはインターフェイス ロールに関して、次に挙げるように、さまざまな高度な設定を定義できます。

- Cisco Discovery Protocol（CDP）設定。
- インターネット制御メッセージ プロトコル（ICMP）設定。
- ダイレクト ブロードキャスト設定。
- 平均負荷を求めるための負荷間隔。
- ルーティング プロトコルに使用するスループット遅延。
- TCP 最大セグメント サイズの設定。
- UDP ブロードキャストを転送するためのヘルパー アドレス。ヘルパー アドレスを入力する方法の詳細については、ヘルパー アドレスについて （3022 ページ）を参照してください。
- Maintenance Operation Protocol（MOP; メンテナンス オペレーション プロトコル）のイネーブル化。
- Virtual Fragmentation Reassembly（VFR; 仮想フラグメンテーション再構成）のイネーブル化。
- プロキシ ARP のイネーブル化。
- NBAR プロトコル検出のイネーブル化。
- Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）のイネーブル化および設定。

ヒント　特定のインターフェイスではなくインターフェイス ロールを選択すると、デバイス上の複数のインターフェイスに対してこれらの設定を一度にまとめて定義できます。たとえば、All-Ethernets インターフェイス ロールを定義した場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じ高度な設定を定義できます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

はじめる前に

- 基本的なインターフェイス設定を定義します。Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [詳細設定（Advanced Settings）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [詳細設定（Advanced Settings）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Advanced Interface Settings] ページが表示されます（[Advanced Interface Settings] ダイアログボックス （3025 ページ）を参照）。

ステップ 2　次のいずれかを実行します。

- [追加（Add）] ボタンをクリックして、インターフェイスまたはインターフェイスロールをテーブルに追加します。[詳細インターフェイス設定（Advanced Interface Settings）] ダイアログボックスで、インターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックして既存のロールを選択するか、または新しいロールを作成します。
- テーブル内の既存エントリを選択し、[編集（Edit）] ボタンをクリックしてそのエントリの設定を変更します。

ステップ 3　選択したインターフェイスに必要な高度な設定を設定します。各設定の詳細については、[Advanced Interface Settings] ダイアログボックス （3025 ページ）を参照してください。

ステップ 4　[OK] をクリックして定義を保存します。定義が、[Advanced Interface Settings] テーブルに表示されます。

ヘルパー アドレスについて

ネットワーク ホストが、ユーザ データグラム プロトコル（UDP）ブロードキャストを使用して、アドレス、設定、名前の情報を確認することがあります。これは、そのホストが存在するネットワーク セグメントに必要なサーバが配置されていない場合には問題となります。ルータは、デフォルトでは自身が属しているサブネットを越えて UDP ブロードキャストを転送しな

いためです。特定のクラスのブロードキャストをヘルパーアドレスに転送するようにインターフェイスを設定すると、この状況を改善できます。

ヘルパー アドレスがよく使用されるのは、ルータが DHCP クライアントのリレー エージェントとして機能しており、そのクライアントが別のサブネットにある DHCP サーバに問い合わせる必要がある場合です。ヘルパー アドレスは、特定の DHCP サーバであるか、または複数の DHCP サーバが含まれているセグメントのネットワーク アドレスとなります。また、DHCP サーバごとにヘルパー アドレスを設定することもできます。

図 46 : Helper Addresses （3023 ページ）では、ネットワーク 192.168.1.0 にあるホストは、10.44.23.7 をヘルパー アドレスとして使用して、UDP ブロードキャストを他のネットワークに転送できます。一方、ネットワーク 10.44.0.0 にあるホストは、192.168.1.19 をヘルパー アドレスとして使用できます。

図 *46 : Helper Addresses*

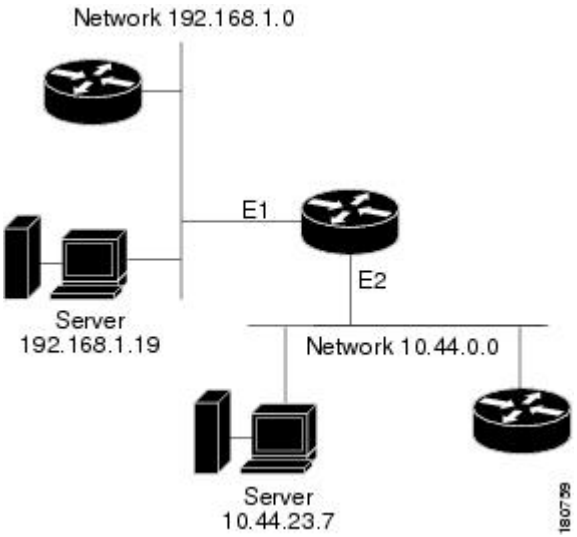


表 824 : ヘルパー アドレスに転送されるデフォルトの UDP サービス （3023 ページ）に、ヘルパー アドレスに転送できるデフォルトの UDP サービスを示します。

表 *824 :* ヘルパー アドレスに転送されるデフォルトの *UDP* サービス

Service	ポート
BOOTP/DHCP クライアント	68
BOOTP/DHCP サーバ	67
DNS	53
NetBIOS データグラム サービス	138
NetBIOS ネーム サービス	137

Service	ポート
TACACS	49
TFTP	69
Time	37

ヒント　他の UDP サービスを転送するには、CLI または FlexConfig を使用して、ip forward-protocol コマンドを設定します。表 824 : ヘルパー アドレスに転送されるデフォルトの UDP サービス （3023 ページ）に記載されているデフォルト サービスのいずれも転送できないようにするには、このコマンドの no 形式を使用します。

UDP パケットまたは IP パケットがヘルパー アドレスを使用するためには、次に挙げるすべての条件を満たす必要があります。

- 受信したフレームの MAC アドレスは、すべてが 1 のブロードキャスト アドレス（ffff.ffff.ffff）である必要があります。
- IP の宛先アドレスは、すべてが 1 のブロードキャスト（255.255.255.255）または受信インターフェイスのサブネット ブロードキャストであるか、あるいは no ip classless コマンドも設定されている場合には受信インターフェイスのメジャーネットブロードキャストである必要があります。
- IP の存続可能時間（TTL）値は 2 以上である必要があります。
- IP プロトコルは UDP（17）である必要があります。

関連項目

- [Advanced Interface Settings] ページ （3024 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）

[Advanced Interface Settings] ページ

[Advanced Interface Settings] ページは、ルータに高度なインターフェイス定義（物理および仮想）を設定する場合に使用します。高度な設定の例としては、Cisco Discovery Protocol（CDP）設定、ICMP メッセージ設定、仮想フラグメント再構成設定などがあります。特定のインターフェイスまたはインターフェイス ロールの設定値を設定できます。テーブルの各カラムはエントリの高度な設定の概要であり、それぞれの説明については [Advanced Interface Settings] ダイアログボックス （3025 ページ）を参照してください。

高度な設定を設定するには、次の手順を実行します。

- [追加（Add）] ボタンをクリックして、インターフェイスまたはインターフェイスロールをテーブルに追加し、[高度なインターフェイスの設定（Advanced Interface Settings）] ダイアログボックスに入力します。
- エントリを選択し、[編集（Edit）] ボタンをクリックして、既存のエントリを編集します。
- エントリを選択し、[削除（Delete）] ボタンをクリックして削除します。

詳細については、Cisco IOS ルータでの高度なインターフェイス設定 （3021 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [Advanced Settings] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [詳細設定（Advanced Settings）] を選択します。[高度な設定（Advanced Settings）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Router Interfaces] ページ （3012 ページ）
- 使用可能なインターフェイス タイプ （3006 ページ）
- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

[Advanced Interface Settings] ダイアログボックス

[Advanced Interface Settings] ダイアログボックスは、次の表の説明に従って、選択したインターフェイスのさまざまな高度な設定を定義する場合に使用します。

ナビゲーション パス

[Advanced Interface Settings] ページ （3024 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- Cisco IOS ルータでの高度なインターフェイス設定 （3021 ページ）
- Cisco IOS ルータ インターフェイスの削除 （3011 ページ）

- 使用可能なインターフェイス タイプ （3006 ページ）

フィールド リファレンス

表 *825 : [Advanced Interface Settings]* ダイアログボックス

要素	説明
インターフェイス（Interface）	高度な設定を定義するインターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。目的の項目が表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） レイヤ 2 インターフェイスでサポートされている高度な設定は、[Max Bandwidth]、[Load Interval]、および [CDP] だけです。
最大帯域幅（Max Bandwidth）	上位のプロトコルとキロビット/秒（kbps）で通信するための帯域幅値。このフィールドに定義する値は情報パラメータにすぎず、物理インターフェイスには影響を与えません。
Load Interval	インターフェイスでの平均負荷の計算に使用される時間の長さ（秒単位）。有効値の範囲は 30 ～ 600 秒（30 秒の倍数単位）です。デフォルトは 300 秒（5 分）です。負荷間隔は、サブインターフェイスではサポートされません。 平均負荷の計算に使用する時間を短くするには、デフォルト値を変更します。時間を短くすると、負荷計算に短いトラフィック バーストが強く反映されるようになります。 負荷データは 5 秒おきに収集されます。このデータは、秒あたりのビット数およびパケット数単位で表される入出力速度、負荷、信頼性など、負荷統計を算出するために使用されます。負荷データは加重平均計算を使用して算出され、新しい負荷データの方が古い負荷データよりも加重が大きくなります。 ヒント このオプションを使用すると、バックアップインターフェイスをアクティブにする可能性を増減できます。たとえば、アクティブインターフェイスで負荷が突然急増して、バックアップ ダイヤル インターフェイスがトリガーされる場合があります。

要素	説明
TCP 最大セグメント サイズ（TCP Maximum Segment Size）	このインターフェイスを通過する TCP SYN パケットの Maximum Segment Size（MSS; 最大セグメント サイズ）。有効値の範囲は 500 ～ 1460 バイトです。値を指定しない場合、MSS は発信元ホストによって設定されます。 このオプションは、TCP セッションがルータを通過する際にドロップされるのを防ぐのに役立ちます。このオプションは、TCP フレーム サイズのオートネゴシエーションを実行する ICMP メッセージが（ファイアウォールなどによって）ブロックされるときに使用します。DMVPN ネットワークのトンネル インターフェイスには、このオプションを使用することを強く推奨します。 （注） 一般に、最適な MSS は 1452 バイトです。この値に、20 バイトの IP ヘッダー、20 バイトの TCP ヘッダー、および 8 バイトの PPPoE ヘッダーが追加されて、イーサネット リンクの MTU サイズと同じ 1500 バイトのパケットになります。
Helper Addresses	このインターフェイスで受信されるユーザ データグラム プロトコル（UDP）ブロードキャストを転送するために使用されるヘルパー アドレス。ネットワーク/ホスト オブジェクトのアドレスまたは名前を 1 つ以上入力します。あるいは、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新規オブジェクトを作成します。 ルータは、デフォルトでは自身のサブネットの外部にブロードキャストを転送しません。ヘルパー アドレスを使用すると、ルータは特定のタイプの UDP ブロードキャストをユニキャストとして宛先サブネット上のアドレスに転送できるようになります。詳細については、ヘルパー アドレスについて （3022 ページ）を参照してください。
Interface Throughput Delay	インターフェイスで想定される遅延（数十マイクロ秒単位。たとえば、3000 は 30,000 マイクロ秒になります）。1 ～ 16777215 の値を入力でき、デフォルトはインターフェイスのタイプによって異なります。 上位のプロトコルが、遅延情報を使用して動作を決定することがあります。たとえば、IGRP では遅延情報を使用して衛星のリンクと地上のリンクを区別できます。この設定値は情報を提供するだけのものであり、インターフェイスの実際の遅延には影響を与えません。

要素	説明
Cisco Discovery Protocol settings	Cisco Discovery Protocol（CDP）に関連する設定。CDP は、メディアおよびプロトコルに依存しないデバイス検出プロトコルであり、すべてのシスコ製装置（ルータ、アクセス サーバ、ブリッジ、スイッチなど）上で動作します。主としてネイバーデバイスのプロトコルのアドレスを取得し、そのデバイスのプラットフォームを検出するのに使用されます。次のオプションがあります。 • [Enable CDP]：このインターフェイスで Cisco Discovery Protocol（CDP）をイネーブルにするかどうかを指定します。ATM インターフェイスでは CDP をイネーブルにできません。 • [Log CDP Messages]：イーサネット インターフェイスで、このインターフェイスのデュプレックスの不一致をログに記録するかどうかを指定します。
ICMP メッセージ設定	
Enable Redirect Messages	デバイスが受信時と同じインターフェイス経由でパケットを同じサブネット上の他のデバイスに再送信するようになっている場合には、インターネット制御メッセージ プロトコル（ICMP）リダイレクト メッセージの送信をイネーブルにするかどうかを指定します。リダイレクトメッセージは、デバイスがパケットの発信者に対して、宛先へのルートからそのデバイスを削除し、宛先までより直接的に到達できるパスを提供する別のデバイスに置き換えるように指示する場合に送信されます。
Enable Unreachable Messages	ICMP 到達不能メッセージの送信をイネーブルにするかどうかを指定します。到達不能メッセージは、次の 2 つの状況で送信されます。 • インターフェイスは、不明なプロトコルを使用する自身宛の非ブロードキャストパケットを受信した場合、ICMP 到達不能メッセージを送信元に送信します。 • デバイスは、最終宛先宛のパケットを受信したものの、その宛先アドレスへのルートがないためにパケットを配信できない場合、ICMP ホスト到達不能メッセージをパケットの発信者に送信します。 （注） これは、null0 インターフェイスでサポートされている唯一の高度な設定です。
Enable Mask Reply Messages	ICMP マスク応答メッセージの送信をイネーブルにするかどうかを指定します。マスク応答メッセージは、マスク要求メッセージに応えて送信されます。マスク要求メッセージは、デバイスが特定のサブネットワークのサブネット マスクを知る必要があるときに送信されます。
追加設定（Additional Settings）	
Enable Maintenance Operation Protocol (MOP)	インターフェイスで MOP をイネーブルにするかどうかを指定します。システム ソフトウェアのアップグレードとダウンロード、リモート テスト、問題診断など、ユーティリティ サービスの MOP を使用できます。

要素	説明
Enable Virtual Fragment Reassembly (VFR)	このインターフェイスで Virtual Fragmentation Reassembly（VFR; 仮想フラグメンテーション再構成）をイネーブルにするかどうかを指定します。VFR は、Cisco IOS ファイアウォールがダイナミック ACL を作成してさまざまなフラグメンテーション攻撃からネットワークを保護できるようにする機能です。
Enable Proxy ARP	インターフェイスでプロキシアドレス解決プロトコル（ARP）をイネーブルにするかどうかを指定します。RFC 1027 に規定されているプロキシ ARP は、あるホスト（通常はルータ）が他のマシン向けの ARP 要求に応答して、パケットを実際の宛先にルーティングするという手法です。プロキシ ARP を使用すると、ルーティングやデフォルト ゲートウェイを設定しなくても、サブネット上のマシンがリモートのサブネットに容易に到達できるようになります。
Enable NBAR Protocol Discovery	このインターフェイスで Network-Based Application Recognition（NBAR）をイネーブルにして、トラフィックを検出し、すべてのプロトコルのトラフィック統計情報が NBAR に認識されるようにするかどうかを指定します。プロトコル検出により、インターフェイスを通過するアプリケーション プロトコルを検出し、QoS ポリシーを策定してプロトコルに適用できます。詳細については、次の URL にアクセスしてください。 http://www.cisco.com/en/US/products/ps6616/products_qanda_item09186a00800a3ded.shtml

要素	説明
Enable Directed Broadcasts ACL	このインターフェイスが宛先サブネットに直接接続されているときに、ダイレクトブロードキャストパケットがリンクレイヤブロードキャストとして「展開」されるかどうかを指定します。選択解除されている場合、このインターフェイスが直接接続されているサブネット宛のダイレクトブロードキャストパケットはブロードキャストされず、ドロップされます。これがデフォルトです。 IP ダイレクト ブロードキャストは、宛先アドレスが発信元のノードとは別のサブネットで有効なブロードキャスト アドレスとなっている IP パケットです。このような場合、パケットは宛先サブネットに達するまでユニキャスト パケットであるかのように転送されます。 このオプションは、宛先サブネットでのダイレクトブロードキャストの最終伝送にだけ影響を与えます。IP ダイレクトブロードキャストの送信ユニキャスト ルーティングには影響を与えません。 ダイレクトブロードキャストをイネーブルにした場合は、宛先サブネットでどのダイレクト ブロードキャストをブロードキャストできるかを ACL に基づいて決定できます。このインターフェイスが直接接続されているサブネット宛のそれ以外のダイレクト ブロードキャストはドロップされます。標準または拡張 ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** ダイレクト ブロードキャストと特に ICMP ダイレクト ブロードキャストはこれまで悪意のある個人によって悪用されたことがあるため、ダイレクトブロードキャストが必要ないインターフェイスではこのオプションを選択しないことを推奨します。ダイレクトブロードキャストをイネーブルにするときは、その使用を制限する ACL を適用してください。
Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）設定	
Enable Unicast RPF	インターフェイスで Unicast Reverse Path Forwarding（uRPF; ユニキャスト リバース パス転送）をイネーブルにするかどうかを指定します。インターフェイスでユニキャスト RPF をイネーブルにすると、ルータはそのインターフェイスで受信されるすべてのパケットを検査します。ルータは、送信元アドレスが FIB にあることを確認し、ユニキャスト RPF 設定に基づいて必要な対策を講じます。ユニキャスト RPF を使用すると、不正な形式の IP 送信元アドレスまたは偽装（スプーフィング）された IP 送信元アドレスがルータを通過したために発生する問題を軽減できます。不正な形式の送信元アドレスまたは偽装された送信元アドレスは、送信元 IP アドレスのスプーフィングに基づく DoS 攻撃である場合があります。ユニキャスト RPF の詳細については、『*Cisco IOS Interface and Hardware Component Command Reference*』で **ip verify unicast source reachable-via** コマンドの説明を参照してください。 ユニキャスト RPF をイネーブルにするには、Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）もグローバルにイネーブルにする必要があります。CEF の詳細については、Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）を参照してください。

要素	説明
[モード（Mode）]	ユニキャスト RPF の厳格さを示します。 • loose モード：デフォルト。着信パケットを調べて送信元アドレスが Forwarding Information Base（FIB; 転送情報ベース）にあるかどうかを判断し、ルータ上のいずれかのインターフェイスを経由して送信元に到達可能である場合にはパケットを許可します。 loose モードは、非対称パスが有効な送信元ネットワーク（FIB に含まれるネットワーク）からのパケットを許可するインターフェイスで使用します。たとえば、ISP ネットワークのコアに存在するルータでは、ルータから転送されるパケットに最適なパスが、ルータに戻ってくるパケットに対しても選択されるとはかぎりません。 • strict モード：着信パケットを調べて送信元アドレスが FIB にあるかどうかを判断し、パケットを受信したインターフェイスを経由して送信元に到達可能である場合にだけパケットを許可します。 strict モードは、1 つのパスだけが有効な送信元ネットワーク（FIB に含まれるネットワーク）からのパケットを許可するインターフェイスで使用します。このほか、有効なネットワークが着信インターフェイスで切り替えられる場合にかぎり、ルータに特定のネットワークへのパスが複数あるときにも strict モードを使用します。無効なネットワークのパケットはドロップされます。たとえば、ISP ネットワークのエッジにあるルータには、対称リバース パスが設定されている可能性があります。strict モードは、マルチホームにも適用できる場合があります。ただし、加重やローカル プリファレンスなど任意のボーダー ゲートウェイ プロトコル（BGP）属性を使用して対称ルーティングを実現する場合にかぎられます。
Allow Use Of Default Route for RPF Verification	パケットを通過させるかどうかを判断するときに、ユニキャスト RPF がデフォルト ルート経由で確認したプレフィックスに対して照合を正しく実行できるようにするかどうかを指定します。通常、FIB に存在する送信元であっても、デフォルト ルートを経由するだけであればドロップされます。
Allow Self Ping	ルータが自身のインターフェイスに対して ping を実行できるかどうかを指定します。デフォルトでは、ユニキャスト RPF をイネーブルにすると、ルータによって生成され、かつルータを宛先とするパケットがドロップされるため、トラブルシューティングと管理が困難になることがあります。 **注意** self-ping を許可すると、Denial of Service（DoS; サービス拒絶）ホールとなる可能性があります。
ACL（ユニキャスト RPF の場合）	ユニキャスト RPF をイネーブルにした場合は、ACL を適用して、リバース パスが見つからない場合のパケットの処理方法を改良できます。ACL を指定した場合は、パケットがユニキャスト RPF のチェックに失敗したときに、ACL の内容に基づいて、（ACL で拒否ステートメントを使用して）パケットをドロップするか、（ACL の許可ステートメントを使用して）転送するかが判断されます。標準または拡張 ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

Cisco IOS ルータでの IPS モジュール インターフェイス設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS および IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

ルータによっては、Cisco Intrusion Prevention System Advanced Integration Module や Network Module などの IPS モジュールをインストールできます。このようなモジュールをインストールし、アクティブにするときには、IPS モジュール インターフェイス設定ポリシーで次の情報を定義する必要があります。

- モジュールとルータ間のインターフェイスの名前。
- モジュールの障害モード。モジュールが失敗する場合は、すべてのトラフィックを許可するか、またはすべてのトラフィックを拒否するようにモジュールを設定できます。
- モニタするルータ インターフェイス。特定のインターフェイスに名前を付けたり、インターフェイス ロールを使用して複数のインターフェイスを一度に処理したりできます。たとえば、All-Ethernets インターフェイス ロールを定義した場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じモニタリング設定を定義できます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

ヒント IPS モジュール インターフェイス設定ポリシーを定義したあと、ポリシーを共有し、他のデバイスにポリシーを割り当てることができます。これにより、同じ設定の複数のデバイスを簡単に設定できます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）を参照してください。

はじめる前に

基本的なインターフェイス設定を定義します。Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから [インターフェイス（Interfaces）]>[設定（Settings）]>[IPS モジュール（IPS Module）] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから [ルータ インターフェイス（Router Interfaces）]>[設定（Settings）]>[PVC] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[IPS Module Interface Settings] ページが表示されます。このページのフィールドの説明については、[IPS Module Interface Settings] ページ （3033 ページ）を参照してください。

ステップ 2 [IPS Module Interface Settings] の各フィールドには、IPS インターフェイスの名前（IDS-Sensor1/0 など）を入力するか、または [Select] をクリックしてリストから名前を選択します。また、モジュールが失敗した場合にすべてのトラフィックを許可するのか（フェールオープン）、すべてのトラフィックを拒否するのか（フェール クローズ）を決定します。

ステップ 3 モジュールがモニタするルータ インターフェイスを特定します。[IPSモジュールサービスのモジュールモニタリング設定（IPS Module Service Module Monitoring Settings）] テーブルの下にある [追加（Add）] ボタンをクリックしてインターフェイスをリストに追加するか、またはインターフェイスを選択し、[編集（Edit）] ボタンをクリックして既存のインターフェイスの設定を変更します。[IPS Monitoring Information] ダイアログボックスを使用して、インターフェイス名またはインターフェイス ロール、モニタリング モード、およびアクセス リスト（ある場合）を定義します。詳細については、[IPS Monitoring Information] ダイアログボックス （3035 ページ）を参照してください。

[IPS Module Interface Settings] ページ

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

[IPS Module Interface Settings] ページは、Cisco Intrusion Prevention System Advanced Integration Module または Network Module に関する設定を定義する場合に使用します。モジュールは、IPS 6.0 以降を実行している必要があります。IPS インターフェイスの障害モード、およびモジュールがモニタするインターフェイスを定義できます。ルータが IPS モジュールをホストしている場合にだけ、このポリシーを設定します。

注意 Cisco IOS IPS と Cisco IPS モジュールは併用できません。IPS モジュールがインストールされているときには、Cisco IOS IPS はディセーブルである必要があります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [IPSモジュール（IPS Module）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。新しいポリシーを作成するか、共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの IPS モジュール インターフェイス設定 （3032 ページ）

- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *826 : [IPS Module Interface Settings]* ページ

要素	説明
Interface Name	IPS モジュール インターフェイスの名前。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Fail Over Mode	モジュールの障害時にモジュールがトラフィック検査を処理する方法。フェール オープン（検査なしですべてのトラフィックを通過させる）か、またはフェール クローズ（すべてのトラフィックをドロップする）のいずれかになります。デフォルトはフェール オープンです。
[IPS Module Service Module Monitoring Settings] テーブル	IPS モジュールがモニタするルータ上のインターフェイスのリスト。 テーブルには、インターフェイスまたはインターフェイス ロールの名前、モニタリングがインラインか無差別か、およびインターフェイスでの検査のために ACL を使用してトラフィックをフィルタリングするかどうかが表示されます。インライン モードの場合、IPS モジュールが直接トラフィック フローに入り込むため、悪意のあるトラフィックを目的のターゲットに到達する前にドロップして、攻撃を阻止できます。無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されたパケットではなくモニタ対象トラフィックのコピーを分析します。ACL が一致した場合、一致したトラフィックは検査されません。 • インターフェイスをテーブルに追加するには、[Add] ボタンをクリックし、[IPS Monitoring Information] ダイアログボックス （3035 ページ）に入力します。 • インターフェイスの設定を編集するには、そのインターフェイスを選択し、[Edit] ボタンをクリックします。 • インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] ボタンをクリックします。

[IPS Monitoring Information] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

[IPS Monitoring Information] ダイアログボックスは、IPS モジュールがモニタするインターフェイスのプロパティを追加または編集する場合に使用します。

ナビゲーション パス

[IPS Module Interface Settings] ページ （3033 ページ）に移動し、[IPSモジュールサービスのモジュールモニタリング設定（IPS Module Service Module Monitoring Settings）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータでの IPS モジュール インターフェイス設定 （3032 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）

フィールド リファレンス

表 *827 : [IPS Monitoring Information]* ダイアログボックス

要素	説明
Interface Name	モジュールがモニタするインターフェイスまたはインターフェイス ロールの名前。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Monitoring Mode	インターフェイスをモニタする方法。 • [Inline mode]：IPS モジュールが直接トラフィック フローに入り込むため、悪意のあるトラフィックを目的のターゲットに到達する前にドロップして、攻撃を阻止できます。 • [Promiscuous mode]：パケットはセンサーを通過しません。センサーは、実際に転送されたパケットではなくモニタ対象トラフィックのコピーを分析します。

要素	説明
アクセス リスト（Access List）	検査のためにこのインターフェイスでトラフィックをフィルタリングするのに使用する標準または拡張アクセス リスト ポリシー オブジェクトの名前（そのポリシー オブジェクトを適用する場合）。ACL が一致すると、その ACL に対してトラフィックは検査されません。[選択（Select）] をクリックして、ACL を選択するか、または新規 ACL を作成します。

Cisco IOS ルータでの CEF インターフェイス設定

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は高度なレイヤ 3 IP スイッチング テクノロジーで、Web 中心のアプリケーションまたは対話型セッションを特徴とするインターネットや各種ネットワークなど、少量のトラフィックを伝送するネットワークから複雑なパターンで大量のトラフィックを伝送するネットワークまで、あらゆる種類のネットワークのネットワーク パフォーマンスおよびスケーラビリティを最適化します。CEF は、ほとんどの Cisco IOS ルータでデフォルトでイネーブルになります。

一般に、ルータで **show ip cef** コマンドを使用して統計情報を表示できるように CEF アカウンティングをイネーブルにする場合を除き、CEF ポリシーを設定する必要はありません。このほか、CEF を無効にする場合や、送信元/宛先パケット ストリームではなくパケットに基づいてロード バランスを実施するなどデフォルト以外の CEF 動作を特定のインターフェイスに設定する場合にも、CEF ポリシーを設定します。

インターフェイスの代替 CEF 設定を設定する場合は、特定のインターフェイスに名前を付けたり、インターフェイス ロールを使用して複数のインターフェイスを一度に処理したりできます。たとえば、All-Ethernets インターフェイス ロールを定義した場合は、1 つの定義だけでデバイス上のあらゆるイーサネット インターフェイスに対して同じ CEF 設定を定義できます。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。

ヒント CEF インターフェイス設定ポリシーを定義したあと、ポリシーを共有し、他のデバイスにポリシーを割り当てることができます。これにより、同じ設定の複数のデバイスを簡単に設定できます。デバイス ビューまたは Site-to-Site VPN Manager における共有ポリシーの使用 （256 ページ）を参照してください。

はじめる前に

基本的なインターフェイス設定を定義します。Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）]>[設定（Settings）]>[CEF] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [CEF] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[CEF Interface Settings] ページが表示されます。このページのフィールドの説明については、[CEF Interface Settings] ページ （3037 ページ）を参照してください。

ステップ 2 CEF をイネーブルにする場合は、目的に応じたアカウンティング オプションを選択します。

ステップ 3 特定のインターフェイスにデフォルト以外の動作を設定する場合は、そのインターフェイスを [CEF Interface Settings] テーブルに追加します。テーブルの下にある [追加（Add）] ボタンをクリックしてインターフェイスをリストに追加するか、またはインターフェイスを選択し、[編集（Edit）] ボタンをクリックして既存のインターフェイスの設定を変更します。これらのオプションの詳細については、[CEF Interface Settings] ダイアログボックス （3039 ページ）を参照してください。

[CEF Interface Settings] ページ

[CEF Interface Settings] ページは、シスコ エクスプレス フォワーディングの設定を定義する場合に使用します。CEF は高度なレイヤ 3 IP スイッチング テクノロジーで、Web 中心のアプリケーションまたは対話型セッションを特徴とするインターネットや各種ネットワークなど、少量のトラフィックを伝送するネットワークから複雑なパターンで大量のトラフィックを伝送するネットワークまで、あらゆる種類のネットワークのネットワーク パフォーマンスおよびスケーラビリティを最適化します。CEF は、ほとんどの Cisco IOS ルータでデフォルトでイネーブルになります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インタフェイス（Interfaces）] > [設定（Settings）] > [CEF] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [CEF] を選択します。新しいポリシーを作成するか、共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *828 : [CEF Interface Settings]* ページ

要素	説明
Enable Cisco Express Forwarding	デバイスでグローバルに CEF をイネーブルにするかどうかを指定します。デバイスで CEF をディセーブルにできない場合にはグレーになります。CEF をグローバルにイネーブルにする場合にだけ、ページの他の設定を設定できます。
CEF Network Accounting	CEFアカウンティングをグローバルに設定するためのオプションです。アカウンティング統計情報を収集すると、ルータで **show ip cef** コマンドを使用してその情報を表示できます。次のオプションを選択して、さまざまなタイプのアカウンティングをイネーブルにできます。 • [Enable Accounting for Traffic Through Non-Recursive Prefixes]：ネクストホップが直接接続されたネットワーク プレフィックスの場合、非再帰アカウンティングにより、プレフィックスを介したパケット収集のエクスプレスフォワーディングがイネーブルになります。 • [プレフィックス単位のアカウンティングの有効化（Enable Per-Prefix Accounting）]：パケットのネットワークプレフィックスに基づいたアカウンティング統計情報。 • [Enable Prefix Length Accounting]：ネットワーク プレフィックス長に基づいたアカウンティング統計情報。 • [Enable Load Balance Hash Accounting]：宛先単位のロード バランシング（デフォルト）を使用すると、CEF は 16 の一続きのハッシュ バケットを使用して、送信元アドレスおよび宛先アドレスに基づいて使用可能なパスを配布します。ロード バランス ハッシュ アカウンティングをイネーブル化すると、ハッシュ バケット単位のカウンタが用意されます。

要素	説明
CEF Interface Settings table	特殊な CEF 設定を定義しているルータ上のインターフェイス。CEF をグローバルにイネーブルにすると、デフォルトではルータ上のすべてのインターフェイスが CEF をイネーブルにし、宛先単位のロードバランシングを使用します。インターフェイスに別の動作を設定する場合にだけ、インターフェイスをこのテーブルに追加します。 テーブルには、インターフェイスまたはインターフェイス ロールの名前、CEF がイネーブルかディセーブルか、およびインターフェイスがロード バランシングを宛先またはパケット単位で実施しているかが表示されます。各フィールドの詳細については、[CEF Interface Settings] ダイアログボックス （3039 ページ）を参照してください。 • テーブルにインターフェイスを追加するには、[Add] ボタンをクリックします。 • インターフェイスの設定を編集するには、そのインターフェイスを選択し、[Edit] ボタンをクリックします。 • インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] ボタンをクリックします。

[CEF Interface Settings] ダイアログボックス

[CEF Interface Settings] ダイアログボックスは、グローバルなデフォルトとは異なる設定にするときに、インターフェイスの CEF プロパティを追加または編集する場合に使用します。

ナビゲーション パス

[CEF Interface Settings] ページ （3037 ページ）に移動してから、[CEF インターフェイス設定（CEF Interface Settings）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

• Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）
• Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）

フィールド リファレンス

表 *829 : [CEF Interface Settings]* ダイアログボックス

要素	説明
Interface Name	CEF を設定しているインターフェイスまたはインターフェイス ロールの名前。名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Enable CEF on Interface	インターフェイスでCEFをイネーブルにするかどうかを指定します。CEFは、デフォルトでイネーブルになっています。
ロードバランシング	インターフェイスがトラフィックのロードバランシングを実施する方法。宛先単位またはパケット単位になります。 宛先単位のロードバランシングでは、特定の送信元/宛先ペアのすべてのパケットが同じパスを通ります。パケット単位ロードバランシングでは、特定の送信元/宛先ペアのパケットが常に同じ等コストルートを取るとはかぎらないため、宛先への到着順序がばらばらになることがあります。 デフォルトは、トラフィックの宛先に基づいたロードバランシングです。

Cisco IOS ルータ上のダイヤラ インターフェイス

サイト間VPN（ダイヤル バックアップの設定 （1432 ページ）を参照）のダイヤル バックアップ ポリシーを設定する場合は、事前に適切な Cisco IOS ルータにダイヤラ インターフェイス ポリシーを設定する必要があります。ダイヤラ インターフェイス ポリシーは、ダイヤラ プールを使用して、ダイヤル バックアップで使用されているダイヤラ インターフェイスをルータ上の物理 BRI インターフェイスに関連付けます。各ダイヤラ インターフェイスは、単一のダイヤラ プールに関連付けられます。ダイヤラ プールには、1 つ以上の物理インターフェイスを含めることができます。複数のダイヤラ インターフェイスが、同じダイヤラ プールを参照できます。

以降のトピックでは、Cisco IOS ルータでダイヤラ インターフェイス ポリシーを作成する方法について説明します。

- ダイヤラ プロファイルの定義 （3040 ページ）
- BRI インターフェイス プロパティの定義 （3042 ページ）

ダイヤラ プロファイルの定義

ダイヤラ プロファイルを設定するときには、ダイヤラ インターフェイスを表すインターフェイスまたはインターフェイス ロールを選択し、ダイヤルする番号を指定する必要があります。

また、プール ID を割り当てる必要があります。プール ID は、物理ダイヤラ インターフェイスを設定するときに、このダイヤラインターフェイスを参照するために使用されます。また、回線のデフォルトのタイムアウト設定を変更することもできます。

（注） IP は、Security Manager がダイヤラ プロファイルに対してサポートする唯一のプロトコルです。

（注） ダイヤラ プロファイルの認証パラメータが、PPP ポリシーに定義されています。

はじめる前に

ルータに仮想および物理ダイヤラ インターフェイスを定義します。 Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

（注） また、オプションで仮想および物理ダイヤラ インターフェイスのインターフェイス ロールを定義できます。 ダイヤラ プロファイルの定義 （3040 ページ）を参照してください。

関連項目

- BRI インターフェイス プロパティの定義 （3042 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インタフェース（Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dialer] ページが表示されます。このページのフィールドの説明については、表 830 : [Dialer] ページ （3044 ページ）を参照してください。

ステップ 2 [ダイヤラインターフェイス（Dialer Interfaces）] ページの上部にあるテーブルからダイヤラプロファイルを選択し、[編集（Edit）] をクリックします。あるいは、プロファイルを作成するときには [追加（Add）] をクリックします。[Dialer Profile] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 831 : [Dialer Profile] ダイアログボックス （3046 ページ）を参照してください。

ステップ 3 仮想ダイヤラインターフェイスを表すインターフェイスまたはインターフェイスロールの名前を入力します。あるいは [選択（Select]） をクリックしてインターフェイス ロール オブジェクトを選択するか、

または新しいインターフェイス ロール オブジェクトを作成します。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

ステップ 4 ダイヤラ プロファイルの名前を入力します。名前を付けると、適切なダイヤラ プールを物理インターフェイスに割り当てるのが容易になります。BRIインターフェイスプロパティの定義 （3042ページ）を参照してください。

ヒント ダイヤラ インターフェイスがバックアップとして機能するサイトに論理的に関連付けられた名前を定義することを推奨します。たとえば、ダイヤラインターフェイスがLondonサイトのバックアップ接続として機能している場合は、ダイヤラ プロファイルに London という名前を定義します。

ステップ 5 このダイヤラ インターフェイスに関連付けるダイヤラ プールの ID 番号を入力します。各ダイヤラ インターフェイスは、単一のプールに関連付けられます。ただし、複数のインターフェイスを同じダイヤラ プールに関連付けることもできます。

ステップ 6 ダイヤラ インターフェイスに割り当てるダイヤラ グループの数を入力します。

ステップ 7 （任意）[インタレスティングトラフィックACL（Interesting Traffic ACL）] フィールドに、このダイヤラ プロファイルを使用したコールの開始を許可するパケットを定義する拡張ACLオブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックしてリストから拡張ACLオブジェクトを選択するか、または新しい拡張 ACL オブジェクトを作成します。このオプションは、ダイヤラを使用できる IP トラフィックを制限する場合に使用します。

ステップ 8 ダイヤラ インターフェイス接続のリモート側の電話番号となるダイヤラ文字列を入力します。

ステップ 9 （任意）必要に応じてデフォルトのタイムアウト値（[Idle Timeout] および [Fast Idle Timeout]）を変更します。

ステップ 10 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。ダイヤラ プロファイルは、[Dialer] ページの [Dialer Profile] テーブルに表示されます。

BRI インターフェイス プロパティの定義

適切なインターフェイスまたはインターフェイス ロールを選択し、インターフェイスが属するダイヤラ プールを定義し、ISDN スイッチ タイプを定義して、ダイヤラ インターフェイス ポリシーに使用される物理BRIインターフェイスのプロパティを設定します。物理インターフェイスを仮想ダイヤラ インターフェイスに結び付けるのがダイヤラ プールです。

（注） ATM やイーサネットなど、物理ダイヤラ インターフェイスの他のタイプを定義するには、FlexConfig を使用します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

はじめる前に

ルータに仮想および物理ダイヤラ インターフェイスを定義します。Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

（注） また、オプションで仮想および物理ダイヤラ インターフェイスのインターフェイス ロールを定義できます。インターフェイス ロール オブジェクトの作成 （383 ページ） を参照してください。

関連項目

- ダイヤラ プロファイルの定義 （3040 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インタフェース（Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルーターインターフェイス（Router Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Dialer Interfaces] ページが表示されます。このページのフィールドの説明については、表 830 : [Dialer] ページ （3044 ページ）を参照してください。

ステップ 2 [ダイヤラ物理インタフェース（Dialer Physical Interfaces）] テーブルから物理 BRI インターフェイスを選択し、[編集（Edit）] をクリックするか、または [追加（Add）] をクリックして物理 BRI インターフェイスを追加します。[Dialer Physical Interface] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 832 : [Dialer Physical Interface] ダイアログボックス （3047 ページ）を参照してください。

ステップ 3 物理ダイヤラインターフェイスを表すインターフェイスまたはインターフェイスロールの名前を入力します。あるいは [選択（Select）] をクリックしてリストからインターフェイス ロール オブジェクトを選択するか、または新しいインターフェイス ロール オブジェクトを作成します。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

ステップ 4 物理インターフェイスに関連付けるダイヤラプールの名前を入力するか、または [選択（Select）] をクリックしてセレクタを表示します。複数のエントリを指定する場合は、カンマで区切ります。

ステップ 5 物理インターフェイスで使用する ISDN スイッチ タイプを選択します。 <Table> 使用可能なスイッチタイプについて説明します。

ステップ 6 （任意）スイッチ タイプとして Basic-DMS-100、Basic-NI、または Basic-5ess を選択した場合は、最大 2 つの Service Provider Identifier（SPID; サービス プロバイダー識別子）を入力します。

（注） Basic-5ess スイッチ タイプの場合は、SPID がサポートされていても入力しないことを推奨します。

ステップ 7 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。インターフェイス定義は、[Dialer Interfaces] ページの [Dialer Physical Interfaces] テーブルに表示されます。

[Dialer Policy] ページ

[Dialer] ページは、物理 Basic Rate Interface（BRI; 基本インターフェイス）と仮想ダイヤラ インターフェイスとの関係を定義する場合に使用します。これらのダイヤラインターフェイスは、サイト間 VPN のダイヤル バックアップ機能を設定したときに使用します。

詳細については、Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）を参照してください。

ナビゲーション パス

- （デバイス ビュー）ポリシー セレクタから **[インタフェース（Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[ルータ インターフェイス（Router Interfaces）] > [設定（Settings）] > [ダイヤラ（Dialer）]** を選択します。[ダイヤラ（Dialer）] を右クリックしてポリシーを作成するか、または共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- ダイヤル バックアップの設定 （1432 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 830 : [Dialer] ページ

要素	説明
Dialer Profiles table	ダイヤラ プールを定義するダイヤラ プロファイル。物理 BRI インターフェイスを追加する場合は、事前にプロファイルを追加する必要があります。テーブルには、ダイヤラ インターフェイスが使用するインターフェイスまたはインターフェイス ロールの名前、プロファイル名、プール、グループ、どのトラフィックがこのプロファイルを使用できるかを定義する ACL、ダイヤル文字列、およびアイドル時間が表示されます。 • プロファイルを追加するには、[行の追加（Add Row）] ボタンをクリックし、 [Dialer Profile] ダイアログボックス （3045 ページ）に入力します。 • プロファイルを編集するには、プロファイルを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • プロファイルを削除するには、プロファイルを選択し、[行の削除（Delete Row）] ボタンをクリックします。

要素	説明
Dialer Physical Interfaces (BRI) table	ダイヤラ プロファイルを使用する物理インターフェイス。テーブルには、インターフェイスまたはインターフェイス ロールの名前、ダイヤル プール、ISDN スイッチ タイプ、およびインターフェイスに関連する 1 つめおよび 2 つめの Service Provider Identifier（SPID; サービス プロバイダー識別子）が表示されます。 • インターフェイスを追加するには、[行の追加（Add Row）] ボタンをクリックし、[Dialer Physical Interface] ダイアログボックス （3046 ページ）に入力します。 • インターフェイスを編集するには、インターフェイスを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • インターフェイスを削除するには、インターフェイスを選択し、[行を削除（Delete Row）] ボタンをクリックします。

[Dialer Profile] ダイアログボックス

[Dialer Profile] ダイアログボックスは、ダイヤラ プロファイルを追加または編集する場合に使用します。

ナビゲーション パス

[Dialer Policy] ページ （3044 ページ）に移動してから、[ダイヤラプロファイル（Dialer Profile）] テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [Dialer Physical Interface] ダイアログボックス （3046 ページ）
- ダイヤラ プロファイルの定義 （3040 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）

フィールド リファレンス

表 *831 : [Dialer Profile]* ダイアログボックス

要素	説明
名前	ダイヤラ プロファイルのわかりやすい名前。名前を付けると、適切なダイヤラプールを物理インターフェイスに割り当てることができます。プロファイル名は、このダイヤラ インターフェイスがバックアップとして機能するサイトへの参照として使用することもできます。
インターフェイス	ダイヤラ プロファイルに関連付ける仮想ダイヤラ インターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Pool ID	ダイヤラ プール ID。各プールは複数の物理インターフェイスを含めることができ、複数のダイヤラ インターフェイスに関連付けることができます。ただし、各ダイヤラインターフェイスは、1つのプールにだけ関連付けられます。
グループ	このダイヤラ インターフェイスが使用するダイヤラ グループを識別するグループ ID。
Interesting Traffic ACL	どのパケットにこのダイヤラ プロファイルを使用したコールの開始を許可するかを定義する拡張番号付き ACL。有効な ACL 番号は 100 ～ 199 です。 ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Dialer String (Remote Phone Number)	ダイヤラが問い合わせる宛先の電話番号。
アイドル タイムアウト	デフォルトのアイドル時間。この時間を過ぎると、非コンテンション方式の回線が切断されます。デフォルトは 120 秒です。
Fast Idle Timeout	デフォルトのアイドル時間。この時間を過ぎると、コンテンション方式の回線が切断されます。デフォルトは 20 秒です。 別のパケットを異なる宛先に送信するためにビジー状態の回線が要求されると、回線コンテンションが発生します。

[Dialer Physical Interface] ダイアログボックス

[Dialer Physical Interface] ダイアログボックスは、物理 BRI インターフェイスをダイヤラ インターフェイスに関連付けるプロパティを追加または編集する場合に使用します。

（注） ATM やイーサネットなど、物理ダイヤラ インターフェイスの他のタイプを定義するには、FlexConfig を使用します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

ナビゲーション パス

[Dialer Policy] ページ （3044 ページ）に移動してから、[ダイヤラの物理インターフェイス（Dialer Physical Interfaces）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [Dialer Profile] ダイアログボックス （3045 ページ）
- BRI インターフェイス プロパティの定義 （3042 ページ）
- Cisco IOS ルータ上のダイヤラ インターフェイス （3040 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *832 : [Dialer Physical Interface]* ダイアログボックス

要素	説明
ISDN BRI	ダイヤラ インターフェイスに関連付けられた物理 BRI インターフェイス。インターフェイスまたはインターフェイス ロール オブジェクトの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイス ロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
プール	ダイヤラ プールを物理インターフェイスに関連付けます。1 つ以上のプールの名前を（[Dialer Profile] ダイアログボックス （3045 ページ）で定義されているように）入力するか、または [選択（Select）] をクリックしてセレクタを表示します。複数のエントリを指定する場合は、カンマで区切ります。

要素	説明
スイッチ タイプ	ISDN スイッチ タイプ。 北米の場合、オプションは次のとおりです。 • [basic-5ess]：Lucent（AT&T）基本速度 5ESS スイッチ • [basic-dms100]：Northern Telecom DMS-100 基本速度スイッチ • [basic-ni]：National ISDN スイッチ オーストラリア、ヨーロッパ、およびイギリスの場合、オプションは次のとおりです。 • [basic-1tr6]：ドイツ 1TR6 ISDN スイッチ • [basic-net3]：ノルウェー NET3、オーストラリア NET3、ニュージーランド NET3 の各スイッチ タイプの NET3 ISDN BRI。Euro-ISDN E-DSS1 シグナリング システムの ETSI 準拠のスイッチ タイプ • [vn3]：フランス VN3 スイッチおよび VN4 ISDN BRI スイッチ 日本の場合、オプションは次のとおりです。 • [ntt]：日本 NTT ISDN スイッチ 音声/PBX システムの場合、オプションは次のとおりです。 • [basic-qsig]：Q.931 準拠の QSIG シグナリングを搭載した PINX（PBX）スイッチ
SPID1	スイッチ タイプとして Basic-DMS-100、Basic-NI、Basic-5ess のいずれかを選択したときにだけ適用されます。 インターフェイスがサブスクライブする ISDN サービスの Service Provider Identifier（SPID; サービス プロバイダー識別子）。北米のサービス プロバイダーによっては、ISDN サービスを初めてサブスクライブしたときに、SPID が ISDN デバイスに割り当てられることがあります。SPID を必要とするサービス プロバイダーを使用している場合、ISDN デバイスはスイッチにアクセスして接続を初期化するときに、有効な割り当て済み SPID をサービス プロバイダーに送信するまで、コールを発信または受信できません。 有効な SPID は、スペースや特殊文字を含めて最大 20 文字です。 （注） AT&T 5ESS スイッチ タイプを使用するインターフェイスの場合、サポートされていても、SPID は入力しないことを推奨します。

要素	説明
SPID2	スイッチ タイプとして DMS-100 または NI を選択したときにだけ適用されます。 インターフェイスがサブスクライブする 2 つめの ISDN サービスの Service Provider Identifier（SPID; サービス プロバイダー識別子）。有効な SPID には、最大 20 文字の英数字を含めることができます（スペースは含めることができません）。

Cisco IOS ルータでの ADSL

Digital Subscriber Line（DSL; デジタル加入者線）は、既存のツイストペア銅線上でデータを転送するテクノロジーのファミリです。DSL では、POTS（単純な旧式の電話サービス）で使用される上位リストを超える周波数を使用して、電話会社の交換局をカスタマーサイトに接続するローカルループ（またはラストマイル）上でマルチメディアやビデオなどのブロードバンド アプリケーションを配信します。

Asymmetric Digital Subscriber Line（ADSL; 非対称デジタル加入者線）は、DSL の一形態で、カスタマー サイトへのデータ フロー ダウンストリームの方が、Central Office（CO; 交換局）へのデータ フロー アップストリームよりもはるかに大きくなっています。この非対称設定は、Web サーフィン、ビデオオンデマンド、リモート LAN アクセスなど、ダウンロードするときの方が送信するときよりも情報量が多い用途に適しています。ADSL の接続速度は、カスタマー サイトと、複数のカスタマー サイトの接続を 1 つの高速回線に集約する Digital Subscriber Line-Access Multiplexer（DSLAM; デジタル加入者線アクセス マルチプレクサ）との距離に関係があります。

ADSL のダウンストリームの帯域幅は 1.5 ～ 9 Mbps であり、アップストリームの帯域幅は 16 ～ 640 kbps です。ADSL では、単一の銅ツイスト ペアで最大 18,000 フィート（5,488 m）まで正常に伝送できます。ADSL2 や ADSL2+ など最新の ADSL テクノロジーでは、短距離でのデータ レートを高めるだけでなく、電源管理およびリアルタイム パフォーマンス モニタリングを実現しています。

ATM は、小さな固定長のセル サイズであることから数多くの ADSL 実装に使用されており、音声やビデオなど時間が重要となるトラフィックを、他のトラフィックとともに伝送するのに適しています。Security Manager では、Cisco IOS ルータに ATM over DSL を設定できます。Security Manager で ADSL ポリシーを設定する方法の詳細については、ADSL 設定の定義 （3051 ページ）を参照してください。

Security Manager で ADSL を設定するには、次の手順を実行する必要があります。

1. ATM インターフェイスまたはサブインターフェイスを設定します。基本的なルータ インターフェイス設定の定義 （3009 ページ）を参照してください。
2. ATM インターフェイスまたはサブインターフェイスに ADSL 設定を設定します。ADSL 設定の定義 （3051 ページ）を参照してください。
3. ATM インターフェイスまたはサブインターフェイスに PVC を設定します。ATM PVC の定義 （3071 ページ）を参照してください。

（注） デバイスで検出を実行した場合は、Security Manager が [Interfaces] ポリシーに ATM インターフェイスおよびサブインターフェイスを入力し、[ADSL] ポリシーにそのインターフェイスの ADSL 設定を入力します。検出された PVC は PVC ポリシーに追加されます。

関連項目

- サポートされる ADSL 動作モード （3050 ページ）

サポートされる ADSL 動作モード

表 833 : ADSL カードとサポートされている DSL 動作モード （3050 ページ）では、Security Manager で設定できる各 ADSL インターフェイス カードでどのような動作モードがサポートされているかを説明します。

表 *833 : ADSL* カードとサポートされている *DSL* 動作モード

ADSL インターフェイス カード	サポートされる DSL 動作モード
WIC-1ADSL	auto、ansi-dmt、itu-dmt、splitterless
WIC-1ADSL-I-DG	auto、etsi、itu-dmt
WIC-1ADSL-DG	auto、ansi-dmt、itu-dmt、splitterless
HWIC-1ADSL	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
HWIC-1ADSLI	auto、etsi、itu-dmt、adsl2、adsl2+
HWIC-ADSL-B/ST	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
HWIC-ADSLI-B/ST	auto、etsi、itu-dmt、adsl2、adsl2+

表 834 : 固定 ADSL デバイスとサポートされている DSL 動作モード （3050 ページ）では、Security Manager で設定できる各 ADSL デバイスでどのような動作モードがサポートされているかを説明します。

表 *834 :* 固定 *ADSL* デバイスとサポートされている *DSL* 動作モード

デバイス	サポートされる DSL 動作モード
857 サービス統合型ルータ	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
876 サービス統合型ルータ	auto、etsi、itu-dmt、adsl2、adsl2+
877 サービス統合型ルータ	auto、ansi-dmt、itu-dmt、adsl2、adsl2+
1801 サービス統合型ルータ	auto、ansi-dmt、itu-dmt、adsl2、adsl2+

デバイス	サポートされる DSL 動作モード
1802 サービス統合型ルータ	auto、etsi、itu-dmt、adsl2、adsl2+

関連項目

- ADSL 設定の定義 （3051 ページ）
- Cisco IOS ルータでの ADSL （3049 ページ）

ADSL 設定の定義

Security Manager で ADSL 定義を設定するときには、ADSL を定義する ATM インターフェイスを選択する必要があります。また、ルータ タイプまたはルータに組み込まれている WAN Interface Card（WIC; WAN インターフェイス カード）のタイプを指定することを強く推奨します。DSL ポリシー定義の有効性は、ハードウェアに大きく依存します。このポリシーで使用されているハードウェアを指定すると、Security Manager では定義した値が正しく検証されるため、展開の失敗を回避できます。

次のパラメータを任意で指定することもできます。

- DSL 動作モード。
- Inverse Multiplexing over ATM（IMA; ATM の逆多重化）を使用している場合に、VC 帯域幅の動的な調整をイネーブルにするかどうか。
- 特定のインターフェイス カードで特定のキャリア トーン セットを使用するかどうか。

モジュラ Cisco IOS ルータに複数のインターフェイス カードが含まれ、それぞれのカードに単一の ATM インターフェイスが含まれることがあります。インターフェイスごとに ADSL 定義を 1 つだけ定義することもできます。

はじめる前に

- デバイスに ADSL ATM インターフェイスが含まれていることを確認します。 Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ） を参照してください。

関連項目

- サポートされる ADSL 動作モード （3050 ページ）
- Cisco IOS ルータでの ADSL （3049 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[ADSL] ページが表示されます。このページのフィールドの説明については、表 835 : [ADSL] ページ （3053 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[ADSL設定（ADSL Settings）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 836 : [ADSL Settings] ダイアログボックス （3055 ページ）を参照してください。

ステップ 3 [ATMインターフェイス（ATM Interface）] フィールドに、ADSL 設定を定義する ATM インターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックしてインターフェイスロールを選択するか、または新規にインターフェイスロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

（注） 選択するインターフェイスは、デバイスに物理的に存在する必要があります。存在しないと、展開が失敗します。

ステップ 4 （任意）ルータに組み込まれているインターフェイス カードのタイプを選択します。

（注） ライブ デバイスから検出したときは、正しいインターフェイス カード タイプがすでに表示されています。ライブデバイスで検出を実行しなかった場合、または Cisco Security Manager がデバイスに取り付けられているインターフェイスカードのタイプを検出できない場合、このフィールドに「Unknown」と表示されます。

ステップ 5 （任意）IMA グループを使用している場合は、[ATM PVCで帯域幅変更を許可（Allow bandwidth change on ATM PVCs）] チェックボックスをオンにして、グループ帯域幅の変更に応じて VC 帯域幅が動的に調整されるようにします。このチェックボックスをオフのままにした場合は、このような調整を手動で行う必要があります。

ステップ 6 （任意）この ATM インターフェイスの DSL 動作モードを指定します。各カード タイプでサポートされている動作モードのリストについては、表 833 : ADSL カードとサポートされている DSL 動作モード （3050 ページ）を参照してください。

ステップ 7 （任意）インターフェイスカードでキャリアトーン 29 ～ 48 を使用するには、[低トーンセットを使用（Use low tone set）] チェックボックスをオンします。

ステップ 8 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[ADSL] テーブルに表示されます。

（注） ADSL 定義を編集するには、テーブルから目的の PVC を選択し、[編集（Edit）] をクリックします。ADSL 定義を削除するには、そのエントリを選択し、[削除（Delete）] をクリックします。

ステップ 9 他の ATM インターフェイスについてもステップ 2 （3052 ページ）～ステップ 8 （3052 ページ）を繰り返して ADSL 設定を定義します。インターフェイスに定義できる ADSL 定義は 1 つだけです。

[ADSL] ポリシー ページ

[ADSL] ページは、ルータの ATM インターフェイスに関する ADSL 定義を作成、編集、および削除する場合に使用します。詳細については、ADSL 設定の定義 （3051 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [ADSL]** を選択します。[ADSL] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [PVC] ポリシー ページ （3075 ページ）
- [SHDSL] ポリシー ページ （3059 ページ）
- Cisco IOS ルータでの ADSL （3049 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 835 : [ADSL] ページ

要素	説明
ATM インターフェイス	ADSL 設定が定義されている ATM インターフェイス。
インターフェイス カード	ATM インターフェイスが存在するデバイスまたは ADSL インターフェイス カードのタイプ。
Bandwidth Change	帯域幅全体の変更に応じてルータが VC 帯域幅を動的に調整するかどうかを示します（これは、IMA グループが ATM インターフェイスに設定されているときにだけ重要な意味を持ちます）。
DSL動作モード（DSL Operating Mode）	この ATM インターフェイスの DSL 動作モード。
Tone Low	インターフェイスが低トーン セット（キャリア トーン 29 ～ 48）を使用しているかどうかを示します。

要素	説明
[追加（Add）] ボタン	[ADSL Settings] ダイアログボックス （3054 ページ）が開きます。ここから、選択した ATM インターフェイスの ADSL 設定を定義できます。
[編集（Edit）] ボタン	[ADSL Settings] ダイアログボックス （3054 ページ）が開きます。ここから、選択した ADSL 定義を編集できます。
[削除（Delete）] ボタン	選択した ADSL 定義をテーブルから削除します。

[ADSL Settings] ダイアログボックス

[ADSL Settings] ダイアログボックスは、選択した ATM インターフェイスの ADSL 設定を設定する場合に使用します。

（注） ADSL 設定を設定した場合は、ATM インターフェイスが定義されているデバイスまたはインターフェイス カードのタイプを選択することを強く推奨します。ADSL 設定は、ハードウェアに大きく依存します。Security Manager でハードウェア タイプを定義すると、設定が適切に検証されるため、デバイスへの展開を正常に完了できます。

ナビゲーション パス

[ADSL] ポリシー ページ （3053 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- ADSL 設定の定義 （3051 ページ）
- [PVC] ポリシー ページ （3075 ページ）

フィールド リファレンス

表 *836 : [ADSL Settings]* ダイアログボックス

要素	説明
ATM インターフェイス	ADSL 設定が定義されている ATM インターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） インターフェイス ロールを定義するときには、同じインターフェイス カードからの ATM インターフェイスだけを含めることを推奨します。各カード タイプでサポートされている設定が異なると、展開に失敗することがあります。 （注） インターフェイスごとに ADSL 定義を 1 つだけ作成できます。
インターフェイス カード	ルータに組み込まれているデバイスまたはインターフェイス カードのタイプ。 • [blank]：インターフェイス カード タイプは定義されません。 • [WIC-1ADSL]：ADSL over POTS（通常の電話回線）を提供する 1 ポート ADSL WAN インターフェイス カード。 • [WIC-1ADSL-I-DG]：Dying Gasp サポートのある ADSL over ISDN を提供する 1 ポート ADSL WAN インターフェイス カード（Dying Gasp を使用すると、ルータは、ルータの電力が失われかけているときに、差し迫った回線ドロップを DSLAM に警告します）。 • [WIC-1ADSL-DG]：Dying Gasp サポートのある ADSL over POTS を提供する 1 ポート ADSL WAN インターフェイス カード。 • [HWIC-1ADSL]：ADSL over POTS を提供する 1 ポート高速 ADSL WAN インターフェイス カード。 • [HWIC-1ADSLI]：ADSL over ISDN を提供する 1 ポート高速 ADSL WAN インターフェイス カード。 • [HWIC-ADSL-B/ST]：バックアップのために ISDN BRI ポートに ADSL over POTS を提供する 2 ポート高速 ADSL WAN インターフェイス カード。 • [HWIC-ADSLI-B/ST]：バックアップのために ISDN BRI ポートに ADSL over ISDN を提供する 2 ポート高速 ADSL WAN インターフェイス カード。

要素	説明
Interface Card（続き）	• [857 ADSL]：ADSL インターフェイスがある Cisco 857 サービス統合型ルータ。 • [876 ADSL]：ADSL インターフェイスがある Cisco 876 サービス統合型ルータ。 • [877 ADSL]：ADSL インターフェイスがある Cisco 877 サービス統合型ルータ。 • [1801 ADSLoPOTS]：ADSL over POTS を提供する Cisco 1801 サービス統合型ルータ。 • [1802 ADSLoISDN]：ADSL over ISDN を提供する Cisco 1802 サービス統合型ルータ。 （注） ライブデバイスから検出したときは、正しいインターフェイスカード タイプがすでに表示されています。ライブデバイスで検出を実行しなかった場合、または Cisco Security Manager がデバイスに取り付けられているインターフェイスカードのタイプを検出できない場合、このフィールドに「Unknown」と表示されます。
Allow bandwidth change on ATM PVCs	選択されている場合、ATM インターフェイスに定義されている Inverse Multiplexing over ATM（IMA; ATM の逆多重化）グループの帯域幅全体の変更に応じて、ルータは VC 帯域幅を動的に調整します。 選択解除されている場合、IMA グループの個々の物理リンクがアップまたはダウンするたびに、PVC 帯域幅を（CLI を使用して）手動で調整する必要があります。
DSL動作モード（DSL Operating Mode）	この ADSL 回線に設定された動作モード。 • [auto]：Central Office（CO; 交換局）にある DSLAM とのオートネゴシエーションを実施します。これがデフォルトです。 • [ansi-dmt]：回線は、ANSI T1.413 Issue 2 モードでトレインします。 • [itu-dmt]：回線は、G.992.1 モードでトレインします。 • [splitterless]：回線は、G.992.2（G.Lite）モードでトレインします。 • [etsi]：回線は、European Telecommunications Standards Institute（ETSI）モードでトレインします。 • [adsl2]：回線は、G.992.3（adsl2）モードでトレインします。 • [adsl2+]：回線は、G.992.5（adsl2+）モードでトレインします。 （注） 各カード タイプでサポートされている動作モードについては、表 833：ADSL カードとサポートされている DSL 動作モード（3050 ページ）を参照してください。

要素	説明
Use low tone set	選択されている場合、インターフェイス カードはキャリア トーン 29 ～ 48 を使用します。 選択解除されている場合、インターフェイス カードはキャリア トーン 33 ～ 56 を使用します。 （注） Deutsche Telekom 仕様 U-R2 に従ってインターフェイス カードが動作しているときには、このオプションを選択しないでください。

Cisco IOS ルータでの SHDSL

Digital Subscriber Line（DSL; デジタル加入者線）は、既存のツイストペア銅線上でデータを転送するテクノロジーのファミリです。DSL では、POTS（単純な旧式の電話サービス）で使用される上位リストを超える周波数を使用して、電話会社の交換局をカスタマーサイトに接続するローカルループ（またはラストマイル）上でマルチメディアやビデオなどのブロードバンド アプリケーションを配信します。

Symmetric High-Speed Digital Subscriber Line（SHDSL; 対称高速デジタル加入者線）は、International Telecommunications Union（ITU; 国際電気通信連合）G.991.2 グローバル業界標準に基づいて、単一のワイヤ ペアで 192 kbps ～ 2.3 Mbps までの対称データ レートを実現します。T1、E1、ISDN、ATM、IP など多くの信号タイプを転送します。また、G.SHDSL 信号は、交換局からの到達距離が ADSL 接続および独自の SDSL 接続よりも長くなっています。

Security Manager で SHDSL を設定するには、次の手順を実行します。

1. SHDSL コントローラを設定します。SHDSL コントローラの定義 （3058 ページ）を参照してください。
2. SHDSL ポリシーを展開します。ATM モードがアクティブである場合は、ルータは展開時にコントローラに対応する ATM インターフェイスを作成します。展開および Configuration Archive の使用 （511 ページ）を参照してください。
3. デバイスを再検出して、その新規 ATM インターフェイスを Security Manager に追加します。Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。
4. （任意）ATM インターフェイスに 1 つ以上のサブインターフェイスを作成します。基本的なルータ インターフェイス設定の定義 （3009 ページ）を参照してください。
5. ATM インターフェイスまたはサブインターフェイスに PVC を設定します。ATM PVC の定義 （3071 ページ）を参照してください。

（注） デバイスで検出を実行した場合、Security Manager は [SHDSL] ポリシーにコントローラの定義を読み込み、[Interfaces] ポリシーに ATM インターフェイスおよびサブインターフェイスを読み込みます。検出された PVC は PVC ポリシーに追加されます。

関連項目

- Cisco IOS ルータでの PVC （3065 ページ）

SHDSL コントローラの定義

Security Manager で SHDSL コントローラを設定した場合、Cisco IOS ルータにインストールされているコントローラの名前を入力する必要があります。名前を入力すると、次の設定が自動的に適用されます。

- ATM モードがイネーブルになります。
- 回線終端が、Customer Premises Equipment（CPE; 宅内装置）に設定されます。
- 回線モードが、Auto に設定されます。

任意で回線終端を CO に変更し、DSL モードおよび回線モードを指定できます。また、信号対雑音比マージンを定義して、回線の安定性を高めることができます。

1 台の Cisco IOS ルータに、複数の SHDSL コントローラを含めることができます。その場合、SHDSL 定義はコントローラごとに 1 つだけ定義できます。

（注） ATM モードをイネーブルにして SHDSL ポリシーを展開すると、ルータに ATM インターフェイスが自動的に作成されます。再検出を実行して、インターフェイスを Security Manager に追加します。次に、必要に応じて ATM インターフェイスに PVC を定義できます。 ATM PVC の定義 （3071 ページ）を参照してください。

はじめる前に

- SHDSL コントローラがデバイスにインストールされていることを確認します。

関連項目

- Cisco IOS ルータでの SHDSL （3057 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SHDSL] ページが表示されます。このページのフィールドの説明については、[SHDSL] ポリシー ページ（3059 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[SHDSL] ダイアログボックスを表示します。

ステップ 3 コントローラの名前を入力します。または [選択（Select）] をクリックしてコントローラ名を生成するためのユーティリティを表示します。[Controller Auto Name Generator] ダイアログボックス （3064 ページ）を参照してください。

（注） 選択するコントローラは、デバイスに物理的に存在する必要があります。存在しないと、展開が失敗します。

ステップ 4 必要に応じて SHDSL コントローラを定義します。詳細については、表 838 : [SHDSL] ダイアログボックス（3061 ページ）を参照してください。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[SHDSL] テーブルに表示されます。

（注） SHDSL コントローラを編集するには、編集するコントローラをテーブルから選択し、[編集（Edit）] をクリックします。SHDSL コントローラを削除するには、削除するコントローラを選択し、[削除（Delete）] をクリックします。

ステップ 6 ステップ 2（3059 ページ）～ステップ 5（3059 ページ）を繰り返して、他の SHDSL コントローラを定義します。定義は、コントローラごとに 1 つだけ定義できます。

[SHDSL] ポリシー ページ

[SHDSL] ページは、ルータで DSL コントローラ定義を作成、編集、および削除する場合に使用します。詳細については、SHDSL コントローラの定義 （3058 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL] を選択します。
- （ポリシー ビュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [DSL] > [SHDSL] を選択します。[SHDSL] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [PVC] ポリシー ページ （3075 ページ）
- [ADSL] ポリシー ページ （3053 ページ）
- Cisco IOS ルータでの SHDSL （3057 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *837 : [SHDSL]* ページ

要素	説明
名前	DSL コントローラの名前。
説明	（任意）コントローラの説明。
シャットダウン	DSL コントローラがシャットダウン モードであるかどうかを示します。
Configure ATM Mode	DSL コントローラが ATM モードに設定されているかどうかを示します。
Line Termination	ルータに設定されている回線終端（CPE または CO）。
DSL Mode	DSL コントローラに対して定義されている動作モード。
[回線モード（Line Mode）]	DSL コントローラに対して定義されている回線モード。
Line Rate	DSL コントローラに対して定義されている回線レート（kbps 単位）。 （注） 回線モードが Auto に設定されている場合にだけ、値がこの列に表示されます。
SNR Margin Current	コントローラの現在の信号対雑音比。
SNR Margin Snext	コントローラの Self Near-End Crosstalk（Snext; セルフ近端クロストーク）信号対雑音比。
[追加（Add）] ボタン	[SHDSL Controller] ダイアログボックス （3061 ページ）が開きます。ここから、DSL コントローラの設定を定義できます。
[編集（Edit）] ボタン	[SHDSL Controller] ダイアログボックス （3061 ページ）が開きます。ここから、選択した DSL コントローラ定義を編集できます。
[削除（Delete）] ボタン	選択した DSL コントローラ定義をテーブルから削除します。

[SHDSL Controller] ダイアログボックス

[SHDSL Controller] ダイアログボックスは、SHDSL コントローラを設定する場合に使用します。

ナビゲーション パス

[SHDSL] ポリシー ページ （3059 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- SHDSL コントローラの定義 （3058 ページ）
- [PVC] ポリシー ページ （3075 ページ）
- Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）

フィールド リファレンス

表 *838 : [SHDSL]* ダイアログボックス

要素	説明
名前	コントローラの名前。名前を手動で入力するか、または [選択（Select）] をクリックして名前を生成するためのダイアログボックスを表示します。[Controller Auto Name Generator] ダイアログボックス （3064 ページ）を参照してください。
説明	コントローラに関する追加の情報（最大 80 文字）。
シャットダウン	選択されている場合、DSL コントローラがシャットダウン状態になります。ただし、その定義は削除されません。 選択解除されている場合、DSL コントローラがイネーブルになります。これがデフォルトです。
Configure ATM mode	選択されている場合、コントローラを ATM モードに設定し、コントローラと同じ ID で ATM インターフェイスを作成します。これがデフォルトです。ATM モードをイネーブルにし、再検出を実行してデバイスに ATM または PVC を設定する必要があります。 選択解除されている場合、ATM モードがディセーブルになります。展開時に ATM インターフェイスが作成されません。 （注） いったん Security Manager に保存された ATM モードは、コントローラから削除できません。

要素	説明
Line Termination	ルータに設定されている回線終端。 • [CPE]：宅内装置。これがデフォルトです。 • [CO]：交換局。
DSL Mode	地域の動作パラメータなど、コントローラで使用されている DSL 動作モード。 • [blank]：動作モードは定義されません（展開時には、北米の Annex A 規格が使用されます）。 • A：北米の G.991.2 規格の Annex A をサポートします。 • AB：Annex A または Annex B をサポートします。Line Term が CPE に設定されている場合にのみ使用できます。回線トレイン時に適切なモードが選択されます。 • A-B-ANFP：Annex A または Annex B-ANFP をサポートします。[Line Term] が [CPE] に設定されている場合にだけ使用可能です。回線トレイン時に適切なモードが選択されます。 • B：ヨーロッパの G.991.2 規格の Annex B をサポートします。 • B-ANFP：Annex B-Access Network Frequency Plan（ANFP）をサポートします。 （注） 使用可能な DSL モードは、選択した回線終端によって異なります。
回線モード設定	
[回線モード（Line Mode）]	コントローラで使用されている回線モード。 • [Auto]：コントローラは、他の回線終端と同じモードで動作します（2 線式回線 0、2 線式回線 1、または 4 線式拡張）。これは CPE 回線終端のデフォルトです。 • [2-wire]：コントローラは、2 線式モードで動作します。これは CO 回線終端のデフォルトです。 • [4-wire]：コントローラは、4 線式モードで動作します。 （注） コントローラを CPE として設定したときにだけ、[Auto] を選択できます。

要素	説明
回線（Line）	[Line Mode] が [2-wire] に定義されているときにだけ適用されます。 使用するワイヤのペアは次のとおりです。 • [line-zero]：RJ-11 PIN 1 および PIN 2。これは CO 回線終端のデフォルトです。 • [line-one]：RJ-11 PIN 3 および PIN 4。
Exchange Handshake	回線モードが [4-wire] に定義されているときにだけ適用されます。 使用するハンドシェイク モードのタイプは次のとおりです。 • [blank]：ハンドシェイク モードは指定されません（展開時には、[拡張（enhanced）] オプションが使用されます）。これがデフォルトです。 • [enhanced]：両方のワイヤ ペアでハンドシェイク ステータスを交換します。 • [標準（standard）]：メインワイヤペアでのみハンドシェイクステータスを交換します。
Line Rate	[Line Mode] が [Auto] に定義されているときには適用されません。 SHDSL ポートが対応する DSL 回線レート（kbps 単位）。 • [auto]：コントローラは、回線レートを選択します。2 線式モードでだけ使用可能です。 • サポートされている回線レートは次のとおりです。 • 2 線式モードの場合：192、256、320、384、448、512、576、640、704、768、832、896、960、1024、1088、1152、1216、1280、1344、1408、1472、1536、1600、1664、1728、1792、1856、1920、1984、2048、2112、2176、2240、および 2304。 • 4 線式モードの場合：384、512、640、768、896、1024、1152、1280、1408、1536、1664、1792、1920、2048、2176、2304、2432、2560、2688、2816、2944、3072、3200、3328、3456、3584、3712、3840、3968、4096、4224、4352、4480、および 4608。 （注） サードパーティ機器によっては、2 線式モードで 8 kbps、4 線式モードで 16 kbps の SHDSL オーバーヘッドを考慮に入れた回線レートを使用できるものもあります。
SNR Margin の設定	

要素	説明
現在（Current）	コントローラの現在の Signal-To-Noise（SNR; 信号対雑音）比をデシベル単位（dB）で表した値。有効値の範囲は -10 ～ 10 dB です。 このオプションを選択すると、トレイン時に回線トレインが現在の雑音マージンに SNR 比しきい値を加えた値を上回るため、回線の安定性を高めることができます。設定された SNR マージンよりも外部のノイズが低いと、回線は安定します。 （注） 現在の SNR を無効にするには、[無効（disable）] を選択します。
Snext	コントローラの Self Near-End Crosstalk（Snext; セルフ近端クロストーク）信号対雑音比をデシベル単位で表した値。有効値の範囲は -10 ～ 10 dB です。 このオプションを選択すると、トレイン時に回線トレインが SNEXT しきい値を上回るため、回線の安定性を高めることができます。設定された SNEXT マージンよりも外部のノイズが低いと、回線は安定します。 （注） SNEXT SNR を無効にするには、[無効（disable）] を選択します。

[Controller Auto Name Generator] ダイアログボックス

[Controller Auto Name Generator] ダイアログボックスは、ルータ内での DSL コントローラの場所に基づいて DSL コントローラの名前を Security Manager で自動的に生成する場合に使用します。

ナビゲーション パス

[SHDSL Controller] ダイアログボックス （3061 ページ）に移動し、[名前（Name）] フィールドの [選択（Select）] をクリックします。

関連項目

- SHDSL コントローラの定義 （3058 ページ）
- [SHDSL] ポリシー ページ （3059 ページ）
- [PVC] ポリシー ページ （3075 ページ）

フィールド リファレンス

表 839 : [Controller Auto Name Generator] ダイアログボックス

要素	説明
タイプ	インターフェイスのタイプ。このフィールドには DSL という値が表示され、読み取り専用となります。

要素	説明
カード	コントローラに関連するカード。
スロット	コントローラに関連するスロット。
[ポート（Port）]	コントローラに関連するポート。 （注） これらのフィールドに入力した情報によって、[Result] フィールドに表示される、生成される名前の残りの部分が形成されます。
結果	コントローラの場所に入力した情報を基に Security Manager が生成した名前。このフィールドに表示される名前は読み取り専用です。 ヒント このダイアログボックスを閉じたあと、必要に応じて [SHDSL] ダイアログボックスで生成した名前を編集できます。

Cisco IOS ルータでの PVC

非同期転送モード（ATM）は、セルリレー技術を使用したパブリック ネットワークおよびプライベート ネットワークで音声、ビデオ、およびデータを高速転送するために定められた International Telecommunication Union（ITU-T; 国際電気通信連合）規格です。ATM はセルの交換と多重化の技術により、回線交換の利点（一定した伝搬遅延、容量保証）とパケット交換の利点（断続的なトラフィックへの柔軟かつ効率的な対応）とを兼ね備えたものとなっています。ATM ネットワークは、Cisco IOS ルータなど、1 つ以上の ATM スイッチと ATM エンドポイントで構成されます。

ATM サービスには一般に 3 つのタイプがあります。Permanent Virtual Connection（PVC; 相手先固定接続）、Switched Virtual Connection（SVC; 相手先選択接続）、およびコネクションレス型サービスです。PVC では、リース回線に似たサービスを提供するためにサイト間に直接および永続的な接続を確立できます。PVC の利点は、接続の可用性が保証されていることと、スイッチ間でコール確立手順が不要であることです。発信元から宛先までの間にある各機器は、PVC に対応するように手動でプロビジョニングする必要があります。

ATM PVC の詳細については、次の項目を参照してください。

- 仮想パスおよび仮想チャネルについて （3066 ページ）
- ATM サービス クラスについて （3067 ページ）
- ATM 管理プロトコルについて （3068 ページ）

Security Manager での PVC の定義の詳細については、次の項目を参照してください。

- ATM PVC の定義 （3071 ページ）
- Cisco IOS ルータでの SHDSL （3057 ページ）

関連項目

- Cisco IOS ルータでの ADSL （3049 ページ）
- Cisco IOS ルータでの SHDSL （3057 ページ）

仮想パスおよび仮想チャネルについて

ATM ネットワークは、基本的にはコネクション型です。つまり、データ転送を開始する前に ATM ネットワークに仮想接続を確立する必要があります。ATM 接続には、2 つのタイプがあります。

- Virtual Path Connection（VPC; 仮想パス接続）。Virtual Path Identifier（VPI; 仮想パス識別子）で識別されます。
- Virtual Channel Connection（VCC; 仮想チャネル接続）。VPI と Virtual Channel Identifier（VCI; 仮想チャネル識別子）の組み合わせで識別されます。PVC は、2 つのサイト間に永続的な接続が定義されているタイプの VCC です。

図 47 : ATM 仮想パスおよび仮想チャネル接続 （3066 ページ）に示すように、仮想パスは仮想チャネルをいくつかバンドルしたもので、いずれのチャネルも共通の VPI に基づいて ATM ネットワークで透過的にスイッチングされます。VPC は、VPI 値が同じ VCC をいくつかバンドルしたものであると考えることができます。

図 *47 : ATM* 仮想パスおよび仮想チャネル接続

どのセル ヘッダーにも VPI フィールドおよび VCI フィールドが含まれており、両フィールドともセルを物理リンク上の特定の仮想チャネルに明示的に関連付ける働きをします。VPI および VCI については次の属性に留意することが重要です。

- VPI および VCI は、LAN スイッチングで使用される MAC アドレスのようなアドレスではありません。
- VPI および VCI は接続の各セグメントで明示的に割り当てられるため、有効範囲が特定のリンクにローカルになります。各スイッチング ポイントで必要に応じて再マッピングされます。

ATM レイヤで VPI/VCI 識別子を使用すると、セルの多重化（インターリーブ）や逆多重化を行ったり、複数の接続からセルを切り替えることができます。VPI/VCI 識別子によっては、Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）など、特定の用途に予約されているものもあります。

関連項目

- ATM サービス クラスについて （3067 ページ）
- ATM 管理プロトコルについて （3068 ページ）
- ATM PVC の定義 （3071 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ATM サービス クラスについて

ATM フォーラムが公表したトラフィック管理仕様のバージョン 4.0 には、サービス クラスが 5 つ定義されています。各クラスには、ネットワークで送信されるユーザ トラフィックと、ネットワークがそのトラフィックで実現する必要があるサービスの品質が記述されています。Security Manager は、次の ATM サービス クラスをサポートします。

- 使用可能ビットレート（ABR、Available Bit Rate ）：ATM スイッチがセル配信を保証せず、最小ビットレートを保証し、フィードバックメカニズムを使用してセル損失をできるかぎり抑えるサービスクラス。ABR サービス カテゴリは、ファイル転送をはじめ、最小限の帯域幅を必要とするバーストで非リアルタイムなトラフィックを伝送する VC 向けに設計されています。この帯域幅は、VC が設定されてアクティブである場合に確保する必要がある最小セル レートで指定されます。詳細については、次の URL にある「Understanding the Available Bit Rate (ABR) Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a00800fbc76.shtm

- 固定ビットレート（CBR、Constant Bit Rate）：音声およびビデオの QoS ニーズを満たすように、セルが連続ビットストリームで送信されるサービスクラス。CBR サービス クラスは、接続がアクティブである間、固定量の帯域幅を継続して使用できることが求められる ATM 仮想回線（VC）向けに設計されています。CBR として設定された ATM VC は、Peak Cell Rate（PCR; ピーク セル レート）でいつでも好きな期間だけセルを送信できます。また、PCR を下回るレートでセルを送信したり、セルを送信しないようにしたりすることもできます。CBR に関する設定は、プラットフォームによって異なることがあります。詳細については、次の URL にある「Understanding the CBR Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094e6a.shtml

- 未指定ビットレート（UBR、Unspecified Bit Rate）：ネットワーク管理で Quality of Service（QoS）が保証されないサービスクラス。インターネットが通常提供するベストエフォート型のサービスをモデル化したもので、リアルタイムの応答を必要とせず、遅延が発生しても問題ないアプリケーションに適しています。たとえば、電子メール、FAX 転送、ファイル転送、Telnet、LAN、リモート オフィスの相互接続などです。詳細については、次の URL にある「Understanding the UBR Service Category for ATM Virtual Circuits」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a00800a4837.shtml

- 未指定ビットレート（UBR+、Unspecified Bit Rate）：シスコでは、UBR+ という UBR サービスクラスのバリアントを提供しています。UBR+ サービス クラスの主な利点は、ATM

エンド システムが接続要求時に ATM スイッチまで最小セル レートを確保し、ATM ネットワークがエンドツーエンド保証としてこの最小セル レートを維持しようとすることです。詳細については、次の URL にある「Understanding the UBR+ Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094b40.shtml

- 可変ビットレート - 非リアルタイム（VBR-nrt、Variable Bit Rate - Non-Real Time）：このサービスクラスは、バースト性の非リアルタイム アプリケーションを送信する場合に使用します。トラフィック特性は、Peak Cell Rate（PCR; ピーク セル レート）、平均セルレート (Sustained Cell Rate)、および Minimum Burst Size（MBS; 最小バースト サイズ）の観点から定義されます。詳細については、次の URL にある「Understanding the VBR-nrt Service Category and Traffic Shaping for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080102a42.shtml

- 可変ビット レート - リアルタイム（VBR-rt、Variable Bit Rate - Real Time ）：このサービスクラスは、圧縮した Voice over IP やビデオ会議など、時間遅延が重要な要素となるリアルタイムデータを送信する場合に使用します。VBR-nrt と同じく、VBR-rt トラフィックは PCR、SCR、および MBS の観点から定義されます。詳細については、次の URL にある「Understanding the Variable Bit Rate Real Time (VBR-rt) Service Category for ATM VCs」を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk51/technologies_tech_note09186a0080094cd0.shtml

このようなサービス クラスを使用すると、トラフィック シェーピングなど、ATM の Quality of Service（QoS）保証を定義できます。トラフィック シェーピングとは、トラフィック コントラクトによって定義されているエンベロープにトラフィックが収まるように、キューを使用してデータ バーストを抑制し、ピーク データ レートを制限し、ジッタを抑えることです。ATM デバイスは、トラフィック シェーピングを使用して、トラフィック コントラクトの条件に準拠します。

関連項目

- 仮想パスおよび仮想チャネルについて （3066 ページ）
- ATM 管理プロトコルについて （3068 ページ）
- ATM PVC の定義 （3071 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ATM 管理プロトコルについて

ATM は、2 種類のシグナリングを使用して PVC のステータスを追跡します。

- Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）。詳細については、ILMI について （3069 ページ）を参照してください。

- フロー 4（F4）およびフロー 5（F5）の Operation, Administration, and Maintenance（OAM; 運用管理および保守）セル。詳細については、OAM について （3070 ページ）を参照してください。

Security Manager では、特定の PVC で ILMI をイネーブルまたはディセーブルにし、F5 OAM 機能を設定できます。

関連項目

- 仮想パスおよび仮想チャネルについて （3066 ページ）
- ATM サービス クラスについて （3067 ページ）
- ATM PVC の定義 （3071 ページ）
- ATM PVC での OAM 管理の定義 （3074 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ILMI について

Integrated Local Management Interface（ILMI; 統合ローカル管理インターフェイス）は、ATM インターフェイスで物理層、ATM レイヤ、仮想パス、および仮想回線パラメータを設定およびキャプチャするためのプロトコルとして、ATM フォーラムが定義したものです。ILMI を使用すると、デバイスが物理リンクの反対側にあるコンポーネントのステータスを判断し、動作パラメータの共通セットをネゴシエートして相互運用性を確保できるようになるため、ネットワーク全体での自動設定が容易になります。Private Network to Network Interface（PNNI; プライベート ネットワーク間インターフェイス）と IISP（Interim-Interswitch Signaling Protocol）という ATM ルーティング プロトコルは、この情報を使用して、ATM スイッチ ルータを検出し、それらを相互接続したネットワークを構築します。

2 つの ATM インターフェイスが ILMI プロトコルを実行すると、互いに物理的な接続で ILMI パケットを交換します。このようなパケットは、484 オクテットの大きさの SNMP メッセージで構成されています。ATM インターフェイスは、このようなメッセージを ATM アダプテーション レイヤ 5（AAL5）トレーラにカプセル化し、パケットをセルにセグメント化し、セル伝送をスケジューリングします。ATM インターフェイスは、相手先固定接続（PVC）自動検出などのネットワーク機能で SNMP オブジェクト ID を使用します。特に、Digital Subscriber Line（DSL; デジタル加入者線）アプリケーションで便利です。

ILMI は、管理対象オブジェクトを管理情報ベース（MIB）に編成します。リンク管理用のものなどがあります。この MIB には、各 ATM インターフェイスで使用される次のオブジェクト グループが含まれています。

- 物理層：ILMI 4.0 が、物理層 ILMI 値を中断または「廃止」し、標準のインターフェイス MIB（RFC 1213）を使用することを指定します。
- ATM レイヤ：ATM セル ヘッダーの VPI 値および VCI 値に使用可能なビット数、許可された Virtual Path Connection（VPC; 仮想パス接続）および Virtual Channel Connection（VCC; 仮想チャネル接続）の最大数、設定した PVC の数などを示します。

- 仮想パス接続：VPC のアップ/ダウン ステータスとその Quality of Service（QoS）パラメータを示します。
- 仮想チャネル接続：VCC のアップ/ダウン ステータスとその QoS パラメータを示します。

管理者は任意に ILMI をイネーブルまたはディセーブルにできますが、イネーブルにすることを強く推奨します。ILMI がイネーブルになっていないと、ATM デバイスを正しく動作させるために ILMI が管理するパラメータの多くを手動で設定しなければならなくなります。ILMI は、VPI=X、VCI=16 の予約済み PVC で動作します。

関連項目

- ATM 管理プロトコルについて （3068 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

OAM について

Operation, Administration, and Maintenance（OAM; 運用管理および保守）機能は、ATM の障害管理およびパフォーマンス管理を実現するもので、ITU 推奨事項 I.610 に定義されている規格に基づいています。OAM は、PVC でネットワーク接続障害を検出し、問題の PVC を停止することによって障害に対応します。OAM がないと、ネットワーク接続が失われても、PVC はアップのままとなります。そのような状況では、ルーティング テーブル エントリが引き続き PVC を指しているため、パケットが失われます。

Security Manager では、F5 OAM を使用できます。これは、仮想回線（VC）レベルで動作します。OAM は、Cisco IOS ルータなどのエンド デバイスで PVC パスに沿って障害を検出するため、次のセルを使用します。

- ループバック セル：OAM 対応のルータは、通常の間隔でループバック セルを送信します。ループバック セルは、ネットワークでループします。このループ ポイントは、PVC の終端にあるマシン（エンドツーエンド ループバック セル）か、またはパス上にあるデバイス（セグメント ループバック セル）とします。ループバック セルが失敗して発信元に戻ると、障害が発生します。
- Continuity Check（CC; 連続性チェック）セル：CC セルは、OAM 対応のルータによって定期的に送信されて、リンクの整合性がチェックされます。CC セルの送信先は、エンドツーエンドにすることも、PVC の特定のセグメントに限定することもできます。アクティベーション セルおよびディアクティベーション セルは、連続性チェックを開始する場合と、一時停止する場合に使用します。接続障害があれば、特殊な SNMP 通知で報告されます。
- Alarm Indication Signal（AIS; アラーム表示信号）セル：物理層で障害が発生したときには、AIS セルがダウンストリーム デバイスに送信されて、ATM レイヤでの仮想接続障害が報告されます。PVC は、定義した数だけ AIS セルを受信したあとでダウン状態に移行し、AIS セルを追加せずに定義済みの間隔が経過するまでアップしません。
- Remote Detection Indication（RDI; リモート検出表示）セル：ダウンストリーム デバイスに接続障害を警告するために AIS セルが送信されると、ネットワークの制御とフィードバックのメカニズムが働いてアップストリームに RDI セルが送信されます。

障害が解決されるまで、障害の影響を受ける PVC 上のユーザ セルと同じ VPI/VCI を使用して、AIS/RDI セルが送信されます。

関連項目

- ATM 管理プロトコルについて （3068 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）
- ATM PVC での OAM 管理の定義 （3074 ページ）

ATM PVC の定義

ATM 相手先固定接続（PVC）を定義するには、ATM インターフェイスを選択し、次の設定を定義します。

- PVC ID。
- 使用するカプセル化のタイプ。
- この PVC で ILMI 管理がイネーブルになるかどうか。
- Inverse ARP（InARP）を使用して宛先デバイスの IP アドレスを学習するかどうか。
- PPP over Ethernet（PPPoE）および PPP over ATM（PPPoA）に関連するオプション。
- トラフィック シェーピングなどの Quality of Service（QoS）設定。
- InARP の代わりとなるスタティック IP アドレス マッピング。

ループバックや連続性チェックなど、PVC での F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）管理の定義の詳細については、 ATM PVC での OAM 管理の定義 （3074 ページ）を参照してください。

はじめる前に

- ATM over DSL を設定する場合は、ADSL ポリシー（Cisco IOS ルータでの ADSL （3049 ページ）を参照）または SHDSL ポリシー（Cisco IOS ルータでの SHDSL （3057 ページ））をすでに設定していることを確認してください。
- デバイスに ATM インターフェイスおよびサブインターフェイスが含まれていることを確認します（PVC は一般に、ATM サブインターフェイスに設定されます）。 Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）を参照してください。

（注） ATM を SHDSL 対応に設定した場合、SHDSL コントローラを定義し、ATM モードをイネーブルにすると、ATM インターフェイスが作成されます。その場合、デバイスを再検出して、ATM インターフェイスを Security Manager に追加する必要があります。 SHDSL コントローラの定義 （3058 ページ） を参照してください。

関連項目

- ATM PVC での OAM 管理の定義 （3074 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [PVC] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[PVC] ページが表示されます。このページのフィールドの説明については、表 840 : [PVC] ページ （3076 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[PVC] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 841 : [PVC] ダイアログボックス （3078 ページ）を参照してください。

ステップ 3 [インターフェイス（Interface）] フィールドに、PVC を定義する ATM インターフェイス、ATM サブインターフェイス、またはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックしてインターフェイスロールを選択するか、または新規にインターフェイスロールを作成します。

ステップ 4 ATM インターフェイスが組み込まれているデバイスまたは DSL WAN インターフェイス カードのタイプを選択します。

（注） この設定値を定義して、PVC ポリシーを適切に検証することを強く推奨します。このポリシーの設定は、ハードウェアに強く依存するためです。

ステップ 5 [PVC] ダイアログボックスの [Settings] タブで、PVC の基本的な設定を定義します。

a) VPI/VCI 識別子を入力します。任意でテキスト ハンドルを入力することもできます。管理 PVC を定義している場合は、[管理 PVC（ILMI）（Management PVC (ILMI)）] チェックボックスをオンにします。

（注） 2 人のユーザが同じ識別子で同時に PVC を定義しようとすると、エラーが発生します。

b) 使用する ATM カプセル化のタイプを選択します。aal5autoppp または aal5ciscoppp を選択した場合は、PPPoA に使用する仮想テンプレートを定義するか、または [Select] をクリックしてセレクタを表示する必要があります。カプセル化のタイプとして aal5mux を選択した場合は、PVC によって伝送されるプロトコルを選択する必要があります。

（注） 管理 PVC を定義するときには、カプセル化のタイプを選択しないでください。

（注） 既存の PVC の仮想テンプレート設定を修正する場合は、ATM サブインターフェイスで **shutdown** コマンドに続けて **no shutdown** コマンドを入力して、インターフェイスを再起動する必要があります。これにより、新規に設定したパラメータが有効になります。

c) ILMI でこの PVC を管理するには、[Enable ILMI] チェックボックスをオンにします。詳細については、ILMI について （3069 ページ）を参照してください。

（注） サブインターフェイスには、管理 PVC を設定できません。

d) トラフィックをそのようなデバイスに転送するのに必要なレイヤ 3 アドレスを PVC で動的に学習するには、[Inverse ARP] チェックボックスをオンにします。

（注） このほか、ステップ 7 （3073 ページ）の説明に従って、スタティック アドレス マッピングを作成する方法もあります。

e) [PPPoE Max Sessions] フィールドに、PVC で許可されている PPPoE セッションの最大数を定義します。

f) [VPN Service Name] フィールドに、PVC での PPPoA セッションに使用するスタティック ドメイン名を定義します。

[設定（Settings）] タブのフィールドの説明については、表 842 : [PVC] ダイアログボックス - [Settings] タブ （3079 ページ）を参照してください。

ステップ 6 （任意）[PVC] ダイアログボックスの [QoS] タブで、この PVC によって伝送されるトラフィックで実行する ATM トラフィック シェーピングのタイプを定義します。トラフィック シェーピングは、定義されたビット レートを超えるトラフィックをキューに入れて、PVC によって伝送されるトラフィックのフローを規制します。[QoS] タブのフィールドの説明については、表 843 : [PVC] ダイアログボックス - [QoS] タブ （3083 ページ）を参照してください。

ステップ 7 （任意）[PVC] ダイアログボックスの [Protocol] タブで、PVC の反対側にある IP アドレス用にスタティック マッピングを作成します。

a) [追加（Add）] をクリックして、[マッピングの定義（Define Mapping）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 845 : [Define Mapping] ダイアログボックス （3088 ページ）を参照してください。

b) IP アドレスを選択し、マッピングするアドレスまたはネットワーク/ホストオブジェクトを入力します。あるいは、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新規のネットワーク/ホストオブジェクトを作成します。

c) [OK] をクリックスタティック マッピングが、[Protocol] タブに表示されます。

d) 7.a （3073 ページ）～7.c （3073 ページ）を繰り返して、他のスタティック マッピングを定義します。

（注） [Protocol] タブではこのほか、使用する InARP のタイプをブロードキャストまたは非ブロードキャストに変更することもできます。

ステップ 8 [詳細設定（Advanced）] をクリックして、PVC での OAM 管理を設定します。ATM PVC での OAM 管理の定義 （3074 ページ）を参照してください。

ステップ 9 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[PVC] テーブルに表示されます。

（注） PVC を編集するには、テーブルから目的の PVC を選択し、[編集（Edit）] をクリックします。PVC を削除するには、目的の PVC を選択し、[削除（Delete）] をクリックします。

ステップ 10 ステップ 2 （3072 ページ）～ステップ 9 （3073 ページ）を繰り返して、他の PVC を定義します。

ATM PVC での OAM 管理の定義

Security Manager では、次の F5（VC レベル）の Operation, Administration, and Maintenance（OAM; 運用管理および保守）セルを設定して、Cisco IOS ルータで PVC 障害を検出できます。

- ループバック セル
- 連続性チェック（CC）セル
- アラーム表示信号（AIS）セル
- リモート検出表示（RDI）セル

このようなセル タイプを個別にイネーブルおよびディセーブルにできます。また、障害が検出されたときに、各セル タイプが PVC にどのように影響を与えるかを左右する設定を定義できます。

はじめる前に

- PVC が定義されている ATM インターフェイスを選択します。
- PVC の一般的な設定および QoS 設定を定義します。ATM PVC の定義 （3071 ページ） を参照してください。

関連項目

- ATM PVC の定義 （3071 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）

ステップ 1 [PVC] ダイアログボックスで、[詳細設定（Advanced）] をクリックして [PVC の詳細設定（PVC Advanced Settings）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 846 : [PVC Advanced Settings] ダイアログボックス （3089 ページ）を参照してください。

ステップ 2 選択した PVC で OAM ループバック セルをイネーブルにします。

a) [OAM-PVC] タブをクリックします。このタブのフィールドの説明については、表 848 : [PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ （3092 ページ）を参照してください。

b) [OAM 管理の有効化（Enable OAM Management）] チェックボックスをオンにします。

c) ループバック セル伝送の頻度を定義します。

ステップ 3 （任意）PVC でセグメント CC セルをイネーブルにします。

a) [セグメント連続性チェック（Segment Continuity Check）] で、[連続性チェックの設定（Configure Continuity Check）] を選択します。

b) ルータがシンク、ソース、あるいはその両方として機能するのかを選択します。これにより、CC セルの送信方向が決まります。

c) セグメント障害またはエンドツーエンド障害が検出されても、PVC はアップしたままとするかどうかを選択します。

（注） [アクティベーション要求を拒否（Deny Activation Requests）] を選択すると、ルータはピアから受信した CC アクティベーション要求を拒否します。

ステップ 4 （任意）セグメント CC セル向けにステップ 3 （3074 ページ）で説明している手順に従って、PVC でエンドツーエンド CC セルをイネーブルにします。

ステップ 5 （任意）他のループバック セル パラメータを設定します。

a) [OAM] タブをクリックします。

b) [OAM 再試行の有効化（Enable OAM Retry）] チェックボックスをオンにし、ダウンカウント、アップカウント、および再試行頻度を定義します。使用可能なオプションの説明については、表 847 : [PVC Advanced Settings] ダイアログボックス - [OAM] タブ （3090 ページ）を参照してください。

ステップ 6 （任意）他の CC セル パラメータを設定します。

a) セグメント CC セルの [有効化（Enable）] チェックボックスをオンにし、アクティベーションカウント、ディアクティベーション カウント、および再試行頻度を定義します。これらのフィールドによって、ピアに送信されるアクティベーション要求とディアクティベーション要求の数、およびルータの試行間隔が決まります。使用可能なオプションの説明については、表 847 : [PVC Advanced Settings] ダイアログボックス - [OAM] タブ （3090 ページ）を参照してください。

b) エンドツーエンド CC セルについても6.a （3075 ページ）を繰り返します。

ステップ 7 （任意）PVC で AIS/RDI セルを設定します。

a) [OAM] タブで、[AIS-RDI 検出の有効化（Enable AIS-RDI Detection）] チェックボックスをオンにします。

b) PVC がダウン状態に移行するために必要な AIS/RDI セルの数を定義します。

c) どのくらいの時間 AIS/RDI セルを受信しなければ PVC がアップ状態に移行できるかを秒単位で定義します。

ステップ 8 [OK] をクリックして、ダイアログボックスを閉じ、[PVC] ダイアログボックスに戻ります。

[PVC] ポリシー ページ

[PVC] ページは、ルータで Permanent Virtual Connection（PVC; 相手先固定接続）を作成、編集、および削除する場合に使用します。PVC では、リース回線に似たサービスを提供するためにサイト間に直接および永続的な接続を確立できます。このような PVC は、ADSL、SHDSL、または基本的な ATM 環境に使用できます。詳細については、ATM PVC の定義 （3071 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [インターフェイス（Interfaces）] > [設定（Settings）] > [PVC] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルーターインターフェイス（Router Interfaces）] > [設定（Settings）] > [PVC] を選択します。[PVC] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [ADSL] ポリシー ページ （3053 ページ）
- [SHDSL] ポリシー ページ （3059 ページ）
- Cisco IOS ルータでの PVC （3065 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *840 : [PVC]* ページ

要素	説明
ATM インターフェイス	PVC が定義されている ATM インターフェイス。
インターフェイス カード	ATM インターフェイスが存在するデバイスまたは WAN インターフェイス カードのタイプ。
PVC ID	PVC の Virtual Path Identifier（VPI; 仮想パス識別子）および Virtual Channel Identifier（VCI; 仮想チャネル識別子）。
設定	カプセル化、PPPoE セッションの数、VPN サービス名など、PVC 用のその他の設定。
QoS	トラフィック シェーピングなど、PVC に対して定義する QoS 設定。
プロトコル	PVC 用に設定される IP プロトコル マッピング（スタティック マップまたは Inverse ARP）。
OAM	PVC 用に設定される F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）ループバック、連続性チェック、および AIS/RDI 定義。
OAM-PVC	PVC 用に設定される OAM 管理セル。
[追加（Add）] ボタン	[PVC] ダイアログボックス （3077 ページ）が開きます。ここから、PVC を定義できます。
[編集（Edit）] ボタン	[PVC] ダイアログボックス （3077 ページ）が開きます。ここから、選択した PVC を編集できます。
[削除（Delete）] ボタン	選択した PVC をテーブルから削除します。

[PVC] ダイアログボックス

[PVC] ダイアログボックスは、ATM Permanent Virtual Circuit（PVC; 相手先固定接続）を設定する場合に使用します

次のインターフェイス カード タイプを設定できます。

- [Unknown]：インターフェイス カード タイプは定義されません。
- [WIC-1ADSL]：ADSL over POTS（通常の電話回線）を提供する 1 ポート ADSL WAN インターフェイス カード。
- [WIC-1ADSL-I-DG]：Dying Gasp サポートのある ADSL over ISDN を提供する 1 ポート ADSL WAN インターフェイス カード（Dying Gasp を使用すると、ルータは、ルータの電力が失われかけているときに、差し迫った回線ドロップを DSLAM に警告します）。
- [WIC-1ADSL-DG]：Dying Gasp サポートのある ADSL over POTS を提供する 1 ポート ADSL WAN インターフェイス カード。
- [HWIC-1ADSL]：ADSL over POTS を提供する 1 ポート高速 ADSL WAN インターフェイス カード。
- [HWIC-1ADSLI]：ADSL over ISDN を提供する 1 ポート高速 ADSL WAN インターフェイス カード。
- [HWIC-ADSL-B/ST]：バックアップのために ISDN BRI ポートに ADSL over POTS を提供する 2 ポート高速 ADSL WAN インターフェイス カード。
- [HWIC-ADSLI-B/ST]：バックアップのために ISDN BRI ポートに ADSL over ISDN を提供する 2 ポート高速 ADSL WAN インターフェイス カード。
- [WIC-1-SHDSL-V2]：2 線式モードおよび拡張 4 線式モードに対応した、1 ポート複数回線 G.SHDSL WAN インターフェイス カード。
- [WIC-1-SHDSL-V3]：2 線式モードおよび 4 線式モード（標準および拡張）に対応した、1 ポート複数回線 G.SHDSL WAN インターフェイス カード。
- [NM-1A-T3]：T3 リンクを備えた 1 ポート ATM ネットワーク モジュール。
- [NM-1A-OC3-POM]：光信号レベル 3（OC-3）リンクおよび 3 つの動作モード（マルチモード、Single-Mode Intermediate Reach（SMIR; シングルモード中距離）、および Single-Mode Long-Reach（SMLR; シングルモード長距離））に対応した、1 ポート ATM ネットワーク モジュール。
- [NM-1A-E3]：E3 リンクを備えた 1 ポート ATM ネットワーク モジュール。
- [857 ADSL]：ADSL インターフェイスがある Cisco 857 サービス統合型ルータ。
- [876 ADSL]：ADSL インターフェイスがある Cisco 876 サービス統合型ルータ。
- [877 ADSL]：ADSL インターフェイスがある Cisco 877 サービス統合型ルータ。
- [878 888 G.SHDSL]：G.SHDSL インターフェイスがある Cisco 878 サービス統合型ルータ。

- [1801 ADSLoPOTS]：ADSL over POTS を提供する Cisco 1801 サービス統合型ルータ。
- [1802 ADSLoISDN]：ADSL over ISDN を提供する Cisco 1802 サービス統合型ルータ。
- [1803 G.SHDSL]：4 線式 G.SHDSL を提供する Cisco 1803 サービス統合型ルータ。

ナビゲーション パス

[PVC] ポリシー ページ （3075 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- ATM PVC の定義 （3071 ページ）

フィールド リファレンス

表 *841 : [PVC]* ダイアログボックス

要素	説明
ATM インターフェイス	PVC が定義されている ATM インターフェイス。インターフェイス、サブインターフェイス、またはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしていずれかを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） インターフェイス ロールを定義するときには、同じインターフェイス カードからの ATM インターフェイスだけを含めることを強く推奨します。各カードタイプでサポートされている設定が異なると、展開に失敗することがあります。
インターフェイス カード	ルータに組み込まれている WAN インターフェイス カードのタイプ、またはルータ タイプ。サポートされるカード タイプは上記のとおりです。 （注） ポリシーを適切に検証するために、このフィールドに値を定義することを強く推奨します。ライブ デバイスを検出したときは、正しいインターフェイス カード タイプがすでに表示されています。ライブデバイスで検出を実行しなかった場合、または Cisco Security Manager がデバイスに取り付けられているインターフェイスカードのタイプを検出できない場合、このフィールドに「Unknown」と表示されます。
[設定（Settings）] タブ	VPI/VCI やカプセル化など、基本的な PVC 設定を定義します。[PVC] ダイアログボックス - [Settings] タブ （3079 ページ）を参照してください。
[QoS] タブ	ATM トラフィック シェーピングをはじめ、PVC のその他の QoS 設定を定義します。[PVC] ダイアログボックス - [QoS] タブ （3082 ページ）を参照してください。

要素	説明
[Protocol] タブ	PVC 用に設定される IP プロトコル マッピングを定義します（スタティック マップまたは Inverse ARP）。[PVC] ダイアログボックス - [Protocol] タブ （3086 ページ）を参照してください。
[Advanced] ボタン	PVC の F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）設定を定義します。[PVC Advanced Settings] ダイアログボックス - [OAM] タブ （3089 ページ） を参照してください。

[PVC] ダイアログボックス - [Settings] タブ

[PVC] ダイアログボックスの [Settings] タブは、PVC の基本的な設定を設定する場合に使用します。

- ID 設定。
- カプセル化設定。
- ILMI および Inverse ARP が有効になるかどうか。
- PPPoE セッションの最大数。
- PPPoA に使用するスタティック ドメイン（VPN サービス）名。

ナビゲーション パス

[PVC] ダイアログボックス （3077 ページ）に移動し、[設定（Settings）] タブをクリックします。

関連項目

- [PVC] ダイアログボックス - [QoS] タブ （3082 ページ）
- [PVC] ダイアログボックス - [Protocol] タブ （3086 ページ）
- [PVC Advanced Settings] ダイアログボックス （3088 ページ）
- ATM PVC の定義 （3071 ページ）

フィールド リファレンス

表 842 : [PVC] ダイアログボックス - [Settings] タブ

要素	説明
PVC ID 設定	

要素	説明
VPI	PVC の仮想パス識別子。VCI と組み合わせて、セルの次の宛先を特定します。この組み合わせは、宛先に至るまでに存在する一連の ATM スイッチを通過します。ほぼどのプラットフォームでも有効値の範囲は 0 ～ 255 です。 Inverse Multiplexing over ATM（IMA; ATM の逆多重化）を使用する Cisco 2600 および 3600 シリーズ ルータの場合、有効値の範囲は 0 ～ 15、64 ～ 79、128 ～ 143、および 192 ～ 207 です。 （注） VPI/VCI 値は、選択したインターフェイスに設定されているすべての PVC で一意である必要があります。VPI/VCI 値は、単一のリンクに対してだけ一意であり、セルが ATM ネットワークを通過するときに変化することがあります。
VCI	PVC の 16 ビット仮想チャネル識別子。VPI と組み合わせて、セルの次の宛先を特定します。この組み合わせは、宛先に至るまでに存在する一連の ATM スイッチを通過します。有効な値は、プラットフォームによって異なります。一般に、最大 31 までの値は、特殊なトラフィック（ILMI など）用に予約されているため、使用しないでください。3 および 4 は無効です。 （注） VPI/VCI 値は、選択したインターフェイスに設定されているすべての PVC で一意である必要があります。VPI/VCI 値は、単一のリンクに対してだけ一意であり、セルが ATM ネットワークを通過するときに変化することがあります。
ハンドル	PVC を識別するために任意で指定する名前。最大長は 15 文字です。
Management PVC (ILMI)	サブインターフェイスに PVC を設定する場合には適用されません。 選択されている場合、Interim Local Management Interface（ILMI; 暫定ローカル管理インターフェイス）との通信がイネーブルになって、この PVC はこの ATM インターフェイスの管理 PVC となります。ILMI は、ATM インターフェイスで物理層、ATM レイヤ、仮想パス、および仮想回線パラメータを設定およびキャプチャするためのプロトコルとして、ATM フォーラムが定義したものです。ILMI について （3069 ページ）を参照してください。 選択解除されている場合、この PVC は管理 PVC として機能しません。これがデフォルトです。 （注） 管理 PVC の VPI/VCI は、一般に 0/16 に設定されます。
カプセル化設定	

要素	説明
タイプ（Type）	[Management PVC (ILMI)] チェックボックスがオンになっているときには適用されません。 PVC で使用する ATM Adaptation Layer（AAL; ATM アダプテーション レイヤ）およびカプセル化のタイプ。 • [blank]：カプセル化のタイプは定義されません（展開時に aal5snap が適用されます）。 • [aal2]：AAL2 Voice over ATM 専用の PVC。AAL2 は、Variable Bit Rate（VBR; 可変ビット レート）トラフィックに使用されます。リアルタイム（VBR-RT）とすることも、非リアルタイム（VBR-NRT）とすることもできます。 • [aal5autoppp]：ルータは、着信 PPP over ATM（PPPoA）と PPP over Ethernet（PPPoE）セッションとを区別し、要求に応じて両方の PPP タイプの仮想アクセスを確立します。 • [aal5ciscoppp]：Cisco 独自の PPP over ATM 用。 • [aal5mux]：[Protocol] フィールドでの定義に従って、PVC を単一のプロトコル専用にします。 • [aal5nlpid]：ATM インターフェイスは、ATM Data Service Unit（ADSU; ATM データ サービス ユニット）を使用し、かつ ATM-Data Exchange Interface（DXI; データ交換インターフェイス）を実行している High-Speed Serial Interface（HSSI）と連携して動作できるようになります。 • [aal5snap]：Inverse ARP をサポートし、プロトコル データグラムの前にある Logical Link Control/Subnetwork Access Protocol（LLC; 論理リンク制御/SNAP; サブネットワーク アクセス プロトコル）を組み込みます。これにより、複数のプロトコルが同じ PVC を通過できます。
Virtual Template	この PVC で PPP over ATM に使用される仮想テンプレート。仮想テンプレート インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックして仮想テンプレート インターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 ユーザがダイヤルインすると、仮想テンプレートを使用して仮想アクセス インターフェイスが設定されます。ユーザがダイヤルアウトすると、仮想アクセス インターフェイスがダウンし、他のダイヤルインユーザのためにリソースが解放されます。 （注） 既存の PVC の仮想テンプレート設定を修正する場合は、ATM サブインターフェイスで shutdown コマンドに続けて no shutdown コマンドを入力して、インターフェイスを再起動する必要があります。これにより、新規に設定したパラメータが有効になります。

要素	説明
プロトコル	aal5mux がカプセル化のタイプとして定義されたときにだけ適用されます。 MUX カプセル化 PVC によって伝送されるプロトコル。 • [frame-relay]：Cisco MC3810 上のフレーム リレー/ATM ネットワーク インターワーキング（FRF.5）。 • [fr-atm-srv]：Cisco MC3810 上のフレーム リレー/ATM サービス インターワーキング（FRF.8）。 • [ip]：IP プロトコル。 • [ppp]：IETF 準拠の PPP over ATM。このプロトコル タイプを使用するときには、仮想テンプレートを指定する必要があります。 • [voice]：Voice over ATM。
その他の設定	
Enable ILMI	選択されている場合、この PVC で ILMI 管理がイネーブルになります。 選択解除されている場合、この PVC で ILMI 管理がディセーブルになります。
Inverse ARP	選択されている場合、PVC で Inverse Address Resolution Protocol（Inverse ARP）がイネーブルになります。 選択解除されている場合、Inverse ARP がディセーブルになります。これがデフォルトです。 Inverse ARP は、確立済み接続のリモート エンドでレイヤ 3 アドレスを学習する場合に使用します。仮想回線を使用するには、事前にこのようなアドレスを学習する必要があります。 （注） [Protocol] タブは、Inverse ARP を使用してアドレスを動的に学習するのではなく、IP アドレスのスタティック マッピングを定義する場合に使用します。[PVC] ダイアログボックス - [Protocol] タブ （3086 ページ）を参照してください。
PPPoE Max Sessions	PVC に許可されている PPP over Ethernet セッションの最大数。
VPN Service Name	この PVC で使用するスタティック ドメイン名。最大長は 128 文字です。 このオプションは、PPP を開始せずに、指定されたドメイン名に従って PVC の PPP over ATM（PPPoA）セッションを転送する場合に使用します。

[PVC] ダイアログボックス - [QoS] タブ

[PVC] ダイアログボックスの [QoS] タブは、ATM トラフィック シェーピングをはじめ、PVC のその他の QoS 設定を設定する場合に使用します。

- 伝送リングでパケットに課される制限。
- QoS サービス。
- ランダム検出がイネーブルになるかどうか。

これらの設定は、定義済みの許容可能なビット レートを超えるトラフィックをキューに入れて、PVC を経由するトラフィックのフローを規制します。

（注） QoS 値は、ハードウェアに強く依存します。デバイスに設定できる設定の詳細については、ルータのマニュアルを参照してください。

ナビゲーション パス

[PVC] ダイアログボックス （3077 ページ）に移動し、[QoS] タブをクリックします。

関連項目

- [PVC] ダイアログボックス - [Settings] タブ （3079 ページ）
- [PVC] ダイアログボックス - [Protocol] タブ （3086 ページ）
- [PVC Advanced Settings] ダイアログボックス （3088 ページ）
- ATM PVC の定義 （3071 ページ）
- サービス品質ポリシーページ （3312 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）

フィールド リファレンス

表 *843 : [PVC]* ダイアログボックス - *[QoS]* タブ

要素	説明
Tx Ring Limit	WAN Interface Card（WIC; WAN インターフェイス カード）またはインターフェイスで伝送リングに配置できる伝送パケットの最大数。 有効な値の範囲は、[Settings] タブで選択されているインターフェイス カードのタイプによって異なります。[PVC] ダイアログボックス - [Settings] タブ （3079 ページ）を参照してください。
トラフィック シェーピング設定	

要素	説明
Traffic Shaping	PVC に定義するサービスのタイプ。 • [null]：ビット レートは定義されません。 • [ABR]：使用可能ビット レート。セルの損失または遅延の保証が必要ないアプリケーションに適したベスト エフォート型のサービス。 • [CBR]：固定ビット レート サービス。音声やビデオなど遅延に影響されやすいデータを固定レートで送信して、専用線と同じようなサービスを提供します。 • [UBR]：未指定ビット レート サービス。遅延が問題にならず、リアルタイムの応答を必要としないアプリケーションに適したベスト エフォート型のサービス。 • [UBR+]：未指定ビット レート サービス。UBR と異なり、UBR+ は保証した最小レートを維持しようとしています。 • [VBR-NRT]：可変ビット レート - 非リアルタイム サービス。バースト性がある非リアルタイムアプリケーションに適したサービス。VBR は、CBR よりも効率的で、UBR よりも信頼性が高くなっています。 • [VBR-RT]：可変ビット レート - リアルタイム サービス。バースト性があるリアルタイム アプリケーションに適したサービス。 各サービス クラスの詳細については、ATM サービス クラスについて （3067 ページ）を参照してください。
ABR	ビット レートとして [ABR] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位でのピーク セル レート。これが、ABR の最大値となります。 • [MCR]：キロビット/秒（kbps）単位での最小セル レート。これが、ABR の最小値となります。 ABR は、MCR と PCR の間で変化します。輻輳制御メカニズムによって動的に制御されます。
CBR	ビット レートとして [CBR] を選択すると、次のフィールドが表示されます。 • [Rate]：キロビット/秒（kbps）単位での PVC の固定ビット レート（平均セル レートとも呼ばれます）。CBR 用に設定された ATM VC は、必要とされるかぎり、このレートでセルを送信できます。
UBR	ビット レートとして [UBR] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位での出力のピーク セル レート。PCR を超えるセルは廃棄されることがあります。

要素	説明
UBR+	ビット レートとして [UBR+] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位での出力のピーク セル レート。PCR を超えるセルは廃棄されることがあります。 • [MCR]：キロビット/秒（kbps）単位での出力の最小保証セル レート。トラフィックは、常にこのレートで送信できます。 （注） UBR+ を使用するには、Cisco IOS ソフトウェア Release 12.4(2)XA 以降、またはバージョン 12.4(6)T 以降が必要です。
VBR-NRT	ビット レートとして [VBR-NRT] を選択すると、次のフィールドが表示されます。 • [PCR]：キロビット/秒（kbps）単位での出力のピーク セル レート。PCR を超えるセルは廃棄されることがあります。 • [SCR]：キロビット/秒（kbps）単位での出力の平均セル レート。この値は、PCR 以下である必要があり、データを損失させずにセルを送信できる最大レートとなります。 • [MBS]：出力の最大バースト セル サイズ。この値は、ペナルティなしで送信できるセルの数で、SCR よりも大きく、PCR よりも小さくなります。
VBR-RT	ビット レートとして [VBR-RT] を選択すると、次のフィールドが表示されます。 • [Peak Rate]：キロビット/秒（kbps）単位でのリアルタイム トラフィックのピーク情報レート。 • [Average Rate]：キロビット/秒（kbps）単位でのリアルタイム トラフィックの平均情報レート。この値は、ピーク レート以下である必要があります。 • [Burst]：セル数単位でのリアルタイム トラフィックのバースト サイズ。この値は、PVC がバースト トラフィックを伝送する場合に設定します。 これらの値はリアルタイム トラフィック（音声やビデオなど）とデータ トラフィックとの間のトラフィック シェーピングを設定するもので、これにより、音声コールなどのリアルタイム トラフィックが廃棄されなくなります。
IP QoS 設定	

要素	説明
Random Detect	選択されている場合、PVC で Weighted Random Early Detection（WRED; 重み付けランダム早期検出）または VIP-Distributed WRED（DWRED; VIP 分散 WRED）がイネーブルになります。 選択解除されている場合、WRED および DWRED がディセーブルになります。これがデフォルトです。 WRED はキュー管理方法の 1 つで、インターフェイスが輻輳状態になるとパケットを選択してドロップします。テール ドロップと WRED （3294 ページ） を参照してください。

[PVC] ダイアログボックス - [Protocol] タブ

[PVC] ダイアログボックスの [Protocol] タブは、PVC 用に設定されるプロトコル マッピングを追加、編集、または削除する場合に使用します。PVC ごとにスタティック マッピングまたは Inverse ARP（ブロードキャストまたは非ブロードキャスト）の両方ではなくいずれか一方を設定することもできます。

（注） IP は、ATM ネットワークのプロトコル マッピングに Security Manager がサポートする唯一のプロトコルです。管理 PVC（ILMI）にプロトコル マッピングは定義できません。

ナビゲーション パス

[PVC] ダイアログボックス （3077 ページ）に移動し、[プロトコル（Protocol）] タブをクリックします。

関連項目

- [PVC] ダイアログボックス - [Settings] タブ （3079 ページ）
- [PVC] ダイアログボックス - [QoS] タブ （3082 ページ）
- [PVC Advanced Settings] ダイアログボックス （3088 ページ）
- ATM PVC の定義 （3071 ページ）

フィールド リファレンス

表 844 : [PVC] ダイアログボックス - [Protocol] タブ

要素	説明
IP Protocol Mapping	PVC 用に設定される IP プロトコル マッピングを表示します。

要素	説明
[追加（Add）] ボタン	[Define Mapping] ダイアログボックス （3087 ページ）が開きます。ここから、IP プロトコル マッピングを定義できます。
[編集（Edit）] ボタン	[Define Mapping] ダイアログボックス （3087 ページ）が開きます。ここから、選択したマッピングを編集できます。
[削除（Delete）] ボタン	選択したマッピングをテーブルから削除します。

[Define Mapping] ダイアログボックス

[Define Mapping] ダイアログボックスは、ATM PVC で使用する IP プロトコル マッピングを設定する場合に使用します。どの IP アドレスが接続の反対側に到達可能であるかを PVC が検出するには、マッピングが必要です。マッピングは、Inverse ARP（InARP）を使用して動的に学習することも、静的に定義することもできます。スタティック マッピングは、ノードの数が少ない簡単なネットワークに最適です。

（注） Inverse ARP は、カプセル化のタイプが aal5snap である場合にだけサポートされます。[PVC] ダイアログボックス - [Settings] タブ （3079 ページ）を参照してください。

ヒント IP 以外のプロトコルのマッピングを設定するには、CLI または FlexConfig を使用します。

ナビゲーション パス

[PVC] ダイアログボックス - [Protocol] タブ （3086 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックします。

関連項目

- [PVC] ダイアログボックス （3077 ページ）
- ATM PVC の定義 （3071 ページ）

フィールド リファレンス

表 845 : [Define Mapping] ダイアログボックス

要素	説明
IP オプション	使用する IP プロトコル マッピングのタイプ。 • [IP Address]：スタティック マッピングを使用しているときには、このオプションを選択します。ネットワーク/ホストオブジェクトのアドレスまたは名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 • [InARP]：Inverse ARP。ダイナミック マッピングを使用しているときには、このオプションを選択します。これにより、PVC はスタティック マップを設定せずに独自のネットワーク アドレスを解決できます。ダイナミック マッピングは、デフォルトでは 15 分おきに期限切れになってリフレッシュされます。 （注） InARP は、aal5snap が PVC のカプセル化のタイプとして定義されたときにだけ使用できます。[PVC] ダイアログボックス - [Settings] タブ（3079 ページ）を参照してください。
Broadcast Options	IP ブロードキャスト パケット（EIGRP 更新など）の送信時に、このマップ エントリを使用するかどうかを示します。 • [Broadcast]：マップ エントリがブロードキャスト パケットに使用されます。 • [No Broadcast]：ユニキャスト パケットに対してだけマップ エントリが使用されます。 • [None]：ブロードキャスト オプションがディセーブルになります。

[PVC Advanced Settings] ダイアログボックス

[PVC Advanced Settings] ダイアログボックスは、ATM PVC に F5 Operation, Administration, and Maintenance（OAM; 運用管理および保守）機能を設定する場合に使用します。OAM を使用すると、ATM レイヤで接続障害を検出できます。

詳細については、ATM PVC での OAM 管理の定義 （3074 ページ）を参照してください。

ナビゲーション パス

[PVC] ダイアログボックス （3077 ページ）に移動し、[詳細設定（Advanced）] をクリックします。

関連項目

- [PVC] ポリシー ページ （3075 ページ）

フィールド リファレンス

表 *846 : [PVC Advanced Settings]* ダイアログボックス

要素	説明
[OAM] タブ	ループバック、接続性チェック、およびAIS/RDI設定を定義します。[PVC Advanced Settings] ダイアログボックス - [OAM] タブ （3089 ページ）を参照してください。
[OAM-PVC] タブ	PVC で OAM ループバックおよび接続性チェックをイネーブルにします。[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ （3092 ページ） を参照してください。

[PVC Advanced Settings] ダイアログボックス - [OAM] タブ

[PVC Advanced Settings] ダイアログボックスの [OAM] タブは、次の項目を定義する場合に使用します。

- PVC がダウン状態またはアップ状態に移行するループバック セル応答の数。
- PVC がダウン状態またはアップ状態に移行する Alarm Indication Signal/Remote Defect Indication（AIS; アラーム表示信号/RDI; リモート障害表示）セルの数。
- この PVC で送信されるセグメント/エンド Continuity Check（CC; 連続性チェック）アクティベーション要求およびディアクティベーション要求の数と頻度。

詳細については、 ATM PVC での OAM 管理の定義 （3074 ページ）を参照してください。

（注） このタブに定義される設定は、[OAM-PVC] タブに定義される設定によって異なります。[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ （3092 ページ）を参照してください。

ナビゲーション パス

[PVC Advanced Settings] ダイアログボックス （3088 ページ）に移動し、[OAM] タブをクリックします。

関連項目

- [PVC] ダイアログボックス （3077 ページ）

フィールド リファレンス

表 *847 : [PVC Advanced Settings]* ダイアログボックス - *[OAM]* タブ

要素	説明
再試行設定	
Enable OAM Retry	選択されている場合、OAM 管理設定を定義できます。 選択解除されている場合、OAM 管理設定を定義できません。 （注） [OAM-PVC] タブで [Enable OAM Management] を選択しないと、これらの設定はデバイス設定に保存されますが、適用はされません。
Down Count	エンドツーエンド ループバック セル応答を連続していくつ受信しなかった場合に、PVC がダウン状態に移行するかを示す値。デフォルトは 3 です。
Up Count	連続していくつのエンドツーエンド ループバック セル応答を受信した場合に、PVC がアップ状態に移行するかを示す値。デフォルトは 5 です。
再試行の頻度（Retry Frequency）	秒単位でのループバック セル検証の伝送間隔。デフォルト値は 1 秒です。 PVC がアップ状態で、ループバック セル応答が（[PVC-OAM] タブの [Frequency] フィールドで定義されている）指定の間隔内に受信されなかった場合は、ここに定義された頻度でループバック セルが送信され、PVC がダウンしているかどうかが確認されます。連続して応答を受信しないセルの数が定義済みのダウン カウントに一致すると、PVC はダウン状態に移行します。
AIS-RDI 設定	
Enable AIS-RDI Detection	選択されている場合、Alarm Indication Signal（AIS; アラーム表示信号）セルおよび Remote Defect Indication（RDI; リモート障害表示）セルを使用して、PVC の ATM レイヤで発生した接続障害が報告されます。 選択解除されている場合、AIS/RDI セルがディセーブルになります。 AIS セルは、ダウンストリーム デバイスに接続障害を通知します。最後の ATM スイッチが、元の障害通知を送信したデバイスに至るアップストリーム方向に RDI セルを生成します。
Down Count	AIS/RDI セルがいくつ連続すると PVC のダウンを引き起こすかを示す値。有効値の範囲は 1 ～ 60 です。デフォルトは 1 です。
Up Count	AIS/RDI セルを受信しない場合に、PVC がアップするまでの秒数。有効値の範囲は、3 ～ 60 秒です。デフォルトは 3 です。

要素	説明
セグメント連続性チェック設定	
Enable Segment Continuity Check	選択されている場合、OAM F5 Continuity Check（CC; 連続性チェック）アクティベーション要求およびディアクティベーション要求がセグメントの反対側にあるデバイスに送信されます。 選択解除されている場合、セグメント CC アクティベーションおよびディアクティベーション要求はディセーブルになります。 （注） [OAM-PVC] タブで [Configure Continuity Check] が選択解除されている場合、これらの設定はデバイス設定に保存されますが、適用はされません。
Activation Count	確認応答の受信前にアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
Deactivation Count	確認応答の受信前にディアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
再試行の頻度（Retry Frequency）	アクティベーション/ディアクティベーションの再試行間隔（秒単位）。デフォルトは 30 秒です。
エンドツーエンド連続性チェック設定	
Enable End-to-End Continuity Check	選択されている場合、OAM F5 Continuity Check（CC; 連続性チェック）アクティベーション要求およびディアクティベーション要求が PVC の反対側にあるデバイスに送信されます。 選択解除されている場合、セグメント CC アクティベーションおよびディアクティベーション要求はディセーブルになります。 （注） [OAM-PVC] タブで [Configure Continuity Check] が選択解除されている場合、これらの設定はデバイス設定に保存されますが、適用はされません。
Activation Count	確認応答の受信前にアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
Deactivation Count	確認応答の受信前にディアクティベーション要求が送信される最大回数。有効値の範囲は 3 ～ 600 です。デフォルトは 3 です。
再試行の頻度（Retry Frequency）	アクティベーション/ディアクティベーションの再試行間隔（秒単位）。デフォルトは 30 秒です。

[PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ

[PVC Advanced Settings] ダイアログボックスの [OAM-PVC] タブは、PVC でループバック セルおよびConnectivity Check（CC; 接続性チェック）をイネーブルにする場合に使用します。その機能により、仮想接続の接続がテストされます。

詳細については、 ATM PVC での OAM 管理の定義 （3074 ページ）を参照してください。

（注） [OAM] タブでは、このタブの設定に関連する他の設定を定義できます。 [PVC Advanced Settings] ダイアログボックス - [OAM] タブ （3089 ページ）を参照してください。

ナビゲーション パス

[PVC Advanced Settings] ダイアログボックス （3088 ページ）に移動し、[OAM-PVC] タブをクリックします。

関連項目

- [PVC] ダイアログボックス （3077 ページ）

フィールド リファレンス

表 848 : [PVC Advanced Settings] ダイアログボックス - [OAM-PVC] タブ

要素	説明
OAM 設定	
[Enable OAM Management]	選択されている場合、PVC で OAM ループバック セル生成および OAM 管理がイネーブルになります。 選択解除されている場合、OAM ループバック セルおよび OAM 管理がディセーブルになります。ただし、連続性チェックは引き続き実行できます。
周波数（Frequency）	ループバック セルの伝送間隔。有効値の範囲は、0 ～ 600 秒です。
セグメント連続性チェック設定	

要素	説明
Segment Continuity Check	PVC セグメントで実行される OAM F5 連続性チェックの現在の設定。 • [None]：セグメント Continuity Check（CC; 連続性チェック）がディセーブルになります。 • [Deny Activation Requests]：PVC は、ピア デバイスからのアクティベーション要求を拒否します。これにより、OAM F5 CC 管理は PVC でアクティブにならなくなります。 • [Configure Continuity Check]：PVC でセグメント CC がイネーブルになります。CC 管理が設定されているルータは、CC アクティベーション要求をセグメントの反対側にあるルータに送信し、そのルータに対してソースまたはシンクとして機能するように指示します。 ルータと第 1 ホップ ATM スイッチとの間にある PVC セグメントで、セグメント CC が実行されます。
方向	CC 管理がイネーブルになっている場合にだけ適用されます。 CC セルが送信される方向。 • [both]：CC セルは両方向に送信されます。 • [sink]：CC セルは、CC アクティベーション要求を開始したルータの方向に送信されます。 • [source]：CC セルは、CC アクティベーション要求を開始したルータの方向から送信されます。
Keep VC up after segment failure	選択されている場合は、CC セルが接続の障害を検出した場合でも PVC はアップ状態のままになります。 選択解除されている場合は、CC セルが接続の障害を検出した場合に PVC がダウンします。
Keep VC up after end-to-end failure	選択されている場合、エンド CC 障害またはループバック障害が発生したために AIS/RDI セルを受信しても、PVC はダウンしません。 選択解除されている場合、エンド CC 障害またはループバック障害が発生した場合には、PVC がダウンします。
エンドツーエンド連続性チェック設定	

要素	説明
End-to-End Continuity Check	PVC で実行される OAM F5 エンドツーエンド連続性チェックの現在の設定。 • [None]：エンドツーエンド Continuity Check（CC; 連続性チェック）がディセーブルになります。 • [Deny Activation Requests]：PVC は、ピア デバイスからのアクティベーション要求を拒否します。これにより、OAM F5 CC 管理は PVC でアクティブにならなくなります。 • [Configure Continuity Check]：PVC でエンドツーエンド CC がイネーブルになります。CC 管理が設定されているルータは、CC アクティベーション要求を接続の反対側にあるルータに送信し、そのルータに対してソースまたはシンクとして機能するように指示します。 2 台の ATM 端末間にある PVC 全体で、エンドツーエンド CC モニタリングが実行されます。
方向	CC 管理がイネーブルになっている場合にだけ適用されます。 CC セルが送信される方向。 • [both]：CC セルは両方向に送信されます。 • [sink]：CC セルは、CC アクティベーション要求を開始したルータの方向に送信されます。 • [source]：CC セルは、CC アクティベーション要求を開始したルータの方向から送信されます。
Keep VC up after end-to-end failure	選択されている場合は、CC セルが接続の障害を検出した場合でも PVC はアップ状態のままになります。 選択解除されている場合は、CC セルが接続の障害を検出した場合に PVC がダウンします。
Keep VC up after segment failure	選択されている場合、セグメント CC 障害が発生したために AIS/RDI セルを受信しても、PVC はダウンしません。 選択解除されている場合、セグメント CC 障害が発生した場合には、PVC がダウンします。

Cisco IOS ルータでの PPP

Point-to-Point Protocol（PPP）は、RFC 1661 で規定されているように、物理リンクまたは論理リンクを使用して、2 つのデバイスまたはホスト間でパケットを転送するための手段となるも

のです。PPP は、IP、IPX、AppleTalk など複数のレイヤ 3 ネットワーク層プロトコルと連携して動作できるレイヤ 2 データリンク プロトコルです。

PPP は、次に挙げるようなよくあるシナリオに使用されます。

- ダイヤルイン接続でリモート ユーザを中央のネットワークに接続する。
- インターネットにアクセスするため、企業ネットワークのゲートウェイを ISP に接続する。
- 2 つの LAN（たとえば、本社と支社）を接続して両者間でデータを交換する。

PPP 接続は、段階的に確立されます。

1. まず、Link Control Protocol（LCP; リンク コントロール プロトコル）が、データリンク接続を確立、設定、およびテストします。
2. （任意）認証により、両当事者のアイデンティティが検証されます。
3. Network Control Protocol（NCP; ネットワーク コントロール プロトコル）のファミリが、必要なネットワーク層プロトコルを確立し、設定します。

Security Manager の PPP ポリシーを使用すると、LCP 段階で 2 つのノード間でネゴシエートされるパラメータを選択し、設定できます。このようなパラメータには、認証（一般に CHAP または PAP）や Multilink PPP（MLP; マルチリンク PPP）などがあります。MLP の詳細については、マルチリンク PPP バンドルの定義 （3099 ページ）を参照してください。

ここでは、Cisco IOS ルータ上に PPP ポリシーを作成するために実行するタスクについて説明します。

- PPP 接続の定義 （3096 ページ）
- マルチリンク PPP バンドルの定義 （3099 ページ）

マルチリンク PPP（MLP）について

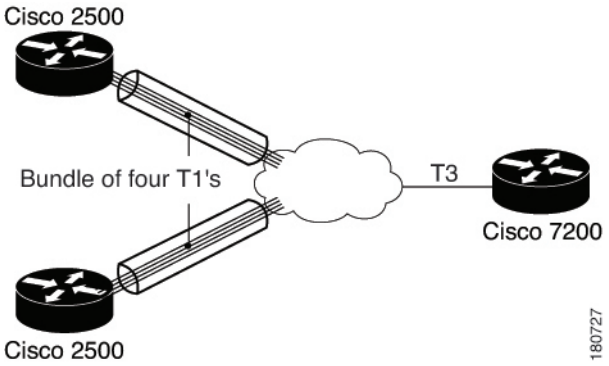
MLP は、RFC 1990 で規定されているように、複数の論理データ リンクでデータグラムを分割、再結合、および順序付けるための手段となるものです。MLP は、元々 ISDN で複数のベアラ チャネルを利用するために設計されたものですが、非同期リンクなど複数の PPP リンクが 2 つのシステムを接続するときにも使用できます。

MLP は、インバウンド トラフィックとアウトバウンド トラフィックを複数の物理的な WAN リンク（まとめてバンドルと呼ばれる）分散させます。これには、次の利点があります。

- パケットのフラグメンテーションと再構成
- 適切な順序付け
- マルチベンダーの相互運用性
- Load balancing

図 48 : マルチリンク PPP （3096 ページ）に示すように、MLP リンクにルーティングされるトラフィックがフラグメント化され、そのフラグメントがそれぞれ異なる物理リンクで送信されます。リンクのリモート エンドで、フラグメントが再構築され、最終宛先に至るネクスト ホップに転送されます。MLP では、複数の物理リンクを使用することによって、このようなリンクから得られる追加の帯域幅を一時的に使用できます。

図 *48 : マルチリンク PPP*



どの MLP バンドルも、バンドルディレクターと呼ばれる、仮想アクセスインターフェイスである単一のインターフェイスによって制御されます。このインターフェイスは、バンドルが初めて作成されるときに、バックグラウンドで作成されます。物理インターフェイスは、バンドルディレクターによって管理されるバンドルの一部になります。バンドルはこのほか、マルチリンク インターフェイスとその関連するシリアル インターフェイスで構成されるマルチリンク グループを作成するときにも使用されます。マルチリンク グループは、静的な専用線環境でよく見られるセットアップです。

MLP は、エンドポイント識別子を使用して、パケットを送信するシステムを識別します。デフォルトでは、この識別子はルータのホスト名に基づいていますが、インターフェイスの IP アドレスまたは MAC アドレス、電話番号、ユーザ定義の文字列など他の基準に基づくこともできます。エンドポイント識別子が既存のリンクの識別子に一致する場合、新規リンクは一致したバンドルに追加されます。一致する識別子がない場合は、新規バンドルが作成されます。認証を使用している場合、一致する識別子がないか、または 2 つのノード間で認証情報が交換されるたびに、新規バンドルが確立されます。

関連項目

- マルチリンク PPP バンドルの定義 （3099 ページ）
- Cisco IOS ルータでの PPP （3094 ページ）

PPP 接続の定義

PPP 接続を定義する場合、最初に実行する手順は、PPP をイネーブルにするインターフェイスを選択することです。次のいずれかのインターフェイス タイプを選択する必要があります。

- Async

- Group-Async
- シリアル
- HSSI（High-Speed Serial Interface）
- ダイヤラ
- [BRI]、[PRI]（ISDN）
- Virtual template
- マルチリンク

次の要素には、PPP 接続を定義できません。

- サブインターフェイス。
- フレーム リレー カプセル化のあるシリアル インターフェイス。
- イーサネットまたはトンネル タイプとして定義された仮想テンプレート インターフェイス（シリアルがサポートされます）。

（注） フレーム リレー カプセル化用に設定されているシリアル インターフェイスには、PPP を設定できません。基本的なルータ インターフェイス設定の定義 （3009 ページ）を参照。

（注） 802.1x ポリシーでも使用されている仮想テンプレートに PPP を定義した場合は、展開に失敗することがあります。802.1x ポリシーの定義 （3247 ページ）を参照してください。

1 つ以上の認証プロトコルを選択し、いつ認証を実行するかを定義できます。

また、リモート セキュリティ サーバで AAA を実行するときに使用する認証と認可の方式を設定できます。すべての PPP 接続に使用するデフォルトの方式リストをデバイスに定義することも、特定の接続に適用する独自の方式リストを定義することもできます。

はじめる前に

- デバイスに PPP を設定できるインターフェイスが含まれていることを確認します。Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ） を参照してください。

関連項目

- マルチリンク PPP バンドルの定義 （3099 ページ）
- Cisco IOS ルータでの PPP （3094 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルーターインターフェイス（Router Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[PPP/MLP] ページが表示されます。このページのフィールドの説明については、[PPP/MLP] ポリシーページ （3100 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[PPP] ダイアログボックスを表示します。

ステップ 3 [インターフェイス（Interface）] フィールドに、PPP 接続を定義するインターフェイスまたはインターフェイスロールの名前を入力します。あるいは、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか新規にインターフェイスロールを作成します。

ステップ 4 （任意）[PPP] タブで、PPP 接続の認証を定義します。

a) 1 つ以上の認証プロトコルを選択します。

b) 1 つ以上の認証オプションを選択します。これらのオプションでは、認証（コールイン、コールアウト、およびコールバック）をいつ実行するか、ワンタイム パスワードを使用するかどうか、および PDSN 設定でモバイル ステーションを許可して CHAP または PAP を使用せずに Simple IP サービスおよび Mobile IP サービスを受信するかどうかを決定します。

（注） [Call Back] オプションは、コールバック時に認証をイネーブルにするだけです。デバイスにコールバック機能を設定するには、CLI または FlexConfig を使用します。

c) このタブのフィールドの説明については、[PPP] ダイアログボックス - [PPP] タブ （3104 ページ）を参照してください。

ステップ 5 （任意）リモート AAA サーバを使用して認証を実行している場合は、[Authenticate Using] フィールドで [Default List] または [Custom Method List] を選択し、[Prioritized Method List] フィールドに使用する方式を定義します。

（注） デフォルト リストを変更した場合、変更内容はそのリストを使用するデバイス上のすべての PPP 接続に影響を与えます。このフィールドを空白のままにした場合は、デバイス上のローカル データベースを使用して認証が実行されます。

ステップ 6 （任意）リモート AAA サーバを使用して認可を実行している場合は、[AAA Policy Default List] または [Custom Method List] を選択し、[Prioritized Method List] フィールドに使用する方式を定義します。

（注） [AAA Policy Default List] を選択した場合、デバイスは AAA ポリシーに定義されているデフォルトの認可方式を使用します。AAA サービスの定義 （3117 ページ）を参照してください。

ステップ 7 （任意）PAP 認証要求に応えて送信するユーザ名およびパスワードを定義します。

（注） パスワードの暗号化バージョンを入力した場合は、[暗号化（Encrypted）] チェックボックスをオンにします。

ステップ 8 （任意）ルータ独自のホスト名の代わりに、すべての CHAP チャレンジおよびレスポンスで送信する別のホスト名を定義します。

（注） パスワードの暗号化バージョンを入力した場合は、[暗号化（Encrypted）] チェックボックスをオンにします。

ステップ 9 （任意）この接続でマルチリンク PPP をイネーブルにするには、[MLP] タブをクリックします。マルチリンク PPP バンドルの定義 （3099 ページ）を参照してください。

ステップ 10 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が、[PPP] テーブルに表示されます。

（注） PPP 接続を編集するには、テーブルから目的の PVC を選択し、[編集（Edit）] をクリックします。PPP 接続を削除するには、目的の PVC を選択し、[削除（Delete）] をクリックします。

ステップ 11 他のインターフェイスで PPP 接続を定義するには、ステップ 2 （3098 ページ）～ステップ 10 （3099 ページ）を繰り返します。インターフェイスに定義できる PPP 接続は 1 つだけです。

マルチリンク PPP バンドルの定義

選択したインターフェイスで Multilink PPP（MLP; マルチリンク PPP）をイネーブルにするには、[PPP] ダイアログボックスの [Multilink] タブの最上部にあるチェックボックスをオンにします。任意で、Multiclass Multilink PPP（MCMP; マルチクラス マルチリンク PPP）をイネーブルにできます。これにより、遅延に影響されやすいトラフィックのフラグメント化とインターリーブを回避でき、その結果パケットをさらに大きなパケットのフラグメントに分散させることができます。シリアルインターフェイスを特定のバンドルに制限する場合は、そのバンドルを表すマルチリンク インターフェイスを選択できます。

また、任意で次のデフォルト設定を変更できます。

- 最大フラグメント遅延。
- MLP の使用をネゴシエートするときにルータを識別するエンドポイント識別子。
- ルータとそのピアによって許可される Maximum Receive Reconstructed Unit（MRRU）。
- First-In, First-Out（FIFO; ファーストイン ファーストアウト）キューおよび非 FIFO キューの最大キュー深度。

はじめる前に

- PPP 接続をイネーブルにするインターフェイスを選択します。

関連項目

- PPP 接続の定義 （3096 ページ）
- Cisco IOS ルータでの PPP （3094 ページ）

ステップ 1 [PPP] ダイアログボックスで、[MLP] タブをクリックします。このタブのフィールドの説明については、[PPP] ダイアログボックス - [MLP] タブ （3107 ページ）を参照してください。

ステップ 2 [マルチリンクプロトコル（MLP）を有効にする（Enable Multilink Protocol (MLP)）] チェックボックスをオンにします。

ステップ 3 （任意）次のオプションを設定します。

a) 遅延に影響されやすいトラフィックのフラグメント化を回避するために、マルチクラス機能をイネーブルにするかどうかを指定します。そのためには、遅延に影響されやすいトラフィックを通常のトラフィックとは別のクラスに配置します。

b) MLP バンドルで大きなパケットのフラグメントに対してパケットのインターリーブをイネーブルにするかどうかを指定します。

c) 物理リンクを指定のマルチリンク グループだけの加入に制限するかどうかを指定します（マルチリンク インターフェイスを選択して定義します）。リンクの反対側のピアが別のバンドルに参加しようとした場合は、接続が重大になります。

d) MLP バンドルでフラグメントを送信するために必要なデフォルトの時間を変更するかどうかを指定します。デフォルトは 30 ミリ秒です。

（注） フラグメント遅延を定義せずにインターリーブをイネーブルにした場合は、デフォルトの遅延である 30 秒が設定されます。この値は、Security Manager またはデバイス設定に表示されません。

ステップ 4 （任意）[Endpoint] で、MLP バンドルで使用されるデフォルトのエンドポイント識別子を変更します。

エンドポイント識別子は、MLP バンドルでルータを識別する場合に使用します。デフォルトのエンドポイント識別子は、グローバルに設定したホスト名か、または（使用する認証プロトコルに応じて）PAP ユーザ名か CHAP ホスト名となります。ただし、[PPP] タブで対応する値を設定した場合にかぎります。 PPP 接続の定義 （3096 ページ）を参照してください。

ステップ 5 （任意）MRRU のフィールドで、ルータ（ローカル）またはピア（リモート）が受信できるデフォルトの最大パケット サイズを変更します。

ステップ 6 （任意）FIFO キューおよび非 FIFO（QoS）キューを使用している場合、リンク送信キューのデフォルトの最大サイズを変更します。

ステップ 7 [OK] をクリックして、ダイアログボックスを閉じます。定義が、[PPP] ページに表示されます。

[PPP/MLP] ポリシー ページ

[PPP/MLP] ページは、ルータの PPP 接続を作成、編集、および削除する場合に使用します。詳細については、 PPP 接続の定義 （3096 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[インターフェイス（Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータインターフェイス（Router Interfaces）] > [設定（Settings）] > [PPP/MLP]** を選択します。[PPP/MLP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの PPP （3094 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *849 : [PPP/MLP]* ページ

要素	説明
インターフェイス（Interface）	PPP/MLP 用に設定されているインターフェイス。
認証	PPP 接続で使用される認証タイプ。
許可	PPP 接続での AAA 認可に使用される方式リスト。
マルチリンク	この PPP 接続で Multilink PPP（MLP; マルチリンク PPP）がイネーブルになるかどうかを示します。
エンドポイント（Endpoint）	ピアと MLP の使用をネゴシエートするときに使用するデフォルトのエンドポイント識別子のタイプ。
Multiclass	この PPP 接続で Multiclass Multilink PPP（MCMP; マルチクラス マルチリンク PPP）機能がイネーブルになるかどうかを示します。
グループ	物理リンクが制限されているマルチリンク グループ インターフェイスの番号。
Interleave	この PPP 接続で PPP マルチリンク インターリーブ機能がイネーブルになるかどうかを示します。
[追加（Add）] ボタン	[PPP] ダイアログボックス （3102 ページ）が開きます。ここから、PPP 接続の認証設定およびマルチリンク設定を定義できます。
[編集（Edit）] ボタン	[PPP] ダイアログボックス （3102 ページ）が開きます。ここから、選択した PPP 接続を編集できます。
[削除（Delete）] ボタン	選択した PPP 接続をテーブルから削除します。

[PPP] ダイアログボックス

[PPP] ダイアログボックスは、ルータで PPP 接続を設定する場合に使用します。PPP 接続を設定した場合は、マルチリンク パラメータを実行および定義する認証および認可のタイプを定義できます。

ナビゲーション パス

に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

-

フィールド リファレンス

表 *850 : [PPP]* ダイアログボックス

要素	説明
インターフェイス（Interface）	PPP カプセル化がイネーブルになるインターフェイス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）]をクリックしてインターフェイスまたはインターフェイスロールを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 次のインターフェイス タイプが PPP をサポートしています。 • Async • Group-Async • シリアル • HSSI（High-Speed Serial Interface） • ダイヤラ • [BRI]、[PRI]（ISDN） • Virtual template • マルチリンク 次の要素には、PPP を定義できません。 • サブインターフェイス。 • フレーム リレー カプセル化のあるシリアル インターフェイス。 • イーサネットまたはトンネル タイプとして定義された仮想テンプレート インターフェイス（シリアルがサポートされます）。 （注） インターフェイスごとに PPP 接続を 1 つだけ定義できます。 （注） 802.1x ポリシーでも使用されている仮想テンプレートに PPP を定義した場合は、展開に失敗することがあります。を参照してください。
[PPP] タブ	PPP 接続で実行する認証および認可のタイプを定義します。[PPP] ダイアログボックス - [PPP] タブ （3104 ページ）を参照してください。
[MLP] タブ	Multilink PPP（MLP; マルチリンク PPP）を使用して、複数の論理データ リンクで一連のデータグラムを分割し、再結合する方法を定義します。を参照してください。 デバイスがこの設定をサポートしていない場合には、このタブはグレーになり、開くことができません。

[PPP] ダイアログボックス - [PPP] タブ

[PPP] ダイアログボックスの [PPP] タブは、PPP 接続で実行する認証および認可のタイプを定義する場合に使用します。

ナビゲーション パス

[PPP] ダイアログボックス （3102 ページ）に移動し、[PPP] タブをクリックします。

関連項目

- [PPP] ダイアログボックス - [MLP] タブ （3107 ページ）

フィールド リファレンス

表 851 : [PPP] ダイアログボックス - [PPP] タブ

要素	説明
認証設定	
PPP のカプセル化	選択されている場合、選択したインターフェイスではPPPカプセル化がイネーブルになります。このフィールドは読み取り専用です。
プロトコル	使用する認証プロトコル。 • [CHAP]：チャレンジ ハンドシェイク認証プロトコル。 • [PAP]：パスワード認証プロトコル。 • [MS-CHAP]：Microsoft バージョンの CHAP のバージョン 1（RFC 2433）。 • [MS-CHAP-2]：Microsoft バージョンの CHAP のバージョン 2（RFC 2759）。 • [EAP]：拡張認証プロトコル。 必要に応じて 1 つ以上の認証プロトコルを選択できます。

要素	説明
オプション	使用する認証オプション。 • [Call In]：選択されている場合、着信コールで認証が実行されます。 • [Call Out]：選択されている場合、発信コールで認証が実行されます。 • [Call Back]：選択されている場合、コールバックで認証が実行されます。 • [One Time]：選択されている場合、認証にワンタイム パスワードが使用されます。ワンタイム パスワードは、各パスワードが 1 度しか使用されないため、セキュリティ強度が高いと考えられています。選択解除されている場合、ワンタイム パスワードは使用されません。 （注） ワンタイム パスワードを使用するには、AAA 認証をイネーブルにする必要があります。[AAA] ポリシー ページ （3119 ページ）を参照してください。CHAP ではワンタイム パスワードを使用できません。 • [Optional]：選択されている場合、Packet Data Serving Node（PDSN; パケット データ サービス ノード）設定のモバイル ステーションが、CHAP または PAP を使用せずに、Simple IP サービスおよび Mobile IP サービスを受信できます。 選択解除されている場合、モバイル ステーションは、CHAP または PAP を使用して、Simple IP サービスおよび Mobile IP サービスを受信する必要があります。

要素	説明
Authenticate Using	PPP 接続の AAA 認証設定。 • [PPP Default List]：PPP のユーザを認証するときに問い合わせるデフォルトの方式リストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大4つ）の名前を[優先順位付けされた方式リスト（Prioritized Method List）]フィールドに入力するか、または[選択（Select）]をクリックして目的のオブジェクトを選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 **ヒント** 1 つの PPP 接続のデフォルト リストを作成したあと、そのリストをこのデバイスの他の PPP 接続にも使用できます。 • [Prioritized Method List]：この PPP 接続だけのユーザを認証するときに問い合わせる一連の方式リストを定義します。 **（注）** ルータ上のローカルデータベースを使用して認証を実行するには、このフィールドを空白のままにします。
PAP 認証設定	
ユーザー名	PAP 認証要求で送信するユーザ名。ユーザ名は、大文字と小文字が区別されます。
パスワード	PAP 認証要求で送信するパスワード。[Confirm] フィールドにパスワードを再入力します。パスワードには、1 ～ 25 文字の大文字と小文字の英数字を使用できます。パスワードは大文字と小文字が区別されます。 ピアがルータに PAP を使用して自己認証するように要求すると、ユーザ名およびパスワードが送信されます。
Encrypted Password	選択されている場合、これは入力したパスワードがすでに暗号化されていることを示します。 選択解除されている場合、これは入力したパスワードがクリア テキストであることを示します。
CHAP 認証設定	

要素	説明
ホストネーム	デフォルトでは、ルータは自身のホスト名を使用して、ピアに対して自身の身元を明らかにします。必要に応じて、別のホスト名をすべての CHAP チャレンジおよびレスポンスに使用するホスト名として入力できます。たとえば、このフィールドを使用して、ロータリー グループのすべてのルータに共通のエイリアスを指定します。
秘密（Secret）	不明なピアから受け取った CHAP チャレンジのレスポンス値を計算するのに使用されるシークレット。[Confirm] フィールドにシークレットをもう一度入力します。
Encrypted Secret	選択されている場合、これは入力したパスワードがすでに暗号化されていることを示します。選択解除されている場合、これは入力したパスワードがクリア テキストであることを示します。
認可設定	
Authorize Using	PPP 接続の AAA 認可設定。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。 [AAA] ポリシー ページ （3119 ページ）を参照してください。 • [Prioritized Method List]：ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。上向きおよび下向き矢印を使用して、選択したサーバー グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） ルータ上のローカル データベースを使用して認可を実行するには、このフィールドを空白のままにします。

[PPP] ダイアログボックス - [MLP] タブ

[PPP] ダイアログボックスの [MLP] タブは、選択した PPP 接続の Multilink PPP（MLP; マルチリンク PPP）パラメータを定義する場合に使用します。

ナビゲーション パス

[PPP] ダイアログボックス （3102 ページ）に移動し、[MLP] タブをクリックします。

関連項目

- [PPP] ダイアログボックス （3102 ページ）

フィールド リファレンス

表 *852 : [PPP]* ダイアログボックス - *[MLP]* タブ

要素	説明
Enable Multilink PPP (MLP)	選択されている場合、この PPP 接続で MLP がイネーブルになります。 選択解除されている場合、MLP がディセーブルになります。
Allow Multiple Data Classes	選択されている場合、MLP バンドルで複数のデータ クラスがイネーブルになります。遅延に影響されやすいトラフィックがクラス 1 に配置され、インターリーブはできますが、フラグメント化はできなくなります。通常のデータ トラフィックはクラス 0 に配置され、通常のマルチリンク パケットと同じく、フラグメント化の対象となります。 選択解除されている場合、すべてのトラフィックがフラグメント化の対象となります。
Enable Interleaving of Packets Among Fragments of Larger Packets	選択されている場合、MLP バンドルで大きなパケットのフラグメントに対してパケットのインターリーブがイネーブルになります。 （注） フラグメント遅延を定義せずにインターリーブをイネーブルにした場合は、デフォルトの遅延である 30 秒が設定されます。この値は、Security Manager またはデバイス設定に表示されません。 選択解除されている場合、インターリーブがディセーブルになります。 （注） シリアルインターフェイスは、インターリーブをサポートしません。

要素	説明
Multilink Group	シリアル インターフェイス、Group-Async インターフェイス、およびマルチリンク インターフェイスにだけ適用されます。 物理リンクは、選択したマルチリンク グループインターフェイスに制限されます。マルチリンクインターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）]をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 このオプションは、一般的に静的な専用線環境で、デバイスのシリアル回線が接続されているリモートシステムが事前にわかっている場合に使用されます。 このオプションは実質的に特定のインターフェイスを特定のユーザ専用にするもので、これはそのユーザが接続されていない場合でも同じです。リンクの反対側のピアが別のバンドルに参加しようとした場合は、接続が重大になります。
Maximum Fragment Delay	MLPバンドルでフラグメントを送信するために必要な最大期間。有効値の範囲は 1 ～ 1000 ミリ秒です。 フラグメントサイズは、定義されたフラグメント遅延およびリンクの帯域幅によって決まります。 （注）　シリアル インターフェイスは、この機能をサポートしません。

要素	説明
エンドポイントタイプ	MLP バンドルでパケットを送信するときにルータが使用する識別子。 • [null]：エンドポイント識別子を使用せずに、ネゴシエーションが実施されます（CLI コマンドが生成されません）。 • [Hostname]：ルータのホスト名。このオプションは、複数のルータが認証に同じユーザ名を使用しているものの、各ルータのホスト名が異なるときに便利です。 • [IP]：定義済みの IP アドレス。ネットワーク/ホストオブジェクトのアドレスまたは名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 • [MAC]：特定のインターフェイスの MAC アドレス。インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 • [None]：エンドポイント識別子を使用せずに、ネゴシエーションが実施されます（関連する CLI コマンドは生成されますが、エンドポイント識別子は提供されません）。このオプションは、ルータの接続先であるピアが正常に動作せず、エンドポイント識別子が正しく処理されないときに役立ちます。 • [Phone]：E.164 準拠の電話番号。表示されたフィールドに番号を入力します。 • [String]：文字列。表示されたフィールドに文字列を入力します。 デフォルトのエンドポイント識別子は、グローバルに設定したホスト名か、または（使用する認証プロトコルに応じて）PAP ユーザ名か CHAP ホスト名となります。ただし、[PPP] タブで対応する値を設定した場合にかぎります。
MRRU Local Peer	ローカル ピアの Maximum Receive Reconstructed Unit（MRRU）値。この値は、ローカル ルータが受信できる最大パケット サイズとなります。 有効値の範囲は 128 ～ 16384 バイトです。デフォルトはマルチリンク グループ インターフェイスでは最大伝送単位（MTU）で、それ以外のインターフェイスでは 1524 バイトとなります。
MRRU Remote Peer	リモート ピアの Maximum Receive Reconstructed Unit（MRRU）値。この値は、リモート ルータが受信できる最大パケット サイズとなります。 有効値の範囲は 128 ～ 16384 バイトです。デフォルトは 1524 バイトです。

要素	説明
Maximum FIFO Queue Size	バンドルが First-In, First-Out（FIFO; ファーストイン ファーストアウト）キューを使用する場合の最大キュー深度。有効値の範囲は 2 ～ 255 パケットです。デフォルトは 8 です。
Maximum QoS Queue Size	バンドルが非 FIFO キューを使用する場合の最大キュー深度。有効値の範囲は 2 ～ 255 パケットです。デフォルトは 2 です。

第 63 章

ルータ デバイス管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

この章は次のトピックで構成されています。

- Cisco IOS ルータにおける AAA （3114 ページ）
- [AAA] ポリシー ページ （3119 ページ）
- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）
- [アカウントおよびログイン情報ポリシー（Accounts and Credentials Policy）] ページ （3132 ページ）
- Cisco IOS ルータにおけるブリッジング （3135 ページ）
- [Bridging] ポリシー ページ （3139 ページ）
- Cisco IOS ルータにおけるタイム ゾーン設定 （3141 ページ）
- [Clock] ポリシー ページ （3142 ページ）
- Cisco IOS ルータにおける CPU 使用率設定 （3145 ページ）
- [CPU] ポリシー ページ （3146 ページ）
- Cisco IOS ルータにおける HTTP と HTTPS （3149 ページ）
- [HTTP] ポリシー ページ （3152 ページ）
- Cisco IOS ルータにおける回線アクセス （3157 ページ）
- [Console] ポリシー ページ （3165 ページ）
- [VTY] ポリシー ページ （3177 ページ）
- Cisco IOS ルータにおける任意の SSH 設定 （3194 ページ）
- [Secure Shell] ポリシー ページ （3196 ページ）
- Cisco IOS ルータの SNMP （3198 ページ）
- [SNMP] ポリシー ページ （3201 ページ）
- Cisco IOS ルータにおける DNS （3208 ページ）
- [DNS] ポリシー ページ （3210 ページ）
- Cisco IOS ルータにおけるホスト名とドメイン名 （3212 ページ）

• [Hostname] ポリシー ページ （3213 ページ）
• Cisco IOS ルータにおけるメモリ設定 （3214 ページ）
• [Memory] ポリシー ページ （3215 ページ）
• Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）
• [Secure Device Provisioning] ポリシー ページ （3222 ページ）
• Cisco IOS ルータにおける DHCP （3224 ページ）
• [DHCP] ポリシー ページ （3230 ページ）
• Cisco IOS ルータにおける NTP （3237 ページ）
• [NTP Policy] ページ （3239 ページ）

Cisco IOS ルータにおける AAA

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張はサポートしていません。

認証、許可、アカウンティング（AAA）ネットワーク セキュリティ サービスは、Cisco IOS ルータのアクセス コントロールを設定する際に使用する主要なフレームワークを提供します。Security Manager で AAA ポリシーを使用すると、Cisco IOS ルータ上の AAA 機能をイネーブルにしたり、デフォルトの AAA 設定を指定したりできます。このポリシーで定義したデフォルト設定は、HTTP や回線アクセス（コンソールと VTY）のポリシーなど、他のポリシーで使用できます。AAA 機能をイネーブルにすることは、NAC、SDP、802.1x などの AAA を利用するデバイス ポリシーの前提条件です。

AAA の詳細については、次を参照してください。

- サポートされる認可タイプ （3115 ページ）
- サポートされるアカウンティング タイプ （3115 ページ）
- 方式リストについて （3116 ページ）

AAA ポリシーの設定については、次を参照してください。

- AAA サービスの定義 （3117 ページ）

関連項目

- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- Cisco IOS ルータにおける回線アクセス （3157 ページ）

サポートされる認可タイプ

AAA 認可を使用すると、認証済みのユーザが利用できるサービスを制限できます。Security Manager では、次のタイプの認可がサポートされます。

- ネットワーク：PPP、SLIP、ARAP などのさまざまなタイプのネットワーク接続を認可します。
- EXEC：EXEC（CLI）セッションの起動を認可します。
- コマンド：特定の権限レベルに関連付けられているすべての EXEC モード コマンドの使用を認可します。

認可を有効にすると、ルータはユーザーのプロファイルから取得した情報を使用してユーザーセッションを設定します。プロファイルは、ローカルユーザデータベースまたはセキュリティサーバにあります。ユーザに要求したサービスへのアクセス権が付与されるのは、プロファイルで許可されている場合だけです。

関連項目

- サポートされるアカウンティング タイプ （3115 ページ）
- 方式リストについて （3116 ページ）
- AAA サービスの定義 （3117 ページ）
- Cisco IOS ルータにおける AAA （3114 ページ）

サポートされるアカウンティング タイプ

AAA アカウンティングを使用すると、ユーザがアクセスしているサービスとそれらのサービスが消費しているネットワーク リソースの量を追跡できます。Security Manager では、次のアカウンティング タイプがサポートされます。

- 接続：Telnet、Local-Area Transport（LAT; ローカルエリア トランスポート）、TN3270、Packet Assembler/Disassembler（PAD; パケット アセンブラ/ディスアセンブラ）、rlogin 接続など、このデバイスから確立されたすべてのアウトバウンド接続に関する情報を記録します。

たとえば、アウトバウンド Telnet 接続の RADIUS 接続アカウンティング レコードには、Network Access Server（NAS; ネットワーク アクセス サーバ）のポートや IP アドレス、接続の開始時刻と終了時刻、ユーザの ID、セッション中に送信されたパケットの数などの情報が含まれます。

- EXEC：ユーザ名、日付、開始時刻と終了時刻、NAS の IP アドレスなど、デバイス上のユーザ EXEC（CLI）セッションに関する情報を記録します。ダイヤルインユーザの場合、レコードには、コールの発信元の電話番号が含まれます。
- コマンド：特定の権限レベルを持つユーザがデバイスで実行する EXEC コマンドに関する情報を記録します。各コマンド アカウンティング レコードには、その権限レベルに対し

て実行されたコマンドのリスト、各コマンドが実行された日時、およびそのコマンドを実行したユーザの名前が含まれます。

アカウンティング タイプごとに、アカウンティング レコードを各ユーザ セッションの開始時と終了時に生成するか、または終了時にだけ生成するかを選択できます。

AAAアカウンティングをイネーブルにすると、ルータはユーザアクティビティのアカウンティング レコードをTACACS+またはRADIUSセキュリティ サーバに送信します。各アカウンティング レコードにはアカウンティングのAttribute-Value（AV）ペアが含まれ、レコードはセキュリティ サーバに格納されます。このデータをあとでネットワーク管理、クライアント請求、および監査のために分析できます。

関連項目

- サポートされるアカウンティング タイプ （3115 ページ）
- 方式リストについて （3116 ページ）
- AAA サービスの定義 （3117 ページ）
- Cisco IOS ルータにおける AAA （3114 ページ）

方式リストについて

方式リストは、特定の AAA 機能を実行するために使用する方式を記述した順序付きリストです。Security Manager では、AAA サーバ グループを選択して方式リストを定義します。AAA サーバ グループは、一般に RADIUS や TACACS+ などの同じプロトコルを実行している 1 つ以上の AAA サーバを含む再利用可能なオブジェクトです。方式リストを使用すると、各 AAA 機能に使用するセキュリティ プロトコルを 1 つ以上指定できるため、最初の方式が失敗した場合のバックアップ システムを確保できます。

（注） Security Manager には、イネーブル パスワードまたはローカル データベースを使用するための定義済みの AAA サーバ グループ オブジェクトもあります。 定義済みの AAA 認証サーバ グループ （328 ページ）を参照してください。

各 AAA 機能について、デバイスは最初にリストに定義されている最初の方式を使用します。その方式で応答がない場合、デバイスはリスト内の次の方式を選択します。このプロセスは、リスト内の方式との通信に成功するまで、または方式リストに定義されているすべての方式が試されるまで続行されます。

（注） デバイスは、前の方式で応答がない場合にだけリスト内の次の方式と通信しようとします。AAA サービスがこのサイクルのある時点で失敗した場合、つまり、セキュリティ サーバまたはローカル ユーザ名データベースの応答でユーザ アクセスまたはサービスが拒否された場合、プロセスは停止し、他の方式は試されません。

関連項目

- サポートされる認可タイプ （3115 ページ）
- サポートされるアカウンティング タイプ （3115 ページ）
- AAA サービスの定義 （3117 ページ）
- Cisco IOS ルータにおける AAA （3114 ページ）

AAA サービスの定義

Cisco IOS ルータで AAA サービスを定義するには、まずルータで AAA 機能をイネーブルにする必要があります。その後、デバイスで実装する機能の種類（認証、許可、アカウンティング）を定義できます。各機能の方式リスト（イネーブルにする認可およびアカウンティングのタイプごとのリストなど）を定義する必要があります。

たとえば、EXEC 認可とコマンド認可を設定する場合は、EXEC 認可用に 1 つの方式リストを定義し、コマンド認可を実行する権限レベルごとに他の方式リストを定義する必要があります。

（注） 認証に RADIUS を使用する場合は、認可にも同じ RADIUS サーバ グループを使用する必要があります。

関連項目

- 方式リストについて （3116 ページ）
- Cisco IOS ルータにおける AAA （3114 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[AAA] ページが表示されます。このページのフィールドの説明については、[AAA] ポリシー ページ （3119 ページ）を参照してください。

ステップ 2 デバイスにアクセスするユーザに対して使用するログイン認証方式を定義します。

a) [認証（Authentication）] タブ（[AAA] ページ - [Authentication] タブ （3120 ページ）を参照）で、[デバイスログイン認証の有効化（Enable Device Login Authentication）] チェックボックスをオンにします。

b) 1 つ以上の AAA サーバーグループ オブジェクト（最大 4 つ）の名前を [優先順位付けされた方式リスト（Prioritized Method List）] フィールドに入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。

（注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

ステップ 3 （任意）[Maximum Number of Attempts] フィールドで、許可する認証試行の失敗回数の最大数を定義します。その回数を超えると、ユーザはロックアウトされます。

ステップ 4 （任意）正常に認証されたユーザに対して使用する認可方式を定義します。

a) [AAA] ページの [許可（Authorization）] タブをクリックします。このタブのフィールドの説明については、表 855 : [AAA] ページ - [Authorization] タブ （3122 ページ）を参照してください。

b) 次の 1 つ以上の認可タイプの方式リストを定義します。

- ネットワーク（Network）
- EXEC
- コマンド : [追加（Add）] ボタンをクリックして、[コマンド許可（Command Authorization）] ダイアログボックス（[Command Authorization] ダイアログボックス （3123 ページ）を参照）を表示します。ここから、権限レベルとそれに適用する方式リストを選択できます。

これらの認可タイプの詳細については、サポートされる認可タイプ （3115 ページ）を参照してください。

（注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。

ステップ 5 （任意）ユーザによって実行されるアクティビティに対して使用するアカウンティング方式を定義します。

a) [AAA] ページの [アカウンティング（Accounting）] タブをクリックします。このタブのフィールドの説明については、表 857 : [AAA] ページ - [Accounting] タブ （3125 ページ）を参照してください。

b) 次の 1 つ以上のアカウンティング タイプの方式リストを定義します。

- Connection
- EXEC
- コマンド : [追加（Add）] ボタンをクリックして、[コマンドアカウンティング（Command Accounting）] ダイアログボックス（[Command Accounting] ダイアログボックス （3127 ページ）を参照）を表示します。ここから、権限レベルとそれに適用する方式リストを選択できます。

これらのアカウンティング タイプの詳細については、サポートされるアカウンティング タイプ （3115 ページ）を参照してください。

c) 前の手順で定義した各アカウンティング タイプについて、[Accounting Process Notices] リストから値を選択します。これにより、アカウンティング レコードをユーザ プロセスの開始時と終了時に作成するか、または終了時にだけ作成するかを定義します。

d) 前の手順で定義した各アカウンティングタイプについて、方式リストに定義されている各 AAA サーバーグループ内の最初のサーバに同時にアカウンティング情報を送信する場合は、[複数サーバーへのブロードキャストを有効化（Enable broadcast to multiple servers）] チェックボックスをオンにします。

[AAA] ポリシー ページ

[AAA] ページでは、ルータで使用するデフォルトの認証、許可、アカウンティング方式を定義します。この定義は、使用する方式とその方式を使用する順序を定義する方式リストを設定することによって行います。

（注） このポリシーに定義された方式リストは、ルータのコンソールポートおよび VTY 回線の AAA を設定するときに、デフォルト設定として使用できます。[Console] ポリシー ページ （3165 ページ）および [VTY] ポリシー ページ （3177 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [AAA]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [AAA]** を選択します。[AAA] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- Cisco IOS ルータにおける AAA （3114 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- [Console] ポリシー ページ （3165 ページ）
- [VTY] ポリシー ページ （3177 ページ）

フィールド リファレンス

表 853 : [AAA] ページ

要素	説明
[Authentication] タブ	使用するログイン認証方式とそれらの認証方式を使用する順序を定義します。[AAA] ページ - [Authentication] タブ （3120 ページ）を参照してください。

要素	説明
[Authorization] タブ	実行するネットワーク認可、EXEC 認可、およびコマンド認可のタイプと各タイプに使用する方式を定義します。[AAA] ページ - [Authorization] タブ （3121 ページ）を参照してください。
[Accounting] タブ	実行する接続、EXEC、およびコマンド アカウンティングのタイプと各タイプに使用する方式を定義します。[AAA] ページ - [Accounting] タブ （3124 ページ） を参照してください。

[AAA] ページ - [Authentication] タブ

[AAA] ページの [Authentication] タブでは、デバイスにアクセスするユーザの認証に使用する方式を定義します。認証方式は、LDAP、RADIUS、および TACACS+ などの使用するセキュリティ プロトコルを定義する方式リストで定義します。

（注） コンソールおよびデバイスとの通信に使用される VTY 回線でこのポリシーに定義された方式リストを使用できます。[Console] ポリシー ページ （3165 ページ）および [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）を参照してください。

ナビゲーション パス

[AAA] ポリシー ページ （3119 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- AAA サービスの定義 （3117 ページ）
- 方式リストについて （3116 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）
- 定義済みの AAA 認証サーバ グループ （328 ページ）

フィールド リファレンス

表 854 : [AAA] ページ - [Authentication] タブ

要素	説明
Enable Device Login Authentication	選択すると、デバイスへのログイン時に、方式リストに定義されている方式を使用したすべてのユーザの認証がイネーブルになります。 選択を解除すると、認証は実行されません。

要素	説明
Prioritized Method List	ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）]をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバグループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[Line]、[Local]、[Kerberos]、[LDAP]、[RADIUS]、[TACACS+]、および [None] があります。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Maximum Number of Attempts	認証試行の失敗回数の最大数を定義します。その回数を超えると、ユーザはロックアウトされます。この機能は、デフォルトではディセーブルになっています。有効値の範囲は 1 ～ 65535 です。 （注） ユーザから見ると、通常の認証失敗と、ロックアウトによる認証失敗に違いはありません。システム管理者は、**clear** コマンドを使用して、ロックアウトされたユーザーのステータスを明示的にクリアする必要があります。

[AAA] ページ - [Authorization] タブ

[AAA] ページの [Authorization] タブでは、デバイスに対してイネーブルにする認可サービスのタイプと各タイプで使用する方式を定義します。Security Manager では、次のタイプの認可がサポートされます。

- ネットワーク：PPP などのさまざまなタイプのネットワーク接続を認可します。
- EXEC：EXEC セッションの起動を認可します。
- コマンド：特定の権限レベルに関連付けられているすべての EXEC モード コマンドの使用を認可します。

（注） コンソールおよびデバイスの通信に使用される VTY 回線でこのポリシーに定義された方式リストを使用できます。[Console] ポリシー ページ （3165 ページ）および [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）を参照してください。

ナビゲーション パス

[AAA] ポリシー ページ （3119 ページ）に移動し、[承認（Authorization）] タブをクリックします。

関連項目

- AAA サービスの定義 （3117 ページ）
- サポートされる認可タイプ （3115 ページ）
- 方式リストについて （3116 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 855 : [AAA] ページ - [Authorization] タブ

要素	説明
[Network Authorization] 設定	
Enable Network Authorization	選択すると、方式リストに定義されている方式を使用した PPP、SLIP、ARAP 接続などのネットワーク接続の認可がイネーブルになります。 選択を解除すると、ネットワーク認可は実行されません。
Prioritized Method List	ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバー グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[LDAP]、[RADIUS]、[TACACS+]、[Local]、および [None] があります。 （注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

要素	説明
[EXEC Authorization] 設定	
Enable CLI/EXEC Operations Authorization	選択すると、このタイプの認可は、方式リストに定義されている方式を使用して、EXEC（CLI）セッションを開くことをユーザに許可するかどうかを決定します。 選択を解除すると、EXEC 認可は実行されません。
Prioritized Method List	ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクトセレクタの上向きおよび下向き矢印を使用して、選択したサーバグループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Authorization] ダイアログボックス （3123 ページ）が開きます。ここから、コマンド認可定義を設定できます。
[編集（Edit）] ボタン	[Command Authorization] ダイアログボックス （3123 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[Command Authorization] ダイアログボックス

[Command Authorization] ダイアログボックスでは、特定の権限レベルに関連付けられている EXEC コマンドを認可するときに使用する方式を定義します。これにより、特定の権限レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

ナビゲーション パス

[AAA] ページ - [Authorization] タブ （3121 ページ）で、[コマンド認可（Command Authorization）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- AAA サービスの定義 （3117 ページ）
- サポートされる認可タイプ （3115 ページ）
- 方式リストについて （3116 ページ）

フィールド リファレンス

表 *856 : [Command Authorization]* ダイアログボックス

要素	説明
Privilege Level	コマンド アカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。
Prioritized Method List	ユーザを認可する場合に使用する方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[TACACS+]、[Local]、および [None] が含まれます。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[AAA] ページ - [Accounting] タブ

[AAA] ページの [Accounting] タブでは、デバイスに対してイネーブルにするアカウンティング サービスのタイプと各タイプで使用する方式を定義します。Security Manager では、次のタイプのアカウンティングがサポートされます。

- 接続：このデバイスから確立されたすべてのアウトバウンド接続に関する情報を記録します。
- EXEC：ユーザ名、日付、開始時刻と終了時刻、IP アドレスなど、デバイス上のユーザ EXEC セッションに関する情報を記録します。
- コマンド：特定の権限レベルを持つユーザがデバイスで実行する EXEC コマンドに関する情報を記録します。

さらに、[Accounting] ページでは、アカウンティング レコードをいつ生成し、それらのレコードを複数の AAA サーバにブロードキャストするかどうかを指定します。

（注） コンソールおよびデバイスの通信に使用される VTY 回線でこのポリシーに定義された方式リストを使用できます。[Console] ポリシー ページ （3165 ページ）および [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）を参照してください。

ナビゲーション パス

[AAA] ポリシー ページ （3119 ページ）に移動し、[アカウンティング（Accounting）] タブをクリックします。

関連項目

- AAA サービスの定義 （3117 ページ）
- サポートされるアカウンティング タイプ （3115 ページ）
- 方式リストについて （3116 ページ）
- [AAA Server Group] ダイアログボックス （351 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *857 : [AAA] ページ - [Accounting] タブ*

要素	説明
[Connection Accounting] 設定	
Enable Connection Accounting	選択すると、方式リストに定義されている方式を使用した、このデバイスを介して確立されたアウトバウンド接続（Telnet など）に関する情報の記録がイネーブルになります。 選択を解除すると、接続アカウンティングは実行されません。

要素	説明
Generate Accounting Records for	デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：このタイプのアカウンティングをディセーブルにします。
Prioritized Method List	ユーザの接続アカウンティング レコードの作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（IOS 12.4(22)T+ の場合は 10 個まで、それ以外は 4 個まで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 サポートされる方式には、LDAP、RADIUS および TACACS+ が含まれます。
Enable Broadcast to Multiple Servers	選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[EXEC Accounting] 設定	
Enable CLI/EXEC Operations Accounting	選択すると、方式リストに定義されている方式を使用したユーザEXEC セッションに関する基本情報の記録がイネーブルになります。 選択を解除すると、EXEC アカウンティングは実行されません。
Generate Accounting Records for	表 546 : [Add Cat6k Block VLAN]/[Modify Cat6k Block VLAN] ダイアログボックス （2297 ページ）を参照してください。

要素	説明
Prioritized Method List	ユーザの接続アカウンティング レコードの作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（IOS 12.4(22)T+ の場合は 10 個まで、それ以外は 4 個まで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Enable Broadcast to Multiple Servers	選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。
[Command Accounting] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Generate Accounting Records for	プロセスで、デバイスがアカウンティング通知をアカウンティング サーバに送信するポイント。
Enable Broadcast	アカウンティング レコードが複数のサーバに同時にブロードキャストされるかどうか。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Accounting] ダイアログボックス （3127 ページ）が開きます。ここから、コマンド アカウンティング定義を設定できます。
[編集（Edit）] ボタン	[Command Accounting] ダイアログボックス （3127 ページ）が開きます。ここから、コマンド アカウンティング定義を編集できます。
[削除（Delete）] ボタン	選択したコマンドアカウンティング定義をテーブルから削除します。

[Command Accounting] ダイアログボックス

[Command Accounting] ダイアログボックスでは、特定の権限レベルに対して実行される EXEC コマンドに関する情報を記録するときに使用する方式を定義します。各アカウンティング レコードには、その権限レベルに対して実行されるコマンドのリストと、各コマンドが実行された日時およびそのコマンドを実行したユーザ名が含まれます。

ナビゲーション パス

[AAA] ページ - [Accounting] タブ （3124 ページ）で、[コマンドアカウンティング（Command Accounting）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- AAA サービスの定義 （3117 ページ）
- サポートされるアカウンティング タイプ （3115 ページ）
- 方式リストについて （3116 ページ）

フィールド リファレンス

表 *858 : [Command Accounting]* ダイアログボックス

要素	説明
Privilege Level	コマンド アカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。
Generate Accounting Records for	デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	ユーザのアカウンティング レコードの作成時に使用する方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（IOS 12.4(22)T+ の場合は 10 個まで、それ以外は 4 個まで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式は [TACACS+] だけですが、[TACACS+] が設定された複数の AAA サーバ グループを選択できます。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。

Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル

アカウントおよびクレデンシャル ポリシーでは、各ユーザ アカウントに与えられた権限レベルなど、ルータにアクセスするための接続情報を定義します。ユーザ アカウントは、必要な数だけ設定できます。ただし、Security Manager がルータへの接続に使用するユーザ アカウントは、常に [Device Properties] ページで設定されているアカウントです。

さらに、デバイス アクセス ポリシーを使用して、特権 EXEC モードへのアクセスに必要なイネーブル パスワードまたはイネーブル シークレット パスワードを定義します。このモードは、ルータの設定変更に必要です。

（注） このポリシーを使用してパスワードを定義する場合、次の展開までは置換ポリシーを割り当てずにこのポリシーの割り当てを解除しないように注意してください。このパスワードを削除するデバイス アクセス ポリシーを展開したときに、Security Manager が認識できない別のタイプのパスワード（ライン コンソール パスワードなど）がデバイスに含まれている場合、今後このデバイスを設定できなくなります。これは、Security Manager が以前に設定したイネーブル パスワードを削除すると、デバイスによってパスワードがこの認識できないパスワードに戻されるためです。

関連項目

- アカウントおよびクレデンシャル ポリシーの定義 （3130 ページ）

アカウントおよびクレデンシャル ポリシーの定義

ここでは、Cisco IOS ルータにデバイス アクセス ポリシーを定義する方法について説明します。ルータに接続するために [Device Properties] ページで設定したユーザ名（デバイス プロパティの表示または変更 （136 ページ）を参照）が、このポリシーで定義したユーザ アカウントのいずれかと一致する場合、Security Manager はポリシー定義に従ってデバイス クレデンシャルを更新します。

Security Manager がデバイスへの設定の展開に使用するデバイス プロパティで定義したユーザのパスワードを変更する場合、またはイネーブル パスワードを変更する場合は、Security Manager は、デバイス プロパティで定義された既存のクレデンシャルを使用して、デバイスにログインし、変更を展開します。展開に成功したら、デバイス プロパティは、新しい設定を使用するように変更されます。デバイス プロパティのクレデンシャルの詳細については、[Device Credentials] ページ （143 ページ）を参照してください。

（注） 暗号化されたパスワードは検出できますが、入力するパスワードはクリア テキストである必要があります。暗号化されたパスワードを検出し、そのパスワードを変更した場合、パスワードはクリア テキストで保存されます。

関連項目

- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）デバイス ポリシー セレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。

- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Accounts and Credentials] ページが表示されます。このページのフィールドの説明については、表 859 : [Accounts and Credentials] ページ （3133 ページ）を参照してください。

ステップ 2 ルータで特権 EXEC モードに切り替えるためのパスワードを入力します。

a) [パスワードの有効化（Enable Password）] または [シークレットパスワードの有効化（Enable Secret Password）] を選択します。[Enable Secret Password] オプションを選択すると、MD5 暗号化を使用してパスワードが保存されるため、[Enable Password] オプションよりもセキュリティが向上します。このオプションは、パスワードがネットワークをまたがって使用される場合、または TFTP サーバに格納される場合に役立ちます。

（注） イネーブル シークレット パスワードを設定したあとは、イネーブル シークレットがディセーブルになっている場合、または古い rxboot イメージを実行しているときなど、Cisco IOS ソフトウェアの古いバージョンが使用されている場合にだけイネーブル パスワードに切り替えることができます。

b) パスワードを入力し、[Confirm] フィールドにパスワードを再入力します。入力するパスワードはクリアテキストである必要があります。イネーブル シークレット パスワードを設定すると、パスワードは展開時に暗号化されます。

ステップ 3 （任意）[パスワード暗号化サービスを有効にする（Enable Password Encryption Service）] チェックボックスをオンにして、デバイス上のすべてのパスワードを暗号化します。たとえば、イネーブル パスワード、ユーザ名パスワード、認証キー パスワード、コンソールと VTY 回線アクセス パスワード、BGP ネイバー パスワードなどがあります。

未認可ユーザによる設定ファイル内のパスワードの表示を防ぐために、この機能を使用することを推奨します。

（注） このオプションでは、高レベルのセキュリティは確保されません。したがって、このオプションを他のネットワーク セキュリティ対策の代わりに使用しないでください。

ステップ 4 ルータの新しいユーザ アカウントを定義するには、次の手順を実行します。

a) テーブルの下にある [追加（Add）] ボタンをクリックして、[ユーザーアカウント（User Accounts）] ダイアログボックスを表示します。

b) 新規ユーザの詳細を入力します。使用可能なフィールドの説明については、表 860 : [User Account] ダイアログボックス （3135 ページ）を参照してください。

c) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [User Accounts] テーブルに表示されます。

（注） ユーザーアカウントを編集するには、[ユーザーアカウント（User Accounts）] テーブルからユーザーアカウントを選択し、[編集（Edit）] をクリックします。ユーザーアカウントを削除するには、そのアカウントを選択し、[削除（Delete）] をクリックします。

注意 ユーザーアカウントの削除中に Cisco Security Manager がタイムアウトになり、展開が失敗します。これを回避するには、エラーが発生してもダウンロードするように Security Manager をセットアップします。Configuration Manager の [ツール（Tools）] > [管理者（Administrator）] > [展開（Deployments）] で、[エラー時にダウンロードを許可（Allow Download on Error）] をオンにします。

[アカウントおよびログイン情報ポリシー（Accounts and Credentials Policy）] ページ

[Accounts and Credentials] ページでは、ルータに割り当てるイネーブル パスワードまたはイネーブル シークレット パスワードを定義します。さらに、ルータへのアクセスに使用できるユーザ名のリストを定義できます。

詳細については、アカウントおよびクレデンシャル ポリシーの定義 （3130 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [アカウントおよびログイン情報（Accounts and Credentials）]** を選択します。[アカウントおよびログイン情報（Accounts and Credentials）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）
- [User Account] ダイアログボックス （3134 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *859 : [Accounts and Credentials]* ページ

要素	説明
イネーブル シークレット パスワード（Enable Secret Password）	ルータで特権 EXEC モードを開始するためのイネーブル シークレット パスワード。このオプションを選択すると、[Enable Password] オプションを選択する場合よりもセキュリティが向上します。 イネーブル シークレット パスワードには、1 ～ 25 文字の英数字を使用できます。最初の文字は文字である必要があります。スペースは使用できますが、先頭のスペースは無視されます。疑問符も使用できます。 （注） 暗号化されたパスワードは検出できますが、入力するパスワードはクリア テキストである必要があります。暗号化されたパスワードを変更した場合、パスワードはクリア テキストで保存されます。 （注） イネーブル シークレット パスワードを設定したあとは、イネーブル シークレットがディセーブルになっている場合、または古い rxboot イメージを実行しているときなど、Cisco IOS ソフトウェアの古いバージョンが使用されている場合にだけイネーブル パスワードに切り替えることができます。
パスワードを有効にする（Enable Password）	ルータで特権EXECモードを開始するためのイネーブル パスワード。 イネーブル パスワードには、1 ～ 25 文字の英数字を使用できます。最初の文字は文字である必要があります。スペースは使用できますが、先頭のスペースは無視されます。疑問符も使用できます。 （注） パスワードはクリア テキストで入力する必要があります。
Enable Password Encryption Service	選択すると、選択しなければクリアテキストで保存されるイネーブル パスワードなど、デバイス上のすべてのパスワードが暗号化されます。 たとえば、このオプションを使用して、ユーザ名パスワード、認証キー パスワード、コンソールおよびVTY回線アクセス パスワード、およびBGPネイバーパスワードを暗号化します。このオプションは、主に未認可ユーザによる設定ファイル内のパスワードの表示を防ぐために使用します。 選択を解除すると、デバイスパスワードは暗号化されずに設定ファイルに保存されます。 （注） このオプションでは、高レベルのネットワーク セキュリティは確保されません。他のネットワーク セキュリティ対策も必要になります。

要素	説明
[User Accounts] テーブル	
ユーザー名	ルータへのアクセスに使用できるユーザ名。ユーザ名は、長さが最大64文字の1つの単語にする必要があります。スペースと引用符は使用できません。
暗号化（Encryption）	MD5 暗号化を使用してユーザのパスワード情報が暗号化されるかどうかを示します。
特権レベル	ユーザに割り当てられる権限レベル。
[追加（Add）] ボタン	[User Account] ダイアログボックス （3134ページ）が開きます。ここから、ユーザ アカウントを定義できます。
[編集（Edit）] ボタン	[User Account] ダイアログボックス （3134ページ）が開きます。ここから、選択したユーザを編集できます。
[削除（Delete）] ボタン	選択したユーザ アカウントをテーブルから削除します。

[User Account] ダイアログボックス

[User Account] ダイアログボックスでは、Security Manager でルータへのアクセスに使用できるユーザ名とパスワードの組み合わせを定義します。ユーザアカウントの権限レベルを定義することもできます。これにより、このルータ上のすべてのコマンドを設定できるか、またはそのサブセットだけを設定できるかが決まります。

（注） CLI などの他の方法を使用して、ルータに他のユーザ アカウントが定義されている場合があります。

ナビゲーション パス

[アカウントおよびログイン情報ポリシー（Accounts and Credentials Policy）] ページ （3132ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- アカウントおよびクレデンシャル ポリシーの定義 （3130 ページ）
- Cisco IOS ルータにおけるユーザ アカウントおよびデバイス クレデンシャル （3129 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）

フィールド リファレンス

表 *860 : [User Account]* ダイアログボックス

要素	説明
[ユーザー名（Username）]	ルータにアクセスするためのユーザ名。
パスワード	このユーザ アカウントでルータにアクセスするためのパスワード。 （注） 暗号化されたパスワードは検出できますが、入力するパスワードはクリア テキストである必要があります。
確認（Confirm）	このユーザ アカウントのパスワードを確認します。
Ecrypt password using MD5	選択すると、MD5 暗号化を使用してこのユーザ アカウントのパスワードが暗号化されます。これがデフォルトです。 選択を解除すると、パスワードは暗号化されずにルータに送信されます。
特権レベル	ユーザ アカウントに割り当てられる権限レベル。有効値の範囲は 0 ～ 15 です。 • 0：**disable**、**enable**、**exit**、**help**、および **logout** の各コマンドにだけアクセス権を付与します。 • 1：ルータへの権限なしアクセスをイネーブルにします（通常の EXEC モードでは権限が使用されます）。 • 15：ルータへの権限付きアクセスをイネーブルにします（従来のイネーブル権限）。 （注） レベル 2 ～ 14 は、通常はデフォルト設定では使用されませんが、通常はレベル 15 にあるコマンドをそれよりも低いレベルに移動し、通常はレベル 1 にあるコマンドをそれよりも高いレベルに移動することで、カスタム設定を作成できます。CLI を使用するか FlexConfig を定義することにより、コマンドの権限レベルを設定できます。

Cisco IOS ルータにおけるブリッジング

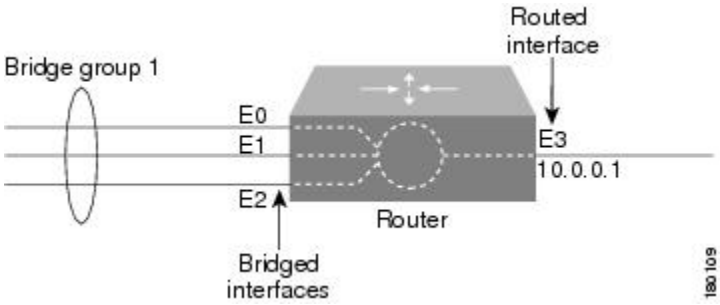
ブリッジング ポリシーを使用すると、ブリッジ グループとして機能するように設定した選択済みインターフェイスに対して、RFC 1286 で規定されているトランスペアレント ブリッジングを実行できます。Security Manager では、Integrated Routing and Bridging がサポートされます。Integrated Routing and Bridging を使用すると、ルーテッド インターフェイスとブリッジ グループ間、またはブリッジ グループ間で特定のプロトコルをルーティングできます。図 49 : トラ

ンスペアレントブリッジング（3136ページ）に示すように、ローカルトラフィックやルーティング不可能なトラフィックは、同じブリッジ グループ内のブリッジド インターフェイス間でブリッジングでき、ルーティング可能なトラフィックは、他のルーテッドインターフェイスやブリッジ グループにルーティングできます。

Integrated Routing and Bridging を使用して、次の処理を実行できます。

- パケットをブリッジド インターフェイスからルーテッド インターフェイスにスイッチングする。
- パケットをルーテッド インターフェイスからブリッジド インターフェイスにスイッチングする。
- パケットを同じブリッジ グループ内でスイッチングする。

図 *49*：トランスペアレント ブリッジング



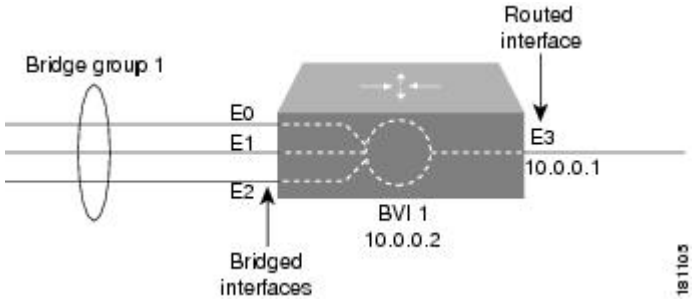
関連項目

- ブリッジ グループの定義 （3137 ページ）
- ブリッジ グループ仮想インターフェイス （3136 ページ）

ブリッジ グループ仮想インターフェイス

ブリッジングはデータ リンク層で実行され、ルーティングはネットワーク層で実行されるため、ブリッジングとルーティングはプロトコル コンフィギュレーション モデルが異なります。たとえば、IP では、ブリッジ グループ インターフェイスは同じネットワークに属し、共通の IP ネットワーク アドレスを持ちます。一方、各ルーテッド インターフェイスは個別のネットワークを表し、独自の IP ネットワーク アドレスを持ちます。Integrated Routing and Bridging では、Bridge-group Virtual Interface（BVI; ブリッジ グループ仮想インターフェイス）の概念を使用して、これらのインターフェイスが特定のプロトコルのパケットを交換できるようにします。図 50：ブリッジ グループ仮想インターフェイス （3137 ページ）に示すように、BVI に割り当てられたインターフェイス番号は、BVI が表すブリッジ グループに対応します。この番号は、仮想インターフェイスとブリッジ グループ間のリンクです。

図 *50* : ブリッジ グループ仮想インターフェイス



BVI 上の特定のプロトコルのルーティングをイネーブルにすると、ルーテッドインターフェイスからブリッジドドメイン内のホスト宛に送信されたパケットは、BVI にルーティングされ、対応するブリッジドインターフェイスに転送されます。BVI にルーティングされたすべてのトラフィックは、ブリッジド トラフィックとして対応するブリッジ グループに転送されます。ブリッジドインターフェイスで受信したすべてのルーティング可能なトラフィックは、BVI から直接送信されているかのように他のルーテッドインターフェイスにルーティングされます。

（注） BVI インターフェイスは、インターフェイス ポリシーを使用して設定します。 基本的なルータ インターフェイス設定の定義 （3009 ページ）を参照してください。BVI インターフェイスには、同じ番号を持つ、対応するブリッジ グループが必要です。このようなブリッジ グループがなければ、展開は失敗します。

（注） ブリッジ グループに 3 つ以上のインターフェイスが含まれている場合は、BVI インターフェイスをグループに追加して、セキュリティ上の問題となる可能性があるユニキャスト フラッディングを防ぎます。

関連項目

- ブリッジ グループの定義 （3137 ページ）
- Cisco IOS ルータにおけるブリッジング （3135 ページ）

ブリッジ グループの定義

ブリッジ グループを定義するには、ブリッジ グループに含める L3 インターフェイスを選択し、グループに番号を割り当てます。Security Manager 内のすべてのブリッジ グループは、IP トラフィックに対してだけ Integrated Routing and Bridging を実行し、標準のスパニングツリー プロトコル（IEEE 802.1D）を使用します。

（注） CLI コマンドまたは FlexConfig を使用して、AppleTalk や IPX などの他のプロトコルにブリッジングしたり、VLAN-Bridge などの他のスパニングツリー プロトコルを使用したりします。同時ルーティングおよびブリッジングはサポートされません。

関連項目

- Cisco IOS ルータにおけるブリッジング （3135 ページ）
- ブリッジ グループ仮想インターフェイス （3136 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Bridging] ページが表示されます。このページのフィールドの説明については、表 861 : [Bridging] ページ（3139 ページ）を参照してください。

ステップ 2 テーブルの下にある [追加（Add）] ボタンをクリックして、[ブリッジグループ（Bridge Group）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 862 : [Bridge Group] ダイアログボックス （3140 ページ）を参照してください。ここから、ブリッジグループを定義できます。

ステップ 3 ブリッジ グループを識別する番号を入力します。

ステップ 4 ブリッジグループに含めるインターフェイスとインターフェイスロールの名前を入力します。または [選択（Select）] をクリックしてインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、 ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

X.25 を除くほとんどのレイヤ 3 インターフェイスと Integrated Services Digital Network（ISDN）ブリッジド インターフェイス、および特定のタイプの論理インターフェイス（ループバック、トンネル、ヌル、BVI など）を選択できます。各インターフェイスは、1 つのブリッジ グループだけに含めることができます。

親インターフェイスがスイッチ間リンク（ISL）または 802.1Q カプセル化で設定されている場合にだけ LAN サブインターフェイスを選択できます。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。ブリッジグループが [Bridging] ページのテーブルに表示されます。

（注） ブリッジグループを編集するには、[グループ（Groups）] テーブルからブリッジグループを選択し、[編集（Edit）] をクリックします。ブリッジグループを削除するには、そのグループを選択し、[削除（Delete）] をクリックします。

[Bridging] ポリシー ページ

[Bridging] ページでは、ルータに対して Integrated Routing and Bridging を実行できるブリッジ グループを定義します。詳細については、ブリッジ グループの定義 （3137 ページ）を参照してください。

ナビゲーション パス

- （デバイス ビュー）ポリシー セレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [ブリッジング（Bridging）]** を選択します。[ブリッジング（Bridging）] を右クリックしてポリシーを作成するか、共有ポリシー セレクタから既存ポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるブリッジング （3135 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 861 : [Bridging] ページ

要素	説明
グループ番号（Group Number）	ブリッジ グループを識別する番号。
Group Interfaces	ブリッジ グループに含めるインターフェイスとインターフェイス ロール。
[追加（Add）] ボタン	[Bridge Group] ダイアログ ボックス （3140 ページ）が開きます。ここから、ブリッジ グループを定義できます。
[編集（Edit）] ボタン	[Bridge Group] ダイアログ ボックス （3140 ページ）が開きます。ここから、ブリッジ グループを編集できます。
[削除（Delete）] ボタン	選択したブリッジ グループをテーブルから削除します。

[Bridge Group] ダイアログボックス

[Bridge Group] ダイアログボックスでは、ルータ上のブリッジ グループを定義します。各ブリッジ グループには、シリアル インターフェイスなど、さまざまなタイプの複数のレイヤ 3 インターフェイスを含めることができます。

（注） すべてのブリッジ グループは、標準のスパニングツリープロトコル（IEEE 802.1D）を使用します。CLI コマンドまたは FlexConfig を使用して、AppleTalk や IPX などの他のプロトコルにブリッジングしたり、VLAN-Bridge などの他のスパニングツリー プロトコルを使用したりします。

ナビゲーション パス

[Bridging] ポリシー ページ （3139 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- ブリッジ グループの定義 （3137 ページ）
- Cisco IOS ルータにおけるブリッジング （3135 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *862 : [Bridge Group]* ダイアログボックス

要素	説明
グループ番号（Group Number）	ブリッジ グループに割り当てる番号。有効値の範囲は、1 ～ 255 です。

要素	説明
Group Interfaces	ブリッジ グループに含めるインターフェイス。1 つ以上のインターフェイスとインターフェイス ロールの名前を入力するか、または [選択（Select）] をクリックしてそれらを選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 シリアル インターフェイス（High-level Data Link Control（HDLC; ハイレベル データリンク コントロール）またはフレームリレー カプセル化が設定されている場合）などのほとんどのレイヤ 3 インターフェイスを選択できます。各インターフェイスは、1 つのブリッジ グループだけに属することができます。 親インターフェイスがスイッチ間リンク（ISL）または 802.1Q カプセル化で設定されている場合にだけ LAN サブインターフェイスを選択できます。 （注） ループバック、トンネル、ヌル、BVI などの特定のタイプのインターフェイスはブリッジングできません。 （注） ブリッジ グループにより、Security Manager とデバイスとの通信が妨害されていないことを確認してください。

Cisco IOS ルータにおけるタイム ゾーン設定

Cisco IOS ルータの現地時間は、一般に CLI で clock set コマンドを使用して設定するか、またはNTP サーバから時刻を動的に取得して設定します。これらの時刻設定を調整するには、ルータが存在するタイム ゾーンおよびそのタイム ゾーンの Daylight Saving Time（DST; 夏時間）の開始日と終了日を定義します。

関連項目

- タイム ゾーンと DST 設定の定義 （3141 ページ）
- Cisco IOS ルータにおける NTP （3237 ページ）

タイム ゾーンと DST 設定の定義

Security Manager では、Cisco IOS ルータが配置されているタイム ゾーンを定義できます。Daylight Saving Time（DST; 夏時間）の開始日と終了日を定義することもできます。

関連項目

- NTP サーバの定義 （3237 ページ）
- Cisco IOS ルータにおけるタイム ゾーン設定 （3141 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Clock] ページが表示されます。このページのフィールドの説明については、表 863 : [Clock] ページ （3143 ページ）を参照してください。

ステップ 2 ルータが配置されているタイム ゾーンを選択します。タイム ゾーンは、Greenwich Mean Time（GMT; グリニッジ標準時）との時差に従ってリストに表示されます。

ステップ 3 （任意）DST の開始日と終了日を決定するための方法を選択します。

- [Set by Date]：このオプションは、DST が指定日に開始し、終了する場合に選択します。「ステップ 4 （3142 ページ）」に進みます。
- [Set by Day]：このオプションは、特定の曜日（日付はその年によって異なる）に開始し、終了する場合に選択します。「ステップ 5 （3142 ページ）」に進みます。
- [None]：このオプションは、DST を使用しない場合に選択します。

ステップ 4 （[Set by Date] を選択した場合）DST が開始および終了する日付を定義します。

a) [Start] の下にあるカレンダー アイコンをクリックし、適切な日付をクリックします。
b) 表示されるリストから時間と分を選択します。
c) 手順 a と b を繰り返して終了日と終了時刻を設定します。

ステップ 5 （[曜日による設定（Set by Day）] を選択した場合）米国の大部分で使用されるデフォルト以外の DST 期間を定義する場合は、[繰り返し時刻を指定（Specify Recurring Time）]チェックボックスをオンにします。

ステップ 6 （[Specify Recurring Time] を選択した場合）DST の開始と終了を指定します。

a) [Start] で、DST が開始する月を選択します。
b) 月の週を選択します（1、2、3、4、first、または last）。
c) 曜日を選択します。
d) 表示されるリストから時間と分を選択します。たとえば、DST が毎年 3 月の最後の日曜日の午前 1:00 に開始する場合は、[3月 （March）]、[最後（last）]、[日曜日 （Sunday）]、[1]、および [00] を選択します。
e) 手順 a ～ d を繰り返して終了日と終了時刻を設定します。

[Clock] ポリシー ページ

[Clock] ページでは、ルータが配置されているタイム ゾーンと Daylight Saving Time（DST; 夏時間）を設定します。詳細については、Cisco IOS ルータにおけるタイム ゾーン設定 （3141 ページ）を参照してください。

ヒント　NTP ポリシーを定義するか、または CLI を使用して **clock set** コマンドを設定することによって、ルータの現地時間を設定できます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [クロック（Clock）]** を選択します。[クロック（Clock）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [NTP Policy] ページ （3239 ページ）

フィールド リファレンス

表 863 : [Clock] ページ

要素	説明
Device Time Zone	Coordinated Universal Time（UTC; 協定世界時）とも呼ばれる Greenwich Mean Time（GMT; グリニッジ標準時）との関連で表現される、ルータが配置されているタイム ゾーン。 **注意**　CLI（コマンドラインインターフェイス）を使用してルータのタイムゾーンを設定する場合は、『Cisco IOS Configuration Fundamentals Command Reference』に記載されている必要なタイムゾーンの頭字語を使用する必要があります。タイムゾーンに他の形式を使用してから、Security Manager を使用してルータを検出した場合、Security Manager はタイムゾーン CLI を検出しません。
Daylight Savings Time (Summer Time)	ルータの現地時間に適用する DST のタイプ。 • [Set by Date]：DST が開始および終了する正確な日時を定義できます。 • [Set by Day]：DST が開始および終了する相対的な繰り返し日時を定義できます。たとえば、DST が 3 月の最後の日曜日に開始し、10 月の最後の日曜日に終了する場合にこのオプションを使用できます。 • [None]：夏時間を使用しません。

要素	説明
[Set by Date] の追加フィールド	
開始（Start）	DST が開始する日時： • [Date]：カレンダーアイコンをクリックして、開始日を選択します。 • [Hour]：開始時刻（時間）を選択します。 • [Minute]：開始時刻（分）を選択します。
終了（End）	DST が終了する日時： • [Date]：カレンダーアイコンをクリックして、終了日を選択します。 • [Hour]：終了時刻（時間）を選択します。 • [Minute]：終了時刻（分）を選択します。 （注） Cisco IOS ソフトウェアでは、2035 年 12 月 31 日までの日付がサポートされます。
[Set by Day] の追加フィールド	
Specify Recurring Time	選択すると、ルータはこのポリシーで指定された日付と時刻に従って DST を実装します。 選択を解除すると、ルータは米国の大部分で使用されているスケジュールに従って DST を実装します。
開始（Start）	夏時間が開始する相対的な日時： • [Month]：月を選択します。 • [Week]：月の週を選択します（1、2、3、4、first、または last）。 • [Weekday]：曜日を選択します。 • [Hour]：時間を選択します。 • [Minute]：分を選択します。 たとえば、DST が毎年 3 月の最後の日曜日の午前 1:00 に開始する場合は、[3月（March）]、[最後（last）]、[日曜日（Sunday）]、[1]、および [00] を選択します。

要素	説明
終了（End）	夏時間が終了する相対的な日時： • [Month]：月を選択します。 • [Week]：月の週を選択します（1、2、3、4、first、または last）。 • [Weekday]：曜日を選択します。 • [Hour]：時間を選択します。 • [Minute]：分を選択します。

Cisco IOS ルータにおける CPU 使用率設定

CPU ポリシーでは、CPU 使用率に関する設定を行います。このポリシーを使用すると、CPU リソースをモニタしたり、事前に決定されているレベルの使用率を超えるプロセスを追跡したりできます。

（注） CPU ポリシーは、Cisco IOS ソフトウェア Release 12.3(14)T 以降を実行しているルータでサポートされます。

関連項目

- CPU 使用率設定の定義 （3145 ページ）

CPU 使用率設定の定義

Security Manager を使用して、次のデフォルトの CPU 使用率設定を変更できます。

- CPU 履歴テーブルのサイズ
- 拡張 CPU 負荷履歴テーブルのサイズ
- 自動 CPU Hog プロファイリングをイネーブルにするかどうか

また、オプションで次の項目を定義できます。

- プロセスを履歴テーブルに含める CPU 使用率レベル。
- イネーブルにする CPU 使用率しきい値のタイプ。しきい値のタイプごとに、通知をトリガーするしきい値を指定できます。

関連項目

- CPU 使用率設定の定義 （3145 ページ）

- Cisco IOS ルータにおけるロギング （3269 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [CPU] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [CPU] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[CPU] ページが表示されます。

ステップ 2 （任意）ルータのCPU使用率設定を必要に応じて定義します。使用可能なフィールドの説明については、表 864 : [CPU] ページ （3147 ページ）を参照してください。

[CPU] ポリシー ページ

[CPU] ページでは、ログ メッセージを送信するしきい値、CPU 履歴テーブルのサイズ、自動 CPU Hog プロファイリングをイネーブルにするかどうかなど、ルータの CPU 使用率に関する設定を定義します。

詳細については、 CPU 使用率設定の定義 （3145 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイスアクセス（Device Access）] > [CPU]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイスアクセス（Device Access）] > [CPU]** を選択します。[CPU] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [Memory] ポリシー ページ （3215 ページ）
- Syslog ロギングの設定ポリシーのページ （3278 ページ）
- Syslog サーバ ポリシーのページ （3282 ページ）

フィールド リファレンス

表 *864 : [CPU]* ページ

要素	説明
CPU Utilization Statistics	CPU 使用率の統計情報の履歴テーブルに関する設定： • [History Table Entry Limit]：プロセスで使用される CPU 使用率で、この値を超えるとプロセスは履歴テーブルに格納されます。 • [History Table Size]：CPU 統計情報を履歴テーブルに格納しておく期間。有効値の範囲は 5 ～ 86400 秒（24 時間）です。デフォルトは 600 秒（10 分）です。
CPU Total Utilization	通知をトリガーする合計 CPU 使用率のしきい値。 • [Enable CPU Total Utilization]：選択されている場合、合計 CPU 使用率しきい値がイネーブルになります。選択解除されている場合、これらのしきい値はディセーブルになり、通知をトリガーしません。これがデフォルトです。 • [リソースの最大合計使用率（Maximum Total Utilization Resources）]：定義された間隔に使用状況がこのレベルを超えた場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Maximum Total Utilization Violation Duration]：最大 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。 • [リソースの最小合計使用率（Minimum Total Utilization Resources）]：定義された間隔に使用状況がこのレベルを下回った場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Minimum Total Utilization Violation Duration]：最小 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。

要素	説明
CPU Interrupt Utilization	通知をトリガーする合計 CPU 割り込み使用率のしきい値。 • [Enable CPU Interrupt Utilization]：選択されている場合、CPU 割り込み使用率のしきい値がイネーブルになります。選択解除されている場合、これらのしきい値はディセーブルになり、通知をトリガーしません。これがデフォルトです。 • [リソースの最大割り込み使用率（Maximum Interrupt Utilization Resources）]：定義された間隔に使用状況がこのレベルを超えた場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Maximum Interrupt Utilization Violation Duration]：最大 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。 • [リソースの最小割り込み使用率（Minimum Interrupt Utilization Resources）]：定義された間隔に使用状況がこのレベルを下回った場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Minimum Interrupt Utilization Violation Duration]：最小 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。
CPU Process Utilization	通知をトリガーする合計 CPU プロセス使用率のしきい値。 • [Enable CPU Process Utilization]：選択されている場合、CPU プロセス使用率のしきい値がイネーブルになります。選択解除されている場合、これらのしきい値はディセーブルになり、通知をトリガーしません。これがデフォルトです。 • [リソースの最大プロセス使用率（Maximum Process Utilization Resources）]：定義された間隔に使用状況がこのレベルを超えた場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Maximum Process Utilization Violation Duration]：最大 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。 • [リソースの最小プロセス使用率（Minimum Process Utilization Resources）]：定義された間隔に使用状況がこのレベルを下回った場合に通知をトリガーする CPU リソースのパーセンテージ。 • [Minimum Process Utilization Violation Duration]：最小 CPU しきい値の通知をトリガーする違反間隔。有効値の範囲は 5 ～ 86400 秒（24 時間）です。
Extended CPU History Size	5 秒間隔で収集する拡張 CPU 負荷の履歴のサイズ。有効値の範囲は 2 ～ 720 です。デフォルトは 12 で、これは 1 分間の履歴に相当します。

要素	説明
Enable Automatic CPU Hog Profiling	選択すると、自動 CPU Hog プロファイリングがイネーブルになります。これがデフォルトです。 選択を解除すると、自動 CPU Hog プロファイリングがディセーブルになります。 この機能は、プロセスがいつ CPU を独占する可能性があるかを予測し、そのプロセスのプロファイリングを開始します。 （注） CPU Hog プロファイルデータを表示するには、CLI で **show processes cpu autoprofile hog** コマンドを使用します。

Cisco IOS ルータにおける HTTP と HTTPS

Security Manager では、Cisco IOS ルータ上の HTTP および HTTP over Secure Socket Layer（HTTP over SSL または HTTPS とも呼ぶ）サーバ機能を設定できます。この機能により、HTTP 1.1 サーバで SSL バージョン 3.0 がサポートされます。

セキュアな HTTP 接続とは、HTTP サーバとの間で送受信されるデータがインターネットを介して送信される前に暗号化されることを意味します。SSL 暗号化を使用した HTTP により、セキュアな接続が提供され、Web ブラウザからのルータの設定などの機能を実行できます。

HTTP と HTTPS は、Cisco Web ブラウザ ユーザ インターフェイスを使用したデバイスへのアクセスを提供する以外に、デバイスと通信するために Cisco Router and Security Device Manager（SDM）などのデバイス管理アプリケーションで使用されます。

関連項目

- HTTP ポリシーの定義 （3149 ページ）

HTTP ポリシーの定義

HTTP ポリシーを定義すると、次の処理を実行できます。

- ルータにおける HTTP および SSL 機能のイネーブル化とディセーブル化
- 各プロトコルで使用されるポートの指定
- （任意）これらのプロトコルを使用したデバイスへのアクセスを制限する標準の番号付き ACL の定義

さらに、ユーザに対して実行する AAA 認証と認可の方式を定義できます。

HTTP ポリシーを定義するときは注意が必要です。設定が Security Manager（およびこれらのプロトコルを使用する他の管理アプリケーション）とデバイス間の通信に影響する可能性があるためです。

（注） 原則として、Security Manager は SSL を Cisco IOS ルータとの通信のデフォルト プロトコルとして使用するため、Security Manager によって検出された Cisco IOS ルータではすでに HTTPS がイネーブルになっています。Cisco IOS ルータでの SSL の設定 （75 ページ）を参照してください。

はじめる前に

- ルータで AAA サービスをイネーブルにします。AAA サービスの定義 （3117 ページ） を参照してください。

関連項目

- Cisco IOS ルータにおける HTTP と HTTPS （3149 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [HTTP] を選択し、作業領域で [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[HTTP Setup] タブが表示されます。このタブのフィールドの説明については、表 865 : [HTTP] ページ - [Setup] タブ （3153 ページ）を参照してください。

ステップ 2 チェックボックスをオンにして、ルータにおける HTTP および SSL（HTTPS）機能をイネーブルにします。

（注） SSL がディセーブルになっている（または HTTP ポリシー全体が割り当てられていない）場合、デバイスから SSH へのトランスポート プロトコルを変更しないかぎり、Security Manager は展開後にそのデバイスと通信できません。この設定は、[Device Properties] にあります。デバイス通信設定および証明書の管理 （576 ページ）を参照してください。

ヒント SSL がイネーブルになっているときは HTTP をディセーブルにすることを推奨します。サーバに対してセキュアな接続だけを確立するには、これが必須です。

ステップ 3 （任意）HTTP（80）および HTTPS（443）によって使用されるデフォルト ポートを変更します。

ステップ 4 （任意）[ここからの接続を許可（Allow Connection From）] フィールドに、このデバイス上の HTTP および HTTPS を使用できるアドレスを指定する標準の番号付き ACL の名前オブジェクトを入力します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。このオプションは、これらのプロトコルへのアクセスを制限する場合に使用します。標準の ACL オブジェクトを作成する方法の詳細については、標準アクセス コントロール リスト オブジェクトの作成 （360 ページ）を参照してください。

（注） 選択した ACL で Security Manager サーバが許可されていることを確認してください。許可されていない場合、デバイスとの通信は失われます。

ステップ 5 （任意）[AAA] タブで、HTTP または HTTPS を使用してデバイスにアクセスしようとするユーザに対して実行する認証のデフォルト タイプを変更します。オプションには、[AAA]、[Enable Password]（デフォルト）、[Local Database]、および [TACACS] があります。

[AAA] を選択した場合はステップ 6 （3151 ページ）に進みます。[AAA] 以外を選択した場合はステップ 8 （3151 ページ）に進みます。

（注） [TACACS] オプションは、12.3(8) よりも前の IOS ソフトウェア バージョンを使用するデバイスにだけ適用されます。

[AAA] タブのフィールドの説明については、表 866 : [HTTP] ページ - [AAA] タブ （3154 ページ）を参照してください。

ステップ 6 ユーザに対して実行する認証方式を選択します。

- デバイスの AAA ポリシー（AAA サービスの定義 （3117 ページ）を参照）で定義されているデフォルトの AAA ログイン認証方式を使用する場合は、[デバイスログイン認証を有効にする（Enable Device Login Authentication）] チェックボックスをオフにしてください。「ステップ 7 （3151 ページ）」に進みます。
- このポリシー用に特別に方式リストを定義する場合は、次の手順を実行します。

a) [デバイスログイン認証を有効にする（Enable Device Login Authentication）] チェックボックスをオンにします。

b) [優先方法リスト（Prioritized Method List）] で、認証に使用する AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックしてリストから AAA サーバーグループを選択するか、新しい AAA サーバーグループを作成します。セレクタの上向きおよび下向き矢印を使用して、これらの認証方式を適用する順序を定義します。

（注） Security Manager ユーザが AAA サーバで定義されていることを確認します。定義されていない場合、デバイスとの通信は失われます。

ステップ 7 HTTP または HTTPS を使用して EXEC セッションを開始するユーザに対して実行する認可方式を選択します。

- デバイスの AAA ポリシーで定義されているデフォルトの AAA 認証方式を使用する場合は、[CLI/EXEC 操作認証を有効にする（Enable CLI/EXEC Operations Authorization）] チェックボックスをオフにしてください。「ステップ 8 （3151 ページ）」に進みます。
- このポリシー用に特別に方式リストを定義する場合は、[CLI/EXEC操作認証を有効にする（Enable CLI/EXEC Operations Authorization）] チェックボックスをオンにし、方式リストを定義します。

（注） このオプションを選択解除のままにした場合は、ルータの AAA ポリシーで EXEC認証が有効になっていることを確認してください。イネーブルになっていない場合は、HTTP または HTTPS （SSL）を介してデバイスに接続できません。これは、Security Manager および SDM などのその他のアプリケーションに適用されます。 AAA サービスの定義 （3117 ページ）を参照してください。

ステップ 8 （任意）特定の権限レベルのコマンド認可定義を作成します。

a) [コマンド認証の上書き（Command Authorization Override）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Authorization Override] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 867 : [Command Authorization] ダイアログボックス （3157 ページ）を参照してください。
b) 必要に応じてコマンド認可定義を設定します。
c) [OK] をクリックダイアログボックスが閉じ、認可方式が [Command Authorization Override] テーブルに表示されます。
d) 8.a （3152 ページ）～8.c （3152 ページ）を繰り返して、追加のコマンド認可定義を作成します。

[HTTP] ポリシー ページ

[HTTP] ページでは、ルータ上の HTTP および HTTPS アクセスを設定します。[HTTP] ポリシーページの次のタブから Cisco IOS ルータ上の HTTP ポリシーを設定できます。

- [HTTP] ページ - [Setup] タブ （3152 ページ）
- [HTTP] ページ - [AAA] タブ （3154 ページ）

詳細については、Cisco IOS ルータにおける HTTP と HTTPS （3149 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [HTTP] を選択します。[HTTP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

[HTTP] ページ - [Setup] タブ

[HTTP] ページの [Setup] タブでは、ルータ上の HTTP および HTTP over Secure Socket Layer（HTTP over SSL または HTTPS）をイネーブルにします。これらのプロトコルへのアクセスをアクセス コントロール リストで定義されているアドレスに制限することもできます。

（注） 原則として、Security Manager は SSL を Cisco IOS ルータとの通信のデフォルト プロトコルとして使用するため、Security Manager によって検出された Cisco IOS ルータではすでに HTTPS がイネーブルになっています。Cisco IOS ルータでの SSL の設定 （75 ページ）を参照してください。

ナビゲーション パス

[HTTP] ポリシー ページ （3152 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- [HTTP] ページ - [AAA] タブ （3154 ページ）
- Cisco IOS ルータにおける HTTP と HTTPS （3149 ページ）

フィールド リファレンス

表 *865 : [HTTP] ページ - [Setup] タブ*

要素	説明
HTTP の有効化	選択すると、ルータで HTTP サーバがイネーブルになります。 選択を解除すると、ルータでHTTPがディセーブルになります。これは、検出されなかったデバイスのデフォルトです。
HTTP ポート（HTTP Port）	HTTP で使用するポート番号。有効値は、80 または 1024 ～ 65535 の任意の値です。デフォルトは 80 です。
SSL の有効化（Enable SSL）	選択すると、セキュアな HTTP サーバ（HTTP over SSL または HTTPS）がルータでイネーブルになります。 選択を解除すると、HTTPS がディセーブルになります。これは、検出されなかったデバイスのデフォルトです。 （注） SSL がディセーブルになっている（または HTTP ポリシー全体が割り当てられていない）場合、デバイスから SSH へのトランスポート プロトコルを変更しないかぎり、Security Manager は展開後にそのデバイスと通信できません。この設定は、[Device Properties] にあります。 （注） SSL がイネーブルになっているときは HTTP をディセーブルにすることを推奨します。サーバに対してセキュアな接続だけを確立するには、これが必須です。
SSL Port	HTTPS で使用するポート番号。有効値は、443 または 1025 ～ 65535 の任意の値です。デフォルトは 443 です。

要素	説明
Allow Connection From	このデバイス上の HTTP および HTTPS の使用を制限する標準の番号付き ACL の名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 （注） ACL を定義する場合は、ACL に Security Manager サーバが含まれていることを確認してください。含まれていない場合、Security Manager は SSL を使用してこのデバイスと通信できません。

[HTTP] ページ - [AAA] タブ

[HTTP] ページの [AAA] タブでは、HTTP または HTTPS を使用してルータにアクセスしようとするユーザに対して実行する認証方式および認可方式を定義します。

ナビゲーション パス

[HTTP] ポリシー ページ （3152 ページ）に移動し、[AAA] タブをクリックします。

関連項目

- [HTTP] ページ - [Setup] タブ （3152 ページ）
- Cisco IOS ルータにおける HTTP と HTTPS （3149 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 866 : [HTTP] ページ - [AAA] タブ

要素	説明
Authenticate Using	使用する認証のタイプ： • [AAA]：AAA ログイン認証を実行します。 • [Enable Password]：ルータに設定されているイネーブル パスワードを使用します。これがデフォルトです。 • [Local Database]：ルータに設定されているローカル ユーザ名データベースを使用します。 • [TACACS]：ルータに設定されている TACACS または XTACACS サーバを使用します。12.3(8) または 12.3(8)T よりも前の IOS ソフトウェア バージョンを使用するデバイスにだけ適用されます。
[Login Authentication] 設定	

要素	説明
Enable Device Login Authentication	[AAA] が認証方式として選択されている場合にだけ適用されます。 選択すると、認証は [Prioritized Method List] フィールドで定義されている方式に基づいて実行されます。 選択を解除すると、ルータの AAA ポリシーで定義されているデフォルトの認証リストが使用されます。[AAA] ページ - [Authentication] タブ （3120 ページ）を参照してください。
Prioritized Method List	[Enable Device Login Authentication] チェックボックスがオンになっている場合にだけ適用されます。 ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
[EXEC Authorization] 設定	
Enable CLI/EXEC Operations Authorization	[AAA] が認証方式として選択されている場合にだけ適用されます。 選択すると、EXEC 認可は [Prioritized Method List] フィールドで定義されている方式に基づいて実行されます。このタイプの認可では、EXEC（CLI）セッションを開くことをユーザに許可するかどうかを決定します。 選択を解除すると、ルータの AAA ポリシーで定義されているデフォルトの EXEC 認可リストが使用されます。[AAA] ページ - [Authorization] タブ（3121 ページ）を参照してください。 （注） このオプションを選択解除のままにした場合は、ルータの AAA ポリシーで EXEC 認可がイネーブルになっていることを確認してください。イネーブルになっていない場合は、HTTP または HTTPS（SSL）を介してデバイスに接続できません。これは、Security Manager および SDM やデバイスの Web インターフェイスなどのその他のアプリケーションに適用されます。

要素	説明
Prioritized Method List	[Enable CLI/EXEC Operations Authorization] チェックボックスがオンになっている場合にだけ適用されます。 EXEC（CLI）セッションを開くことをユーザに許可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Authorization Override] ダイアログボックス （3156 ページ）が開きます。ここから、コマンド認可定義を設定できます。
[編集（Edit）] ボタン	[Command Authorization Override] ダイアログボックス （3156 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[Command Authorization Override] ダイアログボックス

[Command Authorization Override] ダイアログボックスでは、特定の権限に関連付けられている EXEC コマンドを認可するときに使用する方式を定義します。これにより、特定の権限レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

ナビゲーション パス

[HTTP] ページ - [AAA] タブ （3154 ページ）で、[コマンド許可のオーバーライド（Command Authorization Override）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- [HTTP] ポリシー ページ （3152 ページ）

- [AAA] ポリシー ページ （3119 ページ）

フィールド リファレンス

表 *867 : [Command Authorization]* ダイアログボックス

要素	説明
Privilege Level	コマンド アカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。
Prioritized Method List	ユーザを認可する場合に使用する方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 サポートされる方式には、[TACACS+]、[Local]、および [None] が含まれます。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

Cisco IOS ルータにおける回線アクセス

Security Manager では、次の方法を使用したルータへのコマンドライン アクセス（EXEC アクセスとも呼ばれる）を設定できます。

- コンソール ポート：ローカル アクセスのための標準の RS232 ケーブルによる物理接続。詳細については、以下を参照してください。
  - コンソール ポートの設定パラメータの定義 （3158 ページ）
  - コンソール ポートの AAA 設定の定義 （3159 ページ）
- VTY 回線：一般に Telnet、SSH、rlogin などのプロトコルを使用したリモート アクセスのための仮想端末回線。詳細については、以下を参照してください。
  - VTY 回線の設定パラメータの定義 （3161 ページ）
  - VTY 回線の AAA 設定の定義 （3164 ページ）

これらのポリシーを設定して展開したあと、CLI を使用した設定または診断時にこれらの回線を使用して個々のデバイスと直接通信できます。

コンソール ポートの設定パラメータの定義

ルータのコンソール ポートは、一般的にデバイスに物理的にアクセスできる管理者によってローカル システム アクセスに使用されます。デフォルトでは、コンソール ポートは次のように設定されます。

- 許可されるすべてのユーザは、すべてのコンフィギュレーション コマンド（権限レベル 15）を含む、ルータへの権限付きアクセス権を持ちます。
- 回線は、ユーザ入力がなくなってから 10 分経過後に切断されます。
- 着信接続は許可されません。
- 発信接続では Telnet だけがサポートされます。

デフォルト設定を変更する以外に、次の設定を定義することもできます。

- コンソールにアクセスするためのパスワード
- コンソール上のすべての EXEC セッションをディセーブルにするかどうか
- コンソール上で許可される接続を制限する着信 ACL と発信 ACL
- コンソール上で VRF 接続を許可するかどうか

関連項目

- Cisco IOS ルータにおける回線アクセス （3157 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）] を選択し、作業領域で [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

[Console Setup] タブが表示されます。このタブのフィールドの説明については、表 868 : [Console] ページ - [Setup] タブ （3166 ページ）を参照してください。

ステップ 2 （任意）コンソール ポートにアクセスするためのパスワードを入力し、[Confirm] フィールドに再入力します。

ステップ 3 （任意）コンソール ポートのユーザに付与するデフォルト（15）を変更します。 [Console] ページ - [Authorization] タブ （3170 ページ）を参照してください。

ステップ 4 （任意）[この回線を介したルータへの EXEC セッションをすべて無効にする（Disable all the EXEC sessions to the router via this line）] チェックボックスをオンにして、コンソールを介した着信接続を阻止します。

（注） このオプションを選択すると、コンソール ポートを介したデバイスへのすべてのアクセスがブロックされます。

ステップ 5 （任意）デフォルトのタイムアウトを変更します。この時間の経過後もユーザ入力が検出されない場合は、回線が切断されます。

（注） この値を 0 に設定するとタイムアウトがディセーブルになります。タイムアウトがディセーブルになると、ネットワークのセキュリティが低下する可能性があります。

ステップ 6 （任意）コンソール ポート上のアウトバウンド接続に使用できるプロトコルを指定します。

- [All]：サポートされるすべてのプロトコルが許可されます。
- [None]：プロトコルは許可されません。
- [Protocol]：SSH、Telnet、rlogin のプロトコルの 1 つ以上をイネーブルにします。

（注） コンソール ポートで SSH および rlogin プロトコルを許可するデバイスに AAA 認証を設定する必要があります。 コンソール ポートの AAA 設定の定義 （3159 ページ）を参照してください。

ステップ 7 （任意）ACL の名前を入力して、デバイスとこれらのリスト内のアドレス間における着信接続と発信接続を制限します。または、[選択（Select）] をクリックして ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。セレクタの最上部にある [Type] フィールドで、ACL タイプとして [Standard] または [Extended] を選択します。

ステップ 8 （任意）[AAA] タブをクリックして、コンソールポートの認証、許可、アカウンティング設定を定義します。 コンソール ポートの AAA 設定の定義 （3159 ページ） を参照してください。

コンソール ポートの AAA 設定の定義

デフォルトでは、認証、許可、アカウンティングはコンソール ポートに対して実行されません。これらのアクセス コントロール オプションの 1 つ以上を設定するときに、デバイスの AAA ポリシーで定義されたデフォルトの方式リストを使用するか、1 つ以上の AAA 方式を含むカスタム方式リストを定義できます。

関連項目

- コンソール ポートの設定パラメータの定義 （3158 ページ）
- Cisco IOS ルータにおける回線アクセス （3157 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択し、作業領域で [認証（Authentication）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[エリア（Area）] タブをクリックします。

[Console Authentication] タブが表示されます。

ステップ 2 （任意）コンソール回線にアクセスしようとするユーザに対して実行する認証方式を選択します。

[Authentication] タブのフィールドの説明については、表 869 : [Console] ページ - [Authentication] タブ （3169 ページ）を参照してください。

（注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

ステップ 3 （任意）[Authorization] タブで、コンソール回線にアクセスして EXEC セッションを開始するユーザに対して実行する認可方式を選択します。

[Authorization] タブのフィールドの説明については、表 870 : [Console] ページ - [Authorization] タブ （3171 ページ）を参照してください。

（注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。

ステップ 4 （任意）特定の権限レベルのコマンド認可定義を作成します。

a) [コマンド認可（Commands Authorization）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Authorization] ダイアログボックスが表示されます。詳細については、表 878 : [Command Authorization] ダイアログボックス - [Line Access] （3191 ページ）を参照してください。
b) 必要に応じてコマンド認可定義を設定します。
c) [OK] をクリックダイアログボックスが閉じ、認可方式が [Commands Authorization] テーブルに表示されます。
d) 6.a （3160 ページ）～6.c （3161 ページ）を繰り返して、追加のコマンド認可定義を作成します。

ステップ 5 （任意）[Accounting] タブで、コンソール回線にアクセスするユーザに対して実行する EXEC および接続アカウンティング方式を選択します。

このタブのフィールドの説明については、表 871 : [Console] ページ - [Accounting] タブ （3172 ページ）を参照してください。

ステップ 6 （任意）特定の権限レベルのコマンド アカウンティング定義を作成します。

a) [コマンドアカウンティング（Commands Accounting）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Accounting] ダイアログボックス - [Line Access] （3192 ページ）が表示されます。
b) 必要に応じてコマンド アカウンティング定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、アカウンティング方式が [Commands Accounting] テーブルに表示されます。
d) 6.a（3160ページ）～6.c（3161ページ）を繰り返して、追加のコマンドアカウンティング定義を作成します。

VTY 回線の設定パラメータの定義

すべての Cisco IOS ルータには、デフォルトで 5 本の VTY 回線（ラベル 0 ～ 4）が設定されており、これらの回線は次のように設定されています。

- 許可されるすべてのユーザは、すべてのコンフィギュレーション コマンド（権限レベル 15）を含む、ルータへの権限付きアクセス権を持ちます。
- VTY 回線は、ユーザ入力がなくなってから 10 分経過後に切断されます。
- 着信接続は許可されません。
- 発信接続では Telnet だけがサポートされます。

Security Manager を使用して、これらの 5 本の VTY 回線のデフォルト設定を変更したり、追加の回線（最大 16 本）を設定したりできます。さらに、各回線に次の設定を行うこともできます。

- 回線にアクセスするためのパスワード
- 回線上のすべての EXEC セッションをディセーブルにするかどうか
- 回線上で許可される接続を制限する着信 ACL と発信 ACL
- 回線上で VRF 接続を許可するかどうか

VTY 回線のグループの定義

複数の VTY 回線を連続したグループとして設定できます。これにより、1 つの手順でグループ内のすべての回線に同じ設定を定義できます。グループ内のすべての回線は、0 ～ 4 または 6 ～ 15 のどちらかの範囲内である必要があります。グループがこれらの 2 つの範囲にまたがることはできません。

VTY 回線 5 を設定するためのルールは次のとおりです。回線 5 は回線 0 ～ 4 と同じ定義に含めることができますが、回線 5 よりも上の回線が設定されていない場合にかぎります。回線 5 よりも上の回線が設定されている場合は、設定が同じでも回線 5 を回線 0 ～ 4 の定義に含めることはできません。設定が同じであれば、回線 5 を回線 5 よりも上の回線の定義に含めることができます。

たとえば、回線 0 ～ 5 のすべてがある設定を共有し、回線 6 ～ 9 の設定が異なる場合は、3 つの定義を作成する必要があります。1 つめは回線 0 ～ 4 の定義、2 つめは回線 5 の定義、3 つめは回線 6 ～ 9 の定義です。

（注） VTY 回線を設定する場合は、ユーザがデバイスに接続するときに、ユーザにランダムに回線が割り当てられることに留意してください。

（注） 定義は VTY 回線ごとに 1 つだけ作成できます。既存の定義と重複する VTY 回線の定義を作成すると、エラーが表示されます。

（注） Security Manager を使用してデフォルトの VTY 回線（0 ～ 4）を設定すると、その定義によってデバイス上のデフォルト設定が上書きされます。あとでこの定義を Security Manager から削除した場合は、入力プロトコル設定が保持され、他のデフォルト設定が復元されます。これにより、常にデバイスへのリモートアクセスに使用できる VTY 回線を確保できます。

（注） CLI または FlexConfig を使用して、16 本を超える回線がサポートされるデバイスに追加の VTY 回線を設定できます。

関連項目

- Cisco IOS ルータにおける回線アクセス （3157 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）]>[回線アクセス（Line Access）] > [VTY] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[VTY] ページが表示されます。このページのフィールドの説明については、表 872 : [VTY] 回線ページ （3177 ページ）を参照してください。

ステップ 2 [回線（Lines）] テーブルの下にある [追加（Add）] ボタンをクリックするか、回線の定義を選択して [編集（Edit）] ボタンをクリックします。[VTY Lines] ダイアログボックスの [Setup] タブが表示されます。このタブのフィールドの説明については、表 873 : [VTY Line] ダイアログボックス （3179 ページ）を参照してください。

ステップ 3 VTY 回線の相対回線番号を入力します。VTY 回線のグループを設定する場合は、グループの最初と最後の番号を表示されたフィールドに入力します。

ステップ 4 （任意）コンソール回線にアクセスするためのパスワードを入力し、[Confirm] フィールドに再入力します。

ステップ 5 （任意）このVTY回線（または回線のグループ）のユーザに付与するデフォルト権限（15）を変更します。

ステップ 6 （任意）[この回線を介したルータへのEXECセッションをすべて無効にする（Disable all the EXEC sessions to the router via this line）] チェックボックスをオンにして、この VTY 回線（または回線のグループ）を介した着信接続を阻止します。

ステップ 7 （任意）デフォルトのタイムアウトを変更します。この時間の経過後もユーザ入力が検出されない場合は、回線が切断されます。

（注） この値を 0 に設定するとタイムアウトがディセーブルになります。タイムアウトがディセーブルになると、放棄されたセッションにより、利用可能なVTY回線がブロックされる可能性があります。また、ネットワークのセキュリティが低下する可能性もあります。

ステップ 8 （任意）このVTY回線（または回線のグループ）上のインバウンド接続およびアウトバウンド接続に使用できるプロトコルを指定します。

- [All]：サポートされるすべてのプロトコルが許可されます。
- [None]：プロトコルは許可されません。
- [Protocol]：SSH、Telnet、rlogin のプロトコルの 1 つ以上をイネーブルにします。

注意 インバウンド接続設定を [None] に設定すると、Security Manager は展開後にデバイスに接続できなくなる可能性があります。

（注） VTY 回線で SSH および rlogin プロトコルを許可する場合は、AAA 認証を設定する必要があります。VTY 回線の AAA 設定の定義 （3164 ページ）を参照してください。

ステップ 9 （任意）ACL の名前を入力して、デバイスとこれらのリスト内のアドレス間における着信接続と発信接続を制限します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。標準 ACL または拡張 ACL の中から選択できます。

ヒント 管理アクセスのためだけに VTY 回線を予約する場合は、インバウンド ACL を定義することを推奨します。

ステップ 10 （任意）[AAA] タブをクリックして、このVTY回線（または回線のグループ）の認証、許可、アカウンティング設定を定義します。VTY 回線の AAA 設定の定義 （3164 ページ）を参照してください。

ステップ 11 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Lines] テーブルに表示されます。

（注） VTY 回線の定義を削除するには、その定義を選択し、[削除（Delete）] をクリックします。IOS デバイスからVTY回線を削除した場合、後続の回線もすべて削除されます。たとえば、デバイスに回線 0 ～ 9 が含まれる場合、回線 5 を削除すると、回線 6 ～ 9 も削除されます。回線 0 ～ 4 の定義を Security Manager から削除した場合、ルータはインバウンド プロトコル定義を保持し、デバイス上のこれらの回線に対する他のデフォルト設定を復元します。これにより、5 本の VTY 回線を常に使用できるようになります。

VTY 回線の AAA 設定の定義

デフォルトでは、認証、許可、アカウンティングは VTY 回線に対して実行されません。これらのアクセス制御オプションの 1 つ以上を設定するときに、デバイスの AAA ポリシーで定義されたデフォルトの方式リストを使用するか、1 つ以上の AAA 方式を含むカスタム方式リストを定義できます。

はじめる前に

- VTY 回線または VTY 回線のグループの基本パラメータを定義します。 VTY 回線の設定パラメータの定義 （3161 ページ） を参照してください。

関連項目

- VTY 回線の設定パラメータの定義 （3161 ページ）
- Cisco IOS ルータにおける回線アクセス （3157 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[VTY]ページが表示されます。このページのフィールドの説明については、表 872 : [VTY] 回線ページ （3177 ページ） を参照してください。

ステップ 2 [回線（Lines）] テーブルで VTY 回線の定義を選択し、[編集（Edit）] ボタンをクリックして [VTY回線（VTY Line）] ダイアログボックスを表示します。次に、[認証（Authentication）] タブをクリックします。

ステップ 3 （任意）VTY 回線にアクセスしようとするユーザに対して実行する認証方式を選択します。

このタブのフィールドの説明については、表 875 : [VTY Line] ダイアログボックス - [Authentication] タブ （3183 ページ） を参照してください。

（注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

ステップ 4 （任意）[Authorization] タブで、VTY 回線にアクセスして EXEC セッションを開始するユーザに対して実行する認可方式を選択します。

[Authorization] タブのフィールドの説明については、表 876 : [VTY Line] ダイアログボックス - [Authorization] タブ （3185 ページ） を参照してください。

（注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。

ステップ 5 （任意）特定の権限レベルのコマンド認可定義を作成します。

a) [コマンド認可（Commands Authorization）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Authorization Override] ダイアログボックス （3156 ページ）が表示されます。

b) 必要に応じてコマンド認可定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、認可方式が [Commands Authorization] テーブルに表示されます。

d) 5.a （3165 ページ）～5.c （3165 ページ）を繰り返して、追加のコマンド認可定義を作成します。

ステップ 6 （任意）[Accounting] タブで、VTY 回線にアクセスしようとするユーザに対して実行する EXEC および接続アカウンティング方式を選択します。

[Accounting] タブのフィールドの説明については、表 877 : [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ）を参照してください。

ステップ 7 （任意）特定の権限レベルのコマンド アカウンティング定義を作成します。

a) [コマンドアカウンティング（Commands Accounting）] テーブルの下の [追加（Add）] ボタンをクリックします。[Command Accounting] ダイアログボックス - [Line Access] （3192 ページ）が表示されます。

b) 必要に応じてコマンド アカウンティング定義を設定します。

c) [OK] をクリックダイアログボックスが閉じ、アカウンティング方式が [Commands Accounting] テーブルに表示されます。

d) 7.a （3165 ページ）～7.c （3165 ページ）を繰り返して、追加のコマンドアカウンティング定義を作成します。

[Console] ポリシー ページ

[Console] ページでは、コンソール ポートを介したルータへのアクセスを設定します。[Console] ポリシー ページの次のタブから Cisco IOS ルータ上のコンソール ポリシーを設定できます。

- [Console] ページ - [Setup] タブ （3166 ページ）
- [Console] ページ - [Authentication] タブ （3168 ページ）
- [Console] ページ - [Authorization] タブ （3170 ページ）
- [Console] ページ - [Accounting] タブ （3172 ページ）

詳細については、Cisco IOS ルータにおける回線アクセス （3157 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [コンソール（Console）]** を選択します。[コンソール

（Console）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [VTY] ポリシー ページ （3177 ページ）

[Console] ページ - [Setup] タブ

[Console] ページの [Setup] タブでは、コンソール ポートの基本パラメータを定義します。これには、ポートにアクセスするためのパスワード、ユーザに割り当てる権限レベル、許可するプロトコル、アクセスを制限する ACL などがあります。

ナビゲーション パス

[Console] ポリシー ページ （3165 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- [Console] ページ - [Authentication] タブ （3168 ページ）
- [Console] ページ - [Authorization] タブ （3170 ページ）
- [Console] ページ - [Accounting] タブ （3172 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （3179 ページ）

フィールド リファレンス

表 868 : [Console] ページ - [Setup] タブ

要素	説明
[パスワード（Password）]	コンソール ポートにアクセスするためのパスワード。 パスワードは大文字と小文字が区別され、最大 80 文字の英数字を含むことができます。最初の文字を数値にはできません。スペースは使用できません。 [Confirm] フィールドにパスワードを再入力します。

要素	説明
特権レベル	コンソール ポートに接続するユーザに割り当てる権限レベル。有効値の範囲は 0 ～ 15 です。 • 0：**disable**、**enable**、**exit**、**help**、および **logout** の各コマンドにだけアクセス権を付与します。 • 1：ルータへの権限なしアクセスをイネーブルにします（通常の EXEC モードでは権限が使用されます）。 • 15：ルータへの権限付きアクセスをイネーブルにします（従来のイネーブル権限）。 （注） レベル 2 ～ 14 は、通常はデフォルト設定では使用されませんが、通常はレベル 15 にあるコマンドをそれよりも低いレベルに移動し、通常はレベル 1 にあるコマンドをそれよりも高いレベルに移動することで、カスタム設定を作成できます。CLI を使用するか FlexConfig を定義することにより、コマンドの権限レベルを設定できます。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。
Disable all the EXEC sessions to the router via this line	選択すると、この回線を介した EXEC セッションがディセーブルになります。このオプションは、コンソール上での発信接続だけを許可する場合に選択します。このオプションは、回線を独占する可能性がある割り込みデータがコンソール ポートに着信しないようにする場合に役立ちます。 選択を解除すると、コンソール ポートで EXEC セッションがイネーブルになります。これがデフォルトです。 （注） このオプションを選択すると、コンソール ポートを介したデバイスへのすべてのアクセスがブロックされます。
Exec Timeout	EXEC コマンド インタープリタがコンソール ポート上のユーザ入力を検出するまで待機する時間（秒数）。入力が検出されない場合は、回線が切断されます。有効値の範囲は 0 ～ 2147483 です。デフォルトは 600（10 分）です。値を 0 に設定するとタイムアウトがディセーブルになります。 （注） タイムアウトは秒単位で定義されますが、CLI には [mm ss] の形式で表示されます。

要素	説明
Output Protocols	コンソール ポート上の発信接続に使用できるプロトコル。 • [All]：サポートされるすべてのプロトコルが許可されます。サポートされるプロトコルには、LAT、MOP、NASI、PAD、rlogin、SSH、Telnet、および V.120 があります。 • [None]：プロトコルは許可されません。これにより、ポートを発信接続で使用できなくなります。 • [Protocol]：次のプロトコルの 1 つ以上をイネーブルにします。 • [SSH]：セキュア シェル プロトコル。 • [Telnet]：標準 TCP/IP 端末エミュレーション プロトコル。 • [rlogin]：UNIX rlogin プロトコル。 （注） [SSH] と [rlogin] では、AAA 認証を設定する必要があります。[Console] ページ - [Authentication] タブ （3168 ページ）を参照してください。 （注） すべての IOS ソフトウェア バージョンで rlogin が出力プロトコルとしてサポートされるわけではありません。
Inbound Access List	コンソール ポート上の着信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Permit VRF Interface Connections	インバウンド ACL がコンソール ポート上で定義されている場合にだけ適用されます。 選択されている場合は、VRF に属するインターフェイスからの着信接続を受け入れます。選択解除されている場合は、VRF に属するインターフェイスからの着信接続を拒否します。
Outbound Access List	コンソール ポート上の発信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。

[Console] ページ - [Authentication] タブ

[Console] ページの [Authentication] タブでは、コンソール ポートにアクセスしようとするユーザに対して実行する AAA 認証方式を定義します。

ナビゲーション パス

[Console] ポリシー ページ （3165 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- [Console] ページ - [Setup] タブ （3166 ページ）
- [Console] ページ - [Authorization] タブ （3170 ページ）
- [Console] ページ - [Accounting] タブ （3172 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）

フィールド リファレンス

表 869 : [Console] ページ - [Authentication] タブ

要素	説明
Authenticate Using	コンソール ポートの認証設定： • [None]：認証は実行されません。これがデフォルトです。 • [Local Database]：ローカル ユーザ名データベースを認証に使用します。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。 [AAA] ページ - [Authentication] タブ （3120 ページ）を参照してください。 • [Custom Method List]：[Authentication Method List] フィールドで指定された認証方式を使用します。 （注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

要素	説明
Prioritized Method List	[Custom Method List] が認証方式として選択されている場合にだけ適用されます。 ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[Console] ページ - [Authorization] タブ

[Console] ページの [Authorization] タブでは、コンソール ポートにアクセスするユーザに対して実行する EXEC およびコマンド認可方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。AAA サービスの定義 （3117 ページ）を参照してください。

ナビゲーション パス

[Console] ポリシー ページ （3165 ページ）に移動し、[承認（Authorization）] タブをクリックします。

関連項目

- [Console] ページ - [Setup] タブ （3166 ページ）
- [Console] ページ - [Authentication] タブ （3168 ページ）
- [Console] ページ - [Accounting] タブ （3172 ページ）
- [VTY Line] ダイアログボックス - [Authorization] タブ （3184 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *870 : [Console]* ページ - *[Authorization]* タブ

要素	説明
[EXEC Authorization] 設定	
Authorize EXEC Operations Using	ユーザが EXEC セッションの実行を許可されるかどうかを決定する認可方式。 • [None]：認可は実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。[AAA] ページ - [Authorization] タブ （3121 ページ）を参照してください。 • [Custom Method List]：[EXEC Method List] フィールドで指定された認可方式を使用します。
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。Enter the names of one or more AAA server group objects（up to four）, or click **Select** to select them. オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。 （注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Authorization] ダイアログボックス - [Line Access] （3191 ページ）が開きます。ここから、コマンド認可定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Authorization] ダイアログボックス - [Line Access] （3191 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[Console] ページ - [Accounting] タブ

[Console] ページの [Accounting] タブでは、コンソール ポートにアクセスするユーザに対して実行する EXEC、接続、およびコマンド アカウンティング方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。 AAA サービスの定義 （3117 ページ）を参照してください。

ナビゲーション パス

[Console] ポリシー ページ （3165 ページ）に移動し、[アカウンティング（Accounting）] タブをクリックします。

関連項目

- [Console] ページ - [Setup] タブ （3166 ページ）
- [Console] ページ - [Authentication] タブ （3168 ページ）
- [Console] ページ - [Authorization] タブ （3170 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 871 : [Console] ページ - [Accounting] タブ

要素	説明
[EXEC Accounting] 設定	

要素	説明
Perform EXEC Accounting Using	ユーザEXECセッションに関する基本情報の記録に使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの EXEC アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ（3124 ページ）を参照してください。 • [Custom Method List]：[EXEC Method List] フィールドで指定されたアカウンティング方式を使用します。 EXECアカウンティングは、ユーザ名、日付、開始および終了時刻、アクセス サーバの IP アドレスなど、EXEC セッションに関する基本的な詳細を記録します。
Generate Accounting Records for	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Method List] が EXEC 方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Connection Accounting] 設定	

要素	説明
Perform Connection Accounting Using	コンソール回線を介して確立されたアウトバウンド接続に関する情報を記録するために使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの接続アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ （3124 ページ）を参照してください。 • [Custom Method List]：[Connection Method List] フィールドで指定されたアカウンティング方式を使用します。 接続アカウンティングは、Telnet 接続や rlogin 接続など、回線上の発信接続に関する詳細を記録します。
Generate Accounting Records for	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Command Accounting] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Generate Accounting Records for	プロセスで、デバイスがアカウンティング通知をアカウンティング サーバに送信するポイント。
Enable Broadcast	アカウンティング レコードが複数のサーバに同時にブロードキャストされるかどうか。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （3192 ページ）が開きます。ここから、コマンドアカウンティング定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （3192 ページ）が開きます。ここから、コマンドアカウンティング定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド アカウンティング定義をテーブルから削除します。

[VTY] ポリシー ページ

[VTY] ページでは、ルータへのリモート アクセス用に最大 16 本の VTY 回線を設定します。個々の回線を設定する以外に、同じ定義を共有する回線のグループを設定できます。

詳細については、Cisco IOS ルータにおける回線アクセス （3157 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [回線アクセス（Line Access）] > [VTY] を選択します。[VTY] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- [Console] ポリシー ページ （3165 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *872 : [VTY]* 回線ページ

要素	説明
回線（Line）	VTY 回線の相対回線番号。このフィールドには、連続したグループとして設定された複数の VTY 回線を含めることもできます。
Line/Line Group Parameters	
Input Protocols	VTY 回線上の着信接続に使用できるプロトコル。
Output Protocols	VTY 回線上の発信接続に使用できるプロトコル。

要素	説明
特権レベル	ユーザに割り当てる権限レベル。
Exec Timeout	EXEC コマンド インタープリタがユーザ入力を検出するまで待機する時間。
Inbound ACL	インバウンド トラフィックの制限に使用する ACL。
Outbound ACL	アウトバウンド トラフィックの制限に使用する ACL。
認証	使用する AAA 認証のタイプ。
許可	使用する AAA 認可のタイプ。
アカウンティング	使用する AAA アカウンティングのタイプ。
[VTY] 回線ページのボタン	
[追加（Add）] ボタン	[VTY Line] ダイアログボックス （3178 ページ）が開きます。ここから、VTY 回線または回線グループを定義できます。
[編集（Edit）] ボタン	[VTY Line] ダイアログボックス （3178 ページ）が開きます。ここから、VTY 回線または回線グループを編集できます。
[削除（Delete）] ボタン	選択した VTY 回線をテーブルから削除します。 IOS デバイスから VTY 回線を削除した場合、後続の回線もすべて削除されます。たとえば、デバイスに回線 0 ～ 9 が含まれる場合、回線 5 を削除すると、回線 6 ～ 9 も削除されます。 （注） デバイス上のデフォルトの VTY 回線（0 ～ 4）を削除した場合は、入力プロトコル設定が保持され、他のデフォルト設定が復元されます。これにより、デバイスへのリモート アクセスが中断されるのを防止できます。

[VTY Line] ダイアログボックス

[VTY Line] ダイアログボックスでは、リモート ユーザによるルータへのアクセスを可能にする 1 つ以上の VTY 回線（最大 16 本）を設定します。VTY 回線を設定するときに、回線にアクセスするユーザに対して実行する認証および認可のタイプを定義できます。

ナビゲーション パス

[VTY] ポリシー ページ （3177 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Cisco IOS ルータにおける回線アクセス （3157 ページ）
- [Console] ポリシー ページ （3165 ページ）

フィールド リファレンス

表 *873 : [VTY Line]* ダイアログボックス

要素	説明
[Setup] タブ	VTY 回線または回線グループの基本設定を定義します。 [VTY Line] ダイアログボックス - [Setup] タブ （3179 ページ）を参照してください。
[Authentication] タブ	VTY 回線にアクセスするユーザに対して実行する AAA 認証のタイプを定義します。 [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）を参照してください。
[Authorization] タブ	VTY 回線にアクセスするユーザに対して実行する AAA 認可のタイプを定義します。 [VTY Line] ダイアログボックス - [Authorization] タブ （3184 ページ）を参照してください。
[Accounting] タブ	VTY 回線にアクセスするユーザに対して実行する AAA アカウンティングのタイプを定義します。 [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ） を参照してください。

[VTY Line] ダイアログボックス - [Setup] タブ

[VTY Line] ダイアログボックスの [Setup] タブでは、VTY 回線の基本パラメータを定義します。これには、回線にアクセスするためのパスワード、ユーザに割り当てる権限レベル、回線上で許可するプロトコル、アクセスを制限する ACL などがあります。

ナビゲーション パス

[VTY Line] ダイアログボックス （3178 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- VTY 回線の設定パラメータの定義 （3161 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）
- [VTY Line] ダイアログボックス - [Authorization] タブ （3184 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ）
- [Console] ページ - [Setup] タブ （3166 ページ）

フィールド リファレンス

表 *874 : [VTY Line]* ダイアログボックス - *[Setup]* タブ

要素	説明
Starting VTY Line Number	VTY 回線の相対回線番号。VTY 回線のグループを設定する場合は、グループの最初の回線の番号を入力します。有効値の範囲は 0 ～ 15 です。 （注） サポートされる VTY 回線の数（4 ～数千）はルータごとに異なりますが、Security Manager によってサポートされるデバイスあたりの回線数は最大 16 です。同じ回線番号を複数回設定することはできません。
Ending VTY Line Number	回線のグループを設定する場合にだけ適用されます。 グループ内の最後の VTY 回線の相対回線番号。 （注） 回線のグループを設定する場合、グループ内のすべての回線は 0 ～ 4 または 6 ～ 15 のどちらかの範囲内である必要があります。
パスワード	この VTY 回線にアクセスするためのパスワード。 パスワードは大文字と小文字が区別され、最大 80 文字の英数字を含むことができます。最初の文字を数値にはできません。スペースは使用できません。 [Confirm] フィールドにパスワードを再入力します。
特権レベル	この VTY 回線上のユーザに割り当てる権限レベル。有効値の範囲は 0 ～ 15 です。 • 0：**disable**、**enable**、**exit**、**help**、および **logout** の各コマンドにだけアクセス権を付与します。 • 1：ルータへの権限なしアクセスをイネーブルにします（通常の EXEC モードでは権限が使用されます）。 • 15：ルータへの権限付きアクセスをイネーブルにします（従来のイネーブル権限）。 （注） レベル 2 ～ 14 は、通常はデフォルト設定では使用されませんが、通常はレベル 15 にあるコマンドをそれよりも低いレベルに移動し、通常はレベル 1 にあるコマンドをそれよりも高いレベルに移動することで、カスタム設定を作成できます。CLI を使用するか FlexConfig を定義することにより、コマンドの権限レベルを設定できます。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。

要素	説明
Disable all the EXEC sessions to the router via this line	選択すると、この回線を介した EXEC セッションがディセーブルになります。このオプションは、この回線上の発信接続だけを許可する場合に選択します。このオプションは、回線を独占する可能性がある割り込みデータが特定の回線に着信しないようにする場合に役立ちます。 選択を解除すると、この回線を介した EXEC セッションがイネーブルになります。これがデフォルトです。
Exec Timeout	EXEC コマンドインタープリタが回線上のユーザ入力を検出するまで待機する時間（秒数）。入力が検出されない場合は、回線が切断されます。有効値の範囲は 0 ～ 2147483 です。デフォルトは 600（10 分）です。値を 0 に設定するとタイムアウトがディセーブルになります。 （注） タイムアウトは秒単位で定義されますが、CLI には [mm ss] の形式で表示されます。
Input Protocols	この回線上の着信接続に使用できるプロトコル。 • [All]：サポートされるすべてのプロトコルが許可されます。サポートされるプロトコルには、LAT、MOP、NASI、PAD、rlogin、SSH、Telnet、および V.120 があります。 • [None]：プロトコルは許可されません。これにより、ポートを SSH、Telnet、および rlogin の着信接続で使用できなくなります。 （注） 入力プロトコル設定を [None] に設定すると、Security Manager は展開後にデバイスに接続できなくなる可能性があります。HTTP ポリシーで SSL をイネーブルにすると、SSL を使用してデバイスを管理できます。[HTTP] ページ - [Setup] タブ （3152 ページ）を参照してください。 • [Protocol]：次のプロトコルの 1 つ以上をイネーブルにします。 • [SSH]：セキュア シェル プロトコル。 • [Telnet]：標準 TCP/IP 端末エミュレーション プロトコル。 • [rlogin]：UNIX rlogin プロトコル。 （注） [SSH] と [rlogin] では、AAA 認証を設定する必要があります。[VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）を参照してください。 （注） すべての IOS ソフトウェア バージョンで rlogin が入力プロトコルとしてサポートされるわけではありません。

要素	説明
Output Protocols	この回線上の発信接続に使用できるプロトコル。 • [All]：サポートされるすべてのプロトコルが許可されます。サポートされるプロトコルには、LAT、MOP、NASI、PAD、rlogin、SSH、Telnet、および V.120 があります。 • [None]：プロトコルは許可されません。これにより、ポートを発信接続で使用できなくなります。 • [Protocol]：次のプロトコルの 1 つ以上をイネーブルにします。 • [SSH]：セキュア シェル プロトコル。 • [Telnet]：標準 TCP/IP 端末エミュレーション プロトコル。 • [rlogin]：UNIX rlogin プロトコル。 （注） [SSH] と [rlogin] では、AAA 認証を設定する必要があります。[VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）を参照してください。 （注） すべての IOS ソフトウェア バージョンで rlogin が出力プロトコルとしてサポートされるわけではありません。
Inbound Access List	この回線上の着信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。
Permit VRF Interface Connections	インバウンドACLがこの回線上で定義されている場合にだけ適用されます。 選択されている場合は、VRF に属するインターフェイスからの着信接続を受け入れます。選択解除されている場合は、VRF に属するインターフェイスからの着信接続を拒否します。
Outbound Access List	この回線上の発信接続を制限する ACL オブジェクトの名前。ACL オブジェクトの名前を入力するか、[選択（Select）] をクリックして選択します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。

[VTY Line] ダイアログボックス - [Authentication] タブ

[VTY Line] ダイアログボックスの [Authentication] タブでは、選択した VTY 回線または回線グループにアクセスしようとするユーザに対して実行する認証方式を定義します。

ナビゲーション パス

[VTY Line] ダイアログボックス （3178 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- VTY 回線の AAA 設定の定義 （3164 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （3179 ページ）
- [VTY Line] ダイアログボックス - [Authorization] タブ （3184 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ）
- [Console] ページ - [Authentication] タブ （3168 ページ）

フィールド リファレンス

表 875 : [VTY Line] ダイアログボックス - [Authentication] タブ

要素	説明
Authenticate Using	VTY 回線の認証設定： • [None]：認証は実行されません。これがデフォルトです。 • [Local Database]：ローカル ユーザ名データベースを認証に使用します。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスの AAA ポリシーで定義されているデフォルトの認証方式リストを使用します。 [AAA] ページ - [Authentication] タブ （3120 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定された認証方式を使用します。 （注） ローカル認証を選択する場合は、展開の前に設定全体をプレビューして、**aaa new-model** コマンドが、（たとえば、AAA ポリシーで方式リストを設定することにより）別のポリシーで設定されていないこと、またはそのデバイス自体にすでに設定されていることを確認します。

要素	説明
Prioritized Method List	[Custom Method List] が認証方式として選択されている場合にだけ適用されます。 ユーザを認証する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認証を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[VTY Line] ダイアログボックス - [Authorization] タブ

[VTY Line] ダイアログボックスの [Authorization] タブでは、選択した VTY 回線または回線グループにアクセスするユーザに対して実行する EXEC およびコマンド認可方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。AAA サービスの定義 （3117 ページ）を参照してください。

ナビゲーション パス

[VTY Line] ダイアログボックス （3178 ページ）に移動し、 **Authorization** tab.

関連項目

- VTY 回線の AAA 設定の定義 （3164 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （3179 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）
- [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ）
- [Console] ページ - [Authentication] タブ （3168 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *876 : [VTY Line] ダイアログボックス - [Authorization] タブ*

要素	説明
[EXEC Authorization] 設定	
Authorize EXEC Operations Using	ユーザが EXEC セッションの実行を許可されるかどうかを決定する認可方式。 • [None]：認可は実行されません。これがデフォルトです。 • [AAAポリシーデフォルトリスト（AAA Policy Default List）]：デバイスのAAAポリシーで定義されているデフォルトの認証方式リストを使用します。[AAA] ページ - [Authorization] タブ （3121 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定された認可方式を使用します。
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）]をクリックして選択します。オブジェクトセレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。 （注） RADIUS では、認証と認可に同じサーバが使用されます。したがって、認証に RADIUS 方式リストを定義する場合は、認可にも同じ方式リストを定義する必要があります。
[Command Authorization] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）]ボタン	[Command Authorization] ダイアログボックス - [Line Access] （3191 ページ）が開きます。ここから、コマンド認可定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Authorization] ダイアログボックス - [Line Access] （3191 ページ）が開きます。ここから、コマンド認可定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド認可定義をテーブルから削除します。

[VTY Line] ダイアログボックス - [Accounting] タブ

[VTY Line] ダイアログボックスの [Accounting] タブでは、選択した VTY 回線または回線グループにアクセスするユーザに対して実行する EXEC、接続、およびコマンドアカウンティング方式を定義します。

（注） この機能を使用するには、ルータで AAA サービスをイネーブルにする必要があります。そうしないと展開が失敗します。 AAA サービスの定義 （3117 ページ）を参照してください。

ナビゲーション パス

[VTY Line] ダイアログボックス （3178 ページ）に移動し、[アカウンティング（Accounting）] タブをクリックします。

関連項目

- VTY 回線の AAA 設定の定義 （3164 ページ）
- [VTY Line] ダイアログボックス - [Setup] タブ （3179 ページ）
- [VTY Line] ダイアログボックス - [Authentication] タブ （3182 ページ）
- [Console] ページ - [Accounting] タブ （3172 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *877 : [VTY Line]* ダイアログボックス - *[Accounting]* タブ

要素	説明
[EXEC Accounting] 設定	

要素	説明
Perform EXEC Accounting Using	ユーザEXECセッションに関する基本情報の記録に使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAA Policy Default List]：デバイスの AAA ポリシーで定義されているデフォルトの EXEC アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ （3124 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定されたアカウンティング方式を使用します。 EXECアカウンティングは、ユーザ名、日付、開始および終了時刻、アクセス サーバの IP アドレスなど、EXEC セッションに関する基本的な詳細を記録します。
Generate Accounting Records for	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が EXEC 方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Method List] が EXEC 方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Connection Accounting] 設定	

要素	説明
Perform Connection Accounting Using	VTY 回線を介して確立されたアウトバウンド接続に関する情報を記録するために使用するアカウンティング方式。 • [None]：アカウンティングは実行されません。これがデフォルトです。 • [AAA Policy Default List]：デバイスの AAA ポリシーで定義されているデフォルトの接続アカウンティング方式リストを使用します。[AAA] ページ - [Accounting] タブ （3124 ページ）を参照してください。 • [Custom Method List]：[Prioritized Method List] フィールドで指定されたアカウンティング方式を使用します。 接続アカウンティングは、Telnet 接続や rlogin 接続など、回線上の発信接続に関する詳細を記録します。
Generate Accounting Records for	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。

要素	説明
Prioritized Method List	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 ユーザのアカウンティング方式の作成時に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）]ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。
Enable Broadcast to Multiple Servers	[Custom Method List] が接続方式として選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。
[Command Accounting] 設定	
特権レベル	コマンド認可定義が適用される権限レベル。
Generate Accounting Records for	プロセスで、デバイスがアカウンティング通知をアカウンティング サーバに送信するポイント。
Enable Broadcast	アカウンティング レコードが複数のサーバに同時にブロードキャストされるかどうか。
Prioritized Method List	この権限レベルでユーザを認可するときに使用する方式リスト。
[追加（Add）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （3192 ページ）が開きます。ここから、コマンドアカウンティング定義を設定できます。

要素	説明
[編集（Edit）] ボタン	[Command Accounting] ダイアログボックス - [Line Access] （3192 ページ）が開きます。ここから、コマンドアカウンティング定義を編集できます。
[削除（Delete）] ボタン	選択したコマンド アカウンティング定義をテーブルから削除します。

[Command Authorization] ダイアログボックス - [Line Access]

[Command Authorization] ダイアログボックスでは、特定の権限に関連付けられている EXEC コマンドを認可するときに使用する方式を定義します。これにより、特定の権限レベル（0 ～ 15）に関連付けられているすべてのコマンドを認可できます。

ナビゲーション パス

[Console] ページ - [Authorization] タブ （3170 ページ）または [VTY Line] ダイアログボックス - [Authorization] タブ （3184 ページ）で、[コマンド認可（Command Authorization）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- [Console] ポリシー ページ （3165 ページ）
- [VTY] ポリシー ページ （3177 ページ）

フィールド リファレンス

表 878 : [Command Authorization] ダイアログボックス - [Line Access]

要素	説明
Privilege Level	コマンド認可リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。
AAA Policy Default List	このオプションを選択すると、デバイスの AAA ポリシーで定義されているデフォルトの認可リストがこの権限レベルに関連付けられている EXEC コマンドに適用されます。[Command Accounting] ダイアログボックス （3127 ページ）を参照してください。
Custom Method List	このオプションを選択すると、この権限レベルの認可方式リストを定義できます。

要素	説明
Prioritized Method List	[Custom Method List] オプションが選択されている場合にだけ適用されます。 ユーザを認可する場合に問い合わせる方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（4 つまで）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクト セレクタの上向きおよび下向き矢印を使用して、選択したサーバ グループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してユーザの認可を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

[Command Accounting] ダイアログボックス - [Line Access]

[Command Accounting] ダイアログボックスでは、特定の権限に対して実行される EXEC コマンドに関する情報を記録するときに使用する方式を定義します。各アカウンティング レコードには、その権限レベルに対して実行されるコマンドのリストと、各コマンドが実行された日時およびそのコマンドを実行したユーザ名が含まれます。

ナビゲーション パス

[Console] ページ - [Accounting] タブ （3172 ページ）または [VTY Line] ダイアログボックス - [Accounting] タブ （3186 ページ）で、[コマンドアカウンティング（Command Accounting）] テーブルの下にある [追加（Add）] ボタンをクリックします。

関連項目

- [Console] ポリシー ページ （3165 ページ）
- [VTY] ポリシー ページ （3177 ページ）

フィールド リファレンス

表 879 : [Command Accounting] ダイアログボックス - [Line Access]

要素	説明
Privilege Level	コマンドアカウンティング リストを定義する権限レベル。有効値の範囲は 0 ～ 15 です。 （注） 値を定義しない場合は、デフォルトでレベル 1 が割り当てられます。この値はデバイス設定に表示されません。

要素	説明
AAA Policy Default List	このオプションを選択すると、デバイスの AAA ポリシーで定義されているデフォルトのアカウンティングリストがこの権限レベルに対して実行される EXEC コマンドに適用されます。
Custom Method List	このオプションを選択すると、この権限レベルのアカウンティング方式リストを定義できます。
Generate Accounting Records for	[Custom Method List] が選択されている場合にだけ適用されます。 デバイスがアカウンティング通知をアカウンティング サーバにいつ送信するかを定義します。 • [Start and Stop]：ユーザ プロセスの開始時と終了時にアカウンティング レコードを生成します。アカウンティングサーバーが「start」アカウンティングレコードを受信するかどうかにかかわらず、ユーザープロセスが開始されます。これがデフォルトです。 • [Stop Only]：ユーザ プロセスの終了時にだけアカウンティング レコードを生成します。 • [None]：アカウンティング レコードは生成されません。
Prioritized Method List	[Custom Method List] オプションが選択されている場合にだけ適用されます。 ユーザのアカウンティング レコードの作成時に使用するアカウンティング方式の順序付きリストを定義します。1 つ以上の AAA サーバー グループ オブジェクト（最大 4 つ）の名前を入力するか、[選択（Select）] をクリックして選択します。オブジェクトセレクタの上向きおよび下向き矢印を使用して、選択したサーバグループを使用する順序を定義します。必要なオブジェクトが表示されていない場合は、[作成（Create）] ボタンをクリックして作成します。 デバイスは、最初にリスト内の最初の方式を使用してアカウンティングの実行を試みます。その方式で応答がない場合、デバイスは応答を受信するまで次の方式を順番に試します。 （注） 方式として [None] を選択した場合は、リストの最後の方式として表示される必要があります。

要素	説明
Enable Broadcast to Multiple Servers	[Custom Method List] が選択されている場合にだけ適用されます。 選択されている場合、複数の AAA サーバへのアカウンティング レコードの送信をイネーブルにします。アカウンティング レコードは、方式リストに定義されている各 AAA サーバ グループ内の最初のサーバに同時に送信されます。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップ サーバが使用されます。 選択解除されている場合、アカウンティング レコードは、方式リストに定義されている最初の AAA サーバ グループ内の最初のサーバにだけ送信されます。

Cisco IOS ルータにおける任意の SSH 設定

Secure Shell（SSH; セキュア シェル）はアプリケーションであり、暗号化を使用してクライアントとサーバ間のセキュアな通信を提供するプロトコルです。SSH を使用すると、リモートから VTY 回線を介して Cisco IOS ルータに接続したり、EXEC セッションを確立したりできます。セキュリティ面が懸念される環境では、Telnet や rlogin などの他のプロトコルの代わりに SSH を使用することを推奨します。

Security Manager に Cisco IOS ルータを追加するには、それらのすべてのルータに SSH が設定されている必要があります。これは、Security Manager は SSL 以外に SSH を使用してルータと通信するためです。SSH ポリシーを使用すると、選択したデフォルト設定を変更したり、選択した任意の設定を定義したりできます。

関連項目

- 任意の SSH 設定の定義　（3194 ページ）
- デバイスの通信要件について　（71 ページ）
- SSH の設定　（77 ページ）

任意の SSH 設定の定義

SSH は、デフォルトでは次のように設定されます。

- SSH バージョン 1 と SSH バージョン 2 の両方がサポートされます。
- ネゴシエーション フェーズは、120 秒後に正常に完了しない場合は終了します。
- ルータは切断前に SSH クライアントの認証を 3 回試行します。

Security Manager を使用して、次のデフォルト設定を変更したり、任意で次の設定を定義したりできます。

- SSH パケットの送信元インターフェイス
- 使用する RSA キー ペアの名前
- 次の展開時にキーを生成するかどうか

はじめる前に

- ルータで SSH がイネーブルになっていることを確認します。 デバイスの通信要件について （71 ページ）を参照してください。
- ルータ上の VTY 回線でインバウンド SSH トラフィックが許可されていることを確認します。 VTY 回線の設定パラメータの定義 （3161 ページ）を参照してください。
- ルータでホスト名とドメイン名が設定されていることを確認します（別の RSA キー ペアを使用する場合を除く）。このために Security Manager で CLI またはホスト名ポリシーを使用できます。 Cisco IOS ルータにおけるホスト名とドメイン名 （3212 ページ）を参照してください。

関連項目

- Cisco IOS ルータにおける任意の SSH 設定 （3194 ページ）
- SSH の設定 （77 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Secure Shell] ページが表示されます。このページのフィールドの説明については、 [Secure Shell] ポリシー ページ （3196 ページ）を参照してください。

ステップ 2 （任意）次のデフォルト設定を変更します。

a) サポートする SSH のバージョン
b) SSH 接続のネゴシエーション フェーズを完了するためのタイムアウト
c) SSH クライアントの認証を試行する回数

ステップ 3 （任意）[送信元インターフェイス（Source Interface）] フィールドに、インターフェイスまたはインターフェイスロールの名前を入力します。これが、SSH クライアントに送信されるすべての SSH パケットの送信元インターフェイスとして使用されます。あるいは、[選択（Select）] をクリックしてリストからインターフェイス ロール オブジェクトを選択するか、新しいインターフェイス ロール オブジェクトを作成します。送信元インターフェイスには IP アドレスが必要です。

このフィールドに値を入力しない場合は、宛先に最も近いインターフェイスのアドレスが使用されます。

ステップ 4 （任意）SSH 接続に使用する RSA キー ペアの名前を入力します。このフィールドに値を入力しない場合は、ホスト名とドメイン名に基づくキー ペアが使用されます。

ヒント CLI コマンド show crypto key mypubkey rsa を使用して、デバイスに設定されている各キー ペアの名前と値を表示します。

ステップ 5 （任意）SSHに使用するRSAキーペアをルータで再生成する場合は、[展開中にキーを再生成する（Regenerate Key During Deployment）]チェックボックスをオンにします。このオプションは、キーの機密性が失われる可能性がある場合に便利です。キーの再生成に使用する係数のサイズを入力します。

（注） 展開後にこのポリシーに戻ってチェックボックスをオフにする必要があります。チェックボックスをオフにしないと、展開のたびに新しいキーが生成されます。

（注） このオプションでは、展開中にデバイスとの対話が必要です。したがって、ファイルを展開するときではなく、ライブ デバイスを展開するときにだけ使用する必要があります。

（注） キーペアは、このオプションを選択する前にデバイスにすでに存在する必要があります。そうでないと展開が失敗します（IOS ルータを Security Manager に追加するには、ルータで SSH がイネーブルになっている必要があるため、一般的にはこのような状況になります）。

[Secure Shell] ポリシー ページ

[Secure Shell] ページでは、必要に応じて、ルータ上のデフォルトの SSH 設定を変更したり、他の任意の設定を定義したりできます。

詳細については、Cisco IOS ルータにおける任意の SSH 設定 （3194 ページ）を参照してください。

（注） デバイスを Security Manager に追加する前に、CLI コマンドを使用してデバイスに SSH を設定する必要があります。これは、Security Manager は SSH と SSL を使用して Cisco IOS ルータと通信するためです。詳細については、SSH の設定 （77 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [Secure Shell] を選択します。[Secure Shell] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- デバイスの通信要件について （71 ページ）
- [VTY] ポリシー ページ （3177 ページ）
- [Console] ポリシー ページ （3165 ページ）

フィールド リファレンス

表 *880 : [Secure Shell]* ページ

要素	説明
SSH Version	ルータに接続するときに使用する SSH のバージョン。 • [1 and 2]：SSH バージョン 1 と SSH バージョン 2。これがデフォルトです。 • [1]：SSH バージョン 1 だけ。 • [2]：SSH バージョン 2 だけ。
タイムアウト（Timeout）	接続の切断前に、ルータがネゴシエーション フェーズ中に SSH クライアントの応答を待機する時間。デフォルト値（および最大値）は 120 秒です。 （注） ネゴシエーションが終了して EXEC セッションが開始されると、VTY 回線に設定されているタイムアウトが適用されます。[VTY Line] ダイアログボックス - [Setup] タブ （3179 ページ）を参照してください。
Authentication Retries	ルータが SSH クライアントの認証を試行する回数有効値の範囲は 0 ～ 5 です。デフォルトは 3 です。
送信元インターフェイス（Source Interface）	SSH クライアントに送信されるすべての SSH パケットの送信元アドレス。 このフィールドで値を定義しない場合は、宛先に最も近いインターフェイス（つまり、SSH パケットの送信に使用される出力インターフェイス）のアドレスが使用されます。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
RSA キーペア	SSH 接続に使用する RSA キー ペアの名前。 値を入力しない場合は、ホスト名とドメイン名に基づいて生成された RSA キー ペアが使用されます。これがデフォルトです。 ヒント　CLI コマンド **show crypto key mypubkey rsa** を使用して、デバイスに設定されている各キーペアの名前と値を表示します。これらは、このフィールドに入力できる有効な名前です。
展開中にキーを再生成	選択すると、次回の展開時にルータで RSA キーペアを再生成します。このオプションは、キーの機密性が失われる可能性がある場合に便利です。 選択を解除すると、新しいキー ペアは生成されません。 （注）　このチェックボックスは、展開後に自動的にオフになりません。このポリシーに戻ってチェックボックスの選択を解除しないと、展開を行うたびにキーが再生成されます。 （注）　このオプションでは、展開中にデバイスとの対話が必要です。したがって、ファイルを展開するときではなく、ライブ デバイスを展開するときにだけ使用する必要があります。 （注）　キーペアは、このオプションを選択する前にデバイスにすでに存在する必要があります。そうでないと展開が失敗します（IOS ルータを Security Manager に追加するには、ルータで SSH が有効になっている必要があるため、一般的にはこのような状況になります）。
Modulus Size	[Regenerate Key] チェックボックスがオンになっている場合にだけ適用されます。 新しいキー ペアの生成に使用される係数のサイズ。係数が大きいほどセキュリティが高くなりますが、生成に時間がかかります。有効な値の範囲は 360 ～ 2048 ビットです。デフォルトは 1024 ビットです。

Cisco IOS ルータの SNMP

簡易ネットワーク管理プロトコル（SNMP）は、ネットワーク管理ステーションまたはワークステーションが、スイッチ、ルータ、ファイアウォールデバイスなどのさまざまなタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。SNMP は、プロトコル、データベース構造の仕様、および一連の管理データベース オブジェクトで構成されます。各 SNMP デバイスまたはメンバはコミュニティに含まれ、コミュニティによって各デバイスのアクセス権（読み取り専用または読み取り/書き込み）が決まります。

SNMP は、管理情報ベース（MIB）を介して管理対象デバイスから情報を取得します。MIB は、MIB オブジェクトと呼ばれるコード ブロックのデータベースであり、各 MIB オブジェクトは固有の 1 つの機能を制御します。MIB オブジェクトは、MIB オブジェクト名、説明、デ

フォルト値などを定義する MIB 変数で構成されます。MIB オブジェクトは MIB ツリーという階層構造になっています。

SNMP ポリシーを使用して、ルータで実行されている SNMP エージェントの動作を設定できます。エージェントは、イベントが発生すると、未承諾の情報を SNMP ホストに送り返します。ルータ上で事前に定義された重要なイベントに応答して生成されるこれら未承諾のメッセージは、トラップと呼ばれます。

ここでは、Cisco IOS ルータ上に SNMP ポリシーを作成するために実行するタスクについて説明します。

• SNMP エージェントのプロパティの定義 （3199 ページ）
• SNMP トラップの有効化 （3200 ページ）

SNMP エージェントのプロパティの定義

SNMP エージェントのプロパティを定義するときに、コミュニティストリングとコミュニティストリング タイプ、およびトラップを受信する SNMP ホストのアドレスとプロパティを定義する必要があります。

SNMP コミュニティストリングは MIB に対する組み込みパスワードであり、ルータの動作に関するデータを格納して、リモートユーザーの認証に使用できます。コミュニティストリングには 2 つのタイプがあります。「パブリック」コミュニティストリングは、MIB 内のすべてのオブジェクト（コミュニティストリング自体を除く）への読み取りアクセスを提供し、「プライベート」コミュニティストリングは、MIB 内のすべてのオブジェクト（コミュニティストリングを除く）への読み書きアクセスを提供します。

SNMP ホストは、ルータによって生成されたトラップを受信します。SNMP ホストにアクセスするためのアドレス、パスワード、ポート番号、および使用する SNMP バージョンを定義する必要があります。Security Manager は、SNMP バージョン 1、バージョン 2c（「コミュニティベースの SNMP」とも呼ばれる）、およびバージョン 3（認証と暗号化を提供）をサポートしています。

関連項目

• Cisco IOS ルータの SNMP （3198 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[SNMP] ページが表示されます。このページのフィールドの説明については、表 881 : [SNMP] ページ （3202 ページ）を参照してください。

ステップ 2 MIB へのアクセスに必要なコミュニティ ストリングを定義します。

a) [権限（Permissions）] の下にある [追加（Add）] をクリックして、[権限（Permission）] ダイアログボックスを表示します。

b) ストリングを定義します。使用可能なフィールドの説明については、表 882 : [Permission] ダイアログボックス （3204 ページ）を参照してください。

c) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Permissions] テーブルに表示されます。

（注） SNMP ホストで使用中のコミュニティ ストリングを編集または削除しようとすると、警告が表示されます。操作を続行すると、デバイスは、[トラップ受診者（Trap Receiver）] テーブルに含まれるホストの定義に一致するプライベートの読み取り専用文字列を作成します。

ステップ 3 SNMP エージェントによって生成されたトラップを受信する SNMP ホストを定義します。

a) [トラップ受信者（Trap Receiver）] の下にある [追加（Add）] をクリックして、[トラップ受信者（Trap Receiver）] ダイアログボックスを表示します。

b) ホストを定義します。使用可能なフィールドの説明については、[Trap Receiver] ダイアログボックス （3204 ページ）を参照してください。

c) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Trap Receiver] テーブルに表示されます。

ステップ 4 [SNMP Server Properties] で、この SNMP ポリシーが設定されたルータを担当する管理者の場所と連絡先情報を入力します。

この定義はテキストで指定します。ルータの動作には影響を与えません。SNMP ホストのマネージャが特定のトラップを調査するときに役立つ情報を指定します。

ステップ 5 [トラップの設定（Configure Traps）] をクリックして [SNMP トラップ（SNMP Traps）] ダイアログボックスを表示します。このダイアログボックスは、ルータ上でイネーブルにするトラップを選択するために使用します。詳細については、SNMP トラップの有効化 （3200 ページ）を参照してください。

SNMP トラップの有効化

定義されている条件（リンク アップ、リンク ダウン、syslog イベントなど）が発生すると、ルータはすぐに SNMP トラップとも呼ばれる通知を、指定された SNMP ホスト（管理ステーション）に送信します。

SNMP トラップをイネーブルにするには、関連する各トラップの横にあるチェックボックスをオンにします。複数の関連するトラップをアクティブにするチェックボックスもあります。

（注） イネーブルにした各トラップは、システム リソースを消費します。システム パフォーマンスへの影響を軽減するには、ネットワーク モニタリングに必要なトラップだけを選択します。

関連項目

- Cisco IOS ルータの SNMP （3198 ページ）

ステップ 1 SNMP エージェントのプロパティの定義 （3199 ページ）の説明に従って、Cisco IOS ルータ上の SNMP サーバ ポリシーを定義するための [SNMP] ページを開きます。

ステップ 2 [SNMP] ページで、[トラップの設定（Configure Traps）] をクリックします。[SNMP Traps] ダイアログボックスが表示されます。

ステップ 3 イネーブルにするトラップの各タイプの横にあるチェックボックスをオンにします。トラップは、次の 4 つのカテゴリに分類されます。

- 標準の SNMP トラップ（Authentication、Cold Start、Warm Start など）
- ISAKMP トラップ（IPsec プロセスのフェーズ 1 に関連するトラップ）
- IPsec トラップ（IPsec プロセスのフェーズ 2 に関連するトラップ）
- その他のトラップ（syslog メッセージ、プロトコル関連の通知、CPU 使用率の警告など）

使用可能なトラップの説明については、表 884 : [SNMP Traps] ダイアログボックス （3207 ページ）を参照してください。

（注） IP マルチキャストと CPU トラップを完全に実装するには、コマンドライン インターフェイス（CLI）のコマンドを追加する必要があります。コマンドの入力に使用できる 1 つの方法として、FlexConfig を使用する方法があります。 FlexConfig ポリシーとポリシー オブジェクトについて（432 ページ）を参照してください。

ヒント [すべて選択（Select All）] をクリックしてダイアログボックスに表示されるすべてのトラップをイネーブルにするか、または [すべて選択解除（Deselect All）] をクリックしてすべてのトラップをディセーブルにします。

ステップ 4 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

ヒント このダイアログボックスに表示されない SNMP トラップを設定するには、FlexConfig を定義します。

[SNMP] ポリシー ページ

[SNMP] ページでは、トラップをルータから指定した SNMP ホストに送信するために必要なパラメータを設定します。これらのトラップは、SNMP ホストにルータで発生している重要なイベントを通知する割り込みメッセージです。

詳細については、 SNMP エージェントのプロパティの定義 （3199 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [デバイスアクセス（Device Access）] > [SNMP] を選択します。[SNMP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータの SNMP （3198 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *881 : [SNMP]* ページ

要素	説明
[Permissions] テーブル	
コミュニティ ストリング（Community String）	ルータの MIB へのアクセスに使用するコミュニティストリング。
タイプ（Type）	コミュニティ ストリング タイプ（[read-only] または [read-write]）。
ACL	ルータの MIB へのアクセスが許可される IP アドレスを定義する標準の ACL。
[追加（Add）] ボタン	[Permission] ダイアログボックス （3203 ページ）が開きます。ここから、トラップの生成に必要なコミュニティ ストリングとタイプを入力できます。
[編集（Edit）] ボタン	[Permission] ダイアログボックス （3203 ページ）が開きます。ここから、選択した権限プロファイルを編集できます。
[削除（Delete）] ボタン	選択した権限プロファイルをテーブルから削除します。
[Trap Receiver] テーブル	
ホスト IP アドレス	ルータによって生成されたトラップを受信する SNMP ホストの IP アドレス。

要素	説明
SNMP バージョン（SNMP Version）	ルータによって使用される SNMP バージョン。
UDP ポート（UDP Port）	SNMP ホストによって使用される UDP ポート。
[追加（Add）] ボタン	[Trap Receiver] ダイアログボックス （3204 ページ）が開きます。ここから、ルータによって生成されたトラップを受信する SNMP ホストを定義できます。
[編集（Edit）] ボタン	[Trap Receiver] ダイアログボックス （3204 ページ） を開きます。ここから、選択した SNMP ホストを編集できます。
[削除（Delete）] ボタン	選択した SNMP ホストをテーブルから削除します。
その他のフィールドおよびボタン	
SNMP Server Properties	SNMP サーバ/エージェント（つまりルータ）を担当するシステム管理者の名前と連絡先情報。SNMP ホストを管理する担当者は、異常なイベントの発生元を追跡するときにこの情報を使用できます。 これらの各プロパティの最大長は、スペースを含めて 255 文字です。 （注） これらのフィールドに入力した値はすべてテキストであり、ルータの動作に影響しません。
[Configure Traps] ボタン	ルータが生成する SNMP トラップを選択するためのダイアログボックスを開きます。 [SNMP Traps] ダイアログボックス （3206 ページ） を参照してください。

[Permission] ダイアログボックス

[Permission] ダイアログボックスでは、SNMP ポリシーに必要なコミュニティ ストリングとストリング タイプを定義します。コミュニティ ストリングは、ルータに関する動作データが格納されている管理情報ベース（MIB）にアクセスするための、組み込みパスワードです。

ナビゲーション パス

[SNMP] ポリシー ページ （3201 ページ）に移動し、[権限（Permissions）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [SNMP] ポリシー ページ （3201 ページ）
- [Trap Receiver] ダイアログボックス （3204 ページ）

- [SNMP Traps] ダイアログボックス （3206 ページ）
- SNMP エージェントのプロパティの定義 （3199 ページ）
- Cisco IOS ルータの SNMP （3198 ページ）

フィールド リファレンス

表 *882 : [Permission]* ダイアログボックス

要素	説明
コミュニティ ストリング（Community String）	ルータの MIB にアクセスするためのコミュニティストリング。文字列の長さの範囲は 1 ～ 128 文字です。
アクセス コントロール リスト	Cisco IOS ソフトウェア Release 12.3(2)T 以上（T トレイン）または 12.4 バージョンを実行しているルータだけに適用されます。 ルータの MIB にアクセスできる IP アドレスを含む標準の ACL。ACL を定義すると、コミュニティ ストリングを使用できる送信元アドレスを制限することによって、セキュリティを強化できます。 標準の ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。
Read-Write	このコミュニティ ストリング タイプを選択すると、MIB 内のすべてのオブジェクト（コミュニティ ストリングを除く）への読み書きアクセスが提供されます。
読み取り専用	このコミュニティ ストリング タイプを選択すると、MIB 内のすべてのオブジェクト（コミュニティ ストリングを除く）への読み取り専用アクセスが提供されます。これがデフォルトです。

[Trap Receiver] ダイアログボックス

[Trap Receiver] ダイアログボックスでは、ルータによって生成されたトラップを受信する SNMP ホストを定義します。これには、使用する SNMP のバージョンの定義が含まれます。

ナビゲーション パス

[SNMP] ポリシー ページ （3201 ページ）に移動してから、[トラップの受信者（Trap Receiver）] テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [SNMP] ポリシー ページ （3201 ページ）

- [Permission] ダイアログボックス （3203 ページ）
- [SNMP Traps] ダイアログボックス （3206 ページ）
- SNMP エージェントのプロパティの定義 （3199 ページ）
- Cisco IOS ルータの SNMP （3198 ページ）

フィールド リファレンス

表 *883 : [Trap Receiver]* ダイアログボックス

要素	説明
[ホストIPアドレス（Host IP Address）]	ルータによって生成されたトラップを受信する SNMP ホストの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
SNMP バージョン（SNMP Version）	使用する SNMP のバージョン（バージョン 1、バージョン 2c、またはバージョン 3）。
コミュニティ ストリング（Community String）	バージョン 1 またはバージョン 2c が選択されている場合にだけ適用されます。 SNMP ホストへのアクセスに必要なパスワード。[Confirm] フィールドに文字列をもう一度入力します。 （注） SNMP ホストへのパスワードとして [Permissions] テーブルで定義されている文字列の 1 つを使用することを推奨します。ただし、別のパスワードも入力できます。文字列の長さの範囲は 1 ～ 128 文字です。入力した内容は [Permissions] テーブルに表示されず、読み取り専用です。
ユーザー名	バージョン 3 が選択されている場合にだけ適用されます。 SNMP ホストへのアクセスに必要なパスワード。[Confirm] フィールドに文字列をもう一度入力します。 （注） SNMP ホストへのパスワードとして [Permissions] テーブルで定義されている文字列の 1 つを使用することを推奨します。ただし、別のパスワードも入力できます。文字列の長さの範囲は 1 ～ 128 文字です。入力した内容は [Permissions] テーブルに表示されず、読み取り専用です。

要素	説明
SNMPv3 セキュリティ	バージョン 3 が選択されている場合にだけ適用されます。 SNMP トラフィックに適用するセキュリティのレベル： • [No MD5, No DES]：パケット認証なし。 • [MD5 (auth)]：MD5 認証あり、暗号化なし。 • [DES (priv)]：MD5 認証あり、DES 暗号化あり。
UDP ポート（UDP Port）	SNMP ホストのポート番号。デフォルトは 162 です。有効な値の範囲は 0 ～ 65535 です。

[SNMP Traps] ダイアログボックス

[SNMP Traps] ダイアログボックスでは、SNMP トラップを生成するルータにおけるイベントを選択します。システム パフォーマンスが低下する可能性を軽減するには、ネットワーク モニタリングに必要なトラップだけを選択します。

ヒント　このダイアログボックスに表示されない SNMP トラップを設定するには、FlexConfig を定義します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについて（432 ページ）を参照してください。

ナビゲーション パス

[SNMP] ポリシー ページ （3201 ページ）に移動してから、[トラップの設定（Configure Traps）] をクリックします。

関連項目

- [SNMP] ポリシー ページ （3201 ページ）
- [Permission] ダイアログボックス （3203 ページ）
- [Trap Receiver] ダイアログボックス （3204 ページ）
- SNMP トラップの有効化 （3200 ページ）
- Cisco IOS ルータの SNMP （3198 ページ）

フィールド リファレンス

表 *884 : [SNMP Traps]* ダイアログボックス

要素	説明
[標準SNMPトラップ（Standard SNMP Traps）]	標準 SNMP トラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [Cold start]：SNMP エージェント（または、その他いずれかのトラップ受信エンティティ）の設定が変化する可能性がある方法でルータが再初期化する場合に、トラップを送信します。 • [Warm start]：SNMP エージェント（または、その他いずれかのトラップ受信エンティティ）の設定が変化しない方法でルータが再初期化する場合に、トラップを送信します。 • [Authentication]：コミュニティ ストリングが無効であるため、SNMP ホストからの SNMP 要求が失敗した場合に、トラップを送信します。
IPsec Traps	個々の IPsec 関連のトラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [クリプトマップ（Cryptomap）]：デバイスのクリプトマップセットに対してクリプトマップエントリが追加または削除されるときに、トラップを送信します。さらに、クリプト マップ セットがアクティブ インターフェイスに対して適用または適用解除されたときに、トラップを送信します。 • [Too Many SAs]：デバイス上のメモリが不足しているときに Security Association（SA; セキュリティ アソシエーション）の作成が試行された場合に、トラップを送信します。 • [Tunnel]：IPsec フェーズ 2 トンネルがアクティブまたは非アクティブになったときに、トラップを送信します。 詳細については、サイト間 VPN の IPsec プロポーザルについて （1500 ページ）を参照してください。
[ISAKMPトラップ（ISAKMP Traps）]	個々の Internet Security Association and Key Exchange Protocol（ISAKMP）トラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [ポリシー（Policy）]：ISAKMP ポリシーが作成または削除されたときにトラップを送信します。 • [Tunnel]：フェーズ 1 IKE トンネルがアクティブまたは非アクティブになったときに、トラップを送信します。 詳細については、IKE について （1482 ページ）を参照してください。

要素	説明
Other Traps	その他の SNMP トラップをイネーブルまたはディセーブルにします。次のオプションがあります。 • [Syslog]：syslog メッセージを SNMP ホストに送信します。 • [TTY]：伝送制御プロトコル（TCP）接続が閉じたときに、シスコ固有の通知を送信します。 • [BGP]：ボーダー ゲートウェイ プロトコル（BGP）の状態変化が発生したときに、通知を送信します。 Cisco IOS ルータにおける BGP ルーティング （3331 ページ）を参照してください。 • [IP Multicast]：（マルチキャスト ルータにのみ適用可能）ルータが、定義された期間中に定義された数のハートビート パケットをハートビート ソースから受け取ることができなかった場合に、トラップを送信します。 [IPマルチキャスト（IP Multicast）] を選択した場合は、デバイスで **ip multicast heartbeat** コマンドを手動で設定して、マルチキャストアドレスとハートビート制限も設定する必要があります。FlexConfig を使用してこれを行います。 • [CPU]：CPU 使用率が上昇して上限しきい値を超えたままになるか、低下して下限しきい値を下回ったままになった場合にトラップを送信します。 CPU を選択した場合は、デバイスで **process cpu threshold type** コマンドを手動で設定して、しきい値を設定する必要もあります。FlexConfig を使用してこれを行います。 • [HSRP]：Hot Standby Routing Protocol（HSRP）通知を送信します。
[Select All] ボタン	ダイアログボックスに表示されるすべての SNMP トラップを有効にします。
[Deselect All] ボタン	ダイアログボックスに表示されるすべての SNMP トラップを無効にします。

Cisco IOS ルータにおける DNS

ドメイン ネーム システム（DNS）は、DNS サーバから DNS プロトコルを使用してホスト名を IP アドレスにマッピングできる分散データベースです。一意の各 IP アドレスにホスト名を関連付けることができます。DNS を使用すると、ホストの 32 ビットの IP アドレスがわからない場合でも、そのホストに接続できます。DNS サーバーは、指定されたホスト名を取得して、適切な IP アドレスに変換します。

リモート DNS サーバによって変換が行われる以外に、ホストから IP アドレスへのスタティック マッピングを含むローカル ホスト テーブルを Cisco IOS ルータに設定できます。connect、telnet、ping などのコマンドを使用すると、ルータはこのホスト テーブルを確認してから DNS サーバに問い合わせます。これにより、変換プロセスが速くなります。

デフォルトでは、DNS 機能はすべての Cisco IOS ルータで有効になっています。

関連項目

- DNS ポリシーの定義　（3209 ページ）

DNS ポリシーの定義

Security Manager で DNS ポリシーを定義すると、ルータによってホスト名とアドレス間の変換に使用されるリモート DNS サーバを指定できます。さらに、このデバイスによって排他的に使用されるローカル変換を含む静的ホストテーブルを定義できます。このタイプのキャッシュでアドレスを選択すると、DNS サーバーにクエリを実行する必要がなくなるため、変換プロセスを高速化できます。

関連項目

- Cisco IOS ルータにおける DNS　（3208 ページ）

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [DNS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [DNS]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[DNS] ページが表示されます。このページのフィールドの説明については、表 885 : [DNS] ページ　（3211 ページ）を参照してください。

ステップ 2　[サーバー（Servers）] フィールドに、ルータのホスト名からアドレスへの変換を実行できる DNS サーバー（最大 6）のアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、[選択（Select）] をクリックしてセレクタを表示できます。詳細については、 ポリシー定義中の IP アドレスの指定　（401 ページ）を参照してください。

ヒント　必要なネットワークがセレクタに表示されていない場合は、セレクタで [作成（Create）] ボタンまたは [編集（Edit）] ボタンをクリックして、 [Add Network/Host]/[Edit Network/Host] ダイアログ ボックス　（395 ページ）を表示します。ここから、ポリシーで使用するネットワーク/ホスト オブジェクトを作成できます。

ステップ 3　（任意）[ホスト（Hosts）] フィールドに、ルータのホストテーブルに定義する静的ホストマッピングを入力します。

a) [追加（Add）] をクリックして、 [IP Host] ダイアログボックス （3211 ページ）を表示します。
b) 変換するホスト名を入力します。
c) アドレスまたはネットワーク/ホストオブジェクトを最大 3 つまで入力し、[選択（Select）] をクリックしてセレクタを表示します。これらはホスト名の変換先のアドレスです。
d) [OK] をクリックマッピングが [DNS] ページの [Hosts] フィールドに表示されます。
e) 3.a （3210 ページ）から 3.d （3210 ページ） を繰り返すと、さらに多くのホストをホストテーブルに追加できます。

（注） ホストマッピングを編集するには、[ホスト（Hosts）] フィールドから定義を選択し、[編集（Edit）] をクリックします。ホストマッピングを削除するには、そのマッピングを選択し、[削除（Delete）] をクリックします。

ステップ 4 （任意）[ドメインルックアップ（Domain Lookup）] チェックボックスをオフにして、ルータの DNS 機能を無効にします。

[DNS] ポリシー ページ

[DNS] ポリシー ページでは、ルータがホスト名を IP アドレスに変換するために使用するローカル IP ホスト テーブルとドメイン ネーム システム（DNS）サーバを定義します。DNS 機能をディセーブルにして、ルータが DNS ルックアップを実行できないようにすることもできます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [DNS]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [DNS]** を選択します。[DNS] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおける DNS （3208 ページ）

フィールド リファレンス

表 *885 : [DNS]* ページ

要素	説明
サーバー	DNS ルックアップを実行するためにルータによって使用される DNS サーバーです。1 つ以上のアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。最大 6 個の DNS サーバーを定義することができます。
ホスト（Hosts）	ルータに設定するローカル ホスト テーブル。ユーザがホスト名を入力すると、ルータはまずこのテーブルを確認してから [Servers] フィールドに定義されている DNS サーバに問い合わせます。 [追加（Add）] をクリックして、[IP Host] ダイアログボックス （3211 ページ）を表示します。ここから、ホスト名とそのホスト名に関連付ける IP アドレスを定義できます。 （注） ホストテーブルのエントリを編集するには、エントリを選択して [編集（Edit）] をクリックします。エントリを削除するには、そのエントリを選択し、[削除（Delete）] をクリックします。
ドメイン検索（Domain Lookup）	選択すると、ルータは定義済みの DNS サーバ上で検索を実行します。これがデフォルトです。 選択を解除すると、リモート DNS サーバ上での検索はディセーブルになります。

[IP Host] ダイアログボックス

[IP ホスト（IP Host）] ダイアログボックスを使用して、ルータのホストテーブルを設定します。これは、ルータがホスト名を IP アドレスに変換するために使用するスタティックなローカルマッピングのテーブルです。ルータは、ホストテーブルで必要なエントリを見つけられない場合、[DNS] ページで定義されている DNS サーバーにクエリを実行します。

ナビゲーション パス

[DNS] ポリシー ページ （3210 ページ）に移動し、[ホスト（Hosts）] の下にある [追加（Add）] をクリックします。

関連項目

- Cisco IOS ルータにおける DNS （3208 ページ）

フィールド リファレンス

表 *886 : [IP Host]* ダイアログボックス

要素	説明
ホスト名	ルータのローカルホストテーブルに含めるホスト名。
アドレス	ホスト名に関連付けるアドレス。1つ以上のアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。ホスト名ごとに最大 3 つのアドレスを定義できます。

Cisco IOS ルータにおけるホスト名とドメイン名

ホスト名ポリシーでは、選択したルータのホスト名とドメイン名を設定します。このポリシーを展開すると、ホスト名とドメイン名に対する変更が [Device Properties] ページに反映されます（デバイス プロパティの表示または変更 （136 ページ）を参照）。

関連項目

- ホスト名ポリシーの定義 （3212 ページ）

ホスト名ポリシーの定義

ホスト名ポリシーを定義すると、Security Manager は展開後に [Device Properties] ダイアログボックスのホスト名とドメイン名のフィールドを更新します。デバイス プロパティの表示または変更 （136 ページ） を参照してください。

関連項目

- Cisco IOS ルータにおけるホスト名とドメイン名 （3212 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [ホスト名（Hostname）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Hostname] ページが表示されます。このページのフィールドの説明については、表 887 : [Hostname] ページ（3213 ページ）を参照してください。

ステップ 2 ルータのホスト名を入力します。名前は文字で始まり、文字または数字で終了し、文字、数字、およびハイフンだけから構成される必要があります。最大で 63 文字です。

ステップ 3 ルータのドメイン名を入力します。ルータは、RSA キーを生成するときにこのドメイン名を使用します。また、完全修飾ドメイン名を入力しなかった場合に、ポリシーでこのドメイン名を使用します。

[Hostname] ポリシー ページ

[Hostname] ページでは、ルータに割り当てるホスト名とドメイン名を定義します。詳細については、ホスト名ポリシーの定義 （3212 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）] > [ホスト名（Hostname）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）]>[デバイス管理（Device Admin）]>[ホスト名（Hostname）]** を選択します。[ホスト名（Hostname）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるホスト名とドメイン名 （3212 ページ）

フィールド リファレンス

表 *887 : [Hostname]* ページ

要素	説明
ホスト名	ルータのホスト名。 名前は文字で始まり、文字または数字で終了し、文字、数字、およびハイフンだけから構成される必要があります。最大で 63 文字です。
ドメイン名	ルータのデフォルトのドメイン名。最大で 63 文字です。 ルータは、RSA キーを生成するときにこのドメイン名を使用します。また、Fully-Qualified Domain Name（FQDN; 完全修飾ドメイン名）を入力しなかった場合に、ポリシーでこのドメイン名を使用します。

Cisco IOS ルータにおけるメモリ設定

メモリ ポリシーでは、ルータのメモリに関する設定を定義します。このポリシーは、使用可能なメモリが定義済みのしきい値を下回った場合に通知メッセージを生成する機能など、メモリ使用量をモニタするための手段を提供します。

（注） メモリ ポリシーは、Cisco IOS ソフトウェア Release 12.3(14)T 以降を実行しているルータでサポートされます。

関連項目

- ルータのメモリ設定の定義 （3214 ページ）

ルータのメモリ設定の定義

Security Manager を使用して、次のデフォルトのメモリ設定を変更できます。

- ルータがメモリ使用量のログを保持する時間数
- Memory Allocation Lite 機能をイネーブルにするかどうか
- 重要なシステム ログ メッセージ用に予約するメモリ容量

さらに、次の項目を定義できます。

- プロセッサおよび I/O メモリの下限しきい値。使用可能なメモリがこれらのしきい値を下回ると、ログ メッセージが送信されます。
- 実行する健全性チェックのタイプ。

関連項目

- Cisco IOS ルータにおけるメモリ設定 （3214 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [メモリ（Memory）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）]>[メモリ（Memory）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Memory] ページが表示されます。

ステップ 2 （任意）必要に応じて、ルータのメモリ設定を定義します。使用可能なフィールドの説明については、表 888 : [Memory] ページ （3216 ページ）を参照してください。

[Memory] ポリシー ページ

[Memory] ページでは、ルータのメモリに関する次の設定を定義します。

- メモリ ログを保持する時間
- 使用可能なプロセッサおよび I/O メモリのしきい値
- 重要なログ メッセージ用に予約するメモリ容量
- バッファおよびキューで健全性チェックを実行するかどうか
- 「memory-allocation lite」機能をイネーブルにするかどうか

詳細については、 ルータのメモリ設定の定義 （3214 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [メモリ（Memory）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [メモリ（Memory）]** を選択します。[メモリ（Memory）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるメモリ設定 （3214 ページ）
- [CPU] ポリシー ページ （3146 ページ）
- Syslog ロギングの設定ポリシーのページ （3278 ページ）
- Syslog サーバ ポリシーのページ （3282 ページ）

フィールド リファレンス

表 *888 : [Memory]* ページ

要素	説明
Maintain Memory Log	ルータがデバイス上のメモリ使用量の履歴が格納されたログを保持する時間数。有効値の範囲は 12 ～ 72 時間です。デフォルトは 24（1 日）です。 （注） メモリ ログはデフォルトでイネーブルになっており、ディセーブルにすることはできません。
Processor Threshold	プロセッサのメモリしきい値（KB 単位）。使用可能なプロセッサ メモリがこのしきい値を下回った場合は、通知メッセージがトリガーされます。有効値の範囲は 1 ～ 4294967295 KB（4096 GB）です。 （注） 使用可能な空きメモリがしきい値を 5% 上回ると、別の通知メッセージが生成されます。
I/O Threshold	I/O メモリのしきい値（KB 単位）。使用可能なプロセッサ メモリがこのしきい値を下回った場合は、通知メッセージがトリガーされます。有効値の範囲は 1 ～ 4294967295 KB（4096 GB）です。 （注） 使用可能な空きメモリがしきい値を 5% 上回ると、別の通知メッセージが生成されます。
Memory Allocation Lite	選択すると、ルータ上の「memory-allocation lite」（malloc_lite）機能がイネーブルになります。この機能により、128 バイト以上のメモリが必要ではない状況で、過剰なメモリ割り当てによるオーバーヘッドを防ぐことができます。これがデフォルトです。 選択を解除すると、「memory-allocation lite」機能がディセーブルになります。 （注） この機能は、プロセッサ メモリ プールだけでサポートされます。
Memory Region For Critical Notifications	重要なシステムログメッセージ用に予約するメモリ容量（キロバイト）有効値の範囲は 1 ～ 4294967295 KB（4096 GB）ですが、メモリ合計の 25% を超える値を指定することはできません。 このオプションは、システムリソースが過負荷になっている場合でも、ルータが重要なシステムログメッセージを発行できるように、ルータにメモリ領域を予約します。

要素	説明
Perform Sanity Checks	実行する健全性チェックのタイプ： • [Buffer]：すべてのバッファに対して健全性チェックを実行します。健全性チェックは、パケットバッファが割り当てられるとき、およびパケットバッファがバッファ プールに戻されるときに実行されます。 • [Queue]：すべてのキューに対して健全性チェックを実行します。 • [All]：すべてのバッファとキューに対して健全性チェックを実行します。 （注） これらのオプションのいずれかをイネーブルにすると、ルータパフォーマンスが多少低下する可能性があります。

Cisco IOS ルータにおけるセキュア デバイス プロビジョニング

Secure Device Provisioning（SDP; セキュア デバイス プロビジョニング）は、VPN およびネットワーク セキュリティの展開を効率化するための統合ソリューションを提供します。SDP（以前の Easy Secure Device Deployment（EzSDD））を使用すると、リモートサイト ユーザは使いやすい Web インターフェイスで VPN デバイスを安全にブートストラップできます。これにより、展開の負担やコストが軽減され、ネットワーク開発サイクルが短縮されます。たとえば、在宅勤務者や小規模のブランチ オフィス ユーザは、新しいデバイスを出荷パッケージから取り出して接続し、簡単な Web 管理インターフェイスを開いて VPN 接続を確立できます。これらのすべての作業をほんの数分間で行うことができます。

SDP の詳細については、Cisco IOS セキュリティ コンフィギュレーション ガイド、リリース 12.4T [英語] の「Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI」を参照してください。

（注） SDP を使用するには、Cisco IOS ソフトウェア Release 12.3(8)T 以降が必要です。これよりも前のバージョンが実行されているルータにこのポリシーを展開しようとすると、展開が失敗する可能性があります。また、NO-VPN ルータ モデル（3845 NOVPN など、VPN 設定ができないモデル）ではポリシーを設定できません。

Trusted Transitive Introduction（TTI）は、SDP を実装するための主なメカニズムとして機能するプロトコルです。図 51 : Secure Device Provisioning（Secure Device Provisioning） （3218 ページ）に示すように、TTI は次の 3 つのエンティティで構成されています。

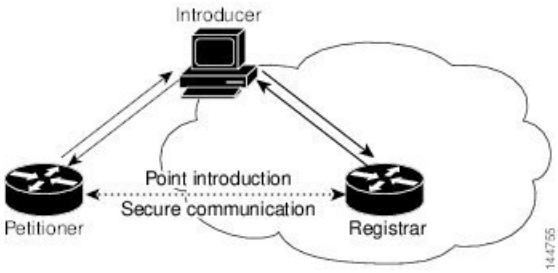
- イントロデューサ：ペティショナをレジストラに紹介する、相互に信頼できるデバイス。イントロデューサは、SDP を使用して自分に関連付けられた VPN デバイスを PKI ネットワークに配置するエンド ユーザ、または SDP を使用して多くの VPN デバイスを PKI ネッ

トワークに配置する管理者/管理システムのいずれかです。後者のイントロデューサは、管理イントロデューサと呼ばれます。詳細については、管理イントロデューサの AAA サーバ グループの設定 （3221 ページ）を参照してください。

- ペティショナ：セキュア ドメインに参加しているリモートサイト デバイス。ペティショナは、イントロデューサに Web ページを提供し、イントロデューサの Web ブラウザからブートストラップ設定を受信します。ペティショナコンポーネントは、すべての Cisco IOS デバイスでデフォルトで有効になっています。
- レジストラ：認証、許可、アカウンティング（AAA）サーバと直接通信してユーザ クレデンシャルの確認、登録の許可または拒否、およびユーザ固有の設定情報の取得を行うことによって、ペティショナを認可するサーバ。

ルータをレジストラとして設定するには、Security Manager で SDP ポリシーを使用します。

図 *51 : Secure Device Provisioning*（*Secure Device Provisioning*）



Secure Device Provisioning の詳細については、次を参照してください。

- ブートストラップ設定の内容 （3218 ページ）
- セキュア デバイス プロビジョニングのワークフロー （3219 ページ）
- セキュア デバイス プロビジョニング ポリシーの定義 （3219 ページ）

ブートストラップ設定の内容

SDP によって提供されるブートストラップ設定では、一般に次のことを行います。

- ペティショナのホスト名の設定
- ペティショナのシステムクロックとレジストラとの同期
- ペティショナのトラストポイントの設定
- ペティショナの認証および許可メカニズムの設定
- CA 証明書のプッシュ
- PKI サーバへのペティショナの登録
- 管理トンネルの確立に必要な設定など、他の VPN 設定の定義

- Cisco Networking Services（CNS）の設定
- ペティショナの DHCP プールの設定

関連項目

- セキュア デバイス プロビジョニングのワークフロー （3219 ページ）
- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）

セキュア デバイス プロビジョニングのワークフロー

ここでは、SDP を使用してリモートサイト デバイスをセキュア ネットワークに登録するために必要な手順を示します。

1. ルータを開梱し、電源、LAN、および WAN ケーブルを接続します。
2. ルータ上の DHCP サーバから IP アドレスが割り当てられているコンピュータ（イントロデューサ）に電源を投入し、Web ブラウザを開いてルータ上のペティショナの URL（http://device/ezsdd/welcome）に移動します。ルータから登録ページ（ローカル ログイン ダイアログボックスとも呼ばれる）が返されます。
3. ユーザー名とパスワードを入力し、[OK] をクリックします。初期ページでレジストラの URL を入力します。次が実行されます。
   1. ブラウザは、中央サイトのレジストラとのセッションを開きます。このセッションは HTTPS で保護されます。レジストラは、AAA サーバを使用してユーザ名を検証し、適切なブートストラップ設定をブラウザに返します。
   2. ブラウザは、ブートストラップ設定をリモートサイトのルータに提供し、PKI トラストポイントの登録と IPsec VPN 接続の設定およびシステム属性やその他の情報のプロビジョニングを行います。
   3. ブートストラップ設定の完了が通知されます。

関連項目

- ブートストラップ設定の内容 （3218 ページ）
- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）

セキュア デバイス プロビジョニング ポリシーの定義

ペティショナ コンポーネントは、すべての Cisco IOS ルータで自動的にイネーブルになります。Security Manager の SDP ポリシーにより、レジストラが有効になります。SDP ポリシーを定義するには、以下を定義する必要があります。

- レジストラがイントロデューサの認証と認可に使用する AAA サーバが含まれている AAA サーバ グループ

- ブートストラップ プロセス中にペティショナの登録先となる CA サーバ
- 認可の実行後に表示される初期ページの場所
- ペティショナに提供されるブートストラップ設定の場所

関連項目

- セキュア デバイス プロビジョニングのワークフロー （3219 ページ）
- 管理イントロデューサの AAA サーバ グループの設定 （3221 ページ）
- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [セキュアデバイスプロビジョニング（Secure Device Provisioning）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [セキュアデバイスプロビジョニング（Secure Device Provisioning）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[セキュアデバイスプロビジョニング（Secure Device Provisioning）] ページが表示されます。このページのフィールドの説明については、表 889 : [Secure Device Provisioning] ページ （3223 ページ）を参照してください。

ステップ 2 [Introducer Authentication] で、関連する AAA サーバーが含まれている AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

選択した AAA サーバによって、イントロデューサが指定したユーザ名とパスワードが認可されたユーザを表すかどうかが判断されます。AAA サーバは TACACS+ や RADIUS を使用するか、またはローカルである必要があります。

（注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。管理イントロデューサの認証と認可に別の AAA サーバ グループを設定する場合は、 管理イントロデューサの AAA サーバ グループの設定 （3221 ページ）を参照してください。

ステップ 3 [Petitioner Authentication] で、次のいずれかの手順を実行して、ペティショナの ID を認証する CA サーバを定義します。

- [ローカルCAサーバー（Local CA Server）] を選択し、表示されるフィールドにローカル CA の名前を入力します。レジストラ上で CA サーバをすでにローカルに設定している場合は、トラストポイントが自動的に生成されます。

（注） ルータを CA サーバーとして設定していない場合は、CLI または FlexConfig を使用してコマンド **Crypto pki server [name]** を入力します。このコマンドは、ローカル CA サーバで設定された SDP ポリシーを展開する場合は必須です。

- [リモートCAサーバー（Remote CA Server）] を選択し、PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。

PKI 登録オブジェクトでは、SDP ポリシーで使用される外部 CA サーバを定義します。

ステップ 4 レジストラへのログイン後に表示される初期ページの場所を選択します。初期ページには、認可が正常に完了したかどうかが表示され、ブートストラップ設定の取得プロセスを完了するためのボタンが表示されます。

デフォルトの初期ページを選択しない場合は、他の場所に準備した別の初期ページにアクセスするために必要な URL を入力する必要があります。

ステップ 5 ペティショナに提供するブートストラップ設定の場所を選択して、その最初の設定を実装します。

- ブートストラップ設定の場所が Security Manager 以外の URL である場合は、その URL を入力します。必要に応じて、その URL にアクセスするためのユーザ名とパスワードも入力します。
- 設定ファイルの場所が Security Manager の URL である場合：
  - FlexConfig の名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。FlexConfig には、適切なブートストラップ設定の取得に必要なデバイス コマンドが含まれています。詳細については、[Add FlexConfig]/[Edit FlexConfig] ダイアログボックス （467 ページ）を参照してください。
  - FlexConfig が、イントロデューサによって送信されたユーザ名に基づいて、ペティショナのデバイス名を設定するために必要なデバイス名の式を入力します（通常、2 つの名前の関連付けは変更されません）。デフォルトの式は$nで、イントロデューサ名を使用してデバイス名を決定します。

デバイス名によって、ペティショナが受信するブートストラップ設定が決まります。生成される URL には、選択した FlexConfig の名前および定義したパラメータと式が含まれます。

- FlexConfig が含まれている Security Manager サーバにアクセスするためのユーザ名とパスワードを入力します。パスワードには、英数字を使用できますが、単一の数字だけでは構成できません。

管理イントロデューサの AAA サーバ グループの設定

管理イントロデューサは、多くのデバイスを PKI ネットワークに導入する管理者または管理システムです。次の FlexConfig をルータの設定に追加することによって、管理イントロデューサを認証および認可するための AAA サーバ グループを設定できます。

```
aaa new-model
radius-server host 1.2.3.4 auth-port 1645 acct-port 1646 key key
aaa group server radius default-radius-group2
server 1.2.3.4 auth-port 1645 acct-port 1646
exit
aaa authentication login CSM_SDP2 group default-radius-group2
crypto provisioning registrar
```

```
administrator authentication list CSM_SDP2
administrator authorization list CSM_SDP2
exit
```

この FlexConfig は、2 つの機能を提供します。使用する AAA サーバ グループを設定し、このサーバ グループを SDP 暗号に関連付けます。

管理イントロデューサの詳細については、次の URL にある Cisco.com の『Administrative Secure Device Provisioning Introducer』を参照してください。
http://www.cisco.com/en/US/docs/ios/12_3t/12_3t14/feature/guide/gtadintr.html

関連項目

- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）
- セキュア デバイス プロビジョニング ポリシーの定義 （3219 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）

[Secure Device Provisioning] ポリシー ページ

Secure Device Provisioning（SDP）のポリシー（以前の Easy Secure Device Deployment（EzSDD））を使用すると、Cisco IOS ルータをレジストラとして設定できます。これは、ペティショナのブートストラップ設定を取得する SDP コンポーネントです。ペティショナは、ネットワークセキュリティインフラストラクチャに登録されるリモートサイトデバイスです。これらのデバイスは、初回の設定のためにブートストラップ設定を使用します。レジストラは、ペティショナをレジストラに紹介するユーザであるイントロデューサの ID の検証も行います。

詳細については、セキュア デバイス プロビジョニング ポリシーの定義 （3219ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[セキュアデバイスプロビジョニング（Secure Device Provisioning）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]>[デバイス管理（Device Admin）]>[セキュアデバイスプロビジョニング（Secure Device Provisioning）]** を選択します。新しいポリシーを作成するか、または既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるセキュア デバイス プロビジョニング （3217 ページ）
- セキュア デバイス プロビジョニングのワークフロー （3219 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）

フィールド リファレンス

表 *889 : [Secure Device Provisioning]* ページ

要素	説明
Introducer Authentication (AAA)	イントロデューサによって指定されたユーザ名とパスワードを認証する AAA サーバ グループ。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 （注） 管理イントロデューサの認証に別の AAA サーバ グループを設定する場合は、管理イントロデューサの AAA サーバ グループの設定 （3221 ページ）を参照してください。
Petitioner Authentication	ペティショナの ID を認証する CA サーバ。 • ローカル CA サーバー：ルータ自体が CA サーバーとして機能するようにすでに設定されている場合は、このオプションを選択します。表示されるフィールドにローカル CA の名前を入力します。 （注） ルータを CA サーバーとして設定していない場合は、CLI または FlexConfig を使用してコマンド **Crypto pki server [name]** を入力します。このコマンドは、ローカル CA サーバで設定された SDP ポリシーを展開する場合は必須です。 • [Remote CA Server]：外部 CA サーバを使用する場合は、このオプションを選択します。PKI 登録オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。PKI 登録オブジェクトの詳細については、[PKI Enrollment] ダイアログボックス （1554 ページ）を参照してください。
Introduction Page	認可の実行後にイントロデューサに表示する初期ページの場所： • [デフォルトの初期ページを使用（Use default introduction page）]：Security Manager で提供されるデフォルトのページを使用します。 • [Specify introduction page URL]：[URL] フィールドに指定された初期ページを使用します。サポートされるプロトコルには、FTP、HTTP、HTTPS、null、NVRAM、RCP、SCP、system、TFTP、Webflash、および XMODEM があります。

要素	説明
Bootstrap Configuration	初回の設定用にペティショナに提供するブートストラップ設定の場所 • [Non-Security Manager URL]：ブートストラップ設定が Security Manager の外部にある場合に使用します。その場所を [URL] フィールドに入力します。 必要に応じて、ブートストラップ設定を含むサーバにアクセスするためのユーザ名とパスワードを入力します。 • [Security Manager URL]：Security Manager によってブートストラップ設定が提供される場合に使用します。次のフィールドに情報を入力します。 • [FlexConfig]：ブートストラップ設定の作成に必要な基本 CLI 構造が含まれている FlexConfig。FlexConfig オブジェクトの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。 FlexConfig の選択後、FlexConfig が格納されている Security Manager サーバにアクセスするためのユーザ名とパスワードを入力する必要があります。 • [Device name formula]：Security Manager が、イントロデューサが指定したユーザ名に基づいて、ペティショナのデバイス名を決定するために必要な式。 通常、ユーザ名とデバイス名の間には一定の関係があるため、このような式を設定できます。デフォルトの式は $n で、イントロデューサ名を使用してデバイス名を決定します。ペティショナが受信する設定ファイルを特定するには、デバイス名が必要です。 必要に応じて、ブートストラップ設定を含むサーバにアクセスするためのユーザ名とパスワードを入力します。パスワードには、英数字を使用できますが、単一の数字だけでは構成できません。

Cisco IOS ルータにおける DHCP

Security Manager では、Easy VPN や 802.1x などの特定のセキュリティ機能を使用するときに、Dynamic Host Configuration Protocol（DHCP）のクライアント/サーバ設定が必要となります。DHCP は、中央のサーバーからホスト IP アドレスを動的に割り当てるために LAN 環境で広く使用されており、それによって IP アドレス管理のオーバーヘッドが大幅に軽減されます。

DHCP サーバは、ルータ内の指定したアドレス プールから DHCP クライアントに IP アドレスを割り当てて管理します。DHCP サーバーが自身のデータベースで DHCP 要求を実行できない場合、この要求をネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバーに転送できます。

Security Manager を使用すると、デバイスの内部インターフェイスに接続されているクライアント（ホスト）の DHCP サーバーとして Cisco IOS デバイスを設定できます。DHCP サーバを

設定する場合は、IP プール（DHCP サーバ用に予約された IP アドレスの範囲）を使用します。選択した IP プールによって、サーバが使用できる IP アドレスの範囲が決まります。これらのアドレスは、リースと呼ばれる定義済みの期間、クライアントデバイスに提供されます。このリースの期限が切れると、アドレスがアドレスプールに返され、DHCP サーバはそのアドレスを別のデバイスに割り当てることができるようになります。

DHCP の詳細については、次を参照してください。

- DHCP データベース エージェントについて （3225 ページ）
- DHCP リレーエージェントについて （3226 ページ）
- DHCP Option 82 について （3226 ページ）
- Secured ARP について （3227 ページ）

DHCP ポリシーの設定については、次を参照してください。

- DHCP ポリシーの定義 （3228 ページ）
- DHCP アドレス プールの定義 （3229 ページ）

DHCP データベース エージェントについて

DHCP データベース エージェントは、DHCP バインディング データベースが格納されている外部ホスト（FTP、TFTP、RCP サーバなど）です。各 DHCP ポリシーに 1 つ以上の DHCP データベースエージェントを含めたり、エージェントのデータベース更新の間隔を設定したりできます。

（注） 外部 DHCP データベース エージェントを設定する場合、IP アドレス プールの定義は必須ではありませんが、必要に応じて定義することもできます。IP アドレス プールの詳細については、 DHCP アドレス プールの定義 （3229 ページ）を参照してください。

関連項目

- DHCP リレーエージェントについて （3226 ページ）
- DHCP Option 82 について （3226 ページ）
- Secured ARP について （3227 ページ）
- DHCP ポリシーの定義 （3228 ページ）
- Cisco IOS ルータにおける DHCP （3224 ページ）

DHCP リレーエージェントについて

DHCP リレーエージェントは、クライアントとサーバが同じ物理サブネット上に存在しない場合に、それらのクライアントとサーバの間で DHCP パケットを転送するホストです。リレーエージェントは DHCP メッセージを受信し、別のインターフェイス上で送信する新しい DHCP メッセージを生成します。転送メッセージにすでにリレー情報が含まれている場合の DHCP リレーエージェントによる処理方法を決定する、情報再転送ポリシーを設定できます。

Security Manager には次の DHCP リレー オプションがあります。

- [Drop]：Option 82 情報も存在する場合、リレーエージェントは、既存のリレー情報を含むメッセージを廃棄します。
- [Keep]：リレー エージェントは、既存のリレー情報を保持します。
- [Replace]：リレー エージェントは、既存の情報を独自のリレー情報で上書きします。

たとえば、転送されたメッセージを DHCP リレー エージェントで新しいリレー メッセージに置き換えることができます。さらに、転送された BOOTREPLY メッセージ内に含まれているリレー情報の有効性をリレー エージェントで確認するかどうかを選択できます。

関連項目

- DHCP データベース エージェントについて （3225 ページ）
- DHCP Option 82 について （3226 ページ）
- Secured ARP について （3227 ページ）
- DHCP ポリシーの定義 （3228 ページ）
- Cisco IOS ルータにおける DHCP （3224 ページ）

DHCP Option 82 について

DHCP Option 82 を使用すると、DHCP リレー エージェントは、DHCP クライアントからの要求を DHCP サーバに転送するときに、エージェント自体に関する情報と、接続されているクライアントに関する情報を含めることができます。DHCP サーバは、この情報を使用して IP アドレスを割り当てたり、アクセス コントロールを実行したり、各サブスクライバの Quality of Service（QoS）やセキュリティ ポリシーを設定したりできます。DHCP Option 82 機能がイネーブルになっている場合、サブスクライバは、MAC アドレスではなく、ネットワークへの接続に使用しているスイッチ ポートによって識別されます。サブスクライバ LAN 上の複数のホストをアクセス スイッチの同じポートに接続できます。これらのホストは一意に識別されます。また、Option 82 を使用すると、ユーザの IP アドレスを使用してユーザが接続されているポートを特定できるため、アクセススイッチ上のセキュリティを強化できます。

関連項目

- DHCP データベース エージェントについて （3225 ページ）

• DHCP リレーエージェントについて （3226 ページ）
• Secured ARP について （3227 ページ）
• DHCP ポリシーの定義 （3228 ページ）
• Cisco IOS ルータにおける DHCP （3224 ページ）

Secured ARP について

DHCP セキュア IP アドレス割り当て機能（DHCP 認可 ARP とも呼ばれる）を使用すると、DHCP データベース内の DHCP リースに対するアドレス解決プロトコル（ARP）テーブルのエントリを保護できます。この機能では、クライアントの MAC アドレスを DHCP バインディングに保護して同期させることで、無許可のクライアントまたはハッカーが DHCP サーバーをスプーフィングして、許可されたクライアントの DHCP リースを横取りすることを防ぎます。

この機能をイネーブルにすると、DHCP サーバは IP アドレスを DHCP クライアントに割り当ててから、クライアントの割り当て済み IP アドレスと MAC アドレスを持つ ARP テーブルに、セキュアな ARP エントリを追加します。これらの ARP エントリは、他の動的な ARP パケットによって更新することはできず、リースがアクティブであるかぎり ARP テーブルに存在します。

セキュアな ARP エントリは、DHCP クライアントからの明示的な終了メッセージによって削除されるか、またはバインディングの期限が切れたときに DHCP サーバによって削除されます。クライアントのログアウトを検出するために、Secured ARP は、認可ユーザだけが応答できる ARP メッセージを定期的に送信します。未認可応答は DHCP サーバでブロックされるため、セキュリティが強化されます。

（注） Secured ARP により、インターフェイスにおける動的な ARP 学習がディセーブルになります。

関連項目

• DHCP データベース エージェントについて （3225 ページ）
• DHCP リレーエージェントについて （3226 ページ）
• DHCP Option 82 について （3226 ページ）
• DHCP ポリシーの定義 （3228 ページ）
• Cisco IOS ルータにおける DHCP （3224 ページ）

DHCP ポリシーの定義

DHCP ポリシーを設定する場合、サーバが DHCP クライアントにアドレスを提供するために使用する IP アドレス プールを定義する必要があります。さらに、任意で次を定義できます。

- 外部の DHCP データベース エージェント
- DHCP から除外する IP 範囲
- DHCP リレーパラメータ

（注） Cisco IOS ルータで DHCP を設定する場合は、ルータに Bootstrap Protocol（BootP; ブートストラップ プロトコル）トラフィックを拒否するアクセス ルールが含まれていないことを確認してください。このようなルールが設定されていると、DHCP トラフィックはブロックされます。

関連項目

- Cisco IOS ルータにおける DHCP （3224 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[DHCP] ポリシー ページが表示されます。このページのフィールドの説明については、表 890 : [DHCP] ポリシー ページ （3231 ページ）を参照してください。

ステップ 2 （任意）[データベース（Databases）] で、[追加（Add）] ボタンをクリックして [DHCP Database] ダイアログボックス （3233 ページ）を表示します。ここから、外部の DHCP データベース エージェントを定義できます。詳細については、DHCP データベース エージェントについて （3225 ページ）を参照してください。

ステップ 3 （任意）[Excluded IPs] で、DHCP クライアントで使用できないようにする DHCP アドレス プール内の IP アドレスまたはアドレス範囲を入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、[選択（Select）] をクリックしてセレクタを表示できます。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ヒント 必要なネットワークがセレクタに表示されていない場合は、[作成（Create）] ボタンをクリックして、[Add Network/Host]/[Edit Network/Host] ダイアログボックス （395 ページ）を表示します。ここから、ネットワーク/ホスト オブジェクトを作成できます。

ステップ 4 [IP プール（IP Pools）] で、[追加（Add）] ボタンをクリックして [IP Pool] ダイアログボックス （3234 ページ）を表示します。ここから、DHCP サーバによって使用されるアドレス プールを定義できます。詳細については、 DHCP アドレス プールの定義 （3229 ページ）を参照してください。

ステップ 5 （任意）リレーエージェントを使用して、DHCP サーバーとは異なるサブネットにある DHCP クライアントからの要求を管理する場合は、次の DHCP リレーオプションを定義します。

a) リレーエージェント情報再転送ポリシー（[Drop]、[Keep]、または [Replace]）を選択します。DHCP リレー エージェントは、すでにリレー情報が含まれているメッセージを受信すると、このポリシーを実装します。

b) リレーエージェントが DHCP サーバーに転送する要求に Option 82 データを挿入できるようにするには、[オプション（Option）] チェックボックスをオンにします。

c) [チェック（Check）] チェックボックスをオンにして、DHCP サーバーによって送信された DHCP Option 82 リレーパケットを検証します。

このオプションをイネーブルにすると、無効なメッセージはドロップされます。有効なメッセージは、DHCP クライアントに転送される前に option-82 フィールドが削除されます。このオプションをディセーブルにすると、先に有効性が確認されることなく option-82 フィールドはパケットから削除されます。

詳細については、 DHCP リレーエージェントについて （3226 ページ）を参照してください。

DHCP アドレス プールの定義

外部データベース エージェントを含まない DHCP ポリシーを設定する場合は、少なくとも 1 つの IP アドレス プールを定義する必要があります。DHCP サーバは、このプールに含まれているアドレスを DHCP クライアントに動的に割り当てることができます。さらに、次の IP プール固有のオプションを定義できます。

- DHCP クライアントで使用するデフォルト ルータ、DNS サーバ、WINS サーバ、およびドメイン
- Secured ARP 機能を使用するかどうか
- IP プール オプションに関する情報を中央の DHCP サーバからインポートするかどうか
- リースの期間
- IP テレフォニー デバイスがこのプールのアドレスを使用するために必要な TFTP サーバの場所

関連項目

- DHCP ポリシーの定義 （3228 ページ）
- Cisco IOS ルータにおける DHCP （3224 ページ）

ステップ 1 [DHCP] ページで、[IPプール（IP Pools）] の下にある [作成（Create）] ボタンをクリックします。[IP Pool] ダイアログボックスが表示されます。

ステップ 2 アドレス プールを定義します。使用可能なフィールドの説明については、表 892 : [IP Pool] ダイアログボックス （3235 ページ）を参照してください。

ステップ 3 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。IP プールが [DHCP] ページの [IP Pools] の下にあるテーブルに表示されます。

ステップ 4 必要に応じてステップ 1 （3230 ページ）～ステップ 3 （3230 ページ）を繰り返して、他のアドレス プールを定義します。

（注） IP プールを編集するには、テーブルからプールを選択し、[編集（Edit）] ボタンをクリックします。IP プールを削除するには、テーブルからプールを選択し、[削除（Delete）] ボタンをクリックします。アドレスが DHCP クライアントに割り当てられているプールを削除することはできません。

[DHCP] ポリシー ページ

[DHCP] ポリシー ページでは、選択したルータ上の DHCP サーバ ポリシーを定義します。たとえば、要求側クライアントへのアドレスの割り当て時に DHCP サーバで使用するアドレス プールを指定します。

詳細については、DHCP ポリシーの定義 （3228 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [DHCP] を選択します。[DHCP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおける DHCP （3224 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *890 : [DHCP]* ポリシー ページ

要素	説明
[データベーステーブル（Database Table）]	
Database URL	外部の DHCP データベース エージェントの URL。
タイムアウト（Timeout）	データベース転送を中断するまでに外部の DHCP データベースエージェントからの応答を待機する時間（秒単位）。
Write Delay	外部の DHCP データベース エージェントに送信される DHCP 割り当て更新の間隔（秒数）。
[追加（Add）] ボタン	[DHCP Database] ダイアログボックス （3233 ページ）が開きます。ここから、DHCP データベース エージェントを定義できます。
[編集（Edit）] ボタン	[DHCP Database] ダイアログボックス （3233 ページ）が開きます。ここから、選択した DHCP データベース エージェントを編集できます。
[削除（Delete）] ボタン	選択した DHCP データベース エージェントを削除します。
Excluded IPs	
[除外 IP または IP 範囲（Excluded IPs or IP Ranges）]	DHCP から除外する IP アドレスまたはアドレス範囲。これらのアドレスは、DHCP サーバによって、アドレスを要求している DHCP クライアントに割り当てられません。 1 つ以上のネットワークアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 詳細については、 ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。
[IP Pools] テーブル	
名前	IP プールの名前。
ネットワーク（Network）	IP プールの IP アドレスおよびサブネットマスク。
デフォルト ルータ	DHCP クライアントで使用するデフォルト ルータの IP アドレス。
DNS サーバー	DHCP クライアントで使用する DNS サーバの IP アドレス。

要素	説明
[NetBIOS（WINS）サーバー（NetBIOS (WINS) Server）]	Microsoft DHCP クライアントで使用する Windows インターネット ネーム サービス（WINS）サーバーの IP アドレス。
ドメイン名	DHCP クライアントのドメイン名。
Import All	リモート DHCP サーバが特定の DHCP オプションを中央の DHCP サーバからインポートするかどうかを示します。
Secured ARP	Secured ARP がこの IP プールでイネーブルになっているかどうかを示します。この機能を使用すると、未認可ユーザによる IP スプーフィングを防止できます。
Lease	この IP プールから DHCP サーバーによって割り当てられた各 IP アドレスのリース期間。
オプション 150	DHCP option 150 を使用して定義された、IP 電話での設定に必要な TFTP サーバの IP アドレス。
Option 66	DHCP option 66 を使用して定義された、IP 電話での設定に必要な TFTP サーバの IP アドレス。
[追加（Add）] ボタン	[IP Pool] ダイアログボックス （3234 ページ）が開きます。ここから、DHCP IP アドレス プールを定義できます。
[編集（Edit）] ボタン	[IP Pool] ダイアログボックス （3234 ページ）が開きます。ここから、選択した IP プールを編集できます。
[削除（Delete）] ボタン	選択した IP プールを削除します。
Relay parameters	
ポリシー	DHCP リレーエージェントがすでにリレー情報が含まれているメッセージを受信するときに実装するポリシー。 • [Drop]：Option 82 情報も存在する場合、リレー エージェントは、既存のリレー情報を含むメッセージを廃棄します。 • [Keep]：リレーエージェントは、既存のリレー情報を保持します。 • [Replace]：リレーエージェントは、既存の情報を独自のリレー情報で上書きします。

要素	説明
オプション	選択すると、DHCP クライアントからサーバに転送されたメッセージ要求への DHCP Option 82 データの挿入がイネーブルになります。DHCP Option 82 は、DHCP サーバに要求側クライアントのスイッチおよびポート ID の両方を提供します。このオプションにより、ユーザーがネットワークに物理的に接続している場所を特定し、スプーフィングを防ぐことができます。 DHCP リレーエージェントについて （3226 ページ）を参照してください。 選択を解除すると、DHCP Option 82 がディセーブルになります。
Check	選択すると、DHCP サーバーから受信される DHCP Option 82 応答パケットが検証されます。無効なメッセージはドロップされます。有効なメッセージは、DHCP クライアントに転送される前に option-82 フィールドが削除されます。 選択を解除すると、先に有効性が確認されることなく option-82 フィールドはパケットから削除されます。

[DHCP Database] ダイアログボックス

[DHCP Database] ダイアログボックスを使用して、自動バインディングが含まれている外部の DHCP データベースを定義します。定義する各データベース URL は一意である必要があります。

詳細については、DHCP データベース エージェントについて （3225 ページ）を参照してください。

ナビゲーション パス

[DHCP] ポリシー ページ （3230 ページ）に移動してから、データベーステーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- DHCP ポリシーの定義 （3228 ページ）
- Cisco IOS ルータにおける DHCP （3224 ページ）
- [IP Pool] ダイアログボックス （3234 ページ）

フィールド リファレンス

表 *891 : [DHCP Database]* ダイアログボックス

要素	説明
Database URL	自動バインディングが含まれている外部の DHCP データベース エージェントの URL。URL は、HTTP、FTP、TFTP、または RCP 形式で入力できます。 （注） URL を定義する場合、IP アドレス プールを定義する必要はありません。ただし、定義することもできます。
タイムアウト（Timeout）	DHCP サーバがデータベース転送を中断するまで外部の DHCP データベース エージェントからの応答を待機する時間（秒数）。デフォルトは 300 秒（5 分）です。 （注） 値を 0 に設定するとタイムアウトがディセーブルになります。
Write Delay	DHCP サーバから外部の DHCP データベース エージェントに送信される更新の間隔（秒数）。最小遅延は 60 秒です。デフォルトは 300 秒（5 分）です。

[IP Pool] ダイアログボックス

[IP Pool] ダイアログボックスでは、DHCP サーバがダイナミック アドレスを DHCP クライアントに割り当てるために使用するアドレス プールを 1 つ以上定義します。外部の DHCP データベース エージェントが定義されている場合を除き、少なくとも 1 つのアドレス プールを定義する必要があります。

ナビゲーション パス

[DHCP] ポリシー ページ （3230 ページ）に移動してから、[IPプール（IP Pools）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- DHCP アドレス プールの定義 （3229 ページ）
- DHCP データベース エージェントについて （3225 ページ）
- [DHCP Database] ダイアログボックス （3233 ページ）
- Cisco IOS ルータにおける DHCP （3224 ページ）

フィールド リファレンス

表 *892 : [IP Pool]* ダイアログボックス

要素	説明
プール名（Pool Name）	IP プールの名前。
ネットワーク（Network）	IP プールの IP アドレスおよびサブネットマスク。このサブネットには、DHCP サーバがクライアントへの割り当てに使用できる IP アドレスの範囲が含まれます。 ネットワーク/ホストオブジェクトのアドレスとマスク、または名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 **ヒント** 範囲内の特定のアドレスを [Excluded IPs] フィールドで定義して、それらのアドレスを除外できます。[DHCP] ポリシー ページ （3230 ページ）を参照してください。
Default Router Addresses	この IP プールを使用している DHCP クライアントのデフォルトルータの IP アドレス。DHCP クライアントが起動した後、このルータへのパケットの送信が開始されます。ルータは、クライアントとして同じサブネット上に存在する必要があります。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
DNS Server Addresses	この IP プールを使用する DHCP クライアントがホスト名を IP アドレスに関連付ける必要があるときに問い合わせる DNS サーバの IP アドレス。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
NetBIOS (WINS) Server Addresses	Microsoft DHCP クライアントでホスト名を一般的なネットワーク グループ内の IP アドレスに関連付けるために使用する Windows Internet Naming Service（WINS）サーバの IP アドレス。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
ドメイン名	この IP プールを使用している DHCP クライアントのドメイン名。この名前を指定すると、これらのクライアントはドメインを構成する一般的なネットワーク グループ内に配置されます。

要素	説明
Import All	選択すると、リモート DHCP サーバは中央のサーバから特定の DHCP オプション（DNS サーバなど）をインポートできます。このオプションは、設定情報を自動的に更新できるようにする場合に使用します。 選択を解除すると、すべての DHCP オプションがこの特定のサーバに対してローカルになります。
Secured ARP	選択すると、DHCP 認可 ARP 機能がイネーブルになり、認可されたモバイル ユーザへの IP アドレスのリースが制限されます。この機能は、権限のないユーザーによる IP スプーフィングの防止に役立ちます。 Secured ARP について （3227 ページ）を参照してください。 選択を解除すると、DHCP 認可 ARP 機能はディセーブルになります。 （注） この機能を使用すると、インターフェイスにおける動的な ARP 学習がディセーブルになります。
Lease Never Expires	選択すると、DHCP サーバは IP アドレスをクライアントに永続的に割り当てます。 選択を解除すると、アドレスは、[Time Length] フィールドに定義された期間だけリースされます。
Time Length (DD:HH:MM)	[Lease Never Expires] チェックボックスがオフになっている場合にだけ適用されます。 この IP プールから割り当てられた各 IP アドレスに対して指定するリース期間（DD:HH:MM の形式）。リース期間が終了すると、割り当てられた IP アドレスが無効になり、プールに返されます。
[オプション66（Option 66）]（IP アドレス）	IP 電話に設定ファイルを提供するために使用される TFTP サーバの IP アドレス。これらの設定ファイルでは、Cisco CallManager に接続するために IP 電話で必要とされるパラメータを定義します。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） このオプションは、機能的には [Option 150] と似ています。一方または両方のオプションを使用できます。

要素	説明
Option 150 (IP Addresses)	IP 電話に設定ファイルを提供するために使用される TFTP サーバの IP アドレス。これらの設定ファイルでは、Cisco CallManager に接続するために IP 電話で必要とされるパラメータを定義します。 最大 8 つのアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） このオプションは、機能的には [Option 66] と似ています。一方または両方のオプションを使用できます。

Cisco IOS ルータにおける NTP

ネットワーク タイム プロトコル（NTP）は、ネットワーク デバイス間の時間同期の標準です。時間の同期により、syslog およびその他のデバッグ出力を特定のイベントに関連付けることができます。これは、トラブルシューティング、障害分析、およびセキュリティ インシデントの追跡に必要です。時間の比較は、ネットワーク内で発生するロギング、管理、および AAA 機能の間で正確な時間の同期がない限り、実行できません。

NTP では、ストラタムの概念を利用して、マシンが信頼できる時刻源からどれだけ離れているかを示します。たとえば、ストラタム 1 タイム サーバは、ラジオ クロックまたはアトミック クロックに直接接続されています。NTP は、この信頼できる時刻源の時刻をネットワーク全体に配信します。ストラタム 2 タイムサーバーは、ストラタム 1 タイムサーバーと同期します。ストラタム 3 タイムサーバーは、ストラタム 2 タイムサーバーと同期します。以降、同様に続きます。1 分あたり 1 つの NTP トランザクションを実行するだけで、2 台のマシンを 1 ミリ秒以内に同期できます。

NTP はポート 123 を使用し、ユーザ データグラム プロトコル（UDP）で動作します。Security Manager では、RFC 1305 で規定されている NTP バージョン 3 がサポートされます。

関連項目

- NTP サーバの定義 （3237 ページ）

NTP サーバの定義

ここでは、ルータが時間の同期に使用する NTP サーバを定義する方法について説明します。NTP ポリシーの展開後、ルータは、遅延、分散、ジッタなどの要素に基づくアルゴリズムを使用して、最も正確な NTP サーバを特定し、そのサーバと同期をとります。

グローバル レベルでは、MD5 認証をイネーブルにし、ルータから送信されたすべての NTP パケットに対して使用する送信元アドレスを指定します。

ポリシーへの NTP サーバーの追加は、その IP アドレスを入力するだけで完了します。さらに、任意で認証パラメータを定義したり、精度が同程度の他の NTP サーバよりも特定のサーバを優先するかどうかを指定したりできます。

関連項目

- NTP サーバの定義 （3237 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[NTP] ページが表示されます。このページのフィールドの説明については、表 893 : [NTP] ページ （3240 ページ）を参照してください。

ステップ 2 （任意）[ソースインターフェイス（Source Interface）] フィールドに、インターフェイスまたはインターフェイスロールの名前を入力します。このインターフェイスまたはインターフェイスロールのアドレスが、ルータから送信されるすべての NTP パケットの送信元インターフェイスとして使用されます。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。送信元インターフェイスには IP アドレスが必要です。

このオプションは、NTP サーバが（たとえばファイアウォールが原因で）接続元のアドレスに到達できない場合に役立ちます。このフィールドに値を入力しない場合は、発信インターフェイスのアドレスが使用されます。

（注） ステップ 5 （3238 ページ）の手順に従って、個々の NTP サーバについてこのグローバル設定を上書きできます。

ステップ 3 （任意）[NTP認証の有効化（Enable NTP Authentication）] チェックボックスをオンにして、このルータとこのポリシーで定義する NTP サーバー間のすべてのアソシエーションを認証します。

ステップ 4 [サーバー（Servers）] テーブルの下にある [追加（Add）] ボタンをクリックして、[NTPサーバー（NTP Server）] ダイアログボックスを表示します。ここから、NTP サーバを定義できます。

ステップ 5 NTP サーバを定義します。使用可能なフィールドの説明については、表 894 : [NTP Server] ダイアログボックス （3241 ページ）を参照してください。

ステップ 6 （任意）この NTP サーバの認証パラメータを定義します。

（注） 前に定義した認証キーの値を変更すると、変更はこのキーを共有するすべての NTP サーバに反映されます。

（注） Security Manager で認証キーを定義すると、CLI コマンドの最後に値 0 が自動的に付加されます。この値は、デフォルトの認証キー暗号化タイプを表し、CLI を使用して変更できます。

ステップ 7 ステップ 5 （3238 ページ）～ステップ 6 （3238 ページ）を繰り返して、他の NTP サーバを定義します。

ステップ 8 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義が [Servers] テーブルに表示されます。

（注） NTP サーバーを編集するには、[サーバー（Servers）] テーブルからサーバーを選択し、[編集（Edit）] をクリックします。NTP サーバーを削除するには、そのサーバーを選択し、[削除（Delete）] をクリックします。削除するサーバに定義されているキーが別の NTP サーバに定義されていない場合は、キーも削除されます。

[NTP Policy] ページ

[NTP] ページでは、ルータが時間の同期に使用できる NTP サーバを 1 つ以上定義します。たとえば、必要に応じて認証をイネーブルにしたり、これらのサーバに送信されるすべてのトラフィックのグローバル送信元インターフェイスを定義したりします。

詳細については、NTP サーバの定義 （3237 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]** を選択します。[NTP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおける NTP （3237 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *893 : [NTP]* ページ

要素	説明
送信元インターフェイス（Source Interface）	NTP サーバに送信されるすべてのパケットの送信元アドレス。この設定は、NTP サーバが（たとえばファイアウォールが原因で）パケットの送信元のアドレスに応答できない場合に必要になることがあります。送信元インターフェイスには IP アドレスが必要です。 このフィールドで値を定義しない場合、発信インターフェイスのアドレスが使用されます。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） このフィールドで定義した送信元インターフェイスは、個々の NTP サーバに対して上書きできるグローバル設定です。詳細については、[NTP Server] ダイアログボックス（3241 ページ）を参照してください。
Enable NTP Authentication	選択すると、NTP サーバに接続するときに MD5 を使用した認証がイネーブルになります。 選択を解除すると、認証がディセーブルになります。
[Servers] テーブル	
IPアドレス	NTP サーバの IP アドレス。
送信元インターフェイス（Source Interface）	この NTP サーバに送信されるすべてのパケットの送信元アドレス。この設定は、ページの上部で定義されたグローバル設定を上書きします。
優先（Preferred）	精度が同程度の他の NTP サーバーよりもこの NTP サーバーが優先されるかどうかを示します。 （注） デフォルトでは、優先サーバがテーブルの最初に表示されます。
Key Number	この NTP サーバによる認証に使用されるキーの ID 番号。
信頼できる	この NTP サーバ用に定義された認証キーが trusted key であるかどうかを示します。
[追加（Add）] ボタン	[NTP Server] ダイアログボックス （3241 ページ）が開きます。ここから、NTP サーバを定義できます。

要素	説明
[編集（Edit）] ボタン	[NTP Server] ダイアログボックス （3241 ページ）が開きます。ここから、選択した NTP サーバを編集できます。
[削除（Delete）] ボタン	選択した NTP サーバをテーブルから削除します。 削除するサーバに定義されているキーが別の NTP サーバに定義されていない場合は、キーも削除されます。

[NTP Server] ダイアログボックス

[NTP Server] ダイアログボックスでは、ルータが時間の同時を実行するために使用できる NTP サーバのアドレスを定義します。さらに、このダイアログボックスを使用して、このサーバに送信される NTP パケットのデフォルトの送信元インターフェイスと認証パラメータを定義できます。

ナビゲーション パス

[NTP Policy] ページ （3239 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- NTP サーバの定義 （3237 ページ）
- Cisco IOS ルータにおける NTP （3237 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *894 : [NTP Server]* ダイアログボックス

要素	説明
IPアドレス	NTP サーバの IP アドレス。ネットワーク/ホストオブジェクトのアドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
送信元インターフェイス（Source Interface）	この NTP サーバに送信されるすべてのパケットの送信元アドレス。この設定は、NTP サーバが（たとえばファイアウォールが原因で）パケットの送信元のアドレスに応答できない場合に必要になることがあります。送信元インターフェイスには IP アドレスが必要です。 このフィールドで値を定義せず、グローバル設定がない場合は、発信インターフェイスのアドレスが使用されます。 （注） この設定は、[NTP Policy] ページ （3239 ページ）で定義したグローバル設定を上書きします。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
優先（Preferred）	選択すると、精度が同程度の他の NTP サーバよりもこの NTP サーバが優先されます。このサーバが同期に使用される場合、ローカルクロックの修正に使用される時間オフセットは、このサーバだけに基づいて計算されます。 （注） 別の NTP サーバが優先サーバよりも著しく正確な場合（たとえば、ストラタム 2 対ストラタム 3）、ルータはより正確なサーバと同期をとります。 選択を解除すると、この NTP サーバは、精度が同程度の他の NTP サーバよりも優先されません。ローカルクロックの修正に使用される時間オフセットは、すべての NTP サーバのオフセットを組み合わせて計算されます。 複数のサーバのストラタムが同じであり、優先サーバの精度を信頼できる場合にだけ、特定の NTP サーバを優先サーバとして設定することを推奨します。
認証キー（Authentication Key）	NTP サーバによるアソシエーションの認証に使用される MD5 キー。 • [Key Number]：認証キーの ID 番号。キー番号を入力するか、またはリストから定義済みの番号を選択します。 • [Key Value]：認証キーを定義する最大 32 文字の文字列。[Confirm] フィールドに文字列をもう一度入力します。 • [Trusted]：選択すると、このキーはこのサーバと同期しようとしているシステムの ID を認証します。選択を解除すると、このキーは認証に使用されません。 リストからキー番号を選択してキー値を変更する場合は、この変更を保存すると同じ認証キーを使用する他の NTP サーバに影響する、という内容の警告が表示されます。 （注） 認証を使用するには、[NTP Policy] ページ （3239 ページ）で認証をイネーブルにする必要があります。

第 64 章

アイデンティティ ポリシーの設定

IEEE 802.1x 規格では、クライアントサーバ ベースのアクセス コントロールとしての 802.1x ポートベース認証と、未認可のクライアントがパブリック ポート経由で LAN に接続することを制限する認証プロトコルを規定しています。認証サーバは、インターフェイスに接続された各クライアントを検証してから、ルータまたは LAN により提供されたサービスを使用可能にします。

クライアントが認証されるまでは、802.1x アクセス コントロールにより、クライアントの接続先のインターフェイスを介した Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許可されます。認証が成功すると、通常のトラフィックはそのインターフェイスを通過できるようになります。

802.1x 認証は VPN アクセス コントロールを提供します。この場合、未認証のトラフィックはインターネットにはアクセスできますが、VPN トンネルにはアクセスできません。企業の社員が、他の家族会員がインターネットへのアクセスに使用するホーム アクセス ルータを介して企業 VPN にアクセスする場合は、特にこのソリューションが役立ちます。802.1x を使用する場合、仮想インターフェイスを作成して、未認証トラフィックを伝送します。認証済みトラフィックは引き続き物理インターフェイスを通過します。

802.1x では、DHCP を使用して、認証を要求するクライアントに IP アドレスを提供する必要があります。認証済みトラフィック用と未認証トラフィック用に 1 つずつ、2 つの IP アドレス プールを使用することを推奨します。2 つのプールを使用する場合、企業 DHCP プール内の DNS サーバが企業 DNS サーバを指している必要があります。企業以外の DHCP プールの DNS サーバは、パブリック インターフェイス上の ISP により提供された DNS サーバを使用する必要があります。DHCP を設定するには、DHCP ポリシーを選択します。

- Cisco IOS ルータでの 802.1x （3244 ページ）
- [802.1x] ポリシー ページ （3249 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）
- [Network Admission Control Policy] ページ （3260 ページ）

Cisco IOS ルータでの 802.1x

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IEEE 802.1x 規格では、クライアントサーバ ベースのアクセス コントロールとしての 802.1x ポートベース認証と、未認可のクライアントがパブリック ポート経由で LAN に接続することを制限する認証プロトコルを規定しています。認証サーバは、インターフェイスに接続された各クライアントを検証してから、ルータまたは LAN により提供されたサービスを使用可能にします。

クライアントが認証されるまでは、802.1x アクセス コントロールにより、クライアントの接続先のインターフェイスを介した Extensible Authentication Protocol over LAN（EAPOL）トラフィックだけが許可されます。認証が成功すると、通常のトラフィックはそのインターフェイスを通過できるようになります。

802.1x 認証は VPN アクセス コントロールを提供します。この場合、未認証のトラフィックはインターネットにはアクセスできますが、VPN トンネルにはアクセスできません。企業の社員が、他の家族会員がインターネットへのアクセスに使用するホーム アクセス ルータを介して企業 VPN にアクセスする場合は、特にこのソリューションが役立ちます。802.1x を使用する場合、仮想インターフェイスを作成して、未認証トラフィックを伝送します。認証済みトラフィックは引き続き物理インターフェイスを通過します。

802.1x では、DHCP を使用して、認証を要求するクライアントに IP アドレスを提供する必要があります。認証済みトラフィック用と未認証トラフィック用に 1 つずつ、2 つの IP アドレス プールを使用することを推奨します。2 つのプールを使用する場合、企業 DHCP プール内の DNS サーバが企業 DNS サーバを指している必要があります。企業以外の DHCP プールの DNS サーバは、パブリック インターフェイス上の ISP により提供された DNS サーバを使用する必要があります。DHCP を設定するには、DHCP ポリシーを選択します。詳細については、Cisco IOS ルータにおける DHCP （3224 ページ）を参照してください。

（注） 802.1x は、Cisco 800、1700、1800、1900、2600、2800、2900、3600、3700、3800、3900 シリーズ ルータのプラットフォームでサポートされます。

802.1x の詳細については、次の項を参照してください。

- 802.1x デバイス ロールについて （3245 ページ）
- 802.1x インターフェイス認可状態 （3245 ページ）
- 802.1x でサポートされるトポロジ （3246 ページ）
- 802.1x ポリシーの定義 （3247 ページ）

802.1x デバイス ロールについて

802.1x ポートベース認証では、次のデバイス ロールが使用されます。

- クライアント：VPN へのアクセスを要求しているワークステーション。このクライアントでは、Microsoft Windows XP オペレーティング システムで提供されるような、802.1x 準拠クライアント ソフトウェアが実行されている必要があります。
- 認証サーバ：クライアントを認証します。認証サーバーは、クライアントのアイデンティティを検証し、クライアントがネットワークへのアクセスを認可されているかどうかをルータに通知します。サポートされている認証サーバは、EAP 拡張機能付きの Remote Authentication Dial-In User Service（RADIUS）セキュリティ システムだけです。Security Manager では、AAA サーバ オブジェクトで定義されているように、AAA（認証、許可、アカウンティング）サーバが 802.1x ポリシー用の認証サーバです。
- ルータ（エッジルータまたはワイヤレスアクセスポイント）：クライアントの認証ステータスに基づいてネットワークへの物理アクセスを制御します。ルータは、クライアントと認証サーバの中間（プロキシ）です。クライアントからのアイデンティティ情報を要求し、認証サーバを使用してその情報を検証し、応答をクライアントにリレーします。Security Manager では、802.1x ポリシーを設定するルータがスイッチとして機能します。

関連項目

- 802.1x インターフェイス認可状態 （3245 ページ）
- 802.1x でサポートされるトポロジ （3246 ページ）
- 802.1x ポリシーの定義 （3247 ページ）
- Cisco IOS ルータでの 802.1x （3244 ページ）

802.1x インターフェイス認可状態

802.1x を使用する場合、クライアント ネットワーク アクセスが許可されるかどうかは、インターフェイス状態によって決まります。デフォルトでは、インターフェイスは未認可状態で開始されます。インターフェイスがこの状態の間は、EAPOL パケットを除き、両方向のすべてのトラフィックが禁止されます。クライアントが認証されると、インターフェイスは認可済み状態に移行し、すべてのクライアント トラフィックを正常に伝送できるようになります。

802.1x がサポートされていないクライアントが未認可の 802.1x インターフェイスに接続する場合、ルータはクライアントのアイデンティティを要求します。この状況ではクライアントは要求に応答せず、インターフェイスは未認可状態のままであり、クライアントはネットワークへのアクセスを許可されません。これに対し、802.1x 対応のクライアントが、802.1x プロトコルを実行していないインターフェイスに接続される場合、クライアントでは、EAPOL-Start フレームを送信することによって認証プロセスを開始します。応答を受信できない場合、クライアントは要求を一定の回数送信します。応答を受信できないため、クライアントは、インターフェイスが未認可状態のときと同様にフレームの送信を開始します。

次のいずれかのオプションを選択することにより、インターフェイス認可状態を制御できます。

- [Auto]：802.1x 認証をイネーブルにします。この場合、インターフェイスは未認可状態で開始されます。EAPOL フレームだけが、インターフェイスを介して送受信されます。インターフェイスのリンク状態が down から up に移行したとき、または EAPOL-Start フレームが受信されると、認証が開始されます。ルータはクライアントのアイデンティティを要求し、クライアントと認証サーバー間で認証メッセージのリレーを開始します。ルータは、ネットワークにアクセスしようとする各クライアントの MAC アドレスを、一意のクライアント識別子として使用します。
- [Force authorized]：802.1x 認証をディセーブルにします。この場合、インターフェイスはクライアントを認証せずに認可済み状態に移行します。

クライアントの認証が正常に完了すると、インターフェイス状態が認可済みに変わります。これにより、クライアントからのすべてのフレームがネットワークに入ることができます。認証に失敗した場合、インターフェイスは未認可状態のままになりますが、認証は再試行できます。認証サーバに到達できない場合、ルータは要求を再送信できます。定義された回数試行したあとも認証サーバが応答しない場合、認証は失敗し、クライアントに対してネットワークアクセスが拒否されます。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。これにより、インターフェイスは未認可状態に戻ります。

関連項目

- 802.1x デバイス ロールについて （3245 ページ）
- 802.1x でサポートされるトポロジ （3246 ページ）
- 802.1x ポリシーの定義 （3247 ページ）
- Cisco IOS ルータでの 802.1x （3244 ページ）

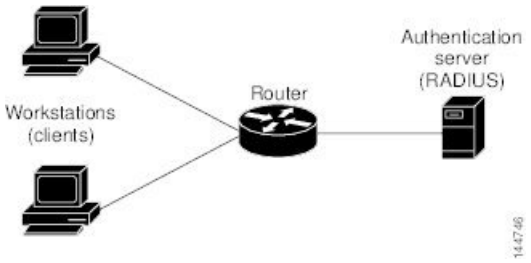
802.1x でサポートされるトポロジ

802.1x ポートベース認証では、次の 2 つのトポロジがサポートされます。

- ポイントツーポイント
- Wireless LAN（ワイヤレス LAN）

ポイントツーポイント設定では、1 つだけのクライアントを 802.1x 対応インターフェイスに接続できます。インターフェイス状態が down から up に変わると、ルータはクライアントを検出します。クライアントがネットワークを出ると、または別のクライアントに置き換えられると、インターフェイス状態が up から down に変わります。これにより、インターフェイスは未認可状態に戻ります。

図 *52 : 802.1x* トポロジ



ワイヤレス LAN 設定においては、802.1x インターフェイスはマルチホスト モードで設定され、1 つのクライアントが認証されるとすぐに認可されます。インターフェイスが認可されると、そのインターフェイスに間接的に接続されている他のすべてのクライアントに対してネットワークへのアクセスが許可されます。（再認証が失敗したか、または EAPOL-Logoff メッセージが受信されたかのいずれかの理由で）ポートが未認可になると、ルータは、接続されているすべてのクライアントに対してネットワークへのアクセスを拒否します。このトポロジでは、ワイヤレス アクセス ポイントがルータへのクライアントとなり、接続されているクライアントを認証します。

関連項目

- 802.1x デバイス ロールについて （3245 ページ）
- 802.1x インターフェイス認可状態 （3245 ページ）
- 802.1x ポリシーの定義 （3247 ページ）
- Cisco IOS ルータでの 802.1x （3244 ページ）

802.1x ポリシーの定義

802.1x ポリシーを設定するには、次のものを定義します。

- ネットワークへの接続を試行しているホストを認証する AAA サーバが含まれる AAA サーバ グループ。
- 未認証のトラフィックを伝送する仮想インターフェイスと、認証済みのトラフィックを伝送する物理インターフェイス。
- （任意）物理インターフェイスのプロパティ。コントロール タイプ、自動再認証、および複数のタイムアウト値が含まれます。

802.1x ポリシーを定義するルータが VPN の一部でない場合（たとえば、アクセスを制限する対象の企業ネットワークに直接接続されている場合）、手動でアクセス リストを定義する必要があります。このためには、アクセス ルール ポリシーを定義します（アクセス ルールについて （913 ページ）を参照）。

はじめる前に

- 選択したルータを、2 つの IP アドレス プール（認証済みクライアント用と未認証クライアント用に 1 つずつ）を含む DHCP ポリシーとともに設定します。 DHCP ポリシーの定義 （3228 ページ）を参照してください。
- ルータが設定済みの AAA（RADIUS）サーバにパケットをルーティングできることを確認します。このことは、ルータからサーバに ping を実行することによって確認できます。

関連項目

- 802.1x デバイス ロールについて （3245 ページ）
- 802.1x インターフェイス認可状態 （3245 ページ）
- 802.1x でサポートされるトポロジ （3246 ページ）
- Cisco IOS ルータでの 802.1x （3244 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [802.1x] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [802.1x] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[802.1x] ページが表示されます。このページのフィールドの説明については、表 895 : [802.1x] ページ （3250 ページ）を参照してください。

ステップ 2 802.1x を使用してクライアントを認証するために使用する AAA サーバーを含む AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックして、リストからサーバーグループを選択するか、新しいサーバーグループを作成します。選択した AAA サーバは、EAP 拡張機能付きの RADIUS を使用する必要があります。

（注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。

ステップ 3 [仮想テンプレート（Virtual Template）] フィールドに、未認証トラフィックを伝送するための非信頼仮想インターフェイスとして使用する、インターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックして、リストからインターフェイスロールを選択するか、新しいロールを作成します。詳細については、 ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

（注） （Cisco 800、1800、1900、2800、2900、3800、および 3900 シリーズなどの）サービス統合型ルータ（ISR）では、未認証トラフィックを伝送するとき、自動的に VLAN を使用します。ただし、仮想テンプレートを定義した場合は、VLAN の代わりにその仮想テンプレートが使用されます。

（注） ここで定義した仮想テンプレートに PPP が定義されている場合は、展開に失敗することがあります。 PPP 接続の定義 （3096 ページ）を参照してください。

ステップ 4 認証済みトラフィックを伝送するための信頼物理インターフェイスとして使用するインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックして、リストからロールを選択します。

選択するインターフェイス ロールは、VPN トポロジの一部として設定された内部の保護対象インターフェイスを表す必要があり、選択したルータ上のそれ以外の物理インターフェイスを表さない必要があります。詳細については、エンドポイントおよび保護対象ネットワークの定義 （1424 ページ）を参照してください。

ステップ 5 （任意）802.1x 認証に使用される物理インターフェイスのデフォルトを変更します。詳細については、表 895 : [802.1x] ページ （3250 ページ）を参照してください。

[802.1x] ポリシー ページ

[802.1x] ポリシー ページを使用して、認可済みユーザに対して VPN アクセスを制限するポリシーを作成します。認証済みトラフィックは、ルータ上の指定された物理インターフェイスを通過することを許可されます。未認証トラフィックは、インターネットへの仮想インターフェイスを通過することを許可されますが、VPN へのアクセスは許可されません。

詳細については、802.1x ポリシーの定義 （3247 ページ）を参照してください。

（注） 802.1x ポリシーでは、IP アドレスをクライアントに割り当てるために DHCP アドレス プールが必要です。これらのプールを定義するには、同じルータ上で DHCP ポリシーを定義します。[DHCP] ポリシー ページ （3230 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）>[アイデンティティ（Identity）] > [802.1x] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [802.1x] を選択します。[802.1x] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータでの 802.1x （3244 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *895 : [802.1x]* ページ

要素	説明
AAA サーバー グループ	VPN トンネルにアクセスしようとするユーザのクレデンシャルを認証する RADIUS AAA サーバ グループ。AAA サーバー グループ オブジェクトの名前を入力します。または、[追加（Add）] をクリックして、リストから AAA サーバー グループ オブジェクトを選択するか、新しい AAA サーバー グループ オブジェクトを作成します。 （注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。
Virtual Template	サービス統合型ルータ（ISR）を除くすべてのルータで必須です。 未認証トラフィックに対してインターネット アクセスを提供する非信頼仮想インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいグループオブジェクトを作成します。 （注） ISR では自動的に VLAN を使用してアクセスを提供するため、ISR の仮想テンプレートを設定する必要はありません。ただし、仮想テンプレートを定義した場合は、VLAN の代わりにその仮想テンプレートが使用されます。 （注） ここで定義した仮想テンプレートに PPP が定義されている場合は、展開に失敗することがあります。 [PPP] ダイアログボックス - [PPP] タブ （3104 ページ）を参照してください。
インターフェイス	認証済みトラフィックに対して VPN アクセスを提供する信頼仮想インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいグループオブジェクトを作成します。 インターフェイス ロールを使用する場合、インターフェイス ロール内に定義されているパターンは、選択したデバイス上の 1 つだけの物理インターフェイスを表している必要があります。このインターフェイスは、VPN トポロジの一部として設定した内部の保護対象インターフェイスである必要があります。詳細については、 エンドポイントおよび保護対象ネットワークの定義（1424 ページ）を参照してください。

要素	説明
リトライ回数	応答を受信できない場合に物理インターフェイスが認証を再開する前に Extensible Authentication Protocol（EAP）request/identity フレームをクライアントに再送信する回数。 有効な値の範囲は 1 ～ 10 です。デフォルトは 2 です。 （注） リンクが信頼できない場合や、特定のクライアントおよび認証サーバに関連する特定の問題がある場合など、異常な状況を調整する目的以外では、デフォルトを変更しないでください。
Control type	インターフェイスのコントロール状態。ホストがネットワークへのアクセスを許可されるかどうかは、この状態によって決まります。次のオプションがあります。 • [Force Authorize]：802.1x 認証をディセーブルにします。これにより、インターフェイスは認証交換を行わなくても認可済み状態に移行します。つまり、インターフェイスは、ホストの 802.1x ベースの認証なしで通常のトラフィックを送受信します。これがデフォルトです。 • [Auto]：802.1x 認証をイネーブルにします。これにより、インターフェイスは未認可状態で開始されるため、このインターフェイスではEAPOLフレームだけを送受信できるようになります。ホストの認証が正常に完了すると、インターフェイス状態が認可済みに変わります。これにより、このインターフェイスを介するホストからのすべてのフレームがイネーブルになります。
Enable client reauthentication	選択すると、802.1x インターフェイスでのクライアント PC の定期的な再認証がイネーブルになります。再認証は、[Client reauthentication period timeout] フィールドで定義されている時間間隔の経過後に実行されます。デフォルトの期間は 3600 秒（1 時間）です。 選択しない場合、定期的な再認証は実行されません。
Client reauthentication period timeout	[Enable client reauthentication] チェックボックスがオンになっている場合にだけ適用されます。 クライアントの再認証の試行と試行の間の秒数。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 3600 秒（1 時間）です。
待機時間	クライアントとの認証交換が失敗したあとにルータが待機状態でいる時間。認証交換は、クライアントが無効なパスワードを指定したなどの原因で失敗することがあります。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 120 秒です。 （注） デフォルトより小さい値を入力すると、ユーザへの応答時間が速くなります。

要素	説明
Rate Limit period	インターフェイスが、誤作動しているクライアントPCから受信したEAP-Startパケットをスロットルするまでの時間間隔。レート制限と呼ばれるこの設定を使用して、このようなクライアントによってルータ処理能力が浪費されることを回避します。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトでは、レート制限はディセーブルになっています。 （注） 既存のレート制限をディセーブルにするには、このフィールドで定義されている値を削除し、フィールドをブランクにしておきます。
AAA Server timeout	ルータがパケットを AAA サーバに再送信するまでに待機する秒数。ルータが 802.1x パケットを AAA サーバに送信したが、サーバが応答しない場合、ルータはこの時間間隔の経過後に別のパケットを送信します。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 30 秒です。
Supplicant period	ルータが EAP-Request/Identity パケットをサプリカント（クライアント PC）に再送信するまでに待機する秒数。ルータが EAP-Request/Identity パケットをクライアントPC（サプリカント）に送信したが、サプリカントが応答しない場合、ルータはこの時間間隔の経過後に再びパケットを送信します。 有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 30 秒です。

Cisco IOS ルータでのネットワーク アドミッション コントロール

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Network Admission Control（NAC; ネットワーク アドミッション コントロール）は、シスコが後援している業界の先進機能です。NAC では、ネットワーク インフラストラクチャを使用して、ネットワーク コンピューティング リソースへのアクセスを要求するすべてのデバイスにセキュリティ ポリシーを適用することにより、ウイルスやワームによる被害を抑制します。企業はNAC を使用することにより、PC、PDA、サーバなど、確立されたセキュリティ ポリシーに完全に適合することが確認されたエンドポイント デバイスにネットワーク アクセスを提供できます。また、適合しないデバイスを識別してこれらのアクセスを拒否したり、これらを隔離エリアに移したり、コンピューティング ソースへのアクセスを制限したりすることもできます。

ネットワーク アクセスの決定は、ポスチャ検証のプロセスを通して行われます。このプロセスでは、エンドポイント デバイスにより提示されたポスチャ クレデンシャルが評価されます。

これらのクレデンシャルには、エンドポイントのアンチウイルス状態、オペレーティング システム バージョン、オペレーティング システム パッチ レベル、または Cisco Security Agent のバージョンと設定などの情報が含まれることがあります。

NAC を使用して、ブランチ オフィス、リモート アクセス、ダイヤルイン アクセスなど、多くのタイプの展開でセキュリティ ポリシーを適用できます。

Security Manager で NAC ポリシーを使用すると、Cisco IOS ルータを、ネットワークへのアクセスを要求するデバイスにポリシーを適用するためのネットワーク アクセス デバイス（NAD）として使用できます。ここでは、NAC に関する追加情報を示します。

- NAC コンポーネントについて （3254 ページ）
- NAC システム フローについて （3254 ページ）

ここでは、Cisco IOS ルータ上に NAC ポリシーを作成するために実行するタスクについて説明します。

- NAC 設定パラメータの定義 （3255 ページ）
- NAC インターフェイス パラメータの定義 （3257 ページ）
- NAC アイデンティティ パラメータの定義 （3258 ページ）

NAC をサポートするルータ プラットフォーム

ルータに NAC ポリシーを設定するには、そのルータが（拡張セキュリティ機能セットを搭載した）Cisco IOS ソフトウェア Release 12.3(8)T イメージ以降を実行している必要があります。ただし、次のルータは NAC をサポートしていません。

- Cisco 7600 シリーズ（7603、7604、7606、7609、7613）
- Cisco 7300 シリーズ（7301、7304）
- Cisco 7100 シリーズ VPN ルータ（7120、7140、7160）
- Cisco 3600 シリーズ マルチサービス プラットフォーム（3620、3631、3661、3662）
- Cisco 1700 シリーズ モジュラ アクセス ルータ（1710、1720、1750）
- Cisco 1600 シリーズ（1601、1602、1603、1604、1605）
- Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ（全モデル）
- Cisco 800 シリーズ（801、803、805、811、813、828、851、857、871、876、877、878）
- Cisco SOHO 90 シリーズ セキュア ブロードバンド ルータ（91、96、97）
- Cisco SOHO 77 シリーズ（71、76、77 ADSL、77 H ADSL、78）

NAC コンポーネントについて

NAC には、次のコンポーネントが含まれます。

- Cisco Trust Agent（CTA）：CTA は NAC クライアントとして動作します。CTA は、オペレーティング システムのタイプや、インストールされているアンチウイルス ソフトウェアのバージョンなど、インストールされているエンドポイント デバイスのポスチャ クレデンシャルを提供します。
- ネットワーク アクセス デバイス（NAD）：NAD は、インターセプト ACL がトリガーされると、CTA を使用してポスチャ検証を開始します。NAD は、CTA から受信したポスチャ クレデンシャルを AAA サーバにリレーします。代わりに、NAD は AAA サーバから設定情報を受信します。この設定は、選択したインターフェイスに適用されます。また、NAD は次の処理も行います。
  - 定期的に CTA をポーリングして、CTA がこの IP アドレスで同じクライアントと通信していることを確認します。
  - 現在のセッションをすべて再検証します。
  - CTA（クライアントレス ホスト）の存在しないデバイスから、認証のためにユーザ名およびパスワードの情報を AAA サーバに送信します。
  - デバイス IP アドレスまたは MAC アドレスに基づいて、特定のデバイスに適用される定義済みアクションの例外リストをサポートします。

Security Manager で NAC ポリシーを設定すると、NAD として使用する Cisco IOS ルータの動作が設定されます。

- AAA サーバ：AAA サーバは、CTA から受信したポスチャ クレデンシャルを取得して検証し、NAD に適用するアクセス ポリシーを返します。AAA サーバは、RADIUS プロトコルを実行している Cisco Secure Access Control Server（ACS）である必要があります。クライアントレス ホストへのアクセスを提供するために、既存の ACS 認可サポートを使用できます。ポスチャ検証ルールおよびこれらのルールの結果としてのアクセス ポリシーは、ACS で設定します。

関連項目

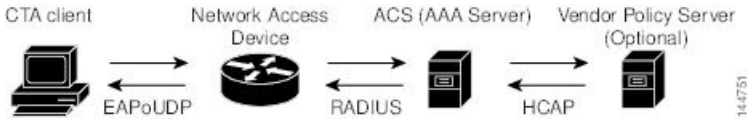
- NAC システム フローについて （3254 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）

NAC システム フローについて

図 53 : NAC システム フロー （3255 ページ）に示すように、NAC のシステム フローは次のようになります。

1. 接続デバイスからの IP パケットが、NAD で設定されているインターセプト ACL をトリガーします。
2. NAD は、Extensible Authentication Protocol over User Datagram Protocol（EAP over UDP、または単に EoU とも呼ばれる）を使用して、デバイスで設定されている CTA を使用してポスチャ検証をトリガーします。
3. CTA は、EAP over UDP を使用して、そのポスチャ クレデンシャルを NAD に送信します。
4. NAD は、RADIUS を使用して、これらのポスチャ クレデンシャルを ACS に送信します。
5. ACS はポスチャ検証を実行します。これにより、デバイスがネットワークへのアクセスを許可されるかどうかが決まります（必要に応じて、ACS はサードパーティ製サーバから追加のポスチャ検証を要求します。たとえば、CTA が特定のアンチウイルス アプリケーションに固有のクレデンシャルを転送した場合、ACS は HCAP プロトコルを介して、検証のためにこの情報をベンダーサーバーに転送します）。デバイスがクライアントレスホストの場合、ACS は、受信したユーザ名とパスワードを、ローカルに格納されているリストと照合してチェックします。
6. ACS は、適切なアクセス ポリシーを要求側デバイスに適用するように NAD に指示します。アクセスは許可、拒否、リダイレクト、または制限されます。

図 *53 : NAC* システム フロー



関連項目

- NAC コンポーネントについて （3254 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）

NAC 設定パラメータの定義

NAC 設定パラメータを設定するには、ネットワークに接続しようとするデバイスから受信したポスチャ クレデンシャルを取得して検証する AAA サーバ グループを選択します。Cisco Secure Access Control Server（ACS）に格納されている定義済みのユーザ名とパスワードによって、Cisco Trust Agent（CTA）の存在しないデバイスを認証できるようにするオプションを設定できます。また、EAP over UDP のデフォルト設定も変更できます。これは、ネットワーク アクセス デバイス（NAD）として機能する Cisco IOS ルータと、ネットワークにアクセスしようとするデバイスの間のポスチャ検証通信に使用されるプロトコルです。

関連項目

- NAC インターフェイス パラメータの定義 （3257 ページ）
- NAC アイデンティティ パラメータの定義 （3258 ページ）

• Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択し、作業領域で [設定（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）]>[ネットワークアドミッションコントロール（Network Admission Control）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

[NAC Setup] タブが表示されます。このタブのフィールドの説明については、表 899 : [Network Admission Control] の [Identities] タブ （3266 ページ）を参照してください。

ステップ 2 ポスチャ検証を実行する AAA サーバーを含む AAA サーバーグループの名前を入力します。または、[選択（Select）] をクリックして、リストからサーバーグループを選択するか、新しいサーバーグループを作成します。選択した AAA サーバ グループには、RADIUS を実行している ACS デバイスが含まれる必要があります。

（注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。

ステップ 3 （任意）メイン サーバ グループのバックアップとして、最大 2 つの AAA サーバ グループを選択します。メイン サーバ グループ内のすべてのサーバが停止した場合、バックアップ サーバ グループ内のサーバが NAC を実行します。

両方のバックアップ サーバ グループは、RADIUS を実行している ACS デバイスで構成されている必要があります。

ステップ 4 （任意）[EAP over UDP] で、次のいずれかまたは両方の [Allow] パラメータを選択します。

a) ACS に送信される RADIUS 要求に IP アドレスを含める場合は、[IPステーションIDを許可（Allow IP Station ID）] チェックボックスをオンにします。

b) CTA がインストールされていないデバイスへのアクセスを提供する場合は、[クライアントレスを許可（Allow Clientless）] チェックボックスをオンにします。このような場合、ACS では、ユーザ名とパスワードを定義済みリストと照合してチェックすることによって、これらのデバイスを認証します。

このチェックボックスをオフにした場合、トラフィックがインターセプト ACL に一致すると、CTA のないデバイスはネットワークへのアクセスを禁止されます。これは、CTA がないと、ポスチャ検証を実行できないためです。

（注） この機能は、Cisco IOS ソフトウェア Release 12.4(6)T 以降を実行しているルータではサポートされません。

ステップ 5 （任意）[Under EAP over UDP] で、必要に応じて、EAP over UDP（EoU）プロトコルに関連するデフォルト設定を変更します。詳細については、表 896 : [Network Admission Control] の [Setup] タブ （3261 ページ）を参照してください。

NAC インターフェイス パラメータの定義

NAC インターフェイス パラメータを設定するには、NAC を実行するインターフェイスを選択します。また、インターセプト ACL を定義する必要もあります。これにより、これらのインターフェイス上のどのトラフィックがポスチャ検証を受けるかが決まります。また任意で、EAP over UDP セッションを開始するためのデバイスレベルの設定を上書きし、すべてのセッションを定期的に再検証することもできます（NAC設定パラメータの定義 （3255ページ）を参照）。

NAC ポリシーが機能するには、少なくとも 1 つのインターフェイス定義が含まれている必要があります。

はじめる前に

- ポスチャ検証を実行する ACS デバイスを含む AAA サーバ グループを選択します。 NAC 設定パラメータの定義 （3255 ページ）を参照してください。
- NAC ポリシーでポスチャ検証を受けるトラフィックを定義する ACL オブジェクトを定義します。 アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。
- 選択したインターフェイスのデフォルト アクセスを定義する ACL オブジェクト（デフォルト ACL）を定義します。 アクセス コントロール リスト オブジェクトの作成 （356 ページ） を参照してください。

関連項目

- NAC 設定パラメータの定義 （3255 ページ）
- NAC アイデンティティ パラメータの定義 （3258 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択し、作業領域で [インターフェイス（Interfaces）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[インターフェイス（Interface）] タブをクリックします。

[NAC Interfaces] タブが表示されます。このタブに含まれるフィールドの説明については、を参照してください。

ステップ 2 NAC の [インターフェイス（Interfaces）] タブで、テーブルからインターフェイス定義を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックして定義を作成します。[NAC Interface Configuration] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、[NAC Identity Action] ダイアログボックス （3267 ページ）を参照してください。

ステップ 3 NAC を実行するインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックして、リストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

ステップ 4 （任意）インターセプト ACL として機能する ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックして、リストから ACL オブジェクトを選択するか、新しいオブジェクトを作成します。

選択したインターフェイス上のどのトラフィックが、ネットワークへのアクセスを許可される前にポスチャ検証を受けるかは、インターセプト ACL によって決まります。ACL を選択しない場合、選択したインターフェイス上のすべてのトラフィックがポスチャ検証を受けます。

（注） NAC インターフェイスと同じインターフェイス上に認証プロキシを定義した場合、両方のポリシーで同じインターセプト ACL を使用する必要があります。このようにしない場合、展開が失敗することがあります。認証プロキシの詳細については、IOS デバイスの AAA ルールの設定 （877 ページ）を参照してください。

ステップ 5 （任意）EAP over UDP セッションを開始するための最大試行回数に定義されているデバイスレベルの値を上書きするには、[EAP over UDP Max Retries] フィールドに新しい値を入力します。

ステップ 6 （任意）NAD ですべての EAP over UDP セッションを定期的に再検証しない場合には、[EOUセッション再検証を有効化（Enable EOU Session Revalidation）] チェックボックスをオフにします。

（注） サブインターフェイスでは、ステップ 5 （3258 ページ）およびステップ 6 （3258 ページ）で説明されているオプションについてだけ、デフォルト値がサポートされています。

ステップ 7 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。インターフェイス定義は、[NAC Interfaces] タブのテーブルに表示されます。

NAC アイデンティティ パラメータの定義

デフォルトでは、選択したインターフェイスを介するトラフィックのうちインターセプト ACL に一致したトラフィックは、ネットワークに入ることを許可される前に、ポスチャ検証されます。ただし、定義済みアクションの例外リストを作成して、特定のデバイスに適用できます。この例外リストを作成するには、アイデンティティプロファイルを使用します。各プロファイルには次の 2 つの要素が含まれています。

- プロファイル定義。プロファイルが適用されるデバイスを識別します。デバイスは、IP アドレス、MAC アドレス、またはタイプ（Cisco IP Phone の場合）で識別できます。

- アクション。このデバイスがネットワークへのアクセスを試行したときの結果を定義します。各アクションには、ACL、リダイレクト URL、またはその両方を含めることができます。アクションを指定しない場合は、デフォルトの ACL が適用されます。

NAC アイデンティティ パラメータを設定するときは、まず 1 つ以上のアイデンティティ アクションを定義してから、これらのアクションを適用するアイデンティティ プロファイルを作成します。各アクションを複数のプロファイルに適用できます。

関連項目

- NAC 設定パラメータの定義 （3255 ページ）
- NAC アイデンティティ パラメータの定義 （3258 ページ）
- Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択し、作業領域で [アイデンティティ（Identities）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）]>[ネットワークアドミッションコントロール（Network Admission Control）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[アイデンティティ（Identities）] タブをクリックします。

[NAC Identities] タブが表示されます。このタブのフィールドの説明については、表 899 : [Network Admission Control] の [Identities] タブ （3266 ページ）を参照してください。

ステップ 2 1 つ以上のアイデンティティ アクションを定義します。

a) [NACアイデンティティ（NAC Identities）] タブの下半分のテーブルからアイデンティティアクションを選択し、[追加（Add）] をクリックします。[NAC Identity Action] ダイアログボックスが表示されます。

b) アイデンティティ アクションを定義します。使用可能なフィールドの説明については、表 901 : [NAC Identity Action] ダイアログボックス （3268 ページ）を参照してください。

c) [OK] をクリックして定義を保存し、ダイアログボックスを閉じます。[NAC Identities] タブの [Identity Actions] テーブルに、アクションが表示されます。

d) （任意）2.a （3259ページ）～2.c （3259ページ）を繰り返して、必要に応じて追加のアイデンティティアクションを定義します。

ステップ 3 アイデンティティ プロファイルを定義します。

a) [NACアイデンティティ（NAC Identities）] タブの上半分のテーブルからアイデンティティ プロファイルを選択し、[追加（Add）] をクリックします。[NAC Identity Profile] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 900 : [NAC Identity Profile] ダイアログボックス （3267 ページ）を参照してください。

b) （ステップ2（3259ページ）で定義されているように）アイデンティティアクションの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。
c) プロファイルを適用するデバイスを識別するプロファイル定義を選択および定義します。
d) [OK] をクリックして定義を保存し、ダイアログボックスを閉じます。[NAC Identities] タブの [Identity Profiles] テーブルに、プロファイルが表示されます。
e) （任意）3.a（3259ページ）～3.d（3260ページ）を繰り返して、必要に応じて追加のアイデンティティプロファイルを定義します。

[Network Admission Control Policy] ページ

Network Admission Control（NAC; ネットワーク アドミッション コントロール）ポリシーを使用すると、エンドポイントがネットワークに接続しようとするときに、Network Access Devices（NAD; ネットワーク アクセス デバイス）として機能する Cisco IOS ルータにアクセス権限を適用できます。アクセス決定は、エンドポイントデバイスにより提供された情報（現在のアンチウイルス状態など）に基づいて行われるため、セキュアでないノードからネットワークが感染することを回避できます。

[Network Admission Control] ポリシー ページの次のタブから Cisco IOS ルータ上の NAC ポリシーを設定できます。

- [Network Admission Control] ページ - [Setup] タブ （3261 ページ）
- [Network Admission Control] ページ - [Interfaces] タブ （3263 ページ）
- [Network Admission Control] ページ - [Identities] タブ （3265 ページ）

詳細については、Cisco IOS ルータでのネットワーク アドミッション コントロール （3252 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [アイデンティティ（Identity）] > [ネットワークアドミッションコントロール（Network Admission Control）] を選択します。[ネットワークアドミッションコントロール（Network Admission Control）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存ポリシーを選択します。

[Network Admission Control] ページ - [Setup] タブ

[Network Admission Control] の [Setup] タブを使用して、NAC プロセス中に認証に使用される Cisco Secure Access Control Server を選択します。また、NAD と、ネットワークへのアクセスを試行するクライアントとの間の通信に対して EAP over UDP 設定を定義します。

ナビゲーション パス

[Network Admission Control Policy] ページ （3260 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- NAC 設定パラメータの定義 （3255 ページ）
- [Network Admission Control] ページ - [Interfaces] タブ （3263 ページ）
- [Network Admission Control] ページ - [Identities] タブ （3265 ページ）
- AAA サーバおよびサーバ グループ オブジェクトについて （323 ページ）

フィールド リファレンス

表 *896 : [Network Admission Control] の [Setup] タブ*

要素	説明
AAA サーバーグループ	NAC 認証に使用される AAA サーバ グループ。RADIUS プロトコルを実行している Cisco Secure Access Control Server（ACS）デバイスを構成するサーバ グループを選択する必要があります。AAA サーバー グループ オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） 選択したグループの各 AAA サーバは、ルータ上に存在するインターフェイスと通信するように設定する必要があります。そうしないと、検証が失敗します。
Backup AAA Server Group 1	メイン グループの AAA サーバが停止した場合のバックアップ AAA サーバ グループ。
Backup AAA Server Group 2	メイン グループの AAA サーバおよび最初のバックアップ グループが停止した場合のセカンダリ バックアップ AAA サーバ グループ。
EAP over UDP (EoU) settings	

要素	説明
Allow IP Station ID	選択すると、ACS に送信される RADIUS 要求の calling-station-id フィールドに IP アドレスを含めることができます。 選択しない場合、ACS に送信される RADIUS 要求の calling-station-id フィールドに IP アドレスは含められません。
Allow Clientless	選択すると、Cisco Trust Agent（CTA）がインストールされていないデバイスを、ACS で設定されているユーザ名とパスワードを使用して認証できます。 このチェックボックスをオンにした場合は、提供されたフィールドにユーザ名とパスワードを（確認も含めて）入力します。 選択しない場合、NAC では、トラフィックがインターセプト ACL に一致すると、CTA のないデバイスによるネットワークへのアクセスが禁止されます（[NAC Interface Configuration] ダイアログボックス （3264 ページ）を参照）。 （注） この機能は、Cisco IOS ソフトウェア Release 12.4(6)T 以降を実行しているルータではサポートされません。
Max Retry	接続デバイスと EAP over UDP セッションを開始するときに、このルータ上のすべての NAC インターフェイスで行う最大試行回数。 有効値の範囲は 1 ～ 3 です。デフォルトは 3 です。 （注） 必要に応じて、特定のインターフェイス上のこのグローバル値を上書きできます。 [Network Admission Control] ページ - [Interfaces] タブ （3263 ページ）を参照してください。
レート制限	ルータが同時に処理できる EAP over UDP ポスチャ検証の数。1 つ以上のデバイスを削除しないかぎり、追加のデバイスを検証できません。 有効値の範囲は 1 ～ 200 です。デフォルトは 20 です。この値を 0 に設定すると、レート制限がオフになります。
[ポート（Port）]	EAP over UDP セッションで使用する UDP ポート。 有効値の範囲は 1 ～ 65535 です。デフォルトは 21862 です。 （注） NAC が機能するためには、このルータ上のデフォルト ACL が、EAP over UDP トラフィックに対してここで指定したポートを介する UDP トラフィックを許可している必要があります。詳細については、アクセス ルールについて （913 ページ）を参照してください。

要素	説明
Enable Logging	選択すると、このルータ上の EAP over UDP イベントがデバイスに記録されます。 選択しない場合、EAP over UDP ロギングがディセーブルになります。これがデフォルトです。

[Network Admission Control] ページ - [Interfaces] タブ

[Network Admission Control] の [Interfaces] タブを使用して、NAC を実行するルータ インターフェイスを選択および設定します。このとき、インターセプト ACL および選択済み EoU インターフェイス パラメータを設定します。NAC ポリシーが機能するためには、少なくとも 1 つのインターフェイス定義が含まれている必要があります。

ナビゲーション パス

[Network Admission Control Policy] ページ （3260 ページ）に移動し、[インターフェイス（Interfaces）] タブをクリックします。

関連項目

- NAC インターフェイス パラメータの定義 （3257 ページ）
- NAC インターフェイス パラメータの定義 （3257 ページ）
- [Network Admission Control] ページ - [Identities] タブ （3265 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 897 : [Network Admission Control] の [Interfaces] タブ

要素	説明
インターフェイス	NAC を実行するインターフェイスの名前。
Intercept ACL	インターセプト ACL の名前。インターフェイスによるポスチャ検証チェックをトリガーする着信トラフィックは、インターセプト ACL によって決まります。
EoU Max Retries	このインターフェイスが接続デバイスとの EoU セッションを開始するときに実行する最大再試行回数。
Revalidate	インターフェイスがその EoU セッションを再検証して、それらがまだアクティブであることを確認するかどうかを示します。

要素	説明
[追加（Add）] ボタン	[NAC Interface Configuration] ダイアログボックス （3264 ページ）が開きます。ここから、NAC インターフェイスを定義できます。
[編集（Edit）] ボタン	[NAC Interface Configuration] ダイアログボックス （3264 ページ）が開きます。ここから、選択した NAC インターフェイスを編集できます。
[削除（Delete）] ボタン	選択した NAC インターフェイスをテーブルから削除します。

[NAC Interface Configuration] ダイアログボックス

[NAC Interface Configuration] ダイアログボックスを使用して、NAC を実行するルータ インターフェイスを追加または編集します。

ナビゲーション パス

[Network Admission Control] ページ - [Interfaces] タブ （3263 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- NAC インターフェイス パラメータの定義 （3257 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトの作成 （383 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）

フィールド リファレンス

表 898 : [NAC Interface Configuration] ダイアログボックス

要素	説明
インターフェイス（Interface）	接続デバイス上で NAC を実行するインターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Intercept ACL	ポスチャ検証を必要とするトラフィックを定義するACL。ACLオブジェクトの名前を入力します。または、[追加（Add）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） 認証プロキシがNACと同じインターフェイスで設定されている場合、両方のポリシーで同じインターセプトACLを使用する必要があります。このようにしないと、展開が失敗する場合があります。認証プロキシの詳細については、IOSデバイスのAAAルールの設定 （877ページ）を参照してください。
EAP over UDP Max Retries	ルータが接続デバイスとのEoUセッションの開始を試行する最大回数。有効値の範囲は1 ～ 3です。デフォルトは3です。 （注） サブインターフェイスではデフォルト値だけがサポートされます。
Enable EoU Session Revalidation	選択すると、ルータは必要に応じてそのEoUセッションを再検証します。これがデフォルトです。 選択しない場合、EoUセッション再検証は実行されません。 （注） サブインターフェイスではデフォルト値だけがサポートされます。

[Network Admission Control] ページ - [Identities] タブ

[Network Admission Control] の [Identities] タブを使用して、NACアイデンティティ プロファイルとアイデンティティ アクションを表示、作成、編集および削除します。アイデンティティ プロファイルは、選択済みのデバイス（IPアドレス、MACアドレス、またはデバイス タイプで識別される）から受信されたトラフィックに対して実行する特定のアクションを定義します。このように、アイデンティティ プロファイルを持つデバイスはNACによって処理されます。ACSと照合してポスチャ検証を実行する必要はありません。

ナビゲーション パス

[Network Admission Control Policy] ページ （3260ページ）に移動し、[インターフェイス（Interfaces）] タブをクリックします。

関連項目

- NACインターフェイス パラメータの定義 （3257ページ）
- [Network Admission Control] ページ - [Setup] タブ （3261ページ）
- [Network Admission Control] ページ - [Identities] タブ （3265ページ）
- テーブル カラムおよびカラム見出しの機能 （66ページ）

- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 899 : [Network Admission Control] の [Identities] タブ

要素	説明
[Identity Profiles] テーブル	
Profile Definition	アイデンティティ プロファイルのタイプ。デバイス IP アドレス、MAC アドレス、またはデバイス タイプ（IP Phone）です。
アクション名	このNACアイデンティティ プロファイルに割り当てられる（[Identity Actions] テーブルで定義されている）アクションの名前。
[追加（Add）] ボタン	[NAC Identity Profile] ダイアログボックス （3266 ページ）を開きます。ここから、アイデンティティ プロファイルを定義できます。
[編集（Edit）] ボタン	[NAC Identity Profile] ダイアログボックス （3266 ページ）が開きます。ここから、選択したアイデンティティ プロファイルを編集できます。
[削除（Delete）] ボタン	選択したアイデンティティ プロファイルをテーブルから削除します。
[Identity Actions] テーブル	
アクション名	アイデンティティ アクションの名前。
ACL	このアイデンティティ アクションが割り当てられたプロファイルに適用される ACL。
リダイレクト URL	このアイデンティティ アクションが割り当てられたデバイスからのトラフィックがリダイレクトされる宛先の URL。
[追加（Add）] ボタン	NAC アイデンティティ アクションを定義するための [NAC Identity Action] ダイアログボックス （3267 ページ）を開きます。
[編集（Edit）] ボタン	選択した NAC アイデンティティ アクションを編集するための [NAC Identity Action] ダイアログボックス （3267 ページ）を開きます。
[削除（Delete）] ボタン	選択したアイデンティティ アクションをテーブルから削除します。

[NAC Identity Profile] ダイアログボックス

[NAC Identity Profile] ダイアログボックスを使用して、特定のアイデンティティに一致するデバイスに割り当てられた NAC プロファイルを追加または編集します。アイデンティティ プロファイルでは、IP アドレス、MAC アドレス、またはデバイス タイプ（IP Phone の場合）に基づいて、特定のデバイスから送信されたすべてのトラフィックに適用される NAC アクションを定義します。

ナビゲーション パス

[Network Admission Control] ページ - [Identities] タブ （3265 ページ）に移動してから、[アイデンティティプロファイル（Identity Profiles）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [NAC Identity Action] ダイアログボックス （3267 ページ）
- NAC アイデンティティ パラメータの定義 （3258 ページ）

フィールド リファレンス

表 *900 : [NAC Identity Profile]* ダイアログボックス

要素	説明
アクション名	プロファイルに割り当てるアクションの名前。アクションの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。アクションの作成の詳細については、[NAC Identity Action] ダイアログボックス （3267 ページ）を参照してください。
Profile Definition	このプロファイルを割り当てるデバイス。 • [IP Address]：このプロファイルを割り当てるデバイスの IP アドレス。複数のプロファイルで同じ IP アドレスを使用することはできません。 • [MAC Address]：このプロファイルを割り当てるデバイスの MAC アドレス。 • [Cisco IP Phone]：Cisco IP Phone に NAC アイデンティティ プロファイルを定義する場合に使用します。

[NAC Identity Action] ダイアログボックス

[NAC Identity Action] ダイアログボックスを使用して、NAC アイデンティティ プロファイルに割り当てるアクションを追加または編集します。

ナビゲーション パス

[Network Admission Control] ページ - [Interfaces] タブ （3263 ページ）に移動してから、[アイデンティティアクション（Identity Action）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

- [NAC Identity Profile] ダイアログボックス （3266 ページ）

- NAC アイデンティティ パラメータの定義 （3258 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）

フィールド リファレンス

表 *901 : [NAC Identity Action]* ダイアログボックス

要素	説明
名前	アイデンティティ アクションを説明する名前。NAC アイデンティティ プロファイルに割り当てるアクションを選択するときは、この名前を使用します。 [NAC Identity Action] ダイアログボックス （3267 ページ）を参照してください。
アクセス コントロール リスト	このアクションを含むプロファイルが割り当てられたデバイスから受信したトラフィックを処理する方法を定義する ACL。ACL オブジェクトの名前を入力します。または、[追加（Add）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） インターセプト ACL に使用されている ACL オブジェクトと同じ ACL オブジェクトは選択できません。 [NAC Interface Configuration] ダイアログボックス （3264 ページ）を参照してください。
リダイレクト URL	デバイスからのトラフィックをリダイレクトする宛先の修復サーバのアドレス。通常、リダイレクト URL の形式は、**http://URL** または **https://URL** です。

第 65 章

ロギング ポリシーの設定

Security Manager には、Cisco IOS ルータでロギングを設定するための次のポリシーが用意されています。

[Syslog Logging Setup]：syslog ロギング機能をイネーブルにし、基本的なロギング パラメータを定義します。詳細については、「Syslog ロギングの設定パラメータの定義」を参照してください。

[Syslog Servers]：syslog メッセージの送信先となるリモート サーバを定義します。詳細については、「Syslog サーバの定義」を参照してください。

[NetFlow]：パラメータおよびインターフェイスを指定して、NetFlow ロギングをイネーブルにします。「NetFlow パラメータの定義」を参照してください。

- Cisco IOS ルータにおけるロギング （3269 ページ）
- Syslog ロギングの設定ポリシーのページ （3278 ページ）
- Syslog サーバ ポリシーのページ （3282 ページ）
- NetFlow ポリシー ページ （3284 ページ）

Cisco IOS ルータにおけるロギング

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Security Manager には、Cisco IOS ルータでロギングを設定するための次のポリシーが用意されています。

- [Syslog Logging Setup]：syslog ロギング機能をイネーブルにし、基本的なロギング パラメータを定義します。詳細については、 Syslog ロギングの設定パラメータの定義 （3270 ページ）を参照してください。
- [Syslog Servers]：syslog メッセージの送信先となるリモート サーバを定義します。詳細については、 Syslog サーバの定義 （3272 ページ）を参照してください。

- [NetFlow]：パラメータおよびインターフェイスを指定して、NetFlow ロギングをイネーブルにします。詳細については、NetFlow パラメータの定義 （3275 ページ）を参照してください。

（注） ロギングがイネーブルになっているすべてのルータにネットワーク タイム プロトコル（NTP）ポリシーを設定することを強く推奨します。NTP 同期によって、syslog メッセージの正確なタイムスタンプが提供されます。正確なタイムスタンプは、複数のデバイス上のログを比較する場合に不可欠です。

Syslog ロギングの設定パラメータの定義

この手順では、ルータ上で syslog ロギングをイネーブルにし、syslog サーバに送信されるメッセージを定義する方法について説明します。また、オプションで次の項目を定義できます。

- このデバイスから送信されるすべての syslog メッセージの送信元インターフェイス。
- ローカル バッファに保存されるメッセージ。
- 各メッセージに追加される送信元識別子。
- 送信できるメッセージ数に対するレート制限。

（注） ルータから syslog サーバに syslog メッセージを送信するには、syslog サーバの IP アドレスも定義する必要があります。詳細については、Syslog サーバの定義 （3272 ページ）を参照してください。

関連項目

- Syslog サーバの定義 （3272 ページ）
- ログ メッセージの重大度について （3273 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）

ステップ 1 次のいずれかを実行して、ルータの [Syslogロギングのセットアップ（Syslog Logging Setup）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogロギング設定（Syslog Logging Setup）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogロギングのセットアップ（Syslog Logging Setup）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Syslog Logging Setup] ページが表示されます。このページのフィールドの説明については、表 903 : [Syslog Logging Setup] ページ （3279 ページ）を参照してください。

ステップ 2 [ロギングを有効化（Enable Logging）] を選択して、syslog ロギング機能を有効にします。このオプションが選択されていない場合、ログ メッセージは作成されません。

ヒント デバイスのデフォルトロギング設定を使用するか、またはデフォルト設定を復元する場合は、単に [ロギングを有効化（Enable Logging）] を選択し、その他のすべてのフィールドが空白であることを確認してから、[保存（Save）] をクリックします。デフォルト設定は、デバイスごとに異なります。詳細については、ご使用のルータのマニュアルを参照してください。

ステップ 3 （任意）[ソースインターフェイス（Source Interface）] フィールドに、インターフェイスまたはインターフェイスロールの名前を入力します。このインターフェイスまたはインターフェイスロールのアドレスが、syslog サーバに送信されるすべてのログメッセージの送信元インターフェイスとして使用されます。あるいは、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、または新しいインターフェイスロールを作成します。送信元インターフェイスには IP アドレスが必要です。

このオプションは、syslog サーバが（たとえばファイアウォールが原因で）接続の発生元のアドレスに到達できない場合に役立ちます。このフィールドに値を入力しない場合は、発信インターフェイスのアドレスが使用されます。

ステップ 4 （任意）syslog サーバにログ メッセージを送信するには、次の手順を実行します。

a) [トラップの有効化（Enable Trap）] を選択します。このオプションは、デフォルトで選択されます。
b) [Trap Level] リストから値を選択します。この重大度以上の（つまり、重大度番号が同じまたはより小さい）すべてのメッセージが、syslog サーバに送信されます。これよりも重大度が低いメッセージは無視されます。重大度の詳細については、表 860 : [User Account] ダイアログボックス （3135 ページ）を参照してください。

ステップ 5 （任意）ログ メッセージをルータ上のバッファにローカルに保存するには、次の手順を実行します。

a) [バッファの有効化（Enable Buffer）] を選択します。このオプションは、デフォルトで選択されます。
b) バッファ サイズ（バイト単位）を入力します。
c) バッファに保存されるメッセージの最も低い重大度を選択します。その重大度以上のすべてのメッセージが、バッファに保存されます。
d) [XML形式を使用（Use XML Format）] を選択して、メッセージを XML 形式で保存します（同じポリシーで通常のバッファと XML バッファの両方を設定できます）。このオプションを選択する場合は、XML バッファのサイズをバイト単位で入力します。

（注） バッファを大きくしすぎて、ルータで他のタスク用のメモリが不足することがないようにしてください。メモリが不足すると、展開が失敗する場合があります。

ステップ 6 （任意）出力メッセージのフラッドを防止するために、レート制限を定義します。

a) [レート制限の有効化（Enable Rate Limit）] を選択します。このオプションは、デフォルトで選択されます。
b) 1 秒ごとに送信できるメッセージの最大数を入力します。
c) レート制限から除外するシビラティ（重大度）を選択します。たとえば、[2]（クリティカル）を選択すると、重大度が 0 ～ 2 であるすべての syslog メッセージが、定義されているレート制限に関係なく syslog サーバに送信されます。

d) コンソール メッセージを除く（および上で特に除外しているシビラティ（重大度）を除く）すべてのsyslogメッセージにレート制限を適用するには、[すべてのメッセージ（All Messages）] を選択します。
e) コンソールメッセージにだけレート制限を適用するには、[コンソールメッセージ（Console Messages）] を選択します。

（注） レート制限をイネーブルにし、かつ、オプションを指定しないと、デフォルト設定（1秒ごとに 10 メッセージ、コンソール メッセージにだけ適用される）が適用されます。

ステップ 7 （任意）送信元識別子を各 syslog メッセージの先頭に追加するには、次の手順を実行します。

a) 送信する送信元 ID のタイプ（ルータの IP アドレス、ルータのホスト名、または指定するテキスト文字列）を選択します。
b) [String] を選択した場合は、表示されるフィールドに任意のテキストを入力します。スペースを使用できます。

送信元識別子は、複数のデバイスの出力を単一の syslog サーバに送信する場合に、syslog メッセージの送信元の識別に役立ちます。

（注） 送信元識別子は、バッファ、コンソール、モニタなど、ローカルの宛先に送信されるメッセージには追加されません。

Syslog サーバの定義

この手順では、ルータがsyslogメッセージを送信するサーバを定義する方法について説明します。syslog サーバを定義する場合、サーバが受信したロギング メッセージをプレーン テキストとして転送するか、XML 形式で転送するかを選択できます。

複数の syslog サーバを定義した場合、ロギング メッセージはこれらすべてのサーバに送信されます。

はじめる前に

- syslog ロギングをイネーブルにし、[Syslog Logging Setup] ページで基本的なロギング パラメータを定義します。詳細については、Syslog ロギングの設定パラメータの定義 （3270 ページ）を参照してください。

関連項目

- Syslog ロギングの設定パラメータの定義 （3270 ページ）
- ログ メッセージの重大度について （3273 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）

ステップ 1 次のいずれかの手順を実行して、ルータの [Syslogサーバー（Syslog Servers）] ページにアクセスします。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。

- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Syslog Servers] ページが表示されます。このページのフィールドの説明については、表 904 : [Syslog Servers] ページ （3282 ページ）を参照してください。

ステップ 2 ルータから syslog メッセージを受信するサーバーを定義するには、テーブルの下にある [追加（Add）] ボタンをクリックして、[Syslogサーバー（Syslog Server）] ダイアログボックスを開きます。このダイアログボックスの詳細については、表 905 : [Syslog Server] ダイアログボックス （3283 ページ）を参照してください。

ステップ 3 [IPアドレス（IP Address）] フィールドで、目的の syslog サーバーのアドレスを入力するか、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 4 （任意）[XML形式でメッセージを転送（Forward Messages in XML Format）] を選択して、受信した syslog メッセージをプレーンテキストではなく XML 形式で転送します。

ステップ 5 [OK] をクリックして定義を保存し、ダイアログボックスを閉じます。定義した syslog サーバーが、テーブルに表示されます。

（注） syslog サーバーを編集するには、テーブルからサーバーを選択して [編集（Edit）] をクリックします。syslog サーバーを削除するには、そのサーバーを選択し、[削除（Delete）] をクリックします。

ログ メッセージの重大度について

Cisco IOS ルータ上の syslog メッセージは、8 つの重大度に分類されます。各重大度は、番号によって識別され、対応する名前が付けられています。次のテーブルに示すように、この番号が低いほど、重大度は高くなります。

表 *902 : Syslog* メッセージの重大度

レベル番号	重大度の名前	説明
[0]	emergency	システムが使用不可
1	アラート	即時処理が必要
2	critical	クリティカルな状態
3	errors	エラー状態
4	警告	警告状態
5	通知	正常だが注意を要する状態

レベル番号	重大度の名前	説明
6	情報	情報メッセージだけ
7	デバッグ	デバッグ メッセージ

関連項目

- Syslog ロギングの設定パラメータの定義 （3270 ページ）
- Syslog サーバの定義 （3272 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）

Cisco IOS ルータにおける NetFlow

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IP トラフィックの特性を明確化し、IP トラフィックが、どのような方法で、どこを通過するかを把握することが、ネットワークの可用性、パフォーマンス、およびトラブルシューティングにとって重要となります。IP トラフィック フローをモニタリングすることで、正確な容量計画を容易に策定でき、ネットワーク リソースが組織の目標をサポートするために適切に使用されていることを確認できます。

NetFlow は、IOS デバイスで使用できるロギング機能であり、IP トラフィック フロー情報の記録、キャッシュ、および送信をインターフェイス単位で実行します。NetFlow の基本的な出力は、フローレコードです。フローレコードでは、「フロー」が、所定の送信元と宛先（両方とも、ネットワークレイヤの IP アドレスおよびトランスポートレイヤの送信元ポート番号と宛先ポート番号で定義されています）の間の、パケットの単方向ストリームとして定義されています。

IOS デバイス上で、NetFlow は 2 つの主要コンポーネント（IP フローデータを格納する NetFlow キャッシュ、およびデータ レポートのために NetFlow レコードを収集サーバに送信する NetFlow エクスポート メカニズム）で構成されています。このため、NetFlow は、イネーブルである場合、着信トラフィックと発信トラフィックのフローに関する統計情報を記録およびキャッシュし、これらのレコードをデバイスから NetFlow Collector にユーザ データグラム プロトコル（UDP）データグラム形式で定期的に送信します。

NetFlow の成熟に伴い、エクスポート パケットまたはフロー レコード用の複数の異なる形式が作成されました。これらの形式は、一般に NetFlow バージョンと呼ばれています。これらのバージョンは詳細に文書化されています。バージョンには 1、5、7、および 9 が存在します。最も一般的に使用される形式は NetFlow バージョン 5 ですが、バージョン 9 が最新の形式であり、拡張性、セキュリティ、トラフィック分析、およびマルチキャストの点で優れています。

Security Manager では、現在、IOS デバイスでの Traditional NetFlow の使用がサポートされています。Traditional NetFlow では、固定フロー レコードを提供します（バージョン 9 の場合も同様）。つまり、デバイスでは、フローを生成するとき、フラグと定義済みレコードの特定の組み合わせを使用します。デバイス設定では、エクスポートの宛先、エクスポートインターフェイス、およびバージョン固有の特定の送信オプションを定義します。

トラフィック フローおよび NetFlow の詳細

ルータまたはスイッチを経由する各パケットに対して、IP パケット属性セットが検査されます。これらの属性は、IP パケット ID、つまり「フィンガープリント」であり、パケットが一意であるか、または他のパケットと関連するかを定義します。

送信元/宛先IPアドレス、送信元/宛先ポート、プロトコルインターフェイス、およびサービスクラスが同一であるすべてのパケットは、1 つのフローにグループ化され、これらのパケットおよびバイトが集計されます。このフロー決定の方式（または「フィンガープリント」）では、大量のネットワーク情報を NetFlow キャッシュと呼ばれる NetFlow 情報のデータベースに圧縮できるため、スケーラビリティが高くなります。

一般的に、NetFlowキャッシュにはフローが常に入れられ、ルータまたはスイッチのソフトウェアは、終了したフローや期限切れのフローをキャッシュで検索します。これらのフローはNetFlow Collectorにエクスポートされます（SNMP ポーリングとは異なり、NetFlow エクスポートは、情報を NetFlow コレクタに定期的に送信します）。NetFlow Collector には、エクスポートされたフローを収集および整理して、トラフィックとセキュリティの分析に使用されるリアルタイムレポートまたは履歴レポートを生成するジョブがあります。

NetFlow の概要

NetFlow の処理概要は次のとおりです。

- NetFlowは、IP トラフィック フローをキャプチャするために、ルータまたはスイッチ上で設定されます。
- フロー レコードは、ローカル NetFlow キャッシュに格納されます。
- 定期的に、約 30 ～ 50 のフロー レコードがバンドルされ、NetFlow Collector サーバにエクスポートされます。
- NetFlow Collector ソフトウェアによって、NetFlow データからレポートが作成されます。

関連項目

- Cisco IOS ルータにおけるロギング （3269 ページ）
- NetFlow パラメータの定義 （3275 ページ）
- NetFlow ポリシー ページ （3284 ページ）

NetFlow パラメータの定義

この手順では、ルータ上で NetFlow ロギングをイネーブルにする方法について説明します。

関連項目

- Cisco IOS ルータにおける NetFlow （3274 ページ）
- NetFlow ポリシー ページ （3284 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）

ステップ 1 ルータの [NetFlow] ページにアクセスするには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [NetFlow] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [NetFlow] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ルータの [NetFlow] ページが表示されます。このページのフィールドの詳細な説明については、 NetFlow ポリシー ページ （3284 ページ） を参照してください。

ステップ 2 [NetFlow] ページの [セットアップ（Setup）] タブで、ルータのグローバル NetFlow パラメータを指定します。

- [プライマリ宛先（Primary Destination）]：リストから [IPアドレス（IP Address）] または [ホスト名（Hostname）] を選択して NetFlow 収集を有効にし、プライマリ NetFlow Collector の定義方法を指定します。ブランクのエントリを選択して、このオプションをディセーブルにできます。
  - [IPアドレス（IP Address）]：プライマリ NetFlow Collection Engine をホスティングするデバイスの IP アドレスを入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。
  - [ホスト名（Hostname）]：プライマリ NetFlow Collection Engine をホスティングするデバイスの完全修飾ドメイン名を入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。
- [重複宛先（Redundant Destination）]：リストから [IPアドレス（IP Address）] または [ホスト名（Hostname）] を選択して、バックアップ NetFlow Collector の定義方法を指定します。ブランクのエントリを選択して、このオプションをディセーブルにできます。
  - [IPアドレス（IP Address）]：セカンダリ NetFlow Collection Engine をホスティングするデバイスの IP アドレスを入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。
  - [ホスト名（Hostname）]：セカンダリ NetFlow Collection Engine をホスティングするデバイスの完全修飾ドメイン名を入力し、そのフローコレクタがモニターする **UDP ポート**の番号を入力します（ポート番号の範囲は 1 ～ 65535 です）。

（注） プライマリ宛先および重複宛先を定義した場合、フロー データは両方に送信されます。

- [送信元インタフェース（Source Interface）]：ルータインターフェイスを指定します。このインターフェイスを経由してフローデータがコレクタの宛先に送信されます。
- [バージョン（Version）]：ドロップダウンリストから目的の NetFlow バージョン番号を選択して、フローデータに使用するレコード形式を定義します。ブランクのエントリを選択して、このオプションをディセーブルにできます。
  - [1]：元のレコード形式。追加のパラメータは必要ありません。
  - [5]：ボーダー ゲートウェイ プロトコル（BGP）自律システム（AS）情報およびフローシーケンス番号など、最も広く採用されている形式。

ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。

[BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGP ネクストホップ情報をフローキャッシュに含めます。（バージョン 5 では、この情報はキャッシュに表示されますが、エクスポートはされません）。

- • [9]：テンプレートベースの最新バージョンであり、まだ完全にはサポートされていません。

ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。

[BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGP ネクストホップ情報をフローレコードに含めます。

（注） AS 情報の収集はリソースを大量に消費します。origin-as の場合は特に消費量が多くなります。ピアリングの配置をモニタする必要がない場合は、AS収集をディセーブルにすると、パフォーマンスが向上する場合があります。

ステップ 3 [インタフェース（Interfaces）] タブで、トラフィックフローをレポートするインターフェイスを定義します。

- インターフェイスを追加するには、[Add Row] ボタンをクリックして [Add NetFlow Interface Settings] ダイアログボックスを開きます。このダイアログボックスについては、NetFlow インターフェイス設定の追加および編集 （3287 ページ）で説明しています。
- 既存のインターフェイスを編集するには、[Interfaces] テーブルで目的のエントリを選択し、次に [Edit Row] ボタンをクリックして [Edit NetFlow Interface Settings] ダイアログボックス（NetFlow インターフェイス設定の追加および編集 （3287 ページ）で説明しています）を開きます。
- 既存のインターフェイスを削除するには、そのエントリを [Interfaces] テーブルで選択してから [Delete Row] ボタンをクリックし、次に、削除されたことを確認します。

（注） NetFlow データ収集は、削除しないで、インターフェイスでディセーブルにできます。詳細については、NetFlowインターフェイス設定の追加および編集 （3287ページ）を参照してください。

Syslog ロギングの設定ポリシーのページ

[Syslog Logging Setup] ページを使用して、syslog ロギングをイネーブルにし、選択した Cisco IOS ルータ上で基本的なロギング パラメータを定義します。

詳細については、Syslog ロギングの設定パラメータの定義 （3270 ページ）を参照してください。

（注） 各ログ メッセージに対して正確なタイムスタンプを作成するために、ロギングがイネーブルになっているすべてのルータで NTP ポリシーを定義することを強く推奨します。詳細については、[NTP Policy] ページ （3239 ページ）を参照してください。

（注） ロギングの設定ポリシーを割り当てていない場合、デフォルトのロギング設定が展開時にデバイス上で復元されます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogロギング設定（Syslog Logging Setup）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogロギングのセットアップ（Syslog Logging Setup）] を選択します。[Syslogロギングのセットアップ（Syslog Logging Setup）] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるロギング （3269 ページ）
- Syslog サーバ ポリシーのページ （3282 ページ）
- Cisco IOS ルータにおける NTP （3237 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *903 : [Syslog Logging Setup]* ページ

要素	説明
Enable Logging	選択すると、syslog ロギングがデバイス上でイネーブルになります。 選択を解除すると、ロギングがデバイス上でディセーブルになります。これがデフォルトです。 **ヒント** デバイスのデフォルトの syslog ロギング設定を使用するには、[ロギングの有効化（Enable Logging）] チェックボックスをオンにし、次に、追加の値を入力せずに [保存（Save）] をクリックします。
送信元インターフェイス（Source Interface）	syslog サーバに送信される、すべての発信ログ メッセージの送信元アドレス。この設定は、syslog サーバが（たとえばファイアウォールが原因で）ログ メッセージの発生元のアドレスに応答できない場合に必要となることがあります。 このフィールドで値を定義しない場合、発信インターフェイスのアドレスが使用されます。 インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
トラップ	syslog サーバに転送されるログ メッセージを定義します。 • [Enable Trap]：選択すると、ログ メッセージが syslog サーバに送信されます。これがデフォルトです。選択を解除すると、ログ メッセージは送信されません。 • [Trap Level]：記録され、syslog サーバに送信されるメッセージの最も低い重大度。この重大度以上のすべてのメッセージが記録されます。重大度は、名前と番号で識別されます。詳細については、表 902 : Syslog メッセージの重大度 （3273 ページ）を参照してください。 **ヒント** ルータのデフォルトのトラップ設定を復元するには、[トラップの有効化（Enable Trap）] を選択し、次に [トラップレベル（Trap Level）] リストから空白の設定を選択します。

要素	説明
Logging Buffer	ログ メッセージが、デバイス上のバッファにローカルに保存されるかどうかを指定します。 • [Enable Buffer]：選択すると、ログ メッセージはデバイス上のバッファに保存されます。これがデフォルトです。選択を解除すると、ログ バッファはデバイス上で維持されません。 • [Buffer Size]：バッファのサイズ（バイト単位）。有効値の範囲は 4096 ～ 4294967295 バイト（4 KB ～ 4 GB）です。デフォルトのサイズは、プラットフォームによって異なります。バッファを大きくしすぎて、ルータで他のタスク用のメモリが不足することがないようにしてください。メモリが不足すると、展開が失敗する場合があります。 （注） 一部のデバイスでは最大バッファ サイズがより小さいことがあります。 • [Severity Level]：バッファに保存されるメッセージの最も低い重大度。この重大度以上のすべてのメッセージが保存されます。ほとんどの Cisco IOS ルータにおいて、デフォルトの重大度は 7（[debugging]）です。重大度は、名前と番号で識別されます。詳細については、表 902 : Syslog メッセージの重大度 （3273 ページ）を参照してください。 • [Use XML Format]：選択すると、ログ メッセージが XML 形式でバッファに保存されます（同じポリシーで通常のバッファと XML バッファの両方を設定できます）。選択を解除すると、XML バッファはデバイス上で維持されません。 • [Buffer Size]：XML バッファのサイズ（バイト単位）。有効値の範囲は 4096 ～ 4294967295 バイト（4 KB ～ 4 GB）です。 （注） 一部のデバイスでは最大バッファ サイズがより小さいことがあります。 ヒント ルータのデフォルトのバッファ設定を復元するには、[トラップの有効化（Enable Trap）] を選択し、バッファサイズ設定を消去し、次に [セキュリティ レベル（Security Level）] リストから空白の設定を選択します。

要素	説明
レート制限	syslog サーバに送信されるログ メッセージのレートを制限します。 • [Enable Rate Limit]：選択すると、レート制限がイネーブルになります。選択を解除すると、レート制限がディセーブルになります。 • [Messages per Sec.]：1 秒あたりの送信可能な最大ログ メッセージ数。有効な値の範囲は 1 ～ 10000 です。デフォルトは、1 秒あたり 10 メッセージです。 • [除外（Exclude）]：レート制限から除外するメッセージのタイプ。この設定を適用すると、選択した重大度の、および重大度番号がより低い（つまり、より重大な）メッセージがすべて除外されます。デフォルトは 3（[errors]）です。この場合、重大度が 3、2（[critical]）、1（[alerts]）、または 0（[emergencies]）であるすべてのログ メッセージが、レート制限から除外されます。重大度の詳細については、表 902：Syslog メッセージの重大度 （3273 ページ）を参照してください。 • [All Messages]：選択すると、このレート制限が、コンソール メッセージを除くすべてのメッセージに適用されます。 • [Console Messages]：選択すると、このレート制限が、コンソール メッセージだけに適用されます。 **ヒント** ルータのデフォルトのレート制限設定を復元するには、[レート制限の有効化（Enable Rate Limit）] チェックボックスをオンにして、レート制限値設定を消去します。

Origin ID	デバイスからリモート syslog サーバに送信されるすべての syslog メッセージの先頭に追加される、送信元識別子。送信元識別子は、複数のデバイスから単一の syslog サーバに出力を送信する場合に役立ちます。
	• [ID Type]：各 syslog メッセージに追加される送信元識別子のタイプ。次のオプションがあります。
	  • [IP Address]：送信元デバイスの IP アドレス。
	  • [Hostname]：送信元デバイスのホスト名。
	  • [String]：ユーザ定義のテキスト。
	• [Value]：ID タイプとして [String] を選択した場合にだけ適用されます。ユーザ定義文字列のテキストを入力します。スペースは使用できますが、最初の文字には使用できません。
	（注） 送信元識別子は、バッファ、コンソール、モニタなど、ローカルの宛先に送信されるメッセージには追加されません。

Syslog サーバ ポリシーのページ

[Syslog Servers] ページを使用して、ルータからログ メッセージを収集するサーバを作成、編集、および削除します。

詳細については、Syslog ロギングの設定パラメータの定義 （3270 ページ）を参照してください。

（注） このページに定義されている syslog サーバへのロギングをイネーブルにするには、ロギングをイネーブルにし、Syslog ロギングの設定ポリシーのページ （3278 ページ）で基本パラメータを定義する必要があります。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ロギング（Logging）] > [Syslogサーバー（Syslog Servers）] を選択します。[Syslogサーバー（Syslog Servers）] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるロギング （3269 ページ）
- [Syslog Server] ダイアログボックス （3283 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 904 : [Syslog Servers] ページ

要素	説明
IPアドレス	syslog サーバの名前。ネットワーク/ホスト オブジェクト、または IP アドレスとして表されます。
XML	syslog サーバが、ログ メッセージを XML 形式で受信するかどうかを指定します。

要素	説明
[追加（Add）] ボタン	[Syslog Server] ダイアログボックス （3283 ページ）が開きます。ここから、syslog サーバを定義できます。
[編集（Edit）] ボタン	[Syslog Server] ダイアログボックス （3283 ページ）が開きます。ここから、選択した syslog サーバを編集できます。
[削除（Delete）] ボタン	選択した syslog サーバをテーブルから削除します。

[Syslog Server] ダイアログボックス

[Syslog Server] ダイアログボックスを使用して、ルータから syslog メッセージを収集するサーバを定義します。サーバがログ メッセージを XML 形式またはプレーン テキストのどちらで受信するかを定義することもできます。

（注） このページに定義されている syslog サーバへのロギングをイネーブルにするには、ロギングをイネーブルにし、Syslog ロギングの設定ポリシーのページ （3278 ページ）で基本パラメータを定義する必要があります。

ナビゲーション パス

Syslog サーバ ポリシーのページ （3282 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- Syslog サーバの定義 （3272 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

フィールド リファレンス

表 *905 : [Syslog Server]* ダイアログボックス

要素	説明
IPアドレス	syslog サーバの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Forward Messages in XML Format	選択すると、ログ メッセージが XML 形式で syslog サーバに送信されます。 選択を解除すると、ログ メッセージはプレーンテキストとして syslog サーバに送信されます。

NetFlow ポリシー ページ

[NetFlow] ページを使用して、NetFlow 記録をイネーブルにし、選択した Cisco IOS ルータ上でそのパラメータを定義します。

[NetFlow] ページは、2 つのタブ パネル（[Setup] と [Interfaces]）で構成されています。[Setup] タブには、ルータ上の NetFlow 収集のグローバル設定パラメータが表示されます。[Interfaces] タブには、NetFlow データ収集を設定するルータ インターフェイスが表示されます。このタブを使用して、入力アカウンティングと出力アカウンティングをインターフェイスごとにイネーブルおよびディセーブルにできます。

（注） 各ログ メッセージに対して正確なタイムスタンプを作成するために、ロギングがイネーブルになっているすべてのルータで NTP ポリシーを定義することを強く推奨します。詳細については、[NTP Policy] ページ （3239 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [ロギング（Logging）] > [NetFlow]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [ロギング（Logging）] > [NetFlow]** を選択します。共有ポリシーセレクタから既存のポリシーを選択するか、または [NetFlow] を右クリックして新しいポリシーを作成します。

関連項目

- Cisco IOS ルータにおける NetFlow （3274 ページ）
- NetFlow パラメータの定義 （3275 ページ）
- NetFlow インターフェイス設定の追加および編集 （3287 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）
- Cisco IOS ルータにおける NTP （3237 ページ）

フィールド リファレンス

表 *906 : [NetFlow]* ページ

要素	説明
[Setup] タブ	
Primary Destination Redundant Destination	プライマリおよびセカンダリ NetFlow Collector。プライマリ コレクタを選択して、このデバイスでの NetFlow データ収集をイネーブルにする必要があります。これらのいずれかのコレクタへの NetFlow データの送信をディセーブルにするには、ドロップダウン リストから空白のエントリを選択します。 NetFlow Collector の IP アドレスまたはホスト名を使用して NetFlow Collector を指定するかどうかを選択してから、各オプションの次の必須フィールドを設定します。 • [IPアドレス（IP Address）] : プライマリ NetFlow Collection Engine をホスティングしているデバイスの IP アドレスを入力します。また、IP アドレスを指定するネットワーク/ホストオブジェクトを指定するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。 [UDPポート（UDP Port）] フィールドに、フローコレクタがモニターするポート番号を入力します（ポート番号の範囲は 1 ～ 65535）。ポートリスト オブジェクトの番号または名前を入力するか、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成できます。 • [ホスト名（Hostname）] : プライマリ NetFlow Collection Engine をホスティングするデバイスの完全修飾ドメイン名を入力します。IP アドレスを指定するときと同様、UDP ポートを指定する必要もあります。
送信元インターフェイス（Source Interface）	フロー データがコレクタ宛先に送信されるときに経由するルータ インターフェイス。インターフェイスまたはインターフェイスロール名を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。

要素	説明
バージョン	NetFlowのバージョン番号。この番号によって、フローに使用されるレコード形式が定義されます。ブランクのエントリを選択して、このオプションをディセーブルにできます。 • [1]：元のレコード形式。追加のパラメータは必要ありません。 • [5]：ボーダー ゲートウェイ プロトコル（BGP）自律システム（AS）情報およびフローシーケンス番号など、最も広く採用されている形式。 ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。 [BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGPネクストホップ情報をフローキャッシュに含めます。（バージョン5では、この情報はキャッシュに表示されますが、エクスポートはされません）。 • [9]：テンプレートベースの最新バージョンであり、まだ完全にはサポートされていません。 ネットワークに BGP が設定されている場合は、NetFlow レコードに送信元またはピア AS 情報を含めることができます。[ASタイプ（AS Type）] ドロップダウンリストから、[origin-as] または [peer-as] を選択します。ブランクのエントリを選択して、このオプションをディセーブルにできます。 [BGPネクストホップの有効化（Enable BGP Nexthop）] をオンにして、BGPネクストホップ情報をフローレコードに含めます。 （注） AS 情報の収集はリソースを大量に消費します。origin-as の場合は特に消費量が多くなります。ピアリングの配置をモニタする必要がない場合は、AS収集をディセーブルにすると、パフォーマンスが向上する場合があります。
[インターフェイス（Interfaces）] タブ	
インターフェイス	NetFlow 収集が設定されるインターフェイスの名前。
Enable Ingress	[有効（Enabled）] は、このインターフェイスで着信トラフィックのフロー記録が有効になっていることを示します。[無効（Disabled）] は、このインターフェイスでは着信トラフィックが記録されないことを示します。
Enable Egress	[有効（Enabled）] は、このインターフェイスで発信トラフィックのフロー記録が有効になっていることを示します。[無効（Disabled）] は、このインターフェイスでは発信トラフィックが記録されないことを示します。

要素	説明
行を追加（Add Row）	このボタンをクリックして、[Add NetFlow Interface Settings] ダイアログボックスを開きます。NetFlow インターフェイスの追加については、NetFlow インターフェイス設定の追加および編集 （3287 ページ）で説明しています。
Edit Row	このボタンをクリックして、選択したインターフェイスの [Edit NetFlow Interface Settings] ダイアログボックスを開きます。NetFlow インターフェイスの編集については、NetFlow インターフェイス設定の追加および編集（3287 ページ）で説明しています。
Delete Row	選択したインターフェイスを削除するには、このボタンをクリックします。削除の確認が求められます。

NetFlow インターフェイス設定の追加および編集

[Add NetFlow Interface Settings]/[Edit NetFlow Interface Settings] ダイアログボックスを使用して、特定のルータ インターフェイスの NetFlow 入力レポートおよび出力レポートをイネーブルおよびディセーブルにします。

（注） タイトルを除き、これら 2 つのダイアログボックスは同一です。次の情報は、両方に適用されます。

ナビゲーション パス

NetFlow ポリシー ページ （3284 ページ）に移動してから、テーブルの下にある [行の追加（Add Row）] ボタンまたは [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- NetFlow パラメータの定義 （3275 ページ）
- Cisco IOS ルータにおけるロギング （3269 ページ）

フィールド リファレンス

表 907 : [Add NetFlow Interface Settings]/[Edit NetFlow Interface Settings] ダイアログボックス

要素	説明
インターフェイス（Interface）	インターフェイスまたはインターフェイス ロールの名前。名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新たに作成します。

要素	説明
Enable Ingress Accounting	このオプションを選択すると、このインターフェイスに到着するトラフィックの NetFlow レコードが収集されます。 このオプションを選択解除すると、このインターフェイスでの着信トラフィックのデータ収集が停止されます。
Enable Egress Accounting	このオプションを選択すると、このインターフェイスを出るトラフィックの NetFlow レコードが収集されます。 このオプションを選択解除すると、このインターフェイスでの発信トラフィックのデータ収集が停止されます。

第 66 章

Quality of Service の設定

Cisco Security Manager は、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるセキュリティ サービスやその他のプラットフォーム固有サービスの管理と設定をサポートします。

VTP トランスペアレント モードまたは VTP クライアント/サーバ モードで設定された Catalyst スイッチおよび 7600 デバイスを管理できます。Security Manager は、デバイスにおける VLAN データベース管理（VLAN の作成、削除、スイッチ上の VLAN データベース内の VLAN のモニタリングなど）をバイパスすることによって、クライアント/サーバ モードで設定されたスイッチを管理します。

この章は、次の内容で構成されています。

- Cisco IOS ルータにおける Quality of Service （3289 ページ）
- サービス品質ポリシーページ （3312 ページ）

Cisco IOS ルータにおける Quality of Service

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Quality of Service（QoS）とは、選択されたネットワーク トラフィックに優先的にサービスを提供するというネットワークの機能です。さまざまな基本技術（フレーム リレー、ATM、イーサネットおよび 802.1 ネットワーク、SONET、IP ルーテッド ネットワークなど）が使用されます。QoS 機能では、次の点から、ネットワーク サービスの予測可能性が向上します。

- 専用帯域幅のサポート
- 損失特性の改善
- ネットワークの輻輳の回避と管理。
- ネットワーク トラフィックのシェーピング
- ネットワーク全体でのトラフィックの優先順位の設定。

QoS は一般に、サービス プロバイダーへのエントリ ポイントおよび複数の回線が収束する統合ポイントで使用されます。また、QoS は、速度の不一致が発生する場所（WAN と LAN の間の境界など）で役立ちます。これらの場所は、トラフィックの輻輳ポイントとなる場合が多くあるためです。

Security Manager の QoS ポリシーは、Cisco Systems Modular QoS CLI（MQC）に基づきます。MQC によって、Cisco IOS ソフトウェアでサポートされているすべてのプラットフォーム上で QoS 機能の CLI と意味が標準化されます。また、QoS の展開にモジュール式の拡張性の高いフレームワークが提供されます。Security Manager では、主要な QoS 機能を 1 つのダイアログボックスにまとめた MQC 用の使いやすいインターフェイスが提供されており、ルータに出入りする選択されたトラフィックに対して QoS ポリシーを効率的に作成できます。

Security Manager で QoS ポリシーを定義する手順については、QoS ポリシーの定義 （3300 ページ）を参照してください。

関連項目

- uality of Service と CEF （3290 ページ）
- マーキング パラメータについて （3291 ページ）
- キューイング パラメータについて （3293 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）

uality of Service と CEF

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）は、あらゆる種類のネットワークのパフォーマンスとスケーラビリティを最適化する高度なレイヤ 3 IP スイッチング テクノロジーです。Cisco IOS ルータが入力インターフェイスから出力インターフェイスにパケットを転送する最速の方式を定義します。

Security Manager で設定できる特定の QoS 機能（クラスベースのポリシングやクラスベースの重み付けランダム早期検出など）は、CEF を実行するルータだけでサポートされます。Cisco 800 シリーズから Cisco 7200 シリーズのすべてのルータには、これらの QoS 機能のために CEF が必要です。Cisco 7500 シリーズには、distributed CEF（dCEF; 分散 CEF）が必要です。

（注） 完全なリストについては、次の URL にある Cisco.com の『*When is CEF Required for Quality of Service*』を参照してください。
http://www.cisco.com/en/US/tech/tk39/tk824/technologies_tech_note09186a0080094978.shtmlhttp://www.cisco.com/en/US/tech/tk39/tk824/technologies_tech_note09186a0080094978.shtml [英語]

デフォルトでは、CEF はルータの初期設定の一部として有効になっています。ルータで CEF が有効かどうかを確認するには、**show ip cef** コマンドを使用します。CEF インターフェイス設定ポリシーを使用して、CEF を設定できます（Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）を参照）。ただし、ルータで CEF が有効になっていない場合は、CEF をア

クティブにするとルータのパケットストリーミングに重大な影響を与える場合があります。CEF を有効にする前に、ルータのマニュアルを参照してください。

関連項目

- Cisco IOS ルータにおける Quality of Service （3289 ページ）

マッチング パラメータについて

QoS が実行されるトラフィックを識別することによって、対象パケットを分類し、マッチングパラメータを定義します。分類ツールとして、プロトコル タイプ、IP Precedence（IPP）値、Diffserv コード ポイント（DSCP）値、ACL など、さまざまな基準を使用できます。

トラフィック クラスは、一連の一致基準と、この基準を評価する方法で構成されます。たとえば、特定のプロトコルと DSCP 値に基づく一致基準を使用してクラスを定義するとします。次に、パケットがこのクラスと一致するためには、定義した基準のうちの 1 つとだけ一致すればよいと指定します。または、パケットがこのトラフィック クラスと一致するためには、定義した基準すべてと一致する必要があると指定することもできます。

定義したトラフィック クラスのメンバーであるパケットは、ポリシーマップで定義された QoS 指定に従って転送されます。一致基準を満たさないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。

QoS ポリシーでのマッチング パラメータの定義については、 QoS クラスのマッチング パラメータの定義 （3305 ページ）を参照してください。

関連項目

- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

マーキング パラメータについて

マーキング パラメータを使用してパケットを分類できます。この方法では、トラフィック記述子を使用して特定のグループ内のパケットを分類します。これにより、パケットが定義され、ネットワークで QoS 処理を行うためにアクセスできるようになります。トラフィックポリサーとトラフィックシェーパーはどちらもパケット分類を使用して、ソースとネットワーク間で合意された、契約済みサービスレベルを確実に遵守します。また、マーキング パラメータを使用すると、特定の QoS 分類であればデバイスに到着したであろうパケットを取得して、それを再分類できます。ダウンストリームデバイスでは、この新しい分類を使用してパケットを識別し、適切な QoS 機能をパケットに適用します。

Security Manager では、IPv4 パケット用の 2 つのタイプのマーキングが使用されます。1 つは IPP クラスに基づき、1 つは DSCP 値に基づきます。IPP は、各パケットの Type of Service（ToS; タイプ オブ サービス）バイト内の 3 つの最上位ビットに基づきます。つまり、トラフィックを 8 つのクラスに分けることができます。歴史的な理由から、RFC 791 で定義されているよう

に、各優先順位の値は名前に対応しています。表 908 : IP Precedence クラス （3292 ページ）では、番号とそれに対応する名前を、重要度の低いものから順に示しています。

表 *908 : IP Precedence* クラス

クラス	名前（**Name**）
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

（注） クラス 6 および 7 は一般に、ルーティング更新などのネットワーク制御情報用に予約されています。

DSCP は、ToS バイト内の 6 つの最上位ビットに基づき（残りの 2 ビットはフロー制御に使用される）、値の範囲は 0 ～ 63 です。DSCP ビットには IPP ビットが含まれるため、DSCP は IPP と下位互換性があります。

マーキングは一般に、後続のデバイスが分類マークに基づいてサービスを提供できるように、ネットワーク エッジまたは管理ドメインに近いデバイスで使用されます。

QoS ポリシーでのマーキング パラメータの定義については、 QoS クラスのマーキング パラメータの定義 （3307 ページ）を参照してください。

関連項目

- キューイング パラメータについて （3293 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

キューイング パラメータについて

キューイングでは、パケットに割り当てるプライオリティに基づいて、それらのパケットをインターフェイスから送信する順序を決定することによって、Cisco IOS ルータから出ていくトラフィックの輻輳を管理します。キューイングを使用すると、トラフィックに優先順位を付けて、デスクトップ ビデオ会議などの時間が重要なアプリケーションに対応すると同時に、ファイル転送などの時間への依存が少ないアプリケーションのニーズにも対応できます。

トラフィックが少ない時間帯、つまり輻輳がない場合、パケットはインターフェイスに到着するとすぐに送信されます。ただし、発信インターフェイスで伝送の輻輳が発生しているときは、インターフェイスで送信準備が整う前にパケットが到着します。キューイングなどの輻輳管理機能を使用することによって、インターフェイスで蓄積されたパケットは、インターフェイスで送信できるようになるまでキューイングされます。その後、割り当てられたプライオリティや、インターフェイスに対して設定されているキューイング メカニズムに従って、伝送がスケジュールされます。ルータでは、どのパケットがどのキューに配置されるか、および他のキューとの関係でキューにどのようにサービスが提供されるかを制御することによって、パケット伝送の順序が決定されます。

Security Manager では、Class-Based Weighted Fair Queuing（CBWFQ; クラスベース WFQ）と呼ばれるキューイング形式が使用されます。CBWFQ を使用して、トラフィック クラスを一致条件に基づいて定義します。基準と一致するパケットが、このクラスのトラフィックを構成します。クラスごとに 1 つのキューが予約され、そのクラスに属するトラフィックが含まれます。キューには、割り当てられる帯域幅（固定または最小）やキュー制限（キュー内に蓄積できるパケットの最大数）などの特性を割り当てます。

CBWFQ を使用する場合、インターフェイスでのすべての帯域割り当ての合計が、使用可能なインターフェイス帯域幅の合計の 75% を超えることはできません。残りの 25% は、レイヤ 2 オーバーヘッド、ルーティング トラフィック、ベストエフォート トラフィックなど、その他のオーバーヘッド用に使用されます。たとえば、CBWFQ のデフォルト クラスの帯域幅は、残りの 25% から使用されます。

キューイングの詳細については、次の項を参照してください。

- テール ドロップと WRED （3294 ページ）
- 低遅延キューイング （3295 ページ）
- デフォルト クラス キューイング （3295 ページ）

QoS ポリシーでのキューイング パラメータの定義については、QoS クラスのキューイング パラメータの定義 （3308 ページ）を参照してください。

関連項目

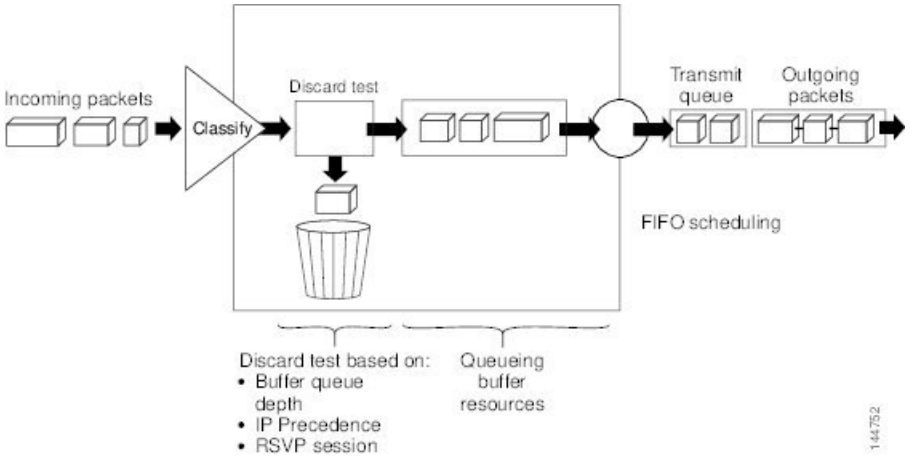
- マーキング パラメータについて （3291 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

テール ドロップと WRED

設定したキュー制限にキューが達したあと、さらにパケットが到着すると、QoS ポリシーの設定方法に応じて、テール ドロップまたはパケット ドロップが有効になります。テール ドロップは、デフォルトの対応であり、すべてのトラフィックを同様に処理し、異なるサービス クラスを区別しません。テール ドロップが有効な場合、輻輳が解消されてキューが一杯ではなくなるまで、キューからパケットがドロップされます。このことにより、グローバルな同期が発生する場合があります。グローバルな同期では、複数の TCP ホストが伝送レートを同時に下げるため、輻輳期間のあとも利用率が低い状態が続きます。

より高度な方法でキューの輻輳を管理するために、シスコでは、重み付けランダム早期検出または WRED と呼ばれるランダム早期検出を提供しています。図 54 : 重み付けランダム早期検出 （3294 ページ）に示されているように、WRED は、出力インターフェイスに輻輳の兆候が表れた際に、選択的にパケットをドロップしてテールドロップの確率を減らします。キューが一杯になるのを待つのではなく、一部のパケットを早期にドロップすることによって、WRED では多数のパケットを一度にドロップすることを回避し、伝送回線を常に十分に使用できるようにします。

図 *54 :* 重み付けランダム早期検出



WRED は、トラフィックの大部分が TCP/IP トラフィックである場合にだけ役立ちます。TCP ホストは輻輳が発生すると伝送レートを下げるためです。その他のプロトコルでは、パケットの送信元が対応しないか、ドロップされたパケットを同じレートで再送信します。このため、パケットをドロップしても輻輳は軽減されません。

（注） WRED では、非 IP トラフィックは precedence 0（最も低い precedence 値）として処理されます。そのため、非 IP トラフィックは IP トラフィックよりもドロップされる可能性が高くなります。

関連項目

- 低遅延キューイング （3295 ページ）

- デフォルト クラス キューイング （3295 ページ）
- キューイング パラメータについて （3293 ページ）

低遅延キューイング

Low-Latency Queuing（LLQ; 低遅延キューイング）機能によって、厳密なプライオリティ キューイングがCBWFQに適用されます。厳密なプライオリティ キューイングでは、音声トラフィックなどの遅延に影響されやすいデータが他のトラフィックよりも優先されます。

（注） さまざまな種類のリアルタイムトラフィックを厳密なプライオリティキューに入力できますが、音声トラフィックのみを指定することを強く推奨します。

LLQは、輻輳時に優先トラフィックに割り当てることが可能な最大帯域幅を定義します。最大を設定することで、非プライオリティ トラフィックの帯域幅が枯渇することがなくなります（つまり、このトラフィックにも帯域幅が与えられます）。デバイスが輻輳していない場合は、プライオリティ クラス トラフィックの割り当て帯域幅を超えることができます。ポリシングによって、プライオリティ キューからパケットがドロップされるため、WRED もテールドロップ（[Queue Limit] フィールドで設定）も使用されません。

LLQが使用されない場合は、CBWFQによって、定義されたクラスに基づいて重み付け均等化キューイングが提供されます。この場合、リアルタイム トラフィックに対して厳密なプライオリティ キューを使用できません。

関連項目

- テール ドロップと WRED （3294 ページ）
- デフォルト クラス キューイング （3295 ページ）
- キューイング パラメータについて （3293 ページ）

デフォルト クラス キューイング

[Fair Queue] フィールドを使用して、デフォルト クラスで使用するために予約する必要があるダイナミック キューの数を定義します。他のクラスの一致基準を満たさないトラフィックには、このクラスが適用されます。デフォルトでは、作成されるキューの数はインターフェイス帯域幅に基づきます。

表 909 : デフォルト クラスのキューのデフォルトの数 （3296 ページ）に、インターフェイスでCBWFQがイネーブルの場合にCBWFQによって使用されるダイナミック キューのデフォルトの数を示します。

表 *909 :* デフォルト クラスのキューのデフォルトの数

帯域幅範囲	ダイナミック キューの数
64 kbps 以下	16
64 kbps より大きく 128 kbps 以下	32
128 kbps より大きく 256 kbps 以下	64
256 kbps より大きく 512 kbps 以下	128
512 kbps より大きい	256

関連項目

- テール ドロップと WRED （3294 ページ）
- デフォルト クラス キューイング （3295 ページ）
- キューイング パラメータについて （3293 ページ）

ポリシング パラメータとシェーピング パラメータについて

Security Manager には、次の 2 種類のトラフィック調整メカニズムがあります。

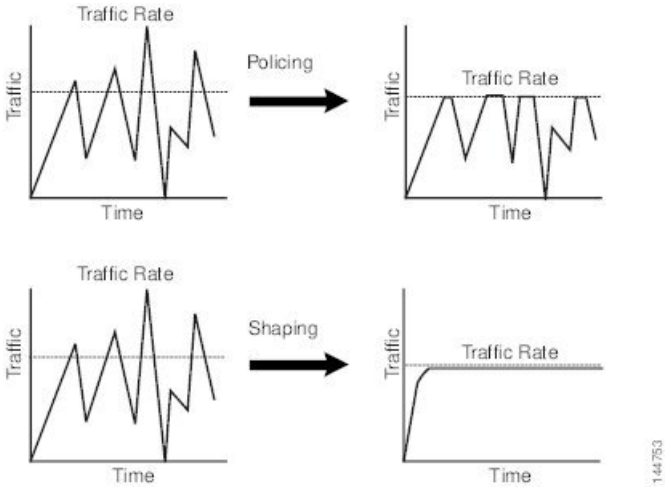
- トラフィックをポリシングするクラスベースのポリシングのレート制限機能。ポリシングによって、設定したレートにトラフィック フローを制限します。ポリシングは、選択したインターフェイスまたはコントロール プレーンで実行できます。 コントロール プレーン ポリシングについて （3299 ページ）を参照してください。
- トラフィックをシェーピングするための Distributed Traffic Shaping（DTS; 分散トラフィック シェーピング）。トラフィック シェーピングを使用すると、リモート ターゲット インターフェイスの速度とトラフィックのフローを一致させ、リモート ターゲット インターフェイスに対して定義されたポリシーにトラフィックを準拠させるために、インターフェイスを出るトラフィック（出力トラフィック）を制御できます。ダウンストリーム要件に合うようにトラフィックをシェーピングすることによって、データ レートの不一致があるトポロジのボトルネックを排除できます。シェーピングは、選択した QoS クラスまたはインターフェイス レベル（階層型シェーピング）で実行できます。

ポリシング メカニズムとシェーピング メカニズムはどちらも、パケット分類によって指定されたパケットのトラフィック記述子（マーキング パラメータについて （3291 ページ）を参照）を使用して、合意されたサービス レベルに適合するようにします。ポリサーとシェーパーは、通常は同じ方法でトラフィック記述子違反を識別しますが、図 55 : トラフィック シェーピングとトラフィック ポリシングの比較 （3297 ページ）に示すように、違反への対応方法は異なります。

- ポリサーでは通常、超過トラフィックはドロップされます。それ以外の場合、トラフィックは異なる（通常は低い）プライオリティで送信されます。

- シェイパーでは通常、バッファ（キューイングメカニズム）を使用して過剰なトラフィックを遅延させ、送信元のデータレートが想定よりも遅い場合に、パケットを保持して、フローをシェーピングします。

図 *55*：トラフィックシェーピングとトラフィックポリシングの比較



QoS ポリシーでのポリシング パラメータとシェーピング パラメータの定義については、QoS クラスのポリシング パラメータの定義 （3309 ページ）およびQoS クラスのシェーピング パラメータの定義 （3311 ページ）を参照してください。

関連項目

- トークン バケット メカニズムについて （3297 ページ）
- マーキング パラメータについて （3291 ページ）
- キューイング パラメータについて （3293 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

トークン バケット メカニズムについて

ポリシングとシェーピングは、どちらもトークンバケットメカニズムを使用してデータフローを規制します。トークン バケットは、転送レートの正式な定義です。バースト サイズ、平均レート、時間間隔（Tc）という 3 つの構成要素があります。次の式を使用して、任意の 2 つの値を 3 番めの値から得ることができます。

平均レート = バースト サイズ / 時間間隔

これらの用語は、次のように定義されます。

- 平均レート：認定情報レート（CIR）とも呼ばれ、単位時間あたりに平均で送信または転送できるデータ量を指定します。CIR は、インターフェイス上で使用可能な帯域幅の絶対

値またはパーセンテージとして定義されます。パーセンテージとして定義された場合、ビット/秒（bps）での同等の値が、ポリシーで定義されたインターフェイス帯域幅およびパーセント値に基づいて展開後に計算されます。

（注） インターフェイス帯域幅が変わる（たとえば、帯域幅が追加される）と、CIR の bps 値は、更新された帯域幅の量に基づいて再計算されます。

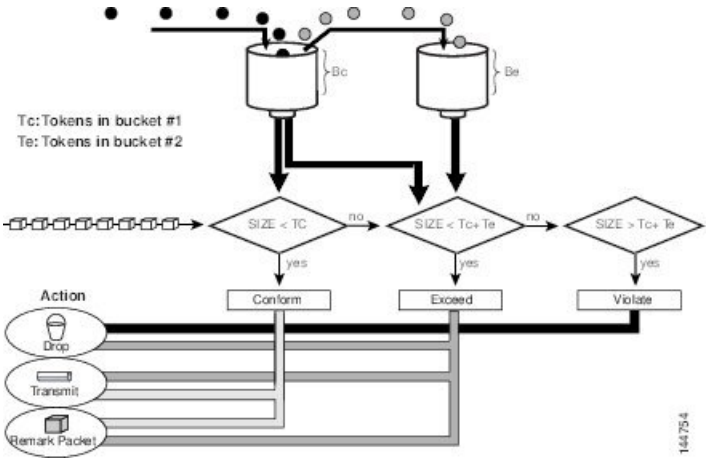
- バースト サイズ：認定バースト（Bc）サイズとも呼ばれ、スケジューリングの問題を発生させずに特定の時間内に送信できるバーストごとのデータ量を指定します。CIR の計算にパーセンテージを使用する場合、バースト サイズはミリ秒単位で測定されます。
- 時間間隔：測定間隔とも呼ばれ、バーストあたりの時間を秒単位で指定します。この間隔の整数倍にわたって、インターフェイスのビット レートが平均レートを超えることはありません。ただし、ビット レートはこの間隔内では任意の速度である場合があります。

トークンバケットのたとえで言えば、トークンは特定のレートでバケットに入れられます。これらのトークンは、送信元が特定の数のビットをネットワークに送信する権限を表します。パケットを送信するには、レギュレータ（ポリサーまたはシェーパー）によって、パケットサイズと等しい数のトークンがバケットから削除される必要があります。

Security Manager では、図 56：2 トークン バケット アルゴリズム （3299 ページ）に示すように、2 バケット アルゴリズムが使用されます。最初のバケットは適合バケット、2 番めのバケットは超過バケットです。適合バケットの全体サイズは、通常のバースト サイズとして指定されたバイト数です。超過バケットの全体サイズは、最大バースト サイズで指定されたバイト数です。どちらのバケットも最初は一杯であり、トークンの到着レート（CIR によって決定される）に基づいて更新されます。到着パケットのバイト数が適合バケット内のバイト数よりも小さい場合、パケットは適合します。必要な数のトークンが適合バケットから削除され、定義された適合アクションが実行されます（たとえば、パケットは送信されます）。超過バケットには影響はありません。

適合バケット内に十分なトークンがない場合、パケットのバイト数に対して超過トークン バケットがチェックされます。2 つのバケットを合わせると十分なトークンがある場合、パケットに対して超過アクションが実行され、必要なバイト数が各バケットから削除されます。超過バケット内に十分なバイト数がない場合、パケットはバースト制限に違反しており、パケットに対して違反アクションが実行されます。

図 *56 : 2* トークン バケット アルゴリズム



トラフィック ポリシングを使用する場合、トークン バケット アルゴリズムには、各パケットに対して3つのアクションがあります。適合アクション、超過アクション、およびオプションの違反アクションです。たとえば、適合したパケットは送信するように設定し、超過したパケットはプライオリティを下げて送信するように設定し、違反したポリシーはドロップするように設定できます。

トラフィック ポリシングは、多くの場合、ネットワークに出入りするトラフィックのレートを制限するためにネットワークのエッジのインターフェイスで設定されます。最も一般的なトラフィック ポリシングの設定では、適合したトラフィックは送信され、超過したトラフィックはプライオリティを下げて送信されるかドロップされます。ネットワークのニーズに合わせて、これらの設定オプションを変更できます。

トラフィック シェーピングを使用する場合、トークン バケット メカニズムには、すぐに送信できないパケットを保持するためのデータ バッファが含まれます（ポリサーにはこのようなバッファはありません）。トークンバケットでは、バーストにおいてパケットの送信が許可されますが、バケットの容量＋時間間隔 X 補充レートよりもフローが速くならないように、この機能には限度が設定されます。また、長期の伝送レートがCIRを超えないことも、バッファによって保証されます。

関連項目

- コントロール プレーン ポリシングについて （3299 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）

コントロール プレーン ポリシングについて

コントロール プレーン ポリシング機能を使用すると、ルータの Control Plane（CP; コントロール プレーン）に入ってくる入力トラフィックを管理できます。CP とは、ルート プロセッサ上でプロセス レベルで実行されるプロセスのコレクションのことです。これらのプロセスのコレクションにより、ほとんどの Cisco IOS 機能に高レベルの制御が提供されます。コントロール プレーン ポリシングによって、Cisco IOS ルータおよびスイッチの CP が偵察や Denial-of-Service

（DoS; サービス拒絶）攻撃から保護され、CP は、ルータまたはスイッチで攻撃や過大なトラフィック負荷があっても、パケットの転送とプロトコルの状態を維持できます。

コントロール プレーン ポリシング機能では、CP は、独自の入力ポートと出力ポートを持つ個別のエンティティとして扱われ、Security Manager を使用して入力で QoS ポリシーを設定できます。これらのポリシーは、パケットが CP に入るときに適用されます。指定したレート制限に達したあとは不要なパケットが増加しないように QoS ポリシーを設定できます。たとえば、システム管理者は、CP 宛のすべての TCP/SYN パケットを 1 Mbps の最大レートに制限できます。この制限を超えるパケットは、サイレントに廃棄されます。

次のタイプのレイヤ 3 パケットが CP に転送され、集約コントロール プレーン ポリシングによって処理されます。

- ルーティング プロトコル制御パケット
- ルータのローカル IP アドレス宛のパケット
- SNMP、Telnet、Secure Shell（SSH; セキュア シェル）などの管理プロトコルからのパケット

（注） 出力ポリシングのサポートは、Cisco IOS Release 12.3(4)T 以降の T トレイン リリースだけで利用できます。

コントロール プレーン ポリシングの定義方法については、コントロール プレーンでの QoS の定義 （3303 ページ）を参照してください。この機能の詳細については、Cisco.com の次の URL で「Control Plane Policing」を参照してください。

http://www.cisco.com/en/US/docs/ios/qos/configuration/guide/ctrl_plane_policng.html

関連項目

- トークン バケット メカニズムについて （3297 ページ）
- ポリシング パラメータとシェーピング パラメータについて （3296 ページ）

QoS ポリシーの定義

QoS ポリシーを定義するときは、ポリシーを特定のインターフェイスで設定するかコントロールプレーンで設定するかを最初に決定する必要があります。この最初の選択によって、次の項で説明するように、ポリシーの残りの部分の設定方法が決まります。

- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）

（注） 同じデバイスのインターフェイスとコントロール プレーンの両方で QoS ポリシーを定義した場合、コントロール プレーンの設定だけが展開されます。

関連項目

- Cisco IOS ルータにおける Quality of Service （3289 ページ）

インターフェイスでの QoS の定義

複数の QoS インターフェイス定義を作成して、それぞれの定義を（ルータに入る）入力トラフィックまたは（ルータを出る）出力トラフィックに適用できます。

出力トラフィックで QoS インターフェイス定義を作成する場合、個別の QoS クラスでシェーピングを設定するのではなく、インターフェイスで全体として階層型シェーピングを設定するオプションがあります。

インターフェイス定義を作成したあと、各インターフェイスで 1 つ以上の QoS クラスを定義する必要があります。QoS クラスには、どのパケットがクラスに含まれるかを決定する一致基準と、そのトラフィックに適用される QoS 機能（マーキング、キューイング、ポリシング、およびシェーピング）が含まれています。各インターフェイス（またはインターフェイス ロール）は、最大 16 個の QoS クラスを使用して設定でき、それぞれのクラスには、独自の一致基準のセットと、そのクラスのトラフィックに適用される QoS 機能の定義済みのセットが含まれています。

インターフェイスごとに、少なくとも 1 つの QoS クラスとデフォルト クラスを定義することを推奨します。デフォルト クラスを設定しない場合、定義された他のクラスの基準に一致しないパケットは、QoS 機能が設定されていないデフォルト クラスのメンバーとして処理されます。このクラスに割り当てられたパケットは、単純な First-In First-Out（FIFO）キューに入れられ、使用できる基本的なリンク帯域幅によって決定されるレートで転送されます。この FIFO キューは、テール ドロップによって管理されます。テール ドロップでは、キューが一杯でなくなるまでパケットをキューからドロップすることによって、輻輳が回避されます。

（注） QoS は、最初に一致したものから順にパケットに適用されます。ルータは、最上位から開始して QoS クラスのテーブルを調べ、一致基準がパケットと一致する最初のクラスのプロパティを適用します。したがって、クラスを慎重に定義して並べることが重要です。特定のクラスと一致するトラフィックが不一致のトラフィックとして扱われることを防ぐために、デフォルト クラスは最後に配置する必要があります。

はじめる前に

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）がルータでイネーブルになっていることを確認します。詳細については、Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）を参照してください。

関連項目

- QoS ポリシーの定義 （3300 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）> [サービスhinshitsu 品s津sロギング（Quality of Service）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [サービス品質（Quality of Service）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Quality of Service] ページが表示されます。このページのフィールドの説明については、表 910 : [Quality of Service] ページ （3313 ページ）を参照してください。

ステップ 2 [適用対象（Applied to）] フィールドで、[インターフェイス（Interfaces）] を選択して、選択されているルータ上の特定のインターフェイスの QoS パラメータを定義します。

ステップ 3 上部のテーブルの下にある [追加（Add）] ボタンをクリックして、[QoSポリシー（QoS Policy）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 911 : [QoS Policy] ダイアログボックス （3315 ページ）を参照してください。

ステップ 4 [インターフェイス（Interface）] フィールドで、インターフェイスまたはインターフェイスロールの名前を入力するか、[選択（Select）] をクリックしてセレクタを表示します。

ヒント 必要なインターフェイスロールがセレクタに表示されていない場合は、[作成（Create）] ボタンまたは [編集（Edit）] ボタンをクリックして、[Interface Role] ダイアログボックス （384 ページ）を開きます。ここから、ポリシーで使用するインターフェイス ロールを定義できます。

ステップ 5 QoS 定義を適用するトラフィック方向を選択します。[Output]（インターフェイスを出るトラフィック）または [Input]（インターフェイスに入るトラフィック）です。キューイングおよびシェーピングは、出力トラフィックだけに適用できます。

ステップ 6 （任意）インターフェイス レベル（階層型）シェーピング パラメータを定義します。詳細については、表 911 : [QoS Policy] ダイアログボックス （3315 ページ）を参照してください。

（注） インターフェイスで階層型シェーピングをイネーブルにすると、特定の QoS クラスのシェーピング パラメータは定義できません。シェーピングは出力トラフィックでだけ使用できます。シェーピングの詳細については、 ポリシング パラメータとシェーピング パラメータについて （3296 ページ）を参照してください。

ステップ 7 [OK] をクリック[Quality of Service] ページの上部のテーブルに、QoS インターフェイス定義が表示されます。

（注） QoS インターフェイス定義を編集するには、上部のテーブルからインターフェイスを選択し、[編集Edit] ボタンをクリックします。インターフェイス定義を削除するには、テーブルからインターフェイスを選択し、[削除（Delete）] ボタンをクリックします。クラスを定義しているインターフェイスを削除することはできません。

ステップ 8 上部のテーブルでインターフェイスが選択されている状態で、[QoSクラス（QoS Classes）] テーブルの下の [追加（Add）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 912 : [QoS Class] ダイアログボックス （3318 ページ）を参照してください。

[QoS Class] ダイアログボックスでは、選択したインターフェイス上のどのトラフィックが QoS クラスに含まれるかと、そのトラフィックの処理方法を決定できます。

ステップ 9 （任意）このインターフェイスのデフォルトの QoS クラスのプロパティを定義している場合は、[デフォルトクラス（Default class）] チェックボックスをオンにします。デフォルト クラスは、定義された他のクラスの基準に一致しないすべてのトラフィックに割り当てられます。

ステップ 10 次の項で説明するように、[QoS Class] ダイアログボックスの 1 つ以上のタブを使用して、QoS クラスを定義します。

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- QoS クラスのマーキング パラメータの定義 （3307 ページ）
- QoS クラスのキューイング パラメータの定義 （3308 ページ）
- QoS クラスのポリシング パラメータの定義 （3309 ページ）
- QoS クラスのシェーピング パラメータの定義 （3311 ページ）

ステップ 11 ステップ 8 （3303 ページ）～ステップ 10 （3303 ページ）を繰り返して、ステップ 3 （3302 ページ）で定義したインターフェイスに QoS クラスを追加します。必要に応じて、[行を上に移動（Up Row）] および [行を下に移動（Down Row）] ボタンを使用してクラスを並べ替えます。

（注） QoS クラスを編集するには、上のテーブルで関連するインターフェイスを選択して、定義されているクラスを [QoS Class] テーブルに表示します。編集するクラスを選択し、[編集（Edit）] ボタンをクリックします。クラスを削除するには、テーブルからクラスを選択し、[削除（Delete）] ボタンをクリックします。

ステップ 12 ステップ 3 （3302 ページ）からステップ 11 （3303 ページ）を繰り返して、選択されているルータの別のインターフェイスに QoS クラスを定義します。

コントロール プレーンでの QoS の定義

コントロール プレーンに入る入力トラフィックで QoS を設定する場合、他のクラスに対して定義した基準と一致しないトラフィック用のデフォルト クラスなど、複数の QoS クラスを定義できます。特定のクラスの一致基準を定義した後に、そのクラスのポリシング定義を設定できます（マーキング、キューイング、およびシェーピングは設定できません）。詳細については、コントロール プレーン ポリシングについて （3299 ページ）を参照してください。

コントロール プレーンで定義された QoS ポリシーは、同じデバイスのインターフェイスで定義されている QoS パラメータよりも優先されます。

（注） QoS は、最初に一致したものから順にパケットに適用されます。ルータは、最上位から開始して QoS クラスのテーブルを調べ、一致基準がパケットと一致する最初のクラスのプロパティを適用します。したがって、クラスを慎重に定義して並べることが重要です。特定のクラスと一致するトラフィックが不一致のトラフィックとして扱われることを防ぐために、デフォルト クラスは最後に配置する必要があります。

はじめる前に

Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）がルータでイネーブルになっていることを確認します。詳細については、Cisco IOS ルータでの CEF インターフェイス設定 （3036 ページ）を参照してください。

関連項目

- QoS ポリシーの定義 （3300 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）> [サービス品質（Quality of Service）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）]> [サービス品質（Quality of Service）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Quality of Service] ページが表示されます。このページのフィールドの説明については、表 910 : [Quality of Service] ページ （3313 ページ）を参照してください。

ステップ 2 [適用先（Applied to）] フィールドで、[コントロールプレーン（Control Plane）] を選択して、コントロールプレーンに着信する入力トラフィックの QoS ポリシングを定義します。

ステップ 3 [コントロールプレーンの QoS クラス（Control Plane QoS Classes）] テーブルの下にある [追加（Add）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 912 : [QoS Class] ダイアログボックス （3318 ページ）を参照してください。

[QoS Class] ダイアログボックスでは、選択したインターフェイス上のどのトラフィックが QoS クラスに含まれるかと、そのトラフィックの処理方法を決定できます。

ステップ 4 （任意）コントロールプレーンのデフォルトの QoS クラスのプロパティを定義している場合は、[デフォルトクラス（Default class）] チェックボックスをオンにします。デフォルト クラスは、定義された他のクラスの基準に一致しないすべてのトラフィックに割り当てられます。

ステップ 5 次の項で説明するように、[QoS Class] ダイアログボックスのタブを使用して、QoS クラスを定義します。

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- QoS クラスのポリシング パラメータの定義 （3309 ページ）

ステップ 6 ステップ 3 （3304 ページ）～ステップ 5 （3305 ページ）を繰り返して、コントロールプレーンに QoS クラスを追加します。必要に応じて、[行を上に移動（Up Row）] および [行を下に移動（Down Row）] ボタンを使用してクラスを並べ替えます。

QoS クラスのマッチング パラメータの定義

マッチングパラメータを定義するときは、マッチング基準を定義し、パケットがクラスの一部と見なされるために基準の 1 つまたはすべてを満たす必要があるかどうかを指定する必要があります。詳細については、マッチング パラメータについて （3291 ページ）を参照してください。

（注） デフォルト クラスを設定するときは、マッチング パラメータを定義しません。

関連項目

- QoS クラスのマーキング パラメータの定義 （3307 ページ）
- QoS クラスのキューイング パラメータの定義 （3308 ページ）
- QoS クラスのポリシング パラメータの定義 （3309 ページ）
- QoS クラスのシェーピング パラメータの定義 （3311 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 [QoS（Quality of Service）] ページで、[QoSクラス（QoS Classes）] テーブルの下にある [追加（Add）] ボタンをクリックするか、クラスを選択して [編集（Edit）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。

ステップ 2 [マッチング（Matching）] タブをクリックします。このタブに含まれるフィールドの説明については、表 912 : [QoS Class] ダイアログボックス （3318 ページ）を参照してください。

ステップ 3 一致方式を選択します。

- [Any]：定義されたパラメータのいずれかと一致するトラフィックがこのクラスに含まれます。
- [All]：定義されたパラメータのすべてと一致するトラフィックだけがこのクラスに含まれます。

ステップ 4 （任意）[プロトコル（Protocol）] で、[追加（Add）] をクリックして、このクラスに含めるプロトコルを選択するためのセレクタを表示します。[利用可能なプロトコル（Available Protocols）] リストから 1 つ以

上のアイテムを選択し、[>>] をクリックしてそれらを [選択済みのプロトコル（Selected Protocols）] リストに追加します。

（注） コントロール プレーンで QoS を設定する場合は、ARP プロトコルだけを選択できます。

終了したら、[OK] をクリックして定義を保存し、[QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [Protocol] フィールドに表示されます。

ステップ 5 （任意）[優先順位（Precedence）] で、[追加（Add）] をクリックして、このクラスに含める IP 優先順位の値（0 ～ 7）を選択するためのセレクタを表示します。[利用可能な優先順位（Available Precedences）] リストから 1 つ以上のアイテムを選択し、[>>] をクリックしてそれらを [選択済みの優先順位（Selected Precedences）] リストに追加します。これらの値の 1 つがマークされている到着トラフィックがこの基準に一致します。

（注） IP precedence 値の詳細については、表 908 : IP Precedence クラス （3292 ページ）を参照してください。

終了したら、[OK] をクリックして定義を保存し、[QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [Precedences] フィールドに表示されます。

ステップ 6 （任意）[DSCP] で、[追加（Add）] をクリックして、このクラスに含める DSCP の値（0 ～ 63）を選択するためのセレクタを表示します。[利用可能なDSCP（Available DSCPs）] リストから 1 つ以上のアイテムを選択し、[>>] をクリックしてそれらを [選択済みDSCP（Selected DSCPs）] リストに追加します。これらの値の 1 つがマークされている到着トラフィックがこの基準に一致します。

終了したら、[OK] をクリックして定義を保存し、[QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [DSCP] フィールドに表示されます。

ステップ 7 （任意）[ACL] で、このクラスの一致基準の一部として ACL を定義します。

a) [編集（Edit）] をクリックして、[ACLの編集（Edit ACLs）] ダイアログボックスを表示します。このダイアログボックスを使用して、このクラスに含める ACL を定義します。

b) 1 つ以上の ACL を入力します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。これらの ACL 定義と一致するトラフィックが、この基準と一致します。

c) 終了したら、[OK] を 2 回クリックして定義を保存し、[QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [ACL] フィールドに表示されます。

ヒント 上向きおよび下向き矢印を使用して、ACL を配置します。より頻繁に使用される ACL をリストの一番上に配置して、一致プロセスを最適化することを推奨します。

ステップ 8 別のタブに移動するか、[OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたクラスが [Quality of Service] ページの [QoS Classes] テーブルに表示されます。

ステップ 9 次のいずれかを実行します。

- インターフェイスに QoS を定義する場合は、インターフェイスでの QoS の定義 （3301 ページ）の説明に従って進みます。

- コントロール プレーン ポリシングを定義する場合は、コントロール プレーンでの QoS の定義 （3303 ページ）の説明に従って進みます。

QoS クラスのマーキング パラメータの定義

マーキング パラメータを定義する場合、precedence 値または DSCP 値を使用して、この QoS クラスのパケットをマークできます。詳細については、マーキング パラメータについて （3291 ページ）を参照してください。

（注） マーキングは、コントロールプレーンで QoS を設定する場合には使用できません。

関連項目

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- QoS クラスのキューイング パラメータの定義 （3308 ページ）
- QoS クラスのポリシング パラメータの定義 （3309 ページ）
- QoS クラスのシェーピング パラメータの定義 （3311 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 [QoS（Quality of Service）] ページで、[QoS クラス（QoS Classes）] テーブルの下にある [追加（Add）] ボタンをクリックするか、クラスを選択して [編集（Edit）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。

ステップ 2 [マーキング（Marking）] タブをクリックします。このタブのフィールドの説明については、表 914 : [QoS Class] ダイアログボックス - [Marking] タブ （3322 ページ）を参照してください。

ステップ 3 [マーキングを有効にする（Enable Marking）] チェックボックスをオンにします。

ステップ 4 次のマーキング オプションのいずれかを選択します。

- [Precedence]：表示されるリストから IP precedence 値（0 ～ 7）を選択します。これらの値の詳細については、表 908 : IP Precedence クラス （3292 ページ）を参照してください。
- [DSCP]：表示されるリストから DSCP 値（0 ～ 63）を選択します。

ステップ 5 別のタブに移動するか、[OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたクラスが [Quality of Service] ページの [QoS Classes] テーブルに表示されます。

ステップ 6 QoS ポリシーの定義 （3300 ページ）の手順に従って進みます。

QoS クラスのキューイング パラメータの定義

キューイング パラメータを定義する場合、この QoS クラスのトラフィックに対して提供できる帯域幅の量を指定できます。プライオリティが高いトラフィックに対して提供する必要がある帯域幅の固定量を定義することもできます。プライオリティパラメータは、インターフェイスごとに1つのクラスだけで定義できます。また、このクラスで実行するキュー管理のタイプを指定する必要があります。詳細については、キューイング パラメータについて （3293 ページ）を参照してください。

（注） キューイングは、コントロール プレーンに QoS を設定する場合には使用できません。

関連項目

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- QoS クラスのマーキング パラメータの定義 （3307 ページ）
- QoS クラスのポリシング パラメータの定義 （3309 ページ）
- QoS クラスのシェーピング パラメータの定義 （3311 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 [QoS（Quality of Service）] ページで、[QoS クラス（QoS Classes）] テーブルの下にある [追加（Add）] ボタンをクリックするか、クラスを選択して [編集（Edit）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。

ステップ 2 [キューイングおよび輻輳回避（Queuing and Congestion Avoidance）] タブをクリックします。このタブのフィールドの説明については、表 915 : [QoS Class] ダイアログボックス - [Queuing and Congestion Avoidance] タブ （3323 ページ）を参照してください。

ステップ 3 [キューイングおよび輻輳回避（Queuing and Congestion Avoidance）] チェックボックスをクリックします。

キューイング オプションは、デフォルト クラスを定義するかその他のクラスを定義するかによって異なります。

- デフォルトクラス以外のクラスを定義する場合は、次のキューオプションのいずれかを選択します。
  - [Priority] : プライオリティが高いトラフィックで使用可能にする帯域幅の量を定義します。低遅延キューイング （3295 ページ）（LLQ）は、このトラフィックが常にこの固定量の帯域幅を受信することを保証します。これは、低遅延を必要とする音声トラフィックに特に役立ちます。この量は、パーセンテージまたはキロビット/秒の絶対値で定義できます。

（注） このオプションは、インターフェイスごとに 1 つのクラスにのみ定義できます。

- • [Bandwidth] : このクラスに割り当てる帯域幅の量を入力します。この量は、パーセンテージまたはキロビット/秒の絶対値で定義できます。

（注） インターフェイス上のすべてのクラスの帯域割り当ての合計が、使用可能な帯域幅の合計の 100% を超えることはできません。

- デフォルトクラスを定義する場合は、次のキューオプションのいずれかを選択します。
  - [Fair queue]：デフォルト クラス用に予約するキューの数を入力します。値の範囲は、2 の累乗で 16 ～ 4096 です。デフォルトでは、キューの数は、選択したインターフェイスの使用可能な帯域幅に基づきます。詳細については、表 909 : デフォルト クラスのキューのデフォルトの数 （3296 ページ）を参照してください。
  - [Bandwidth]：このクラスに割り当てる帯域幅の量を入力します。この量は、パーセンテージまたはキロビット/秒の絶対値で定義できます。

ステップ 4 （任意）次のキュー長管理オプションのいずれかを定義します。

- [Queue Limit]：（デフォルト）許可されるパケットの最大数を指定します。このオプションを選択すると、キューが容量に達したときにテールドロップによって超過パケットがドロップされます。
- [WRED Weight for Mean Queue Depth]：伝送レートを下げて輻輳を軽減することによって伝送プロトコル（通常は TCP）が対応するまで、パケットは WRED によってプロアクティブにドロップされます。平均キューサイズの計算に使用される指数加重係数を入力することによって、WRED を設定します。

詳細については、テール ドロップと WRED （3294 ページ）を参照してください。

（注） 別の値にすることがアプリケーションにメリットがあるとわかっている場合にのみ、デフォルトを変更する必要があります。

（注） WRED は、パケット損失に対応して伝送レートを下げるには堅牢性が十分ではないプロトコル（IPX や AppleTalk など）とともに使用しないでください。[Priority] パーセント オプションを選択した場合、WRED は設定できません。

ステップ 5 別のタブに移動するか、[OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたクラスが [Quality of Service] ページの [QoS Classes] テーブルに表示されます。

ステップ 6 QoS ポリシーの定義 （3300 ページ）の手順に従って進みます。

QoS クラスのポリシング パラメータの定義

ポリシングのパラメータを定義するときは、送信できるトラフィックの量を決定する平均データレートを指定する必要があります。また、このデータ レートを超えたトラフィック バーストに対するアクションを指定する必要があります。

すべての QoS クラス（デフォルト クラスを含む）のポリシングを設定できます。ポリシングの詳細については、ポリシング パラメータとシェーピング パラメータについて （3296 ページ）を参照してください。

コントロールプレーンでポリシングを設定することもできます。詳細については、コントロール プレーン ポリシングについて （3299 ページ）を参照してください。

関連項目

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- QoS クラスのマーキング パラメータの定義 （3307 ページ）
- QoS クラスのキューイング パラメータの定義 （3308 ページ）
- QoS クラスのシェーピング パラメータの定義 （3311 ページ）
- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 [QoS（Quality of Service）] ページで、[QoS クラス（QoS Classes）] テーブルの下にある [追加（Add）] ボタンをクリックするか、クラスを選択して [編集（Edit）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。

ステップ 2 [プリシング（Policing）] タブをクリックします。このタブのフィールドの説明については、表 912 : [QoS Class] ダイアログボックス （3318 ページ）を参照してください。

ステップ 3 [ポリシングの有効化（Enable Policing）] チェックボックスをオンにします。

ステップ 4 CIR、確認バースト、および超過バーストの値を定義します。CIR は、パーセンテージまたはビット/秒の絶対値で定義できます。選択したオプションによって、バースト値の定義方法が決まります。

ステップ 5 レート制限に適合したパケットに対して実行するアクションを選択します。

- [transmit]：パケットを送信します。
- [set-prec-transmit]：IP precedence を定義された値に設定し、パケットを送信します。このオプションは、コントロール プレーンに QoS を設定する場合には使用できません。
- [set-dscp-transmit]：DSCP を定義された値に設定し、パケットを送信します。このオプションは、コントロール プレーンに QoS を設定する場合には使用できません。
- [drop]：パケットをドロップします。

ステップ 6 超過パケットに対して実行するアクションを選択します。使用可能なアクションのリストは、選択した適合アクションによって異なります。

たとえば、適合パケットに対して送信を実行する場合、超過パケットに対して、ステップ 5 （3310ページ）で示されている任意のアクションを選択できます。ただし、適合パケットに対して set アクションのいずれかを選択した場合、超過パケットに対して set アクションまたは drop アクションだけを選択できます。適合アクションとして [drop] を選択した場合、超過アクションとして [drop] を選択する必要があります。

ステップ 7 違反パケットに対して実行するアクションを選択します。使用可能なアクションのリストは、選択した超過アクションによって異なります。

たとえば、超過パケットに対して送信を実行する場合、違反パケットに対して、ステップ 5 （3310ページ）で示されている任意のアクションを選択できます。ただし、超過パケットに対して set アクションのいずれかを選択した場合、違反パケットに対して set アクションまたは drop アクションだけを選択できます。超過アクションとして [drop] を選択した場合、違反アクションとして [drop] を選択する必要があります。

ステップ 8 別のタブに移動するか[OK]をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたクラスが [Quality of Service] ページの [QoS Classes] テーブルに表示されます。

ステップ 9 次のいずれかを実行します。

- インターフェイスにQoSを定義する場合は、QoSポリシーの定義 （3300ページ）の説明に従って進みます。
- コントロール プレーン ポリシングを定義する場合は、コントロール プレーンでのQoSの定義 （3303ページ）の説明に従って進みます。

QoS クラスのシェーピング パラメータの定義

シェーピング パラメータを定義する場合、トラフィック シェーピングを平均データ レートに基づかせるか、平均データ レートとトラフィック ピーク時に発生する超過バースト レートを加算したレートに基づかせるかを指定する必要があります。どちらの場合も、これらの定義を超過したトラフィックは、レートが下がってパケットを送信できるようになるまでバッファに格納されます。

次の条件があります。

- シェーピングは出力トラフィックでだけ使用できます。
- シェーピングは、すべての QoS クラス（デフォルト クラスを含む）に設定できます。
- シェーピングは、プライオリティ トラフィックの QoS クラスを設定する場合には使用できません。
- シェーピングは、コントロール プレーンで QoS を設定する場合には使用できません。

シェーピングの詳細については、ポリシング パラメータとシェーピング パラメータについて（3296 ページ）を参照してください。

ヒント インターフェイスに対して定義されているすべての QoS クラスでシェーピングを設定するには（階層型シェーピング）、インターフェイスでのQoSの定義 （3301ページ）を参照してください。

関連項目

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- QoS クラスのマーキング パラメータの定義 （3307 ページ）
- QoS クラスのキューイング パラメータの定義 （3308 ページ）
- QoS クラスのポリシング パラメータの定義 （3309 ページ）
- QoS ポリシーの定義 （3300 ページ）

- Cisco IOS ルータにおける Quality of Service （3289 ページ）

ステップ 1 [QoS（Quality of Service）] ページで、[QoSクラス（QoS Classes）] テーブルの下にある [追加（Add）] ボタンをクリックするか、クラスを選択して [編集（Edit）] ボタンをクリックします。[QoS Class] ダイアログボックスが表示されます。

ステップ 2 [シェーピング（Shaping）] タブをクリックします。このタブのフィールドの説明については、表 917 : [QoS クラス（QoS Class）] ダイアログボックス : [シェーピング（Shaping）] タブ （3328 ページ）を参照してください。

ステップ 3 [シェーピングの有効化（Enable Shaping）] チェックボックスをオンにします。

ステップ 4 シェーピング タイプ（[Average] または [Peak]）を選択します。

ステップ 5 CIR、持続的バースト、および超過バーストの値を定義します。CIR は、パーセンテージまたはビット/秒の絶対値で定義できます。選択したオプションによって、バースト値の定義方法が決まります。

ステップ 6 別のタブに移動するか [OK] をクリックして、定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたクラスが [Quality of Service] ページの [QoS Classes] テーブルに表示されます。

ステップ 7 QoS ポリシーの定義 （3300 ページ）の手順に従って進みます。

サービス品質ポリシーページ

[Quality of Service] ページを使用して、選択したデバイスの特定のインターフェイス上またはコントロール プレーン上の QoS クラスを表示、作成、および編集します。QoS ポリシーを使用すると、ネットワークで遅延、遅延変動（ジッタ）、帯域幅、およびパケット損失パラメータを管理するための手法を定義できます。また、[Quality of Service] ページを使用して、個々の QoS クラスのシェーピング パラメータを設定する代わりに、インターフェイスで階層型シェーピングを設定できます。

詳細については、 Cisco IOS ルータにおける Quality of Service （3289 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）>[サービス品質（Quality of Service）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）]>[サービス品質（Quality of Service）] を選択します。新しいポリシーを作成するか、共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- QoS ポリシーの定義 （3300 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *910 : [Quality of Service]* ページ

要素	説明
適用先（Apply to）	QoS ポリシーを定義するルータ コンポーネント。 • [Interfaces]：特定のインターフェイスで QoS クラスを設定します。 • [Control Plane]：ルータのコントロール プレーンで QoS を設定します。 コントロールプレーンポリシングについて （3299ページ）を参照してください。 （注） 同じデバイスのインターフェイスとコントロールプレーンの両方で QoS を設定した場合、コントロールプレーンの設定だけが展開されます。
インターフェイス テーブル	インターフェイスでクラスを定義している場合は、上部の表に、QoS クラスを定義しているインターフェイスが一覧表示されます。[direction] カラムで、クラスが適用されるインターフェイスでのトラフィックの方向が示されます（[Output] または [Input]）。定義できるクラスは、方向によって異なります。 その他のフィールドでは、インターフェイスでシェーピングを定義したかどうか、およびシェーピングが定義されている場合は、階層型シェーピングのタイプ（平均またはピーク）、Committed Information Rate（CIR; 認定情報レート）、平均バースト サイズおよび超過バースト サイズが示されます。属性の詳細については、[QoS Policy] ダイアログボックス （3314 ページ）を参照してください。 • テーブルにインターフェイスを追加するには、[Add] ボタンをクリックします。 • インターフェイスの設定を編集するには、そのインターフェイスを選択し、[Edit] ボタンをクリックします。 • インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] ボタンをクリックします。

要素	説明
[QoS Classes] テーブル	上部のテーブルで選択されたインターフェイスに対して、またはコントロールプレーンに対して定義されているクラス。各行は、個々のクラスを表します。[No.] 列はクラスの順序を示し、非常に重要です。QoS は、クラスの順序に基づいて、最初に一致したものから順にパケットに適用されます。 [Default Class] カラムでは、このクラスが、定義された他のクラスの基準に一致しないインターフェイスのすべてのパケットのデフォルトかどうかが示されます。このクラスをリストの最後のクラスにします。 残りのカラムでは、クラスの一致基準、およびクラスに対して定義されたパケット マーキング、キューイングおよび輻輳回避、ポリシング、およびシェーピング（ある場合）が示されます。属性の詳細については、[QoS Policy] ダイアログボックス （3314 ページ）を参照してください。 • テーブルにクラスを追加するには、[Add] ボタンをクリックします。 • クラスの設定を編集するには、そのクラスを選択し、[Edit] ボタンをクリックします。 • クラスを削除するには、クラスを選択し、[Delete] ボタンをクリックします。 • クラスの順序を変更するには、クラスを選択し、上下の矢印ボタンをクリックして位置を変更します。

[QoS Policy] ダイアログボックス

[QoS Policy] ダイアログボックスを使用して、QoS パラメータを定義するインターフェイスを選択します。さらに、このダイアログボックスを使用して、選択したインターフェイス上のすべてのトラフィックに対して単一のシェーピング パラメータ セットを設定できます（階層シェーピングと呼ばれます）。階層型シェーピングを使用すると、インターフェイスで定義されている QoS クラスごとにシェーピング パラメータを設定する必要がなくなります。

（注） このダイアログボックスは、コントロールプレーンで QoS ポリシーを定義する場合には適用されません。詳細については、コントロール プレーンでの QoS の定義 （3303 ページ）を参照してください。

QoS インターフェイス定義を作成した後、各インターフェイスで 1 つ以上の QoS クラスを定義できます。詳細については、[QoS Class] ダイアログボックス （3316 ページ）を参照してください。

ナビゲーション パス

サービス品質ポリシーページ （3312ページ）に移動してから、上部のテーブルの下にある[追加（Add）]ボタンまたは[編集（Edit）]ボタンをクリックして、QoSインターフェイスを定義します。

関連項目

- QoS ポリシーの定義 （3300 ページ）
- Cisco IOS ルータにおける Quality of Service （3289 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *911 : [QoS Policy]* ダイアログボックス

要素	説明
インターフェイス（Interface）	QoSを定義するインターフェイス。インターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
方向	QoS を設定するトラフィックの方向： • [Output]：インターフェイスから出るトラフィック。 • [Input]：インターフェイスに入るトラフィック。
階層型シェーピングの設定	
Enable Shaping	選択した場合、選択されているインターフェイスで階層型トラフィック シェーピングが設定されます。 選択を解除すると、階層型シェーピングは使用されません。 （注） シェーピングは出力トラフィックでだけ実行できます。
タイプ（Type）	実行するシェーピングのタイプ。 • [Average]：各間隔のデータ レートを、平均バースト レート（認定バースト レートまたはBcとも呼ばれる）に制限し、平均レートがCommitted Information Rate（CIR; 認定情報レート）を超えないようにします。追加のパケットは、送信できるようになるまでバッファに格納されます。 • [Peak]：各間隔のデータ レートを、平均バースト レートに超過バースト レート（Be）を加算したレートに制限します。追加のパケットは、送信できるようになるまでバッファに格納されます。

要素	説明
CIR	平均データ レート（認定情報レートまたは CIR とも呼ぶ）。この量は次の単位で定義できます。 • [Percentage]：有効値の範囲は、使用可能な帯域幅全体の 0 ～ 100% です。 • [Bit/sec]：有効値の範囲は 8000 ～ 1000000000 ビット/秒で、8000 の倍数である必要があります。 ある間隔中のデータ バーストはこのレートを超過することがありますが、間隔の多重積分の平均データ レートはこのレートを超過しません。
Sustained Burst	通常のバースト サイズ。シェーピング タイプとして平均を選択した場合は、1 間隔中のデータ バーストがこの値に制限されます。 有効値の範囲は、CIR によって決まります。 • CIR がパーセンテージで定義されている場合：有効値の範囲は 10 ～ 2000 ミリ秒です。 • CIR が絶対値で定義されている場合：有効値の範囲は 1000 ～ 154400000 バイトで、128 バイトの倍数です。 （注） CIR が絶対値で定義されている場合は、このフィールドをブランクのままにすることを推奨します。これにより、デバイスで使用されているアルゴリズムが最適な平均バースト値を決定できます。
Excess Burst	超過バースト サイズ。シェーピング タイプとしてピークを選択した場合、1 間隔中のデータ バーストは、平均バースト値とこの値の合計と等しくなることができます。ただし、複数間隔の平均データ レートは、CIR に準拠します。 有効値の範囲は、CIR によって決まります。 • CIR がパーセンテージで定義されている場合：有効値の範囲は 10 ～ 2000 ミリ秒です。 • CIR が絶対値で定義されている場合：有効値の範囲は 1000 ～ 154400000 バイトで、128 バイトの倍数です。 （注） CIR が絶対値で定義されているときにこのフィールドを設定しない場合、持続的バースト値が使用されます。

[QoS Class] ダイアログボックス

[QoS Class] ダイアログボックスを使用して、Cisco IOS ルータの選択したインターフェイスまたはコントロール プレーン上の QoS クラスを作成または編集します。1 つのインターフェイスで最大 16 個のクラスを定義でき、デバイス全体で最大 256 個のクラスを定義できます。

（注） QoS は、最初に一致したものから順にパケットに適用されます。ルータは、最上位から開始して QoS クラスのテーブルを調べ、一致基準がパケットと一致する最初のクラスのプロパティを適用します。したがって、クラスを慎重に定義して並べることが重要です。特定のクラスと一致するトラフィックが不一致のトラフィックとして扱われることを防ぐために、デフォルト クラスは最後に配置する必要があります。

ナビゲーション パス

サービス品質ポリシーページ （3312 ページ）に移動します。ページの上部にあるオプションを設定し、次のいずれかを実行します。

- QoS クラスを作成するには、上部のテーブルからインターフェイスを選択し、[QoSクラス（QoS Class）] テーブルの下にある [追加（Add）] ボタンをクリックします。コントロールプレーンの QoS クラスは、テーブルの下にある [追加（Add）] ボタンをクリックするだけで作成できます。
- QoS クラスを編集するには、次の手順を実行します。
  - 上部のテーブルから、クラスを編集するインターフェイスを選択します（コントロール プレーンを選択する場合は必要ありません）。
  - [QoS Classes] テーブルで、そのインターフェイスに対して定義されている該当するクラスを選択します（コントロール プレーンを選択する場合は必要ありません）。
  - [QoSクラス（QoS Class）] テーブルの下の [編集（Edit）] ボタンをクリックします。

関連項目

- [QoS Policy] ダイアログボックス （3314 ページ）
- QoS ポリシーの定義 （3300 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）

フィールド リファレンス

表 *912 : [QoS Class]* ダイアログボックス

要素	説明
Set as Default Class	選択すると、このインターフェイスのその他の QoS クラスと一致しないすべてのトラフィックのデフォルト クラスを定義できます。 選択を解除すると、このインターフェイスの特定の QoS クラスを定義できます。 （注） デフォルトクラスを定義する場合は、マッチングパラメータを設定しません。定義上、このクラスは他のクラスと一致しないすべてのトラフィックで構成されます。そのため、[Matching] タブはディセーブルです。
[Matching] タブ	この QoS クラスに含まれるトラフィックを定義します。 [QoS Class] ダイアログボックス - [Matching] タブ （3318 ページ）を参照してください。
[Marking] タブ	ダウンストリームデバイスが適切に識別できるように、このクラスのトラフィックをマークします。 [QoS Class] ダイアログボックス - [Marking] タブ （3321 ページ）を参照してください。
[Queuing and Congestion Avoidance] タブ	このクラスの出力トラフィックをキューイングする方法を定義します。 [QoS Class] ダイアログボックス - [Queuing and Congestion Avoidance] タブ （3322 ページ）を参照してください。
[Policing] タブ	このクラスのトラフィック フローを設定されたレートに制限します。 [QoS Class] ダイアログボックス - [Policing] タブ （3325 ページ）を参照してください。
[Shaping] タブ	ダウンストリーム デバイスの要件を満たすように、このクラスの出力トラフィックのフローを制御します。 [QoS Class] ダイアログボックス - [Shaping] タブ （3327 ページ）を参照してください。

（注） コントロールプレーンで QoS ポリシーを設定すると、[マッチング（Matching）] タブと [ポリシング（Policing）] タブのみが使用可能になります。

[QoS Class] ダイアログボックス - [Matching] タブ

[QoS Class] ダイアログボックスの [Matching] タブを使用して、このクラスの一部と見なす、選択されているインターフェイスのトラフィックを定義します。

（注） デフォルト クラスを定義する場合、[Matching] タブはディセーブルです。

ナビゲーション パス

[QoS Class] ダイアログボックス （3316 ページ）に移動してから、[マッチング（Matching）] タブをクリックします。

関連項目

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- サービス品質ポリシーページ （3312 ページ）
- アクセス コントロール リスト オブジェクトの作成 （356 ページ）

フィールド リファレンス

表 *913 : [QoS Class]* ダイアログボックス - *[Matching]* タブ

要素	説明
Match Method	このクラスに使用されるトラフィック マッチング オプション： • [いずれか（Any）]：定義済みのクラスマップ基準のいずれかに一致するトラフィックをこの QoS クラスに割り当てます。 • [すべて（All）]：定義されたすべてのクラスマップ基準に一致するトラフィックのみをこの QoS クラスに割り当てます。
プロトコル	このクラス マップに含まれる 1 つ以上のプロトコル。[追加（Add）] をクリックしてセレクタを表示します。[利用可能なプロトコル（Available Protocols）] リストから 1 つ以上のアイテムを選択し、[>>] をクリックしてそれらを [選択済みのプロトコル（Selected Protocols）] リストに追加します。 コントロール プレーンで使用できるプロトコルは ARP だけです。ARP および CDP は、インターフェイス上に設定された入力クラスでは使用できません。 終了したら、[OK] をクリックして [QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [Protocol] フィールドに表示されます。 （注） QoS クラスからプロトコルを削除するには、[優先順位（Precedence）] フィールドからプロトコルを選択し、[削除（Delete）] をクリックします。

要素	説明
Precedence	このクラス マップに含まれる 1 つ以上の IP precedence（IPP）。[追加（Add）] をクリックしてセレクタを表示します。[利用可能な優先順位（Available Precedences）] リストから 1 つ以上のアイテムを選択し、[>>] をクリックしてそれらを [選択済みの優先順位（Selected Precedences）] リストに追加します。IP precedence 値の詳細については、表 908 : IP Precedence クラス （3292 ページ）を参照してください。 終了したら、[OK] をクリックして [QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [優先順位（Precedence）] フィールドに表示されます。 （注） QoS クラスから IPP 値を削除するには、[優先順位（Precedence）] フィールドから IPP 値を選択し、[削除（Delete）] をクリックします。
DSCP	このクラス マップに含まれる 1 つ以上の DiffServ コード ポイント（DSCP）値。[追加（Add）] をクリックしてセレクタを表示します。[利用可能なDSCP（Available DSCPs）] リストから 1 つ以上のアイテムを選択し、[>>] をクリックしてそれらを [選択済みDSCP（Selected DSCPs）] リストに追加します。 終了したら、[OK] をクリックして [QoSクラス（QoS Class）] ダイアログボックスに戻ります。選択内容が [DSCP] フィールドに表示されます。 （注） QoS クラスから DSCP 値を削除するには、[優先順位（Precedence）] フィールドから DSCP 値を選択し、[削除（Delete）] をクリックします。
ACL	QoS を必要とするトラフィックを定義するために使用される ACL。[編集（Edit）] をクリックして、ACL オブジェクトを追加または削除します。 上向きおよび下向き矢印を使用して、リスト内で ACL を配置します。頻繁に使用される ACL をリストの一番上に配置して、一致プロセスを最適化することを推奨します。

[Edit ACLs] ダイアログボックス - QoS クラス

Cisco IOS ルータで QoS ポリシーを設定する場合、[Edit ACLs] ダイアログボックスを使用して、選択した QoS クラスの一致基準に含める ACL を指定します。この基準に一致したトラフィックは、クラスの一部として含まれます。

拡張 ACL の名前を入力します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しいオブジェクトを作成します。複数の ACL オブジェクトはカンマで区切り、優先順に配置します。

詳細については、拡張アクセス コントロール リスト オブジェクトの作成 （357 ページ）を参照してください。

ナビゲーション パス

[QoS Class] ダイアログボックス - [Matching] タブ （3318 ページ）に移動し、[ACL] フィールドで [編集（Edit）] をクリックします。

関連項目

- QoS クラスのマッチング パラメータの定義 （3305 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- サービス品質ポリシーページ （3312 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

[QoS Class] ダイアログボックス - [Marking] タブ

[QoS Class] ダイアログボックスの [Marking] タブを使用して、パケットを分類します。トラフィック ポリサーとトラフィック シェーパーは、これらの分類を使用して、契約済みサービス レベルに適合するようにします。ダウンストリーム デバイスでは、この分類を使用してパケットを識別し、適切な QoS 機能をパケットに適用します。

（注） コントロールプレーンで QoS ポリシーを定義する場合、[マーキング（Marking）] タブは使用できません。

ナビゲーション パス

[QoS Class] ダイアログボックス （3316 ページ）に移動し、[マーキング（Marking）] タブをクリックします。

関連項目

- QoS クラスのマーキング パラメータの定義 （3307 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- サービス品質ポリシーページ （3312 ページ）

フィールド リファレンス

表 914 : [QoS Class] ダイアログボックス - [Marking] タブ

要素	説明
Enable Marking	選択すると、（トラフィックが最初にデバイスに入ったときに持っていた可能性がある値にかかわらず）このQoSクラスのトラフィックを特定のprecedence値またはDSCP 値でマークできます。このマークにより、ダウンストリームデバイスがトラフィックを識別し、適切な QoS 機能を適用できます。 選択を解除すると、選択した QoS クラスのマーキング オプションはすべてディセーブルになります。このQoSクラスのトラフィックは、元のprecedence値またはDSCP 値を保持します（ある場合）。
Precedence	このクラスのトラフィックをマークするために使用する precedence 値。 • network（7） • internet match（6） • critical（5） • flash-override（4） • flash（3） • immediate（2） • priority（1） • routine（0）
DSCP	このクラスのトラフィックをマークするために使用するDSCP値（0～63）。

[QoS Class] ダイアログボックス - [Queuing and Congestion Avoidance] タブ

[QoS Class] ダイアログボックスの [Queuing and Congestion Avoidance] タブを使用して、選択したQoSクラスの出力トラフィックでClass-Based Weighted Fair Queuing（CBWFQ; クラスベースWFQ）を実行します。キューイングによって、トラフィックに優先順位が付けられ、パケットをインターフェイスから送信する順序を決定することでネットワーク上の輻輳が管理されます。キューイングおよび輻輳回避は、出力トラフィックのインターフェイスクラスだけに適用されます。

[キューイング（Queuing）] タブに表示されるフィールドは、特定のQoSクラスを定義するか、（[デフォルトクラスとして設定（Set as Default Class）] を選択して）デフォルトクラスを定義するかによって、さらにルータのタイプや Cisco IOS ソフトウェアバージョンによって異なります。

ナビゲーション パス

[QoS Class] ダイアログボックス （3316ページ）に移動し、[キューイングおよび輻輳回避（Queuing and Congestion Avoidance）] タブをクリックします。

関連項目

- QoS クラスのキューイング パラメータの定義 （3308 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- サービス品質ポリシーページ （3312 ページ）

フィールド リファレンス

表 *915 : [QoS Class]* ダイアログボックス - *[Queuing and Congestion Avoidance]* タブ

要素	説明
Enable Queuing and Congestion Avoidance	QoS クラスでキューイングおよび輻輳回避プロパティを設定するかどうか。
プライオリティ （非デフォルト クラスだけ）	このクラスで Low-Latency Queuing（LLQ; 低遅延キューイング）を設定し、音声トラフィックなどのプライオリティ トラフィックに、定義された帯域幅が与えられるようにします（低遅延キューイング （3295 ページ）を参照）。このインターフェイス上のプライオリティが高いトラフィックに割り当てられる帯域幅の量を指定します。 • [Percentage]：有効値の範囲は 1 ～ 100% です。 • [Kbit/sec]：有効値の範囲は 8 ～ 2000000 キロビット/秒です。 （注） このオプションは、インターフェイスごとに 1 つのクラスだけに定義できます。このオプションを選択した場合、[Shaping] タブはディセーブルです。

要素	説明
Fair Queue ダイナミック キューの数 （デフォルト クラスだけ）	このクラスでクラスベース WFQ を設定します。 デバイスで 12.4(20)T よりも前の IOS ソフトウェア バージョンが実行されている場合、このクラス用に予約するダイナミック キューの数を指定する必要があります。この数は、インターフェイスの使用可能な帯域幅に基づいて指定する必要があります。2 のべき乗である 16 から 4096 までの数を指定できます。デバイスで使用されるキューのデフォルトの数については、デフォルト クラス キューイング （3295 ページ）を参照してください。キュー制限を設定しないかぎり、使用可能な帯域幅はキュー間で均等に分散されます。 **ヒント** デフォルト クラスに十分な数のキューを提供できない場合（スタベーションと呼ばれる状態）、トラフィックは送信されない場合があります。
Bandwidth	このクラスに対して保証する最小帯域幅を設定します。この量は次の単位で定義できます。 • [Percentage]：有効値の範囲は、使用可能な帯域幅全体の 1 ～ 100% です。 • [Kbit/sec]：有効値の範囲は 8 ～ 2000000 キロビット/秒です。
Enable Fair Queue （非デフォルト クラスだけ）	非デフォルト クラスの帯域幅を設定する場合、Class-Based Weighted Fair Queuing（CBWFQ; クラスベース WFQ）もイネーブルにするかどうか。デバイスによって、使用可能な帯域幅に基づいて設定するキューの数が計算され、キュー制限を設定しないかぎり、使用可能な帯域幅はキュー間で均等に分散されます。 このオプションは、アグリゲーション サービス ルータ(ASR) および 12.4(20)T 以降が実行されているルータにのみ使用できます。
キュー制限（Queue Limit）	クラスに対してキューイングできるパケットの最大数。それ以外のパケットは、輻輳が解消されるまでテール ドロップを使用してドロップされます。 Weighted Random Early Detection（WRED; 重み付けランダム早期検出）を設定しないかぎり、これがキュー サイズを制限するためのデフォルトのオプションです。

要素	説明
平均キュー深度に対するWRED重み（WRED Weight for Mean Queue Depth）	平均キューサイズの計算に使用される指数加重係数。このクラスに対してテール ドロップ（キュー制限）ではなく WRED を定義する場合に、このオプションを使用します。キューサイズがこの重み係数によって決定された値を超えると、送信プロトコルが輻輳を緩和するために送信レートを下げるまで、WRED はパケットをランダムに破棄します。指数値の範囲は 1 ～ 16 です。デフォルトは 9 です。 このオプションは、パケットがドロップされると伝送レートを下げる TCP などのプロトコルに最適です。値を変更することでアプリケーションに利点があると判断した場合を除き、デフォルト値を変更しないことを推奨します。

[QoS Class] ダイアログボックス - [Policing] タブ

[QoS Class] ダイアログボックスの [Policing] タブを使用して、選択した QoS クラスのトラフィックにレート制限を設定します。超過トラフィックはドロップされるか、または異なる（通常は低い）プライオリティで送信されます。

ナビゲーション パス

[QoS Class] ダイアログボックス （3316 ページ）に移動し、[ポリシング（Policing）] タブをクリックします。

関連項目

- QoS クラスのポリシング パラメータの定義 （3309 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- サービス品質ポリシーページ （3312 ページ）

フィールド リファレンス

表 916 : [QoS Class] ダイアログボックス - [Policing] タブ

要素	説明
[ポリシングの有効化（Enable Policing）]	選択すると、クラスベースのポリシングを設定して、このクラスのトラフィックの最大レートを制御できます。Security Manager では、2 トークン バケット アルゴリズムが使用されます。このアルゴリズムでは、どちらのバケットも着信パケットに対応できない場合に実行する違反アクションが定義されます。 選択を解除すると、選択した QoS クラスのポリシングオプションはすべてディセーブルになります。

要素	説明
CIR	平均データ レート（認定情報レートまたは CIR とも呼ぶ）。この量は次の単位で定義できます。 • [Percentage]：有効値の範囲は、使用可能な帯域幅全体の 0 ～ 100% です。 • [Bit/sec]：有効値の範囲は 8000 ～ 2000000000 ビット/秒です。 トークン バケット アルゴリズムでは、このレートは両方のトークン バケットを一杯にするトークンの到着レートを表します。このレートを下回るトラフィックは、常に適合します。 （注） コントロール プレーン ポリシングについて （3299 ページ）を設定する場合は、CIR をビット/秒単位で定義する必要があります。
[適合バースト（Conform Burst）]	通常のバースト サイズ。これにより、一部のトラフィックがレート制限を超える前に可能なトラフィック バーストの大きさが決まります。トークン バケット アルゴリズムでは、1 番めの（適合）トークンバケットの全体サイズを表します。 有効値の範囲は、CIR によって決まります。 • CIR がパーセンテージで定義されている場合：有効値の範囲は 1 ～ 2000 ミリ秒です。 • CIR が絶対値で定義されている場合：有効値の範囲は 1000 ～ 512000000 バイトです。
Excess Burst	超過バースト サイズ。これにより、すべてのトラフィックがレート制限を超える前に可能なトラフィック バーストの大きさが決まります。トークン バケット アルゴリズムでは、2 番めの（超過）トークン バケットの全体サイズを表します。 有効値の範囲は、CIR によって決まります。 • CIR がパーセンテージで定義されている場合：有効値の範囲は 1 ～ 2000 ミリ秒です。 • CIR が絶対値で定義されている場合：有効値の範囲は 1000 ～ 512000000 バイトです。

要素	説明
Conform アクション	レート制限に適合したパケットに対して実行するアクション。 • [transmit]：パケットを送信します。 • [set-prec-transmit]：IP precedence を指定された値（0 ～ 7）に設定し、パケットを送信します。コントロール プレーンでは使用できません。 • [set-dscp-transmit]：DSCP を指定した値（0 ～ 63）に設定し、パケットを送信します。コントロール プレーンでは使用できません。 • [drop]：パケットをドロップします。
Exceed アクション	レート制限を超えるが 2 番めの（超過）トークンバケットを使用して処理できるパケットに対して実行するアクション。 選択可能なアクションは、定義した適合アクションによって異なります。たとえば、適合アクションとして set オプションのいずれかを選択した場合、超過アクションとして [transmit] を選択できません。適合アクションとして [drop] を選択した場合、超過アクションにも [drop] を選択する必要があります。
[違反アクション（Violate action）]	適合バケットまたは超過バケットで処理できないパケットに対して実行するアクション。 選択可能なアクションは、定義した超過アクションによって異なります。たとえば、超過アクションとして set オプションのいずれかを選択した場合、違反アクションとして [transmit] を選択できません。超過アクションとして [drop] を選択した場合、違反アクションにも [drop] を選択する必要があります。

[QoS Class] ダイアログボックス - [Shaping] タブ

[QoS Class] ダイアログボックスの [Shaping] タブを使用して、選択した QoS クラスの出力トラフィックのレートを制御します。シェーピングでは通常、送信元のデータ レートが想定よりも高い場合はパケットを保持してフローをシェーピングするために、超過トラフィックはバッファ（キューイング メカニズム）を使用して遅延されます。

（注） コントロールプレーンで QoS ポリシーを定義するとき、インターフェイスで階層シェーピングを使用するとき、入力トラフィックの QoS クラスを定義するとき、またはプライオリティトラフィックでキューイングを実行するときは、[シェーピング（Shaping）] タブは使用できません。

ナビゲーション パス

[QoS Class] ダイアログボックス （3316 ページ）に移動し、[シェーピング（Shaping）] タブをクリックします。

関連項目

- QoS クラスのシェーピング パラメータの定義 （3311 ページ）
- インターフェイスでの QoS の定義 （3301 ページ）
- コントロール プレーンでの QoS の定義 （3303 ページ）
- サービス品質ポリシーページ （3312 ページ）

フィールド リファレンス

表 *917 : [QoS*クラス（*QoS Class***）*]* ダイアログボックス：*[*シェーピング（***Shaping***）*]* タブ**

要素	説明
Enable Shaping	選択すると、分散トラフィックシェーピング（DTS）を設定して、このクラスのトラフィックのレートを制御できます。DTS は、キューを使用して、ネットワークの輻輳の原因になるトラフィック サージをバッファリングします。 選択を解除すると、選択した QoS クラスのシェーピング オプションはすべてディセーブルになります。 （注） シェーピングは出力トラフィックでだけ実行できます。
タイプ（Type）	実行するシェーピングのタイプ。 • [Average]：各間隔のデータ レートを、平均バースト レート（認定バースト レートまたは Bc とも呼ばれる）に制限し、平均レートが Committed Information Rate（CIR; 認定情報レート）を超えないようにします。追加のパケットは、送信できるようになるまでバッファに格納されます。 • [Peak]：各間隔のデータ レートを、平均バースト レートに超過バースト レート（Be）を加算したレートに制限します。追加のパケットは、送信できるようになるまでバッファに格納されます。
CIR	平均データ レート（認定情報レートまたは CIR とも呼ぶ）。この量は次の単位で定義できます。 • [Percentage]：有効値の範囲は、使用可能な帯域幅全体の 0 ～ 100% です。 • [Bit/sec]：有効値の範囲は 8000 ～ 1000000000 ビット/秒で、8000 の倍数である必要があります。 ある間隔中のデータ バーストはこのレートを超過することがありますが、間隔の多重積分の平均データ レートはこのレートを超過しません。

要素	説明
Sustained Burst	通常のバースト サイズ。シェーピング タイプとして平均を選択した場合は、1 間隔中のデータ バーストがこの値に制限されます。 有効値の範囲は、CIR によって決まります。 • CIR がパーセンテージで定義されている場合：有効値の範囲は 10 ～ 2000 ミリ秒です。 • CIR が絶対値で定義されている場合：有効値の範囲は 1000 ～ 154400000 バイトで、128 バイトの倍数です。 （注） CIR が絶対値で定義されている場合は、このフィールドをブランクのままにすることを推奨します。これにより、デバイスで使用されているアルゴリズムが最適な平均バースト値を決定できます。
Excess Burst	超過バースト サイズ。シェーピング タイプとしてピークを選択した場合、1 間隔中のデータ バーストは、平均バースト値とこの値の合計と等しくなることができます。ただし、複数間隔の平均データ レートは、CIR に準拠します。 有効値の範囲は、CIR によって決まります。 • CIR がパーセンテージで定義されている場合：有効値の範囲は 10 ～ 2000 ミリ秒です。 • CIR が絶対値で定義されている場合：有効値の範囲は 1000 ～ 154400000 バイトで、128 バイトの倍数です。 （注） CIR が絶対値で定義されているときにこのフィールドを設定しない場合、持続的バースト値が使用されます。

第 67 章

ルーティング ポリシーの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

この章は次のトピックで構成されています。

- Cisco IOS ルータにおける BGP ルーティング （3331 ページ）
- [BGP] ルーティング ポリシー ページ （3335 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）
- [EIGRP] ルーティング ポリシー ページ （3346 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）
- [OSPF Interface] ポリシー ページ （3368 ページ）
- [OSPF Process] ポリシー ページ （3374 ページ）
- Cisco IOS ルータにおける RIP ルーティング （3384 ページ）
- [RIP] ルーティング ポリシー ページ （3388 ページ）
- Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）
- [Static Routing] ポリシー ページ （3396 ページ）

Cisco IOS ルータにおける BGP ルーティング

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

BGP は、Autonomous System（AS; 自律システム）間でのルーティング情報のループフリー交換を保証する Exterior Gateway Protocol（EGP; エクステリア ゲートウェイ プロトコル）です。BGP システムの主要な機能は、到達可能なネットワークに関する情報（AS パス情報など）を他の BGP システムと交換することです。この情報を使用して AS 接続のグラフを作成できま

す。このグラフを使用して、ルーティング ループを排除し、AS レベルのポリシーを決定できます。

BGP は、インターネット上で使用されるルーティング プロトコルであり、インターネット サービス プロバイダー間で一般的に使用されています。このレベルでスケーラビリティを実現するために、BGP は複数のルート パラメータ（属性）を使用して、ルーティング ポリシーを定義し、安定したルーティング環境を維持します。また、BGP は Classless InterDomain Routing（CIDR）を使用して、インターネット ルーティング テーブルのサイズを大幅に削減しています。

BGP ルートは、ネットワーク番号、情報が通過した AS のリスト（自律システムパスと呼ばれる）、および定義されたパス属性で構成されます。

BGP ルータは、ネイバーとして定義されたルータだけとルーティング情報を交換します。BGP ネイバーは、ルータ間で TCP 接続が確立されたときに、完全なルーティング情報を交換します。更新は、ルーティング テーブルの変更が検出された場合にだけネイバーに送信されます。BGP ルータでは、定期的な更新は送信されません。

ここでは、BGP ルーティング ポリシーを作成するために実行するタスクについて説明します。

- BGP ルートの定義 （3332 ページ）
- BGP へのルートの再配布 （3334 ページ）

（注） Security Manager では、RFC 1163、1267、および 1771 で規定されているバージョン 2、3、および 4 の BGP がサポートされます。

関連項目

- Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）
- Cisco IOS ルータにおける RIP ルーティング （3384 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）

BGP ルートの定義

BGP ルーティング ポリシーを設定する場合は、すべての EGP と同様に、ルータとそのネイバーとの関係を定義する必要があります。BGP では、内部（同じ AS 内に配置）と外部（異なる AS 内に配置）という 2 種類のネイバーがサポートされます。通常、外部ネイバーは相互に隣接しており、サブネットを共有しています。内部ネイバーは同じ AS 内の任意の場所に存在できます。

また、次のオプション機能をイネーブルにするかどうかを選択できます。

- 自動サマライズ

- 同期
- ネイバー ロギング

自動サマライズを有効にすると、OSPF や EIGRP などの内部ゲートウェイプロトコル（IGP）から BGP にサブネットが再配布されるときに、ネットワークルートだけが挿入されます。同期は、1 つの AS から別の AS にトラフィックを渡す媒介として AS が機能する場合に役立ちます。同期によって、アドバタイズするルートに関して AS の一貫性が確保されるためです。たとえば、ネットワーク内のすべてのルータが IGP を介してルートを学習する前に BGP がルートをアドバタイズすると、一部のルータでまだルーティングできないトラフィックを AS が受信する可能性があります。ネイバーロギングでは、BGP ネイバーがリセットされた場合、到達不能になった場合、またはネットワークへの接続を復元した場合に、ルータは BGP ネイバーによって発行されたメッセージを追跡できます。

ここでは、BGP ルートを定義する方法について説明します。各ルータで定義できる BGP ルートは 1 つだけです。

関連項目

- BGP へのルートの再配布 （3334 ページ）
- Cisco IOS ルータにおける BGP ルーティング （3331 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [BGP] を選択し、作業領域の [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [BGP] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

BGP の [Setup] が表示されます。このタブのフィールドの説明については、表 918 : BGP の [Setup] タブ（3336 ページ）を参照してください。

ステップ 2 BGP の [Setup] タブで、ルータが属する AS 番号を入力します。

ステップ 3 （任意）この AS に対してローカルなネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用できます。または [選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 4 ルータの外部および内部 BGP ネイバーを定義します。

a) [ネイバー（Neighbors）] の下にある [追加（Add）] をクリックして、[BGPネイバー（BGP Neighbors）] ダイアログボックスを表示します。このダイアログボックスのフィールドの説明については、表 919 : [Neighbors] ダイアログボックス （3338 ページ）を参照してください。

b) AS 番号を入力し、[選択（Select）] をクリックして、定義されている AS 内のネイバーであるホストを選択します。内部ネイバーはルータと同じ AS 内に配置されており、外部ネイバーは異なる AS 内に配置されています。

c) [OK] をクリックして定義を保存し、[BGPネイバー（BGP Neighbors）] ダイアログボックスに戻ります。

d) （任意）4.b（3333 ページ）～4.c（3334 ページ）を繰り返して、その他の AS 内のネイバーを定義します。

（注） BGP ネイバーを定義する場合、IP アドレスは選択したルータのインターフェイスに属することができません。また、複数の AS に同じ IP アドレスは定義できません。

終了したら、[BGPネイバー（BGP Neighbors）] ダイアログボックスの [OK] をクリックして [BGPのセットアップ（BGP Setup）] タブに戻ります。選択内容が [Neighbors] フィールドに表示されます。

ステップ 5 （任意）[Auto-Summary] チェックボックスをオンにして、自動サマライズをイネーブルにします。自動サマライズをイネーブルにすると、サブネットが IGP（OSPF や EIGRP など）から BGP に再配布されるときに、ネットワーク ルートだけが BGP テーブルに注入されます。

ステップ 6 （任意）[同期（Synchronization）] チェックボックスをオンにして、BGP を IGP と同期します。この機能をイネーブルにすると、BGP は、IGP がルーティング情報を AS 全体に伝播するまで待機します。

AS が 1 つの AS から受信したトラフィックを別の AS に渡さない場合、または AS 内のすべてのルータが BGP を実行している場合、同期は必要ありません。同期をディセーブルにすると、BGP の収束が速くなります。

ステップ 7 （任意）[ネイバーのロギング（Log-Neighbor）] チェックボックスをオンにして、BGP ネイバーのリセット、起動、またはダウン時に生成されるメッセージのロギングをイネーブルにします。

BGP へのルートの再配布

再配布とは、BGP などのルーティング プロトコルを使用して、他の方法（別のルーティング プロトコルなど）で学習されたルート、スタティック ルート、または直接接続されたルートをアドバタイズすることです。たとえば、OSPF ルーティング プロトコルから BGP 自律システム（AS）にルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベース ルーティング プロトコルに適用できます。

はじめる前に

- BGP AS を定義します。 BGP ルートの定義 （3332 ページ） を参照してください。

関連項目

- BGP ルートの定義 （3332 ページ）
- Cisco IOS ルータにおける BGP ルーティング （3331 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）]>[BGP] を選択し、作業領域の [再配布（Redistribution）] タブをクリックします。

- （ポリシービュー）ポリシータイプセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [BGP] を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[再配布（Redistribution）] タブをクリックします。

BGP の [Redistribution] タブが表示されます。このタブのフィールドの説明については、表 920 : BGP の [Redistribution] タブ （3339 ページ）を参照してください。

ステップ 2 BGP の [再配布（Redistribution）] タブで、[BGP 再配布マッピング（BGP Redistribution Mappings）] テーブルから行を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてマッピングを作成します。[BGP Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 921 : [BGP Redistribution Mapping] ダイアログボックス （3340 ページ）を参照してください。

ステップ 3 BGP にルートを再配布するプロトコルを選択します。

（注） スタティック ルート、RIP ルート、EIGRP AS、および OSPF プロセスごとに 1 つのマッピングを作成できます。

ステップ 4 （任意）再配布されたルートのデフォルトのメトリック（コスト）を修正します。メトリックによって、ルートのプライオリティが決まります。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。再配布マッピングが、BGP の [Redistribution] タブの [Redistribution Mapping] テーブルに表示されます。

[BGP] ルーティング ポリシー ページ

ボーダー ゲートウェイ プロトコル（BGP）は、複数の自律システムまたはドメイン間でルーティングを実行し、ルーティングおよび到着可能性情報を他の BGP システムと交換する Exterior Gateway Protocol（EGP; エクステリア ゲートウェイ プロトコル）です。BGP は、インターネット上でルーティング情報を交換するために使用され、インターネット サービス プロバイダー間で使用されるプロトコルです。

[BGP] ルーティング ページの次のタブから、BGP ルーティング ポリシーを設定できます。

- [BGP] ページ - [Setup] タブ （3336 ページ）
- [BGP] ページ - [Redistribution] タブ （3338 ページ）

詳細については、Cisco IOS ルータにおける BGP ルーティング （3331 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [BGP] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [BGP] を選択します。[BGP] を右クリックしてポリシーを作成するか、共有ポリシーセレクタから既存のポリシーを選択します。

[BGP] ページ - [Setup] タブ

BGP の [Setup] タブを使用して、選択したルータが配置されている自律システム（AS）の番号を定義します。次に、AS に含まれるネットワークと、ルータの内部ネイバーおよび外部ネイバーであるネットワークを定義する必要があります。さらに、BGP と OSPF や EIGRP などの Interior Gateway Protocol（IGP）間の相互作用を制御するオプションをイネーブルまたはディセーブルにすることができます。3 番めのオプションを使用して、BGP ネイバーからのメッセージのロギングをイネーブルにします。

ナビゲーション パス

[BGP] ルーティング ポリシー ページ （3335 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- BGP ルートの定義 （3332 ページ）
- [BGP] ページ - [Redistribution] タブ （3338 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

フィールド リファレンス

表 918 : BGP の [Setup] タブ

要素	説明
AS 番号（AS Number）	ルータが配置されている自律システムの数。有効な値の範囲は 1 ～ 65535 です。この番号によって、BGP ルーティング プロセスがイネーブルになります。 BGP がデバイスですでに設定されている場合、この番号を変更して展開することはできません。AS 番号を変更する必要がある場合は、最初に BGP ポリシーの割り当てを解除し、変更を展開し（したがって BGP 設定をデバイスから削除し）、新しい番号で BGP ポリシーを設定して、設定を再展開します。
ネットワーク	BGP ルートに関連付けられるネットワーク。1 つ以上のネットワーク アドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 （注） ルートからネットワークを削除するには、[ネットワーク（Network）] フィールドからネットワークを選択し、[削除（Delete）] をクリックします。

要素	説明
ネイバー	ルータの内部ネイバー（ルータと同じ AS 内に配置）および外部ネイバー（異なる AS 内に配置）。[Neighbors] ダイアログボックス （3337 ページ）を参照してください。
自動集約（Auto-Summary）	選択すると、自動サマライズがイネーブルになります。サブネットが IGP（RIP、OSPF、EIGRP など）から BGP に再配布されるときに、この BGP バージョン 3 機能によってネットワーク ルートだけが BGP テーブルに注入されます。自動サマライズによって、ルータで保持する必要があるルーティング テーブルのサイズと複雑さが低減します。 選択解除されている場合、自動サマライズはディセーブルになります。これがデフォルトです。
同期	選択すると、同期がイネーブルになります。この機能を使用して、アドバタイズするルートに関してネットワーク内のすべてのルータの一貫性が確保されるようにします。同期によって、BGP は、IGP がルーティング情報を AS 全体に伝播するまで待機します。 選択を解除すると、同期がディセーブルになります。このルータが別の AS からのトラフィックを第三の AS に渡さない場合、または AS 内のすべてのルータが BGP を実行している場合、同期をディセーブルにすることができます。この機能をディセーブルにすると、IGP が伝送する必要があるルートの数が減少し、コンバージェンス時間が向上するという利点があります。これがデフォルトです。
Log-Neighbor	選択すると、BGP ネイバーのリセット、ネットワークへの接続、または切断時に生成されるメッセージのロギングがイネーブルになります。これがデフォルトです。 選択を解除すると、メッセージ ロギングがディセーブルになります。

[Neighbors] ダイアログボックス

[Neighbors] ダイアログボックスを使用して、選択したルータの内部および外部ネイバーを定義します。

ナビゲーション パス

[BGP] ページ - [Setup] タブ （3336 ページ）に移動してから、[ネイバー（Neighbors）] フィールドにある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- BGP ルートの定義 （3332 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）

- ネットワーク/ホストオブジェクトについて （391 ページ）

フィールド リファレンス

表 *919 : [Neighbors]* ダイアログボックス

要素	説明
AS 番号（AS Number）	BGP ネイバーを含む AS の番号。内部ネイバーは、選択したルータのネットワークと同じ AS 番号を持ちます。外部ネイバーは、異なる AS 番号を持ちます。
IPアドレス	ルータのネイバーであるホストの IP アドレス。ルーティング テーブルの変更が検出されると常に、BGP ネイバーは相互にルーティング情報を交換します。 BGP ネイバーを定義する場合、IP アドレスは選択したルータのインターフェイスに属することができません。また、複数の AS に同じ IP アドレスは定義できません。 1 つ以上のアドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） BGP ネイバーのリストからホストを削除するには、[ホスト（Hosts）] フィールドからホストを選択し、[削除（Delete）] をクリックします。

[BGP] ページ - [Redistribution] タブ

BGP の [Redistribution] タブを使用して、BGP 自律システム（AS）への再配布を実行するときの再配布設定を表示、作成、編集、および削除します。

（注） RIP の [再配布（Redistribution）] タブにアクセスする前に、RIP 設定パラメータを定義する必要があります。 [BGP] ページ - [Setup] タブ （3336 ページ）を参照してください。

ナビゲーション パス

[BGP] ルーティング ポリシー ページ （3335 ページ）に移動し、[再配布（Redistribution）] タブをクリックします。

関連項目

- BGP へのルートの再配布 （3334 ページ）
- [BGP] ページ - [Setup] タブ （3336 ページ）

- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *920 : BGP* の *[Redistribution]* タブ

要素	説明
プロトコル	再配布されているプロトコル。
[AS/プロセスID（AS/Process ID）]	再配布されているルートの AS 番号またはプロセス ID。
メトリック （Metric）	再配布されるルートのプライオリティを決定する値。
一致（Match）	OSPFプロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。
[静的タイプ（Static Type）]	スタティック ルートを再配布する場合、スタティック ルートのタイプ（IP または OSI）を指定します。
[追加（Add）] ボタン	[BGP Redistribution Mapping] ダイアログボックス （3339 ページ）が開きます。ここから、BGP再配布マッピングを定義できます。
[編集（Edit）] ボタン	[BGP Redistribution Mapping] ダイアログボックス （3339 ページ）が開きます。ここから、選択した BGP 再配布マッピングを編集できます。
[削除（Delete）] ボタン	選択したBGP再配布マッピングをテーブルから削除します。

[BGP Redistribution Mapping] ダイアログボックス

[BGP再配布マッピング（BGP Redistribution Mapping）] ダイアログボックスを使用して、BGP再配布マッピングのプロパティを追加または編集します。

ナビゲーション パス

[BGP] ページ - [Redistribution] タブ （3338 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- BGP へのルートの再配布 （3334 ページ）

フィールド リファレンス

表 *921 : [BGP Redistribution Mapping]* ダイアログボックス

要素	説明
Protocol to Redistribute	再配布されているルーティング プロトコル。 • [スタティック（Static）]：IP または OSI スタティックルートを再配布します。ルートごとに 1 つのマッピングを定義できます。 • [EIGRP]：EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに 1 つのマッピングを定義できます。 • [RIP]：RIP ルートを再配布します。ルートごとに 1 つのマッピングを定義できます。 • [OSPF]：別の OSPF プロセスを再配布します。プロセスごとに 1 つのマッピングを定義できます。表示されるリストからプロセスを選択し、1 つ以上の一致基準を選択します。 • [Internal]：特定の AS の内部のルート。 • [External1]：AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1]：AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area（NSSA）ルート。 • [NSAAExternal2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる（NSSA）ルート。 • [Connected]：インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。
メトリック（Metric）	再配布されるルートのコストを表す値。有効値の範囲は、0 ～ 4294967295 です。

Cisco IOS ルータにおける EIGRP ルーティング

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

Enhanced Interior Gateway Routing Protocol（EIGRP）は、シスコが開発した、リンクステート プロトコルの機能を統合する拡張距離ベクトル型プロトコルです。EIGRP は、数多くのさまざまなトポロジおよびメディアに適しています。他のルーティング プロトコルとは異なる EIGRP の重要な機能としては、高速コンバージェンスの実現、可変長サブネット マスク、部分的なアップデート、および複数のネットワーク層プロトコルのサポートがあります。

宛先に到達するため、および他のルータにアドバタイズするためにルータが使用するメトリックは、すべてのネイバーから最適にアドバタイズされたメトリックと最適なネイバーへのリンク コストの合計です。

EIGRP はネイバーテーブルを使用して、ルータの各ネイバーに関するアドレスおよびインターフェイス情報を格納します。hello パケットによってホールド時間がアドバタイズされます。これは、ネイバーを到達可能および動作可能と見なすことができる時間です。トポロジテーブルには、ネイバールータでアドバタイズされたすべての宛先が含まれます。アドバタイズされたメトリックがネイバーごとにエントリに記録され、ネイバーによってそのルーティングテーブルに格納されます。

EIGRP を実行しているルータには、代替ルートに迅速に適応できるように、ネイバーすべてのルーティングテーブルが格納されます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP は、ルーティングテーブルの内容全体を送信する代わりに、宛先の状態が変わったときに差分更新を送信します。EIGRP では、情報を必要とするルータだけが更新されます。この機能により、EIGRP パケットに必要な帯域幅が最小限に抑えられます。

EIGRP は、内部ルートと外部ルートの両方をサポートします。内部ルートは、EIGRP 自律システム（AS）内で発生します。したがって、EIGRP を実行するように設定された直接接続されているネットワークは内部ルートと見なされ、AS 全体にこの情報とともに伝達されます。外部ルートとは、他のルーティングプロトコルによって学習されたルート、またはルーティングテーブルにスタティックルートとして存在するルートです。外部ルートは、生成元の ID によって個別にタグ付けされます。

ここでは、EIGRP ルーティング ポリシーを作成するために実行するタスクについて説明します。

- EIGRP ルートの定義　（3342 ページ）
- EIGRP インターフェイスのプロパティの定義　（3343 ページ）
- EIGRP へのルートの再配布　（3345 ページ）

関連項目

- Cisco IOS ルータにおけるスタティック ルーティング　（3394 ページ）
- Cisco IOS ルータにおける RIP ルーティング　（3384 ページ）
- Cisco IOS ルータにおける OSPF ルーティング　（3355 ページ）
- Cisco IOS ルータにおける BGP ルーティング　（3331 ページ）

EIGRP ルートの定義

EIGRP ルーティング ポリシーを定義するには、各自律システムに番号を割り当てる必要があります。この番号によって、自律システムは他のルータで識別されます。次に、ルートを作成するネットワークを選択する必要があります。さらに、どのインターフェイスが受動かを選択できます。他のルーティングプロトコルとは異なり、EIGRP のパッシブインターフェイスは、ネイバーとの間でルーティング更新を送受信しないため、ネイバー関係が失われます。

EIGRP ルーティングポリシーの設定時に、自動集約を有効にするか決めることもできます。有効にすると、単一のネットワークエントリで多数のサブネットを表すことで、ルーティングテーブルとルーティング情報の交換が大幅に簡素化されます。

関連項目

- EIGRP インターフェイスのプロパティの定義 （3343 ページ）
- EIGRP へのルートの再配布 （3345 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[ルーティング（Routing）] > [EIGRP]** を選択し、作業領域の [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

EIGRP の [Setup] タブが表示されます（[EIGRP] ページ : [セットアップ（Setup）] タブ （3347 ページ）を参照）。

ステップ 2 EIGRP の [セットアップ（Setup）] タブで、テーブルから EIGRP ルートを選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてルートを作成します。[EIGRP Setup] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 923 : [EIGRPのセットアップ（EIGRP Setup）] ダイアログボックス （3348 ページ）を参照してください。

ステップ 3 ルートの自律システム番号を入力します。この番号によって、自律システムは他のルータに対して識別されます。

ステップ 4 EIGRP ルートに含めるネットワークのアドレスを入力します。アドレスとネットワーク/ホスト オブジェクトの組み合わせを使用するか、アドレスをカンマで区切ることができます。[選択（Select）] をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、または新しいネットワーク/ホストオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 5 受動インターフェイスのアドレスを入力します。これは、ネイバーにルーティング更新（存在する場合）を送信しないインターフェイスです。1 つ以上のインターフェイスの名前またはインターフェイスのロールを入力します。アドレスをカンマで区切ります。[選択（Select）] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、または新しいインターフェイス ロール オブ

ジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 6 （任意）[自動集約（Auto-Summary）] をオンにして、ネットワーク レベル ルートへのサブネット ルートの自動集約を有効にします。サマライズによってルーティング テーブルのサイズが削減されるため、ネットワークの複雑さが低減します。

ステップ 7 [OK] をクリックして定義を保存します。EIGRP ルートが、EIGRP の [Setup] タブに表示されるテーブルに表示されます。

EIGRP インターフェイスのプロパティの定義

任意で、選択した EIGRP 自律システムの次の 2 つのインターフェイス プロパティのデフォルト値を変更できます。

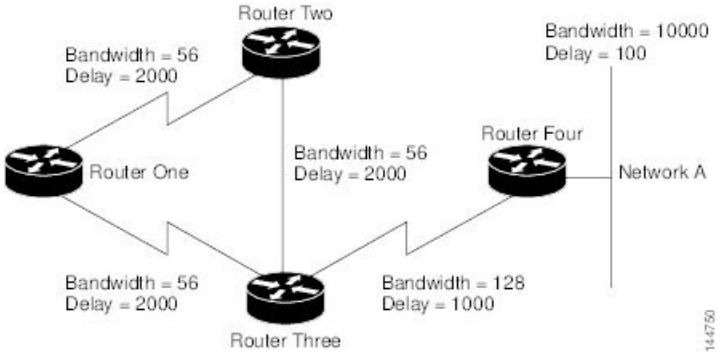
- hello 間隔
- スプリット ホライズン。

hello 間隔によって、hello パケット間の間隔が定義されます。ルーティング デバイスは、これらのパケットを相互に定期的に送信して、直接接続されたネットワーク上の他のルータについて動的に学習します。この情報は、ネイバーを検出したり、ネイバーが到達不能または動作不能になったことを学習したりするために使用されます。デフォルトでは、hello パケットは 5 秒間隔で送信されます。低速（T1 以下）の NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）メディアのデフォルトの間隔は、60 秒ごとです。

スプリット ホライズンは、ルート情報がその情報の発生元の方向に返送されないようにする機能です。スプリット ホライズンをインターフェイスでイネーブルにした場合（これがデフォルトです）、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップである宛先に送信されません。これは、ルーティング ループを防止するのに役立ちます。

たとえば、図 57 : EIGRP スプリット ホライズンの例 （3344 ページ）に示すように、ルータ 1 がルータ 2 および 3 に 1 つのマルチポイント インターフェイスで接続され、ルータ 1 がルータ 2 からネットワーク A について学習した場合、ルータ 1 は、その同じマルチポイント インターフェイスでネットワーク A へのルートをルータ 3 にアドバタイズしません。ルータ 1 では、ルータ 3 はネットワーク A についてルータ 2 から直接学習すると想定します。

図 *57 : EIGRP* スプリット ホライズンの例



スプリットホライズンは、すべてのEIGRPインターフェイスでデフォルトでイネーブルです。通常は、スプリット ホライズンによって、複数のルーティング デバイス間の通信が最適化されるためです。ただし、非ブロードキャスト ネットワーク（フレームリレーや SMDS など）では、スプリットホライズンをディセーブルにする必要がある場合があります。

EIGRPインターフェイスでスプリットホライズンをディセーブルにする場合は、次の点に注意してください。

- ハブアンドスポーク ネットワークでは、ハブだけでスプリット ホライズンをディセーブルにする必要があります。これは、スポークでスプリットホライズンをディセーブルにすると、ハブルータの EIGRP メモリ消費量が大幅に増加するだけでなく、スポークルータで生成されるトラフィックの量も増加するためです。
- インターフェイスでスプリットホライズン設定を変更すると、そのインターフェイスで到達可能な EIGRP ネイバーとの隣接関係はすべてリセットされます。

はじめる前に

- 少なくとも1つのEIGRP自律システムを定義します。EIGRP ルートの定義 （3342 ページ）を参照してください。

関連項目

- EIGRP ルートの定義 （3342 ページ）
- EIGRP へのルートの再配布 （3345 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[ルーティング（Routing）] > [EIGRP]** を選択し、作業領域の [インターフェイス（Interfaces）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[インターフェイス（Interface）] タブをクリックします。

[EIGRPインターフェイス（ EIGRP Interfaces）] タブが表示されます。このタブのフィールドの説明については、表 924 : EIGRP の [Interfaces] タブ （3350 ページ）を参照してください。

ステップ 2 EIGRP の [インターフェイス（Interfaces）] タブで、テーブルからインターフェイスを選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてインターフェイス定義を作成します。[EIGRPインターフェイス（EIGRP Interface）] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 925 : [EIGRP Interface] ダイアログボックス （3351 ページ）を参照してください。

ステップ 3 インターフェイス プロパティを変更する自律システムの AS 番号を選択します。自律システムの定義の詳細については、EIGRP ルートの定義 （3342 ページ）を参照してください。

ステップ 4 定義するインターフェイスの名前またはインターフェイスロールを入力します。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 5 （任意）[Hello Interval] フィールドで、選択したインターフェイスで送信される hello パケット間のデフォルトの間隔を変更します。

デフォルトの間隔が 60 秒の低速（T1 以下）の NBMA メディアを除き、すべてのインターフェイスでデフォルトは 5 秒です。

ステップ 6 （任意）[スプリットホライズン（Split Horizon）] チェックボックスをオフにして、スプリットホライズン機能をディセーブルにします。この機能をディセーブルにすると、選択したインターフェイスで、ルートの学習元のインターフェイスからそのルートをアドバタイズできます。

（注） 一般に、変更によってルートが正しくアドバタイズされることがアプリケーションにとって必要であることが確実な場合以外は、スプリット ホライズンをディセーブルにしないことを推奨します。シリアルインターフェイスでスプリット ホライズンをディセーブルにし、そのインターフェイスがパケット スイッチド ネットワークに接続されている場合、そのネットワーク上のすべての関連するマルチキャスト グループ内のすべてのルータおよびアクセス サーバに対して、スプリット ホライズンをディセーブルにする必要があります。

ステップ 7 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。インターフェイス定義は、[EIGRPインターフェイス（EIGRP Interface）] タブのテーブルに表示されます。

EIGRP へのルートの再配布

再配布とは、EIGRP などのルーティング プロトコルを使用して、他の方法（別のルーティング プロトコルなど）で学習されたルート、スタティック ルート、または直接接続されたルートをアドバタイズすることです。たとえば、RIP ルーティング プロトコルから EIGRP 自律システム（AS）にルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベース ルーティング プロトコルに適用できます。

はじめる前に

- 少なくとも 1 つの EIGRP 自律システムを定義します。EIGRP ルートの定義 （3342 ページ）を参照してください。

関連項目

- EIGRP ルートの定義 （3342 ページ）
- EIGRP インターフェイスのプロパティの定義 （3343 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[ルーティング（Routing）] > [EIGRP]** を選択し、作業領域の [再配布（Redistribution）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[再配布（Redistribution）] タブをクリックします。

EIGRP の [Redistribution] タブが表示されます。このタブのフィールドの説明については、表 926 : EIGRP の [Redistribution] タブ （3352 ページ）を参照してください。

ステップ 2 EIGRP の [再配布（Redistribution）] タブで、[EIGRP再配布マッピング（EIGRP Redistribution Mappings）] テーブルから行を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてマッピングを作成します。[EIGRP Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 927 : [EIGRP再配布マッピング（EIGRP Redistribution Mapping）] ダイアログボックス （3353 ページ）を参照してください。

ステップ 3 表示されるリストから既存の EIGRP AS を選択します。

ステップ 4 選択した EIGRP AS にルートを再配布するプロトコルを選択します。

（注） スタティック ルート、RIP ルート、BGP AS、EIGRP AS、および OSPF プロセスごとに 1 つのマッピングを作成できます。

ステップ 5 （任意）[Metrics] で、メトリックの計算に使用されるフィールドに値を入力して、再配布されるルートのデフォルトのメトリック（コスト）を変更します。メトリックによって、ルートのプライオリティが決まります。

（注） メトリックの入力は任意ですが、値を指定する場合は、5 つのパラメータすべての値を入力する必要があります。1 つの EIGRP プロセスを別の EIGRP プロセスに再配布する場合は、メトリック値を定義する必要はありません。

ステップ 6 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。再配布マッピングが、EIGRP の [再配布（Redistribution）] タブの [再配布マッピング（Redistribution Mapping）] テーブルに表示されます。

[EIGRP] ルーティング ポリシー ページ

Enhanced Interior Gateway Routing Protocol（EIGRP）は、最小のネットワーク トラフィックで非常に迅速なコンバージェンス時間を提供するスケーラブルな Interior Gateway Protocol です。

[EIGRP] ルーティング ページの次のタブから、EIGRP ルーティング ポリシーを設定できます。

- [EIGRP] ページ：[セットアップ（Setup）] タブ （3347 ページ）
- [EIGRP] ページ：[インターフェイス（Interfaces）] タブ （3349 ページ）
- [EIGRP] ページ - [Redistribution] タブ （3351 ページ）

詳細については、Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）を参照してください。

ナビゲーション パス

- （デバイス ビュー）ポリシー セレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [EIGRP] を選択します。
- （ポリシー ビュー）ポリシー タイプ セレクタから **[ルータ プラットフォーム（Router Platform）] > [ルーティング（Routing）] > [EIGRP]** を選択します。[EIGRP] を右クリックしてポリシーを作成するか、または共有ポリシー セレクタから既存ポリシーを選択します。

[EIGRP] ページ：[セットアップ（Setup）] タブ

EIGRP の [Setup] タブを使用して、EIGRP ルートを表示、作成、編集、および削除します。

ナビゲーション パス

[EIGRP] ルーティング ポリシー ページ （3346 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- EIGRP ルートの定義 （3342 ページ）
- [EIGRP] ページ：[インターフェイス（Interfaces）] タブ （3349 ページ）
- [EIGRP] ページ - [Redistribution] タブ （3351 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *922 : EIGRP* の *[セットアップ（Setup）]* タブ

要素	説明
AS 番号（AS Number）	自律システムを他のルータに対して識別する自律システム番号。

要素	説明
ネットワーク	ルートに含まれるネットワークの名前。
パッシブインターフェイス	ルーティング更新をネイバーと送受信しないインターフェイス。
自動集約（Auto-Summary）	選択したルートで自動サマライズがアクティブかどうかを指定します。
[追加（Add）] ボタン	[EIGRPのセットアップ（EIGRP Setup）] ダイアログボックス（3348ページ）が開きます。ここから、EIGRPルートを作成できます。
[編集（Edit）] ボタン	[EIGRPのセットアップ（EIGRP Setup）] ダイアログボックス（3348ページ）が開きます。ここから、選択したEIGRPルートを編集できます。
[削除（Delete）] ボタン	選択した EIGRP ルートをテーブルから削除します。

[EIGRPのセットアップ（EIGRP Setup）] ダイアログボックス

[EIGRP Setup] ダイアログボックスを使用して、EIGRP ルートを追加または編集します。

ナビゲーション パス

[EIGRP] ページ：[セットアップ（Setup）] タブ （3347ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- EIGRP ルートの定義 （3342 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

フィールド リファレンス

表 *923 : [EIGRP*のセットアップ（*EIGRP Setup***）*]* ダイアログボックス**

要素	説明
AS 番号（AS Number）	EIGRP ルートの自律システム番号。この番号は、自律システムを他のルータで識別するために使用されます。有効値は 1 ～ 65535 です。

要素	説明
ネットワーク	EIGRP ルートに関連付けられたネットワーク。1 つ以上のネットワーク アドレスまたはネットワーク/ホスト オブジェクトをカンマで区切って入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成します。
パッシブ インターフェイス	ルーティング ネイバーに更新を送信しないインターフェイス。1 つ以上のインターフェイス名またはロールをカンマで区切って入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイス ロール オブジェクトを作成します。 （注） インターフェイスを受動にすると、EIGRP によってルータ間の hello パケットの交換は抑止され、ネイバー関係は失われます。これにより、ルーティング更新のアドバタイズが停止されるだけでなく、着信するルーティング更新も抑止されます。
自動集約（Auto-Summary）	選択されている場合は、ネットワーク レベル ルートへのサブネット ルートの自動サマライズをイネーブルにします。サマライズによってルーティング テーブルのサイズが削減されるため、ネットワークの複雑さが低減します。 選択解除されている場合、自動サマライズはディセーブルになります。

[EIGRP] ページ：[インターフェイス（Interfaces）] タブ

EIGRP の [Interfaces] タブを使用して、選択した EIGRP 自律システムのインターフェイス プロパティを作成、編集、および削除します。デフォルトの hello 間隔の変更やスプリット ホライズンをディセーブルにすることも含まれます。

（注） EIGRP の [Interfaces] タブには、[Setup] タブで少なくとも 1 つの EIGRP 自律システムを定義したあとにだけアクセスできます。[EIGRP] ページ：[セットアップ（Setup）] タブ（3347 ページ）を参照してください。

ナビゲーション パス

[EIGRP] ルーティング ポリシー ページ （3346 ページ）に移動し、[インターフェイス（Interfaces）] タブをクリックします。

関連項目

• EIGRP インターフェイスのプロパティの定義 （3343 ページ）

- [EIGRP] ページ：[セットアップ（Setup）] タブ （3347 ページ）
- [EIGRP] ページ - [Redistribution] タブ （3351 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *924 : EIGRP* の *[Interfaces]* タブ

要素	説明
AS 番号（AS Number）	インターフェイス プロパティが定義される EIGRP 自律システム番号。
インターフェイス	選択した EIGRP 自律システムに関連する、特に定義された値を持つインターフェイス。
Split Horizon	選択したインターフェイスに対してスプリット ホライズン機能がイネーブルかディセーブルかを指定します。
Hello 間隔（Hello Interval）	ネイバールータに送信される hello パケット間の定義済みインターバル。
[追加（Add）] ボタン	[EIGRP Interface] ダイアログボックス （3350 ページ）が開きます。ここから、EIGRP インターフェイス定義を作成できます。
[編集（Edit）] ボタン	[EIGRP Interface] ダイアログボックス （3350 ページ）が開きます。ここから、選択した EIGRP インターフェイス定義を編集できます。
[削除（Delete）] ボタン	選択した EIGRP インターフェイス定義をテーブルから削除します。

[EIGRP Interface] ダイアログボックス

[EIGRP Interface] ダイアログボックスを使用して、選択した EIGRP 自律システムのインターフェイス定義を追加または編集します。

ナビゲーション パス

[EIGRP] ページ：[インターフェイス（Interfaces）] タブ （3349 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- EIGRP インターフェイスのプロパティの定義 （3343 ページ）

- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *925 : [EIGRP Interface]* ダイアログボックス

要素	説明
AS 番号（AS Number）	インターフェイス プロパティを変更する EIGRP 自律システム番号を選択します。EIGRP 自律システムの詳細については、[EIGRPのセットアップ（EIGRP Setup）] ダイアログボックス （3348 ページ）を参照してください。
インターフェイス	設定する EIGRP インターフェイスを指定します。インターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイス ロール オブジェクトを選択するか、新しいオブジェクトを作成します。
Hello 間隔（Hello Interval）	ルータからそのネイバーに送信される hello パケット間のデフォルトの間隔。ルータは、hello パケットを相互に送信して、直接接続されたネットワーク上の他のルータについて動的に学習します。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
Split Horizon	選択すると、ルーティング ループを防止するためにスプリット ホライズン機能が使用されます。 選択を解除すると、スプリット ホライズンがディセーブルになります。スプリット ホライズンがディセーブルになると、ルータで、ルートの学習元の同じインターフェイスからそのルートをアドバタイズできます。 スプリットホライズンを無効にすると、フレームリレーや SMDS などの非ブロードキャストネットワークを扱う場合に便利です。 （注） インターフェイスでスプリット ホライズン設定を変更すると、そのインターフェイスで到達可能な EIGRP ネイバーとの隣接関係はすべてリセットされます。

[EIGRP] ページ - [Redistribution] タブ

EIGRP の [Redistribution] タブを使用して、EIGRP 再配布マッピングを作成、編集、および削除します。

ナビゲーション パス

[EIGRP] ルーティング ポリシー ページ （3346 ページ）に移動し、[再配布（Redistribution）] タブをクリックします。

関連項目

- EIGRP へのルートの再配布 （3345 ページ）
- [EIGRP] ページ：[セットアップ（Setup）] タブ （3347 ページ）
- [EIGRP] ページ：[インターフェイス（Interfaces）] タブ （3349 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 926 : EIGRP の [Redistribution] タブ

要素	説明
EIGRP AS Number	他のルートが再配布されている EIGRP ルートのエリア ID。
プロトコル	再配布されているプロトコル。
[AS/プロセス ID（AS/Process ID）]	再配布されているルートの AS 番号またはプロセス ID。
Bandwidth	ルート メトリックに対して定義された、EIGRP ルートのパスの最小帯域幅。
遅延	ルートメトリックに対して定義された、パスの平均遅延。
信頼性	ルートメトリックに対して定義された、パスの推定信頼性を表す値。
有効帯域幅（Effective Bandwidth）	ルート メトリックに対して定義された、リンクへの有効負荷を表す値。
[MTU]	ルート メトリックに対して定義された、パスの最小 MTU。
一致（Match）	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。
[追加（Add）] ボタン	[EIGRP再配布マッピング（EIGRP Redistribution Mapping）] ダイアログボックス （3353ページ）が開きます。ここから、EIGRP 再配布マッピングを定義できます。
[編集（Edit）] ボタン	[EIGRP再配布マッピング（EIGRP Redistribution Mapping）] ダイアログボックス （3353ページ）が開きます。ここから、選択した EIGRP 再配布マッピングを編集できます。
[削除（Delete）] ボタン	選択した EIGRP 再配布マッピングをテーブルから削除します。

[EIGRP再配布マッピング（EIGRP Redistribution Mapping）] ダイアログボックス

[EIGRP Redistribution Mapping] ダイアログボックスを使用して、EIGRP 再配布マッピングのプロパティを追加または編集します。

ナビゲーション パス

[EIGRP] ページ - [Redistribution] タブ （3351 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

（注） [EIGRP Redistribution] ダイアログボックスにアクセスする前に、少なくとも 1 つの EIGRP AS を作成する必要があります。 [EIGRP] ページ：[セットアップ（Setup）] タブ （3347 ページ） を参照してください。

関連項目

- EIGRP へのルートの再配布 （3345 ページ）

フィールド リファレンス

表 *927 : [EIGRP*再配布マッピング（*EIGRP Redistribution Mapping*）*]* ダイアログボックス

要素	説明
EIGRP AS Numbers	他のルートが再配布されている EIGRP AS。 [EIGRP] ページ：[セットアップ（Setup）] タブ （3347 ページ）で定義した EIGRP 自律システムのリストから ID 番号を選択する必要があります。
Protocol to Redistribute	再配布されているルーティング プロトコル。 • [Static]：スタティック ルートを再配布します。ルートごとに 1 つのマッピングを定義できます。 • [EIGRP]：EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに 1 つのマッピングを定義できます。 • [BGP]：BGP 自律システムを再配布します。デバイスごとに 1 つの BGP マッピングを定義できます。[BGP Setup] タブで [BGP AS] を設定した場合は、AS 番号が表示されます。それ以外の場合は、BGP AS が定義されていないことを示すメッセージが表示されます。 [BGP] ページ - [Redistribution] タブ （3338 ページ）を参照してください。

要素	説明
Protocol to Redistribute（続き）	• [OSPF]：別の OSPF プロセスを再配布します。プロセスごとに 1 つのマッピングを定義できます。表示されるリストからプロセスを選択し、1 つ以上の一致基準を選択します。 • [Internal]：特定の AS の内部のルート。 • [External1]：AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1]：AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area（NSSA）ルート。 • [NSAAExternal2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる（NSSA）ルート。 • [RIP]：RIP ルートを再配布します。 • [Connected]：インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。
メトリック	再配布されたルートのデフォルトのメトリック（コスト）。次のメトリックパラメータがあります。 • [Bandwidth]：パスの最小帯域幅（キロビット/秒）。有効値の範囲は 1 ～ 4294967295 です。 • [Delay]：パスの平均遅延（10 ミリ秒単位）。有効値の範囲は、0 ～ 4294967295 です。 • 信頼性：リンクの推定信頼性を表す値。有効値の範囲は 0 ～ 255 で、255 は 100% の信頼性を表します。 • 実効帯域幅：リンクの実効負荷を表す値。有効値の範囲は 1 ～ 255 で、255 は 100% の使用率を表します。 • [MTU of Path]：パスの最大伝送単位。有効な値の範囲は 1 ～ 65535 バイトです。

Cisco IOS ルータにおける OSPF ルーティング

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Open Shortest Path First（OSPF）は、距離ベクトルではなくリンク ステートを使用して、1 つの自律システム（AS）内でルーティング情報を配布する Interior Gateway Routing Protocol です。OSPF はルーティング テーブル更新ではなく Link-State Advertisement（LSA; リンクステート アドバタイズメント）を伝播するため、OSPF ネットワークは RIP ネットワークよりも迅速に収束できます。エリアを定義して、エリア内で発生する変更に伝達する必要がある LSA の数を制限します。

複数の OSPF エリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータ間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。どのルータも ABR または ASBR として機能できます。

ここでは、OSPF ルーティングポリシーを作成するために実行するタスクについて説明します。

- OSPF プロセス設定の定義 （3355 ページ）
- OSPF エリア設定の定義 （3356 ページ）
- OSPF へのルートの再配布 （3358 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）

関連項目

- Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）
- Cisco IOS ルータにおける RIP ルーティング （3384 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）
- Cisco IOS ルータにおける BGP ルーティング （3331 ページ）

OSPF プロセス設定の定義

OSPF プロセス パラメータを設定するには、OSPF プロセスを他のルータに対して識別するプロセス ID 番号を指定し、インターフェイスが受動かどうかを決定します。受動インターフェイスは、ネイバーにルーティング更新を送信しません。

関連項目

- OSPF エリア設定の定義 （3356 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）
- OSPF へのルートの再配布 （3358 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから**[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFプロセス（OSPF Process）]** を選択し、作業領域の [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]**[Router Platform] > [Routing] > [RIP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

OSPF プロセスの [Setup] タブが表示されます。このタブのフィールドの説明については、表 930 : OSPF プロセスの [Setup] タブ （3376 ページ）を参照してください。

ステップ 2 OSPF プロセスの [セットアップ（Setup）] タブで、テーブルから OSPF プロセスを選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてプロセスを作成します。[OSPFセットアップ（OSPF Setup）] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 931 : [OSPF Setup] ダイアログボックス （3376 ページ）を参照してください。

ステップ 3 表示されるフィールドにプロセス ID 番号を入力します。ここで定義するプロセス ID は、他のデバイスのプロセス ID と一致している必要はありません。

ステップ 4 どのインターフェイスがネイバーにルーティング更新を送信しないかを定義します。

a) [パッシブインターフェイス（Passive Interfaces）] の下にある [編集（Edit）] をクリックして、[インターフェイスの編集（Edit Interfaces）] ダイアログボックスを表示します。このダイアログボックスを使用して、ネイバーにルーティング更新を送信しないインターフェイスを定義します。

b) 1 つ以上のインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

c) [OK] をクリックして変更を保存し、[OSPFセットアップ（OSPF Setup）] ダイアログボックスに戻ります。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

OSPF エリア設定の定義

OSPF エリア設定を設定するには、エリア ID を特定の OSPF プロセスに関連付け、エリアに含まれるネットワークを選択し、エリア内のルータによって使用される認証のタイプを選択します。

定義する各 OSPF プロセスには、少なくとも 1 つの定義されたエリアが含まれている必要があります。複数のエリアを定義する場合は、1 つのエリアがエリア 0 である必要があります。これはバックボーンと呼ばれます。その他のすべてのエリアは、バックボーンに物理的に接続されている必要があります。これによって、他のエリアがルーティング情報をバックボーンに注入し、バックボーンがその他のエリアに配布できるようになります。

少なくとも 1 つの OSPF プロセスを設定してから、そのプロセスの OSPF エリア/ネットワーク設定を定義する必要があります。

関連項目

- OSPF プロセス設定の定義 （3355 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）
- OSPF へのルートの再配布 （3358 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFプロセス（OSPF Process）]** を選択し、作業領域の [エリア（Area）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）] > [ルーティング（Routing）] > [OSPFプロセス（OSPF Process）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[エリア（Area）] タブをクリックします。

[OSPFプロセスエリア（OSPF Process Area）] タブが表示されます。このタブのフィールドの説明については、表 932 : OSPF プロセスの [Area] タブ （3378 ページ）を参照してください。

ステップ 2 [OSPFプロセスエリア（OSPF Process Area）] タブで、テーブルから OSPF エリアを選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてエリアを作成します。[OSPF Area] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 933 : [OSPF Area] ダイアログボックス （3379 ページ）を参照してください。

ステップ 3 表示されるリストからプロセス ID を選択します。

ステップ 4 選択した OSPF プロセスに関連付けるエリア ID を入力します。

ステップ 5 OSPF エリアに含めるネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを入力できます。または [選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 6 OSPF エリアで使用する認証タイプ（MD5、クリア テキスト、またはなし）を選択します。セキュリティが問題となる場合は、MD5 を推奨します。次の点に注意してください。

- 認証タイプは、同じエリア内のすべてのルータおよびアクセス サーバで同じである必要があります。

- エリアに対してクリア テキスト認証を指定すると、認証はタイプ 1（単純なパスワード）に設定されます。ネットワーク上のすべてのルータは、OSPF を使用して相互に通信するために、同じクリア テキスト パスワードを使用する必要があります。
- エリア全体でMD5パスワードを同じにする必要はありませんが、ネイバー間では同じにする必要があります。
- インターフェイス認証（OSPFインターフェイス設定の定義 （3361ページ）を参照）を使用する場合、エリアで使用する認証タイプが、インターフェイスで使用する認証タイプと一致する必要があります。

ステップ 7 [OK] をクリックして定義を保存します。OSPF エリアが、OSPF の [Area] タブに表示されるテーブルに表示されます。

OSPF へのルートの再配布

再配布とは、OSPF などのルーティング プロトコルを使用して、他の方法（別のルーティング プロトコルなど）で学習されたルート、スタティック ルート、または直接接続されたルートをアドバタイズすることです。たとえば、RIP ルーティング プロトコルから OSPF ドメインにルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベース ルーティング プロトコルに適用できます。

他のルーティング プロトコルまたはスタティック ルートからOSPFへルートを再配布すると、これらのルートは OSPF 外部ルート（タイプ 1 またはタイプ 2）になります。

OSPF へのルートの再配布では、次のことを行います。

- OSPF 再配布マッピングの定義 （3358 ページ）
- OSPF 最大プレフィックス値の定義 （3360 ページ）

関連項目

- OSPF プロセス設定の定義 （3355 ページ）
- OSPF エリア設定の定義 （3356 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）

OSPF 再配布マッピングの定義

OSPF 再配布マッピングを定義するときは、再配布するプロトコルと、そのプロトコルのルートを再配布する先の OSPF プロセスを選択する必要があります。また、再配布されるルートのプライオリティを決定するメトリック、および作成する外部 OSPF ルートのタイプ（タイプ 1 またはタイプ 2）を手動で定義できます。

同じ OSPF プロセスに複数のマッピングを作成できます。たとえば、RIP ルートと EIGRP ルートの両方を同じ OSPF プロセスに再配布できます。他の OSPF プロセスからルートを再配布することもできます。

（注） OSPF Not-So-Stubby Area（NSSA）への再配布によって、NSSA エリア内だけで存在可能な、タイプ 7 と呼ばれる特別なタイプのリンクステート アドバタイズメント（LSA）が作成されます。この LSA は、NSSA Autonomous System Border Router（ASBR; 自律システム境界ルータ）によって生成され、NSSA Area Border Router（ABR; エリア境界ルータ）によってタイプ 5 LSA に変換されて、これが OSPF ドメインに伝播されます。

タイプ 1 とタイプ 2 の外部ルート

タイプ 1 とタイプ 2 という 2 つのタイプの OSPF 外部ルートがあります。2 つの違いは、ルートのコスト（メトリック）の計算方法に関係します。タイプ 1 ルートのコストは、そのルートに到達するために使用される外部コストと内部コストの合計です。タイプ 2 ルートのコストは、外部コストだけに基づきます。デフォルトでは、外部ルートはタイプ 2 として定義されます。ただし、同じ宛先へは、タイプ 1 ルートがタイプ 2 ルートよりも常に優先されます。

はじめる前に

- 少なくとも 1 つの OSPF プロセスを定義します。OSPF プロセス設定の定義 （3355 ページ）を参照してください。

関連項目

- OSPF 最大プレフィックス値の定義 （3360 ページ）
- OSPF へのルートの再配布 （3358 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFプロセス（OSPF Process）] を選択し、作業領域の [再配布（Redistribution）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから [プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]**[Router Platform] > [Routing] > [RIP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[再配布（Redistribution）] タブをクリックします。

[OSPF Process Redistribution] タブが表示されます。このタブのフィールドの説明については、表 934 : OSPF プロセスの [Redistribution] タブ （3380 ページ）を参照してください。

ステップ 2 OSPF プロセスの [再配布（Redistribution）] タブで、[OSPF再配布マッピング（OSPF Redistribution Mappings）] テーブルから行を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてマッピングを作成します。[OSPF Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 935 : [OSPF Redistribution Mapping] ダイアログボックス （3382 ページ）を参照してください。

ステップ 3 表示されるリストから既存の OSPF プロセスを選択します。

ステップ 4 選択した OSPF プロセスにルートを再配布するプロトコルを選択します。

（注） スタティック ルート、RIP ルート、BGP AS、EIGRP AS、および OSPF プロセスごとに 1 つのマッピングを作成できます。

ステップ 5 （任意）再配布されたルートのデフォルトのメトリック（コスト）を修正します。メトリックによって、ルートのプライオリティが決まります。

ステップ 6 作成する外部ルートのメトリック タイプ（タイプ 1 またはタイプ 2）を選択します。デフォルトはタイプ 2 です。

ステップ 7 （オプション）[サブネットに制限（Limit to Subnets）]チェックボックスをオンにして、サブネット化されたルートだけを再配布します。デフォルトでは、このオプションは選択されていません。

ステップ 8 [OK] をクリックして定義を保存します。再配布マッピングが、OSPF プロセスの [Redistribution] タブの [Redistribution Mapping] テーブルに表示されます。

OSPF 最大プレフィックス値の定義

選択した OSPF プロセスに他のプロトコルまたは OSPF プロセスから再配布できるプレフィックス（ルート）の最大数を定義できます。制限を設定すると、再配布されるルートが多すぎてルータがフラッド状態になるのを防止できます。たとえば、最大数を定義しないと、BGP が OSPF に再配布されるときにフラッディングが発生する可能性があります。

最大プレフィックス値を定義する場合、この最大値に達したときに、それ以上ルートが再配布されないようにするか、警告を発行するだけかを決定できます。

再配布制限は、すべての IP 再配布プレフィックスに適用されます。合計されるプレフィックスも含まれます。この制限は、タイプ 7 からタイプ 5 への変換の結果として生成されるデフォルト ルートまたはプレフィックスには適用されません。

はじめる前に

- 少なくとも 1 つの OSPF プロセスを定義します。少なくとも 1 つの OSPF プロセスを定義します。OSPF プロセス設定の定義 （3355 ページ）を参照してください。
- 少なくとも 1 つの OSPF 再配布マッピングを定義します。OSPF 再配布マッピングの定義（3358 ページ） を参照してください。

関連項目

- OSPF 再配布マッピングの定義 （3358 ページ）
- OSPF へのルートの再配布 （3358 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFプロセス（OSPF Process）] を選択し、作業領域の [再配布（Redistribution）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから[ルータプラットフォーム（Router Platform）]>[ルーティング（Routing）]>[OSPFプロセス（OSPF Process）]を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[再配布（Redistribution）] タブをクリックします。

[OSPF Process Redistribution] タブが表示されます。このタブのフィールドの説明については、表 934 : OSPF プロセスの [Redistribution] タブ （3380 ページ）を参照してください。

ステップ 2 OSPF プロセスの [プロセスの再配布（Process Redistribution）] タブで、[最大プレフィックスマッピング（Max Prefix Mapping）] テーブルから行を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックして定義を作成します。[Max Prefix Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 936 : [OSPF Max Prefix Mapping] ダイアログボックス （3383 ページ）を参照してください。

ステップ 3 表示されるリストから既存の OSPF プロセスを選択します。

ステップ 4 [Max Prefix] フィールドで、選択した OSPF プロセスに再配布できるルートの最大数を入力します。

ステップ 5 （任意）デフォルトしきい値のパーセンテージを変更します。再配布されるルートの数がこのしきい値に達すると、警告が発行されます。デフォルトでは、しきい値は定義された最大プレフィックス値の 75% です。

ステップ 6 （任意）最大プレフィックス値に達したときの動作を選択します。

- [Enforce Maximum Route]：選択したプロセスにルートがそれ以上再配布されないようにします。
- [Warning Only]：追加の警告を発行しますが、最大プレフィックス値に達したあともルートの再配布は続行されます。

（注） 最大プレフィックス値を超えたあともルートの再配布を続行すると、フラッディングが発生する可能性があります。

ステップ 7 [OK] をクリックして定義を保存します。最大プレフィックス定義は、OSPF プロセスの [Redistribution] タブの [Maximum Prefix] テーブルに表示されます。

OSPF インターフェイス設定の定義

インターフェイス固有のさまざまな OSPF パラメータを変更できます。ここでは、これらのパラメータを定義する方法について説明します。特定のパラメータについては、次の項を参照してください。

- インターフェイス コストについて （3363 ページ）
- インターフェイス プライオリティについて （3363 ページ）
- MTU 不一致検出のディセーブル化 （3364 ページ）
- OSPF タイマー設定について （3365 ページ）

- LSA フラッディングのブロック （3365 ページ）
- OSPF ネットワーク タイプについて （3366 ページ）
- OSPF インターフェイス認証について （3367 ページ）

関連項目

- OSPF プロセス設定の定義 （3355 ページ）
- OSPF エリア設定の定義 （3356 ページ）
- OSPF へのルートの再配布 （3358 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFインターフェイス（OSPF Interface）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）]>[ルーティング（Routing）] > [OSPFインターフェイス（OSPF Interface）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[OSPF Interface] ページが表示されます。このページのフィールドの説明については、表 928 : [OSPF Interface] ページ （3369 ページ）を参照してください。

ステップ 2 [OSPFインターフェイス（OSPF Interface）] ページで、テーブルからインターフェイス定義を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックして定義を作成します。[OSPF Interface] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 929 : [OSPF Interface] ダイアログボックス （3370 ページ）を参照してください。

ステップ 3 定義するインターフェイスの名前またはインターフェイスロールを入力します。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、 ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

ステップ 4 インターフェイス認証を定義します。インターフェイスに対して選択する認証タイプは、エリアに対して選択する認証タイプと一致している必要があります（OSPF エリア設定の定義 （3356 ページ）を参照）。

OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。詳細については、OSPF インターフェイス認証について （3367 ページ）を参照してください。

キー ID 番号は、複数のパスワードに関連付けることができます。これは、パスワードを移行する簡単で安全な方法です。たとえば、あるパスワードを別のパスワードに移行するには、異なるキー ID でパスワードを設定してから、最初のキーを削除します。

ヒント キー ID 番号は、複数のパスワードに関連付けることができます。これは、パスワードを移行する簡単で安全な方法です。たとえば、あるパスワードを別のパスワードに移行するには、異なるキー ID でパスワードを設定してから、最初のキーを削除します。

（注） セキュリティ上の目的から、OSPF パケットにはクリア テキスト認証を使用しないでください。クリアテキスト認証では、各パケットで暗号化されていない認証キーが送信されます。クリアテキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。

ステップ 5 （任意）[プロパティ（Properties）] で、必要に応じてインターフェイスパラメータを設定します。各パラメータについては、表 929 : [OSPF Interface] ダイアログボックス （3370 ページ）を参照してください。

ステップ 6 [OK] をクリックして定義を保存します。定義されたインターフェイスが、[OSPF Interface] ページに表示されます。

ステップ 7 このプロセスを繰り返して、その他の OSPF インターフェイスのインターフェイス固有のパラメータを定義します。

インターフェイス コストについて

OSPF インターフェイスのコストとは、そのインターフェイスでパケットを送信する場合のコストを表すメトリックのことです。デフォルトでは、このコストは次の式で計算されます。

10^8/帯域幅（ビット/秒）

たとえば、ファストイーサネットインターフェイスの帯域幅が 10 Mbps（10^7 と等しい）の場合、そのインターフェイスでパケットを送信するコストは $10^8 / 10^7$、または 10 として計算されます。この式によって、インターフェイスの帯域幅とそのコスト間の反比例関係が確立されます。帯域幅が大きくなると、コストは低くなります。

コストは計算される値ですが、選択したインターフェイスのコストを手動で入力できます。

関連項目

- インターフェイス プライオリティについて （3363 ページ）
- MTU 不一致検出のディセーブル化 （3364 ページ）
- LSA フラッディングのブロック （3365 ページ）
- OSPF タイマー設定について （3365 ページ）
- OSPF ネットワーク タイプについて （3366 ページ）
- OSPF インターフェイス認証について （3367 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）

インターフェイス プライオリティについて

共通セグメントを共有するルータは、Hello プロトコルによって、そのセグメント上でネイバーに選出されます。選出は、ネイバーの hello パケットにリストされていることをルータ自体が確認するとすぐに行われます。隣接関係は、次のステップです。隣接ルータとは、単純な Hello 交換を越えて、データベース交換へと進むルータです。

各マルチアクセス（ポイントツーポイントではない）セグメントで、OSPF は 1 つのルータをそのセグメントの Designated Router（DR; 指定ルータ）として選出します。DR は、情報交換を最小限にするために接続を一元的に管理する場所として機能します。セグメント内の各ルータは、更新を DR に送信し、DR はその情報を他のルータに中継します。DR がダウンしたときのために、別のルータが Backup Designated Router（BDR; バックアップ指定ルータ）として選出されます。

DR および BDR 選出は、Hello プロトコルを通じて実行されます。OSPF プライオリティが最も高いルータが、そのセグメントの DR になります。次に、BDR について同じプロセスが繰り返されます。プライオリティが同じ場合は、Router ID（RID; ルータ ID）が上位のルータが選出されます。デフォルトでは、各インターフェイスのプライオリティは 1 ですが、必要に応じて、選択したインターフェイスに高いプライオリティを割り当てることができます。

（注） プライオリティ設定は、ポイントツーポイントの非ブロードキャスト インターフェイスには適用されません。

関連項目

- インターフェイス コストについて （3363 ページ）
- MTU 不一致検出のディセーブル化 （3364 ページ）
- LSA フラッディングのブロック （3365 ページ）
- OSPF タイマー設定について （3365 ページ）
- OSPF ネットワーク タイプについて （3366 ページ）
- OSPF インターフェイス認証について （3367 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）

MTU 不一致検出のディセーブル化

MTU は、特定のインターフェイスで処理できる最大パケット サイズです。あるルータが、ネイバールータ上の MTU 設定よりも大きい DBD パケットを送信した場合、ネイバールータはそのパケットを無視します。多くの場合、MTU の不一致によって 2 台のルータは exstart/exchange 状態になり、OSPF 隣接関係が確立されません。そのため、すべてのネイバールータが同じ MTU 設定を共有し、MTU 不一致検出がイネーブルになっていることが重要です。

ただし、MTU 不一致検出をディセーブルにすることもできます。これは、MTU が異なる以外は有効な設定である 2 台のデバイス間で、不一致検出によって隣接関係が確立されない場合に役立ちます。

関連項目

- インターフェイス コストについて （3363 ページ）

• インターフェイス プライオリティについて （3363 ページ）
• LSA フラッディングのブロック （3365 ページ）
• OSPF タイマー設定について （3365 ページ）
• OSPF ネットワーク タイプについて （3366 ページ）
• OSPF インターフェイス認証について （3367 ページ）
• OSPF インターフェイス設定の定義 （3361 ページ）

LSA フラッディングのブロック

デフォルトでは、OSPF は、LSA が到着したインターフェイスを除き、同じエリア内のすべてのインターフェイスで新しい LSA をフラッドします。冗長性は必要ですが、過度な冗長性により帯域幅が浪費されることがあります。完全メッシュなどの特定のトポロジでは、過度のリンクおよび CPU 使用率のために、LSA フラッディングによってネットワークが不安定になる可能性があります。そのため、ブロードキャスト、非ブロードキャスト、およびポイントツーポイント ネットワーク上の選択したインターフェイスへの LSA フラッディングをブロックできます。

関連項目

• インターフェイス コストについて （3363 ページ）
• インターフェイス プライオリティについて （3363 ページ）
• MTU 不一致検出のディセーブル化 （3364 ページ）
• OSPF タイマー設定について （3365 ページ）
• OSPF ネットワーク タイプについて （3366 ページ）
• OSPF インターフェイス認証について （3367 ページ）
• OSPF インターフェイス設定の定義 （3361 ページ）

OSPF タイマー設定について

OSPF では、動作中に一連のタイマーが使用されます。

- [Hello Interval]：インターフェイスが hello パケットを送信する頻度を決定します。hello パケットは、ネイバーの取得に使用され、ルータが機能していることのインジケータの役割を果たします。間隔が短いほど、ネットワーク上のトポロジ変更の検出が速くなります。ただし、間隔が短くなると、インターフェイスで送信されるトラフィックも多くなります。hello 間隔は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じである必要があります。

- [Transmit Delay]：LSA がリンクでフラッドされる前の遅延を決定します。送信遅延設定は、インターフェイスの送信および伝播遅延を考慮する必要があります。これらの要因は、低速リンクおよびオンデマンド リンクを設定する場合に特に重要です。
- [Retransmit Interval]：確認応答されなかった DataBase Description（DBD）パケットをネイバーに再送信する前に待機する時間を決定します。再送信間隔設定を低く設定して、過度の再送信を防止する必要があります。

（注） シリアル回線および仮想リンクの場合は、再送信間隔を大きくする必要があります。

- [Dead Interval]：ネイバーがダウンしていると宣言する前にインターフェイスが待機する時間を決定します。この宣言は、この間隔内にネイバーからの hello パケットが届かない場合に行われます。デッド間隔設定は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じである必要があります。デフォルトでは、この間隔は hello 間隔の 4 倍です。

関連項目

- インターフェイス コストについて （3363 ページ）
- インターフェイス プライオリティについて （3363 ページ）
- MTU 不一致検出のディセーブル化 （3364 ページ）
- LSA フラッディングのブロック （3365 ページ）
- OSPF ネットワーク タイプについて （3366 ページ）
- OSPF インターフェイス認証について （3367 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）

OSPF ネットワーク タイプについて

デフォルトのメディア タイプに関係なく、インターフェイスの OSPF ネットワーク タイプをブロードキャストまたは NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）として手動で設定できます。たとえば、マルチキャスト アドレッシングをサポートしないルータがネットワークに含まれている場合に、この機能を使用して、ブロードキャスト ネットワーク（イーサネット、トークン リング、FDDI など）を NBMA として設定できます。また、NBMA ネットワーク（X.25、フレーム リレー、SMDS など）をブロードキャスト ネットワークとして設定できます。このことにより、ネイバーを設定する必要がなくなります。

NBMA ネットワークをブロードキャストまたは非ブロードキャストとして設定するには、すべてのルータからすべてのルータへの仮想回線（VC）が存在すること（完全にメッシュ化されたネットワーク）が前提となります。各ルータ間に VC が存在しない場合（コストの制約または部分的にだけメッシュ化されたネットワークの存在による）、OSPF ネットワーク タイプをポイントツーマルチポイントとして設定できます。OSPF ポイントツーマルチポイント イン

ターフェイスは、1つ以上のネイバーを持つ番号付きポイントツーポイントインターフェイスとして定義されます。複数のホスト ルートが作成されます。

ポイントツーマルチポイント ネットワーク タイプを使用する場合、直接接続されていない 2 台のルータ間のルーティングは、両方のルータへの VC を持つ第三のルータを経由します。この機能を使用する場合、ネイバーを設定する必要はありません。OSPF ポイントツーマルチポイント ネットワークには、NBMA およびポイントツーポイント ネットワークと比較して、次の利点があります。

- ポイントツーマルチポイントは、IP サブネットを 1 つだけ使用し、ネイバー設定または指定ルータ選出が必要ないため、設定が簡単です。
- 完全にメッシュ化されたトポロジが必要ないため、コストが低くなります。
- VC の障害時に接続が維持されるため、信頼性が高まります。

（注） ポイントツーマルチポイントのブロードキャスト ネットワークでは、任意でネイバーを定義できます。この場合、各ネイバーへのコストを指定する必要があります。ポイントツーマルチポイントの非ブロードキャスト ネットワークでは、ネイバーを識別する必要がありますが、各ネイバーへのコストの指定は任意です。どちらの場合も、FlexConfig を使用してネイバーを定義します。詳細については、FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。

関連項目

- インターフェイス コストについて （3363 ページ）
- インターフェイス プライオリティについて （3363 ページ）
- MTU 不一致検出のディセーブル化 （3364 ページ）
- LSA フラッディングのブロック （3365 ページ）
- OSPF タイマー設定について （3365 ページ）
- OSPF インターフェイス認証について （3367 ページ）
- OSPF インターフェイス設定の定義 （3361 ページ）

OSPF インターフェイス認証について

OSPF インターフェイスのネイバー認証設定を定義するには、インターフェイスを選択し、認証タイプ（MD5 またはクリア テキスト）を選択します。

MD5 認証を使用する場合、ネイバールータは同じパスワードを共有する必要があります。クリア テキスト認証を使用する場合、OSPF を使用するネットワーク上のすべてのルータは同じパスワードを共有する必要があります。

新しいキーを使用してインターフェイスを設定すると、ルータは、それぞれ異なるキーで認証された複数の同一パケットを送信します。すべてのネイバーが新しいキーを採用したことをルータが検出すると、重複パケットの送信を停止します。

（注） 攻撃者はOSPFと他のプロトコル（RIPなど）との間のルート再配布を利用してルーティング情報を操作できるため、可能なかぎり、すべてのルーティング プロトコルで認証を使用する必要があります。

関連項目

- インターフェイス コストについて （3363 ページ）
- インターフェイス プライオリティについて （3363 ページ）
- MTU 不一致検出のディセーブル化 （3364 ページ）
- LSA フラッディングのブロック （3365 ページ）
- OSPF タイマー設定について （3365 ページ）
- OSPF ネットワーク タイプについて （3366 ページ）
- OSPF インターフェイス認証について （3367 ページ）

[OSPF Interface] ポリシー ページ

[OSPF Interface] ページを使用して、インターフェイス固有の OSPF 設定を表示、作成、編集、および削除します。詳細については、OSPFインターフェイス設定の定義 （3361ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから**[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFインターフェイス（OSPF Interface）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）] > [ルーティング（Routing）] > [OSPFインターフェイス（OSPF Interface）]** を選択します。 [OSPFインターフェイス（OSPF Interface）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

関連項目

- [OSPF Process] ポリシー ページ （3374 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *928 : [OSPF Interface]* ページ

要素	説明
インターフェイス	OSPF をイネーブルにするインターフェイスの名前（インターフェイス ロールによって定義）。
認証	選択したインターフェイスでイネーブルにする OSPF ネイバー認証のタイプ。
Key ID	MD5 認証に使用される認証キーの識別番号。
コスト（Cost）	選択したインターフェイスでパケットを送信するコスト（この値が通常計算されるコストと異なる場合）。
プライオリティ	選択したインターフェイスのプライオリティ。
MTU Ignore	選択したインターフェイスで最大伝送単位（MTU）検出がディセーブルかどうかを示します。
Database Filter	選択したインターフェイスでリンクステート アドバタイズメント（LSA）フラッディングがディセーブルかどうかを示します。
Hello 間隔（Hello Interval）	このインターフェイスで送信される hello パケット間の間隔（秒単位）。
送信遅延（Transmit Delay）	LSA がリンク上にフラッディングされる前に OSPF が待機する時間（秒単位）。
再送信間隔（Retransmit Interval）	選択したインターフェイスでの LSA 再送信間隔（秒単位）。
dead 間隔（Dead Interval）	hello パケットがないためネイバールータがデッドであると宣言する前に OSPF が待機する間隔（秒単位）。
ネットワーク タイプ（Network Type）	選択したインターフェイスに対して設定されるネットワーク タイプ（デフォルトのメディアと異なる場合）。
[追加（Add）] ボタン	[OSPF Interface] ダイアログボックス （3370 ページ）が開きます。ここから、OSPF インターフェイスのプロパティを定義できます。
[編集（Edit）] ボタン	[OSPF Interface] ダイアログボックス （3370 ページ）が開きます。ここから、選択した OSPF インターフェイスのプロパティを編集できます。

要素	説明
[削除（Delete）] ボタン	選択したOSPFインターフェイス定義をテーブルから削除します。

[OSPF Interface] ダイアログボックス

[OSPF Interface] ダイアログボックスを使用して、OSPF インターフェイスのプロパティを追加または編集します。

ナビゲーション パス

[OSPF Interface] ポリシー ページ （3368 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- OSPF インターフェイス設定の定義 （3361 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）
- Cisco IOS ルータでの基本的なインターフェイス設定 （3006 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 929 : [OSPF Interface] ダイアログボックス

要素	説明
インターフェイス（Interface）	設定する OSPF インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
認証	[Type]：選択したインターフェイスで使用される認証タイプ。 • [MD5]：認証に MD5 ハッシュ アルゴリズムを使用します。これがデフォルトです。 • [Clear Text]：認証にクリア テキスト パスワードを使用します。 • [None]：認証を使用しません。 （注） インターフェイスで使用される認証タイプは、エリアに対して定義された認証タイプと一致している必要があります。 （注） プレーンテキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。 • [Key ID]：認証タイプとして [MD5] を選択した場合にだけ使用できます。 認証キーの識別番号。この番号は、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。有効値の範囲は、1 ～ 255 です。 • [Key]：認証（MD5 またはクリア テキスト）に使用される共有キー。このキーは、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。[Confirm] フィールドにこのキーを再入力します。 クリア テキストを使用する場合、キーにはキーボードから入力できる任意の連続した文字列を含めることができます（最大 8 バイト）。 MD5 を使用する場合、キーに使用できるのは英数字だけです（最大 16 バイト）。
コスト（Cost）	このインターフェイスでパケットを送信するコスト。ここに入力する値は、デフォルトで計算されるコスト（10 8 / 帯域幅（ビット/秒））よりも優先されます。 有効値の範囲は 1 ～ 65535 です。

要素	説明
プライオリティ	インターフェイスのデフォルトのプライオリティ。プライオリティは、どのルータがそのセグメントの Designated Router（DR; 指定ルータ）および Backup Designated Router（BDR; バックアップ指定ルータ）になるかを決定するために使用されます。数字が大きいほど、優先順位は高くなります。 デフォルトのプライオリティは 1 です。有効値の範囲は 0 ～ 255 です。 （注） インターフェイスが DR または BDR として選出されないようにするには、プライオリティ 0 を割り当てます。ポイントツーポイント ネットワークではなくマルチアクセス ネットワークへのインターフェイスについてだけ、ルータ プライオリティを設定します。
MTU Ignore	選択すると、ネイバールータ間の MTU 不一致を無視します。 選択を解除すると、MTU 不一致検出がイネーブルになります。 （注） 通常、このオプションは使用されません。ルータが exstart/exchange 状態になり、OSPF 隣接関係が確立されなくなる可能性があるためです。
Database Filter	選択すると、選択したインターフェイスへのリンクステート アドバタイズメント（LSA）フラッディングがブロックされます。 選択を解除すると、LSA フラッディングが許可されます。 （注） 完全にメッシュ化されたネットワークでは、このオプションをイネーブルにすることを推奨します。このオプションは、ポイントツーマルチポイント ネットワークには使用できません。
Hello 間隔（Hello Interval）	選択したインターフェイスで送信される hello パケット間のデフォルトの間隔（秒単位）。これらのパケットは、パケットを送信しているルータがまだ動作していることを確認するために、ネイバールータによって使用されます。有効値の範囲は、1 ～ 65535 秒です。 （注） hello 間隔は、ネットワーク内のすべてのルータおよびアクセス サーバで同じである必要があります。
送信遅延（Transmit Delay）	LSA がリンク上にフラッディングされる前に OSPF が待機する時間（秒単位）。 デフォルト値は 1 秒です。有効な値の範囲は、1 ～ 65535 秒です。 （注） トラフィックを大量に送信する前にキューイングする低速リンクまたはオンデマンドリンクを設定する場合は、この値を定義するときに、これらのリンク遅延を考慮することを推奨します。

要素	説明
再送信間隔（Retransmit Interval）	選択したインターフェイスでの LSA 再送信間隔（秒単位）。 デフォルトは 5 秒です。有効な値の範囲は、1 ～ 65535 秒です。 （注） シリアル回線および仮想リンクの場合は、この値を大きくすることを推奨します。
dead 間隔（Dead Interval）	helloパケットが受信されない場合に、ネイバーがデッドであるとインターフェイスが宣言するまでの間隔（秒単位）。有効値の範囲は 1 ～ 655335 秒です。 （注） 通常、デッド間隔の値は hello 間隔値の 4 倍です。デッド間隔は、ネットワーク内のすべてのルータおよびアクセス サーバで同じである必要があります。

要素	説明
Configure Network Type	選択すると、インターフェイスによって使用されるデフォルトのメディアとは異なるネットワーク タイプを選択できます。 選択を解除すると、ネットワーク タイプはインターフェイスによって使用されるデフォルトのメディアと同じです。 NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワーク（ATMやフレーム リレーなど）の場合、オプションは次のとおりです。 • [Broadcast]：NBMA ネットワークをブロードキャスト ネットワークとして処理します。このことにより、ネイバーを設定する必要がなくなります。このオプションは、すべてのルータからすべてのルータへの仮想回線がある場合（完全にメッシュ化されたネットワーク）に使用します。 • [Point-to-Multipoint]：非ブロードキャスト ネットワークを一連のポイントツーポイント リンクとして処理します。このオプションは、NBMA またはポイントツーポイント ネットワークよりも設定が簡単で、コストが小さく、高い信頼性があります。 • [Point-to-Multipoint Non-Broadcast]：ネットワークの既知のネイバーをスタティックに保持します。このオプションを選択すると、hello パケットの受信によって動的に学習されたネイバーが失われる問題を回避するのに役立ちます。 （注） NBMA ネットワークの別のオプションは、FlexConfig を使用してネイバーを手動で設定することです。FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）を参照してください。 ブロードキャスト ネットワーク（イーサネット、トークン リング、FDDI など）の場合、次を選択できます。 • [Non-Broadcast]：ブロードキャスト ネットワークを非ブロードキャスト ネットワークとして処理します。 • [Point-to-Point]：ブロードキャスト ネットワークをポイントツーポイント ネットワークとして処理します。このオプションを使用して、たとえば、ネットワーク内のすべてのルータがマルチキャスト アドレッシングをサポートしているわけではない場合に、ブロードキャスト ネットワーク（イーサネットなど）を NonBroadcast MultiAccess（NBMA; 非ブロードキャスト マルチアクセス）ネットワークとして設定できます。

[OSPF Process] ポリシー ページ

OSPF は、パス選択に距離ベクトルではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF はルーティング テーブル更新ではなく Link-State Advertisement（LSA; リ

ンクステート アドバタイズメント）を伝播するため、OSPF ネットワークは迅速に収束できます。

[OSPF Process] ページの次のタブから、OSPF プロセス ポリシーを設定できます。

- [OSPF Process] ページ - [Setup] タブ （3375 ページ）
- [OSPF Process] ページ - [Area] タブ （3377 ページ）
- [OSPF Process] ページ - [Redistribution] タブ （3379 ページ）

詳細については、 Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）を参照してください。

（注） OSPF インターフェイス ポリシーの詳細については、 [OSPF Interface] ポリシー ページ （3368 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）デバイスポリシーセレクタから[プラットフォーム（Platform）]>[ルーティング（Routing）] > [OSPFプロセス（OSPF Process）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [ルータプラットフォーム（Router Platform）] > [ルーティング（Routing）] > [OSPFプロセス（OSPF Process）] を選択します。 [OSPFプロセス（OSPF Process）] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

[OSPF Process] ページ - [Setup] タブ

OSPF プロセスの [Setup] タブを使用して、OSPF プロセスを作成、編集、および削除します。これには、受動のままのインターフェイスの選択も含まれます。これは、ネイバーにルーティング更新を送信しないことを意味します。プロセスは、ルータごとに必要な数だけ作成できます。

ナビゲーション パス

[OSPF Process] ポリシー ページ （3374 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- OSPF プロセス設定の定義 （3355 ページ）
- [OSPF Process] ページ - [Area] タブ （3377 ページ）
- [OSPF Process] ページ - [Redistribution] タブ （3379 ページ）
- [OSPF Interface] ポリシー ページ （3368 ページ）

- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *930 : OSPF* プロセスの *[Setup]* タブ

要素	説明
プロセス ID（Process ID）	OSPF ルーティング プロセスを他のルータに対して識別するプロセス ID。
パッシブ インターフェイス	ルーティング更新を送信しないインターフェイス。
[追加（Add）] ボタン	[OSPF Setup] ダイアログボックス （3376 ページ）が開きます。ここから、OSPF プロセスを定義できます。
[編集（Edit）] ボタン	[OSPF Setup] ダイアログボックス （3376 ページ）が開きます。ここから、選択した OSPF プロセスを編集できます。
[削除（Delete）] ボタン	選択した OSPF プロセスをテーブルから削除します。

[OSPF Setup] ダイアログボックス

[OSPF Setup] ダイアログボックスを使用して、OSPF プロセスを追加または編集します。

ナビゲーション パス

[OSPF Process] ページ - [Setup] タブ （3375 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- OSPF プロセス設定の定義 （3355 ページ）

フィールド リファレンス

表 *931 : [OSPF Setup]* ダイアログボックス

要素	説明
プロセス ID（Process ID）	OSPF プロセスのプロセス ID 番号。この番号によって、OSPF プロセスは他のルータに対して識別されます。他のデバイス上のプロセス ID と一致している必要はありません。有効値は 1 ～ 65535 です。

要素	説明
パッシブ インターフェイス	ルーティング ネイバーに更新を送信しないインターフェイス。[編集（Edit）] をクリックして、[Edit Interfaces] ダイアログボックス - OSPF 受動インターフェイス （3377ページ）を表示します。ここから、これらのインターフェイスを定義できます。 （注） インターフェイスを受動にすると、OSPF によってネイバールータへの hello パケットの送信は抑止されます。ただし、インターフェイスでルーティング更新の受信は続行されます。

[Edit Interfaces] ダイアログボックス - OSPF 受動インターフェイス

Cisco IOS ルータで OSPF ルーティング ポリシーを設定する場合、[Edit Interfaces] ダイアログボックスを使用して、ルーティング ネイバーに更新を送信しないインターフェイスを指定します。複数の名前またはロールを指定する場合は、カンマで区切ります。[選択（Select）] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイス ロール オブジェクトを作成します。

ナビゲーション パス

[OSPF Setup] ダイアログボックス （3376ページ）に移動してから、[パッシブインターフェイス（Passive Interfaces）] フィールドの [編集（Edit）] ボタンをクリックします。

関連項目

- [OSPF Process] ページ - [Setup] タブ （3375 ページ）
- OSPF プロセス設定の定義 （3355 ページ）

[OSPF Process] ページ - [Area] タブ

OSPF の [Area] タブを使用して、各 OSPF プロセスに含まれるエリアおよびネットワークを作成、編集、および削除します。これには、各エリアによって使用される認証のタイプの選択が含まれます。

ナビゲーション パス

[OSPF Process] ポリシー ページ （3374ページ）に移動し、[エリア（Area）] タブをクリックします。

関連項目

- OSPF エリア設定の定義 （3356 ページ）
- [OSPF Process] ページ - [Setup] タブ （3375 ページ）
- [OSPF Process] ページ - [Redistribution] タブ （3379 ページ）

- [OSPF Interface] ポリシー ページ （3368 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *932 : OSPF* プロセスの *[Area]* タブ

要素	説明
エリア ID（Area ID）	プロセスに関連付けられるエリアの ID 番号。
プロセス ID（Process ID）	OSPF ルーティング プロセスを他のルータに対して識別するプロセス ID。
ネットワーク	エリアに含まれるネットワーク。
認証	エリアによって使用される認証タイプ（MD5、クリアテキスト、またはなし）。
[追加（Add）] ボタン	[OSPF Area] ダイアログボックス （3378 ページ） を開きます。ここから、OSPF エリアを定義できます。
[編集（Edit）] ボタン	[OSPF Area] ダイアログボックス （3378 ページ） が開きます。ここから、選択した OSPF エリアを編集できます。
[削除（Delete）] ボタン	選択した OSPF エリアをテーブルから削除します。

[OSPF Area] ダイアログボックス

[OSPF Area] ダイアログボックスを使用して、OSPF エリアのプロパティを追加または編集します。OSPF プロセスごとに少なくとも 1 つのエリアを定義する必要がありますが（[OSPF Setup] ダイアログボックス （3376 ページ） を参照）、定義しない場合でも展開は失敗しません。

ナビゲーション パス

[OSPF Process] ページ - [Area] タブ （3377 ページ） に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- OSPF エリア設定の定義 （3356 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

フィールド リファレンス

表 *933 : [OSPF Area]* ダイアログボックス

要素	説明
プロセス ID（Process ID）	OSPF エリアに関連付けられるプロセス ID。リストには、[OSPF Process] ページ - [Setup] タブ （3375 ページ）で定義された OSPF プロセスが含まれます。
エリア ID（Area ID）	選択したプロセスに関連付けられるエリア ID 番号。有効値の範囲は、0 ～ 4294967295 です。
ネットワーク	OSPF エリアに追加するネットワーク。1 つ以上のネットワーク アドレスまたはネットワーク/ホストオブジェクトを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。
認証	エリアに対して使用される認証のタイプ。 • [MD5]：（推奨）認証に MD5 ハッシュ アルゴリズムを使用します。 • [Clear Text]：認証にクリア テキストを使用します。 • [None]：認証は使用されません。 （注） 認証タイプは、エリア内のすべてのルータおよびアクセス サーバで同じである必要があります。

[OSPF Process] ページ - [Redistribution] タブ

OSPF プロセスの [Redistribution] タブを使用して、OSPF 再配布マッピングを作成、編集、および削除します。これには、他のプロトコルまたは他の OSPF プロセスから OSPF に再配布できる最大ルート数の定義も含まれます。

ナビゲーション パス

[OSPF Process] ポリシー ページ （3374 ページ）に移動し、[再配布（Redistribution）] タブをクリックします。

関連項目

- OSPF へのルートの再配布 （3358 ページ）
- [OSPF Process] ページ - [Setup] タブ （3375 ページ）
- [OSPF Process] ページ - [Area] タブ （3377 ページ）
- [OSPF Interface] ポリシー ページ （3368 ページ）

- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *934 : OSPF* プロセスの *[Redistribution]* タブ

要素	説明
[OSPF Redistribution Mapping] テーブル	
OSPF プロセス ID（OSPF Process ID）	他のルートが再配布されている OSPF ルーティング ドメインの ID。
プロトコル	再配布されているプロトコル。
[AS/プロセス ID（AS/Process ID）]	再配布されているルートの AS 番号またはプロセス ID。
一致（Match）	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。
メトリック（Metric）	再配布されるルートのプライオリティを決定する値。
メトリック タイプ	OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプ。
サブネット	サブネット化されたルートも再配布されるかどうかを示します。
[追加（Add）] ボタン	[OSPF Redistribution Mapping] ダイアログボックス （3381 ページ）が開きます。ここから、OSPF 再配布マッピングを定義できます。
[編集（Edit）] ボタン	[OSPF Redistribution Mapping] ダイアログボックス （3381 ページ）が開きます。ここから、選択した OSPF 再配布マッピングを編集できます。
[削除（Delete）] ボタン	選択した再配布マッピングをテーブルから削除します。
[OSPF Max Prefix Mapping] テーブル	
OSPF プロセス ID（OSPF Process ID）	最大プレフィックス値が定義された OSPF ルーティング ドメインの ID。
Max Prefix	選択した OSPF プロセスに再配布できるプレフィックス（ルート）の最大数。

要素	説明
[しきい値（Threshold）]	警告メッセージをトリガーするしきい値として機能する最大プレフィックス値のパーセンテージ。
操作	最大値に達したときに、この OSPF プロセスへの再配布が停止されるか、警告が表示されるだけかを示します。
[追加（Add）] ボタン	[OSPF Max Prefix Mapping] ダイアログボックス （3383 ページ）が開きます。ここから、OSPF プロセスの最大プレフィックス値を定義できます。
[編集（Edit）] ボタン	[OSPF Max Prefix Mapping] ダイアログボックス （3383 ページ）が開きます。ここから、選択した OSPF プロセスに対して定義された最大プレフィックス値を編集できます。
[削除（Delete）] ボタン	選択した最大プレフィックスマッピングをテーブルから削除します。

[OSPF Redistribution Mapping] ダイアログボックス

[OSPF Redistribution Mapping] ダイアログボックスを使用して、OSPF 再配布マッピングのプロパティを追加または編集します。

ナビゲーション パス

[OSPF Process] ページ - [Redistribution] タブ （3379 ページ）に移動してから、[再配布マッピング（Redistribution Mapping）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

（注） [OSPF Redistribution] ダイアログボックスにアクセスする前に、少なくとも 1 つの OSPF プロセスを作成する必要があります。[OSPF Process] ページ - [Setup] タブ （3375 ページ）を参照してください。

関連項目

- [OSPF Max Prefix Mapping] ダイアログボックス （3383 ページ）
- OSPF へのルートの再配布 （3358 ページ）

フィールド リファレンス

表 *935 : [OSPF Redistribution Mapping]* ダイアログボックス

要素	説明
プロセス ID（Process ID）	他のルートが再配布されている OSPF プロセス。 [OSPF Process] ページ - [Setup] タブ （3375 ページ）で定義した OSPF プロセスのリストから、プロセス ID 番号を選択する必要があります。
Protocol to Redistribute	再配布されているルーティング プロトコル。 • [Static]：スタティック ルートを再配布します。ルートごとに 1 つのマッピングを定義できます。 • [EIGRP]：EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに 1 つのマッピングを定義できます。 • [BGP]：BGP 自律システムを再配布します。デバイスごとに 1 つの BGP マッピングを定義できます。[BGP Setup] タブで [BGP AS] を設定した場合は、AS 番号が表示されます。それ以外の場合は、BGP AS が定義されていないことを示すメッセージが表示されます。 [BGP] ページ - [Redistribution] タブ （3338 ページ）を参照してください。

Protocol to Redistribute（続き）	• [OSPF]：別の OSPF プロセスを再配布します。プロセスごとに 1 つのマッピングを定義できます。表示されるリストからプロセスを選択し、1 つ以上の一致基準を選択します。
	  • [Internal]：特定の AS の内部のルート。
	  • [External1]：AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。
	  • [External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。
	  • [NSAAExternal1]：AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area（NSSA）ルート。
	  • [NSAAExternal2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる（NSSA）ルート。
	• [RIP]：RIP ルートを再配布します。ルートごとに 1 つのマッピングを定義できます。
	• [Connected]：インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。

要素	説明
デフォルト メトリック（Default Metric）	再配布されるルートのコストを表す値。
メトリック タイプ	OSPF ルーティング ドメインに再配布されているルートに関連付けられる外部リンク タイプ。 • [1]：タイプ 1 外部ルート。メトリックは、外部再配布コストと内部 OSPF コストの合計です。 • [2]：タイプ 2 外部ルート。メトリックは、[Metric] フィールドで定義される外部再配布コストと等しくなります。これがデフォルトです。
Limit to Subnets	選択すると、サブネット化されたルートだけが再配布されます。 選択を解除すると、サブネット化されたルートは再配布されません。

[OSPF Max Prefix Mapping] ダイアログボックス

[OSPF Max Prefix Mapping] ダイアログボックスを使用して、OSPF プロセスに再配布できるルートの最大数を追加または編集します。

ナビゲーション パス

[OSPF Process] ページ - [Redistribution] タブ （3379 ページ）に移動してから、プレフィックス マッピング テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [OSPF Redistribution Mapping] ダイアログボックス （3381 ページ）
- OSPF へのルートの再配布 （3358 ページ）

フィールド リファレンス

表 *936 : [OSPF Max Prefix Mapping]* ダイアログボックス

要素	説明
プロセス ID（Process ID）	他のルートが再配布されている OSPF プロセス。リストには、[OSPF Process] ページ - [Setup] タブ （3375 ページ）で定義された OSPF プロセスが含まれます。
Max Prefix	選択した OSPF プロセスに再配布できるプレフィックス（ルート）の最大数。再配布されるルートの数を制限すると、過剰な数のルートによってルータがフラッドされるのを防ぐのに役立ちます。

要素	説明
[しきい値（Threshold）]	警告メッセージをトリガーするしきい値として機能する最大プレフィックス値のパーセンテージ。デフォルトは 75 % です。 （注） この警告は、[Warning-Only] チェックボックスがオンかどうかに関係なくトリガーされます。
When maximum routes reached	再配布ルートの最大数に達したときに実行するアクション。 • [Enforce Maximum Route]：定義された最大プレフィックス値に達した場合、ルートがそれ以上再配布されないようにします。これがデフォルトです。 • [Warning Only]：ルートの最大数に達したときに警告を表示しますが、追加のルートの再配布は抑止しません。

Cisco IOS ルータにおける RIP ルーティング

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

Routing Information Protocol（RIP; ルーティング情報プロトコル）は、小規模な同種のネットワークで使用するために作成された Interior Gateway Protocol（IGP）です。RIP は距離ベクトル型プロトコルであり、定期的な間隔（アドバタイジングと呼ばれるプロセス）でルーティング更新メッセージを送信します。また、ネットワークトポロジが変更されるたびに更新メッセージを送信します。ルータは、エントリの変更が含まれるルーティングアップデートを受け取ると、新しいルートを反映するようにそのルーティングテーブルを更新します。別のルータから更新を 180 秒以上受信しない場合、ルータは更新のないルータによって提供されるルートを使用不可としてマークします。240 秒後もまだ更新がない場合、ルータは更新のないルータのルーティング テーブル エントリをすべて削除します。ルーティング情報は UDP パケットを使用して交換されます。

RIP は、送信元から宛先へのホップ数（通過したルータの数）を測定することによってルートを評価します。直接接続されているネットワークのメトリックは 0 です。RIP で許可される最大ホップ カウントは 15 です。ホップ カウントが 15 を超えるルートは、到達不能と見なされます。

Security Manager では、RFC 1723 に記載されている RIP バージョン 2 だけがサポートされます。RIP 2 ではオリジナルの RIP が改善されており、RIP メッセージでより多くの情報を伝送できます。これにより、単純な認証メカニズム（クリアテキストまたは MD5）を使用してテーブル更新を保護できます。RIP 2 では、サブネット マスクもサポートされています。これは、元のバージョンの RIP では使用できなかった重要な機能です。

ここでは、RIP ルーティング ポリシーを作成するために実行するタスクについて説明します。

• RIP 設定パラメータの定義 （3385 ページ）
• RIP インターフェイス認証設定の定義 （3386 ページ）
• OSPF へのルートの再配布 （3358 ページ）

関連項目

• Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）
• Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）
• Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）
• Cisco IOS ルータにおける BGP ルーティング （3331 ページ）

RIP 設定パラメータの定義

RIP 設定パラメータを定義するには、ルートに含めるネットワークを選択し、いずれかのインターフェイスを受動にする必要があるかどうかを決定します。これらのインターフェイスは、ネイバーにルーティング更新を送信しません。また、自動サマライズをイネーブルにすると、ルータが維持するルーティング テーブルのサイズと複雑さを軽減できます。

関連項目

• RIP インターフェイス認証設定の定義 （3386 ページ）
• OSPF へのルートの再配布 （3358 ページ）
• Cisco IOS ルータにおける RIP ルーティング （3384 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから**[プラットフォーム（Platform）]>[ルーティング（Routing）] > [RIP]** を選択し、作業領域の [セットアップ（Setup）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]** を選択します。既存のポリシーを選択するか新しいポリシーを作成し、[セットアップ（Setup）] タブをクリックします。

RIP の [Setup] タブが表示されます（[RIP] ページ - [Setup] タブ （3389 ページ）を参照）。

ステップ 2 インターフェイスで RIP 更新を受信する、直接接続されているネットワークのアドレスを入力します。アドレスとネットワーク/ホストオブジェクトの組み合わせを使用するか、アドレスをカンマで区切ることができます。[選択（Select）] をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、新しいネットワーク/ホストオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 3 受動インターフェイスのアドレスを入力します。これは、ネイバーにルーティング更新（存在する場合）を送信しないインターフェイスです。これらのインターフェイスは、引き続き RIP ルーティング ブロード

キャストを受信し、それを使用してルーティング テーブルに読み込みます。1 つ以上のインターフェイスの名前またはインターフェイスのロールを入力します。アドレスをカンマで区切ります。[選択（Select）] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイス ロール オブジェクトを作成します。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

ステップ 4 （任意）[自動集約（Auto Summary）] チェックボックスをオンにして、ネットワークレベルルートへのサブネットルートの自動集約を有効にします。サマライズによってルーティング テーブルのサイズが削減されるため、ネットワークの複雑さが低減します。

切断されているサブネット間のルーティングを実行する場合は、自動サマライズをディセーブルにします。自動サマライズをオフにすると、サブネットがアドバタイズされます。

RIP インターフェイス認証設定の定義

RIP インターフェイスのネイバー認証設定を定義するには、インターフェイスを選択し、認証タイプ（MD5 またはクリア テキスト）を選択します。

関連項目

- RIP 設定パラメータの定義 （3385 ページ）
- OSPF へのルートの再配布 （3358 ページ）
- Cisco IOS ルータにおける RIP ルーティング （3384 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから [プラットフォーム（Platform）]>[ルーティング（Routing）] > [RIP] を選択し、作業領域の [認証（Authentication）] タブをクリックします。
- （ポリシービュー）ポリシー タイプ セレクタから **[Router Platform] > [Routing] > [RIP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[認証（Authentication）] タブをクリックします。

RIP の [Authentication] タブが表示されます。このタブのフィールドの説明については、表 938 : RIP の [Authentication] タブ （3390 ページ）を参照してください。

ステップ 2 RIP の [認証（Authentication）] タブで、テーブルからインターフェイス定義を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックして定義を作成します。[RIP Authentication] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 939 : [RIP Authentication] ダイアログボックス （3391 ページ）を参照してください。

ステップ 3 認証が定義されるインターフェイスまたはインターフェイスロールの名前を入力します。または、[選択（Select）] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成します。詳細については、ポリシー定義中のインターフェイスの指定 （386 ページ）を参照してください。

ステップ 4 インターフェイス認証（MD5 またはクリア テキスト）を定義します。

（注） RIP パケットでクリア テキスト認証を使用することは推奨しません。これは、暗号化されない認証キーがすべてのパケットで送信されるためです。プレーン テキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。定義されたインターフェイスが、RIP の [Authentication] タブに表示されます。

RIP へのルートの再配布

再配布とは、RIP などのルーティング プロトコルを使用して、他の方法（別のルーティング プロトコルなど）で学習されたルート、スタティック ルート、または直接接続されたルートをアドバタイズすることです。たとえば、OSPF ルーティング プロトコルから RIP ルートにルートを再配布できます。再配布は、複数プロトコル環境で動作しているネットワークに必要であり、すべての IP ベース ルーティング プロトコルに適用できます。

RIP に再配布する場合、透過的に再配布することによって、ルートの元のメトリックを保持できます。

はじめる前に

- 少なくとも 1 つの RIP ルートを定義します。 RIP 設定パラメータの定義 （3385 ページ）を参照してください。

関連項目

- RIP 設定パラメータの定義 （3385 ページ）
- RIP インターフェイス認証設定の定義 （3386 ページ）
- Cisco IOS ルータにおける RIP ルーティング （3384 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[ルーティング（Routing）] > [RIP]** を選択し、作業領域の [再配布（Redistribution）] タブをクリックします。
- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成し、[再配布（Redistribution）] タブをクリックします。

RIP の [Redistribution] タブが表示されます。このタブのフィールドの説明については、表 940 : RIP の [Redistribution] タブ （3392 ページ）を参照してください。

ステップ 2 RIP の [再配布（Redistribution）] タブで、[RIP再配布マッピング（RIP Redistribution Mappings）] テーブルから行を選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてマッピングを作成しま

す。[RIP Redistribution Mapping] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 941 : [RIP Redistribution Mapping] ダイアログボックス （3393 ページ）を参照してください。

ステップ 3 RIP にルートを再配布するプロトコルを選択します。

（注） スタティック ルート、BGP AS、EIGRP AS、および OSPF プロセスごとに 1 つのマッピングを作成できます。

ステップ 4 次のいずれかの操作を実行して、再配布されるルートのメトリック（コスト）を定義します。

- [デフォルトメトリック（Default Metric）] チェックボックスをオンにし、再配布されるルートのデフォルトメトリックを入力します。メトリックによって、ルートのプライオリティが決まります。
- [トランスペアレント（Transparent）] チェックボックスをオンにし、RIP に再配布されるルートの元のメトリックを保持します。

ステップ 5 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。再配布マッピングが、RIP の [Redistribution] タブの [Redistribution Mapping] テーブルに表示されます。

[RIP] ルーティング ポリシー ページ

RIP は、ホップ カウントをパス選択のメトリックとして使用するディスタンス ベクター ルーティング プロトコルです。Security Manager では、RIP バージョン 2 だけがサポートされます。これには、ルーティング更新の交換時のネイバー認証のサポートが含まれています。

[RIP] ルーティング ページの次のタブから、RIP ルーティング ポリシーを設定できます。

- [RIP] ページ - [Setup] タブ （3389 ページ）
- [RIP] ページ - [Authentication] タブ （3390 ページ）
- [RIP] ページ - [Redistribution] タブ （3392 ページ）

詳細については、Cisco IOS ルータにおける RIP ルーティング （3384 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [ルーティング（Routing）] > [RIP]** を選択します。[RIP] を右クリックしてポリシーを作成するか、または共有ポリシーセレクタから既存のポリシーを選択します。

[RIP] ページ - [Setup] タブ

RIP の [Setup] タブを使用して、RIP ルートを作成、編集、および削除します。

ナビゲーション パス

[RIP] ルーティング ポリシー ページ （3388 ページ）に移動し、[セットアップ（Setup）] タブをクリックします。

関連項目

- RIP 設定パラメータの定義 （3385 ページ）
- [RIP] ページ - [Authentication] タブ （3390 ページ）
- [RIP] ページ - [Redistribution] タブ （3392 ページ）
- ポリシー定義中の IP アドレスの指定 （401 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）

フィールド リファレンス

表 937 : RIP の [Setup] タブ

要素	説明
ネットワーク	RIP ルートに関連付けられる直接接続されたネットワーク。1 つ以上のネットワーク アドレスまたはネットワーク/ホスト オブジェクトをカンマで区切って入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからネットワーク/ホストオブジェクトを選択するか、新しいオブジェクトを作成します。
パッシブ インターフェイス	ルーティング ネイバーに更新を送信しないインターフェイス。1 つ以上のインターフェイス名またはロールをカンマで区切って入力します。[選択（Select）] をクリックして既存のオブジェクトのリストからインターフェイス名またはロールを選択するか、新しいインターフェイス ロール オブジェクトを作成します。
自動集約（Auto-Summary）	選択されている場合は、ネットワーク レベル ルートへのサブネット ルートの自動サマライズをイネーブルにします。サマライズによってルーティング テーブルのサイズが削減されるため、ネットワークの複雑さが低減します。 選択解除されている場合、自動サマライズはディセーブルになります。 （注） 切断されているサブネット間のルーティングを実行する場合は、自動サマライズをディセーブルにします。この機能をディセーブルにすると、サブネットがアドバタイズされます。

[RIP] ページ - [Authentication] タブ

RIP の [Authentication] タブを使用して、RIP インターフェイスのネイバー認証設定を表示、作成、編集、および削除します。

ナビゲーション パス

[RIP] ルーティング ポリシー ページ （3388 ページ）に移動し、[認証（Authentication）] タブをクリックします。

関連項目

- RIP インターフェイス認証設定の定義 （3386 ページ）
- [RIP] ページ - [Setup] タブ （3389 ページ）
- [RIP] ページ - [Redistribution] タブ （3392 ページ）
- [RIP] ルーティング ポリシー ページ （3388 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 938 : RIP の [Authentication] タブ

要素	説明
インターフェイス	RIP をイネーブルにするインターフェイスの名前（インターフェイス ロールによって定義）。
認証	選択したインターフェイス ロールでイネーブルにする RIP ネイバー認証のタイプ（クリア テキストまたは MD5）。
Key ID	MD5 認証に使用される認証キーの識別番号。
[追加（Add）] ボタン	[RIP Authentication] ダイアログボックス （3391 ページ）が開きます。ここから、その他の RIP インターフェイスの認証を定義できます。
[編集（Edit）] ボタン	[RIP Authentication] ダイアログボックス （3391 ページ）が開きます。ここから、選択した RIP インターフェイスの認証プロパティを編集できます。
[削除（Delete）] ボタン	選択した認証定義をテーブルから削除します。

[RIP Authentication] ダイアログボックス

[RIP Authentication] ダイアログボックスを使用して、RIP インターフェイスのネイバー認証プロパティを追加または編集します。

ナビゲーション パス

[RIP] ページ - [Authentication] タブ （3390 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- RIP インターフェイス認証設定の定義 （3386 ページ）

フィールド リファレンス

表 939 : [RIP Authentication] ダイアログボックス

要素	説明
インターフェイス（Interface）	認証プロパティを定義するインターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、または新しいオブジェクトを作成します。 （注） 同じインターフェイスに対して異なる認証設定を指定することはできません。
認証	インターフェイスに適用する認証のタイプ。 • [MD5]：（推奨）認証に MD5 ハッシュ アルゴリズムを使用します。 • [Clear Text]：認証にクリア テキストを使用します。 （注） プレーン テキスト認証は、セキュリティが問題でない場合、たとえば誤って設定されたホストがルーティングに参加しないことを確認する場合にだけ使用します。
Key ID	認証タイプとして [MD5] を選択した場合にだけ使用できます。 認証キーの識別番号。この番号は、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。有効値の範囲は 0 ～ 2147483647 です。

要素	説明
キー（Key）	認証（MD5 またはクリア テキスト）に使用される共有キー。このキーは、選択したデバイスに更新を送信し、選択したデバイスから更新を受信する他のすべてのデバイスと共有される必要があります。 キーには最大 80 文字の英数字を含むことができます。最初の文字を数値にはできません。スペースを使用できます。確認フィールドでもう一度キーを入力します。

[RIP] ページ - [Redistribution] タブ

RIP の [Redistribution] タブを使用して、RIP ルーティング ドメインへの再配布を実行するときの再配布設定を表示、作成、編集、および削除します。

（注） RIP の [Redistribution] タブにアクセスする前に、RIP 設定パラメータを定義する必要があります。 [RIP] ページ - [Setup] タブ （3389 ページ）を参照してください。

ナビゲーション パス

[RIP] ルーティング ポリシー ページ （3388 ページ）に移動し、[再配布（Redistribution）] タブをクリックします。

関連項目

- RIP へのルートの再配布 （3387 ページ）
- [RIP] ページ - [Authentication] タブ （3390 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 940 : RIP の [Redistribution] タブ

要素	説明
プロトコル	再配布されているプロトコル。
[AS/プロセス ID（AS/Process ID）]	再配布されているルートの自律システム（AS）番号またはプロセス ID。
メトリック（Metric）	再配布されるルートのプライオリティを決定する値。
一致（Match）	OSPF プロセスを再配布している場合は、再配布される OSPF ルートのタイプを示します。

要素	説明
[追加（Add）] ボタン	[RIP Redistribution Mapping] ダイアログボックス （3393 ページ）が開きます。ここから、RIP 再配布マッピングを定義できます。
[編集（Edit）] ボタン	[RIP Redistribution Mapping] ダイアログボックス （3393 ページ）が開きます。ここから、選択したRIP再配布マッピングを編集できます。
[削除（Delete）] ボタン	選択した再配布マッピングをテーブルから削除します。

[RIP Redistribution Mapping] ダイアログボックス

[RIP Redistribution Mapping] ダイアログボックスを使用して、RIP 再配布マッピングのプロパティを追加または編集します。

ナビゲーション パス

[RIP] ページ - [Redistribution] タブ （3392 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- RIP へのルートの再配布 （3387 ページ）

フィールド リファレンス

表 *941 : [RIP Redistribution Mapping]* ダイアログボックス

要素	説明
Protocol to Redistribute	再配布されているルーティング プロトコル。 • [Static]：スタティック ルートを再配布します。ルートごとに 1 つのマッピングを定義できます。 • [EIGRP]：EIGRP 自律システムを再配布します。表示されるフィールドに AS 番号を入力します。AS ごとに 1 つのマッピングを定義できます。 • [BGP]：BGP 自律システムを再配布します。デバイスごとに 1 つの BGP マッピングを定義できます。[BGP Setup] タブで [BGP AS] を設定した場合は、AS番号が表示されます。それ以外の場合は、BGP AS が定義されていないことを示すメッセージが表示されます。 [BGP] ページ - [Redistribution] タブ （3338 ページ）を参照してください。

要素	説明
Protocol to Redistribute（続き）	• [OSPF]：別の OSPF プロセスを再配布します。プロセスごとに 1 つのマッピングを定義できます。表示されるリストからプロセスを選択し、1 つ以上の一致基準を選択します。 • [Internal]：特定の AS の内部のルート。 • [External1]：AS の外部にあり、OSPF にタイプ 1 外部ルートとしてインポートされるルート。 • [External2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされるルート。 • [NSAAExternal1]：AS の外部にあり、選択したプロセスにタイプ 1 外部ルートとしてインポートされる Not-So-Stubby Area（NSSA）ルート。 • [NSAAExternal2]：AS の外部にあり、選択したプロセスにタイプ 2 外部ルートとしてインポートされる（NSSA）ルート。 • [Connected]：インターフェイス上で IP をイネーブルにすることにより自動的に確立されるルートを再配布します。これらのルートは、AS の外部として再配布されます。
デフォルト メトリック（Default Metric）	再配布されるルートのデフォルト値を設定します。有効値の範囲は 0 ～ 16 です。
Transparent Metric	選択すると、再配布されるルートの元のメトリックが保持されます。選択を解除すると、[Metric] フィールドで指定した値が使用されます。

Cisco IOS ルータにおけるスタティック ルーティング

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

ルートを動的に構築できない場合にパケットがルータによって宛先に正しく転送されるように、スタティック ルーティング ポリシーを設定できます。スタティック ルートにはデフォルトでアドミニストレーティブディスタンス 1（直接接続されたネットワークを意味する）が設定されるため、デフォルトでは、同じホストまたはネットワークに対して検出されたダイナミック ルートよりも優先されます。ただし、対応するダイナミック ルートよりも優先されないように、大きな値のアドミニストレーティブ ディスタンスをスタティック ルートに定義できます。

たとえば、EIGRP ルートには、デフォルトでアドミニストレーティブ ディスタンス 5 が設定されます。スタティック ルートよりも EIGRP ルートが優先されるようにするには、5 よりも大きいアドミニストレーティブ ディスタンスを指定する必要があります。この機能は、スタティックルートを「フローティング」ルートとして定義する場合に役立ちます。フローティングルートは、優先ルートを使用できない場合にのみルーティングテーブルに挿入されます。

ヒント スタティックルートをバックアップの「フローティング」ルートとして使用する場合は、特定の IP アドレスを入力する代わりに、ネクストホップ IP アドレスに到達できるインターフェイスを指定します。そうしないと、プライマリリンクに障害が発生したときに、「フローティング」ルートはルーティングテーブルに挿入されません。詳細については、Cisco.com の次の URL で『*Specifying a Next Hop IP Address for Static Routes*』を参照してください。http://www.cisco.com/en/US/tech/tk365/technologies_tech_note09186a00800ef7b2.shtml [英語]

関連項目

- スタティック ルートの定義 （3395 ページ）

スタティック ルートの定義

スタティック ルートを定義するには、選択したホストまたはネットワーク宛のパケットをルータが転送するホップ ゲートウェイの IP アドレス（および、任意でメトリック）を定義する必要があります。必要な数のスタティック ルートを定義できます。

関連項目

- Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）
- Cisco IOS ルータにおける RIP ルーティング （3384 ページ）
- Cisco IOS ルータにおける OSPF ルーティング （3355 ページ）
- Cisco IOS ルータにおける EIGRP ルーティング （3340 ページ）
- Cisco IOS ルータにおける BGP ルーティング （3331 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]** > **[ルーティング（Routing）]** > **[スタティックルーティング（Static Routing）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータ プラットフォーム（Router Platform）]** > **[ルーティング（Routing）]** > **[スタティックルーティング（Static Routing）]** を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

[Static Routing] ページが表示されます。このページのフィールドの説明については、表 942 : [Static Routing] ページ （3397 ページ）を参照してください。

ステップ 2 [スタティックルーティング（Static Routing）] ページで、テーブルからスタティックルートを選択し、[編集（Edit）] をクリックするか、[追加（Add）] をクリックしてルートを作成します。[Static Routing] ダイアログボックスが表示されます。このダイアログボックスのフィールドの説明については、表 943 : [Static Routing] ダイアログボックス （3399 ページ）を参照してください。

ステップ 3 （任意）[デフォルトルートとして使用（Use as Default Route）] チェックボックスをオンにして、このルートを不明なすべてのアウトバウンドパケットのデフォルトルートにします。

ステップ 4 [プレフィックス（Prefix）] フィールドに、宛先ネットワークのアドレスを入力します。または、[選択（Select）] をクリックしてリストからネットワーク/ホストオブジェクトを選択するか、または新しいオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 5 転送オプションを選択します。

- パケットをリモートネットワークに転送するルータインターフェイスを定義するには、[転送インターフェイス（Forwarding Interface）] を選択し、インターフェイスまたはインターフェイスロールの名前を入力します。[Select] をクリックしてリストからインターフェイスロールを選択するか、新しいインターフェイスロールを作成できます。インターフェイス ロール オブジェクトについて （381 ページ）およびポリシーのオブジェクトの選択 （288 ページ）を参照してください。
- パケットを受信してリモートネットワークに転送するネクストホップルータを指定するには、[転送IP（Forwarding IP）] を選択し、表示されるフィールドにアドレスを入力します。または、[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。詳細については、ポリシー定義中の IP アドレスの指定 （401 ページ）を参照してください。

ステップ 6 （任意）[Distance Metric] フィールドに、このルータのネクスト ホップ アドレスへのホップ数を入力します。このメトリックは、スタティック ルートのプライオリティを示します。2 つのルーティング エントリで同じネットワークが指定されている場合は、メトリック値の小さい（つまり、コストが低い）ルートに高いプライオリティが与えられ、選択されます。

値を指定しない場合、デフォルトは 1 であり、直接接続されたネットワークを意味します。

ステップ 7 （任意）[永続的なルート（Permanent route）] チェックボックスをオンにして、インターフェイスがシャットダウンされるか、ルータが次のルータと通信できない場合でも、このスタティックルートエントリが削除されないようにします。

ステップ 8 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。スタティック ルートが、[Static Routing] ページのテーブルに表示されます。

[Static Routing] ポリシー ページ

[Static Routing] ページを使用して、スタティック ルートを作成、編集、および削除します。詳細については、スタティック ルートの定義 （3395 ページ）を参照してください。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[プラットフォーム（Platform）]>[ルーティング（Routing）]>[スタティックルーティング（Static Routing）]** を選択します。
- （ポリシービュー）ポリシータイプセレクタから **[ルータプラットフォーム（Router Platform）]>[ルーティング（Routing）]>[スタティックルーティング（Static Routing）]** を選択します。[スタティックルーティング（Static Routing）] を右クリックしてポリシーを作成するか、共有ポリシー セレクタから既存のポリシーを選択します。

関連項目

- Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 942 : [Static Routing] ページ

要素	説明
プレフィックス（Prefix）	スタティック ルートの宛先 IP アドレス。
Prefix Mask	選択した IP アドレスのネット マスク。
Default Route	スタティック ルートがこのルータによって転送される不明なパケットのデフォルト ルートかどうかを示します。
Interface or IP Address	このルータのネクスト ホップ アドレスであるゲートウェイ ルータに関連付けられる IP アドレスまたはインターフェイス名。
距離	ゲートウェイ IP から宛先へのホップ数。メトリックによって、このルートのプライオリティが決まります。ホップが少ないほど、コストが低くなるため、ルートに割り当てられるプライオリティは高くなります。 2 つのルーティング エントリで同じネットワークが指定されている場合、メトリックの小さい（つまり、プライオリティが高い）エントリが選択されます。
Permanent Route	スタティック ルートが永続的なルートとして定義されるかどうかを示します。永続的なルートとは、インターフェイスがシャットダウンされるか、ルータが次のルータと通信できない場合でも、削除されないことを意味します。

要素	説明
[追加（Add）] ボタン	[Static Routing] ダイアログボックス （3398 ページ）が開きます。ここから、スタティック ルートを作成できます。
[編集（Edit）] ボタン	[Static Routing] ダイアログボックス （3398 ページ）が開きます。ここから、選択したスタティック ルートを編集できます。
[削除（Delete）] ボタン	選択したスタティック ルートをテーブルから削除します。

[Static Routing] ダイアログボックス

[Static Routing] ダイアログボックスを使用して、スタティック ルートを追加または編集します。

ナビゲーション パス

[Static Routing] ポリシー ページ （3396 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- スタティック ルートの定義 （3395 ページ）
- Cisco IOS ルータにおけるスタティック ルーティング （3394 ページ）

フィールド リファレンス

表 *943 : [Static Routing]* ダイアログボックス

要素	説明
宛先ネットワーク	このスタティック ルートによって定義される宛先ネットワークのアドレス情報。 • [Use as Default Route]：選択すると、これをこのルータのデフォルト ルートにします。デフォルトルートは、送信元から宛先へのルートが不明な場合、またはルータのルーティング テーブルで多数のルートを保持できない場合に使用されます。すべての不明な送信パケットはデフォルト ルートで送信されます。 選択を解除すると、このスタティック ルートはデフォルト ルートではありません。 • [Prefix]：宛先ネットワークの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 プレフィックスは、クラス A、B、または C ネットワークあるいはホスト IP である必要があります。ホスト IP は、不連続マスクが含まれていないかぎり、0 で開始できます。すべてのサブネット アドレスが有効です。
Forwarding (Next Hop)	宛先ネットワークにデータを転送する方式。 • [Forwarding Interface]：パケットをリモート ネットワークに転送するルータ インターフェイス。インターフェイスの名前またはインターフェイスのロールを入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。 • [Forwarding IP]：パケットを受信してリモート ネットワークに転送するネクスト ホップ ルータの IP アドレス。ネットワーク/ホストオブジェクトの IP アドレスまたは名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。

要素	説明
Distance Metric	宛先ネットワーク（ゲートウェイ IP）へのホップ数。値を指定しない場合、デフォルトは 1 です。範囲は 1 ～ 255 です。 このメトリック（アドミニストレーティブ ディスタンスとも呼ばれる）は、指定したホストが存在するネットワークへのホップ数に基づくルートコストの測定値です。このホップ カウントには、パケットが通過する必要があるすべてのネットワークが含まれています。宛先ネットワークも含まれます。したがって、直接接続されたネットワークのメトリックはすべて 1 です。 メトリックはコストに基づくため、スタティック ルートのプライオリティを識別するために使用されます。2 つのルーティング エントリで同じネットワークが指定されている場合は、メトリック値の小さい（つまり、コストが低い）ルートに高いプライオリティが与えられ、選択されます。 （注） 特定の状況では、スタティック ルートにダイナミック ルートよりも低いプライオリティ（大きいディスタンス メトリック）を割り当てると役立つ場合があります。この設定により、スタティック ルートはダイナミック ルートを使用できない場合のバックアップの「フローティング」ルートとして機能できます。
Permanent route	選択すると、インターフェイスがシャットダウンされるか、ルータが次のルータと通信できない場合でも、このスタティック ルート エントリは削除されません。 選択を解除すると、このスタティック ルートは削除可能です。

第 68 章

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

Cisco Security Manager は、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるセキュリティ サービスやその他のプラットフォーム固有サービスの管理と設定をサポートします。

VTP トランスペアレント モードまたは VTP クライアント/サーバ モードで設定された Catalyst スイッチおよび 7600 デバイスを管理できます。Security Manager は、デバイスにおける VLAN データベース管理（VLAN の作成、削除、スイッチ上の VLAN データベース内の VLAN のモニタリングなど）をバイパスすることによって、クライアント/サーバ モードで設定されたスイッチを管理します。

この章は次のトピックで構成されています。

- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出 （3402 ページ）
- Catalyst サマリー情報の表示 （3403 ページ）
- Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 （3404 ページ）
- インターフェイス （3406 ページ）
- VLANs （3436 ページ）
- VLAN グループ （3444 ページ）
- VLAN ACL（VACL） （3450 ページ）
- IDSM 設定 （3459 ページ）

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータにおけるポリシーの検出

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの設定（およびそれらに関連付けられているサービス モジュールやセキュリティ コンテキストの設定）を検出したり、設定をポリシーとして Security Manager にインポートしたりできます。これにより、既存のデバイスを追加し、それらを Security Manager で管理できるようになり、各デバイスをポリシーごとに手動で設定する必要がなくなります。詳細については、デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。

Security Manager で設定できるコマンドを検出できます。サポートされていないコマンドは検出されません。つまり、これらのコマンドは、次に展開が行われたあともデバイスにそのまま残されています。さらに、Security Manager で検出できるコマンドの場合でも、そのコマンドに関連するサブコマンドとキーワードがすべて検出されるわけではなく、サポートされていない要素は、検出されずにデバイスにそのまま残されます。

また、Security Manager ですでに管理されているデバイスの設定をいつでも再検出できます。ただし、再検出を実行すると Security Manager で定義したポリシーが上書きされるため、通常は再検出を実行することは推奨しません。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

（注） ポリシーの検出後すぐに（ポリシーに変更を加えたり、デバイスからポリシーの割り当てを解除したりする前に）展開を実行することを推奨します（この推奨事項は、デバイスによってホストされるサービスモジュールまたはセキュリティコンテキストにも適用されます）。このようにしないと、Security Manager で設定した変更内容がデバイスに展開されない可能性があります。展開および Configuration Archive の使用 （511 ページ）を参照してください。

関連項目

- ポリシーについて （209 ページ）
- ポリシーの検出 （223 ページ）
- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの管理 （3401 ページ）
- 展開および Configuration Archive の使用 （511 ページ）

Catalyst サマリー情報の表示

[Catalyst Summary Info] ページを使用して、Security Manager によって検出されたサービス モジュール、ポート、VLAN などのシステム情報の概要を表示します。

Catalyst 概要情報を表示するには、デバイスビューで Catalyst スイッチまたは Cisco 7600 シリーズ ルータを右クリックし、[Catalyst サマリー情報（Catalyst Summary Info）] を選択するか、または [ツール（Tools）] > [Catalyst サマリー情報（Catalyst Summary Info）] を選択します。

（注） Security Manager が特定の Cisco Catalyst スイッチまたは Cisco 7600 シリーズ ルータの検出を完了していない場合、そのデバイスの [Catalyst サマリー情報（Catalyst Summary Info）] ページに「No information is available. This information is acquired during device discovery.」（利用できる情報がありません。この情報は、デバイス検出時に取得されます）というメッセージが表示されます。

関連項目

- IDSM 設定 （3459 ページ）
- [VLAN Access Lists] ページ （3454 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *944 : [Catalyst Summary Info]* ページ

要素	説明
ホスト名（Hostname）	デバイスの設定済みホスト名が表示されます。
Device Type	デバイス タイプを表示します。
シリアル番号	デバイスのシリアル番号を表示します。
OS Version	デバイスで実行されている Cisco IOS イメージのバージョンが表示されます。
イメージ（Image）	デバイスで実行されているイメージの名前が表示されます。
Last Update	最新の検出のタイムスタンプを表示します。
合計ポート数	アクセス ポート、ルーテッド ポート、およびトランク ポートを合わせた設定済みポートの合計数が表示されます。
アクセス ポート	シャーシの設定済みアクセスポートの数が表示されます。

要素	説明
トランク ポート	シャーシの設定済みトランク ポートの数が表示されます。
ルーテッド ポート	シャーシの設定済みルーテッド ポートの数が表示されます。
Total VLANs	シャーシおよびそのすべてのサービス モジュールの設定済み VLAN の合計数が表示されます。
Layer 2 VLANs	レイヤ 2 で稼働している VLAN の数が表示されます。
Layer 3 VLANs	レイヤ 3 で稼働している VLAN の数が表示されます。
[Service Module] テーブル	
スロット	サービス モジュールが接続されているスロットが表示されます。
デバイスタイプ	サービスモジュールの簡単な説明を表示します。
シリアル番号	サービス モジュールのシリアル番号が表示されます。
モデル	サービス モジュールのモデル タイプが表示されます。
OS Version	インストールされ、サービス モジュールで稼働している OS バージョンが表示されます。
Assigned VLANs	FWSM が割り当てられている VLAN の合計数が表示されます。 **ヒント** [Interfaces/VLANs] ポリシーの [Summary] タブをクリックすると、IDSM または VPNSM に割り当てられている VLAN を確認できます。
コンテキスト	マルチコンテキストモードで動作する FWSM に設定されているセキュリティコンテキストの総数を表示します。 **ヒント** [インターフェイス/VLAN（Interfaces/VLANs）] ポリシーの [サマリー（Summary）] タブをクリックすると、IDSM に設定されている仮想センサーの数を確認できます。

Catalystインターフェイス、VLAN、およびVLANグループの概要の表示

[インターフェイス/VLAN（Interfaces/VLAN）] ポリシーの [サマリー（Summary）] タブには、サポートされている Catalyst 6500 シリーズおよび 7600 シリーズ シャーシとそれらに関連付けられたサービスモジュールに設定されているすべての VLAN、VLAN グループ、インターフェイス、およびサブインターフェイスの属性が表示されます。

インターフェイスサマリー情報を表示するには、デバイスビューでポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択し、[サマリー（Summary）] タブをクリックします。

（注） [Summary] タブは、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの場合だけ使用できます。

関連項目

- [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）
- [Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）
- [Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）
- Catalyst サマリー情報の表示 （3403 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *945 : [Interfaces/VLANs]* ページ - *[Summary]* タブ

要素	説明
VLAN ID（Admin. VLAN ID）	インターフェイスまたはサブインターフェイスに関連付けられた VLAN ID。VLAN ID は、指定されたインターフェイスまたはサブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、インターフェイスまたはサブインターフェイスでトラフィックを送受信できません。 （注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。
[VLAN 名(VLAN Name)]	インターフェイスまたはサブインターフェイスに対応する VLAN の名前。VLAN003、Trunk1 などです。
VLAN Group	テーブルの行が示す VLAN に設定されている VLAN グループの数値 ID。
VLAN タイプ	VLAN が Layer 2 または Layer 3 にアクセスできるかどうかを指定します。
IP アドレス/マスク（IP Address/Mask）	インターフェイスまたはサブインターフェイスに設定されている VLAN の IP アドレスおよび対応するサブネット マスク。

要素	説明
アクセス ポート	VLANが使用するアクセス ポートに割り当てられている名前が表示されます（名前が割り当てられている場合）。
トランク ポート	トランクを介したトラフィックの伝送が許可されるVLANを示します。
Slot (-Port)	シャーシスロット番号（関連サービスモジュールの取り付け先）を、ハイフンで結び付けられた *x-y* の形式でポート番号に関連付けます（3-1 など）。
[ブレードタイプ（Blade Type）]	特定の VLAN が設定されているサービス モジュールの種類（FWSM、VPNSM など）を示します。
セキュリティコンテキスト	インターフェイスに関連付けられたセキュリティコンテキストを示します。ただし、取り付けられたモジュールでマルチモードがアクティブであり、そのモジュールに管理コンテキストが設定されている場合にかぎります。
[セキュリティ コンテキスト インターフェイス（Security Context Interface）]	セキュリティコンテキストがトラフィックを検査する物理インターフェイスおよびサブインターフェイスIDを表示します。表示されるIDは、物理インターフェイス、単一のサブインターフェイス（範囲を1と定義）、またはサブインターフェイスの範囲を表します。
セキュリティ レベル（Security Level）	インターフェイスのセキュリティ レベルが表示されます。値の範囲は0（最低のセキュリティ）～100（最高のセキュリティ）です。 • 外部インターフェイスの場合、デフォルトは0です。 • 内部インターフェイスの場合、デフォルトは100です。 • DMZのインターフェイスの場合、デフォルトは通常1～99です。

インターフェイス

[Interfaces/VLANs] ページの [Interfaces] タブを使用して、次のタイプのポートを表示および管理します。

- アクセスポート：ホストマシンまたはサービスの接続に使用されるスイッチングポート。アクセス ポートは、1 つの VLAN だけに属し、1 つの VLAN だけのトラフィックを伝送します。トラフィックは、VLANタグが付いていないネイティブ形式で送受信されます。
- トランク ポート：レイヤ 2 で操作され、複数の VLAN のトラフィックを送信するスイッチング ポート。トラフィックには、各 VLAN からのトラフィックを区別する VLAN 番号

がタグ付けされます。トランク ポートは、スイッチ間の接続またはスイッチとルータ間の接続に使用されます。

- ルーテッド ポート：ルータ上のポートのように機能する物理ポート。ルーテッド ポートは特定の VLAN に関連付けられず、通常のルータ インターフェイスのように動作します。ルーテッド ポートにはレイヤ 3 ルーティング プロトコルを設定できます。
- ダイナミック ポート：ネイバー ポートがトランク ポートとして設定されている場合に、トランク ポートに動的に変更できるポート。
- サポートされないポート：Security Manager によってサポートされない Catalyst デバイス上のポート。

[インターフェイス（Interfaces）] タブを表示するには、デバイスビューで Catalyst デバイスを選択し、ポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択して作業領域で [インターフェイス（Interfaces）] タブをクリックします。

次の項では、Catalyst デバイスのインターフェイスを定義するときに実行できるアクションについて説明します。

- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集（3407 ページ）
- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除 （3409 ページ）
- [Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）

関連項目

- VLANs （3436 ページ）
- VLAN グループ （3444 ページ）
- VLAN ACL（VACL） （3450 ページ）

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータのアクセス ポート、ルーテッド ポート、またはトランク ポートを作成できますが、次の制限事項があります。

- 各インターフェイスに名前が必要です。
- アクセス ポートは 1 つの VLAN だけに関連付けることができます。

- トランク ポートは 1 つ以上の VLAN に関連付けることができます。

関連項目

- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除 （3409 ページ）
- VLAN の作成または編集 （3436 ページ）
- VLAN グループの作成または編集 （3444 ページ）
- [Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）
- インターフェイス （3406 ページ）

ステップ 1 （デバイスビュー）Catalyst デバイスを選択し、ポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択して作業領域で [インターフェイス（Interfaces）] タブをクリックします。

[Interfaces] タブが表示されます。このタブの各フィールドの説明については、[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- 新しいインターフェイスの属性を定義するには、[行の追加（Add Row）] をクリックします。
- インターフェイスの属性を編集するには、リストで選択して [行の編集（Edit Row）] をクリックします。

ステップ 3 （任意）このインターフェイスをシャットダウンモードにする場合は、[インターフェイスの有効化（Enable Interface）] チェックボックスをオフにします。

ステップ 4 [タイプ（Type）] リストから [インターフェイス（Interface）] または [サブインターフェイス（Subinterface）] を選択します。

ステップ 5 （インターフェイスだけ）インターフェイスの名前を入力します。[選択（Select）] をクリックするとダイアログボックスが開き、インターフェイスタイプ、およびインターフェイスの位置情報（カード、スロット、サブインターフェイスなど）に基づいて、標準の名前を生成できます。ダイアログボックスを使用してインターフェイス名を生成する方法については、[Interface Auto Name Generator] ダイアログボックス （3020 ページ）を参照してください。

ステップ 6 （インターフェイスのみ）[モード（Mode）] リストからオプションを選択して、ポート設定タイプを指定します。ダイアログボックスのフィールドは、選択に応じて変わります。

ステップ 7 （サブインターフェイスだけ）サブインターフェイスの親インターフェイスを選択し、ID 番号を入力します。

ステップ 8 選択したタイプの設定を定義または指定します。

- [Access Port]：フィールドの説明については、[Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）を参照してください。
- [Routed Port]：フィールドの説明については、[Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ）を参照してください。

- [Trunk Port]：フィールドの説明については、[Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）を参照してください。
- [Dynamic Port]：フィールドの説明については、[Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）を参照してください。
- [Subinterface]：フィールドの説明については、[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス （3431 ページ）を参照してください。
- [Unsupported]：フィールドの説明については、[Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード （3433 ページ）を参照してください。

ステップ 9 [速度（Speed）] リストから、インターフェイスの速度を定義するオプションを選択します。

ステップ 10 インターフェイスに特定の速度を定義した結果、[デュプレックス（Duplex）] リストが有効になっている場合は、デュプレックスオプションを選択します。

ステップ 11 [MTU] フィールドに、最大伝送単位値を入力します。

ステップ 12 インバウンド（受信）トラフィックとアウトバウンド（送信）トラフィックに対してフロー制御を使用するかどうかを設定します。

ステップ 13 （任意）[説明（Description）] フィールドにインターフェイスの説明を入力します。

ステップ 14 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの削除

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き Cisco Catalyst スイッチの機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

インターフェイスの定義はいつでも削除できますが、このオプションは慎重に使用してください。関連デバイスでポリシー定義にインターフェイス定義が含まれている場合は、インターフェイスを削除すると、これらのポリシー定義をデバイスに展開できなくなります。

関連項目

- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集（3407 ページ）
- インターフェイス （3406 ページ）

ステップ 1 （デバイス ビュー）デバイス セレクタから Cisco Catalyst スイッチまたは Cisco 7600 シリーズ ルータを選択します。

ステップ 2 ポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択します。

ステップ 3 作業領域で [Interfaces] タブをクリックします。

[Interfaces] タブが表示されます。このタブの各フィールドの説明については、[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）を参照してください。

ステップ 4 テーブルからインターフェイスを選択し、[行の削除（Delete Row）] をクリックします。インターフェイスが削除されます。

[Interfaces/VLANs] ページ - [Interfaces] タブ

[Interfaces] タブを使用して、サポートされている Cisco Catalyst スイッチと Cisco 7600 シリーズ ルータおよびそれらに関連付けられたサービス モジュール（ブレード）のインターフェイスやサブインターフェイスを表示および設定します。

ナビゲーション パス

（デバイス ビュー）デバイス セレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択し、[インターフェイス（Interfaces）] タブをクリックします。

関連項目

- [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）
- [Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）
- Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 （3404 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 946 : [Interfaces/VLANs] ページ - [Interfaces] タブ

要素	説明
名前	インターフェイス タイプ、シャーシ スロット、およびインターフェイス カードの番号。たとえば、*FastEthernet 2/7* は、ファストイーサネット、スロット 2、インターフェイス 7 を意味します。

要素	説明
[モード（Mode）]	物理ポートのコンフィギュレーション モード： • アクセス（Access） • ルーテッド • トランク • Dynamic Auto • Dynamic Desirable • 非サポート対象
VLAN ID（Admin. VLAN ID）	説明されたサブインターフェイスに関連付けられた VLAN ID。イーサネット インターフェイスおよび VLAN インターフェイスについてのみ表示されます。
IP Address	インターフェイスの IP アドレス。
[有効（Enabled）]	インターフェイスがイネーブルになっているかディセーブル（シャットダウン状態）になっているかを示します。
Interface Roles	命名パターンがこのインターフェイスと一致するインターフェイス ロール。インターフェイス ロール オブジェクトについて （381 ページ）を参照してください。
説明	（任意）インターフェイスの説明。
[Add Row] ボタン	新しいインターフェイスを定義できる [Create Interface] ダイアログボックスを開きます。詳細については、関連するモードの説明を参照してください。 • アクセス ポート モード：[Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）。 • ルーテッド ポート モード：[Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ） • トランク ポート モード：[Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ） • ダイナミック モード：[Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）

要素	説明
[Edit Row] ボタン	[インターフェイスの編集（Edit Interface）] ダイアログボックスを開きます。ここで、選択したインターフェイスを編集できます。詳細については、関連するモードの説明を参照してください。 • アクセス ポート モード： [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）。 • ルーテッド ポート モード： [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ） • トランク ポート モード： [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ） • ダイナミック モード： [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ） • サポートなし： [Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード （3433 ページ）
[Delete Row] ボタン	選択したインターフェイスを削除します。

[Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、アクセス ポート モードで稼働する物理インターフェイスや仮想インターフェイスの属性を設定します。

ナビゲーション パス

[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックして [インターフェイスの作成（Create Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスを開き、[モード（Mode）] リストから [アクセス ポート（Access Port）] を選択します。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）
- [Interface Auto Name Generator] ダイアログボックス （3020 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）

- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *947 : [Create Interface]/[Edit Interface]* ダイアログボックス - アクセス ポート モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。 オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ（Type）	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。 サブインターフェイスを定義する方法の詳細については、[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス （3431 ページ）を参照してください。
Name（[Select] ボタン）	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。 [Interface Auto Name Generator] ダイアログボックス （3020 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード（Mode）]	このインターフェイスのポート設定タイプ。 [アクセスポート（Access Port）] を選択すると、アクセスポートに関連する設定オプションが表示されます。
アクセス ポート設定	

要素	説明
VLAN ID（選択ボタン）	VLAN を選択した場合、アクセスポートモードで使用する VLAN のインターフェイス固有の ID が表示されます。それ以外の場合は、[選択（Select）] をクリックすると [VLAN Selector] ダイアログボックス （3449 ページ）が開きます。 VLAN ID は、サブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。有効値の範囲は 1 ～ 4094 です。接続されているデバイスで VLAN ID が予約されている場合があります。詳細については、デバイスのマニュアルを参照してください。マルチコンテキスト モードの場合、VLAN はシステム設定でしか設定できません。 （注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。メイン インターフェイスに VLAN を設定すると、デバイスに設定できる VLAN の数が多くなります。
Enable Port Security	このチェックボックスをオンにすると、ポートへのアクセスを許可される MAC アドレスを限定して、インターフェイスへの入力を制限できます。 オフにすると、ポート セキュリティがディセーブルになります。
最大MACアドレス（Max. MAC Addresses）	[Enable Port Security] がオンの場合にだけ適用されます。 インターフェイスのセキュア MAC アドレスの最大数。有効な値の範囲は 1 ～ 4097 です。 （注） セキュア MAC アドレスは、接続されたデバイスの MAC アドレスを使用して動的に設定されます。

要素	説明
Violation Policy	セキュリティ違反が発生した場合に実行されるアクション。 • [Port Security Protect]：セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。 • [ポートセキュリティ制限（Port Security Restrict）]：セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。さらに、SecurityViolation カウンタを 1 増やします。 • [Port Security Shutdown]：インターフェイスをただちに error-disabled 状態とし、SNMP トラップ通知を送信します。 セキュリティ違反は、セキュア MAC アドレスが最大数まで設定されたあと、アドレス テーブルに MAC アドレスが登録されていないワークステーションがインターフェイスにアクセスしようとした場合に発生します。
Enable VACL Capture	このチェックボックスをオンにすると、VACL キャプチャがイネーブルになります。キャプチャ ビットが設定されると、キャプチャ機能がイネーブルなポートで、転送されたパケットを受信できます。 オフにすると、VACL キャプチャがディセーブルになります。
Capture VLANs（[Select] ボタン）	転送された VLAN パケットを VACL で受信する必要のある VLAN を識別できます。このオプションは、[Enable VACL Capture] チェックボックスをオンにした場合にだけ使用できます。 カンマで区切られた VLAN ID のリストを入力するか、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。 VACL は、VLAN パケットが VLAN に最初にルーティングまたはブリッジングされた場合だけ、このパケットをキャプチャできます。キャプチャできるのは、転送されたパケットだけです。
共通インターフェイス設定	

要素	説明
速度	物理インターフェイスの速度。 • [10]：10 Mbps で送信します。 • [100]：100 Mbps で送信します。 • [1000]：1,000 Mbps で送信します。 • [10000]：10,000 Mbps で送信します。 • [Auto]：[Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。 • [Non-Negotiate]：リンクのネゴシエーションをディセーブルにします。
デュプレックス	インターフェイスのデュプレックス設定： • [Auto]：デュプレックス設定をオートネゴシエーションします。 • [Half]：データの送受信を同時には行いません。 • [Full]：データの送受信を同時に行います。 [Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。
[MTU]	最大伝送単位。これは、インターフェイスで処理できる最大パケット サイズ（バイト単位）です。有効な値の範囲は、インターフェイス タイプによって異なります。
説明	インターフェイスを説明するテキスト。復帰を使用しないで1行に最大240文字を入力します。 （注） マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。
Flow Control Receive	受信フレームのフロー制御設定。 • [Off]：ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。 • [On]：ネイバー ポートの要求に従って、ポートでフロー制御を使用します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。 フロー制御フレーム（別名ポーズ フレーム）は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。

要素	説明
Flow Control Send	送信フレームのフロー制御設定。 • [Off]：ポートはネイバー ポートにフロー制御フレームを送信しません。 • [On]：ポートはネイバー ポートにフロー制御フレームを送信します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。
ロール（Roles）	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイスIPアドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。インターフェイス ロール オブジェクトについて （381 ページ） を参照してください。

[Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、レイヤ 3 においてルーテッド ポート モードで稼働する物理インターフェイスの属性を設定します。

ナビゲーション パス

[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックして [インターフェイスの作成（Create Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスを開き、[モード（Mode）] リストから [ルーテッド ポート（Routed Port）] を選択します。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）
- ネットワーク/ホストオブジェクトについて （391 ページ）
- ポリシーのオブジェクトの選択 （288 ページ）

フィールド リファレンス

表 *948 : [Create Interface]/[Edit Interface]* ダイアログボックス - ルーテッド ポート モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。 オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ（Type）	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。 サブインターフェイスを定義する方法の詳細については、[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス （3431 ページ）を参照してください。
Name（[Select] ボタン）	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。 [Interface Auto Name Generator] ダイアログボックス （3020 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード（Mode）]	このインターフェイスのポート設定タイプ。 [ルーテッドポート（Routed Port）] を選択すると、ルーテッドポートに関連する設定オプションが表示されます。
ルーテッドポートの設定	
IP タイプ（IP Type）	ポートで使用する IP アドレスのタイプ。 • [Static IP]：インターフェイスで永続的な IP アドレスを使用することを指定し、関連する GUI 要素をアクティブにします。
IP Address（[Select] ボタン）	IP アドレスを入力するか、または [選択（Select）] をクリックして、IP アドレスを選択できる [ネットワーク/ホストセレクタ（Networks/Hosts Selector）] を開くことができます。
Helper IP Addresses（[Select] ボタン）	インターフェイスにヘルパー IP アドレスを割り当てることができます。ヘルパー IP アドレスによって、ブロードキャストの DHCP 要求が、DHCP サーバだけに送信されるユニキャストの要求に変換されます。

要素	説明
Mask	サブネット マスクを指定できます。ネットマスク値を入力するか、またはリストからネットマスクを選択できます。ネットマスクを入力する場合は、その値をドット付き 10 進表記（255.255.255.0 など）で指定するか、またはビット数（24 など）を入力します。 （注） ネットワークに接続されたインターフェイスに対して、255.255.255.254 または 255.255.255.255 を使用しないでください。これらのネットマスクを使用すると、インターフェイス上のすべてのトラフィックが停止します。
共通インターフェイス設定	
速度	物理インターフェイスの速度。 • [10]：10 Mbps で送信します。 • [100]：100 Mbps で送信します。 • [1000]：1,000 Mbps で送信します。 • [10000]：10,000 Mbps で送信します。 • [Auto]：[Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。 • [Non-Negotiate]：リンクのネゴシエーションをディセーブルにします。
デュプレックス	インターフェイスのデュプレックス設定： • [Auto]：デュプレックス設定をオートネゴシエーションします。 • [Half]：データの送受信を同時には行いません。 • [Full]：データの送受信を同時に行います。 [Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。
[MTU]	最大伝送単位。これは、インターフェイスで処理できる最大パケット サイズ（バイト単位）です。有効な値の範囲は、インターフェイス タイプによって異なります。
説明	インターフェイスを説明するテキスト。復帰を使用しないで 1 行に最大 240 文字を入力します。 （注） マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。

要素	説明
Flow Control Receive	受信フレームのフロー制御設定。 • [Off]：ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。 • [On]：ネイバー ポートの要求に従って、ポートでフロー制御を使用します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。 フロー制御フレーム（別名ポーズ フレーム）は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。
Flow Control Send	送信フレームのフロー制御設定。 • [Off]：ポートはネイバー ポートにフロー制御フレームを送信しません。 • [On]：ポートはネイバーポートにフロー制御フレームを送信します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。
ロール（Roles）	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。インターフェイス ロール オブジェクトについて （381 ページ） を参照してください。

[Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、トランク ポート モードで稼働する物理インターフェイスや仮想インターフェイスの属性を設定します。

ナビゲーション パス

[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックして [インターフェイスの作成（Create Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスを開き、[モード（Mode）] リストから [トランク ポート（Trunk Port）] を選択します。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *949 : [Create Interface]/[Edit Interface]* ダイアログボックス - トランク ポート モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。 オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ（Type）	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。 サブインターフェイスを定義する方法の詳細については、[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス （3431 ページ）を参照してください。
Name（[Select] ボタン）	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。 [Interface Auto Name Generator] ダイアログボックス （3020 ページ）を開くには、[選択（Select）]をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード（Mode）]	このインターフェイスのポート設定タイプ。 [トランクポート（Trunk Port）] を選択すると、トランクポートに関連する設定オプションが表示されます。
トランク ポート設定	

要素	説明
カプセル化	次のいずれかを選択します。 • [DOT1Q]：トランク リンクでの VLAN カプセル化を、IEEE 802.1Q 規格で定義されたカプセル化に指定します。イーサネット サブインターフェイスだけに適用されます。 • [ISL]：トランク リンクでの ISL カプセル化を指定します。10 ギガビット イーサネット ポートは ISL カプセル化をサポートしていません。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。メイン インターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。
Native VLAN（[Select] ボタン）	[VLAN ID] フィールドで指定された ID を使用して、このインターフェイスに関連付けるネイティブ VLAN を選択できます（ネイティブ VLAN に VLAN ID が指定されていない場合、デフォルト値は 1 です）。このオプションは、802.1Q トランクインターフェイスとして機能する物理インターフェイスを設定する場合にだけ適用されます。 カプセル化タイプとして DOT1Q を先に指定しておく必要があります。 トランク インターフェイスのネイティブ VLAN は、タグ付けされていないすべての VLAN パケットが論理的に割り当てられる VLAN です。これには、VLAN に関連付けられた管理トラフィックが含まれます。 オフにすると、ネイティブ VLAN はこのインターフェイスに関連付けられません。 （注） トランク インターフェイスのサブインターフェイスには、ネイティブ VLAN を設定できません。リンクの両端には必ず同じ [Native VLAN] 値を設定してください。同じ値を設定しないと、トラフィックが失われたり、間違った VLAN に送信される場合があります。 [VLAN Selector] ダイアログボックス （3449 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、指定したインターフェイスにネイティブ VLAN を関連付けることができます。
Enable DTP negotiation	このチェックボックスをオンにすると、ダイナミック トランキング プロトコル（DTP）ネゴシエーションがイネーブルになります。DTP は、デバイス間のトランク オートネゴシエーション（ISL および 802.1Q）を管理します。 オフにすると、DTP ネゴシエーションがディセーブルになります。

要素	説明
Allowed VLANs（[Select] ボタン）	トランクで許可される VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します（12,17,22 または 2-200 など）。有効な ID の範囲は 1 ～ 4094 です。 あるいは、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。このダイアログボックスで、トランクに含める VLAN を選択できます。
Prune VLANs（[Select] ボタン）	プルーニング可能な VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します（12,17,22 または 2-200 など）。 あるいは、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。このダイアログボックスで、プルーニング可能な VLAN を選択できます。
Enable VACL Capture	このチェックボックスをオンにすると、VACL キャプチャがイネーブルになります。キャプチャ ビットが設定されると、キャプチャ機能がイネーブルなポートで、転送されたパケットを受信できます。 オフにすると、VACL キャプチャがディセーブルになります。
Capture VLANs（[Select] ボタン）	転送された VLAN パケットを VACL で受信する必要のある VLAN を識別できます。このオプションは、[Enable VACL Capture] チェックボックスをオンにした場合にだけ使用できます。 カンマで区切られた VLAN ID のリストを入力するか、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。 VACL は、VLAN パケットが VLAN に最初にルーティングまたはブリッジングされた場合だけ、このパケットをキャプチャできます。キャプチャできるのは、転送されたパケットだけです。
Enable Port Security	IOS ソフトウェア バージョン 12.2(18)SXE2 以降を実行しているデバイスにだけ適用されます。 このチェックボックスをオンにすると、ポートへのアクセスを許可される MAC アドレスを限定して、インターフェイスへの入力を制限できます。 オフにすると、ポート セキュリティがディセーブルになります。 （注） このオプションを選択した場合、[Enable DTP Negotiation] オプションは自動的にオフになります。

要素	説明
[最大 MAC アドレス（Max. MAC Addresses）]	[Enable Port Security] がオンの場合にだけ適用されます。 インターフェイスのセキュア MAC アドレスの最大数。有効な値の範囲は 1 ～ 4097 です。 （注） セキュア MAC アドレスは、接続されたデバイスの MAC アドレスを使用して動的に設定されます。
Violation Policy	セキュリティ違反が発生した場合に実行されるアクション。 • [Port Security Protect]：セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。 • [ポートセキュリティ制限（Port Security Restrict）]：セキュア MAC アドレスを必要な数だけ削除してカウントが最大値を下回るまで、送信元アドレスが不明なパケットをドロップします。さらに、SecurityViolation カウンタを 1 増やします。 • [Port Security Shutdown]：インターフェイスをただちに error-disabled 状態とし、SNMP トラップ通知を送信します。 セキュリティ違反は、セキュア MAC アドレスが最大数まで設定されたあと、アドレス テーブルに MAC アドレスが登録されていないワークステーションがインターフェイスにアクセスしようとした場合に発生します。
共通インターフェイス設定	
速度	物理インターフェイスの速度。 • [10]：10 Mbps で送信します。 • [100]：100 Mbps で送信します。 • [1000]：1,000 Mbps で送信します。 • [10000]：10,000 Mbps で送信します。 • [Auto]：[Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。 • [Non-Negotiate]：リンクのネゴシエーションをディセーブルにします。

要素	説明
デュプレックス	インターフェイスのデュプレックス設定： • [Auto]：デュプレックス設定をオートネゴシエーションします。 • [Half]：データの送受信を同時には行いません。 • [Full]：データの送受信を同時に行います。 [Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。
[MTU]	最大伝送単位。これは、インターフェイスで処理できる最大パケット サイズ（バイト単位）です。有効な値の範囲は、インターフェイス タイプによって異なります。
説明	インターフェイスを説明するテキスト。復帰を使用しないで1行に最大240文字を入力します。 （注） マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。
Flow Control Receive	受信フレームのフロー制御設定。 • [Off]：ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。 • [On]：ネイバー ポートの要求に従って、ポートでフロー制御を使用します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。 フロー制御フレーム（別名ポーズ フレーム）は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。
Flow Control Send	送信フレームのフロー制御設定。 • [Off]：ポートはネイバー ポートにフロー制御フレームを送信しません。 • [On]：ポートはネイバー ポートにフロー制御フレームを送信します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。

要素	説明
ロール（Roles）	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。 インターフェイス ロール オブジェクトについて （381 ページ） を参照してください。

[Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、ダイナミック モードで稼働する物理インターフェイスや仮想インターフェイスの属性を設定します。ダイナミック ポートは、ネイバー ポートの設定に基づいてリンクをトランク リンクに変換できます。

ナビゲーション パス

[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックして [インターフェイスの作成（Create Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスを開き、[モード（Mode）] リストから [ダイナミック（Dynamic）] を選択します。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）
- [Interface Auto Name Generator] ダイアログボックス （3020 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *950 : [Create Interface]/[Edit Interface]* ダイアログボックス - ダイナミック モード

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、インターフェイスがイネーブルになります。 オフにすると、shutdown コマンドを使用してインターフェイスがディセーブルになります。
タイプ（Type）	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。 サブインターフェイスを定義する方法の詳細については、[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス （3431 ページ）を参照してください。
Name（[Select] ボタン）	名前が設定されている場合は、生成されたインターフェイスの名前を表示します。 [Interface Auto Name Generator] ダイアログボックス （3020 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、Security Manager がインターフェイス名の生成に使用する詳細情報を入力または編集できます。
[モード（Mode）]	このインターフェイスのポート設定タイプ。 [Dynamic] を選択すると、ダイナミックポートに関連する設定オプションが表示されます。
ダイナミック ポート設定	
Dynamic Mode	ダイナミック トランク モード： • [Auto]：ポートはリンクをトランク リンクに変換できます。ポートがトランク ポートになるのは、ネイバー ポートが [Trunk] または [Desirable] モードに設定されている場合です。 • [Desirable]：ポートはアクティブにリンクをトランク リンクに変換しようとします。
アクセス VLAN ID	ポートがトランキングリンクとして機能しない場合に使用するアクセス VLAN ID。ネイバー リンクが [Trunk]、[Auto]、または [Desirable] モードに設定されている場合に、このような状況になる可能性があります。 有効値の範囲は 1 ～ 4094 です。

要素	説明
カプセル化	次のいずれかを選択します。 • [DOT1Q]：トランク リンクでの VLAN カプセル化を、IEEE 802.1Q 規格で定義されたカプセル化に指定します。イーサネット サブインターフェイスだけに適用されます。 • [ISL]：トランク リンクでの ISL カプセル化を指定します。10 ギガビット イーサネット ポートは ISL カプセル化をサポートしていません。 • [Negotiate]：インターフェイスがネイバー インターフェイスの設定と機能に基づいて ISL または 802.1Q トランクになるように、ネイバーインターフェイスとネゴシエートすることを指定します。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。メイン インターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。
Native VLAN（[Select] ボタン）	[VLAN ID] フィールドで指定された ID を使用して、このインターフェイスに関連付けるネイティブ VLAN を選択できます（ネイティブ VLAN に VLAN ID が指定されていない場合、デフォルト値は 1 です）。このオプションは、802.1Q トランクインターフェイスとして機能する物理インターフェイスを設定する場合にだけ適用されます。 カプセル化タイプとして DOT1Q を先に指定しておく必要があります。 トランク インターフェイスのネイティブ VLAN は、タグ付けされていないすべての VLAN パケットが論理的に割り当てられる VLAN です。これには、VLAN に関連付けられた管理トラフィックが含まれます。 オフにすると、ネイティブ VLAN はこのインターフェイスに関連付けられません。 （注） トランク インターフェイスのサブインターフェイスには、ネイティブ VLAN を設定できません。リンクの両端には必ず同じ [Native VLAN] 値を設定してください。同じ値を設定しないと、トラフィックが失われたり、間違った VLAN に送信される場合があります。 [VLAN Selector] ダイアログボックス （3449 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、指定したインターフェイスにネイティブ VLAN を関連付けることができます。

要素	説明
Allowed VLANs（[Select] ボタン）	トランクで許可される VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します（12,17,22 または 2-200 など）。有効な ID の範囲は 1 ～ 4094 です。 あるいは、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。このダイアログボックスで、トランクに含める VLAN を選択できます。
Prune VLANs（[Select] ボタン）	プルーニング可能な VLAN を指定できます。VLAN ID を入力してください。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定します（12,17,22 または 2-200 など）。 あるいは、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。このダイアログボックスで、プルーニング可能な VLAN を選択できます。
Enable VACL Capture	このチェックボックスをオンにすると、VACL キャプチャがイネーブルになります。キャプチャ ビットが設定されると、キャプチャ機能がイネーブルなポートで、転送されたパケットを受信できます。 オフにすると、VACL キャプチャがディセーブルになります。
Capture VLANs（[Select] ボタン）	転送された VLAN パケットを VACL で受信する必要のある VLAN を識別できます。このオプションは、[Enable VACL Capture] チェックボックスをオンにした場合にだけ使用できます。 カンマで区切られた VLAN ID のリストを入力するか、[選択（Select）] をクリックして [VLAN Selector] ダイアログボックス （3449 ページ）を開きます。 VACL は、VLAN パケットが VLAN に最初にルーティングまたはブリッジングされた場合だけ、このパケットをキャプチャできます。キャプチャできるのは、転送されたパケットだけです。
共通インターフェイス設定	

要素	説明
速度	物理インターフェイスの速度。 • [10]：10 Mbps で送信します。 • [100]：100 Mbps で送信します。 • [1000]：1,000 Mbps で送信します。 • [10000]：10,000 Mbps で送信します。 • [Auto]：[Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。 • [Non-Negotiate]：リンクのネゴシエーションをディセーブルにします。
デュプレックス	インターフェイスのデュプレックス設定： • [Auto]：デュプレックス設定をオートネゴシエーションします。 • [Half]：データの送受信を同時には行いません。 • [Full]：データの送受信を同時に行います。 [Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。
[MTU]	最大伝送単位。これは、インターフェイスで処理できる最大パケット サイズ（バイト単位）です。有効な値の範囲は、インターフェイスタイプによって異なります。
説明	インターフェイスを説明するテキスト。復帰を使用しないで1行に最大240文字を入力します。 （注） マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。
Flow Control Receive	受信フレームのフロー制御設定。 • [Off]：ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。 • [On]：ネイバー ポートの要求に従って、ポートでフロー制御を使用します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。 フロー制御フレーム（別名ポーズ フレーム）は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。

要素	説明
Flow Control Send	送信フレームのフロー制御設定。 • [Off]：ポートはネイバー ポートにフロー制御フレームを送信しません。 • [On]：ポートはネイバー ポートにフロー制御フレームを送信します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。
ロール（Roles）	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイス IP アドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。インターフェイス ロール オブジェクトについて （381 ページ） を参照してください。

[Create Interface]/[Edit Interface] ダイアログボックス - サブインターフェイス

[Create Interface] ダイアログボックス（または [Edit Interface] ダイアログボックス）を使用して、Catalyst 6500/7600 デバイスに定義されているサブインターフェイスの属性を設定します。

ナビゲーション パス

[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）に移動し、[追加（Add）] または [編集（Edit）] をクリックして [インターフェイスの作成（Create Interface）]/[インターフェイスの編集（Edit Interface）] ダイアログボックスを開き、[タイプ（Type）] リストから [サブインターフェイス（Subinterface）] を選択します。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）
- インターフェイス ロール オブジェクトについて （381 ページ）

フィールド リファレンス

表 *951 : [Create Interface]/[Edit Interface]* ダイアログボックス - サブインターフェイス

要素	説明
[Enable Interface]	このチェックボックスをオンにすると、サブインターフェイスがイネーブルになります。 オフにすると、shutdown コマンドを使用してサブインターフェイスがディセーブルになります。
タイプ（Type）	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。[サブインターフェイス（Subinterface）] を選択します。
親	サブインターフェイスの親インターフェイスを識別します。
サブインターフェイスID（Subint. ID）ID	サブインターフェイスの ID アドレスを指定します。数値 ID 文字列は 10 文字を超えることはできません。
IP タイプ（IP Type）	サブインターフェースで使用される IP アドレスのタイプ: • [Static IP]：サブインターフェイスで永続的な IP アドレスを使用することを指定し、関連する GUI 要素をアクティブにします。
IPアドレス	IP アドレスを入力できます。
Helper IP Addresses	サブインターフェイスにヘルパー IP アドレスを割り当てることができます。ヘルパー IP アドレスによって、ブロードキャストの DHCP 要求が、DHCP サーバだけに送信されるユニキャストの要求に変換されます。
Mask	サブネットマスクを指定できます。ネットマスク値を入力するか、またはリストからネットマスクを選択できます。ネットマスクを入力する場合は、その値をドット付き 10 進表記（255.255.255.0 など）で指定するか、またはビット数（24 など）を入力します。 （注） ネットワークに接続されたインターフェイスに対して、255.255.255.254 または 255.255.255.255 を使用しないでください。これらのネットマスクを使用すると、インターフェイス上のすべてのトラフィックが停止します。

要素	説明
カプセル化	サブインターフェイスに定義するカプセル化タイプ： • [blank]：カプセル化は定義されません。 • [DOT1Q]：トランク リンクでの VLAN カプセル化を、IEEE 802.1Q 規格で定義されたカプセル化に指定します。イーサネット サブインターフェイスだけに適用されます。 • [ISL]：トランク リンクでの ISL カプセル化を指定します。10 ギガビット イーサネット ポートは ISL カプセル化をサポートしていません。 ヒント　VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。メインインターフェイスに VLAN を設定すると、ルータに設定できる VLAN の数が多くなります。
VLAN ID（Admin. VLAN ID）	サブインターフェイスにカプセル化が定義されている場合にだけ適用されます。 サブインターフェイスに関連付ける VLAN ID。
説明	インターフェイスを説明するテキスト。復帰を使用しないで 1 行に最大 240 文字を入力します。 （注）　マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。

[Create Interface]/[Edit Interface] ダイアログボックス - サポートされていないモード

Security Manager でサポートされていないモードが設定されたインターフェイスが検出された場合（dot1q-tunnel、private-vlan など）、そのインターフェイスは [Unsupported] モードで表示されます。このインターフェイスの属性を表示できますが、設定を変更する場合は、まずモードを変更する必要があります。[Mode] を除くすべての定義フィールドは読み取り専用です。

ナビゲーション パス

[Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）に移動し、モードが [サポート対象外（Unsupported）] として定義されているインターフェイスを選択します。次に、[追加（Add）] または [編集（Edit）] をクリックして [インターフェイスの作成/編集（Create/Edit Interface）] ダイアログボックスを開きます。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）

- [Create Interface]/[Edit Interface] ダイアログボックス - ルーテッド ポート モード （3417 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）
- [Create Interface]/[Edit Interface] ダイアログボックス - ダイナミック モード （3426 ページ）

フィールド リファレンス

表 *952 : [Create Interface]/[Edit Interface]* ダイアログボックス - サポートされていないモード

要素	説明
[Enable Interface]	このチェックボックスがオンになっている場合、インターフェイスはイネーブルになっています。 オフになっている場合、インターフェイスはshutdownコマンドを使用してディセーブルになっています。
タイプ（Type）	定義をインターフェイスに適用するか、サブインターフェイスに適用するかを指定します。
Name（[Select] ボタン）	インターフェイスの名前が表示されます。
[モード（Mode）]	[Unsupported] が表示されます。これは、モードが Security Manager によってサポートされないインターフェイスを示します。 インターフェイス モードを変更するには、別のオプションを選択します。 （注） インターフェイス モードを変更すると、このダイアログボックスの他の設定を変更できるようになります。
速度	物理インターフェイスの速度を表示します。 • [10]：10 Mbps で送信します。 • [100]：100 Mbps で送信します。 • [1000]：1,000 Mbps で送信します。 • [10000]：10,000 Mbps で送信します。 • [Auto]：[Speed] を [Auto] に設定すると、[Speed] および [Duplex] がどちらもオートネゴシエーションされます。 • [Non-Negotiate]：リンクのネゴシエーションをディセーブルにします。

要素	説明
デュプレックス	インターフェイスのデュプレックス設定が表示されます。 • [Auto]：デュプレックス設定をオートネゴシエーションします。 • [Half]：データの送受信を同時には行いません。 • [Full]：データの送受信を同時に行います。 [Speed] が [Auto] に設定されている場合は、デュプレックス設定も [Auto] に設定する必要があります。
[MTU]	最大伝送単位が表示されます。これは、インターフェイスで処理できる最大パケットサイズ（バイト単位）です。有効な値の範囲は、インターフェイス タイプによって異なります。
説明	インターフェイスを説明するテキストが表示されます。マルチコンテキストモードの場合、システムの説明とコンテキストの説明に関係はありません。
Flow Control Receive	受信フレームのフロー制御設定が表示されます。 • [Off]：ネイバー ポートがフロー制御を要求しても、ポートではフロー制御を使用しません。 • [On]：ネイバー ポートの要求に従って、ポートでフロー制御を使用します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。 フロー制御フレーム（別名ポーズフレーム）は、バッファが一杯になったときに、指定した間隔だけフレームの送信を停止するよう送信元にシグナリングする特別なパケットです。
Flow Control Send	送信フレームのフロー制御設定が表示されます。 • [Off]：ポートはネイバー ポートにフロー制御フレームを送信しません。 • [On]：ポートはネイバー ポートにフロー制御フレームを送信します。 • [Desired]：ポートでフロー制御フレームは許可されますが、必須ではありません。

要素	説明
ロール（Roles）	インターフェイスに関連付けられたインターフェイス ロールを表示します。インターフェイス ロールとは、各デバイスの設定が生成されるときに、実際のインターフェイスIPアドレスで置き換えられるオブジェクトです。インターフェイス ロールを使用すると、複数のインターフェイスに適用可能な汎用ルールを定義できます。インターフェイス ロール オブジェクトについて （381 ページ） を参照してください。

VLANs

VLANは、物理的な場所には基づかずに、論理的にセグメント化されたスイッチドネットワークです。たとえば、VLANは地理的に分散したワークグループのメンバーを相互接続する場合があります。VLAN は、人員、機器、およびネットワーク インフラストラクチャの物理的な配置を変更する必要性を減らすことで、多くの組織にとって実用的な利便性を提供します。正しく設定された VLAN はスケーラブルかつ安全であり、ネットワーク管理タスクを簡素化できます。

VLANは、単一のブリッジング ドメインで接続されたホストとネットワーク デバイス（ブリッジやルータなど）で構成されます。VLAN間のトラフィックは、ルーティングする必要があります。

Security Manager を使用すると、VLAN を作成して、Cisco Catalyst スイッチと Cisco 7600 シリーズ ルータ、およびそれらをサポートするサービス モジュールやセキュリティ コンテキストに対して定義されたインターフェイスに対する VLAN 設定を定義できます。

次の項では、Catalyst デバイスの VLAN を定義するときに実行できるアクションについて説明します。

- VLAN の作成または編集 （3436 ページ）
- VLAN の削除 （3438 ページ）
- [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）

関連項目

- VLAN グループ （3444 ページ）
- VLAN ACL（VACL） （3450 ページ）

VLAN の作成または編集

VLAN を作成、または VLAN の属性を再設定できます。

関連項目

- VLAN の削除 （3438 ページ）

- VLAN グループの作成または編集 （3444 ページ）
- VACL の作成または編集 （3451 ページ）
- [Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）
- VLANs （3436 ページ）

ステップ 1 （デバイス ビュー）Catalyst デバイスを選択し、ポリシー セレクタから [Interfaces/VLANs] を選択して作業領域で [VLANs] タブをクリックします。

[VLANs] タブが表示されます。このタブの各フィールドの説明については、 [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- 新しい VLAN の属性を定義するには、[行の追加（Add Row）] をクリックします。
- VLAN の属性を編集するには、リストで選択して [行の編集（Edit Row）] をクリックします。

ダイアログボックスにあるフィールドの説明については、[Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）を参照してください。

ステップ 3 [VLAN ID] フィールドに、VLAN の一意の ID 番号を入力します。ブリッジ グループ内の他の VLAN に割り当てられていない番号を入力する必要があります。

ステップ 4 （任意）VLAN の名前を入力します。

ステップ 5 （任意）VLAN が VLAN グループの一部である場合は、グループ ID を選択するか、または [グループの追加（Add Group）] を選択して [VLANグループの作成（Create VLAN Group）] ダイアログボックスを開きます。詳細については、 VLAN グループの作成または編集 （3444 ページ）を参照してください。

ステップ 6 [Status] リストから、VLAN のステータスを指定します（[Active] または [Suspended]）。

ステップ 7 [タイプ（Type）] リストから [レイヤ2（Layer 2）] または [レイヤ3（Layer 3）] を選択します。

ステップ 8 （任意）レイヤ 3 VLAN の場合、Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）を定義します。

a) SVI をアクティブにするには、[インターフェイスの有効化（Enable Interface）] チェックボックスをオンにします。SVI を使用すると、VLAN 間のルーティングが可能になり、スイッチへの IP ホスト接続が提供されます。このチェックボックスをオフにすると、SVI はシャットダウン モードで作成されます。

b) SVI の IP アドレスを入力します。

c) SVI サブネット マスクを入力するか、または [Subnet Mask] リストからネットマスクの値を選択します。

d) （任意）必要に応じて説明を入力します。

ステップ 9 次のいずれかまたは両方を実行します。

- アクセスポートを VLAN に関連付けるには、[アクセスポート（Access Ports）] テキストボックスにポート名を入力するか、または [選択（Select）] をクリックしてインターフェイスセレクタを開きます。

- トランクポートを VLAN に関連付けるには、[トランクポート（Trunk Ports）] テキストボックスにポート名を入力するか、または [選択（Select）] をクリックしてインターフェイスセレクタを開きます。

このダイアログボックスのフィールドの説明については、[Interface Selector] ダイアログボックス - VLAN ACL の内容 （3459 ページ）を参照してください。ポートの定義の詳細については、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集 （3407 ページ）を参照してください。

ステップ 10 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

VLAN の削除

VLAN を削除できます。ただし、VLAN を削除しても、その VLAN を参照する可能性があるポリシーからは削除されません。VLAN を削除する前に、他のポリシーでその VLAN が使用されていないことを確認してください。変更をデータベースに送信するときに、他のポリシーで参照されている未定義の VLAN が示されます。

関連項目

- VLAN の作成または編集 （3436 ページ）
- VLANs （3436 ページ）

ステップ 1 （デバイス ビュー）デバイス セレクタから Cisco Catalyst スイッチまたは Cisco 7600 シリーズ ルータを選択します。

ステップ 2 ポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択します。

ステップ 3 作業領域で [VLANs] タブをクリックします。

[VLANs] タブが表示されます。このタブの各フィールドの説明については、[Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）を参照してください。

ステップ 4 テーブルから VLAN を選択し、[行の削除（Delete Row）] をクリックします。

VLAN が削除されます。

[Interfaces/VLANs] ページ - [VLANs] タブ

[VLANs] タブを使用して、サポートされている Cisco Catalyst スイッチと Cisco 7600 シリーズ ルータの VLAN を表示および設定します。

ナビゲーション パス

- （デバイスビュー）デバイスセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択し、[VLANs] タブをクリックします。

関連項目

- [Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）
- [Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）
- Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 （3404 ページ）
- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）
- [Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 953 : [Interfaces/VLANs] ページ - [VLANs] タブ

要素	説明
VLAN ID（Admin. VLAN ID）	テーブルの行が示す VLAN のインターフェイス固有の ID。VLAN ID は、サブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。有効な値の範囲は 2 ～ 4094 です（VLAN ID 1 は予約されています）。 （注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネットインターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。メイン インターフェイスに VLAN を設定すると、デバイスに設定できる VLAN の数が多くなります。
名前	インターフェイスまたはサブインターフェイスの対応する VLAN の名前。
インターフェイス	インターフェイス（インターフェイスのロール）または物理的なインターフェイスの論理名を示します。
タイプ（Type）	VLAN が Layer 2 または Layer 3 にアクセスできるかどうかを指定します。
ステータス	VLAN がアクティブになっているか一時停止状態になっているかを示します。
[Add Row] ボタン	新しい VLAN を定義する [Create VLAN] ダイアログボックスを開きます。

要素	説明
[Edit Row] ボタン	選択した VLAN を編集する [Edit VLAN] ダイアログボックスを開きます。
[Delete Row] ボタン	選択した VLAN を削除します。

[Create VLAN]/[Edit VLAN] ダイアログボックス

[Create VLAN] ダイアログボックス（または [Edit VLAN] ダイアログボックス）を使用して、VLAN 設定および属性を設定または再設定します。

ナビゲーション パス

[Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- FlexConfig ポリシーとポリシー オブジェクトについて （432 ページ）
- [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス （3447 ページ）
- [Interface Selector] ダイアログボックス - VLAN ACL の内容 （3459 ページ）

フィールド リファレンス

表 *954 : [VLANの作成（Create VLAN）]/[VLANの編集（Edit VLAN）]* ダイアログボックス

要素	説明
VLAN ID（Admin. VLAN ID）	設定されている VLAN ID が表示されます。設定されていない場合は、ID を手動で入力します。VLAN ID は、インターフェイスまたはサブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、インターフェイスまたはサブインターフェイスでトラフィックを送受信できません。各 VLAN には ID が必要です。有効値の範囲は 1 ～ 4094 です。 （注） 同じ物理インターフェイスに設定されたすべてのサブインターフェイスでは、VLAN ID がすべて一意である必要があります。 ヒント VLAN をサブインターフェイスに関連付けずに、イーサネット インターフェイスで DOT1Q カプセル化を設定するには、CLI コマンドまたは FlexConfig を使用して **vlan-id dot1q** コマンドを使用します。メイン インターフェイスに VLAN を設定すると、デバイスに設定できる VLAN の数が多くなります。

要素	説明
名前	VLANの名前を入力します。VLAN名を以前に入力した場合は、その名前が表示されます。各 VLAN に ID が必要であり、名前は任意で指定できます。最大長は 32 文字です。
グループ	VLAN が属している VLAN グループ。VLAN は 1 つのグループだけに関連付けることができます。 VLAN を既存のグループに関連付けるか、または [グループの追加（Add Group）] を選択して [VLANグループの作成（Create VLAN Group）] ダイアログボックスを開きます。
ステータス	VLAN の現在のステータス： • [Active]：VLAN はトラフィックを伝送します。 • [Suspended]：VLAN はパケットを通過させません。
タイプ（Type）	指定された VLAN がレイヤ 2 とレイヤ 3 のどちらに設定されているかを示し、使用する VLAN の種類を選択できます。 レイヤ 3 VLAN の場合、IP アドレスが必要であり、VLAN インターフェイスが作成されます。
Switch Virtual Interface	レイヤ 3 VLAN を定義する場合にだけ適用されます。 • [Enable Interface]：このチェックボックスをオンにすると、任意の VLAN に接続可能な仮想インターフェイスである Switched Virtual Interface（SVI; スイッチ仮想インターフェイス）がイネーブルになります。SVI を使用すると、VLAN 間のルーティングが可能になり、スイッチへの IP ホスト接続が提供されます。オフにすると、SVI がディセーブルになります。 • [IP Address]：SVI の IP アドレス。IP アドレスは管理アクセスに必要です。 • [Subnet Mask]：SVI のサブネット マスク。有効なサブネット マスク エントリのリストからオプションを選択します。 • [Description]：復帰を使用しないで 1 行に最大 240 文字の説明を入力できます。マルチ コンテキスト モードの場合、システムの説明とコンテキストの説明に関係はありません。

要素	説明
Access Ports（[Select] ボタン）	指定した VLAN に関連付けられているアクセス ポートが表示され、指定した VLAN のアクセス ポートの関連付けを追加または削除できます。任意の数のアクセス ポートを VLAN に関連付けることができます。 [Access Port Selector] ダイアログボックス （3442 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、指定した VLAN にアクセス ポートを関連付けたり、VLAN からアクセス ポートの関連付けを削除したりできます。
Trunk Ports（[Select] ボタン）	指定した VLAN に関連付けられているトランク ポートが表示され、指定した VLAN のトランク ポートの関連付けを追加または削除できます。VLAN は、許可された 1 つ以上のトランク ポートに属することができます。トランク ポート グループに VLAN を含めることができます。 [Trunk Port Selector] ダイアログボックス （3443 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、指定した VLAN にトランク ポートを関連付けたり、VLAN からトランク ポートの関連付けを削除したりできます。

[Access Port Selector] ダイアログボックス

[Access Port Selector] ダイアログボックスを使用して、選択した VLAN に関連付けられているアクセス ポートを定義します。

ナビゲーション パス

[Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）を開き、[アクセスポート（Access Ports）] フィールドの [選択（Select）] をクリックします。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - アクセス ポート モード （3412 ページ）
- [Trunk Port Selector] ダイアログボックス （3443 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 955 : [Access Port Selector] ダイアログボックス

要素	説明
Available Access Ports	特定の VLAN に割り当てられていないアクセス ポートが表示されます。

要素	説明
[Add >>] ボタン	[Available Access Ports] リストで選択したインターフェイスを [Selected Access Ports] リストに追加します。
[Remove <<] ボタン	選択したインターフェイスを [Selected Access Ports] リストから削除します。
Selected Access Ports	選択されたインターフェイス オブジェクトを表示します。
[Add Row] ボタン	新しいインターフェイスを定義する [Create Interface] ダイアログボックスを開きます。
[Edit Row] ボタン	選択したインターフェイスを編集する [Edit Interface] ダイアログボックスを開きます。

[Trunk Port Selector] ダイアログボックス

[Trunk Port Selector] ダイアログボックスを使用して、選択した VLAN に関連付けるトランク ポートを定義します。

ナビゲーション パス

[Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）を開き、[トランクポート（Trunk Ports）] フィールドの [選択（Select）] をクリックします。

関連項目

- [Create Interface]/[Edit Interface] ダイアログボックス - トランク ポート モード （3420 ページ）
- [Access Port Selector] ダイアログボックス （3442 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *956 : [Trunk Port Selector]* ダイアログボックス

要素	説明
Available Trunk Ports	使用可能なすべてのトランク ポートが表示されます。
[Add >>] ボタン	[Available Trunk Ports] リストで選択したインターフェイスを [Selected Trunk Ports] リストに追加します。
[Remove <<] ボタン	選択したインターフェイスを [Selected Trunk Ports] リストから削除します。

要素	説明
Selected Trunk Ports	選択されたインターフェイス オブジェクトを表示します。
[Add Row] ボタン	新しいインターフェイスを定義する [Create Interface] ダイアログボックスを開きます。
[Edit Row] ボタン	選択したインターフェイスを編集する [Edit Interface] ダイアログボックスを開きます。

VLAN グループ

VLAN グループは、VLAN の論理集合を定義します。[Interfaces/VLANs] ページの [VLAN Groups] タブに、次の情報が表示されます。

- 選択したデバイスに定義されているすべての VLAN グループ。
- VLAN グループがバインドされているサービス モジュール スロット。
- 各 VLAN グループに属している VLAN。

VLAN グループは、VLAN を FWSM セキュリティ コンテキストに割り当てる場合に使用できます。VLAN グループを複数の FWSM に割り当てたり、各 FWSM に複数の VLAN グループを割り当てたりすることができます。この割り当てを実行するには、[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）を参照してください。

次の項では、Catalyst デバイスの VLAN グループを定義するときに実行できるアクションについて説明します。

- [Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）
- VLAN グループの削除 （3446 ページ）
- [Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）

関連項目

- インターフェイス （3406 ページ）
- VLANs （3436 ページ）
- VLAN ACL（VACL） （3450 ページ）

VLAN グループの作成または編集

VLAN グループを作成できます。VLAN グループを作成する場合は、次の点に留意してください。

- 各グループに ID が必要です。

- VLAN グループは 1 つ以上の FWSM モジュールに関連付けることができます。
- 各 VLAN を複数の VLAN グループのメンバーにすることはできません。

関連項目

- VLAN グループの削除 （3446 ページ）
- VLAN の作成または編集 （3436 ページ）
- VACL の作成または編集 （3451 ページ）
- [Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）
- VLAN グループ （3444 ページ）

ステップ 1 （デバイスビュー）Catalyst デバイスを選択し、ポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択して、作業領域で [VLANグループ（VLAN Groups）] タブをクリックします。

[VLAN Groups] タブが表示されます。このタブの各フィールドの説明については、[Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- 新しい VLAN グループの属性を定義するには、[行の追加（Add Row）] をクリックします。
- VLAN グループの属性を編集するには、リストでグループを選択して [行の編集（Edit Row）] をクリックします。

このダイアログボックスのフィールドの説明については、[Create VLAN Group]/[Edit VLAN Group] ダイアログボックス （3447 ページ）を参照してください。

ステップ 3 [VLAN Group ID] フィールドに、VLAN グループの一意の ID 番号を入力します。他の VLAN グループに割り当てられていない番号を入力する必要があります。

ステップ 4 VLAN グループを特定のサービスモジュールスロットに関連付けるには（[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ））、[サービスモジュールスロット（Service Module Slots）] テキストボックスにスロット番号を入力するか、[選択（Select）] をクリックしてセレクタを開きます。

（注） この関連付けを定義すると、あとでこの VLAN グループを FWSM のセキュリティ コンテキストに割り当てることができます。[Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM） （2986 ページ）を参照してください。

ステップ 5 VLAN グループに追加する VLAN を入力するか、[選択（Select）] をクリックしてセレクタを開きます。

ステップ 6 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

VLAN グループの削除

VLAN グループを削除できます。VLAN グループを削除しても、グループ内の VLAN には影響しません。

関連項目

- VLAN グループの作成または編集 （3444 ページ）
- VLAN グループ （3444 ページ）

ステップ 1 （デバイス ビュー）デバイス セレクタから Catalyst 6500 シリーズ スイッチまたは Cisco 7600 シリーズ ルータを選択します。

ステップ 2 ポリシーセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択します。

ステップ 3 作業領域で [VLAN Groups] タブをクリックします。

[VLANs] タブが表示されます。このタブの各フィールドの説明については、[Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）を参照してください。

ステップ 4 テーブルから VLAN グループを選択し、[行の削除（Delete Row）] をクリックします。VLAN グループが削除されます。

[Interfaces/VLANs] ページ - [VLAN Groups] タブ

[VLAN Groups] タブを使用して、サポートされている 6500 シリーズ スイッチおよび 7600 シリーズ ルータの VLAN グループを表示および設定します。

（注） [VLAN Groups] タブは、Cisco Catalyst 6500 シリーズ スイッチおよび Cisco 7600 シリーズ ルータの場合だけ使用できます。

ナビゲーション パス

- （デバイスビュー）デバイスセレクタから [インターフェイス/VLAN（Interfaces/VLANs）] を選択し、[VLANグループ（VLAN Groups）] タブをクリックします。

関連項目

- [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）
- [Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ）
- Catalyst インターフェイス、VLAN、および VLAN グループの概要の表示 （3404 ページ）
- [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス （3447 ページ）

- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 957 : [Interfaces/VLANs] ページ - [VLAN Groups] タブ

要素	説明
VLAN Group	選択したデバイスに設定されている VLAN グループの数値 ID。
Service Module Slots	シャーシスロット番号（関連サービスモジュールの取り付け先）を、特定の VLAN が VLAN グループへの参加に使用するインターフェイスに関連付けます。
VLAN IDs	このグループに関連付けられている VLAN ID。有効値の範囲は 1 ～ 65535 です。
[Add Row] ボタン	新しい VLAN グループを定義する [Create VLAN Group] ダイアログボックスを開きます。
[Edit Row] ボタン	選択した VLAN グループを編集する [Edit VLAN Group] ダイアログボックスを開きます。
[Delete Row] ボタン	選択した VLAN グループを削除します。

[Create VLAN Group]/[Edit VLAN Group] ダイアログボックス

[Create VLAN Group]/[Edit VLAN Group] ダイアログボックスを使用して、VLAN グループの属性を設定または再設定します。VLAN グループは、VLAN ポート ポリシーを定義するときに相互に関連付ける VLAN の論理グループです。

ナビゲーション パス

次のいずれかを実行します。

- [Interfaces/VLANs] ページ - [VLAN Groups] タブ （3446 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。
- [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）に移動し、テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックして [グループ（Group）] リストから [グループの追加（Add Group）] を選択します。

関連項目

- [Service Module Slot Selector] ダイアログボックス （3448 ページ）

フィールド リファレンス

表 958 : [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス

要素	説明
VLAN Group ID	802.1q VLAN グループ名。有効値の範囲は 1 ～ 65535 です。
Service Module Slots（[Select] ボタン）	特定の VLAN が VLAN グループへの参加に使用するインターフェイスに関連付けられる、シャーシ スロット番号（関連サービス モジュールの取り付け先）。 スロット番号を入力するか、または [選択（Select）] をクリックして [Service Module Slot Selector] ダイアログボックス （3448 ページ）を開きます。 （注） VLAN グループを FWSM などのサービス モジュールに関連付けたあとで、VLAN グループを FWSM のセキュリティ コンテキストに割り当てることができます。 [Add Security Context]/[Edit Security Context] ダイアログボックス（FWSM）（2986 ページ）を参照してください。
VLAN IDs（[Select] ボタン）	グループに含まれるすべての VLAN のカンマで区切られた ID。各 VLAN を複数のグループのメンバーにすることはできません。 [Service Module Slot Selector] ダイアログボックス （3448 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、VLAN グループに含める VLAN を選択できます。

[Service Module Slot Selector] ダイアログボックス

[Service Module Slot Selector] ダイアログボックスを使用して、サービス モジュールを VLAN に関連付けます。

ナビゲーション パス

[Create VLAN Group]/[Edit VLAN Group] ダイアログボックス （3447 ページ）に移動し、[サービスモジュールスロット（Service Module Slots）] フィールドの [選択（Select）] をクリックします。

関連項目

- [VLAN Selector] ダイアログボックス （3449 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *959 : [Service Module Selector]* ダイアログボックス

要素	説明
Available Service Module Slots	定義されているサービス モジュール スロットが表示されます。
[Add >>] ボタン	選択したサービス モジュール スロットを [Available Service Module Slots] リストから [Selected Service Module Slots] リストに移動します。
[Remove <<] ボタン	選択したサービスモジュールスロットを [選択したサービスモジュール（Selected Service Module）] リストから削除します。
選択したサービスモジュールスロット（Selected Service Module Slots）	選択したサービス モジュール スロットが表示されます。

[VLAN Selector] ダイアログボックス

[VLAN Selector] ダイアログボックスを使用して、VLAN をインターフェイス、VLAN グループ、セキュリティ コンテキスト、および VACL に関連付けます。

ナビゲーション パス

インターフェイス、VLAN グループ、IDSM 設定、または VACL を定義するときにこのダイアログボックスにアクセスするには、VLAN の定義に使用するフィールドの [選択（Select）] ボタンをクリックします。

関連項目

- [Service Module Slot Selector] ダイアログボックス （3448 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *960 : [VLAN Selector]* ダイアログボックス

要素	説明
Available VLANs	設定するオブジェクトに関連付けることができる定義済みの VLAN が表示されます。 （注） 使用可能な VLAN は、設定するオブジェクトのタイプおよびデバイスに定義されているその他の設定によって異なります。たとえば、VLAN グループに割り当てる VLAN を選択する場合、[Available VLANs] リストには、別の VLAN グループに割り当てられていない VLAN だけが含まれます。セキュリティ コンテキストに割り当てる VLAN を選択する場合、[Available VLANs] リストには、設定するサービス モジュールに割り当てられている VLAN グループ内の VLAN だけが含まれます。
[Add >>] ボタン	選択した VLAN を [Available VLANs] リストから [Selected VLANs] リストに移動します。
[Remove <<] ボタン	選択した VLAN を [Selected VLANs] リストから削除します。
Selected VLANs	選択した VLAN が表示されます。
VLAN の範囲	セレクタを開く前に手動で入力された VLAN 範囲（ある場合）。

VLAN ACL（VACL）

Cisco IOS の標準 ACL と拡張 ACL は、ルータ インターフェイスに対してだけ設定し、ルーティングされるパケットにだけ適用されます。一方、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでは、VLAN ACL（VACL）を使用して、VLAN 内でブリッジングされるすべてのパケット、または WAN インターフェイスを介した VACL キャプチャのために VLAN との間でルーティングされるすべてのパケットのアクセスを制御できます。VACL の特徴は次のとおりです。

- ハードウェアで処理されます。
- Cisco IOS ACL を使用します。
- ハードウェアでサポートされていない Cisco IOS ACL フィールドを無視します。

（注） Security Manager では、MAC ACL（MACL）の作成または設定はサポートされません。MACL は、MAC アドレスに基づいて IPX、DECnet、AppleTalk、VINES、または XNS トラフィックをフィルタリングするために、VACL とともに使用されることがある名前付き ACL です。

VACL を設定して VLAN に適用すると、VLAN に着信するすべてのパケットは VACL に基づいてチェックされます。

VACL を VLAN に適用し、その同じ VLAN 内のルーテッド インターフェイスに ACL を適用すると、VLANに着信するパケットは、まずVACLに基づいてチェックされます。次に、許可されたパケットは、ルーテッド インターフェイスに到達する前に入力 ACL に基づいてチェックされます。

パケットは、ある VLAN から別の VLAN にルーティングされる場合、まずルーテッド インターフェイスに適用される出力 ACL に基づいてチェックされます。次に、許可されたパケットは、宛先 VLAN に設定された VACL に基づいてチェックされます。

パケット タイプに VACL が設定され、そのタイプのパケットが VACL と一致しない場合のデフォルト アクションは拒否です。

VLAN アクセスマップ（VLAN Access Maps）

Security Manager では、VLAN アクセスマップを使用して VACL を設定します。VLAN アクセスマップは概念的にはルートマップと似ており、1 つ以上のステートメント（アクションと一致する条件）を配置したり、重要度に基づいて番号を付けたりするコンテナです。VLANアクセス マップでは、マップが適用される VLAN を指定したり、マップ名を含めたり、少なくとも 1 つの VACL シーケンスを指定したりする必要もあります。

VACL シーケンスにはシーケンス番号と少なくとも 1 つのアクションが必要であり、VACL シーケンスは少なくとも 1 つの ACL と一致する必要があります。

デバイスはシーケンス内のマップ ステートメントを評価します。複数の VLAN アクセス マップを任意のデバイス シャーシに関連付けることができます。

VACL を管理するには、デバイスビューで Catalyst デバイスを選択し、**[プラットフォーム（Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** を選択します。VLAN アクセスマップを使用して IP トラフィックの VACL を設定します。

次の項では、Catalyst デバイスの VACL を定義するときに実行できるアクションについて説明します。

- VACL の作成または編集 （3451 ページ）
- VACL の削除 （3453 ページ）
- [VLAN Access Lists] ページ （3454 ページ）

関連項目

- VLANs （3436 ページ）
- VLAN グループ （3444 ページ）

VACL の作成または編集

VACL を作成または編集できる場合は、次の操作を実行する必要があります。

- VACL に名前を付けます。
- VACL が適用される VLAN を定義します。
- 少なくとも 1 つの VACL シーケンスが含まれるシーケンス マップを定義します。

関連項目

- VACL の削除 （3453 ページ）
- VLAN の作成または編集 （3436 ページ）
- VLAN グループの作成または編集 （3444 ページ）
- [Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス （3456 ページ）
- [VLAN Access Lists] ページ （3454 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）Catalyst デバイスを選択してから、ポリシーセレクタで **[プラットフォーム（Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** の順に選択します。
- （ポリシービュー）**[Catalystプラットフォーム（Catalyst Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** の順に選択します。

[VLAN Access Lists] ページが表示されます。このページにあるフィールドの説明については、[VLAN Access Lists] ページ （3454 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- 新しい VACL の属性を定義するには、[行の追加（Add Row）] をクリックします。
- VACL の属性を編集するには、リストで選択して [行の編集（Edit Row）] をクリックします。

ダイアログボックスが表示されます。ダイアログボックスにあるフィールドの説明については、[Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス （3456 ページ）を参照してください。

ステップ 3 [VLAN ACL名（VLAN ACL Name）] フィールドに VACL の名前を入力します。

ステップ 4 [VLANs] フィールドで、VACL を適用する VLAN を指定するか、または [選択（Select）] をクリックして VLAN セレクタを開きます。

ステップ 5 シーケンス マップを定義します。

a) [シーケンスマップ（Sequence Map）] テーブルの下にある [行の追加（Add Row）] または [行の編集（Edit Row）] をクリックします。ダイアログボックスが表示されます。[Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス （3457 ページ）を参照してください。

b) シーケンスを識別する番号を入力します。

c) シーケンスに割り当てる標準 ACL または拡張 ACL を指定します。または、[選択（Select）] をクリックしてリストから ACL オブジェクトを選択するか、新しい ACL オブジェクトを作成します。ACL オ

ブジェクトの詳細については、アクセス コントロール リスト オブジェクトの作成 （356 ページ）を参照してください。

d) このシーケンスで定義されている ACL と一致するトラフィックに対して実行するアクションを指定します（アクションとして [リダイレクト（Redirect）] を選択した場合は、物理的な宛先インターフェイスを指定するか、または [選択（Select）] をクリックしてセレクタを表示します。ポリシー定義中のインターフェイスの指定 （386 ページ） を参照してください）。

e) [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。シーケンスが [Sequence Map] テーブルに表示されます。

f) プロセスを繰り返して、シーケンスをシーケンス マップに追加します。

g) 上向きおよび下向き矢印を使用して、必要に応じてシーケンスを並べ替えます。

（注） シーケンスを配置する順序が重要です。フローが許可 ACL エントリと一致する場合、関連付けられたアクションが実行され、残りのシーケンスはチェックされません。フローが拒否 ACL エントリと一致する場合、フローは同じシーケンス内の次の ACL または次のシーケンスに基づいてチェックされます。フローがどの ACL エントリとも一致せず、1 つまたは複数の ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。

VACL の削除

デバイス、ポリシー、またはオブジェクトで使用されていない VACL は削除できます。

はじめる前に

データベースから VACL を削除する前に、VACL へのすべての参照を削除する必要があります。VACL へのすべての参照を確認するには、その VACL のオブジェクト使用状況レポートを実行します。オブジェクト使用状況レポートの生成 （306 ページ） を参照してください。

関連項目

- VACL の作成または編集 （3451 ページ）
- [Interfaces/VLANs] ページ - [VLANs] タブ （3438 ページ）
- VLAN ACL（VACL） （3450 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）Catalyst デバイスを選択してから、ポリシーセレクタで **[プラットフォーム（Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** の順に選択します。
- （ポリシービュー）**[Catalystプラットフォーム（Catalyst Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** の順に選択します。

[VLAN Access Lists] ページが表示されます。このページにあるフィールドの説明については、を参照してください。

ステップ 2 行をクリックして VACL を選択し、[削除（Delete）] をクリックします。
ステップ 3 [OK] をクリックして変更を保存します。 [VLAN Access Lists] ページ （3454 ページ）

[VLAN Access Lists] ページ

[VLAN Access Lists] ページを使用して、Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータの VLAN アクセス リストを表示および設定します。

ナビゲーション パス

このページには次の手順でアクセスできます。

- （デバイスビュー）デバイスポリシーセレクタから **[プラットフォーム（Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** の順に選択します。
- （デバイスビュー）ポリシータイプセレクタから **[プラットフォーム（Platform）] > [VLANアクセスリスト（VLAN Access Lists）]** の順に選択します。

関連項目

- アクセス コントロール リスト オブジェクトの作成 （356 ページ）
- [Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス （3456 ページ）
- [Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス （3457 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 961 : [VLAN Access Lists] ページ

要素	説明
[VLAN Access Lists] テーブル	
VLAN ACL	VLAN ACL 名が表示されます。
シーケンス	マップ シーケンス番号を指定します。VACL シーケンスは、小さい番号から大きい番号の順に適用されます。
マッチング	一致 ACL が表示されます（定義されている場合）。VACL のマッチングは、ACL 許可が見つかった場合にだけ実行されます。ACL 拒否は無視されます。

要素	説明
操作	アクションとして、パケットのドロップ、ドロップと記録、転送、転送とキャプチャ、またはリダイレクトのいずれかを指定します。 （注） リダイレクト アクションを使用すると、最大 5 つのインターフェイス（物理インターフェイスまたはEtherChannel）を指定できます。EtherChannel メンバまたはVLANインターフェイスにはパケットをリダイレクトできません。
VLAN IDs	テーブルの行が示す VLAN のインターフェイス固有の ID。VLAN ID は、サブインターフェイスで 802.1Q タグ付きパケットを送受信する場所を示します。VLAN ID が指定されていない場合は、サブインターフェイスでトラフィックを送受信できません。
[Add Row] ボタン	新しい VACL を定義できる [Create VLAN ACL] ダイアログボックスを開きます。
[Edit Row] ボタン	選択した VACL を編集できる [Edit VLAN ACL] ダイアログボックスを開きます。
[Delete Row] ボタン	選択したアクセス リストを削除します。
その他のフィールド	
Log Table Size	ログ テーブルのサイズが表示されます。 有効なサイズの範囲は 0 ～ 2048 で、デフォルトは 500 です。新しいフローからの記録済みパケットは、テーブルが一杯になるとドロップされます。
最大パケットレート	秒あたりの最大リダイレクト VACL ロギング パケット レートが表示されます。 有効なレートの範囲は秒あたり 10 ～ 5000 パケットで、デフォルト レートは 2000 です。制限を超えるパケットはドロップされます。
Logging Threshold	ロギングしきい値が表示されます（設定されている場合）。デフォルトでは、しきい値は設定されません。 VACL ロギングを設定した場合、フローのしきい値に達すると、拒否された IP パケットにより、5 分未満の間隔でフローごとにログ メッセージが生成されます。記録できるのは、ドロップされた IP パケットだけです。

要素	説明
Capture Interfaces	キャプチャ ビットが設定された転送されるパケットをキャプチャするインターフェイスを示します。任意のインターフェイスをキャプチャ インターフェイスとして設定できます。 captureアクションを指定すると、転送されたパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。 （注） ここに表示される情報は読み取り専用です。キャプチャ インターフェイスを定義するには、[Create Interface]/[Edit Interface] ダイアログボックスを使用します。 [Interfaces/VLANs] ページ - [Interfaces] タブ （3410 ページ） を参照してください。

[Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス

[Create VLAN ACL] ダイアログボックス（または [Edit VLAN ACL] ダイアログボックス）を使用して、VACL 属性を設定または再設定します。

ナビゲーション パス

[VLAN Access Lists] ページ （3454 ページ）に移動してから、テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）
- [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス （3447 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 962 : [Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス

要素	説明
VLAN ACL Name	VACL のユーザ定義名。

要素	説明
VLANs（[Select] ボタン）	VACL を適用する VLAN を指定できます。次のいずれかを実行します。 • VLAN ID を入力します。カンマを使用して複数の VLAN を区切るか、またはハイフンを使用して VLAN の範囲を指定できます。たとえば、12,17,22、2-200 など。有効な ID の範囲は 1 ～ 4094 です。 • [VLAN Selector] ダイアログボックス （3449 ページ）を開くには、[選択（Select）] をクリックします。
[Sequence Map] テーブル	VLAN アクセス マップに含まれるシーケンス マップ。 VLANアクセスマップは、1つ以上のマップシーケンスで構成される場合があります。各シーケンスでは、トラックフィルタリング用の ACL オブジェクトを指定する match 句および一致 ACL で定義されている基準を満たすパケットに対して実行するアクションを指定する action 句がペアになっています。 • シーケンス マップを追加するには、[Add Row]（+）ボタンをクリックし、[Create VLAN ACL Content] ダイアログボックスに入力します（[Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス （3457 ページ）を参照）。 • シーケンス マップを編集するには、そのマップを選択して [Edit Row] ボタンをクリックします。 • シーケンスマップを削除するには、そのマップを選択して [Delete Row] ボタンをクリックします。 • マップの順序を変更するには、マップを選択し、マップが目的の位置に配置されるまで上矢印ボタンまたは下矢印ボタンをクリックします。シーケンス番号は、移動すると変わります。

[Create VLAN ACL Content]/[Edit VLAN ACL Content] ダイアログボックス

[Create VLAN ACL Content] ダイアログボックス（または [Edit VLAN ACL Content] ダイアログボックス）を使用して、VACL シーケンスを設定または再設定します。

ナビゲーション パス

[Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス （3456 ページ）に移動してから、[シーケンスマップ（Sequence Map）] テーブルの下にある [追加（Add）] ボタンまたは [編集（Edit）] ボタンをクリックします。

関連項目

• [Create VLAN]/[Edit VLAN] ダイアログボックス （3440 ページ）

- [Create VLAN Group]/[Edit VLAN Group] ダイアログボックス （3447 ページ）

フィールド リファレンス

表 *963 : [Create VLAN ACL Content]/[Edit VLAN ACL Content]* ダイアログボックス

要素	説明
シーケンス	VLAN アクセス マップのマップ シーケンス番号を指定します。有効値の範囲は 1 ～ 65535 です。
Match ACLs	シーケンスの match 句に含める ACL を指定します。 シーケンスに含める標準 ACL オブジェクトまたは拡張 ACL オブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから ACL を選択するか、または新しい ACL を作成します。 MAC レイヤ ACL は使用できません。
操作	一致 ACL で定義されている基準を満たすパケットに対して実行するオプション。 • [Drop]：パケットをドロップします。 • [Drop/Log]：ドロップされたパケットをログに記録します。 • [Forward]：ハードウェア スイッチングを使用してパケットを宛先に転送します。 • [Forward/Capture]：転送されるパケットにキャプチャ ビットを設定して、キャプチャ機能が有効なポートでこのパケットも受信するようにします。 • [Redirect]：[Interfaces] フィールドで定義されているイーサネット インターフェイスにパケットをリダイレクトします。
Interfaces（[Select] ボタン）	指定したアクションが [Redirect] の場合にだけ適用されます。 リダイレクト パケットの宛先インターフェイス。最大 5 つの物理インターフェイスの名前を入力するか、または [選択（Select）] をクリックして [Interface Selector] ダイアログボックス - VLAN ACL の内容 （3459 ページ） を開きます。リダイレクト インターフェイスは、VACL アクセス マップが設定されている VLAN 内にある必要があります。 （注） EtherChannel メンバまたは VLAN インターフェイスにはパケットをリダイレクトできません。サブインターフェイスにもパケットをリダイレクトできません。

[Interface Selector] ダイアログボックス - VLAN ACL の内容

VACL シーケンス マップのエントリを作成するときに、[Interface Selector] ダイアログボックスを使用して、リダイレクト インターフェイスを定義します。

ナビゲーション パス

- [Create VLAN ACL]/[Edit VLAN ACL] ダイアログボックス （3456 ページ）
- [VLAN Access Lists] ページ （3454 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 964 : [Interface Selector] ダイアログボックス

要素	説明
Available Interfaces	[Interfaces/VLANs] ポリシーで定義されている物理インターフェイスが表示されます。
[Add >>] ボタン	[Available Interfaces] リストで選択されているインターフェイスを [Selected Interfaces] リストに追加します。
[Remove <<] ボタン	選択したインターフェイスを [Selected Interfaces] リストから削除します。
選択されたインターフェイス	選択したインターフェイスが表示されます。

IDSM 設定

デバイスビューで Catalyst デバイスを選択し、ポリシーセレクタから [プラットフォーム（Platform）] > [IDSM設定（IDSM Settings）] を選択すると、次のリストが表示されます。

- Intrusion Detection System Service Module（IDSM）のデータ ポートの設定が表示されます。
- このリストは、IDSM データ ポートをチャネル グループに整理するのに役立ちます。

IDSM カードは、ネットワーク接続上のセキュリティ脅威を検出し、阻止します。2 つのデータ ポートに着信したトラフィックを検査し、セキュリティ脅威が検出された場合はパケットをドロップします。データ ポート設定では、次の定義を行います。

- VLAN ID で定義されたデータ ポートで受信するトラフィック
- データ ポートで使用する検知モード：
  - [Trunk (IPS)]：IDSM は 802.1q トランクとして動作し、同じデータ ポート内にある VLAN ペア間で VLAN ブリッジングを実行します。IDSM は、VLAN ペアの各 VLAN

上で受信するトラフィックを検査し、そのパケットをペアのもう一方のVLANに転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。

- [Capture (IDS)]：IDSMは、VACLキャプチャまたはSPANを使用して、Catalystスイッチがデータ ポートにコピーしたネットワーク トラフィックをパッシブにモニタします。データ ポートは、別のVLANをトランキングするように設定できる802.1qトランクとして動作します。このパッシブ モードで動作している場合、IDSMはネットワーク侵入の試行が検出されてもパケットをドロップできませんが、侵入をブロックする目的でデータ ポートを介してTCPリセットを送信できます。

（注） Security Managerは、IOS 12.2(18)SXF4以降が実行されているシャーシにおける一部のIDSM設定がサポートされます。トランク（IPS）モードとキャプチャ（IDS）モードはサポートされますが、インライン モードはサポートされません。Security Managerでは、スパニングツリーまたはアクセスVLANの一部であるIDSMデータ ポートを管理できません。

トラフィックの多いネットワークでは、EtherChannelを使用して複数のデータ ポート間でロード バランシングを実行します。これらのデータ ポートは、同じCatalystデバイス内の異なるIDSMカードに配置できます。

EtherChannelを使用して、ポート障害時にトラフィックがチャネル グループ内の残りのポートにリダイレクトされることもあります。このような復元力により、ユーザによる介入なしに最小限のパケット損失で侵入の検出や防御を維持できます。

次の項では、IDSM設定を定義するときに実行できるアクションについて説明します。

- EtherChannel VLAN 定義の作成または編集 （3460 ページ）
- EtherChannel VLAN 定義の削除 （3462 ページ）
- データ ポート VLAN 定義の作成または編集 （3463 ページ）
- データ ポート VLAN 定義の削除 （3464 ページ）
- [IDSM Settings] ページ （3465 ページ）

関連項目

- VLANs （3436 ページ）
- Cisco Catalyst スイッチおよび Cisco 7600 シリーズ ルータでのポートの作成または編集 （3407 ページ）

EtherChannel VLAN 定義の作成または編集

EtherChannel VLAN 定義を行う場合は、次の操作を実行する必要があります。

- チャネル グループに追加するデータ ポートを含む、スロットとポートの組み合わせを定義します。
- データ ポートで使用する検知モードを選択します。
- データ ポートに転送する VLAN を定義します。

次の制約事項が適用されます。

- チャネル グループごとに 1 つの定義しか保持できません。
- スロットとデータ ポートの組み合わせごとに1つの定義しか保持できません。つまり、このスロットとデータ ポートに対してすでにデータ ポート定義が存在する場合は、EtherChannel VLAN 定義を作成できません。

関連項目

- EtherChannel VLAN 定義の削除 （3462 ページ）
- データ ポート VLAN 定義の作成または編集 （3463 ページ）
- IDSM 設定 （3459 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）Catalyst デバイスを選択してから、ポリシーセレクタで [プラットフォーム（Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。
- （ポリシービュー）[Catalystプラットフォーム（Catalyst Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[IDSM Settings] ページ （3465 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- IDSM EtherChannel VLAN 定義を作成するには、[EtherChannel VLANs] テーブルの下にある [行の追加（Add Row）] をクリックします。
- IDSM EtherChannel VLAN 定義を編集するには、リストで定義を選択し、テーブルの下にある [行の編集（Edit Row）] をクリックします。

[IDSM EtherChannel VLAN] ダイアログボックスが表示されます。このダイアログボックスにあるフィールドの説明については、[Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス （3467 ページ）を参照してください。

ステップ 3 VLAN のイーサネット インターフェイスにチャネルグループ番号を割り当てたり、チャネルグループ番号を変更したりするには、[チャネルグループ（Channel Group）] テキストボックスに番号を入力します。

ステップ 4 IDSM サービス モジュールを取り付けた番号付きシャーシ スロットに VLAN を関連付け、その VLAN に 1 つのモジュール データ ポートを関連付けるには、次のいずれかを実行します。

- [スロット/ポート（Slot-Ports）] テキストボックスにスロット/ポート番号を入力します。
- [選択（Select）] をクリックして、[IDSMスロット/ポートセレクタ（IDSM Slot-Port Selector）] ダイアログボックスを開きます。

（注） 1 つのモジュール データ ポートを VLAN に関連付けると、データ ポートを手動で設定する代わりに、グループ レベルでポートを設定できます。

ステップ 5 [Mode] リストから、EtherChannel VLAN の動作モードを選択します。[Capture] を選択する場合は、チェックボックスをオンにして、指定したチャネル グループをキャプチャ先として設定します。

（注） このチェックボックスをオンにしなかった場合、キャプチャ ポートはシャットダウン モードで作成されます。

ステップ 6 指定したチャネル グループに VLAN を含めるには、次のいずれかを実行します。

- [VLAN IDs] テキスト ボックスで数値 ID を入力します。
- [選択（Select）] をクリックして、[VLANセレクタ（VLAN Selector）] ダイアログボックスを開きます。

複数の VLAN ID を入力または選択できます。

ステップ 7 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

EtherChannel VLAN 定義の削除

IDSM の EtherChannel VLAN 定義を削除できます。

関連項目

- EtherChannel VLAN 定義の作成または編集 （3460 ページ）
- データ ポート VLAN 定義の削除 （3464 ページ）
- IDSM 設定 （3459 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）Catalyst デバイスを選択してから、ポリシーセレクタで [プラットフォーム（Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。
- （ポリシービュー）[Catalystプラットフォーム（Catalyst Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[IDSM Settings] ページ （3465 ページ）を参照してください。

ステップ 2 テーブル内の行をクリックして、削除する VLAN 定義を選択します。

ステップ 3 [Delete Row] をクリックします。

データ ポート VLAN 定義の作成または編集

データ ポート VLAN 定義を行う場合は、次の操作を実行する必要があります。

- データ ポートを配置するスロットとポートの組み合わせを定義します。
- データ ポートで使用する検知モードを選択します。
- データ ポートに転送する VLAN を定義します。

次の制約事項が適用されます。

- データ ポートごとに 1 つの定義しか保持できません。
- データ ポートがチャネル グループの一部としてすでに定義されている場合は、データ ポート定義を作成できません。

関連項目

- データ ポート VLAN 定義の削除 （3464 ページ）
- EtherChannel VLAN 定義の作成または編集 （3460 ページ）
- IDSM 設定 （3459 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイスビュー）Catalyst デバイスを選択してから、ポリシーセレクタで [プラットフォーム（Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。
- （デバイスビュー）**[Catalystプラットフォーム（Catalyst Platform）] > [IDSM設定（IDSM Settings）]** の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[IDSM Settings] ページ （3465 ページ）を参照してください。

ステップ 2 次のいずれかを実行します。

- IDSM データポート VLAN 定義を作成するには、[データポートVLAN（Data Port VLANs）] テーブルの下にある [行の追加（Add Row）] をクリックします。
- IDSM データポート VLAN 定義を編集するには、リストで定義を選択し、テーブルの下にある [行の編集（Edit Row）] をクリックします。

[IDSM Data Port VLAN] ダイアログボックスが表示されます。このダイアログボックスにあるフィールドの説明については、[Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス （3468 ページ）を参照してください。

ステップ 3 IDSM サービス モジュールを取り付けた番号付きシャーシ スロットに VLAN を関連付け、その VLAN に 1 つのモジュール データ ポートを関連付けるには、次のいずれかを実行します。

- [スロット/ポート（Slot-Ports）] テキストボックスにスロット/ポート番号を入力します。
- [選択（Select）] をクリックして、[IDSMスロット/ポートセレクタ（IDSM Slot-Port Selector）] ダイアログボックスを開きます。

（注） 1 つのモジュール データ ポートを VLAN に関連付けると、データ ポートを手動で設定する代わりに、グループ レベルでポートを設定できます。

ステップ 4 [Mode] リストから、データ ポート VLAN の動作モードを選択します。[Capture] を選択する場合は、チェックボックスをオンにして、指定したデータ ポートをキャプチャ先として設定します。

（注） このチェックボックスをオンにしなかった場合、キャプチャ ポートはシャットダウン モードで作成されます。

ステップ 5 指定したデータ ポートに VLAN を割り当てるには、次のいずれかを実行します。

- [VLAN IDs] テキスト ボックスで数値 ID を入力します。
- [選択（Select）] をクリックして、[VLANセレクタ（VLAN Selector）] ダイアログボックスを開きます。

複数の VLAN ID を入力または選択できます。

ステップ 6 [OK] をクリックして定義をクライアントにローカルに保存し、ダイアログボックスを閉じます。

データ ポート VLAN 定義の削除

IDSM のデータ ポート VLAN 定義を削除できます。

関連項目

- データ ポート VLAN 定義の作成または編集 （3463 ページ）
- EtherChannel VLAN 定義の削除 （3462 ページ）
- IDSM 設定 （3459 ページ）

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）Catalyst デバイスを選択してから、ポリシー セレクタで [プラットフォーム（Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。
- （ポリシー ビュー）[Catalystプラットフォーム（Catalyst Platform）] > [IDSM設定（IDSM Settings）] の順に選択します。

[IDSM Settings] ページが表示されます。このページにあるフィールドの説明については、[IDSM Settings] ページ （3465 ページ）を参照してください。

ステップ 2 テーブル内の行をクリックして、削除する VLAN 定義を選択します。

ステップ 3 [Delete Row] をクリックします。

[IDSM Settings] ページ

[IDSM Settings] ページを使用して、Intrusion Detection System Service Module（IDSM）のデータポートとチャネル グループの VLAN 設定を表示および設定します。

ナビゲーション パス

このページには次の手順でアクセスできます。

- （デバイスビュー）デバイスポリシーセレクタから [プラットフォーム（Platform）] > [IDSM設定（IDSM Settings）] を選択します。
- （ポリシービュー）ポリシータイプセレクタから [Catalystプラットフォーム（Catalyst Platform）] > [IDSM設定（IDSM Settings）] を選択します。

関連項目

- [Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス （3467 ページ）
- [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス （3468 ページ）
- テーブルのフィルタリング （64 ページ）
- ファイアウォール デバイスの管理 （2331 ページ）

フィールド リファレンス

表 965 : [IDSM Settings] ページ

要素	説明
[EtherChannel VLANs] テーブル	
チャネル グループ	イーサネット インターフェイスが割り当てられる EtherChannel グループを示します。

要素	説明
Module Slot-Data Port	2 つのポートを区別する番号（1 または 2）で IDSM サービス モジュールのデータ ポートを示します。 各 IDSM サービス モジュール（ブレード）に 2 つのデータ ポートがあります。データ ポートを個々に設定したり、EtherChannel グループに割り当てたりできます。チャネル グループ内のすべてのデータ ポートは、グループ レベルで設定されます。
[モード（Mode）]	動作モードがトランク（IPS）かキャプチャ（IDS）かを示します。
Capture Enabled	指定したチャネル グループがキャプチャ先として設定されているかどうかを示します。
Allowed VLANs	指定したチャネル グループで許可される VLAN を示します。
[Add Row] ボタン	[Create IDSM EtherChannel VLANs] ダイアログボックスを開きます。このダイアログボックスで、EtherChannel グループ内のデータ ポートに送信するトラフィックと使用する検知モードを定義できます。
[Edit Row] ボタン	[Edit IDSM EtherChannel VLANs] ダイアログボックスを開きます。このダイアログボックスで、EtherChannel VLAN 定義の属性を変更できます。
[Delete Row] ボタン	選択した VLAN を IDSM から削除します。
[Data Port VLANs] テーブル	
Module Slot-Data Port	2 つのポートを区別する番号（1 または 2）で IDSM サービス モジュールのデータ ポートを示します。
[モード（Mode）]	動作モードがトランク（IPS）かキャプチャ（IDS）かを示します。モードを変更するには、関連するテーブル行を選択して編集します。
Capture Enabled	指定したデータ ポートがキャプチャ先として設定されているかどうかを示します。
Allowed VLANs	指定したデータ ポートで許可される VLAN を示します。
[Add Row] ボタン	[Create IDSM Data Port VLANs] ダイアログボックスを開きます。このダイアログボックスで、特定のデータ ポートに送信するトラフィックと使用する検知モードを定義できます。
[Edit Row] ボタン	[Edit IDSM Data Port VLANs] ダイアログボックスを開きます。このダイアログボックスで、データ ポート VLAN 定義の属性を変更できます。
[Delete Row] ボタン	選択した VLAN を IDSM から削除します。

[Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス

[Create IDSM EtherChannel VLANs] ダイアログボックス（または [Edit IDSM EtherChannel VLANs] ダイアログボックス）を使用して、IDSM EtherChannel VLAN の属性を設定または再設定します。

ナビゲーション パス

[IDSM Settings] ページ （3465 ページ）に移動してから、[EtherChannel VLAN（EtherChannel VLANs）] テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス （3468 ページ）
- [IDSM Slot-Port Selector] ダイアログボックス （3469 ページ）
- [Service Module Slot Selector] ダイアログボックス （3448 ページ）

フィールド リファレンス

表 *966 : [Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs]* ダイアログボックス

要素	説明
Channel Group	イーサネット インターフェイスが割り当てられる EtherChannel グループ。
Slot-Ports（[Select] ボタン）	シャーシスロット番号（関連サービスモジュールの取り付け先）を *x* -*y* の形式でデータポートに関連付けます。ここで、*x* はスロット番号、*y* はポート番号です。たとえば、2-1 はスロット 2 のデータ ポート 1 を表します。 [IDSM Slot-Port Selector] ダイアログボックス （3469 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、EtherChannel グループに含める IDSM のスロットとポートの組み合わせを選択できます。
[モード（Mode）]	EtherChannel グループの動作モード： • [Capture (IDS)]：IDSM2 は、VACL キャプチャまたは SPAN を使用して、Catalyst スイッチがデータ ポートにコピーしたネットワーク トラフィックをパッシブにモニタします。 • [Trunk (IPS)]：IDSM2 は 802.1Q トランクとして動作し、同じデータ ポート内にある VLAN ペア間で VLAN ブリッジングを実行します。

要素	説明
Capture Enabled	動作モードが [Capture (IDS)] の場合にだけ適用されます。 このチェックボックスをオンにすると、指定したチャネル グループがキャプチャ先として設定されます。オフにすると、チャネル グループはキャプチャ先として機能しません。
VLAN IDs（[Select] ボタン）	指定したチャネル グループで許可される VLAN を示します。 [VLAN Selector] ダイアログボックス （3449 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、追加または除外する VLAN を選択できます。

[Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス

[Create IDSM Data Port VLANs] ダイアログボックス（または [Edit IDSM Data Port VLANs] ダイアログボックス）を使用して、IDSM データ ポートに送信するトラフィックとそのトラフィックに対して使用する検知モードを定義します。

ナビゲーション パス

[IDSM Settings] ページ （3465 ページ）に移動してから、データポート VLAN テーブルの下にある [追加（Add）] または [編集（Edit）] ボタンをクリックします。

関連項目

- [Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス （3467 ページ）
- [IDSM Slot-Port Selector] ダイアログボックス （3469 ページ）
- [Service Module Slot Selector] ダイアログボックス （3448 ページ）

フィールド リファレンス

表 967 : [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス

要素	説明
Slot-Port	シャーシスロット番号（関連サービスモジュールの取り付け先）を *x* -*y* の形式でデータポートに関連付けます。ここで、*x* はスロット番号、*y* はポート番号です。たとえば、2-1 はスロット 2 のデータ ポート 1 を表します。 [IDSM Slot-Port Selector] ダイアログボックス （3469 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、データポート VLAN 定義に含める IDSM のスロットとポートの組み合わせを選択できます。

要素	説明
[モード（Mode）]	データ ポートの動作モード： • [Capture (IDS)]：IDSM2 は、VACL キャプチャまたは SPAN を使用して、Catalyst スイッチがデータ ポートにコピーしたネットワーク トラフィックをパッシブにモニタします。 • [Trunk (IPS)]：IDSM2 は 802.1Q トランクとして動作し、同じデータ ポート内にある VLAN ペア間で VLAN ブリッジングを実行します。
Capture Enabled	動作モードが [Capture (IDS)] の場合にだけ適用されます。 このチェックボックスをオンにすると、指定したチャネル グループがキャプチャ先として設定されます。オフにすると、チャネル グループはキャプチャ先として機能しません。
VLAN IDs（[Select] ボタン）	指定したデータ ポートで許可される VLAN を示します。 [VLAN Selector] ダイアログボックス （3449 ページ）を開くには、[選択（Select）] をクリックします。このダイアログボックスで、追加または除外する VLAN を選択できます。

[IDSM Slot-Port Selector] ダイアログボックス

[IDSM Slot-Port Selector] ダイアログボックスを使用して、スロットポート オブジェクトを EtherChannel グループに関連付けます。

ナビゲーション パス

[Create IDSM EtherChannel VLANs]/[Edit IDSM EtherChannel VLANs] ダイアログボックス （3467 ページ）または [Create IDSM Data Port VLANs]/[Edit IDSM Data Port VLANs] ダイアログボックス （3468 ページ）に移動し、[スロットポート（Slot-Port）] フィールドの [選択（Select）] をクリックします。

関連項目

- [VLAN Selector] ダイアログボックス （3449 ページ）
- テーブルのフィルタリング （64 ページ）

フィールド リファレンス

表 *968 : [IDSM Slot-Port Selector]* ダイアログボックス

要素	説明
[Available IDSM Slot-Ports] リスト	使用可能なスロットポート定義が表示されます。

要素	説明
[Add >>] ボタン	EtherChannel VLAN のスロットポートを選択する場合にだけ適用されます。 [Available IDSM Slot-Ports] リストで選択した IDSM スロットポート オブジェクトを [Selected IDSM Slot-Ports] リストに追加します。
[Remove <<] ボタン	EtherChannel VLAN のスロットポートを選択する場合にだけ適用されます。 選択した IDSM スロットポート オブジェクトを [Selected IDSM Slot-Ports] リストから削除します。
[Selected IDSM Slot-Ports] リスト	データ ポートまたは EtherChannel グループに関連付けるために選択された IDSM スロットポート オブジェクトが表示されます。

第 VII 部

モニタリング、レポート、および診断

- イベントの表示 （3473 ページ）
- レポートの管理 （3561 ページ）
- ヘルスとパフォーマンスのモニタリング （3611 ページ）
- 外部モニタリング、トラブルシューティング、および診断ツールの使用方法（3673ページ）

第 69 章

イベントの表示

イベントビューアを使用すると、ASA（ASA-SM を含む）、FWSM および IPS デバイスからのイベントを選択してモニタリング、表示、および調査できます。イベントはビューに整理されます。重要なイベントを見つけるためにビューをフィルタリングまたは検索できます。必要に応じて、カスタマイズしたビューおよびフィルタを作成できます。または、アプリケーションに含まれる定義済みのビューを使用できます。

この章は次のトピックで構成されています。

- Event Viewer 機能の概要 （3473 ページ）
- Event Viewer の概要 （3481 ページ）
- イベント管理の準備 （3506 ページ）
- Event Manager サービスの管理 （3509 ページ）
- イベントビューアの使用 （3518 ページ）
- イベント分析の例 （3547 ページ）

Event Viewer 機能の概要

Event Viewer は、ASA および FWSM デバイス、ならびにセキュリティ コンテキストからの syslog（システム ログ）イベント、ならびに IPS デバイスおよび仮想センサーからの Secure Device Event Exchange（SDEE）イベントを対象にネットワークをモニタします。Event Viewer は、これらのイベントを収集し、収集したイベントを表示し、グループ化し、その詳細を調べるためのインターフェイスを備えています。

（注） バージョン 4.5 以降、Security Manager では、syslog を 1 つのローカルコレクタと 2 つのリモートコレクタに転送できます。詳細については、[Event Management] ページ （677 ページ）を参照してください。

ヒント　Event Viewer および関連アプリケーションである Report Manager および Health and Performance Monitor は、ネットワーク内にある特定のタイプのシスコデバイスの動作モニタリングおよびトラブルシューティングに役立ちます。これらのアプリケーションでは、さまざまなイベントの相関付け、コンプライアンスレポート、長期的フォレンジック、またはシスコ製とシスコ製以外の両方のデバイスの統合モニタリングの機能は提供されません。

IPS イベントを処理する際、Cisco Security Manager の Report Manager コンポーネントはイベントを個別に報告します。 Cisco Security Manager のイベント ビューア コンポーネントにアラートが表示されます。イベント ビューア コンポーネントで、IPS Summarizer はイベントを単一のアラートにグループ化するため、IPS センサーが送信するアラートの数が減少します。

ヒント　Cisco IPS Manager Express（IME）と Cisco Security Manager は、まったく同じ方法ではイベントを要約しません。

ここでは、Event Viewer で簡易化できる主要なアクティビティについて簡単に説明します。

- 履歴ビュー　（3474 ページ）
- リアルタイム ビュー　（3475 ページ）
- ビューとフィルタ　（3475 ページ）
- ポリシーのナビゲーション　（3476 ページ）
- Event Viewer のアクセス コントロールについて　（3477 ページ）
- Event Viewer のスコープおよび制限　（3478 ページ）
- 詳細に解析される Syslog　（3479 ページ）

履歴ビュー

履歴ビューは、選択した期間（たとえば、直前の 10 分間）に発生したイベントを表示するビューで、新規イベントが収集された場合でも表示内容は自動的には更新されません。より新しいイベントを表示するには、ビューをリフレッシュする必要があります。

Event Viewer で履歴ビューを使用する場合に考えられるさまざまな可能性の中から、次のアクティビティを見ていきます。

- **接続のトラブルシューティング**：ユーザーが特定のサーバーに到達できないというレポートが生成されたときには、そのユーザーの IP アドレスが送信元または宛先である場合に影響を与えるイベントをすべて表示するように履歴ビュー（たとえば、過去 10 分間）を設定できます。次に、表示された特定のイベントから、リソースに対するユーザーのアクセスを拒否するポリシーに進むことができます。

- **シグニチャの調整**：すべての IPS メッセージ、または特定のカテゴリに属するすべての IPS メッセージを表示するビューを設定すると、イベントが実際には誤検出であることを判別できます。次に、関連付けられたポリシーをクロス起動します。ホストを除外するようにシグニチャを調整するか、または問題のイベントでレポートされた重大度を低くします。

イベントアクションフィルタを作成して、アラートの処理方法を変更することも検討します。false positive の処理には、実際のシグニチャを編集するよりもイベントアクション フィルタを使用する方が良い場合がよくあります。詳細については、イベントアクション フィルタ ルールの管理に関するヒント （2218 ページ）を参照してください。

- **ポリシー展開の検証**：新規または変更したポリシーを展開したあとで、その特定のポリシーに対応するイベントを選択して、ポリシーが効果的に動作していることを確認する必要がある場合があります。たとえば、新規ポリシーによってトリガーされたファイアウォール拒否メッセージを特定できます。

リアルタイム ビュー

リアルタイム ビューには受信した状態のままのイベントが表示され、イベント テーブルがウォータフォール式に自動的に更新されます。「リアルタイム」という用語は正確な表現ではないことに注意してください。システム遅延をはじめとする要因により、真のリアルタイム システム応答は実現されません。

Event Viewer でリアルタイム ビューを使用する場合に考えられるさまざまな可能性の中から、次のアクティビティを見ていきます。

- **ほぼリアルタイムでの攻撃の**調査：特定の送信元 IP アドレスまたは送信元/宛先ペアの詳細を切り分けることで、監視対象デバイスに対する攻撃、または監視対象デバイスを通過している攻撃の詳細をイベントビューアで参照できます。
- **デバイスアクティビティの検証**：ネットワーク内のデバイスを調べて、デバイスの存在の有無、存在する場合にイベントを送信中であるかを判断できます。
- **脅威レベルの高い IPS イベントの表示**：特定の脅威レベルを超えるイベントをすべて表示するようにビューをフィルタ処理できます。IPS センサーを正しく調整すると、リアルタイム ビューで監視するイベントの流れが管理しやすくなります。

ビューとフィルタ

Event Viewer でイベントを表示するには、ビューを開きます。ビューは、フィルタおよび他のプロパティのセットです。これには、イベントのサブセットを定義できる色ルール、選択したカラムとその位置および幅、ならびにデフォルトの時間枠が含まれます。ビューによってイベント リストのスコープを制限できるため、検索内容をより簡単に見つけられます。

Event Viewer には多数の定義済みのビューがあります。定義済みのビューのフィルタ ルールは変更できませんが、ビューのコピーを作成して、コピーのフィルタ ルールを変更できます。作

成するビューはカスタム ビューと呼ばれます。詳細については、カスタム ビューの作成 （3523 ページ）を参照してください。

Event Viewer を最大限活用するには、フィルタの使用が鍵となります。受信中のすべてのイベントから、必要とする情報だけを記載したビューを抽出できます。イベントリストを絞り込む（すでにフィルタリングされたイベントリストのフィルタリング）には、さまざまなフィルタリング方法が使用できます。次のリストに、一般的なフィルタリング機能を示します。詳細については、イベントのフィルタリングおよびクエリー （3526 ページ）を参照してください。

- **時間フィルタ**：時間フィルタを使用すると、クライアントにロードするイベントを制限したり、イベントテーブルに表示されるイベントを制限したりできます。時間のフィルタリングでは、**直前の 1 時間**など定義済みの値を選択したり、日付と時刻で特定の時間範囲を指定したりできます。詳細については、イベントの時間範囲の選択 （3526 ページ）を参照してください。
- **カラムフィルタ**：カラムフィルタを使用すると、イベントの特定の値に基づいてイベントをフィルタリングできます。たとえば、特定の送信元または宛先、あるいはその両方に対してフィルタリングできます。カラムによっては、値の範囲またはポリシーオブジェクトに対してもフィルタリングできます。カラムフィルタは、ビューに対するビュー設定の一部です。詳細については、カラムベース フィルタの作成 （3528 ページ）を参照してください。
- **クイックフィルタ**：クイックフィルタを使用すると、イベントテーブルに一覧表示されたイベントに対してテキストベースのフィルタリングを実行できます。検索ではカラムを区別しません。いずれかのカラムに文字列が存在するイベントがすべて表示されます。フィルタのスコープを変更するには、[Quick Filter] ドロップダウン リスト（虫眼鏡として表示される）を使用します。詳細については、テキスト文字列に対するフィルタリング （3532 ページ）を参照してください。
- **フィルタでのドリルダウン**：フィルタにさらに別のフィルタを集約すると選択性が高まり、要件を満たす特定のイベントまたはイベントセットが表示されるまで「ドリルダウン」できます。別のフィルタを選択するたびに、[Event Monitoring] ウィンドウの最上部にある [View Settings] ペインが更新されて、選択したビューの現在の集約フィルタ定義が表示されます。

ポリシーのナビゲーション

特定のイベントから、そのイベントを制御する Security Manager 内のポリシーにナビゲートできます。特定のポリシーから、そのポリシーに関連付けられたイベントに移動することもできます。詳細については、「Event Viewer からの Security Manager ポリシーの検索 （3541 ページ）」および「Looking Up Events for a Cisco Security Manager Policy （3543 ページ）」を参照してください。

Event Viewer のアクセス コントロールについて

ユーザ名に割り当てられたユーザ権限によって、Event Viewer で実行可能な操作が制御されます。ローカル ユーザまたは他のタイプの ACS 以外のアクセス コントロールを使用している場合は、すべてのユーザが Event Viewer にアクセスできます。ただし、次のアクセス制限が課されます。

- デバイスをモニタ対象として選択または選択解除するためには、システム管理者、ネットワーク管理者、またはアプルーバ権限を持っている必要があります。モニタするデバイスの選択 （3514 ページ）を参照してください。
- Event Management の管理設定ページを変更するには、システム管理者権限を持っている必要があります。このページでは、Event Manager サービスの開始、停止、および設定 （3509 ページ）および [Event Management] ページ （677 ページ）で説明するとおりに、サービスをイネーブルまたはディセーブルにしたり、ストレージの場所の設定やその他の設定を行います。

ACS を使用して Security Manager へのアクセスを制御する場合は、次も制御できます。

- View Event Viewer 権限を使用して、Event Viewer アプリケーションへのアクセスを制御できます。この権限を使用すると、特定のユーザによる Event Viewer へのアクセスを防げます。または、Report Manager へのアクセスを許可せずに Event Viewer へのアクセスを許可するロールを作成できます。すべてのデフォルト ACS ロールで Event Viewer を使用できます。
- [Modify] > [Manage Event Monitoring] 権限を使用して、デバイスのモニタリングをイネーブルまたはディセーブルにできるユーザを制御できます。モニタするデバイスの選択 （3514 ページ）で説明するとおりに、デバイスをモニタ対象として選択するには、ユーザがこの権限を持っている必要があります。この権限を持つデフォルト ACS ロールは、システム管理者、ネットワーク管理者、アプルーバ、セキュリティ管理者、およびセキュリティ アプルーバです。
- ポリシー検索機能の使用を制御できます。ポリシー検索を実行するには、デバイスに対するデバイスの表示権限、およびファイアウォールまたは IPS ポリシーに対する表示権限もユーザが持っている必要があります。すべての権限を持っていないユーザーが一致ルールの検索を試みると、「Unable to Find Matching Rule」エラーが発生します。ポリシー検索の詳細については、Event Viewer からの Security Manager ポリシーの検索 （3541 ページ）を参照してください。
- ユーザは、少なくともデバイスに対する表示権限がある場合にのみ、そのデバイスのイベントを表示できます。
- Event Management の管理設定ページへのアクセスを制御できます。このページでは、Event Manager サービスの開始、停止、および設定 （3509 ページ）および [Event Management] ページ （677 ページ）で説明するとおりに、サービスをイネーブルまたはディセーブルにしたり、ストレージの場所の設定やその他の設定を行います。このページ（またはその他の管理設定ページ）にアクセスするには、ユーザは Admin 権限を持っている必要があります。

ヘルプ デスクを除く、すべてのデフォルト ACS ロールでページを表示できますが、設定を変更できるのはシステム管理者だけです。

- カラム フィルタ（[Device]、[Source]、[Destination]、[Source Service]、および [Destination Service] カラムなど）に対するネットワーク/ホストおよびサービス ポリシー オブジェクトの使用を制御できます。ネットワーク/ホスト、ネットワーク/ホスト-IPv6、およびサービス オブジェクトをフィルタで使用するには、これらに対する適切なオブジェクトの表示権限をユーザが持っている必要があります。カラム フィルタの作成の詳細については、カラムベース フィルタの作成 （3528 ページ）を参照してください。

Cisco Security Manager と Cisco Secure ACS との統合の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

Event Viewer のスコープおよび制限

次の表に、Event Viewer の機能面のスコープおよび制限について詳しく示します。

表 *969 : Event Viewer* のスコープおよび制限

項目	説明
デバイス サポート	次のタイプのデバイスから収集されたイベントを表示できます。Event Viewer は、次に示すソフトウェア リリースでテスト済みですが、より古いソフトウェア リリースで使用できる場合があります。 • **ASA デバイス（ASA-SM を含む）とセキュリティ コンテキスト**：すべての 8.x リリース。 • **FWSM デバイスとセキュリティ コンテキスト**：リリース 3.1.17、3.2.17、4.0.10、および 4.1.1 以降。 • **IPS デバイスと仮想センサー**：リリース 6.1 以降。 IPS サポートに IOS IPS は含まれません。
イベント データストアのサイズと場所	モニタ対象のデバイスから収集されたイベントを格納するために割り当てる場所とディスク スペースを制御できます。[Event Data Store Disk Size] に 90% と入力すると、最古のイベントから順に最新のイベントに置き換わります。 拡張ストレージまたはアーカイブの場所を接続したストレージ デバイス上に設定できます。Security Manager は、自動的に拡張ストレージにイベントをコピーします。過去のイベントを表示したときに、過去のイベントがローカル ディスクに存在しなくなっている場合には自動的に拡張ストレージから取得されます。 これらの設定の構成に関する詳細については、[Event Management] ページ（677 ページ）を参照してください。

項目	説明
イベントの制限	[Event Data Pagination Size] オプションを使用して、イベント テーブル内で一度に表示できるイベントの最大数を制御できます。このオプションの設定の詳細については、[Event Management] ページ （677 ページ）を参照してください。
ポリシー オブジェクト	カラム フィルタを作成する場合には、ネットワーク/ホストやサービス オブジェクトなど一部のタイプのポリシー オブジェクトを使用できます。 [表示（View）] > [ネットワークホストオブジェクトの表示（Show Network Host Objects）] を選択して、送信元および宛先カラムに IP アドレスではなくホストオブジェクト名を表示することもできます。このオプションは、デフォルトで選択されます。 IP アドレスからホスト名へのマッピングは、イベントの送信元および宛先だけでサポートされます。また、マッピングはホスト オブジェクトだけに適用されます。イベントの送信元または宛先がネットワーク オブジェクト、グループ オブジェクト、またはアドレス範囲オブジェクトに一致した場合は、Event Viewer ではオブジェクト名が表示されません。 **ヒント** そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
ビュー	単一の Event Viewer クライアントでは、最大 4 つの履歴ビューと 1 つのリアルタイム ビューを同時に開けます。
クライアント	1 台の Security Manager サーバーに対して、最大 5 つの Security Manager クライアントが同時にイベントビューアを開くことができ、Security Manager クライアントごとにイベントビューアのコピーを 1 つ開くことができます。

詳細に解析される Syslog

標準の syslog の構造と内容、およびそれぞれを構成する要素の詳細については、使用するデバイスおよびソフトウェア バージョンのシステム ログのマニュアルを参照してください。

マニュアルは、Cisco.com の次の場所にあります。

- ASA デバイス:
  http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html [英語]
- FWSM デバイス:
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_system_message_guides_list.html [英語]

ここに挙げられていない syslog は、未処理 syslog として表示されます。syslog の全内容が表示されるのは、詳細に解析される syslog だけです。

Security Manager で詳細に解析される syslog の詳細については、次の表を参照してください。

表 *970 :* 詳細に解析される *Syslog*

syslog カテゴリ	syslog ID	syslog の合計数
フロー、セッション syslog	110002 ～ 110003、209003 ～ 209005、302003 ～ 302004、302009 ～ 302010、302012 ～ 302018、302020 ～ 302021、302035 ～ 302036、302303 ～ 302306、302033 ～ 302034、303002 ～ 302005、313001、313004、313005、313008、324000 ～ 324006、337001 ～ 337009、431001 ～ 431002、407001 ～ 407002、416001、418001 ～ 418002、419001 ～ 419003、424001 ～ 424002、450001、448001、609001 ～ 609002 （注） 302303 ～ 302306 の状態バイパス syslog は、イベントマネージャについてのみ詳細に解析されています。ただし、TCP、UDP、およびSCTP状態バイパス syslog のイベントマネージャのイベント説明には、「State-bypass」キーワードが表示されません。 （注） レポート、イベントからポリシー、およびポリシーからイベントは、状態バイパス syslog ではサポートされていません。	66
ボットネット	338001 ～ 338004、338101 ～ 338104、338201 ～ 338202、338301	11
ACL	106100、106023、106002、106006、106018	5
拒否されたファイアウォール	106001、106007、106008、106010 ～ 106017、106020 ～ 106022、106025 ～ 106027	17
アイデンティティファイアウォール	746003、746005、746010、746016	4
AAA	109001 ～ 109010、109012、109016 ～ 109020、109023 ～ 109029、109031 ～ 109035、113001 ～ 113025	53
検査	108002 ～ 108007、303004 ～ 303005、400000 ～ 400050、406001 ～ 406002、415001 ～ 415020、500001 ～ 500005、508001 ～ 508002、608001 ～ 608005、607001 ～ 607003、703001 ～ 703002、726001	99
NAT	201002 ～ 201006、201009 ～ 201013、202005、202011、305005 ～ 305012	20
IPSec VPN	402114 ～ 402122、602103 ～ 602104、602303 ～ 602304、702305、702307	15

syslog カテゴリ	syslog ID	syslog の合計数
フェールオーバー（HA）	101001 ～ 101005、102001、103001 ～ 103007、104001 ～ 104004、311001 ～ 311004、709001 ～ 709007、210001 ～ 210022（210008、210010 を除く）	48
SSL VPN	725001 ～ 725009、725012 ～ 725013、716001 ～ 716020、716023 ～ 716039、716041 ～ 716060、722001 ～ 722023、722026 ～ 722044、722046 ～ 722051、723001 ～ 723002、723009 ～ 723012、723014、724001 ～ 724004	128
Etherchannel	426001 ～ 426003	3
クラスタ	302022 ～ 302027	6

Event Viewer の概要

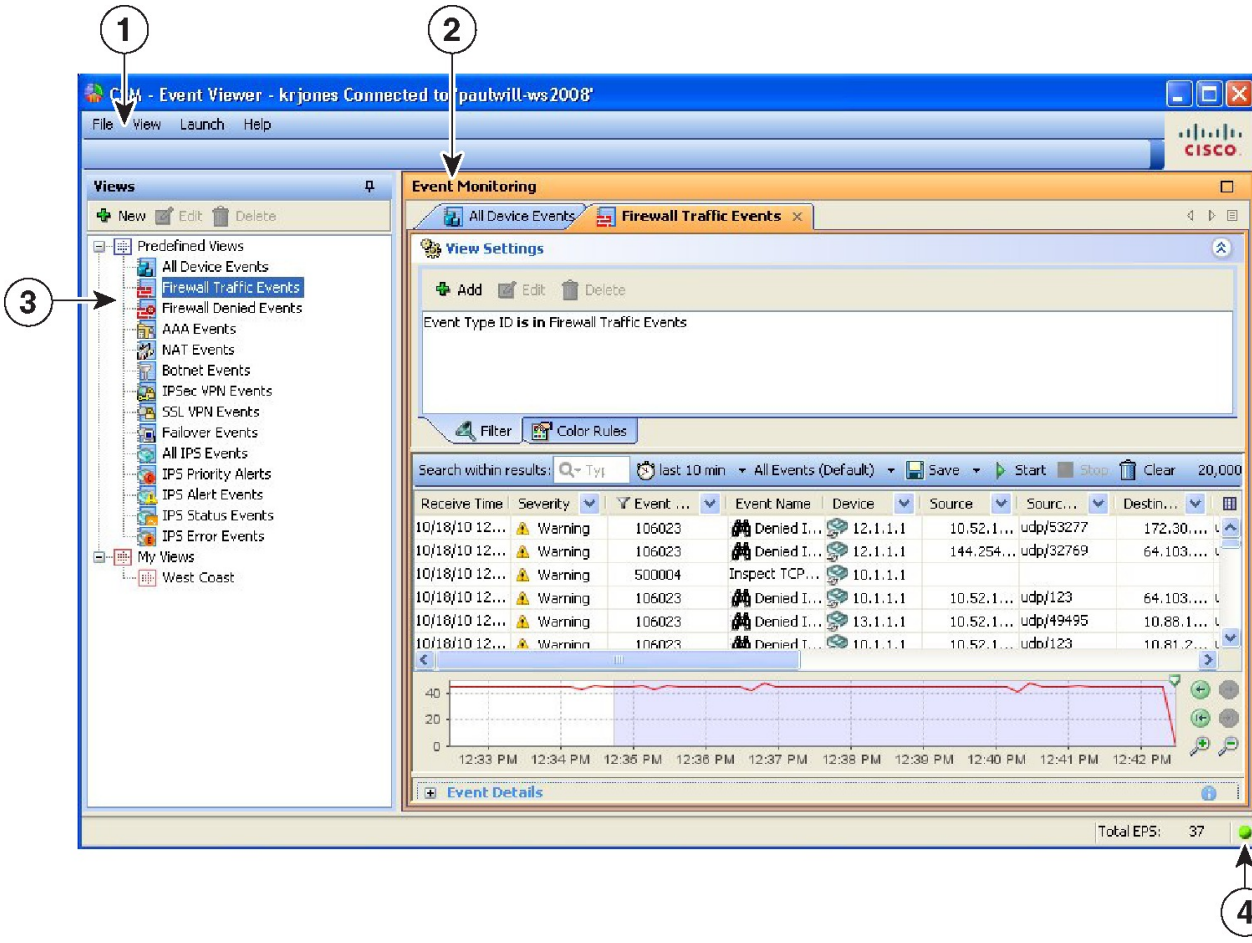
Event Viewer を使用すると、モニタ対象のファイアウォールおよび IPS デバイスから収集したイベントおよびアラートを表示できます。モニタ対象のデバイスの選択の詳細については、モニタするデバイスの選択 （3514 ページ）を参照してください。

Event Viewer を起動するには、次のいずれかを実行します。

- Windows Start メニューから [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Security Managerクライアント（Cisco Security Manager Client）] > [イベントビューア（Event Viewer）] を選択するか（正確なコマンドパスは異なる場合があります）、デスクトップの [イベントビューア（Event Viewer）] アイコンをダブルクリックします。ログインを求められます。Cisco Security Manager クライアント アプリケーションの開始方法の詳細については、Security Manager クライアントへのログインおよび終了 （17 ページ）を参照してください。
- Configuration Manager または Report Manager アプリケーションから [起動（Launch）] > [イベントビューア（Event Viewer）] を選択するか、Configuration Manager ツールバーの [イベントビューア（Event Viewer）] ボタンをクリックします。Event Viewer が他のアプリケーションへのログインに使用したのと同じユーザ アカウントを使用して開かれます。

次の図と後続のリストに、Event Viewer の基本的要素について示します。

図 *58 : Event Viewer* のメイン ウィンドウ



次のリストに、メインの Event Viewer ウィンドウの詳細を示します。

- **（1）メニューバー**：イベントビューアでアクションを実行するための一般的なコマンドです。次のメニューが含まれます。
  - [File]：ビューでの操作に使用します。コマンドの詳細については、『Event Viewer の [File] メニュー （3484 ページ）』を参照してください。
  - [View]：ビュー内での操作および一般的システム管理に使用します。コマンドの詳細については、『Event Viewer の [File] メニュー （3484 ページ）』を参照してください。
  - [Launch]：Configuration Manager または Report Manager アプリケーションの開始に使用します。
  - [Help]：オンライン ヘルプの開始、または著作権とライセンス情報の表示に使用します。

- **（2）イベントモニタリングウィンドウ**：開いているビューが右ペインに表示されます。開いている各ビューは、別々のタブに示されます（最大 4 つの履歴ビューと 1 つのリアルタイム ビューが開けます）。このスペース内でビューを水平または垂直に配置する、また

は別のウィンドウにビューをフローティングもできることに注意してください。ビューの配置方法またはフローティング方法の詳細については、ビューのフローティングと配置（3519 ページ）を参照してください。

[Event Monitoring] ウィンドウの数々の部分の詳細については、[Event Monitoring] ウィンドウ（3489 ページ）を参照してください。

- **（3）ビューリスト**：左ペインはビューのリストです。ビューのリストでは、定義済みのビューとカスタム ビューが別々にフォルダに整理されます。カスタム ビューは [My Views] フォルダに一覧表示されます。最も簡単にビューを開く方法は、ビューをダブルクリックする方法です。これにより、現在開いているビューが置き換えられます。現在開いているビューと置き換えずにビューを開くには、ビューを右クリックし、[新しいタブで開く（Open in New Tab）] を選択します。ビューを開く方法の詳細については、ビューを開く（3519 ページ）を参照してください。

ビューのリストのペインで実行できるその他の操作の詳細については、ビューリスト （3487 ページ）を参照してください。

- **（4）ステータス情報**：ステータスバーの右下部分には、現在の1 秒あたりのイベント（EPS）レートおよびモニタリングシステムの現在のヘルスを示すアイコンが表示されます。アラート ステータス アイコンをクリックして、過去 5 分の統計情報および現在のシステム アラートを表示するバブルを開きます。このビューから [Details] リンクをクリックして詳細情報を表示できます。バブルを閉じるには、アラート ステータス アイコンをもう一度クリックします。詳細については、Event Manager サービスの管理 （3509 ページ）を参照してください。

（注） ステータスバーに表示される 1 秒あたりのイベント（EPS）情報は、2 秒ごとに受信されるイベントの数に基づいて計算されます。一方、タイムスライダーグラフに表示される EPS 情報は、選択した時間範囲で使用可能なすべてのイベントの集約を実行することによって計算されます。したがって、ステータスバーとタイムスライダーグラフに表示される数値が異なる場合があります。

次の例を参照してください。

ステータスバーの EPS 情報の表示例

時間 T1 で、イベント ビューア アプリケーションが 192 個のイベントを受信したとします。ステータスバーに表示される 1 秒あたりのイベント数（EPS）は、192 / 2 = 96 です。これは、Security Manager が 2 秒ごとにイベントを収集し、ステータスバーに 1 秒あたりのイベントを表示するためです。T1 + 2 秒で、イベント ビューア アプリケーションが 384 個のイベントを受信したとします。ステータスバーに表示される EPS は、（384 - 192）/2 = 96 になります。これは、現在の値と以前の値の差を 2 で割ったものです。

タイムスライダーグラフでの EPS 情報の表示例

Security Manager は、10 秒間隔で 1 秒あたりのイベントを保持します。たとえば、イベントビューア アプリケーションが 10 秒間隔で 352 個のイベントを受信した場合、EPS は 352 / 10 = 35 になります。この値は、Security Manager によって保持されます。次の 10 秒の間隔で、イベントビューアが 1056 のイベントを受信すると、EPS は（1056 – 352）/10 = 70 になり、これは Security Manager によって保持されます。

タイムスライダーグラフに値を表示する

タイムスライダーグラフには、開始時刻と終了時刻がある期間の情報が表示されます。指定された時間間隔で収集された 1 秒あたりのすべてのイベントが集計され、グラフにプロットされます。この例では、35 と 70 が 10 秒ごとに保存される値です。したがって、タイムスライダーグラフには EPS が 35 および 70 として表示されますが、これらはステータスバーに表示される値とは異なります。

Event Viewer の [File] メニュー

次の表に、Event Viewer の [File] メニューのコマンドを示します。

表 *971 : Event Viewer* の *[File]* メニュー

コマンド	説明
New View	新規カスタム ビューを作成します。名前および説明の入力を求められます。カスタム ビューの作成 （3523 ページ）を参照してください。 または、ビューリストの [新規（+） （New (+)）] ボタンをクリックします。
Open View	新規タブにビューを開きます。開くビューを選択するように要求されます。最大で 4 つの履歴ビューと 1 つのリアルタイム ビューを開くことができます。ビューを開く （3519 ページ）を参照してください。 **ヒント** ビューのリスト内でダブルクリックして、ビューを開いて表示されているビューと置き換えます。
Save	フィルタ（カスタム ビューの場合のみ）、ならびに選択したカラム、カラム幅、およびソート順序などのテーブル プリファレンス、時間範囲や色ルールなど、アクティブなビューに加えた変更を保存します。ビューの保存 （3525 ページ）を参照してください。 定義済みのビューのフィルタ変更を保存する場合は、[Save As] を使用して新規カスタム ビューを作成する必要があります。
Save As	表示されているビューに加えた変更をカスタム ビューとして保存します。ビューの保存 （3525 ページ）を参照してください。
Close View	表示されているビューを閉じます。

コマンド	説明
Close All Views	開かれているすべてのビューを閉じます。
終了（Exit）	Event Viewer を閉じます。Event Viewer を終了すると、開いているフローティング Event Viewer ウィンドウが閉じられます。

Event Viewer の [View] メニュー

次の表に、Event Viewer の [View] メニューのコマンドを示します。

表 *972 : Event Viewer の [View] メニュー*

コマンド	説明
[モード（Mode）]	イベントテーブルに表示するイベントを選択する時間間隔を指定します。サブメニューから次のオプションのいずれかを選択します。 • **last 10 minutes** • [過去 1 時間（last 1 hour）] • **last 12 hours** • **last 1 day** • **last 1 week** • **is today** • **is yesterday** • **[次の日（is on . . .**（カレンダーが開き、カレンダー上で単一の日付をクリックして指定できます） • [次の期間（is between）]（カレンダーが 2 つ開き、カレンダー上で開始と終了の日付と時刻を指定できます） • [リアルタイム（Real Time）]（イベントを受信した状態のまま表示するモードを設定します） または、ツールバーの [時間セレクタ（Time Selector）] コントロールをクリックして、同じオプションから選択します。イベント テーブル ツールバー （3491 ページ）を参照してください。
Customize Column	イベント テーブルに表示するカラムを変更します。[Choose Columns to Display] ダイアログボックスが開き、表示するカラムを選択できます。使用可能なカラムの詳細については、イベントテーブルのカラム （3494 ページ）を参照してください。

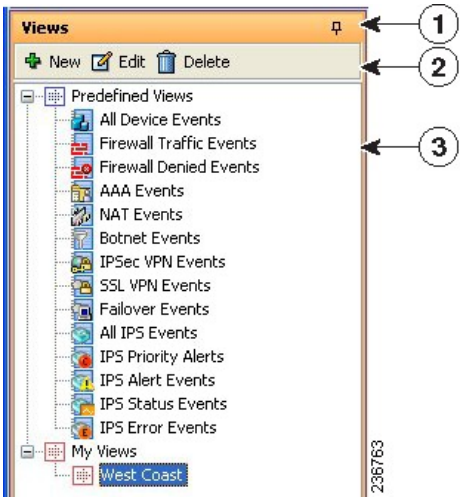
コマンド	説明
開始（Start）	イベントを取得して現在のビューのイベントテーブルを更新する作業を開始します。イベントテーブルには、[開始（Start）] をクリックしたときから時間モードの制限またはイベントテーブルの改ページ制限になるまでに受信したイベントが表示されます。 または、イベントテーブルツールバーの [開始（Start）] ボタンをクリックします。
停止（Stop）	イベント取得を停止します。イベントテーブルには、[停止（Stop）] をクリックするまでに受信したイベントが表示されます。 または、イベントテーブルツールバーの [停止（Stop）] ボタンをクリックします。
Show View Settings	[View Settings] ペインを開きます。ここには、現在のビューのフィルタおよび色設定が表示されます。このような設定は、[View Settings] ペインを使用して変更できます。 または、[View Settings] ペイン タイトル バー内のアイコン、テキスト、またはタイトルバーの右側の二重矢印などの任意の場所をクリックします。見出しをクリックすると、ペインが開閉します。
Show Event Details	[イベントの詳細（Event Details）]ペインを開き、選択されたイベントの詳細を表示します。 または、下記の手順も実行できます。 • [イベントの詳細（Event Details）]ペインのタイトルバーの左側にある展開アイコン（+）をクリックします。 • イベント テーブルのイベントをダブルクリックして、ポップアップ ウィンドウにイベントの詳細データを表示します。 ヒント [Event Details] ダイアログボックスから、イベント詳細を印刷したり、詳細の 1 行以上をクリップボードにコピーしたりできます。また、[Next] および [Previous] ボタンを使用して、イベントリスト全体をスクロールできます。
Manage Monitored Devices	いずれのデバイスまたはデバイス グループのイベントを Event Viewer に表示するかを選択できます。詳細については、モニタするデバイスの選択（3514 ページ）を参照してください。 （注） デフォルトでは、Security Manager インベントリに追加されたすべての ASA、FWSM、または IPS デバイスが監視されます。
Show Event Store Disk Usage	使用されているディスク容量と保存されている最も古いイベントの経過時間を示すウィンドウが開きます。イベント データ ストア用のディスク スペースの使用率のモニタリング （3516 ページ）を参照してください。

コマンド	説明
Show Network Host Objects	オンにすると、送信元または宛先IPアドレスの代わりにホストオブジェクト名が表示されます（使用可能な場合）。このオプションは、デフォルトで選択されます。 ヒント　そのオブジェクトに関連付けられたIPアドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
Reset Layout	非表示にしていたか、または手動で拡大縮小していたビューのリストペインの幅を元の設定に戻します。

ビューリスト

Event Viewer メイン ウィンドウの左ペインには、次の図に示すように使用可能なビューのリストが表示されます。ビューは、フィルタおよび他のプロパティのセットです。これには、イベントのサブセットを定義できる色ルール、選択したカラムとその位置および幅、ならびにデフォルトの時間枠が含まれます。

図 *59* : イベントビューアのビューリスト



ビューのリストには、次のコントロールが含まれます。

- **（1）プッシュピンボタン**：ビューリストペインを開くか閉じるかを制御するには、プッシュピンアイコンをクリックします。ピンが垂直の場合、[Event Monitoring] ウィンドウ（右ペイン）を最大化しないかぎり、ビューのリストは開いたままになります。ピンが水平の場合、ビューのリストは左端に縮小されます。リストを開くには、左端のビューの見出しをクリックする必要があります。
- **（2）ツールバー**：ツールバーには次のボタンが含まれています。

- [新規（New）] ボタン：新規カスタムビューを作成するには、[新規（New）] ボタンをクリックします。ビューの名前および説明の入力を求められます。詳細については、カスタム ビューの作成 （3523 ページ）を参照してください。
- [編集（Edit）] ボタン：選択したカスタムビューの名前または説明を変更するには、[編集（Edit）] ボタンをクリックします。カスタム ビューのみを編集できます。詳細については、カスタム ビューの名前または説明の編集 （3524 ページ）を参照してください。
- [削除（Delete）] ボタン：選択したカスタムビューを削除するには、[削除（Delete）] ボタンをクリックします。カスタム ビューだけが削除できます。詳細については、カスタム ビューの削除 （3525 ページ）を参照してください。

- **（3）ビューのリスト**：リストでは、定義済みのビューとカスタムビューが別々のフォルダに整理されます。カスタムビューは [マイビュー（My Views）] フォルダに一覧表示されます。最も簡単にビューを開く方法は、ビューをダブルクリックする方法です。これにより、現在開いているビューが置き換えられます。現在開いているビューと置き換えずにビューを開くには、ビューを右クリックし、[新しいタブで開く（Open in New Tab）] を選択します。ビューを開く方法の詳細については、ビューを開く （3519ページ）を参照してください。
- **右クリック ショートカット メニュー**：ビューで右クリックすると、実行可能な追加のコマンドのリストが表示されます。
  - [Open]：ビューを開いて現在アクティブなビューと置き換えます。現在アクティブなビューに保存されていない変更が含まれる場合は、変更の保存を求められます。ビューがすでに開いている場合は、最前面に移動されます。ビューを開く （3519ページ）を参照してください。
  - [Open in New Tab]：新規タブにビューを開きます。このため、既存の開いているビューは閉じません。ビューを開く （3519 ページ）を参照してください。
  - [名前を付けて保存（Save As）]：ビューを新しいカスタムビューとして保存します。ビューの保存 （3525 ページ）を参照してください。
  - [Edit]：カスタム ビューの名前と説明を編集します。カスタム ビューの名前または説明の編集 （3524 ページ）を参照してください。
  - [Delete]：カスタム ビューを削除します。カスタム ビューの削除 （3525ページ）を参照してください。
  - [View Description]：ビューの説明を表示します。

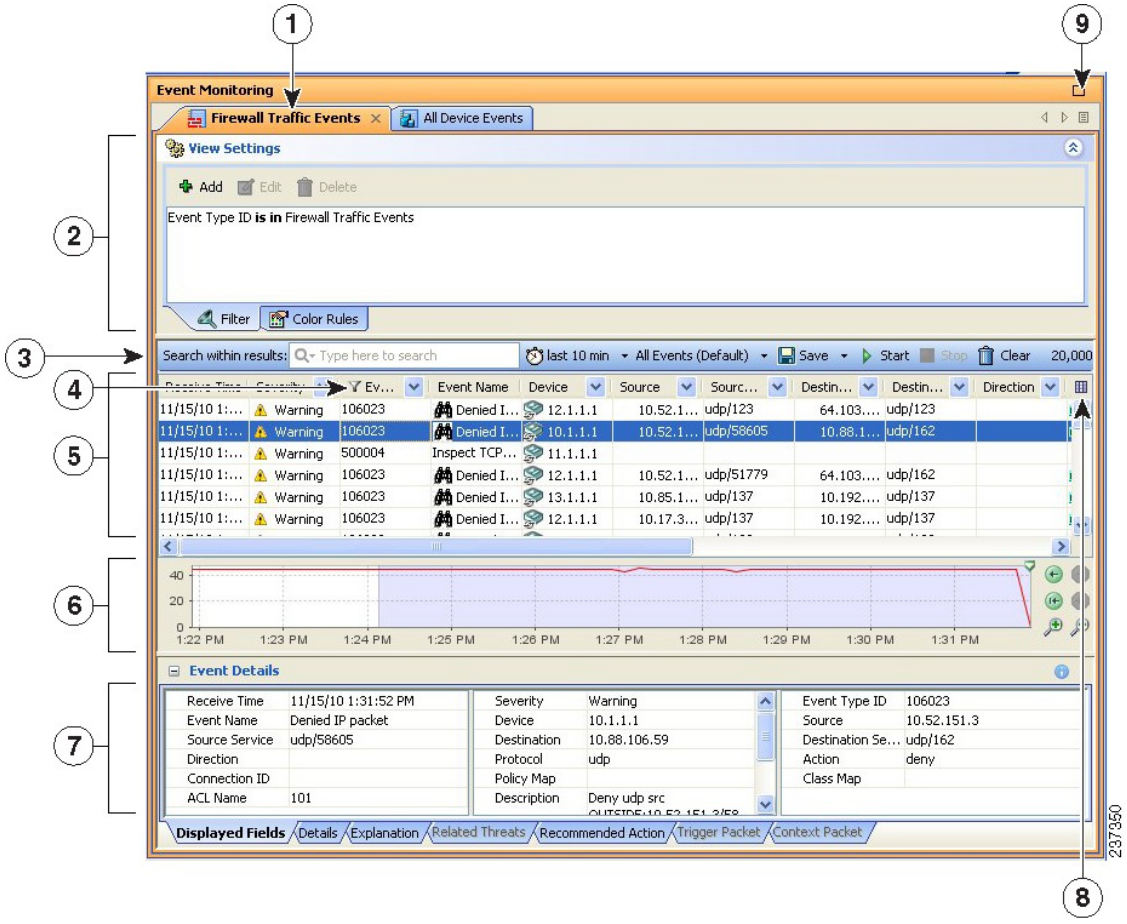
関連項目

- ビューとフィルタ （3475 ページ）
- Event Viewer の概要 （3481 ページ）
- ビューのフローティングと配置 （3519 ページ）

[Event Monitoring] ウィンドウ

[イベント監視（Event Monitoring）] ウィンドウには、開いているイベントビューが表示されます。このウィンドウでビューの設定およびフィルタ イベントの分析ができます。

図 *60 : [Event Monitoring]* ウィンドウ



1	ビューのタブ。	6	時間スライダ。
2	[View Settings] ペイン。	7	[Event Details] ペイン。
3	イベント テーブル ツールバー。	8	[Column Selector] ボタン。
4	[Filtered Column] アイコン。	9	[Open View] スクロール ボタンとリスト。
5	イベント テーブル。		

[Event Monitoring] ウィンドウには、次の主要な要素が含まれています。

- **View tabs (1, 9)**：ビューを開くと、ウィンドウ内のタブとして示されます。ビューを変更するには、タブをクリックする、左右矢印ボタンをクリックしてタブ全体をスクロールする、または [Open View List] ボタンをクリックして目的のビューを選択する、のいずれか

を実行します。タブ名を右クリックし、適切なコマンドを選択して、ビューを並べて表示するまたは別のウィンドウにフローティングするように配置できます。詳細については、ビューのフローティングと配置 （3519 ページ）を参照してください。

（注） 最大で 4 つの履歴ビューと 1 つのリアルタイム ビューを開くことができます。

- **View Settings pane (2)**：[ビューの設定（View Settings）] ペインを使用して、ビューで使用するカラムフィルタおよび色ルールを定義します。見出しの任意の場所をクリックするか、または [ビュー（View）] > [ビューの設定を表示（Show View Settings）] コマンドで切り替えて、ペインを開いたり閉じたりできます。

[View Settings] ペインには、[Filter] および [Color Rules] の 2 つのタブがあります。これらのタブは、ペインの下部に沿って表示されます。各タブ上で、タブの本体には現在のフィルタまたはルールが表示されます。ルールを変更するには、ルールを選択し、必要に応じてペインの上部に沿って表示される [Edit] または [Delete] ボタンをクリックします。新規ルールを作成するには、[Add] ボタンをクリックします。

カラムベース フィルタの作成 （3528 ページ）で説明するとおりに、イベント テーブルのカラム フィルタリング コントロールを使用して、フィルタを追加することもできます。色ルールの詳細については、ビューの色ルールの設定 （3522 ページ）を参照してください。

- **Event Table Toolbar (3)**：イベントテーブルの上部にあるツールバーには、テーブルに一覧表示されたイベントに明確に関連するショートカットボタンやその他のコントロールが含まれます。ツールバー コントロールの詳細については、イベント テーブル ツールバー （3491 ページ）を参照してください。

- [Event Table (4, 5, 8)]：イベントテーブルには、フィルタ基準に一致するイベントが各行に 1 つ表示されます。これらのイベントは、プライマリまたは拡張データ ストアから取得される場合があります。明示的に拡張データ ストアからデータを要求する必要はありません。デバイスからのイベントを表示するには、そのデバイスに対するデバイスの表示権限を持っている必要があります。

イベント テーブルの表示のカスタマイズ （3520 ページ）で説明するとおりに、イベント テーブルを構成しているカラムに対しては、非表示、サイズ変更、順序の並べ替え、およびソートが可能です。カラムの説明、および表示するカラムを選択する [Column Selector] ボタンの使用方法の詳細については、イベント テーブルのカラム （3494 ページ）を参照してください。

カラムにフィルタが適用されている場合は、カラムの見出しにアイコンが表示されます。

- **Time Slider (6)**：履歴ビューの場合、時間スライダには、テーブル内に表示された時間の現在のスライス、およびイベントレート（/秒）が線形グラフとして表示されます。時間スライダの使用方法の詳細については、時間スライダ （3504 ページ）を参照してください。

- **Event Details Pane (7)**：[イベント詳細（Event Details）] ペインには、現在選択されているイベントの詳細情報が表示されます。見出しの任意の場所をクリックするか、または [ビュー（View）] > [イベントの詳細を表示（Show Event Details）] コマンドで切り替えて、

ペインを開いたり閉じたりできます。詳細については、[Event Details] ペイン （3505 ページ）を参照してください。

イベント テーブル ツールバー

次の図と表に、Event Viewer のイベント テーブルのすぐ上にあるツールバーの要素を示します。

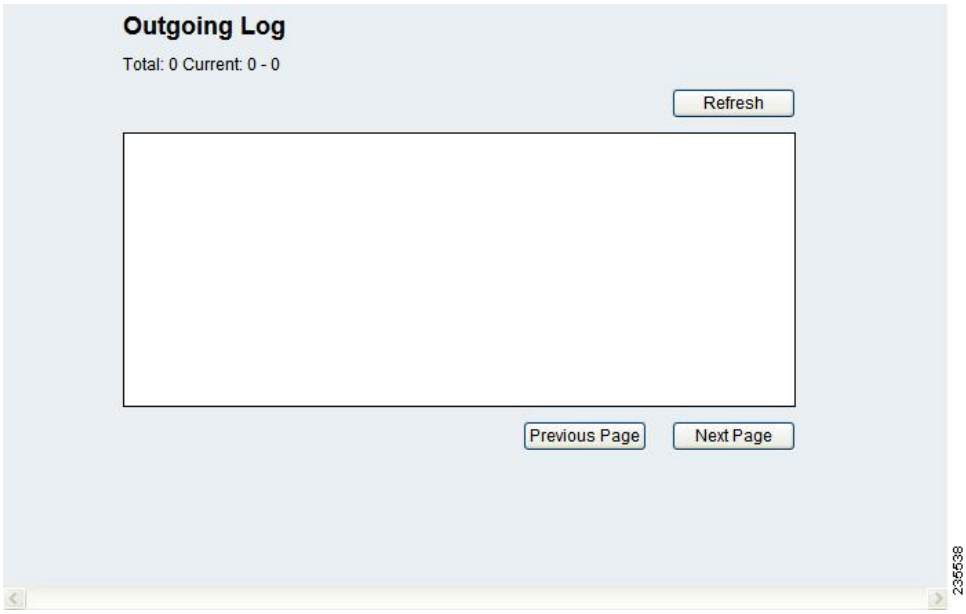


表 *973* : イベント テーブル ツールバーの要素

コールアウト	名前	説明
1	[Search Within Results] フィールド（クイック フィルタ）	このツールは、クイックフィルタとも呼ばれます。この要素は、単語またはフレーズを検索し、検索スコープを特定のカラムに限定する場合に使用します。また、使用する検索語句で大文字と小文字を区別するかどうか、ワイルドカードを使用できるかどうか、および一致は部分一致か、大文字と小文字を区別するか、完全一致か、文字列内の任意の位置に含まれていればよいかを選択できます。この検索は、選択したビューおよびロードされたデータ内でだけ動作します。詳細については、テキスト文字列に対するフィルタリング （3532 ページ）を参照してください。

コールアウト	名前	説明
2	Time Selector（モード） （[表示（View）] > [モード（Mode）]に相当）	時間セレクタは、次の手順を実行する場合に使用します。 • イベント テーブル ペインに表示するイベントを受信した時間に応じてフィルタリングします。イベントの時間範囲の選択 （3526 ページ）を参照してください。 • リアルタイム ビューまたは履歴ビューから選択します。リアルタイム ビューと履歴ビュー間の切り替え （3524 ページ）を参照してください。 • クライアントにロードする時間間隔を指定します。現在時刻から過去にさかのぼってイベントを表示するモードの 1 つを使用している場合は、ポインタをフィールドに重ねると、表示されたイベントの開始と終了時刻が表示されます。特定の時間間隔を使用している場合は、ツールバーに時間間隔が表示されます。
3	Events by IP Address Type Selector	イベントに含まれる IP アドレス タイプに基づいてリストをフィルタリングするために、[Events by IP Address Type Selector] を使用します。次のオプションがあります。 • [全てのイベント（All Events）]（デフォルト）：アドレスタイプに関係なくすべてのイベントを表示します。これがデフォルトのオプションです。 • [IPv4イベントのみ（IPv4 Events Only）]：イベントのすべてのアドレスが IPv4 形式の場合にのみイベントを表示します。 • [IPv6イベントのみ（IPv6 Events Only）]：イベントの少なくとも1つのアドレスが IPv6 形式の場合にのみイベントを表示します。 **ヒント** 選択は保存できません。次回ビューを開いたときにデフォルト以外が必要な場合は、再度オプションを選択する必要があります。

コールアウト	名前	説明
4	保存 （[ファイル（File）] > [保存（Save）] または [ファイル（File）] > [別名で保存（Save As）] に相当）	フィルタ（カスタムビューの場合のみ）、ならびに選択したカラム、カラム幅、およびソート順序などのテーブルプリファレンス、時間範囲や色ルールなど、現在のビューに加えた変更を保存するには、[保存（Save）] をクリックします。 または、下矢印をクリックし、[別名で保存（Save As）] を選択して変更を新規カスタムビューとして保存します。定義済みのビューのフィルタ変更を保存する場合は、[Save As] を使用して新規カスタム ビューを作成する必要があります。詳細については、カスタム ビューの作成 （3523 ページ）を参照してください。
5	開始（Start） （[表示（View）] > [開始（Start）] に相当）	イベントテーブルにイベントリストをリロードまたは再起動するには、[開始（Start）] をクリックします。[Start] をクリックすると、テーブルを最初にロードしてから発生したすべてのイベントを取得します。
6	停止（Stop） （[表示（View）] > [停止（Stop）] に相当）	イベントテーブルのイベントリストを停止するには、[停止（Stop）] をクリックします。現在リアルタイム ビューである場合、時間セレクタは停止した時間だけでなく、ロードされている時間間隔も示します。また、[Stop] をクリックすると、クエリーが停止し、現在 Event Viewer にロードされているイベント セットが表示されます。
7	クリア（Clear）	イベントテーブルを空にするには、[クリア（Clear）] をクリックします。
8	[Event Enumerator] とメッセージ	ツールバーの右側に表示されている数値は、Event Viewer クライアントにロードされているイベント数です。この数はイベントがロードされるたびに増えていき、フィルタ条件と一致するイベントがすべて表示されるか、改ページ制限に達するか、どちらか少ない方で終了します。改ページ制限を変更した場合は（[Event Management] ページ （677 ページ）を参照）、Event Viewer を終了して再び開くことによって新規制限を有効にする必要があります。 クエリが拡張イベントストレージ領域からのイベントの取得を要求する場合は、「Data being fetched from extended store」などのメッセージが表示されます。拡張ストレージ領域からのイベントのフェッチは、通常、プライマリストレージ領域からイベントをフェッチするよりも時間がかかります。

イベント テーブルのカラム

次の表に、Event Viewer のビューに表示できるすべてのカラムをアルファベット順に一覧表示して説明します。イベント タイプによってイベント データが存在する場合と存在しない場合があるように、デバイスに適用できるカラムはデバイスによってさまざまです。

ビューを保存した場合は、選択したカラムとその順序が保持されて、次回ビューを開いたときに表示されます。開いている（またアクティブな）ビューに表示するカラムを選択するには、次のいずれかを実行します。

- （推奨の方法）。イベントテーブルのヘッダー行の右端の [列セレクタ（Column Chooser）] アイコンをクリックします（ [Event Monitoring] ウィンドウ （3489 ページ）を参照）。[Choose Columns to Display] ダイアログボックスが開き、カラムがアルファベット順に一覧表示されます。列の選択または選択解除は、個別に、または [すべて選択（Select All）]/[すべて選択解除（Unselect All）] チェックボックスを使用して実行できます。また、[Revert] をクリックして、ビューのデフォルトのカラム選択に戻せます。
- [ビュー（View）] > [列のカスタマイズ（Customize Columns）] を選択します。
- 任意のカラムの見出しを右クリックし、カラムを個別に選択または選択解除します。または、[More] をクリックして、[View] > [Customize Columns] コマンドで使用したのと同じダイアログボックスを開きます。

（注） [Description]、[Event Name]、[Receive Time] 以外のほとんどのカラムに、フィルタリング機能があります。詳細については、カラムベース フィルタの作成 （3528 ページ）を参照してください。

表 *974 : Event Viewer* のカラムの説明

カラムのラベル	説明
AAA Group	AAA グループ ポリシー。
AAA Server	ユーザのアクセス要求を処理するサーバ。認証、許可、アカウンティングを実行します。
AAA ユーザ（AAA User）	AAA ユーザ名。
ACE Hash1 ACE Hash2	アクセス コントロール リスト エントリ（ACE）のハッシュコード 1 とハッシュコード 2。 syslog 106023 イベントおよび 106100 イベントからポリシー検索を正常に完了するには、ハッシュ コードが必要です。このようなハッシュ コードは、Security Manager を使用して設定を展開した場合にだけ使用できます。
ACL Name	アクセス コントロール リスト（ACL）の名前または ID。

カラムのラベル	説明
Action	フローに対して実行されるアクション。たとえば、終了や拒否。
アラート詳細（Alert Details）	アラートに関する詳細。
アプリ名	イベントを発生させているアプリケーションの名前。
App Stop Reason	アプリケーションがシャットダウンされた方法と理由に関する説明。
アプリケーションバージョン	イベントを発生させているアプリケーションのバージョン。
Attack Relevance Rating	攻撃とその対象となる宛先との関連性を示すために使用される数値。
Backplane Interface	バックプレーンインターフェイス。バックプレーンインターフェイスが物理インターフェイスと異なる場合にだけ識別されます。
Botnet Category	ドメイン名がブロックリストに掲載されている理由を示すカテゴリ。たとえば、ボットネット、トロイの木馬、スパイウェアなど。
Botnet Domain	動的なフィルタデータベースに登録されていて、トラフィックの宛先となったドメイン名または IP アドレス。ブロック リスト、許可リスト、またはグレーリストに追加できます。
Build Time	ソフトウェアが構築された日付と時刻。
Build Type	構築のタイプ。通常、これは「リリース」または「デバッグ」などの語句です。アプリケーションのビルダーの ID である場合もあります。
Byte Count	接続のデータ転送のバイト数。
Call Id	このパケットが属するセッションのピアのコール ID。
クラスマップ	クラスマップ名。
接続期間（Connection Duration）	接続のライフタイム。
Connection ID	接続の一意の識別子。
Connection Limit	接続またはセッションの最大数。
Connection Termination Value	接続終了の要因。バージョンが正しくない、ペイロードタイプが無効であるなど。

カラムのラベル	説明
Current Connection Count	現在の接続の数。
説明	syslog の場合は未処理メッセージが表示され、IPS の場合はイベントの説明が表示されます。
[接続先（Destination）]	トラフィック宛先（ASA および FWSM の場合）または攻撃目標（IPS の場合）の IP アドレスまたはホスト名。複数の値を取ることができ、IPv4 または IPv6 アドレスを含められます。 [View] > [Show Network Host Objects] が選択されて、宛先 IP アドレスと一致するホストオブジェクトが定義されている場合は、ホスト オブジェクト名が表示されます。 **ヒント** そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
Destination Context Data	アラートがトリガーされた直前および直後に送信されたデータを示すコンテキストバッファ。ターゲットから供給されたストリーム データを Base64 でエンコードした表現。
Destination FQDN	宛先 IP アドレスの完全修飾ドメイン名（ある場合）。
Destination Interface	宛先インターフェイス。 Etherchannel アラート（426001 ～ 426003）の場合は、このイベントが発生した Etherchannel インターフェイスの名前。[Source Interface] カラムにメンバ インターフェイスが識別されます。
Destination Locality	侵入で指定されたとおりに、ターゲットアドレスが特定のネットワークの内側に存在するか、外側に存在するか。
Destination OS	ターゲットのオペレーティングシステム情報。
Destination OS Relevance	宛先ターゲット OS 値の関連性を示す数値。
Destination OS Source	ターゲット OS データの情報元。使用できる値は learned、imported、または configured です。
Destination Service	宛先ポート。複数の値になることがあります。
Destination User Identity	トラフィック宛先のユーザ名（存在する場合）。
デバイス	イベントの送信元。通常はデバイス ID です。 Not Available と識別されたデバイスは、Security Manager インベントリから削除されています。

カラムのラベル	説明
Device Identifier	ASA デバイスのクラスタの場合、イベントのソースノードの ID です。これは、[Server Setup] ページ （2664 ページ）の [Syslogデバイス IDを有効にする（Enable Syslog Device ID）] 設定に基づいています。 [デバイスID（Device Identifier）] を使用して、生成された syslog をフェールオーバーデバイスでフィルタリングできます。フェールオーバーが発生した場合、syslog メッセージを生成したフェールオーバーデバイスの IP アドレスがここに表示されます。ただし、Cisco Security Manager で管理されているフェールオーバーデバイスによって生成された syslog メッセージの場合、[デバイス ID（Device Identifier）] 列は空白になります。 （注） [ツール（Tools）] > [Cisco Security Manager管理（Cisco Security Manager Administration）] の [イベント管理（Event Management）] ページで、[フェールオーバースタンバイデバイスからのsyslogを処理（Process Syslogs from Failover Standby Device）] チェックボックスをオンにします。 クラスタは、複数のノードを持つ単一のデバイスとして Security Manager によって管理されます。したがって、すべてのノードのイベントはクラスタ仮想 IP にマップされ、Event Viewer にクラスタ仮想 IP と共に表示されます。[デバイスID（Device Identifier）] を使用して、ノードの特定のクラスタメンバーにより生成された syslog をフィルタリングできます。
方向	トラフィックの方向。inbound または outbound です。
イベント ID（Event ID）	内部で各イベントに割り当てられる一意の連続番号。
Event Name	イベントに付けられたユーザにわかりやすい名前。
Event Summary	サマリーアラートであり、特性が共通する 1 つ以上のアラートを表したものです。数値は、「initialAlert」属性値との一致により、最後のサマリーアラート以降にシグニチャが発行された回数を示します。
イベント タイプ ID	ASA または FWSM の場合は Syslog ID です。 IPS の場合は次のいずれかになります。 • [Sig ID] と [Sub-Sig ID] の組み合わせ（IPS アラート イベントの場合） • IPS ステータス（IPS ステータス イベントの場合） • IPS エラー（IPS エラー イベントの場合）

カラムのラベル	説明
Execution State	アプリケーションの実行ステータス。
Final Alert	サマリーアラートに適用され、特性が共通する1つ以上のアラートを表したものです。このアラートが、 initialAlert 属性に同じ値を含む最後のイベントアラートであるかどうかを示します。
Generation Time	デバイスのローカルイベント生成時刻を表します（IPS イベントでのみ使用可能）。
Global Correlation Audit Mode	アラートが監査モード処理で処理されたかどうか（true または false）。
Global Correlation Deny Attacker	リスク レーティングを算出した結果、内部オーバーライドを超えたために、攻撃者拒否アクションが発生した（または発生することになっていた）のかどうかを示す true または false。
Global Correlation Deny Packet	リスク レーティングを算出した結果、内部オーバーライドを超えたために、パケット拒否アクションが発生した（または発生することになっていた）のかどうかを示す true または false。
Global Correlation Modified Risk Rating	リスク レーティングのためにレピュテーション リスク デルタを追加して、リスク レーティングを調整したかどうかを示す true または false。
グローバル相関その他のオーバーライド（Global Correlation Other Overrides）	リスク レーティングを算出した結果、オーバーライドしきい値を超えたために、他に防御アクションが講じられたかどうかを示す true または false。
Global Correlation Risk Delta	レピュテーション スコアにより、リスク レーティングをどのくらい増やしたかを示す 0 ～ 99 の値。監査モードがイネーブルになっている場合は、監査モードがイネーブルでないと、リスク レーティングをどのくらい調整することになったかを示します。
ヒット カウント（Hit Count）	設定された時間間隔で ACL エントリによってフローが許可または拒否された回数。ASA または FWSM が特定のフローに対して最初の syslog メッセージを生成すると、値が 1 となります。 （注） 画面間を移動した後に ACL ポリシーページに移動すると、すべての ACL ルールについて、[HitCount] および [LastHitTime] の値にそれぞれ [0] および [なし（Never）] が表示されます。実際の [HitCount] および [LastHitTime] の値を取得するには、ACL ポリシーページの [ヒットカウントの更新（Refresh Hit Count）] ボタンをクリックします。値はデータベースから取得され、すべての ACL ルールに表示されます。

カラムのラベル	説明
Hit Count Info	ACL ヒットカウント情報（例：First hit）。
ホスト ID（Host ID）	イベントを発生させたホストのグローバルに一意な識別子。
ICMP コード（ICMP Code）	ICMP タイプのコード。たとえば、ICMP タイプ 3 およびコード 0 はネット到達不能であり、コード 1 はホスト到達不能です。
ICMP Type	ICMP メッセージのタイプ。たとえば、宛先到達不能の場合は3、エコーの場合は 8 です。
初期アラート（Initial Alert）	このフィールドはサマリーアラートに適用され、特性が共通する 1 つ以上のアラートを表したものです。値 initialAlertは、特性（sigid/subsigid）が同じでサマリー アラートではない最後の evIdsAlert のイベント ID です。
Ip Log ID	iplog ドキュメントを（ホスト範囲とともに）一意に識別する IP ログ識別子。
IpLog Address	IP ログに関連付けられた IPv4 または IPv6 アドレス。
IpLog Alert Reference	ログの開始をトリガーした evAlert イベントのグローバル イベント ID。
IpLog Begin Time	ログ ドキュメントに現在使用できる時間範囲の開始。
IpLog Bytes Captured	キャプチャされた総バイト数。キャプチャされたパケットの中には、メモリ制限のためにログからすでに削除されているものもあることに注意してください。
IpLog Bytes Remaining	ログが終了するまでの残りバイト数。
IpLog End Time	ログ ドキュメントに現在使用できる時間範囲の終了。
IpLog残り時間（分）（IpLog Minutes Remaining）	ログが終了するまでの残り分数。
IpLogキャプチャされたパケット（IpLog Packets Captured）	キャプチャおよび記録されたパケットの総数。
IpLog Packets Remaining	ログが終了するまでの残りパケット数。
IpLog Status	ログ ステータスを表す文字列。
IPS Category	SEE イベント カテゴリ。
IPS User	操作を開始しているユーザのユーザ名。

カラムのラベル	説明
License Limit	ライセンスの最大数。
List Name	ドメイン名が記載されているリスト、管理者許可リスト、ブロックリスト、または IronPort リスト。
ログイン アクション（Login Action）	発生したログインアクション：loggedIn、loggedOut、または loginFailed。
Malicious Host	悪意のあるホストのホスト名。
Malicious IP	悪意のあるデバイスの IP アドレス。
Max Connection	NAT 接続の最大数。
MaxEmbryonic Connection	初期接続の最大数。
NAT Destination	変換された（NAT されたとも呼ばれる）宛先 IP アドレス。 変換された宛先のホスト名。
NAT Destination Service	変換された（または NAT された）宛先ポート。
NAT Global IP	グローバルアドレス。IPv4 または IPv6 アドレスを含められます。
NAT Source	変換された（または NAT された）送信元 IP アドレス。IPv4 または IPv6 アドレスを含められます。 変換された送信元のホスト名。
NAT Source Service	変換された（または NAT された）送信元ポート。
NAT Type	ネットワークアドレス変換のタイプ（例：[スタティック（Static）] または [ダイナミック（Dynamic）]）。
New Time	デバイス クロックが変更された時刻。
New Version	アップグレードインストール後のシステム ソフトウェア バージョン。
番号	現在表示されているイベント（行）の数これは単純な連番であり、イベントの内容とは関係ありません。イベントのタイプの情報については、[Event ID] および [Event Name] フィールドを参照してください。
Old Time	変更前のデバイス クロック時間。
Old Version	アップグレードアンインストール前のシステム ソフトウェア バージョン。
Operation Successful	操作が正常に実行されたかどうかを示します。

カラムのラベル	説明
Package File	自動的にダウンロードされてインストールされるパッケージファイルの名前。
Physical Interface	物理インターフェイス。物理インターフェイスが [Interface] カラムの対応する値と異なる場合にだけ識別されます。
ポリシー マップ	ポリシー マップ名。
Protocol	Level-3 プロトコルまたは Level-4 プロトコル。
プロトコルバージョン	プロトコル バージョン。
Protocol (Non L3)	イベントに示された Level-3 または Level-4 以外のプロトコル。たとえば、TACACS、RADIUS、FTP、または H245。
理由	特定のイベントに関連付けられた理由。たとえば、接続のティアダウンが関連付けの理由の場合があります。
Receive Time	イベントが Security Manager によって受信された時刻。
レピュテーション	-10.0 ～ +10.0 で示される攻撃者のレピュテーションスコア。スコアが低い（負の値が大きい）ほど、ホストが悪意のあるホストである可能性が高くなります。
Result Status	操作が正常に完了したかどうかを示す操作のステータス。
Risk Rating	イベントに関連付けられたリスクを計算した値。
[グループでのロール（Role in Group）]	ASA ロードバランシンググループのこのメンバーのロール（[グループ（Group）]、[制御（Control）]、または [データ（Data）]）。
セキュリティコンテキスト	対応する [Interface] カラムに指定された名前付きインターフェイスが関連付けられているセキュリティ コンテキスト。
Sensor Event ID	イベントのシリアル番号。発信元ホストのスコープ内で一意であることが保証されています。
重大度	ファイアウォールまたは IPS の重大度値。
SIA Event Name	[SIA Service Name] フィールドで識別されたサービスに対して発生したイベント。
SIA Service Name	このイベントが発生した Service Insertion Architecture（SIA）サービスの名前。
Sig Details	レポートされたシグニチャの詳細。トリガーされて、アラートの生成を引き起こしたシグニチャです。

カラムのラベル	説明
Sig ID	Sig ID 値は、アラート発信者がアクティビティを特定するために使用されます。この値により、アクティビティにあらかじめ定義されているシグニチャを識別できます。
Signature Version	アラートの生成に使用されたシグニチャ定義のバージョン。
ソース	トラフィック送信元（ASA および FWSM の場合）または攻撃者（IPS の場合）の IP アドレスまたはホスト名。複数の値を取ることができ、IPv4 または IPv6 アドレスを含められます。 [View] > [Show Network Host Objects] が選択されて、送信元 IP アドレスと一致するホスト オブジェクトが定義されている場合は、ホスト オブジェクト名が表示されます。 **ヒント** そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。
Source Context Data	アラートがトリガーされた直前および直後に送信されたデータを示すコンテキスト バッファ。攻撃者から供給されたストリーム データを Base64 でエンコードした表現。
Source FQDN	送信元 IP アドレスの完全修飾ドメイン名（ある場合）。
送信元インターフェイス（Source Interface）	送信元インターフェイス。 Etherchannel アラート（426001 ～ 426003）の場合は、このイベントが発生した Etherchannel バンドルの一部であるインターフェイスの名前。[Destination Interface] カラムに Etherchannel インターフェイスが識別されます。
Source Locality	攻撃者のアドレスが、侵入検知デバイスの設定で指定された特定のネットワークの内側に存在するか、外側に存在するかを識別します。
送信元サービス（Source Service）	送信元ポート。
Source User Identity	トラフィック送信元に関連付けられているユーザ名（ある場合）。
SSO サーバー	シングル サインオン（SSO）サーバ名。
SSO Server Type	シングル サインオン（SSO）サーバ タイプ。たとえば、SiteMinder。
Sub SigId	サブシグニチャ ID 値。シグニチャ ID（sigId）とともに、アラート発信者がアクティビティを特定するために使用されます。

カラムのラベル	説明
Summary Type	サマリーアラートのすべてのアラートに共通する特性を定義します。
Target Value Rating	アラートで特定したターゲットに関連付けられているアセット値。
脅威レベル	脅威度が関連付けられている場合に、次の値のいずれかが表示されます。none、very-low、low、moderate、high、または very-high。
Threat Rating	イベントの脅威レーティング（ある場合）。
タイム ゾーン	発信元ホストがある場所の現地タイムゾーン。
Translated Call ID	このパケットが属するセッションのピアの変換済みコール ID。
Trigger Packet	アラートをトリガーした単一の完全なパケット（base64 バイナリ形式）。
Truncated	イベントに含まれるトリガーパケットが切り捨てられているかどうか。
トンネル タイプ	VPN トンネル タイプ。
タイプ（Type）	AAA タイプ。authentication、authorization、accounting など。
Upgrade Name	アンインストールされたアップグレード パッケージの名前。
URI	自動アップグレード サーバ ディレクトリの URI。
UTC Offset	センサー現地時間の offset 属性は、発信元ホストがある現地時間に変換するために UTC 時間に追加する必要がある分数を示します。
仮想センサー	イベントに関連付けられた仮想センサーの名前。
VLAN Id	アラートをトリガーしたアクティビティにかかわるパケットに関連付けられた VLAN 番号。
[VPNグループ（VPN Group）]	VPN グループ ポリシー。
VPN IPSec SPI	IPSec セキュリティ パラメータ インデックス。
VPN User	VPN ユーザ名。
Watchlist Delta	アラートに関連付けられたアクティビティの送信元がウォッチリストに記載されているために、リスク レーティングに付加された値。

時間スライダ

時間スライダは、履歴ビューの使用中にイベント テーブルの下にあります。リアルタイム ビューでは使用されません。次の図に、時間スライダを示します。右側の改ページコントロールについては、図 61 : 時間スライダの要素 （3504 ページ） で説明します。

図 *61* : 時間スライダの要素

時間スライダは、次の操作を実行する場合に使用できます。

- サーバでの Events Per Second（EPS）傾向を表示します。必要なタイム フレームの期間の EPS 傾向がより良く表示されるように、右側のコントロールを使用してズームインまたはズームアウトできます。

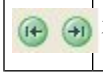
ウィンドウ内に時間範囲を配置するために、時間スライダの背景をクリックしてドラッグすることもできます。背景を動かしても選択した時間範囲に影響はありません。

- イベントテーブル内に表示するイベントの時間のスライスを選択します。選択には、垂直スライダを動かすか、改ページコントロールを使用します。垂直スライダの位置は、イベントテーブルに表示される最新のイベントを決定します。時間のスライスを変更するたびに、その期間に一致するイベントがイベント テーブルにリロードされます。

イベント テーブルに表示されるイベントの時間範囲は、選択した時間間隔によって決まります。詳細については、イベントの時間範囲の選択 （3526 ページ）を参照してください。

次の表に、時間スライダの右側の改ページコントロールについて説明します。

表 *975* : 時間スライダのページ送りボタン

要素	説明
	前のページ（前方）および次のページ（後方）。ページのサイズは、選択した時間モードによって異なります。 （注） たとえば、前方から後方というようにページ コントロールを交互に使用すると、イベント テーブルでのソート順序が逆になります。つまり、最新のイベントが、テーブルの上から下、または下から上の順に並びます。
	先頭ページ（最前方）および最終ページ（最後方）。

要素	説明
	ズームイン（表示される合計時間間隔が短くなります）およびズームアウト（表示される時間間隔が長くなります）。 ズームしても、イベントテーブルの内容は変更されません。青色の影付きの領域は、イベント テーブルに現在表示されている時間間隔を示します。

[Event Details] ペイン

[Event Details] ペイン（[Event Monitoring] ウィンドウ （3489 ページ）に示す）には、単一のイベント内に含まれる情報が表示されます。この情報はペイン内の複数のタブに表示され、その内容はデータを解析する Event Viewer のイベントおよび機能の豊富さによって異なります。コンポーネントには、次のものがあります。

- [表示されるフィールド（Displayed Fields）] タブ：イベントテーブルに表示されるフィールドを表示します。
- [詳細（Details）] タブ：選択したイベントに使用できるすべてのフィールドを表示します。フィールドは、アルファベット順になっています。
- [説明（Explanation）] タブ：このイベントタイプの概要を表示します。
- [関連する脅威（Related Threats）] タブ：イベントと相関関係にある脅威を表示します（IPS イベントのみ）。
- [推奨アクション（Recommended Action）] タブ：このタイプのイベントに対する推奨事項を表示します（Syslogs のみ）。
- [トリガーパケット（Trigger Packet）] タブ：トリガーパケットデータを表示します（IPS イベントのみ）。
- [コンテキストパケット（Context Packet）] タブ：送信元（攻撃者）および宛先（ターゲット）のコンテキストパケットデータを表示します（IPS イベントのみ）。
- [メモ（Notes）]：メモを追加して、後で特定のシグネチャに戻って、自分や他のユーザーがシグネチャやイベントに追加した内容を確認できるようにします。詳細については、[Signatures] ページ （2169 ページ）を参照してください。

（注） ここで追加したメモは、Configuration Manager をクロス起動したときにも保持されます。

（注） 特定のシグネチャに対するイベントが複数ある場合、1 つのイベントに注釈を付けると、そのシグネチャに関連するすべてのイベントに注釈が付けられます。

イベント管理の準備

デバイスから生成されたイベントを表示する場合は、事前にそのデバイスを Event Viewer で機能するように設定する必要があります。

時間の同期

標準のネットワーク管理では、時差およびネットワークデバイス同期が考慮されます。そのために通常、ネットワーク タイム プロトコル（NTP）サーバが使用されます。Event Viewer は、時間基準を統一すると最も使いやすくなります。ただし、Security Manager がイベントを受け取った時刻（[Receive Time]）を表示できるほか、IPS デバイスの場合にはデバイスがイベントを生成した時刻（[Generation Time]）を表示できます。

可能な場合は常に、同じ NTP サーバでモニタリングしている Security Manager サーバおよびデバイスを設定します。

クライアントが開かれたときの Security Manager サーバーのクロックと Security Manager クライアントのクロックの違いは、イベントデータをサーバー時間からクライアント時間に変換/マッピングするときに考慮されます。たとえば、Security Manager サーバーの時間が進んで時差が動的に変化する場合、サーバーから取得されたデータには更新されたタイムスタンプが表示されますが、クライアントが開かれたときに、クライアントは引き続き、サーバーの時間とクライアントの時間に基づいて時差をマッピングします。このような状況では、サーバーでの時間の変化に対応する短い時間だけ、イベントビューアにデータが表示されません。このため、Security Manager サーバーのクロックの変更は、頻度を減らし、影響が最も少ない時間に行うことをお勧めします。

イベント管理のための ASA と FWSM デバイスの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き FWSM の機能をサポートしますが、バグ修正や拡張機能はサポートしていません。

イベントビューアまたは syslog イベントを分析する他のアプリケーションを使用して ASA（ASA-SM を含む）または FWSM デバイスから生成されたイベントを表示する場合は、事前に syslog メッセージを生成および送信するようにそのデバイスでロギングポリシーを設定する必要があります。

（注） 仮想 IP アドレスを持つクラスタデバイス（Security Manager バージョン 4.4 以降）が Security Manager と仮想デバイスの両方で設定されている場合、そのデバイスを追加できます。

ヒント　デバイスごとに適切なロギング設定を指定できますが、ネットワーク内の複数の ASA または FWSM デバイスで同じロギング設定を使用することになる場合もあります。この項では個々のデバイスを設定する方法について説明しますが、共有ポリシーを作成して複数のデバイスに割り当てることもできます。共有ポリシーの設定と割り当ての詳細については、新しい共有ポリシーの作成 （278 ページ）およびポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

ここで説明するロギング設定のほか、ファイアウォール ポリシーまたは ACL ポリシー オブジェクトにアクセス コントロール エントリを設定した場合にはそのエントリごとにロギングを設定することもできます。デフォルトでは拒否されたアクセスだけがログに記録されますが、ログに記録する情報が増えるように ACL ロギング オプションを設定できます。

（注）　マルチ コンテキスト モードでコンテキストからイベントを確実にレポートするには、Cisco Event Viewer は各コンテキストの管理インターフェイスの IP アドレスを必要とします。

ステップ 1　（デバイスビュー）ASA もしくは FWSM デバイスまたはセキュリティコンテキストを選択してから、ポリシーセレクタで [プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [ロギング設定（Logging Setup）] を選択します。

ポリシーで、[ロギングの有効化（Enable Logging）] を選択します。必要に応じて他のオプションを設定できます。オプションの詳細については、[Logging Setup] ページ （2656 ページ）を参照してください。

ステップ 2　[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [Syslogサーバー（Syslog Servers）] を選択します。

Security Manager サーバーの IP アドレスを syslog サーバーテーブルに追加します。UDP プロトコルを使用するようにサーバを設定します。Security Manager Administration の[Event Management] ページ （677 ページ）で別のポートを設定しないかぎり、デフォルト ポート 514 が適切なポートです。

CS-MARS など他のイベント管理アプリケーションを使用している場合には、そのサーバもこのポリシーに追加します。

（注）　必要に応じて EMBLEM メッセージフォーマットを使用できます。従来のフォーマットも EMBLEM フォーマットもサポートされています。CS-MARS では EMBLEM がサポートされないため、CS-MARS サーバには EMBLEM フォーマットのメッセージを送信しないでください。

syslog サーバ ポリシーのオプションの詳細については、[Syslog Servers] ページ （2671 ページ）を参照してください。

ステップ 3　タイムスタンプを syslog メッセージに追加する、メッセージの重大度を変更する、特定のメッセージの生成を抑止するなど、デフォルト以外の syslog サーバー設定を行う場合は、[プラットフォーム（Platform）] > [ロギング（Logging）] > [Syslog] > [サーバーのセットアップ（Server Setup）] ポリシーを設定します。詳細については、[Server Setup] ページ （2664 ページ）を参照してください。

ステップ 4 （任意）[プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslog]>[ロギングフィルタ（Logging Filters）] ポリシーでは、syslog サーバーに送信されるメッセージの種類を微調整できます。このポリシーの詳細については、[Logging Filters] ページ （2651 ページ）および [Edit Logging Filters] ダイアログボックス（2653 ページ）を参照してください。

次に、このポリシーを設定するためのヒントを示します。

- ロギングフィルタを追加するときには、[ロギング先（Logging Destination）] に [Syslogサーバー（Syslog Servers）] を選択します。
- メッセージ重大度に基づいて簡単なフィルタを作成したり、イベントクラスに基づいてはるかに複雑なフィルタを設定したりできます。イベントクラスを使用する場合は、[ロギングフィルタ（Logging Filters）] ポリシーで直接設定を行うことも、[イベントリスト（Event Lists）] ポリシーで個別にイベントリストを設定することもできます（[Event Lists] ページ （2647 ページ）を参照）。

ステップ 5 （任意）メッセージの重大度またはメッセージ番号で時間間隔あたりに生成されるメッセージの数量を制限するように、[プラットフォーム（Platform）]>[ロギング（Logging）]>[Syslog]>[レート制限（Rate Limit）] ポリシーを設定できます。これにより、syslog サーバのフラッディングを回避するのが容易になります。[Rate Limit] ページ （2659 ページ）を参照してください。

ステップ 6 （任意、ただし推奨）ASA デバイスのネットワーク タイム プロトコル サーバーを指定するように、[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[サーバーアクセス（Server Access）]>[NTP] ポリシーを設定できます。NTP を使用すると、日付と時刻情報の一貫性を確保して容易にイベントを相関付けることができます。Security Manager サーバに使用するのと同じ NTP サーバを指定します。異なるサーバを使用する場合は、それらのサーバが同期されていることを確認してください。[NTP] ページ（2624 ページ） を参照してください。

イベント管理のための IPS デバイスの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IPS デバイスから生成されたイベントを Event Viewer を使用して表示する場合は、事前に Security Manager サーバがそのデバイスにアクセスできるようにそのデバイスで [Allowed Hosts] ポリシーを設定する必要があります。[Allowed Hosts] ポリシーでは設定へのアクセスも許可するように Security Manager を設定する必要があるため、IPS デバイスがすでに正しく設定されている可能性があります。また、ネットワーク タイム プロトコル（NTP）も設定する必要があります。

IPS デバイスで効率よくイベントを管理できるように、デバイス ビューで IPS デバイスに対して次のポリシーを設定します。

- [プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[デバイスアクセス（Device Access）]>[許可されたホスト（Allowed Hosts）]：（必須）Security Manager サーバーをテーブルに追加します。Security Manager サーバをそのホスト IP アドレス（たとえ

ば、10.100.10.10）で特定するか、または Security Manager サーバが存在するネットワーク（たとえば、10.100.10.0/24）を指定できます。

デバイスで CS-MARS など他のイベント管理アプリケーションを使用している場合は、そのサーバもポリシーに必ず追加します。

Allowed Hosts ポリシーの設定の詳細については、許可ホストの識別 （2091 ページ）を参照してください。

- [プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [サーバーアクセス（Server Access）] > [NTP]：（推奨）日付と時刻情報の一貫性を確保して容易にイベントを相関付けることができるように、Security Manager サーバーに使用するのと同じ NTP サーバーを設定します。異なるサーバを使用する場合は、それらのサーバが同期されていることを確認してください。詳細については、NTP サーバの識別 （2112 ページ）を参照してください。

ヒント　デバイスごとに適切な許可ホストおよび NTP 設定を指定できますが、ネットワーク内の複数の IPS デバイスで同じ設定を使用することになる場合もあります。この項では個々のデバイスを設定する方法について説明しますが、ポリシーの共有バージョンを作成して複数のデバイスに割り当てることもできます。共有ポリシーの設定と割り当ての詳細については、新しい共有ポリシーの作成 （278 ページ）およびポリシー ビューにおけるポリシー割り当ての変更 （279 ページ）を参照してください。

Event Manager サービスの管理

Event Manager サービスにより、Event Viewer アプリケーションを使用できるようになります。Event Viewer を機能させるには、このサービスを開始する必要があります。サービスの機能全体を設定および管理するために実行できるタスクがいくつかあります。

ここでは、次の内容について説明します。

- Event Manager サービスの開始、停止、および設定 （3509 ページ）
- Event Manager サービスのモニタリング （3511 ページ）
- モニタするデバイスの選択 （3514 ページ）
- イベント データ ストア用のディスク スペースの使用率のモニタリング （3516 ページ）
- イベント データ ストアのアーカイブまたはバックアップと復元 （3516 ページ）

Event Manager サービスの開始、停止、および設定

Event Viewer または Report Manager を使用するには、Event Manager サービスが動作中である必要があります。

Security Manager をインストールすると、『Installation Guide for Cisco Security Manager』に記載のとおり、サーバーが最小メモリ要件を満たさない場合を除き、Event Manager サービスは自動的にイネーブルになります。最小メモリ要件を満たさないシステム上でもサービスを手動で開始できますが、満足できるパフォーマンスが得られない場合があります。主な要因は、管理対象のデバイスの数と各デバイスのイベント生成速度です。

ヒント [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）] ページで [イベント管理の有効化（Enable Event Management）] オプションが選択されているにもかかわらず、[起動（Launch）] > [イベントビューア（Event Viewer）] を選択したときにイベントビューアが使用不可能であるというメッセージが表示される場合は、イベントビューアサービスを再起動してみてください。まず、[Enable] オプションの選択を解除し、[Save] をクリックします。サービスが停止するまで待ちます。次に、[Enable] オプションを選択し、[Save] をクリックし、サービスが再び開始されるまで待機します。その後、Event Viewer を再度開いてみます。

次の手順では、Event Manager サービスを開始、停止、および設定する方法について説明します。

関連項目

- イベント データ ストア用のディスク スペースの使用率のモニタリング （3516 ページ）

ステップ 1 （イベントビューアではなく）メインの [Security Manager] ウィンドウで、**[ツール（Tools）] > [Security Manager管理（Security Manager Administration）]** を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択します。

ステップ 2 次のいずれかを実行します。

- Event Manager サービスをイネーブルまたは開始するには、[イベント管理の有効化（Enable Event Management）] を選択します。
- Event Manager サービスをディセーブルまたは停止するには、[イベント管理の有効化（Enable Event Management）] の選択を解除します。

イベントデータ ストアの場所と最大サイズ、デバイスがイベントを送信する必要のある syslog ポート、改ページサイズ（これにより、イベントテーブルにロードされるイベントの最大数が決まります）など、他の設定も変更できます。拡張イベント ストレージの場所を設定して、プライマリ保管場所を拡張することもできます。これらの設定の詳細については、[Event Management] ページ （677 ページ）を参照してください。

（注） バージョン 4.5 以降、Security Manager では、syslog を 1 つのローカルコレクタと 2 つのリモートコレクタに転送できます。詳細については、[Event Management] ページ （677 ページ）を参照してください。

ステップ 3 [保存（Save）] をクリックして変更を保存します。

[Enable Event Management] オプションを変更した場合、Event Manager サービスを起動または停止してもよいかどうかの確認が求められます。[はい（Yes）] をクリックするとサービスがすぐに開始または停止し、進捗インジケータが表示され、変更が完了したときに通知されます。ステータス変更が完了するまで待ってから続行します。

改ページサイズを除く他の設定を変更する場合は、Event Manager サービスをいったん停止してから再起動する必要があります。進捗インジケータが表示されます。

Event Manager サービスのモニタリング

Event Manager サービスは、着信 syslog メッセージを処理し、モニタ対象の IPS デバイスから SDEE アラートを取得します。処理されるデータ量は、ネットワーク アクティビティによって異なります。ネットワーク内で生成される Events Per Second（EPS）がサービスによって処理できるよりも大きい時間がある可能性があります。この場合、サービスはスロットルモードに移行してイベントを選択的にドロップします。

サービスのステータスをモニタして輻輳を特定し、発生する問題に対処できます。サービスのステータスは、Event Viewer の概要 （3481 ページ）に示すように、Event Viewer のステータスバーの右下隅のアイコンに表示されます。[Total EPS] は、サービスに発生している現在の Events Per Second のレートを示します。アラート ステータス アイコンの色は次を示します。

- 緑色の点：問題はありません。すべてのイベントが正常に処理されています。
- 黄色の点：警告がいくつかあります。たとえば、重大度レベルが低いイベントがドロップされた場合。
- オレンジ色の点：より深刻な問題があります。たとえば、重大度レベルが低いおよび中程度のイベントがドロップされた場合。
- 赤い色の点：クリティカルな状況です。たとえば、重大度レベルが高いイベントがドロップされた、または syslog ポートもしくはイベント データ ストアの場所に問題があるなど、システムに重大な問題がある場合。
- ネットワーク ワイヤの切断：Event Manager サービスが意図的にまたはサーバ問題によってディセーブルになっています。イベントは保存または取得されません。これが意図的ではない場合は、Event Manager サービスの開始、停止、および設定 （3509 ページ）で説明するとおりに、Event Manager サービスを再起動します。

詳細情報を表示するには、アラート ステータス アイコンをクリックします。バブルが開いて、過去 5 分の概要統計情報が表示されます。統計情報には、受信およびドロップしたイベント数や、ある場合はイベント サーバ アラート メッセージが含まれます。アラート ステータス アイコンをもう一度クリックしてバブルを閉じます。

バブルが開いているときに、バブル内の [詳細（Details）] リンクをクリックしてより詳細な情報を表示できます。[Details] リンクをクリックすると、[Event Statistics Details] ダイアログボックスが開いて、次の情報が表示されます。

- **[Last 5 Minutes Statistics]**：

- [受信済みイベント数（Events Received）]：サービスが過去 5 分間に受信した syslog イベントおよび取得した SDEE アラートの総数。
- [ドロップ済みイベント数（Events Dropped）]：輻輳が原因でサービスでドロップする必要があったイベントまたはアラートの総数。この数は、モニタ対象のデバイスからのドロップだけを示します。このため、通常の状況では、この数は 0 である必要があります。0 以外の数の場合は、サービスがスロットル モードであることを示すため、[Event Server Alerts] セクションのメッセージを確認します。
- [監視対象外デバイスからのイベント数（Events from Unmonitored Devices）]：監視対象として選択されていないデバイスからサーバーに送信された syslog メッセージ数（モニタするデバイスの選択 （3514 ページ）を参照）。

モニタ対象外のデバイスからのイベントは常にドロップされますが、サービスに負荷をかけます。最後に検出されたモニタ対象外のデバイスの IP アドレスが表示されます。この IP アドレスを使用してメッセージの送信元を判別します。その後、そのデバイスを監視対象デバイスのリストに追加する必要があるか、または Cisco Security Manager サーバーを syslog サーバーリストから削除するようにデバイスの設定を変更する必要があるか判断できます。

メッセージを送信しているデバイスがネットワーク外にある場合は、この syslog トラフィックがネットワーク内に入ってくることを防ぐようにファイアウォール設定を調整します。

- **[Status Information]**：
  - [秒単位の合計イベント数（EPS）（Total Events Per Second (EPS)）]：イベントを現在処理しているレート。この測定には、ドロップされたイベントは含まれません。
  - [使用されているイベントバッファ（Event Buffer Used）]：イベントの処理に現在使用されている共有イベントバッファのパーセンテージ。バーは、スロットル レベルを示すために次のとおり色分けされます。

緑色：スロットル モードではありません。

黄色：重大度が低いイベントがドロップされました。

オレンジ色：重大度が低いおよび中程度のイベントがドロップされました。

赤色：重大度が高いイベントがドロップされました。

- [イベントサーバーのアラート（Event Server Alerts）]：これらのメッセージには、対処する必要がある特定のステータス問題が表示されます。表示される可能性のあるメッセージと有効なソリューションについては、表 976 : Event Manager ステータス メッセージ （3513 ページ）を参照してください。
- [コピー（Copy）]ボタン：情報をクリップボードにコピーするには、[コピー（Copy）]ボタンをクリックします。コピーした情報には HTML マークアップが含まれます。情報は、HTML ファイルに貼り付けできます。

表 *976 : Event Manager* ステータス メッセージ

アラート メッセージ	アラート レベル	有効なアクション
UDP port <514> could not be acquired, therefore syslog events cannot be collected.	高い	示されたポートを外部アプリケーションがすでに使用している可能性があります（デフォルト syslog ポートは 514）。その外部アプリケーションを停止する必要がある場合があります。**netstat -ao | findstr 514** などの netstat コマンドを使用して、プロセスの PID を識別できます。
The event data store location does not exist, therefore events cannot be stored.	高い	Security Manager の管理設定で設定されたイベント データ ストアの場所が存在しないか、その場所に対して必要な読み取り/書き込み権限が Security Manager サーバにありません。場所の設定の詳細については、[Event Management] ページ （677 ページ）を参照してください。
Low severity events are being dropped.	低い	イベントが非常に高いレートで受信されたか、システムに高い負荷がかかっているかのいずれかです。 デバイスが過度にイベントを頻繁に送信しているかどうかを特定するには、[All Device Events] ビューを開いてリアルタイム ビューと履歴ビュー間の切り替え （3524 ページ）で説明するとおりに、リアルタイム モードに切り替えます。 サーバに高い負荷がかかっているかどうかを特定するには、サーバで Windows にログインして Task Manager または他のツールを使用して Security Manager 以外にシステムに高い負荷をかけているアプリケーションがあるかどうかを確認します。可能であれば、そのアプリケーションをディセーブルにするか停止します。問題が頻繁に発生する場合は、サーバから他のアプリケーションをアンインストールすることを検討します。
Low and medium severity events are being dropped.	中規模	
All events are being dropped.	高い	

アラート メッセージ	アラート レベル	有効なアクション
Events from unknown devices are being received.	低い	モニタするデバイスの選択 （3514ページ）で説明するとおりに、モニタ対象に選択されていないデバイスから syslog イベントが Security Manager サーバに送信されました。これらのデバイスは、モニタリングでサポートされていないデバイス タイプの可能性があり、また Security Manager インベントリにも入っていない可能性があります。 メッセージは、これらのデバイスに対する EPS レートによって異なります。重大度が低いメッセージの場合は、EPS レートが 500 ～ 5,000 であることを示します。中程度の場合は、EPS レートが 5,000 ～ 10,000 であることを示します。高い場合は、EPS レートが 10,000 を超えることを示します。 [最後の5分間の統計（Last 5 Minutes Statistics）] の [監視対象外デバイスからのイベント数（Events from Unmonitored Devices）] 統計情報には、これらのイベントの数および最後のサポート対象外デバイスの IP アドレスが表示されます。モニタ対象にデバイスを選択するか、Security Manager サーバのアドレスを削除するように、デバイスの syslog ポリシーを変更します。複数のモニタ対象外のデバイスがメッセージを送信している場合は、手順を繰り返す必要があります。
Events from unknown devices are being received at a high rate.	中規模	
Events from unknown devices are being received at a very high rate.	高い	

モニタするデバイスの選択

Security Manager データベースに追加されたすべての ASA および FWSM デバイスならびにセキュリティ コンテキスト、ならびに IPS デバイスおよび仮想センサーは、Event Viewer で自動的にモニタ対象に選択されます。

（注） マルチ コンテキスト モードでコンテキストからイベントを確実にレポートするには、Cisco Event Viewer は各コンテキストの管理インターフェイスの IP アドレスを必要とします。

バージョン 4.17 以降、Cisco Security Manager は非管理インターフェイスからもイベントを受け取りますが、次の制限があります。

- 静的 IP アドレスインターフェイスのみがサポートされています。

- Syslog のクラスタープール IP 範囲が使用されるため、クラスターデバイスからのイベントは表示されません。
- Syslog サーバー設定の展開後にのみ、非管理インターフェイス IP を取得するようデバイス イベント マネージャに通知されます。したがって、最初のイベントドロップが発生する可能性があります。
- この拡張機能は、syslog リレーサービスではサポートされていません。

デバイスで Event Viewer を使用しない場合は、そのデバイスをモニタ対象から除外できます。Security Manager サーバを syslog サーバとして使用するように ASA もしくは FWSM デバイスまたはセキュリティ コンテキストを設定していない場合は、デバイスまたはセキュリティ コンテキストからイベントを受信することはいずれにせよないことに注意してください。このため、モニタしない ASA または FWSM の選択を解除する必要はありません。

ヒント Event Viewer では Cisco IOS IPS デバイスをモニタできません。

関連項目

- デバイス インベントリへのデバイスの追加 （94 ページ）
- イベント管理のための ASA と FWSM デバイスの設定 （3506 ページ）
- イベント管理のための IPS デバイスの設定 （3508 ページ）

ステップ 1 イベントビューアで、**[表示（View）] > [監視対象デバイスの管理（Manage Monitored Device）]** を選択して、[監視対象デバイスの管理（Manage Monitored Devices）] ダイアログボックスを開きます。

デバイス リストには、Security Manager インベントリ内のデバイスのうち、表示権限があるすべてのデバイスが表示されます。権限がないデバイスは表示されません。選択できる対象が、表示されたデバイスにかぎられます。いずれのデバイスに対しても選択または選択解除する権限がない場合は、リストは読み取り専用となりデバイスをモニタ対象に選択できません。アクセス権限の詳細については、 Event Viewer のアクセス コントロールについて （3477 ページ）を参照してください。

ステップ 2 Event Viewer でイベントをモニタするデバイスだけが選択されていることを確認します。モニタしないデバイスの選択を解除します。

デバイス グループに属するすべてのデバイスの選択ステータスを変更する場合は、そのグループを選択または選択解除します。

ステップ 3 [OK] をクリック

Event Viewer で変更が有効になるまで待機することが必要になる場合があります。

イベント データ ストア用のディスク スペースの使用率のモニタリング

Event Manager サービスは、指定された量のディスク スペースをプライマリおよび拡張イベント データ ストアに使用します。これにより、サービスが原因でサーバ コンピュータまたは拡張保管場所が過負荷になることが確実になくなります。プライマリおよび拡張イベントデータ ストアのサイズは、[Event Management] ページ （677 ページ）の説明に従い、**[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）]** ページで設定します。

プライマリと拡張の両方の場所で、割り当てたスペースの 90％が使用された場合、新しいデータにスペースを空けるためにストレージから最も古いイベントデータが削除されます。設定した場合は、データはプライマリ ストアから拡張ストアにコピーされます。ほとんどの場合、プライマリ ストレージから削除されたイベントは、循環によって拡張ストレージからなくなるまで拡張保管場所から引き続きクエリーに使用できます（プライマリから拡張データ ストアへのコピーのタイミングは、Events Per Second（EPS）レート、プライマリ ストアの拡張ストアに対する相対的サイズ、および拡張ストアにすでにコピーされたプライマリ データのパーセンテージを含む、多数の要因に依存します）。

イベントビューアで **[表示（View）] > [イベントストアディスク使用率の表示（Show Event Store Disk Usage）]** を選択して、割り当てたスペースのうち現在使用されている量と、最も古いイベントの経過時間をモニターできます。情報は円グラフで表示され、各場所の使用領域と未使用領域が GB 単位で示されます。各場所に現在保存されている最も古いイベントについても示されます。

この情報を参考にして、各場所に割り当てたスペースの増減を判断できます。

ヒント いずれかの場所のサイズを小さくしたときに、その新しいサイズが現在の使用量を下回っている場合は、新たに設定した目標のサイズに達するまで、最も古いイベントから順にすぐに削除されます。

イベント データ ストアのアーカイブまたはバックアップと復元

イベント データ ストアは、標準の Security Manager データベース バックアップには付属していません。イベント データ ストアをアーカイブまたはバックアップする場合は、プライマリまたは拡張のいずれの場所でも、それぞれの作業を別々に実行する必要があります。バックアップは必要に応じて復元できます。

ここでは、イベント データ ストアのバックアップと復元に必要な手順について説明します。

ヒント Event Manager サービスをディセーブルにすると、イベントがデータ ストアに書き込まれないため、バックアップ プロセスまたは復元プロセス中に生成されたイベントが失われることになります。

ステップ 1 イベント データ ストアをバックアップするには、次の手順を実行します。

a) Security Manager クライアントで、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] を選択し、コンテンツテーブルから [イベント管理（Event Management）] を選択します。

b) イベント データ ストア フォルダの名前を特定します。フォルダは、[イベントデータストアの場所（Event Data Store Location）] フィールドに表示されています。デフォルトは *NMSROOT***MDC\eventing\database** で、NMSROOT はインストールディレクトリ（通常は C:\Program Files\CSCOpx）です。

拡張データ ストアをバックアップする場合は、[Extended Data Store Location] フィールドにその場所が指定されます。

c) [Enable Event Management] チェックボックスをオフにして、Event Manager サービスを停止します。[保存（Save）] をクリックして変更を保存します。サービスを停止するかどうかの確認が求められます。[はい（Yes）] をクリックし、サービスが停止したことが通知されるまで待ちます。

d) Security Manager の外部に、*NMSROOT***MDC\eventing\config\collector.properties** ファイルおよびイベントデータ ストア フォルダのコピーを作成します。そのコピーを別のサーバに保存して、ハードウェア障害が発生した場合にバックアップとして使用できるようにします。

拡張データ ストアもバックアップする場合は、そのフォルダもコピーします。

e) Security Manager クライアントの [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [イベント管理（Event Management）] ページで、[イベント管理の有効化（Enable Event Management）] チェックボックスをオンにし、[保存（Save）] をクリックします。サービスを開始するかどうかの確認が求められます。[はい（Yes）] をクリックし、サービスが開始されたことが通知されるまで待ちます。

ステップ 2 イベントデータ ストアを復元するには、次の点を除き、データのバックアップに使用したときと同じプロセスを使用します。

- 既存のイベント データ ストアのコピーを作成するのではなく、イベント データ ストアがある場所にバックアップをコピーします。このとき、まず既存のデータを削除してから、バックアップ データをコピーすることもできます。ただし、データ ストアのサイズ制限を超えていないかぎり、バックアップ データと既存のデータを混在させることができます（データストアの制限は、[ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [イベント管理（Event Management）] ページで設定されます）。

（注） 新旧のデータを混在できるは、collector.properties の既存のコピーを保持している（つまり、まだこのファイルを復元していない）場合で、かつ新旧のデータが同じサーバからのものである場合だけです。複数の異なるサーバからのデータ ストアはマージできません。

- Security Manager の再インストールを必要としたハードウェア障害または他のイベントから回復している場合を除き、collector.properties は復元しないでください。

イベントビューアの使用

モニタ対象のデバイスが関与するネットワーク問題のトラブルシューティングに役立てるために Event Viewer を使用します。ビューおよびフィルタリングを使用して、問題を分析し、原因と有効な対応策を特定することに役立てます。

ここでは、次の内容について説明します。

- イベント ビューの使用方法 （3518 ページ）
- イベントのフィルタリングおよびクエリー （3526 ページ）
- 特定のイベントに対する操作の実行 （3534 ページ）
- Event Viewer からの Security Manager ポリシーの検索 （3541 ページ）
- Looking Up Events for a Cisco Security Manager Policy （3543 ページ）

イベント ビューの使用方法

Event Viewer でイベントを表示するには、ビューを開きます。ビューは、フィルタおよび他のプロパティのセットです。これには、イベントのサブセットを定義できる色ルール、選択したカラムとその位置および幅、ならびにデフォルトの時間枠が含まれます。ビューによってイベント リストのスコープを制限できるため、検索内容をより簡単に見つけられます。

ここでは、次の内容について説明します。

- ビューを開く （3519 ページ）
- ビューのフローティングと配置 （3519 ページ）
- イベント テーブルの表示のカスタマイズ （3520 ページ）
- 送信元/宛先 IP アドレスとホスト オブジェクト名間の切り替え （3521 ページ）
- ビューの色ルールの設定 （3522 ページ）
- カスタム ビューの作成 （3523 ページ）
- カスタム ビューの名前または説明の編集 （3524 ページ）
- リアルタイム ビューと履歴ビュー間の切り替え （3524 ページ）
- ビューの保存 （3525 ページ）
- カスタム ビューの削除 （3525 ページ）

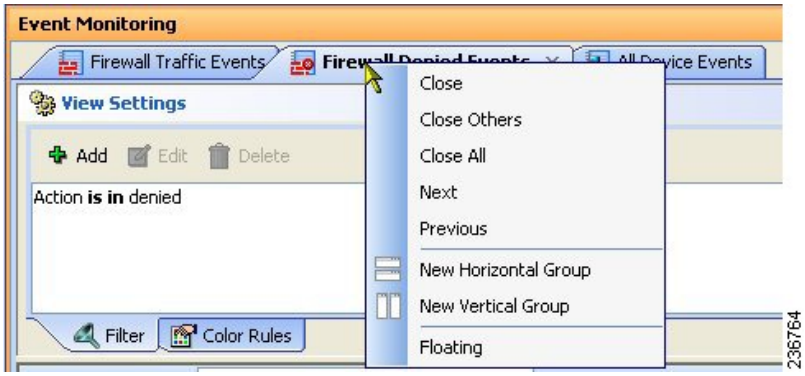
ビューを開く

Event Viewer では、最大 4 つの履歴ビューと 1 つのリアルタイム ビューが開けます。ビューを開くと、Event Viewer はビュー設定および時間範囲を使用してイベント データ ストアからイベントを取得してイベント テーブルに表示します。

- ビューを開いて現在アクティブで開いているビューと置き換えるには、Event Viewer で次のいずれかを実行します。
  - ビューのリストでビューをダブルクリックします。
  - ビューのリストでビューを右クリックして、[開く（Open）] を選択します。
- 新規タブにビューを開くには、次のいずれかを実行します。
  - メニュー バーで **[ファイル（File）] > [ビューを開く（Open View）]** を選択します。[Open a View] ダイアログボックスが開きます。このダイアログボックスは基本的にビューのリストと同じです。ビューを選択して、[OK] をクリックします。
  - ビューのリストでビューを右クリックして、[新しいタブで開く（Open In New Tab）] を選択します。

ビューのフローティングと配置

一度に最大 4 つの履歴ビューと 1 つのリアルタイム ビューが開けます。複数のビューを開いている場合は、Event Viewer のメインウィンドウの右ペインにタブウィンドウとして開かれています。複数のエリアがある場合は、最後に使用したエリア（「タブグループ」）内に開かれています。ウィンドウを配置するコマンドは、次の図に示すようにビュー ウィンドウのタブを右クリックすると表示されます。



必要に応じてビュー ウィンドウを配置するには多くのオプションがあります。たとえば、2 つのビューを並べて比較する、またはビューを閉じずにメイン ウィンドウから削除する必要がある場合があります。

目的の表示にするために、次の方法を使用してビュー ウィンドウを配置できます。

- ビューのフローティング：ビューを閉じずに Event Viewer のメインウィンドウからビューを削除するには、ビューのタブを右クリックして、[フローティング（Floating）] を選択します。ビューは独自のウィンドウに移動されます。

ビューをすでにフローティングしている場合は、[フローティング先（Floating to）] を選択して、すでにフローティングされているウィンドウの 1 つを選択できます。ビューはそのウィンドウ内の新規タブになります。

- ビューのドッキング：フローティングビューを Event Viewer のメインウィンドウに戻すには、ビューのタブを右クリックして、[ドッキング（Docking）] を選択します。
- 並べて比較のためにビューを水平または垂直に配置：ビューをフローティングせずに、簡単に比較できるようにビューを垂直または水平に配置するには、ビューのタブを右クリックして、[新規横方向グループ（New Horizontal Group）] または [新規縦方向グループ（New Vertical Group）] を選択します。これらのコマンドは、現在のタブ付きグループを選択されたレイアウトに分割します。これらのコマンドを使用するには、少なくとも 2 つのビューが開いている必要があります。3 つ以上のビューが開いていて、ビューのすべてを別のウィンドウに開く場合は、コマンドを複数回使用する必要があります。
- 異なるタブグループへのビューの移動：開いているビューがいくつかあり、ビューを水平または垂直なグループに配置している場合に、グループ間でビューを移動するには、ビューのタブを右クリックして、[次のタブグループに移動（Move to Next Tab Group）] または [前のタブグループに移動（Move to Previous Tab Group）] を選択します。コマンドは、このような移動が可能なようにビューが配置されている場合にだけ表示されます。
- グループの方向の変更：水平と垂直間でレイアウトを切り替えるには、ビューのタブを右クリックして、[タブグループの方向を変更（Change Tab Groups Orientation）] を選択します。

イベント テーブルの表示のカスタマイズ

イベント テーブルの定義済みまたはカスタム ビューの表示を要件を満たすようにカスタマイズできます。これらの変更は、定義済みのビューでも保存できます。

イベント テーブルをカスタマイズするために、次の手順を実行できます。

- 一覧表示されるイベントのタイプを制限するために、カラム フィルタを作成します。フィルタを定義するには、カラムベース フィルタの作成 （3528 ページ）で説明するとおりにカラムの見出しの下矢印を使用します。
- 重大度に基づいてイベントを強調表示するには、ビューの色ルールの設定 （3522 ページ）で説明するとおりに色ルールを作成します。
- テーブルに表示するカラムを変更するには、イベント テーブルのカラム （3494 ページ）で説明するとおりにテーブルの見出し行の右側にある [Column Selector] アイコンをクリックします。
- カラムの幅を変更するには、カラムの見出しの右端をクリックし、目的のサイズにドラッグします。

- カラムの順序を変更するには、カラムの見出しをクリックし、カラムを目的の位置にドラッグします。
- カラムでイベント リストをソートするには、カラムの見出しをクリックします。カラム ソートは、昇順、降順、およびデフォルト順（イベント受信時刻順）が3回のクリック サイクルに基づいて実行されます。
- ビューセレクタおよび [イベントモニタリング（Event Monitoring）] ウィンドウの幅をデフォルト値にリセットするには、**[表示（View）]>[レイアウトのリセット（Reset Layout）]** を選択します。
- 送信元および宛先カラムが IP アドレスまたはホスト オブジェクト名のいずれを表示するかを送信元/宛先 IP アドレスとホスト オブジェクト名間の切り替え （3521 ページ）で説明するとおりに変更します。

関連トピック：

- カスタム ビューの作成 （3523 ページ）
- ビューの保存 （3525 ページ）

送信元/宛先 IP アドレスとホスト オブジェクト名間の切り替え

送信元および宛先 IP アドレスを表示できます。または、送信元または宛先 IP アドレスに一致するオブジェクトのホスト オブジェクト名を表示できます。デフォルトでは、Event Viewer はホスト オブジェクト名がある場合にはホスト オブジェクト名を表示します。

IP アドレスからホスト名へのマッピングは、イベントの送信元および宛先だけでサポートされます。また、マッピングはホスト オブジェクトだけに適用されます。イベントの送信元または宛先がネットワーク オブジェクト、グループ オブジェクト、またはアドレス範囲オブジェクトに一致した場合は、Event Viewer ではオブジェクト名が表示されません。

オブジェクトのタイプおよび内容を明らかにします。たとえば、これはホストタイプがネットワーク/ホストオブジェクトの場合だけ機能するのか、つまり、オブジェクトの単一値のホストバージョンか、単一値のグループオブジェクトの場合に機能するのか、またはネットワークか範囲オブジェクトの場合に機能するかなど。

送信元/宛先 IP アドレスとホスト オブジェクト名間で切り替えるには、次の手順を実行します。

- 送信元または宛先 IP アドレスに一致するオブジェクトのホストオブジェクト名を表示するには、[表示（View）] > [ネットワークホストオブジェクトの表示（Show Network Host Objects）] を選択します。このオプションは、デフォルトで選択されます。

ヒント そのオブジェクトに関連付けられた IP アドレスを表示するには、ホスト オブジェクト名にマウス オーバーします。

（注） IP アドレスからホスト オブジェクト名へのキャッシュは、Event Viewer の起動時に作成されます。新規ホスト オブジェクトを定義した場合は、これらの変更をデータベースに送信し、次に Event Viewer を閉じて再起動してこれらのマッピングが使用されるようにする必要があります。

- 送信元および宛先カラム内の IP アドレスを表示するには、[表示（View）] > [ネットワークホストオブジェクトの表示（Show Network Host Objects）] の選択を解除します。

ビューの色ルールの設定

色ルールを使用して、イベントテーブル内に表示されるイベントをイベントの重大度に基づいて色分けできます。色分けを使用すると、最も必要なイベントの識別が簡単にできます。

色ルールを編集して、選択的に色ルールをイネーブルおよびディセーブルにできます。これにより、色ルールを削除せずにオンおよびオフにできます。

ヒント 色ルールは、定義済みビューとカスタム ビューの両方に対して設定できます。ただし、色ルールはビュー間で共有できません。すべての色ルールは、ビューに一意です。同じルールを複数のビューに適用する場合は、各ビューでルールを再作成する必要があります。

色ルールを定義し、イネーブルにするには、次の手順を実行します。

ステップ 1 色ルールを定義するビューを開きます（ビューを開く （3519 ページ）を参照）。

ステップ 2 [ビューの設定（View Settings）] ペインで [色ルール（Color Rules）] タブをクリックします（[Event Monitoring] ウィンドウ （3489 ページ）を参照）。

ステップ 3 次のいずれかを実行します。

- 新規ルールを追加するには、[追加（Add）] ボタンをクリックします。[Add Color Rule] ダイアログボックスで次のとおりルールを設定します。
  - [有効化（Enable）] を選択してルールをアクティブにします。
  - [シビラティ（重大度）（Severity）] リストから、ルールを適用するシビラティ（重大度）レベルを選択します。
  - [フォアグラウンド（Foreground）]（テキストの色）、[バックグラウンド（Background）]、および [フォントタイプ（Font Type）]（太字またはイタリック体）コントロールを使用して、テーブル内でのシビラティ（重大度）の表示方法を定義します。[Preview Text] エリアには、ルールがどのように表示されるかが示されます。
- ルールを編集するには、ルールを選択し、[編集（Edit）] ボタンをクリックします。

- ルールを削除するには、ルールを選択し、[削除（Delete）] ボタンをクリックします。

カスタム ビューの作成

カスタム ビューは、ビュー設定でフィルタを定義するビューです。カスタム ビューを使用すると、モニタリングおよび分析のためにエリアを正確に特定するようにフィルタ ルールを設定できます。カスタム ビューはプライベートなものであり、ユーザ間で共有できません。

カスタム ビューの作成には、最初からビューを作成、または既存のビューから作成の2つの方法があります。

- 定義済みカラム フィルタのないカスタム ビューを作成するには、次のいずれかを実行します。
  - メニューバーで [ファイル（File）] > [新規ビュー（New View）] を選択する。
  - ビューのリストの上の [新規（New）] ボタンをクリックする。

次に、ビューの名前および任意でビューの説明を入力して、[OK] をクリックします。ビューは、ビューのリストの [My Views] フォルダに追加されます。

- 既存のビューに基づいてカスタム ビューを作成するには、次のいずれかを実行します。
  - もとにする目的のビューを開いて、イベントテーブルツールバーの [保存（Save）] ボタンの下矢印をクリックして、[名前を付けて保存（Save As）] を選択、またはメニューバーで [ファイル（File）] > [名前を付けて保存（Save As）] を選択します。
  - ビューのリストでもとにする目的のビューを右クリックして、[名前を付けて保存（Save As）] を選択します。

次に、ビューの名前および任意でビューの説明を入力して、[OK] をクリックします。ビューは、ビューのリストの [My Views] フォルダに追加されます。新規ビューは、もとにするビューと同じフィルタを持ちます。

（注） ビュー名は、最大128文字で、英数字、スペース、ハイフン（-）、アンダースコア（_）、プラス記号（+）、ピリオド、およびアンド記号（&）を使用できます。説明には、最大1024 文字を使用できます。

新規ビューを作成したら、既存のビューと同じ方法でそのビューをカスタマイズできます。

- ビュー設定でフィルタを定義します。カラムベース フィルタの作成 （3528 ページ）を参照してください。
- ビュー設定で色ルールを定義します。ビューの色ルールの設定 （3522 ページ）を参照してください。

- イベントテーブルで表示するカラムを選択します。イベントテーブルのカラム （3494ページ）を参照してください。
- イベント テーブルの表示をカスタマイズします。イベント テーブルの表示のカスタマイズ （3520 ページ） を参照してください。

関連項目

- ビューとフィルタ （3475 ページ）
- イベント テーブル ツールバー （3491 ページ）
- カスタム ビューの名前または説明の編集 （3524 ページ）
- カスタム ビューの削除 （3525 ページ）

カスタム ビューの名前または説明の編集

カスタムビューの名前、またはカスタムビューの説明を変更するには、次のいずれかの手順を実行します。

- ビューリストでカスタムビューを選択して、リストの上にある [編集（Edit）] ボタンをクリックします。
- ビューリストでカスタムビューを右クリックして、[編集（Edit）] を選択します。

次に、カスタムビューの名前または説明に必要な変更を加えて、[OK] をクリックします。

（注） ビュー名は、最大128文字で、英数字、スペース、ハイフン（-）、アンダースコア（_）、プラス記号（+）、ピリオド、およびアンド記号（&）を使用できます。説明には、最大1024 文字を使用できます。

定義済みのビューの名前または説明は変更できません。

リアルタイム ビューと履歴ビュー間の切り替え

リアルタイムまたは履歴期間のいずれかを使用する任意のビューに対してイベントテーブルを更新できます。リアルタイムビューには、受信した状態のままのイベントが表示されます。一方、履歴ビューには、イベントテーブルツールバーの [スタート（Start）] ボタンをクリックするまで更新されないイベントのスタティックリストが表示されます。

開いているビューで、リアルタイムと履歴期間の間を切り替えるには、次の手順を実行します。

- リアルタイムでイベントを表示するには、[表示（View）] > [モード（Mode）] > [リアルタイム（Real Time）] を選択、またはイベントテーブルツールバーの [時間セレクタ（Time Selector）] コントロールをクリックして、[リアルタイム（Real Time）] を選択します。

ツールバーのコントロールの場所を見つけるには、イベントテーブル ツールバー （3491 ページ）を参照します。

- 履歴期間のイベントを表示するには、[表示（View）]>[モード（Mode）] メニューから、またはイベントテーブルツールバーの [時間セレクタ（Time Selector）] コントロールから、目的のタイムフレームを選択します。[Real Time] 以外のオプションすべてが履歴ビューです。詳細については、イベントの時間範囲の選択 （3526ページ）を参照してください。

ビューの保存

ビューの設定を編集した場合は、変更が持続するように設定を保存する必要があります。ビューを保存すると、フィルタ（カスタム ビューの場合のみ）、選択したカラム、カラム幅、およびソート順序などのテーブル プリファレンス、時間範囲、および色ルールの変更が保存されます。定義済みのビューのフィルタを変更する場合は、[Save As] を使用して新規カスタム ビューを作成する必要があります。

- ビューの変更を保存するには、Event Viewer で次のいずれかを実行します。
  - メニューバーから **[ファイル（File）] > [保存（Save）]** を選択する。
  - イベントテーブルツールバーで [保存（Save）] ボタンをクリックする。

変更の保存を確認するように求められます。

- 新規カスタム ビューとして変更を保存するには、次のいずれかを実行して [Save View As] ダイアログボックスを開きます。
  - メニューバーから **[ファイル（File）] > [名前を付けて保存（Save As）]** を選択する。
  - イベントテーブルツールバーの [保存（Save）] ボタンの下矢印をクリックして、[名前を付けて保存（Save As）] を選択する。
  - ビューのリストでビューを右クリックして、[名前を付けて保存（Save As）] を選択する。

次に、ビューの名前および任意でビューの説明を入力して、[OK] をクリックします。ビューは、ビューのリストの [My Views] フォルダに追加されます。

（注） ビュー名は、最大 128 文字で、英数字、スペース、ハイフン（-）、アンダースコア（_）、プラス記号（+）、ピリオド、およびアンド記号（&）を使用できます。説明には、最大 1024 文字を使用できます。

カスタム ビューの削除

カスタム ビューは削除できますが、定義済みのビューは削除できません。カスタム ビューを削除するには、次のいずれかを実行します。

- ビューのリストでカスタムビューを選択して、リストの上にある [削除（Delete）]（ゴミ箱）ボタンをクリックします。
- ビューのリストでカスタムビューを右クリックして、[削除（Delete）] を選択します。

削除の確認が求められます。

イベントのフィルタリングおよびクエリー

イベントテーブルに表示されるイベントのフィルタリングには多くのオプションがあります。適切な時間範囲を選択する、特定のカラムの要素をフィルタリングする、またはテキスト文字列を検索することによってもイベントのリストを絞り込めます。

ここでは、次の内容について説明します。

- イベントの時間範囲の選択 （3526 ページ）
- フィルタリングと時間スライダの使用方法 （3527 ページ）
- イベント テーブルのリフレッシュ （3528 ページ）
- カラムベース フィルタの作成 （3528 ページ）
- 特定のイベントの値に基づいたフィルタリング （3531 ページ）
- テキスト文字列に対するフィルタリング （3532 ページ）
- フィルタのクリア （3533 ページ）

イベントの時間範囲の選択

イベントテーブルツールバーの [時間セレクタ（Time Selector）] コントロール、またはそれに相当する [表示（View）] > [モード（Mode）] コマンドを使用して、イベントを表示するための時間範囲を選択します。イベントテーブルには、選択した時間範囲内に発生したイベントだけが一覧表示されます。ツールバーの [Time Selector] コントロールの場所を見つけるには、イベント テーブル ツールバー （3491 ページ）を参照します。

ヒント 履歴ビューの場合、時間はワークステーションに設定された時間ではなく、サーバの時間に基づいています。

時間範囲を変更すると、選択した範囲内のイベントを表示するようにイベント テーブルがリロードされます。履歴ビューの場合、[開始（Start）] をクリックして、またはイベント テーブルのリフレッシュ （3528ページ）で説明したその他のアクションを実行して、イベントリストをリフレッシュできます。

時間範囲のオプションは、次のとおりです。

- 現在時刻から過去にさかのぼってイベントを表示するには、次のいずれかの期間を選択します。[過去 10 分間（last 10 minutes）]、[過去 1 時間（last 1 hour）]、[過去 12 時間（last 12 hours）]、[過去 1 日間（last 1 day）]、または [過去 1 週間（last 1 week）] です。
- 今日または昨日のイベントを表示するには、必要に応じて [今日（today）] または [昨日（yesterday）] を選択します。
- 特定の日のイベントを表示するには、[次の日（is on）] を選択し、表示されたカレンダーからその日付を選択します。
- 特定の日付と時刻の範囲のイベントを表示するには、[次の期間（is between）] を選択し、表示されたカレンダーから範囲の最初および最後の日付と時刻を選択します。
- リアルタイム イベントを表示するには、[Real Time] を選択します。

フィルタリングと時間スライダの使用方法

時間スライダの垂直スライダ コントロールを使用すると、イベント テーブルに表示されるイベントの開始時刻を変更できます。これは、イベントの場所を特定し、そのおおよその発生時刻を確認するときに特に便利です。

時間スライダの操作の詳細については、時間スライダ （3504 ページ）を参照してください。

時間スライダを使用してフィルタリングを使いやすくするには、次の手順を実行します。

ステップ 1 履歴ビューを開く、またはツールバーの Time Selector を使用する、または **[表示（View）]>[モード（Mode）]** コマンドを使用して、[過去10分間（Last 10 Minutes）] など適切な時間範囲を選択します。詳細については、イベントの時間範囲の選択 （3526 ページ）を参照してください。

ステップ 2 調査するイベントのおおよその時刻に垂直スライダを移動します。

イベント テーブルがリロードされて、垂直スライダで指定した時刻とそれ以前に発生したイベントが表示されます。この時間範囲は時間スライダで共有され、選択した時間の長さは Time Selector で選択した時間の長さに基づきます（たとえば、[過去10分間（Last 10 Minute）] ビューの場合は 10 分間。または、[の間にある（is between）] ビューで選択した時間と同じ長さ）。時間範囲は [Time Selector] コントロールに、たとえば次のように示されます。

ステップ 3 これで、イベントの場所を特定するために、次のいずれかを実行できます。

- カスタム カラム フィルタを適用します。カラムベース フィルタの作成 （3528 ページ）を参照してください。
- テキスト文字列を検索するには、クイック フィルタを使用します。テキスト文字列に対するフィルタリング （3532 ページ）を参照してください。
- イベント テーブルをスクロールするか、またはイベント テーブルのページを切り替えます。
- 時間スライダのページ コントロールを使用して、時間範囲を前方または後方にリセットします。詳細については、時間スライダ （3504 ページ）を参照してください。

（注） 時間スライダでページを切り替えるときに前方または後方に移動する距離は、設定されているモード（時間範囲）またはイベント テーブルが保持できるイベントの数によって決まります。垂直スライダの位置は、イベント テーブルにロードされた最新のイベントを示します。

イベント テーブルのリフレッシュ

「過去 10 分」など履歴モードを使用している場合、表示される最新のイベントは時間範囲を選択した時刻またはビューを開いた時刻に対応しています。同様に、リアルタイム モードを使用していて [Stop] をクリックした場合、イベント テーブルにはイベント ストリームを停止したあとに到着したイベントは含まれません。

イベントテーブルに一覧表示されたイベントをリフレッシュして、現在の選択された時間範囲のイベントにするには、次のいずれかを実行します。

- ツールバーで [開始（Start）] をクリックするか、**[表示（View）] > [開始（Start）]** を選択します。イベントテーブルは、現在の選択された時間範囲に基づいてリフレッシュされます。リアルタイム ビューの場合は、イベント ストリームが再開します。
- ツールバーの日時セレクタを使用するか、**[表示（View）] > [モード（Mode）]** コマンドを使用して、異なる時間範囲を選択します。
- イベント テーブルの下にある時間スライダの垂直スライダまたは改ページ コントロールを使用して、異なる時間のスライスを選択します。これらのコントロールの使用の詳細については、時間スライダ （3504 ページ）を参照してください。

カラムベース フィルタの作成

Event Viewer で特定のカラムの内容に基づいてイベント テーブルをフィルタリングできます。カラム フィルタは、ビュー設定に含まれているフィルタのタイプで、ビューの基本的内容を定義します。カラムフィルタを適用するたびに、新しく選択されたフィルタが含まれるようにビューに対するビュー設定が更新されます。新規フィルタをビュー定義の一部として持続させるには、ビューを閉じる前に保存する必要があります。

カラム フィルタを定義するには、次のとおり多くの方法があります。

- [ビュー設定（View Settings）] ペインで [追加（Add）] ボタンをクリックします。まず、フィルタのもとにするカラムの選択を求められます。[OK] をクリックすると、フィルタの作成を求められます。
- [ビュー設定（View Settings）] ペインでフィルタを選択して、[編集（Edit）] ボタンをクリックしてフィルタを変更します。
- イベント テーブルでカラムの見出しの下矢印ボタンをクリックして、ドロップダウン リストから次のいずれかを選択します。
  - 特定のエントリ。ドロップダウン リストには、テーブルに一覧表示されたイベントに現在表示されているすべての値が含まれています。

- [(All)]。このカラムからフィルタを削除するには、[(All)] を選択します。イベントテーブルは、他のフィルタ基準を満たすイベントを表示するように更新されます。
- [(Custom)]。複数の値もしくは負の値を持つ場合がある、または現在のイベント テーブルのカラムに現在は含まれていないデータに基づく場合があるフィルタを作成するには、[(Custom)] を選択します。[(Custom)] を選択することは、[View Settings] ペインで直接フィルタを作成することと基本的に同じです。

- イベントテーブルで値を右クリックして、[この値でフィルタリング（Filter This Value）] を選択します。このアクションは、ドロップダウン リストからカラムに対して値を選択することと同じ結果になります。

他に、[この値以外でフィルタリング（Filter Not This Value）] を選択して、値を除外するフィルタを作成できます。

- イベントテーブルで値を右クリックして、[イベントからフィルタを作成（Create Filter from Event）] を選択します。含める特定のカラムを選択するように求められます。右クリックしたカラムは当初は選択されていますが、選択を解除できます。

次の手順では、カラムのドロップダウンリストから単純に値を選択しない、カスタム カラム ベース フィルタを構築する方法を説明します。

ヒント

- カラム フィルタは累積的です。ビューのイベントテーブルにイベントが表示されるには、そのイベントがすべてのカラムフィルタ基準を満たす必要があります。論理和を取ったカラムフィルタのセットは作成できません。
- カラムによっては、ネットワーク/ホストまたはサービス ポリシー オブジェクトを選択してフィルタ基準を定義できます。ポリシーオブジェクトを選択すると、フィルタを簡素化できます。ただし、フィルタでポリシーオブジェクトが選択できるようにするには、オブジェクトがデータベースにコミットされている必要があります。フィルタリング目的で新規オブジェクトを作成する場合は、Event Viewer でフィルタ作成を試みる前に、変更を Configuration Manager に必ず送信します（また、Workflow モードをアプルーバで使用している場合は、変更を承認します）。

ポリシーオブジェクトの使用中は、デバイスレベルのオーバーライドがオブジェクトに対して定義されているかどうかがフィルタリングによって認識されます。たとえば、10.10.10.10 を含むネットワーク/ホスト オブジェクトを使用し、デバイス A がアドレスを 10.10.10.12 に変更するオーバーライドを保持している場合は、デバイス A からのイベントはイベントが 10.10.10.12 と一致する場合にだけリストに表示されます。オーバーライドを保持しないデバイスの場合は、イベントは 10.10.10.10 と一致する必要があります。さらに、デバイス A が 10.10.10.10 と一致するイベントを保持している場合は、イベントがデバイスレベルのオーバーライドと一致しないため、イベントは一覧表示されません。つまり、ポリシーオブジェクトを使用するとデバイスごとに異なる結果となるため、ポリシー定義により厳密に一致することになります。

組織がユーザ アクセスの制御に ACS を使用している場合は、ネットワーク/ホスト、ネットワーク/ホスト -IPv6、およびサービス オブジェクトをフィルタで使用するために適切なオブジェクトの表示権限を持っている必要があります。

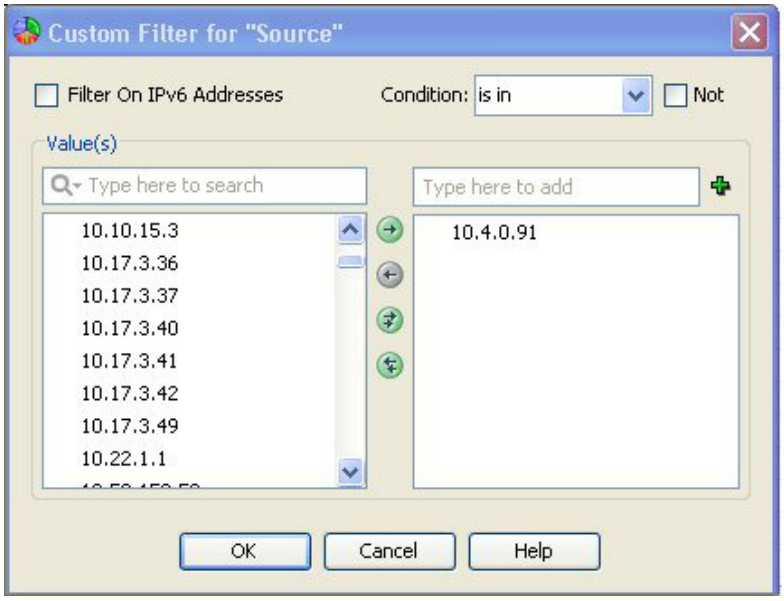
- すべてではありませんが、ほとんどのカラムの内容に対してフィルタリングできます。カラムに下矢印がない場合は、そのカラムに対してはフィルタリングできません。たとえば、[Description]、[Event Name]、[Generation Time]、または [Receive Time] に対してはフィルタリングできません。
- フィルタアイコン（じょうご）はフィルタリングされたカラムの見出しに表示されます。
- 使用可能なカラムの詳細については、イベントテーブルのカラム （3494 ページ）を参照してください。

ステップ 1 次のいずれかを実行します。

- [ビュー設定（View Settings）] ペインで [追加（Add）] ボタンをクリックします。[Add Custom Filter to a Column] ダイアログボックスが開きます。フィルタのもとにするカラムを選択して、[OK] をクリックします。
- [ビュー設定（View Settings）] ペインで、変更するフィルタを選択して [編集（Edit）] ボタンをクリックします。
- ドロップダウンリストからカラムに対して [（カスタム）（(Custom)）] を選択します。
- 目的のカラムに含まれる任意のセルを右クリックして、[カスタムフィルタ（Custom Filter）] を選択します。

選択したカラムに対して [Custom Filter] ダイアログボックスが開きます。

ステップ 2 [Custom Filter] ダイアログボックスで目的の値を選択します。次の図に、[Source] カラムに対するこのダイアログボックスの一般的な例を示します。



次に、[Custom Filter] ダイアログボックスに表示される可能性のあるコントロールについて説明します。すべてのカラムに対してすべてのコントロールが表示されるわけではありません。

- [使用可能な項目（Available Items）] と [選択された項目（Selected Items）] のリスト：ほとんどの場合、項目を選択するには、使用可能な値が含まれる左側のリストで項目を強調表示してから、右矢印をクリックして選択された値のリストに移動します。複数の値を選択できます。右側のリストはフィルタリングする値を定義します。

使用可能な値のカラムに一覧表示される項目は、イベントテーブルに一覧表示されたイベントに現在表示されている値によって決定されます。アドレスおよびサービスフィールドの場合は、ポリシーオブジェクトもリストに含まれます。使用可能な値がたくさんある場合は、リストの上にある編集ボックスに目的の値を入力して検索できます。入力するとリストがフィルタリングされます。Q の横にある下矢印をクリックして、一致する検索文字列の評価方法を変更します。

次の方法を使用して、値の選択または選択解除をすることもできます。

- 選択された値のリストの上にある編集ボックスに項目を入力して、+ ボタンをクリックします。この方法は、使用可能な値が多数ある場合、または現在のイベントリストにない値に対してフィルタリングする場合に役立ちます。
- 他方のリストに移動する、一方のリストの項目をダブルクリックします。
- 選択に関係なく、すべての項目を移動するには、二重矢印のボタンをクリックします。

（注） 限られた場合ですが、[Custom Filter] ダイアログボックスに単一のリストが含まれる場合があります。たとえば、[Event Type ID] および [Device] カラムに対する [Custom Filter] ダイアログボックスには単一のセレクタが含まれます。この場合、項目の隣にあるチェックボックスを使用して選択します。フォルダを選択すると、フォルダ内のすべての項目が選択されます。

- [IPv6アドレスに対するフィルタリング（Filter on IPv6 Addresses）]：アドレスを含むカラムの場合、このオプションを使用して、使用可能な値のカラムの IPv4 アドレスと IPv6 アドレスおよびネットワーク/ホストオブジェクトを切り替えて一覧表示します。単一のビュー内では、IPv4 アドレスまたは IPv6 アドレスのいずれかに対してフィルタリングできますが、両方に対してはできません。
- [条件（Condition）]、[次ではない（Not）]：選択された項目に適用する条件を定義します。通常は、[次に含まれる（is in）] です。

ネガティブ条件を作成して、選択された値で定義されるイベントをイベントテーブルに含めないようにするには、[Not] オプションを選択します。

ステップ 3 [OK] をクリック

ビュー設定は、新規フィルタが含まれるように更新されます。また、イベントテーブルは、すべてのフィルタを満たすイベントだけを表示するように更新されます。

特定のイベントの値に基づいたフィルタリング

イベント内に含まれる情報、またはイベント内の単一のセルに基づいて新規にフィルタを作成できます。そのためには、右クリックしてフィルタ コマンドを選択します。フィルタ コマンドを使用してフィルタリングする場合、カラム フィルタがビュー設定に追加されます。次を実行できます。

- 選択したイベントの複数の値に基づいてフィルタを作成するには、[イベントからフィルタを作成（Create Filter from Event）] を選択し、ダイアログボックスからフィルタリングする値を選択します。ダイアログボックスには、テーブルに表示されたカラムだけが一覧表示されます。現在の値はカッコで囲まれて表示されます。カラムの説明については、イベント テーブルのカラム （3494 ページ）を参照してください。
- セルの値だけに対してフィルタリングするには、セルを右クリックして、[この値でフィルタリング（Filter This Value）] を選択します。
- セルの値だけに対してフィルタリングするには、セルを右クリックして、[この値以外でフィルタリング（Filter Not this Value）] を選択します。すべての空のセルを含む、このカラムの選択された値を含まないすべてのイベントがテーブルに表示されます。
- 送信元、送信元サービス、宛先、および宛先サービスに基づいて、選択したイベントのフローに対してフィルタリングするには、[このフローをフィルタリング（Filter This Flow）] を選択します。

テキスト文字列に対するフィルタリング

イベント内のテキスト文字列を検索するには、クイック フィルタを使用します。検索キーワードを入力すると、イベントテーブルから一致しないイベントが自動的に除外されます。すべてのカラムを検索できます（デフォルト）。または特定のカラムを選択して検索できます。

次の図に、イベント テーブル ツールバーの右側にあるクイック フィルタを示します（イベント テーブル ツールバー （3491 ページ）を参照）。

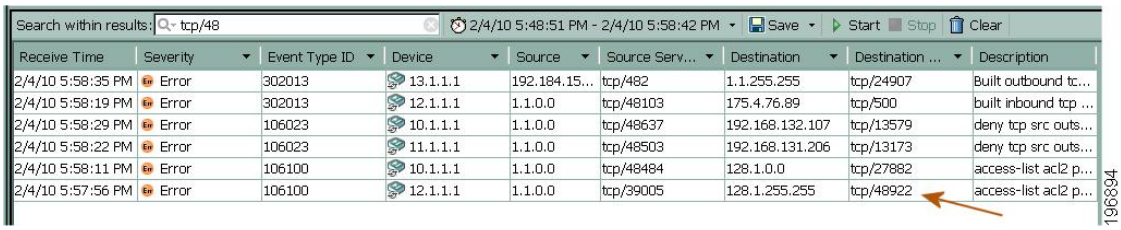
検索を実行するには、単に検索文字列を入力します。文字列の評価方法を変更するには、編集ボックスの左側の [Q]（虫眼鏡）の隣にある下矢印をクリックします。次のコントロールを使用して、検索スコープを制限できます。

- カラム名：特定のカラムを選択して、そのカラム内だけを検索します。テーブルに現在表示されているすべてのカラムがリストに含まれています。デフォルトでは、すべてのカラムを検索します。
- 大文字と小文字の区別：一致の選択時に大文字を考慮するかどうかを制御するには、[大文字小文字の区別あり（Case sensitive）] または [大文字小文字の区別なし（Case insensitive）] を選択します。デフォルトでは、大文字と小文字の区別なしです。
- ワイルドカードの使用：次の文字をワイルドカードとして評価するには、[ワイルドカードを使用（Use Wild Cards）] を選択します。
  - *（アスタリスク）：0 文字以上と一致します。
  - ?（疑問符）：1 文字と一致します。
- 一致方法：セル内で検索文字列が存在する場所を指定するために、次から 1 つを選択します。

- [Match from start]：文字列は、セルの先頭にある必要があります。
- [Match exactly]：セルには、すべての検索文字列、かつ検索文字列だけが含まれている必要があります。
- [Match anywhere]：文字列は、セル内の任意の場所に存在できます。

検索文字列を削除するには、単にクイック フィルタ編集ボックスから検索文字列を削除します。

たとえば、tcp/48 で始まるポートに関連するイベントを検索するには、**tcp/48** をクイックフィルタに入力します。次の図で、6 つを除いてすべてのイベントがフィルタリングによってテーブルから除外されたことに注意してください。この例では、検索文字列は、最初の 5 つのイベントでは [Source Service] カラムで見つかりましたが、6 番めのイベントでは [Destination Service] カラムで見つかりました。宛先サービスだけが重要なことが事前にわかっている場合は、クイック フィルタ ドロップダウン リストから [接続先サービス（Destination Service）] を選択すると、テーブルに最後のイベントだけが表示されます。



フィルタのクリア

イベントテーブルにフィルタを適用すると、一致しないイベントは表示されません。一致しないイベントを表示する必要がある場合があります。この場合、異なるフィルタ（またはフィルタなし）を適用する異なるビューを開くか、現在のビューからフィルタをクリアします。

フィルタをクリアすると、フィルタ定義がビュー設定から削除されますが、変更は [保存（Save）] をクリックするまで永続化されません。したがって、ビュー設定を再定義せずに、フィルタを一時的に削除できます。

フィルタを一度に 1 つずつ、またはすべてのフィルタをクリアできます。

- 単一のフィルタをクリアするには、次のいずれかを実行します。
  - [表示設定（View Settings）] ペインでフィルタを選択して、[削除（Delete）] をクリックします。
  - フィルタリングされた列のドロップダウンリストから [（すべて）（(All)）] を選択します。
  - フィルタリングされた列を右クリックして、[このフィルタをクリア（Clear This Filter）] を選択します。
- すべてのフィルタをクリアするには、イベントテーブル内で右クリックして、[すべてのフィルタをクリア（Clear All Filters）] を選択します。

特定のイベントに対する操作の実行

イベントテーブル内の単一のイベントに対して、次のような操作をさまざまな方法で実行できます。

- **右クリック**：イベントテーブルの単一のイベントを右クリックすると、そのイベントで使用できるコマンドを含むコンテキストメニューが開きます。右クリック メニューから実行可能な操作の詳細については、次の項を参照してください。
  - イベント コンテキスト（右クリック）メニュー （3534 ページ）
  - 単一のイベントの詳細の参照 （3539 ページ）
  - イベント レコードのコピー （3540 ページ）
  - ビューの保存 （3525 ページ）
  - 特定のイベントの値に基づいたフィルタリング （3531 ページ）

（注） イベントビューアで有効な IPv4 アドレスの上にマウスを置くと、その IP アドレスの IP インテリジェンスツールを起動できます。IP インテリジェンスツールは、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS 情報など、IPv4 アドレスに関するさまざまな情報を提供します。IP インテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence） （3723 ページ）を参照してください。

- **イベントの選択**：イベントテーブルの単一のイベントをクリックすると、そのイベントが強調表示され、[イベントの詳細（Event Details）] ペインにその特定のイベントの詳細が表示されます。別のイベントを選択するには **Ctrl** キーを押した状態で選択し、ある範囲のイベントを選択するには **Shift** キーを押した状態で選択します。
- **イベントのダブルクリック**：イベントテーブルの単一のイベントをダブルクリックすると、[イベントの詳細（Event Details）] ダイアログボックスが開き、読みやすい形式でイベント情報が表示されます。[Event Details] ダイアログボックスでは、表示された詳細を印刷できます。または、詳細の一部またはすべてを他のプログラムに貼り付けるためにクリップボードにコピーできます。[Next] および [Previous] ボタンを使用してイベント テーブルに一覧表示されたイベント全体をスクロールできます。属性の意味の詳細については、イベント テーブルのカラム （3494 ページ）を参照してください。

または、イベントを右クリックし、[すべての詳細を表示（Show All Details）] を選択して [イベントの詳細（Event Details）] ダイアログボックスを開くこともできます。

イベント コンテキスト（右クリック）メニュー

イベント テーブルのイベントを右クリックすると、コンテキスト メニューが表示され、選択したイベントに使用できるコマンドが提供されます。使用可能なコマンドの特定のリストは、右クリックしたイベントのタイプおよび特定のセルによって異なります。次の表に、使用可能なコマンドすべてについて説明します。

（注） 以下にリストされている右クリックオプションに加えて、イベントビューアで有効なIPv4アドレスの上にマウスを置くと、そのIPアドレスのIPインテリジェンスツールも起動できます。IP インテリジェンスツールは、完全修飾ドメイン名（FQDN）、地理的位置情報、WHOIS情報など、IPv4アドレスに関するさまざまな情報を提供します。IPインテリジェンスツールの詳細については、IPインテリジェンス（IP Intelligence）（3723ページ）を参照してください。

表 *977*：イベント コンテキスト メニュー

コマンド	説明
Clear This Filter	このカラムに定義されたフィルタを削除します。このコマンドが使用できるのは、フィルタリングされたカラムのセルを右クリックした場合だけです。 フィルタはビュー設定から削除されます。変更を持続させるには、ビューを保存する必要があります。
Clear All Filters	ビュー設定からすべてのフィルタを削除します。このコマンドが使用できるのは、少なくとも 1 つのカラム フィルタがある場合だけです。 変更を持続させるには、ビューを保存する必要があります。
Filter This Value Filter Not This Value	右クリックしたセルの値に基づいてカラムフィルタを作成します。値に基づいて、ポジティブまたはネガティブ フィルタを作成できます。 ビュー設定は新規フィルタで更新されて、このカラムの既存のフィルタがあればそのフィルタと置き換えられます。変更を持続させるには、ビューを保存する必要があります。
Create Filter from Event	選択したイベントの値に基づいて一連のカラムフィルタを作成します。含める特定のカラムを選択するように求められます。右クリックしたカラムは当初は選択されていますが、選択を解除できます。 ビュー設定は新規フィルタで更新されて、選択したカラムの既存のカラムフィルタはすべて置き換えられます。変更を確定させるには、ビューを保存する必要があります。
カスタム フィルタ（Custom Filter）	カラムベースフィルタの作成（3528ページ）で説明するとおりに、カスタム カラム フィルタを作成します。 ビュー設定は新規フィルタで更新されて、選択したカラムの既存のフィルタはすべて置き換えられます。変更を確定させるには、ビューを保存する必要があります。

コマンド	説明
Filter This Flow	特定のトラフィック フローに関連するイベントを示すカラムベース フィルタのセットを作成します。フィルタリングされるカラムは、送信元および送信元サービス、ならびに宛先および宛先サービスです。 ビュー設定は新規フィルタで更新されて、選択したカラムの既存のフィルタはすべて置き換えられます。変更を確定させるには、ビューを保存する必要があります。
Show IPLogs	外部パケットアナライザ ツールを使用して、IPS アラート イベントに対して IP ログを開きます。パケット アナライザがインストールされていて、*.pcap ファイル拡張子に関連付けられている必要があります。
Show All Details	イベントに対する [Event Details] ダイアログボックスが開き、読みやすい形式ですべてのイベント情報が表示されます。詳細を印刷またはクリップボードにコピーすることもできます。 この詳細は、イベント テーブルの下の [Event Details] ペインに表示される詳細と同じです。
Copy commands	次のコマンドを使用して、イベントデータをクリップボードにコピーできます。その後、データを使用するためにスプレッドシートまたは他のプログラムに貼り付けられます。詳細については、イベント レコードのコピー（3540 ページ）を参照してください。 • [セルのコピー（Copy Cell）]：右クリックしたセルの内容をクリップボードにコピーします。 • [選択されたイベントをコピー（Copy Selected Events）]：すべての選択された（強調表示された）イベントの内容をクリップボードにコピーします。 • [すべてのイベントをコピー（Copy All Events）]：すべての一覧表示されたイベントの内容をクリップボードにコピーします。 このコマンドは、イベントテーブルを管理可能な数のイベントにフィルタリングした場合にだけ役立ちます。
Save Selected Events as HTML Save All Events as HTML Save Selected Events as CSV Save All Events as CSV	イベントテーブルに一覧表示されたすべてのイベント、またはすべての選択された（強調表示された）イベントをワークステーションのHTMLまたは Comma-Separated Values（CSV; カンマ区切り値）ファイルに保存します。エクスポートファイルのフォルダ選択およびファイル名の入力を求められます。 詳細については、ファイルへのイベントの保存 （3540ページ）を参照してください。

コマンド	説明
Go To Policy	Configuration Manager のデバイスのポリシー設定でこのイベントを生成したポリシーを検索します。このコマンドは、[Event Name] セルに双眼鏡アイコンが表示されるイベントに対してだけ使用できます。詳細については、 Event Viewer からの Security Manager ポリシーの検索 （3541 ページ）を参照してください。
パケット キャプチャ	パケット キャプチャ ツールが開き、デバイス上でのパケット キャプチャに対する条件が定義できます。
Ping and TraceRoute	ping、TraceRoute、および NS ルックアップ ツールが開き、これらのアプリケーションをイベントの送信元デバイスで使用できます。詳細については、 ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析 （3713 ページ）を参照してください。

コマンド	説明

Tune Signature	選択したイベントに関連付けられたシグネチャを有効または無効にしたり、デバイスまたは共有ポリシーに割り当てられているシグネチャの基本リスクレーティングを変更したりできる [IPSシグネチャのクイック調整（IPS Signature Quick Tune）] ダイアログボックスを開きます。
	
	シグネチャを調整するには、チケットを作成するか、開く必要があります。詳細については、アクティビティ/チケットの操作 （185 ページ）を参照してください。
	
	シグネチャの基本リスクレーティング値。この値は、忠実度評価と重大度係数を掛け合わせたものを 100 で割る（忠実度評価 X 重大度係数 /100）ことによって計算されます。この値は読み取り専用です。直接変更できません。基本リスクレーティングを変更するには、重大度と忠実度の値を変更する必要があります。
	
	• 重大度：シグネチャによってレポートされる重大度レベル（[High]、[Medium]、[Low]、または [Informational]）。
	  • High = 100
	  • Medium = 75
	  • Low = 50
	  • Informational = 25
	
	• 忠実度：忠実度評価、または Signature Fidelity Rating（SFR; シグネチャの忠実度評価）は、ターゲットに関する具体的な情報がない場合のシグネチャの実行忠実度に関連付ける重みを示します。この評価には、0 ～ 100 の任意の数字を指定できます。100 は、シグニチャの信頼性が最も高いことを意味します。
	
	シグネチャを有効または無効にするか、基本リスクレーティングを変更した後、変更をデバイスに反映させるために、Configuration Manager を使用して設定をデバイスに再展開する必要があります。このような変更はリアルタイムのイベントにのみ影響し、過去のイベントには影響しません。設定の展開の詳細については、展開について （481 ページ）を参照してください。

IPS シグネチャ クイック チューン ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

選択したイベントに関連付けられたシグネチャを有効または無効にしたり、デバイスまたは共有ポリシーに割り当てられているシグネチャの基本リスクレーティングを変更したりするには、[IPSシグネチャのクイック調整（IPS Signature Quick Tune）] ダイアログボックスを使用します。

ナビゲーション パス

イベントビューアで、行（イベント）を右クリックし、[シグネチャの調整（Tune Signature）] をクリックします。詳細については、イベント コンテキスト（右クリック）メニュー （3534 ページ）を参照してください。

単一のイベントの詳細の参照

各イベントには、多くの別々のフィールドに特定の情報が多数含まれています。通常、これらのフィールドのサブセットはイベントテーブルに表示します。イベントの全詳細を表示する必要がある場合は、次のいずれかを使用します。

- [イベントの詳細（Event Details）] ペイン：イベントを選択して、イベントテーブルの下にある [イベントの詳細（Event Details）] ペインを開きます。このペインを開くには、[イベントの詳細（Event Details）] タイトル行の任意の場所をクリックするか、メニューから [表示（View）] > [イベントの詳細の表示（Show Event Details）] を選択します。[Event Details] ペインでは、情報がタブに整理されます。このペインの詳細については、[Event Details] ペイン （3505 ページ）を参照してください。
- [イベントの詳細（Event Details）] ダイアログボックス：このダイアログボックスを開くには、イベントをダブルクリックするか、イベントを右クリックして、[すべての詳細を表示（Show All Details）] を選択します。情報は、フラットなリストで表示され、[Event Details] ペインの [Details] タブに表示される情報が示されます。属性の意味の詳細については、イベント テーブルのカラム （3494 ページ）を参照してください。

[Event Details] ダイアログボックスには、次のコントロールが含まれています。

- [Print] ボタン：情報を印刷するには、このボタンをクリックします。プリンタを選択するプロンプトが表示されます。
- [コピー（Copy）] ボタン：このボタンの下矢印をクリックして [すべての行（All Rows）] または [選択した行（Selected Rows）] を選択します。情報がクリップボードにコピーされます。情報は別のアプリケーションに貼り付けられます。テーブルで少なくとも 1 行を選択した場合にだけ、[Selected Rows] コマンドが機能することに注意してください。
- [Next]、[Previous] ボタン：イベント テーブルに現在表示されているイベント全体をスクロールするには、このボタンをクリックします。[Next] で上に、[Previous] で下にテーブル内を移動します。

イベント レコードのコピー

単一のイベント、複数のイベント、すべてのイベント、さらに単一のセルの内容をクリップボードにコピーできます。その後、スプレッドシートや電子メール メッセージなどの別のアプリケーションに情報を貼り付けられます。

イベント テーブルで次の手順を実行できます。

- [選択したイベントのコピー（Copy selected events）]：1 つ以上の選択したイベントをコピーするには、イベントテーブル内で右クリックして、[選択したイベントをコピー（Copy Selected Events）] を選択します。いずれのイベントを右クリックするかは重要ではありません。テーブル内で選択された（強調表示された）イベントがコピーされます。

イベントをクリックして選択します。さらに別のイベントを選択するには **Ctrl** キーを押した状態で選択し、ある範囲のイベントを選択するには **Shift** キーを押した状態で選択します。

- **単一のセルの内容のコピー**：1 つのイベント内の単一のセルの内容をコピーするには、セルを右クリックして、[セルのコピー（Copy Cell）] を選択しますテーブル内で複数のイベントが選択されている場合は、セルの内容をコピーできません。
- **すべてのイベントのコピー**：イベント テーブルに表示されているすべてのイベントをコピーするには、テーブル内の任意の場所で右クリックして、[すべてのイベントのコピー（Copy All Events）] を選択します。

ファイルへのイベントの保存

イベントをクリップボードにコピーして別のアプリケーションに貼り付ける代わりに、イベントを HTML または Comma-Separated Values（CSV; カンマ区切り値）ファイルに直接保存できます。HTML ファイルは情報を表示する場合に便利です。一方で、CSV ファイルはスプレッドシート アプリケーションで開いて詳細分析およびレポート生成に使用できます。

イベント データを保存すると、フォルダの選択およびファイル名の入力を求められます。

イベント テーブルで次の手順を実行できます。

- **選択したイベントの保存**：1 つ以上の選択したイベントを保存するには、イベントテーブル内で右クリックして、[選択したイベントをHTMLとして保存（Save Selected Events as HTML）] または [選択したイベントをCSVとして保存（Save Selected Events as CSV）] のいずれかを選択します。いずれのイベントを右クリックするかは重要ではありません。テーブル内で選択された（強調表示された）イベントが保存されます。

イベントをクリックして選択します。さらに別のイベントを選択するには **Ctrl** キーを押した状態で選択し、ある範囲のイベントを選択するには **Shift** キーを押した状態で選択します。

- **すべてのイベントの保存**：イベントテーブルに表示されているすべてのイベントを保存するには、テーブル内の任意の場所で右クリックして、[選択したイベントをHTMLとして保存（Save Selected Events as HTML）] または [選択したイベントをCSVとして保存（Save Selected Events as CSV）] のいずれかを選択します。

Event Viewer からの Security Manager ポリシーの検索

Event Viewer では、イベントが IPS シグニチャ ポリシーまたは明示的なアクセス ルールに関連する特定のアクション（アクセスの拒否など）から生成されたものである場合、そのイベント自体から関連するシグニチャまたはアクセス ルールを迅速に特定できます。

ポリシー検索を実行する主な理由は、ポリシーが生成しているイベントに基づいてポリシーを調整することです。たとえば、アクセスルールにより、実際には許可すべきトラフィックがドロップされることがあります。イベントが表示中であるため、そのイベントを発生させているポリシーがあることがわかります。数回のクリックで、そのイベントから再設定する必要があるポリシーにたどり着くことができます。

次のタイプのイベントからポリシーを検索できます。

- ファイアウォール イベント：次の syslog メッセージのポリシーを検索できます。
  - 106023：IP パケットの拒否。
  - 106100：ACL による許可/拒否。
  - 302013：TCP の確立（TCP セッションの開始）。
  - 302015：UDP の確立（UDP セッションの開始）。
- IPS アラート イベント：有効なシグニチャ識別子およびサブシグニチャ識別子が設定されているすべての IPS イベント。

ヒントおよび注意事項

- IPv6 アドレスを含むイベントではファイアウォール ポリシーを検索できません。ただし、IPv6 アドレスの IPS ポリシーは検索できます。
- ポリシーが IP アドレスのみに基づいており、イベントを発生させたユーザ名に基づいていない場合、デバイスは Active Directory 内の IP アドレスを検索し、ユーザ名がその IP アドレスに関連付けられている場合、ユーザ名が syslog に追加されます。したがって、ポリシーにユーザ名が含まれていなくても、生成される syslog には含まれている可能性があります。ポリシーは宛先ユーザでは作成できないため、このフィールドはポリシーの検索時には使用されません。
- イベントが送信元 FQDN/宛先 FQDN に基づいて設定されたポリシーに対して生成された場合、生成される syslog には、デバイス障害のため FQDN が含まれません。こうした場合には、ポリシーの検索は機能しません。
- イベントがユーザ グループに基づいたポリシーに対して設定された場合には、syslog には、ユーザ グループではなくイベントを発生させた特定のユーザ名が含まれます。こうした場合には、ポリシーの検索は機能しません。
- syslog 106023 イベントおよび 106100 イベントからポリシー検索を正常に完了するには、ハッシュ コードが必要です。このようなハッシュ コードは、Security Manager を使用して設定を展開した場合にだけ使用できます。ポリシー検索が失敗した場合は、設定を（デバイスまたはファイルに）展開してから、ポリシー検索を再度試してみてください。

- フィルタをデバイスのポリシーテーブルに適用し、イベントを生成したルールまたはシグニチャが現在のビューからフィルタリングされている場合、Security Manager ではそれを強調表示できません。フィルタをクリアしてからやり直してください。
- アクセスルールの最後に配置された暗黙の **deny any** など、イベントが暗黙のルールによって生成された場合、Security Manager ではそのルールを強調表示できません。アクセス リストの最後に明示的な deny any ルールを作成するようにすると効果的です。
- ターゲットポリシーは、デバイスが共有ポリシーを使用している場合も含め、常にデバイス ビューにあります。必要に応じてデバイス ビューを開いてポリシーを強調表示します。
- IPS シグニチャの場合、そのシグニチャがデフォルト シグニチャである場合には編集できないことがあります。
- アクセスルールの場合、選択したルールがイベントの最適な一致となります。ルールに重複する部分があったり、ルールが冗長であったりすると、複数のルールが同じイベントを生成することがあります。このような場合、選択したルールを編集しても、後続のルールで同じアクションが実行される可能性があるため、イベントが完全には削除されないことがあります。アクセスルール ツールを使用して、重複するルールを分析し、結合します。
- アクセスルールの場合、セッション確立中に複数のルールがパケットを許可することがありますが、最初のルールだけが強調表示されます。
- 組織がアクセスの制御に ACS を使用している場合、ポリシー検索を実行するためには、デバイスに対するデバイスの表示権限、およびファイアウォールまたは IPS ポリシーに対する表示権限も持っている必要があります。ユーザがすべての権限を持っていない場合は、一致ルールの検索を試みたときに「Unable to Find Matching Rule」エラーが発生します。

ステップ 1 Event Viewer でイベントを右クリックし、[ポリシーに移動（Go To Policy）] を選択します。

ヒント テーブルで [Event Name] セルを確認することにより、イベントからポリシーを検索できるかどうかを識別できます。イベント名の前に双眼鏡アイコンがある場合は、ポリシーを検索できます。また、[Go To Policy] コマンドがグレーになっている場合、そのタイプのイベントではポリシーを検索できません。

ステップ 2 Security Manager は、デバイスの関連するアクセス ルールまたは IPS シグニチャを検索し、ポリシー テーブルで該当する項目を強調表示します。ここから、表示または変更するポリシーを編集できます。詳細な手順については、アクセス ルールの設定 （920 ページ）およびシグニチャの設定 （2169 ページ）を参照してください。

変更内容は、更新した設定を送信し、展開するまで有効になりません。

Looking Up Events for a Cisco Security Manager Policy

特定のファイアウォール アクセス ルールまたは IPS シグネチャに関連するイベントをイベントビューアで検索できます。ヘルスとパフォーマンスのモニタで、特定のデバイスまたはサイト間トンネルに関連するイベントを検索することもできます。

イベントビューアがイベントを受信すると、イベントは解析され、「セッション化」されて、イベントバッファに書き込まれてから、データベースに書き込まれます。セッション化には 2 つの形式があります。セッション指向プロトコル（TCP など）では、セッションには初期ハンドシェイクから接続のティアダウンまでが含まれます。セッションレス プロトコル（UDP など）では、セッションの開始時刻と終了時刻は、制限された時間内で追跡される最初と最後のパケットに基づきます。時間外のパケットは、他のセッションの一部と見なされます。

新しく受信したデータと完全に処理されたデータには違いがあるため、リアルタイムイベントまたは過去イベントのいずれも検索できます。

- [リアルタイム（Real-time）]：イベントをキャッシュ内に最大 2 分間保持するためセッション化には時間がかかります。そのため、リアルタイム イベント クエリーを使用して解析直後にイベントを表示し、受信した最新データへのアクセスを可能にします。
- 履歴（Historical）]：過去のイベントのレポートは、リアルタイムモニタリングで可能な期間よりも長期にわたる傾向を識別するのに役立ちます。過去のイベントの場合、[Result Format] は [All Matching Events] オプションであり、[Filter By Time] 値は過去 10 分に設定されます。

次の項では、イベント検索についてより詳細に説明します。

- アクセスルールのイベントの表示　（3543 ページ）
- IPS シグニチャのイベントの表示　（3545 ページ）
- HPM デバイスとサイト間 VPN のイベントの表示　（3546 ページ）

アクセスルールのイベントの表示

Security Manager の [ファイアウォール（Firewall）] > [アクセスルール（Access Rules）] ポリシーから、アクセスルールを選択し、イベントビューアの関連するイベント情報を表示できます。ルールに一致するリアルタイムまたは過去のイベントを表示できます。ASA（ASA-SM を含む）および FWSM デバイスのイベントを表示できます。

ファイアウォール アクセス ルールは、順序が付けられたリストまたは表の形式で提供されます。展開されると、このポリシーは Access-Control List（ACL; アクセス コントロール リスト）となります。リスト内の各エントリは、Access-Control Entry（ACE; アクセス コントロール エントリ）と呼ばれます（詳細については、アクセス ルールについて　（913 ページ）を参照してください）。

パケットを転送するかドロップするかを決定するときに、デバイスは、リストされている順序で各アクセス ルールに照らしてパケットをテストします。アクセス ルールに対してロギングをイネーブルにすると、テストの結果はルールごとのログ設定に従って記録されます。ASA などの一部のデバイスでは、ロギングを明示的に設定しない場合でも、拒否されたアクセスのロ

グ エントリが生成されます。ロギング オプションを含むアクセス ルールの作成の詳細については、アクセス ルールの設定 （920 ページ）を参照してください。

（[Advanced]/[Edit Options] ダイアログボックス （936 ページ）で）ルールに対してロギングが有効な場合、イベントをログに記録するために、デバイスはイベントビューアに syslog メッセージを送信します。このクエリーには、使用可能なキーワード情報などのアクセス ルール パラメータが含まれています。レポートされるイベントには、接続の設定およびティアダウンは含まれません。

ルール関連のイベントを表示するには、次の右クリック コマンドを使用します。

- **Show Events > Realtime**：このルールに一致するイベントのリアルタイムクエリ結果をイベントビューアに表示します。いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。
- **Show Events > Historical**：このルールに一致するイベントの履歴クエリ結果をイベントビューアに表示します。いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、履歴結果を変更できます。

アクセスルール イベント クエリの基準として、Security Manager からイベントビューアに次の情報が提供されます。

- [Device details]：ホスト名、ドメイン名、管理 IP アドレス、表示名などのデバイスに関する一般情報。
- [Source addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの送信元アドレス。
- [Destination addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの宛先アドレス。
- [Service]：プロトコルおよびポート情報。
- [イベントタイプ（Event Type）]：許可ルールの場合は「構築/ティアダウン/許可された IP 接続」、拒否ルールの場合は「セキュリティポリシーによってパケットを拒否」。

（注）

- 一度に照会できるアクセス ルールは 1 つだけです。
- セキュリティデバイスで NAT または PAT が設定されている場合、送信元アドレスと宛先アドレスは変換前および変換後のアドレスにそれぞれマッピングされ、Security Manager からイベントビューアにクエリーが送信されるときは変換後のアドレスが使用されます。インバウンド アクセス ルールの場合、宛先アドレスは変換前アドレスと見なされ、アウトバウンド アクセス ルールの場合、送信元アドレスは変換後アドレスと見なされます。
- 複数のサービス（UDP、TCP、ICMP など）でフィルタリングすると、正確な結果が得られない場合があります。この問題を回避するには、イベントビューアの起動後に一部のフィルタを削除します。

- ICMP サブタイプに基づくフィルタリングはサポートされていません。たとえば、ACE で「ICMP Echo」が稼働している場合、フィルタはプロトコル（ICMP）にのみ適用され、イベントビューアのタイプカラム（Echo）には適用されません。
- 「eq」、「neq」、「gt」、および「lt」のサービスポートは、イベントビューアへのクロス起動ではサポートされていません。

関連項目

- [Access Rules] ページ （924 ページ）
- Looking Up Events for a Cisco Security Manager Policy （3543 ページ）
- IPS シグニチャのイベントの表示 （3545 ページ）
- HPM デバイスとサイト間 VPN のイベントの表示 （3546 ページ）

IPS シグニチャのイベントの表示

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

着信トラフィックを設定済みのシグニチャと比較することにより、IPS デバイスによってネットワーク侵入が検出およびレポートされると、デバイス上で syslog メッセージが生成されます。デバイスが Security Manager によってモニタされている場合、シグニチャに関連付けられたログがデバイスから取得されたあと、イベントビューアでインシデントが生成されます。特定のシグニチャに関連付けられたイベントを検索すると、攻撃を迅速に識別し、デバイス設定を調整して侵入を最小限に抑えるか、または防止できます。

レポートされたネットワーク侵入イベントをイベントビューアで表示するには、Security Manager のデバイスのシグネチャポリシーで 1 つ以上のエントリを選択し、イベントビューアに移動してリアルタイムイベントおよび過去のイベントを表示します。

関連項目

- Looking Up Events for a Cisco Security Manager Policy （3543 ページ）
- アクセスルールのイベントの表示 （3543 ページ）
- HPM デバイスとサイト間 VPN のイベントの表示 （3546 ページ）

ステップ 1 （デバイスビュー）IPS デバイスを選択して、[IPS]>[シグネチャ（Signatures）]>[シグネチャ（Signatures）] を選択し、 [Signatures] ページ （2169 ページ）を表示します。

ステップ 2 シグニチャテーブルで目的のエントリを右クリックするか、または複数のエントリを選択してそのうちの 1 つを右クリックし、[イベントの表示（Show Events）] メニューから次のコマンドのいずれかを選択します。

- [Realtime（リアルタイム）]：このシグニチャに一致するイベントのリアルタイムクエリ結果をイベントビューアに表示します。イベントビューアへのストリーミング中の未処理イベントを表示するには、このオプションを使用します。

いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- [履歴（Historical）]：このシグニチャに一致するイベントの履歴クエリ結果をイベントビューアに表示します。

いつでも [イベント監視（Event Monitoring）] ウィンドウでクエリ基準を変更し、新しいパラメータを適用して、結果を変更できます。

ヒント：

- シグニチャがディセーブルの場合、警告が表示され、イベント検索に進むかどうかが確認されます。
- タイプが Packet Data および Context Data のイベントはシグニチャ ルールによってトリガーされないため、これらのイベントはクエリー結果に表示されません。

HPM デバイスとサイト間 VPN のイベントの表示

Health and Performance Monitor から、監視対象デバイスのイベント、またはトンネルアップ/ダウンイベントが発生したサイト間 VPN のイベントにすばやくアクセスできます。

監視対象デバイスのイベントを表示するには、[すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[IPSデバイス（IPS Devices）]、[優先デバイス（Priority Devices）]、またはカスタムデバイス関連のビューからデバイスを選択し、デバイスの詳細領域で [概要（Summary）] タブを選択して、[イベントの表示（View Events）] ボタンをクリックします。イベントビューアが開き、[イベントモニタリング（Event Monitoring ）] ウィンドウに、選択したデバイスでフィルタリングされたイベントと、スライダバーで指定された期間が一覧表示されます。

トンネルのアップ/ダウンイベントが発生したサイト間 VPN の関連イベントを表示するには、次のいずれかを実行します。

- サイト間トンネルビューで、[ステータス（Status）] 列の [ダウン（Down）] 通知ハイパーリンクをクリックします。
- アラートビューで、トンネルアップ/ダウンアラートの [説明（Description）] 列のハイパーリンクをクリックします。

イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のアップ/ダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。

関連項目

- 正常性とパフォーマンスのモニタリングの準備 （3615 ページ）
- Looking Up Events for a Cisco Security Manager Policy （3543 ページ）
- アクセスルールのイベントの表示 （3543 ページ）
- IPS シグニチャのイベントの表示 （3545 ページ）

イベント分析の例

多種多様な手法を使用して、ネットワーク デバイスが生成したイベントを分析して対応できます。ここで示す例を参照すると、Security Manager の Event Viewer で実行できる操作の一部が理解しやすくなります。

ここでは、次の内容について説明します。

- ヘルプ デスク：サーバへのユーザ アクセスがファイアウォールでブロックされている （3547 ページ）
- ボットネット アクティビティのモニタリングと軽減 （3550 ページ）
- イベント テーブルからの false positive IPS イベントの削除 （3557 ページ）

ヘルプ デスク：サーバへのユーザ アクセスがファイアウォールでブロックされている

この例では、ヘルプ デスクがサーバにアクセスできないユーザから電話を受けます。

ユーザがサーバにアクセスできない場合、次に示すように数多くの理由があります。

- ネットワークのサーバー側の問題。サーバーがダウンしている、ネットワーク接続が確立されていない、ポリシーによってサーバーのファイアウォールがアクティブにアクセスが禁止されているなど。
- ユーザとサーバ間のネットワーク クラウドの問題。ルーティングなど。
- ユーザーのネットワークの問題。ワークステーションの問題、ネットワーク接続に関する物理的な問題（ワイヤの破損など）、スイッチポートまたはワイヤレスアクセスポイントに関する問題、DNS ルックアップの失敗など。

Security Manager の Event Viewer では、このような問題を特定して解決することができません。ただし、制御しているファイアウォールがサーバへのアクセスをブロックしているかどうかはわかります。これにより、問題の発生源であるとしてファイアウォールを取り外すか、またはファイアウォールがアクセスをブロックしている場合には問題を修正したり、ポリシーに基づいてサーバがブロックされていることをユーザに通知したりできます。

この手順では、まずサーバへのアクセスがポリシーで拒否されていないことを確認し、ファイアウォールはサーバへのアクセスを許可する必要があるものと想定しています。

ステップ 1 ユーザにワークステーションおよびサーバの IP アドレスを確認します。

ステップ 2 イベントビューアを開きます。たとえば、Configuration Manager で **[起動（Launch）] > [イベントビューア（Event Viewer）]** を選択します。

ステップ 3 [ファイアウォールトラフィックイベント（[Firewall Traffic Events）] ビューをダブルクリックして開きます。必要に応じて、ワークステーションに関連する IPS イベントの有無も確認する場合は、[すべてのデバイスイベント（All Device Events）] ビューを使用できます。

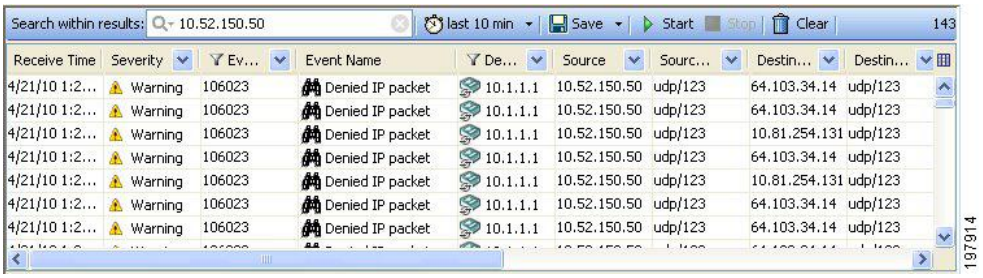
ヒント また、[ファイアウォール拒否イベント（Firewall Denied Events）] ビューを選択して、拒否されたイベントだけを表示できます。ただし、ユーザーのワークステーションに関連する他のイベントも確認することを推奨します。

ステップ 4 ユーザにサーバへのアクセスを再試行するように求めます。

ステップ 5 [開始（Start）] ボタンをクリックするか、または [表示（View）] > [開始（Start）] を選択し、イベントテーブルを更新して、最新のイベントを表示します。

ステップ 6 [結果内の検索（Search within Results）] ボックスにユーザーの IP アドレスを入力します。入力した内容に従ってイベントのリストがフィルタリングされ、いずれかのカラムに検索文字列が存在するイベントが表示されます。次の図のイベント リストには、過去 10 分間に発生した IP アドレス 10.52.150.50 に関するイベントがすべて表示されています。

図 *62 : 1* つの *IP* アドレスに限定したイベント リスト



ヒント また、[送信元（Source）] 列のドロップダウンリストから IP アドレス、および [宛先（Destination）] 列のドロップダウンリストからサーバーの IP アドレス（またはその逆）を選択して、関心のある送信元と宛先に関するイベントだけを表示できます。検索文字列ではイベントリストを十分に絞り込めないために分析が容易ではない場合には、カラム フィルタを使用します。

ステップ 7 ユーザーのワークステーションからサーバーに向かうトラフィック、またはサーバーからワークステーションに向かうトラフィックが拒否されたことを示すイベントを探します。syslog **106xxx** メッセージは、拒否アクションを示します。

テーブルでイベントを選択し、ウィンドウの一番下に [Event Details] ペインを開きます。このペインのタブには、メッセージ情報全体が表示され、わかりやすい説明と推奨するアクションが示されます。

ステップ 8 イベントがメッセージ **106023** または **106100** の場合は、接続を拒否しているアクセスルールを容易に特定して修正できます。テーブルで [Event Name] セルを確認することにより、イベントからポリシーを検索できるかどうかを識別できます。イベント名の前に双眼鏡アイコンがある場合は、ポリシーを検索できます。また、[Go To Policy] コマンドがグレーになっている場合、そのタイプのイベントではポリシーを検索できません。

ヒント アクセスリストの最後で暗黙の **deny any** ルールのためにトラフィックが拒否されている場合、Go To Policy コマンドではそのルールに移動できません。ルール検索のヒントについては、Event Viewer からの Security Manager ポリシーの検索 （3541 ページ）を参照してください。

a) イベントを右クリックし、[Go To Policy] を選択します。ルールが選択された状態でデバイス ビューが表示されます。一致するルールが見つからない場合には通知されます。

b) 目的のアクセスが許可されるようにルールを変更します。そのためには単にルールを削除するだけでよい場合もあれば、具体的に宛先サーバとのトラフィックを許可する新規ルールを追加することが必要になる場合もあります（拒否ルールよりも上位に許可ルールを配置します）。組織のセキュリティポリシーによって、許容される変更が決まります。アクセス ルール ポリシーの設定の詳細については、アクセス ルールの設定 （920 ページ）を参照してください。

c) 更新した設定をデバイスに送信して展開します。展開プロセスの詳細については、Workflow 以外のモードでの設定の展開 （515 ページ）またはWorkflow モードでの設定の展開 （523 ページ）を参照してください。

展開が正常に完了するまで待機します。

ステップ 9 ユーザにサーバへのアクセスを再試行するように求めます。アクセスが再度拒否される場合は、イベントビューアで [開始（Start）] をクリックしてイベントリストを更新し、最新の拒否イベントを探します。

ヒント サーバとの通信を拒否するアクセスルールが複数存在する場合もあります。アクセスルール ポリシーは上から下に順に処理されるため、アクセスを阻止するルールを削除すると、それまで適用されていなかったルールが突然アクティブになることがあります。アクセス ルール ポリシーがきわめて長い場合には、ルールをいくつか順に削除していくことが必要になる場合があります。このほか、Rule Combiner ツールを使用して、アクセス ルール ポリシーを統合して簡素化する方法もあります。詳細については、ルールの結合 （785 ページ）を参照してください。

ステップ 10 ファイアウォールがアクセスをブロックしなくなるまで、アクセス拒否イベントの解決を続けます。

ヒント また、Packet Tracer ツールを使用して、ASA デバイスを経由してワークステーションからサーバに流れるトラフィックをシミュレートすることもできます。デバイスビューで、アクセスを拒否しているデバイスを右クリックし、[パケットトレーサ（Packet Tracer）] を選択します。詳細については、Packet Tracer を使用した ASA または PIX の設定の分析 （3709 ページ）を参照してください。

すべてのイベントを解決したあとも、ユーザがサーバに到達できない場合、ファイアウォールはアクセスをブロックしているネットワーク要素の 1 つではないということになります。他の仲介ネットワーク デバイスを検討してみてください。トラフィックをブロックするアクセス ルールがルータに組み込まれていることなどが考えられます。

ボットネット アクティビティのモニタリングと軽減

Botnet Traffic Filter について （1163 ページ）の説明に従ってボットネット トラフィック フィルタリングを設定したあと、そのフィルタリングをモニタし、ネットワークで明らかになった問題の解決にあたることを推奨します。以降の項での説明に従って、Security Manager および ASDM を使用して、ボットネット アクティビティをモニタし、明らかになった問題を軽減できます。

- 対処可能なイベントであることを示す syslog メッセージについて （3550 ページ）
- Security Manager の Event Viewer を使用したボットネットのモニタリング （3551 ページ）
- Security Manager の Report Manager を使用したボットネットのモニタリング （3553 ページ）
- Adaptive Security Device Manager（ASDM）を使用したボットネット アクティビティのモニタリング （3554 ページ）
- ボットネット トラフィックの軽減 （3555 ページ）

対処可能なイベントであることを示す syslog メッセージについて

ボットネット トラフィック フィルタ イベントは、syslog メッセージ番号 338xxx を使用します。ただし、メッセージの中には単なる情報であり、メッセージに対するアクションが必要ないものもあります。

ボットネット イベントの syslog を表示するときには、次のメッセージ番号に特に注意してください。ブロックリストに掲載または許可されたトラフィックであることを示すメッセージの処理の詳細については、ボットネット トラフィックの軽減 （3555 ページ）を参照してください。syslog メッセージの詳細については、http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html で、ご使用の ASA ソフトウェアバージョンの Syslog メッセージ [英語] を参照してください。

- **338001 ～ 338004**：ASA がログに記録しているブロックリスト掲載のトラフィックを停止していないことを示します。進行中のボットネットアクティビティを停止する場合には、このようなメッセージに早急に対処する必要があります。
- **338005 ～ 338008**：ASA がログに記録し、ドロップしているブロックリスト掲載のトラフィックであることを示します。これは、トラフィックが廃棄ルールに該当したことを示します。したがって、ネットワークは保護されています。ただし、攻撃対象のコンピュータから感染を除去する必要があります。
- **338201、338202**：ASAがログに記録し、ドロップしていないグレーリスト掲載のトラフィックであることを示しますこのようなメッセージは、早急な対処を必要とするアクティブなボットネット接続であることを示す場合があります。
- **338203、338204**：ASAがログに記録し、ドロップしているグレーリスト掲載のトラフィックであることを示します。ネットワークは、このトラフィックから保護されています。ただし、グレーリスト掲載のサイトが正規のサイトである場合は、トラフィックがドロップされていること自体が早急の対処を必要とする問題であることがあります。グレーリスト掲載のアドレスが正規のアドレスであり、設定を再展開する場合は、スタティック デー

タベースへのエントリの追加 （1168ページ）の説明に従ってそのアドレスを許可リストに追加できます。

- **338305 ～ 338307、338310**：ASA が動的なフィルタデータベースをダウンロードできませんでした。デバイスに DNS ルックアップを設定しており、Cisco Intelligence Security Operations Center にルーティング可能なネットワーク パスがあることを確認してください。Cisco Technical Support への問い合わせが必要になる場合があります。
- **338309**：ボットネット トラフィック フィルタ ライセンスが最新ではないため、動的なデータベースをダウンロードできません。適切なライセンスを購入してインストールしてください。ボットネット トラフィック フィルタ ライセンスは時間ベースであるため、有効なライセンスが期限切れになった可能性があります。

Security Manager の Event Viewer を使用したボットネットのモニタリング

Event Viewer アプリケーションを使用して、ASA デバイスが生成した syslog イベントをモニタできます。Event Viewer には、発生したばかりのボットネット イベントを表示する定義済みのビューがあります。

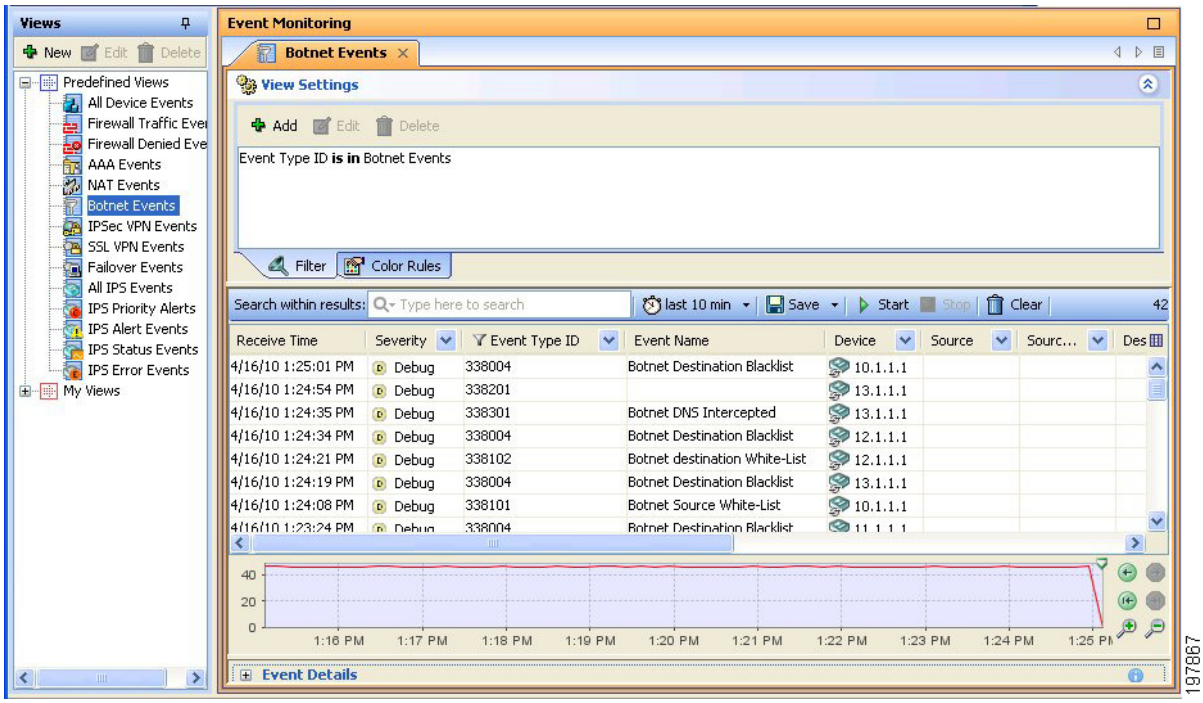
ボットネット メッセージはデバッグ重大度を知らせる情報であり、338xxx の番号が付与されています。

ヒント この手順では、Event Manager サービスがイネーブルになっていることを想定しています。そうでない場合は、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [イベント管理（Event Management）] ページを使用してイネーブルにします。

ステップ 1 イベントビューアを開きます。たとえば、Configuration Manager で **[起動（Launch）] > [イベントビューア（Event Viewer）]** を選択します。

ステップ 2 左ペインにある定義済みのビューのリストから、[ボットネットイベント（Botnet Events）] をダブルクリックします。ビューをダブルクリックしてアクティブにし、右ペインにロードする必要があります。ビューが開いていることを確認するには、右ペインでビューのタブ名が「Botnet Events」であることを確認します。次の図に、ボットネットイベントビューの一例を示します。

図 *63 : Security Manager の Event Viewer* へのボットネット イベント ビュー

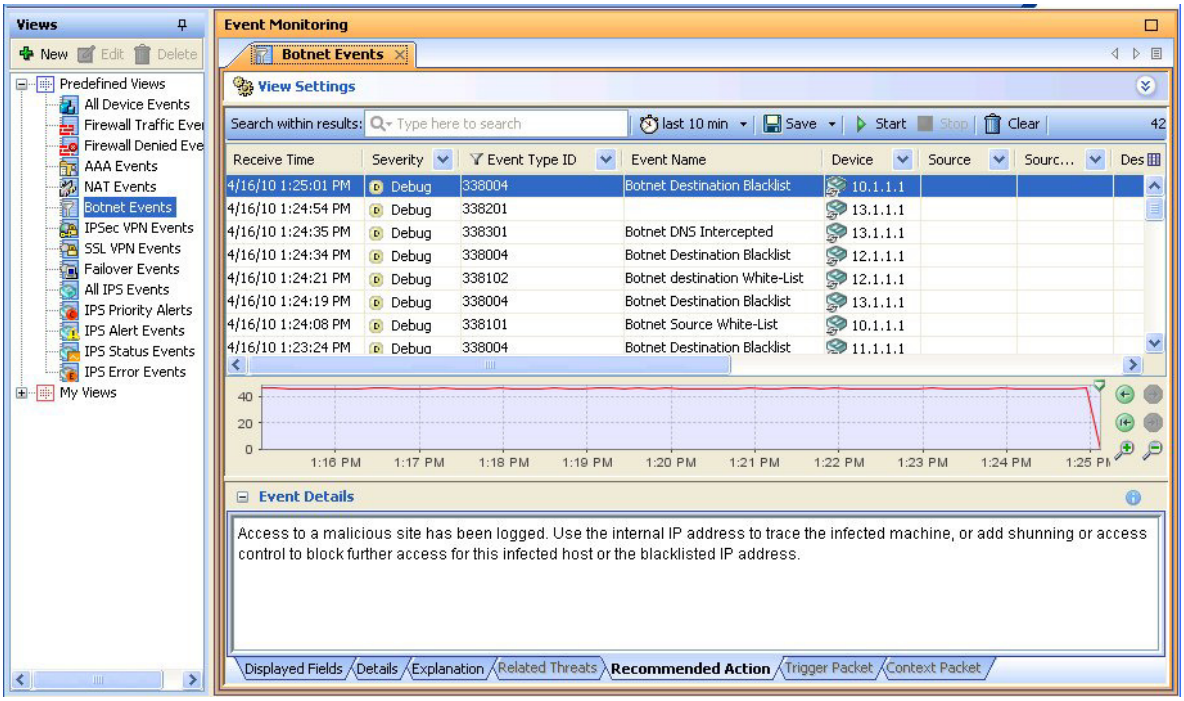


ステップ 3 特定のイベントの詳細を参照するには、テーブルでそのイベントを選択します。続いて、次の手順を実行します。

- イベントをダブルクリックして、読みやすい表形式で情報を表示します。
- ウィンドウの一番下に[イベントの詳細（Event Details）]セクションを開きます。詳細ペインには、イベントに関する情報がタブに編成されて表示されます。[Explanation] タブおよび[Recommended Action] タブには、イベントに関する情報と、イベントへの推奨の対処方法がわかりやすく示されています。

次の図に、Botnet Destination Blocklist メッセージ 338004 の [イベントの詳細（Event Details）] ペインを示します。この例には、推奨するアクションが表示されています。このメッセージの説明には、「This syslog message is generated when traffic to an IP address in the block list in the dynamic filter database appears.」（この syslog メッセージは、ダイナミック フィルタ データベース内のブロックリストの IP アドレスへのトラフィックが発生した場合に生成されます）とあります。このタイプのイベントの詳細については、ボットネット トラフィックの軽減 （3555 ページ）を参照してください。

図 *64 : Botnet Destination Blocklist* メッセージ *338004* に関するボットネットイベントの詳細



ステップ 4 イベント リストの対象を単一の ASA が生成したイベントに絞り込むには、[Device] カラムのドロップダウン矢印をクリックし、リストから目的のデバイスを選択します。リストの対象を複数の ASA に絞り込む場合は、ドロップダウン リストから [Custom] を選択し、表示されたダイアログボックスで目的のデバイスを選択します。

他のカラムに対するフィルタを使用して、リストを絞り込むこともできます。フィルタリングは、どのカラムでも同じように機能します。ドロップダウン リストから目的の値を選択するか、または [Custom] を選択してさらに複雑なカラム フィルタを作成します。

Security Manager の Report Manager を使用したボットネットのモニタリング

Report Manager アプリケーションを使用して、ボットネット アクティビティのレポートを生成できます。定義済みレポートがあり、上位の感染したホスト、上位のマルウェア ポート、および上位のマルウェア サイトが示されます。これらのレポートの詳細については、ファイアウォール サマリー ボットネット レポートについて （3579 ページ）を参照してください。

ヒント この手順では、Event Manager サービスがイネーブルになっていることを想定しています。そうでない場合は、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [イベント管理（Event Management）] ページを使用してイネーブルにします。

ステップ 1 Report Manager を開きます。そのためには、たとえば、Configuration Manager で [起動（Launch）] > [Report Manager] を選択します。

ステップ 2 [システム（System）] > [FW] > [サマリーボットネット（Summary Botnet）] フォルダから目的のレポートを開きます。レポートを開くには、レポートをダブルクリックするか、レポートを右クリックして、[レポートを開く（Open Report）] を選択します。

ステップ 3 （任意）目的の時間範囲およびデバイスを選択してレポートに含めるために、レポートをカスタマイズします。詳細については、レポート設定の編集 （3589 ページ）を参照してください。

今後そのレポートを再生成するためにカスタム設定を保存するには、[名前を付けて保存（Save As）] をクリックしてカスタムレポートを作成します。詳細については、カスタム レポートの作成 （3588 ページ）を参照してください。

ステップ 4 [レポートの生成（Generate Report）] をクリックして収集した情報を取得して、グラフおよび表形式データで表示します。詳細については、レポートの起動と生成 （3586 ページ）を参照してください。

定期的にレポートを生成する場合は、レポート スケジュールの設定 （3604 ページ）で説明するとおりに、スケジュールを設定できます。

Adaptive Security Device Manager（ASDM）を使用したボットネット アクティビティのモニタリング

Adaptive Security Device Manager（ASDM）には、ボットネット レポート機能が含まれています。ASDM の読み取り専用バージョンがデバイス マネージャとして Security Manager クライアントとともにインストールされ、Security Manager 内から ASDM を起動できます。

ヒント 完全な形の ASDM アプリケーションを別途インストールすることもできます。ただし、ASDM で実施した設定変更は、Security Manager ではアウトオブバンド変更であると見なされ、次回 Security Manager から設定を展開すると上書きされます。それでも ASDM を使用して設定変更を実施する必要がある場合は、その設定の Security Manager のビューが最新のものとなるように、Security Manager でデバイスに対するポリシーを再検出してください。

ステップ 1 Configuration Manager のデバイス ビューで ASA デバイスを選択します。

ステップ 2 **[起動（Launch）] > [Device Manager]** を選択して、ASA への ASDM 接続を開きます。設定変更が実施できないことが警告されます。[はい（Yes）] をクリックして続行します。

ステップ 3 ASDM で、次の領域のボットネット トラフィック フィルタ モニタリング情報を参照します。

- **[ホーム（Home）] > [ファイアウォールダッシュボード（Firewall Dashboard）]** には、ボットネット トラフィック フィルタの概要があります。

- **[モニタリング（Monitoring）] > [ボットネットトラフィックフィルタ（Botnet Traffic Filter）] > [レポート（Reports）]**には、上位のボットネットサイト、ポート、および感染したホストに関するチャートが含まれています。
- **[モニタリング（Monitoring）] > [ロギング（Logging）] > [ログバッファ（Log Buffer）]** には、syslog メッセージの履歴が表示されます。
- **[モニタリング（Monitoring）] > [ロギング（Logging）] > [リアルタイムログビューア（Real-Time Log Viewer）]** は、syslog メッセージが生成されたままの状態で表示されます。

ヒント　**[設定（Configure）] > [ボットネットトラフィックフィルタ（Botnet Traffic Filter）] > [ボットネットデータベース（Botnet Database）]**ページで、動的なデータベースを検索することもできます。このページではこのほか、手動でデータベースのダウンロードを開始したり、動的なデータベースを消去したりすることもできます。これらのアクションは、デバイスの設定を変更しません。Security Manager でポリシーを再検出する必要もありません。

ボットネット トラフィックの軽減

ボットネット トラフィックの軽減は、次の 2 つの手順からなります。

1. ネットワークからボットネット制御サイトへのトラフィックを停止する。
2. 攻撃対象のコンピュータから感染を除去する。

次の手順では、このプロセスをさらに詳しく説明します。

ステップ 1　好ましくないアドレスとの間でパケットがやり取りされていることを示すsyslogイベントが表示されます。一般には、メッセージ番号 338001 ～ 338008 または 338201 ～ 3382004 です。このようなメッセージの詳細については、対処可能なイベントであることを示すsyslogメッセージについて （3550ページ）を参照してください。

ヒント　メッセージ338201 ～ 3382004 はグレーリスト掲載のトラフィックです。トラフィックを停止する前にまず、グレーリスト掲載のトラフィックが本当に好ましくないものであるかどうかを判断します。

ステップ 2　ボットネット トラフィックを停止します。

- メッセージ 338005 ～ 338008 および 338203 ～ 338204 は、ASA がトラフィックをすでにドロップしていることを示します。トラフィック分類ドロップルールは、ブロックリストまたはグレーリストに含まれているアドレスを対象とします。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170 ページ）を参照してください。
- メッセージ 338001 ～ 338004 および 338201 ～ 338202 は、ASA がイベントをログに記録しているものの、トラフィックをドロップしていないことを示します。まずはこのトラフィックを停止する必要があります。

廃棄ルールのために ASA がまだボットネット トラフィックをドロップしていない場合には、ボットネット トラフィックを停止するためのオプションとして次のものが用意されています。

- （推奨の方法）。ボットネットサイトのドロップルールを設定し、設定を再展開します。ボットネット トラフィック フィルタのトラフィック分類とアクションのイネーブル化 （1170ページ）を参照してください。
- （2 番目に推奨の方法）。SSH クライアントを使用して ASA にログインし、特権 EXEC モードを開始し、**shun** コマンドを使用してボットネットサイトとの間でやり取りされるトラフィックを阻止します。このコマンドは CLI ウィンドウで ASDM から発行することもできますが、Security Manager からは発行できません。shun コマンドは、トラフィックをブロックする永続的なルールを作成するものではありません。

たとえば、ボットネット サイトが 10.1.14.14 で、内部の感染したコンピュータが 10.100.10.10 である場合は、次のコマンドを発行します。最初のコマンドはボットネットコマンドセンターからの着信トラフィックをすべてブロックし、2つめのコマンドはボットネットサイトに感染したコンピュータからのトラフィックをブロックします。

shun 10.1.14.14

shun 10.100.10.10 10.1.14.14

- (Not recommended.) shun コマンドを推奨しますが、ボットネットサイトとの間でやり取りされるトラフィックを拒否する永続的なルールをインターフェイスのアクセス制御リスト（ACL）に作成することもできます。Cisco Security Manager でデバイスを選択した状態で、**[ファイアウォール（Firewall）] > [アクセスルール（Access Rule）]** を選択し、ルールを 2 つ作成します。1 つは宛先アドレスに関係なく、送信元アドレスであるボットネットサイトを拒否するルール、もう 1 つはボットネットサイトが宛先アドレスである送信元アドレスをすべて拒否するルールです。サービスの場合、すべてのトラフィックがブロックされるように IP を選択します。ルールを有効にするには、設定を展開する必要があります。

アクセス ルールを作成する方法は推奨しません。ボットネット サイトが一時的なものであるのに対して、永続的なルールを作成するためです。このタイプのネットワーク攻撃には、従来のアクセス ルールよりも、ボットネット トラフィック フィルタを使用してボットネット トラフィックを動的にブロックする方が適しています。

ステップ 3 感染したコンピュータに対するネットワーク アクセスをシャットダウンします。たとえば、コンピュータが接続されているスイッチポートを特定し、スイッチの CLI を使用してそのポートをシャットダウンします。問題のコンピュータが他にワイヤレスアクセスを備えている場合もあるため、ネットワーク アクセスを完全にシャットダウンするのは簡単な作業であるとはかぎりません。

ステップ 4 攻撃対象のコンピュータの所有者にそのコンピュータが感染していることを通知し、IT 担当者を派遣してコンピュータから感染を除去します。コンピュータから感染を除去するためのツールおよび手法については、このマニュアルでは取り上げません。

イベント テーブルからの false positive IPS イベントの削除

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしていますが、バグの修正や拡張機能はサポートしていません。

ある特定のパケットまたは一連のパケットが、IPS シグニチャに定義されている既知の攻撃プロファイルの特性に一致すると、IPS アプライアンスまたはサービス モジュール（IPS デバイス）がアラームをトリガーします。IPS が良性のアクティビティを悪意のあるアクティビティであるとレポートした場合、false positive（良性のトリガー）が発生します。各イベントの診断には人手の介入が必要であるため、false positive イベントの分析に時間をかけると、リソースが大量に消費されます。

悪意のあるアクティビティの検出に使用される IPS シグニチャの性質により、IPS の有効性を大幅に低下させたり、組織のコンピューティング インフラストラクチャ（ホストやネットワークなど）を大きく混乱させたりすることなく、false positive を完全に排除することはほぼ不可能です。IPS の展開時に独自に調整を実施すると、false positive が最小限に抑えられます。コンピューティング環境が変更されたとき（新規にシステムやアプリケーションを展開するときなど）には、定期的に再調整を実施する必要があります。IPS デバイスは柔軟な調整機能を備えており、定常状態の動作中に false positive が発生するのを最小限に抑えることができます。

false positive の一例が、ping スイープを実行してネットワーク検出マップを定期的に構築するネットワーク管理ステーションです。ping スイープは、ICMP Network Sweep with Echo シグニチャ（シグニチャ ID 2100）をトリガーします。このため、送信元アドレスがネットワーク管理ステーションの IP アドレスとなっている ICMP Network Sweep with Echo イベントは、実際には想定どおりの望ましいイベントです。

Event Viewer のイベント テーブルから false positive IPS イベントを削除するときには、次のオプションが用意されています。

- **既知の「クリーンな」ソースからイベントを除外します。**

イベントを除外すると、イベントが生成されなくなるのではなく、テーブルにイベントが表示されなくなります。イベントは引き続き使用できるため（フィルタを削除できます）、特定のネットワーク動作を調べるには除外されたホストからのアクティビティを確認する必要がある場合には、イベントを参照できます。

この手法の使用には、主に次の 2 つの欠点があります。

- イベントは引き続き生成されて、イベント ストアに追加されます。
- フィルタは、ホストからすべてのイベントを除外します。ホスト/シグニチャ ID のペアを除外する複雑なフィルタは作成できません。

次の手順では、クリーンであると識別した送信元からのイベントを除外する方法を示します。

- **false positive イベントの生成を阻止するイベント アクション フィルタ ルールを作成します。**

イベント アクション フィルタ ルールは、イベントの生成を阻止するための最も簡単な方法です。また、作業が難しくなるシグニチャの編集やカスタム シグニチャの作成にも、この方法を推奨します。イベント アクション フィルタ ルールでホストを除外すると、IPS デバイスはイベントをトリガーしても、アラームを生成せず、ログに記録を残しません。

ホストからすべてのイベントを全面的に除外するのではなく、特定のシグニチャを対象にできるため、良性であるとの確信があるイベントだけを排除できます。たとえば、次のイベント フィルタ ルールは、ネットワーク管理ステーション 10.100.15.75 の ICMP Network Sweep with Echo（2100）シグニチャから Produce Alert アクションを排除します。このネットワーク管理ホストが攻撃者アドレスであると見なされますが、実際にはイベント フィルタ ルールに指定されているアクションが、イベントから削除されるアクションです。他のアラート生成アクションを ICMP Network Sweep with Echo イベントに追加するイベント アクション オーバーライド ルールを作成する場合は、このルールでオーバーライド アクションも削除する必要があることに注意してください。

Name	Active	IDs	Subs	Attackers	Attack Ports	Victims	Victim Ports	Actions	RR	Stop
Local (1 Filter)										
NMS_Ping_Sweep	Yes	2100	0-255	10.100.15.75	0-65535	0.0.0.0-255.255.255.255	0-65535	Produce Alert	0-100	No

198055

イベント アクション フィルタ ルールの設定の詳細については、[Event Action Filters] ページ（2219 ページ）を参照してください。

次の手順では、Event Viewer でフィルタリングを使用して、イベント リストから false positive を削除する方法を示します。ネットワーク/ホスト ポリシー オブジェクトを使用して、フィルタリングを実現します。

ヒント ネットワーク/ホスト オブジェクトを使用して送信元アドレス フィルタまたは宛先アドレス フィルタを作成すると、単にそのオブジェクトの内容を変更するだけでフィルタを更新できます。ビューに対してフィルタを追加または削除する必要はありません。利点にはもう 1 つ、イベント テーブルに現在表示されていないアドレスのフィルタをプロアクティブに作成できることがあります。Event Viewer の送信元/宛先カラム フィルタ コントロールには、イベント リストに現在掲載されているアドレスだけが一覧表示されます。

ステップ 1 クリーンなホストまたはネットワークの IP アドレスが含まれているネットワーク/ホスト ポリシー オブジェクトを作成します。

a) **[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）]** を選択して [Policy Object Manager] ウィンドウを開きます（Policy Object Manager （290 ページ）を参照）。
b) コンテンツテーブルから [ネットワーク/ホスト（Networks/Hosts）] を選択します。
c) ネットワーク/ホストポリシーオブジェクトのテーブルの下にある [行の追加（Add Row）]（+） ボタンをクリックし、オブジェクトタイプとして [グループ（Group）] を選択します。
d) [Add Network/Host Group] ダイアログボックスで IPS_Safe_Hosts などのオブジェクト名を入力します。
e) [IPv4アドレス情報の入力（Enter IPv4 Address Information）] を選択して、10.100.15.75 などの IP アドレスを入力します。

f) [追加>>（Add>>）] をクリックして IP アドレスを [グループ内のメンバー（Members in Group）] リストに追加します。

g) [OK] をクリックしてオブジェクトを作成します。

h) [閉じる（Close）] をクリックして、[Policy Object Manager] ウィンドウを閉じます。

ステップ 2 **[ファイル（File）] > [送信（Submit）]** を選択して、変更内容をデータベースに送信します（Workflow 以外のモード）。新規ポリシー オブジェクトだけでなく、すべての設定変更が送信されることに留意してください。

Workflow モードを使用している場合は、必要に応じてアクティビティを送信し、アクティビティの承認を得る必要があります。

ヒント Event Viewer では、データベースにすでに送信されたポリシー オブジェクトだけを表示できるため、そのオブジェクトを使用してフィルタを作成する場合は事前に変更内容を送信しておく必要があります。あとでポリシー オブジェクトを変更した場合には、そのオブジェクトの新規定義に使用しているフィルタの変更内容も送信する必要があります。

ステップ 3 **[起動（Launch）] > [イベントビューア（Event Viewer）]** を選択して、イベントビューア アプリケーションを開きます。

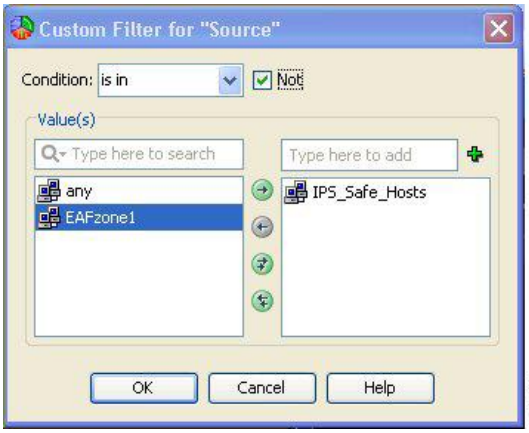
ステップ 4 ネットワーク管理ステーションを除外するカスタム ビューを作成します。

a) [すべてのIPSイベント（All IPS Events）] など、カスタムビューの土台として使用する定義済みのビューをダブルクリックします。[Views] リストでビューをダブルクリックすると、そのビューが開きます。更新するカスタム ビューがすでにある場合は、そのビューを開きます。

b) イベントテーブルで [ソース（Source）] 列のタイトルにある下向き矢印ボタンをクリックし、[カスタム（Custom）] を選択して [ソースのカスタムフィルタ（Custom Filter for Source）] ダイアログボックスを開きます。

ヒント：このダイアログボックスは、[設定の表示（View Settings）] ペインから開くこともできます。そのためには、[追加（Add）] ボタンをクリックし、[カスタムフィルタを列に追加（Add Custom Filter to a Column）] ダイアログボックスで [ソース（Source）] を選択し、[OK] をクリックします。

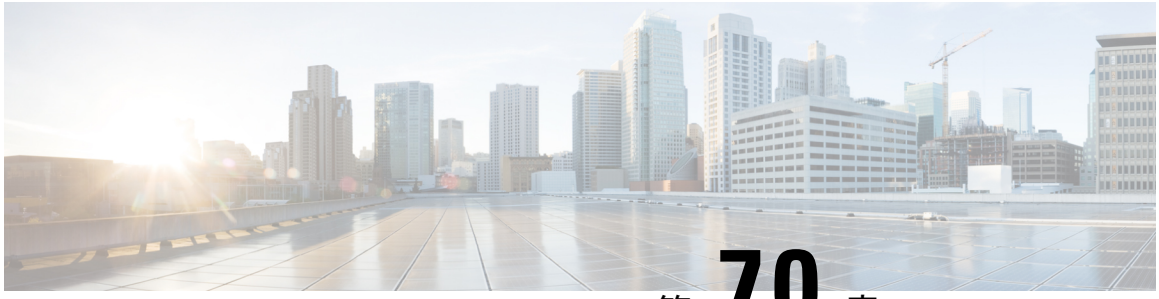
c) [Custom Filter for Source] ダイアログボックスで、作成したポリシー オブジェクトを選択し、右矢印ボタンをクリックしてそのオブジェクトを選択済みリストに移動します。また、[条件（Condition）] オプションの横にある [一致しない（Not）] オプションを選択します。次の図に、ダイアログボックスの内容を示します。



d) [OK] をクリックフィルタがビュー設定に追加され、テーブルからイベントを削除するために使用されます。

e) **[ファイル（File）] > [名前を付けて保存（Save As）]** を選択して、変更を新規カスタムビューとして保存します。ビューの名前と説明を入力するように求められます。それぞれ入力し、[OK] をクリックします。

次の図に、[All IPS Events] 定義済みビューから開始し、Filtered IPS Events という名前を指定した場合に、ビュー設定がどのようになるかを示します。



第 70 章

レポートの管理

Re

Report Manager アプリケーションを使用して、デバイス、およびリモート アクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。

この章は次のトピックで構成されています。

port Manager アプリケーションを使用して、デバイス、およびリモートアクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。

この章は次のトピックで構成されています。

- レポート管理について （3561 ページ）
- Security Manager で使用可能なレポートのタイプについて （3562 ページ）
- Report Manager レポート用のデバイスの準備 （3564 ページ）
- Report Manager データ集約について （3565 ページ）
- Report Manager のアクセス コントロールについて （3567 ページ）
- Report Manager の概要 （3568 ページ）
- Report Manager の事前定義システム レポートについて （3578 ページ）
- Report Manager でのレポートの使用 （3585 ページ）
- レポートのスケジュール設定 （3603 ページ）
- Report Manager のトラブルシューティング （3607 ページ）

レポート管理について

Report Manager アプリケーションを使用して、デバイス、およびリモート アクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。これらのレポートは、ご使用のネットワークに関する有益な情報を提供します。

Report Manager は、Event Manager サービスによってモニタ対象デバイスから収集される情報を集約します。このため、デバイスに関するレポートを表示するには、Event Viewer のデバイスもモニタリングする必要があります。一部の統計情報（VPN 統計情報など）は、通常の 5 分間隔のポーリングによってデバイスから直接取得されます。集約データには、15 分、毎時、毎日、および毎月の間隔で集約されるデータがあり、90 日間保持されます。15 分の集約データ

は最大3日間、毎時のデータは最大1週間保持されます。データ集約の詳細については、Report Manager データ集約について （3565 ページ）を参照してください。

Report Manager を使用して、以下に関するレポートを作成できます。

- ASA ソフトウェアリリース 8.0 以降を実行する適応型セキュリティアプライアンス（ASA）。VPN レポートの場合、ASA ソフトウェア 7.x リリースもサポートされます。

（注） VPN レポートは、VPN 設定をサポートしていない Cisco Catalyst 6500 シリーズ ASA Services Modules（ASA-SM; ASA サービス モジュール）では使用できません。その他のタイプのレポートは、ASA-SM で使用できます。

- IPS ソフトウェアリリース 6.1 以降を実行する IPS デバイス（IOS IPS デバイス以外）。これには、ASA、ルータ、およびスイッチに取り付けられた専用 IPS モジュールが含まれます。
- サポートされる ASA デバイスでホストされているリモート アクセス IPsec および SSL VPN。

（注） Event Viewer は FWSM を処理しますが、Report Manager は FWSM イベントについては報告しません。

次のトピックでは、Report Manager および使用可能なレポートをさらに詳細に説明し、Security Manager で使用可能なその他のタイプのレポートについても説明します。

- Security Manager で使用可能なレポートのタイプについて （3562 ページ）
- Report Manager レポート用のデバイスの準備 （3564 ページ）
- Report Manager データ集約について （3565 ページ）
- Report Manager のアクセス コントロールについて （3567 ページ）
- Report Manager の事前定義システム レポートについて （3578 ページ）

Security Manager で使用可能なレポートのタイプについて

Security Manager は、さまざまなレポート機能を提供します。以下に、使用可能なレポートのタイプを示します。

- **セキュリティおよび使用状況のレポート（Report Manager アプリケーション）**：Report Manager アプリケーションを使用して、Event Manager サービスによってモニター対象デバイスから収集された集約情報を表示できます。デバイスから直接取得される情報もあります。これらのレポートは、ネットワーク セキュリティおよびリモート アクセス IPsec および SSL VPN の使用状況に関する情報を提供します。

- **アクティビティ（設定セッション）変更レポート**：これらのレポートは、特定アクティビティ（Workflow モード）または設定セッション（Workflow 以外のモード）内で変更されたポリシーに関する詳細情報を提供します。詳細については、変更レポートの表示 （197 ページ）を参照してください。
- **アウトオブバンド変更レポート**：これらのレポートは、デバイスに存在する設定と Security Manager で管理されるデバイスの設定の間の不整合を識別します。この情報を使用して、設定を展開する前にこれらの不整合に事前に対処できます。この場合、展開ジョブで選択する動作に応じて、変更が上書きされるか、または展開が失敗します。詳細については、アウトオブバンド変更の検出および分析 （537 ページ）を参照してください。
- **監査レポート**：このレポートは、Security Manager およびデータベースに含まれているオブジェクトに対する変更内容に関する情報を提供します。このレポートには、ランタイム環境（ログインや認証の失敗など）、オブジェクトに対する変更（アクティビティの変更や展開など）、および管理対象デバイスに対する変更（インベントリの追加や削除など）に関する情報が含まれています。詳細については、監査レポートの生成 （623 ページ）を参照してください。
- **インベントリステータス**：このレポートは、ポリシー展開ステータスに関する情報を提供します。詳細については、インベントリ ステータスの表示 （3694 ページ）を参照してください。
- **ポリシー検出ステータスレポート**：デバイスからポリシーを検出するときに（インベントリへの追加時または管理対象デバイスのポリシーの再検出時のいずれか）、ポリシー検出に関する情報はあとで表示できるように保持されます。詳細については、ポリシー検出タスクのステータスの表示 （237 ページ）を参照してください。
- **展開ステータスレポート**：管理対象デバイスに設定を展開するときに、展開に関する情報はあとで表示できるように保持されます。詳細については、ジョブおよびスケジュールの展開ステータスおよび展開履歴の表示 （512 ページ）を参照してください。
- **トラブルシューティングのための展開および検出ステータスレポート**：展開およびポリシー検出ステータスレポートを Cisco Technical Support（TAC）への送信に適した形式でエクスポートし、問題のトラブルシューティングに役立てることができます。これらのレポートがユーザ独自の目的に役立つ場合もあります。詳細については、展開ステータス レポートまたは検出ステータス レポートの生成 （636 ページ）を参照してください。
- **エクストラネット VPN 設定概要**：エクストラネット VPN 設定概要の PDF ファイルを印刷または生成できます。この概要には、接続に使用されている事前共有キーが含まれている場合があります。この情報を使用して、ご使用のネットワークとパートナーまたはサービス プロバイダーのネットワークの間の現在の接続記録を維持できます。詳細については、[VPNトポロジの設定の概要の表示（Viewing a Summary of a VPN Topology's Configuration）] （1464 ページ）を参照してください。
- **ポリシーオブジェクト使用状況レポート**：このレポートは、ポリシーオブジェクトの使用場所（そのポリシーオブジェクトがポリシーまたは別のポリシーオブジェクトによって参照されているインスタンスなど）を示します。この情報を使用すると、提案されたオブジェクトに対する変更が、そのオブジェクトのすべての使用ケースで目的の効果を提供するかどうかの判別に役立ちます。ポリシーや別のポリシーオブジェクトによってアクティ

ブに使用されているオブジェクトは削除できないため、この情報はオブジェクトを削除する場合にも役立ちます。詳細については、オブジェクト使用状況レポートの生成 （306 ページ）を参照してください。

- **ポリシー オブジェクト オーバーライド レポート**：このレポートは、ポリシーオブジェクトに対して現在定義されているデバイスレベルのオーバーライドをすべて表示します（オーバーライドを許可するようにそのオブジェクトが定義されている場合）。このレポートからオーバーライドの作成および削除を行うこともできます。詳細については、単一デバイスのオブジェクト オーバーライドの作成または編集 （312 ページ）および[Policy Object Overrides] ウィンドウ （314 ページ）を参照してください。
- **デバイスマネージャレポート**：Security Manager には、ほとんどのサポート対象デバイスについて、Adaptive Security Device Manager（ASDM）などの個々のデバイスマネージャの読み取り専用バージョンが含まれています。これらのデバイスマネージャを Security Manager の Configuration Manager アプリケーションから直接開始し、それらのデバイスマネージャで使用できる任意のタイプのレポートを使用できます。これらのレポートは単一のデバイスに対するものであり、Report Manager を介して使用できるレポートを増強できます。Event Viewer または Report Manager では直接サポートされていないデバイスのステータス情報を提供することもできます。詳細については、デバイスマネージャの起動 （3697 ページ）を参照してください。

Report Manager レポート用のデバイスの準備

Report Manager でデバイスに関するレポートを表示する前に、Security Manager にイベントを送信するようにデバイスを設定し、そのデバイスをモニタするように Security Manager を設定する必要があります。Report Manager は Event Viewer でモニタリングしているデバイスに関するレポートのみを提供できるため、レポートのためのデバイス設定はイベントモニタリングのための設定と同じです。

ステップ 1 Security Manager にイベントを送信するようにデバイスを設定します。次のタイプのデバイスで Report Manager を使用できます。

- ASA 8.0 以降：詳細な設定手順については、イベント管理のための ASA と FWSM デバイスの設定 （3506 ページ）を参照してください。
- IPS 6.1 以降：詳細な設定手順については、イベント管理のための IPS デバイスの設定 （3508 ページ）を参照してください。

ステップ 2 モニタするデバイスの選択 （3514 ページ）の説明に従って、デバイスがイベント管理用に選択されていることを確認します。

ステップ 3 Event Manager サービスの開始、停止、および設定 （3509 ページ）の説明に従って、Event Manager サービスがイネーブルであることを確認します。

Report Manager データ集約について

Report Manager は、Event Manager サービスによってモニタ対象デバイスから収集される情報を集約します。このため、デバイスに関するレポートを表示するには、Event Viewer のデバイスもモニタリングする必要があります。

Report Manager は、2 つの方法を使用してデータを収集します。まず、Event Manager サービスは、関連するイベントを Report Manager に提供し、次に Report Manager が定義済みのレポートと現在設定されているカスタムレポートに基づき、それらのイベントを保存する必要があるかどうかを決定します。次に、VPN 統計情報などの一部の統計情報は、通常のポーリングを使用して 5 分間隔でデバイスから直接取得されます。

表 *978 : Report Manager* のデータ ソース

レポート（**Reports**）	データ ソース（**Data Sources**）
FW レポート	
上位ソース 上位接続先 最上位サービス（Top Services）	構築された Syslog： 302013、302015、302017、302020 syslog を拒否： 106001、106006、106007、106010、106011、106014、106015、106016、106017
上位マルウェア サイト（Top Malware Sites） 上位マルウェアポート 上位感染ホスト	BOTNET Syslog： 338001、338002、338003、338004、338005、338006、338007、338008、338201、338202、338203、338204
IPS レポート	
すべての IPS レポート	すべての IPS アラート
VPN レポート	

上位帯域幅ユーザ（フルクライアント）
上位継続時間ユーザ（フルクライアント）
上位スループットユーザ（フルクライアント）
	ASA バージョン 8.3 以前：
	`show vpn-sessiondb full svc`
	ASA バージョン 8.4.1 以降：
	`show vpn-sessiondb full anyconnect`

レポート（Reports）	データ ソース（Data Sources）

上位帯域幅ユーザ（IPSec-RA）
上位継続時間ユーザ（IPSec-RA）
上位スループットユーザ（IPSec-RA）
	ASA バージョン 8.3 以前：
	`show vpn-sessiondb full remote`
	ASA バージョン 8.4.1 以降：
	`show vpn-sessiondb full ra-ikev1-ipsec`

上位帯域幅ユーザ（クライアントレス） 上位継続時間ユーザ（クライアントレス） 上位スループットユーザ（クライアントレス）	すべての ASA バージョンの場合： `show vpn-sessiondb full webvpn`
ユーザ レポート	上記すべての show コマンド。
VPN デバイス使用状況レポート	上記すべての show コマンド。

Report Managerは、15分、毎時、毎日、および毎月の間隔で、この収集情報を集約します。15分の集約データは1日、毎時のデータは最大5日間、その他のデータは90日間保持されます。

集約スケジュールは固定された時刻に発生します。15 分の集約は正時からの時間で 00 分、15 分、30 分、および45 分に発生します。毎時の集約は正時（00 分）に発生します。毎日の集約は日付が変わるときに発生します（0 時になると、その日付が集約されます）。毎月の集約は月が変わるときに発生します。

集約サイクルは、レポートに表示される内容に影響します。

- レポートデータは直前のデータを対象にするわけではありません。代わりに、選択された期間について、最後に完了した期間全体を対象にします。たとえば、1 日のレポートは昨日を対象にします。今日のデータは含まれません。つまり、1 日のレポートは、レポート生成時刻から始まる直前の 24 時間ではありません。
- カスタム期間を使用してレポートを設定する場合、15分より短い期間を選択することはできません。レポートには、少なくとも 15 分の集約データが必ず含まれます。分のエントリは、最も近い集約時刻（つまり、00、15、30、または45）に丸められます。開始と終了が当日であるカスタム レポートの場合にのみ、分の値を設定できます。

また、毎時のデータは最大で5日間しか保持されないため、過去5日間についてのみ、カスタム期間内の時間を指定できます。

- デバイスがモニタされている期間より長い期間のレポートを生成することはできません。たとえば、初めてEvent Managerサービスを開始する場合、月が変わるまでは毎月のレポートを生成できません。これは、数日のみである場合（たとえば、29日にサービスを開始する場合）も、ほとんど月全体である場合（たとえば、月の最初の日にサービスを開始する場合）もあります。

このルールに対する例外は、カスタム期間レポートです。カスタム期間レポートは毎日の集約データを使用して生成されるため、任意のカスタム期間を選択できます。

（注） 最初の月の集約データは、1か月に相当するデータよりもかなり少ない可能性があることに注意してください。毎月のレポートを比較する場合、実際に（例として）30日間のデータと 15 日間のデータを比較していると、これは重大な相違に見える可能性があります。

事前定義システム レポートのデフォルトの時間間隔の設定、および個々のレポートの時間間隔の設定を行うことができます。次のトピックでは、時間コントロールについて説明します。

- レポートのデフォルト設定値の設定 （3598 ページ）
- レポート設定の編集 （3589 ページ）

Report Manager のアクセス コントロールについて

ユーザ名に対して割り当てられるユーザ権限により、Report Manager で行うことができる操作が制御されます。ローカル ユーザ、またはその他のタイプの非 ACS アクセス コントロールを使用する場合は、すべてのユーザが Report Manager およびすべてのレポートにアクセスできます。ただし、次のアクセス制限が課されます。

- 事前定義システム レポートのデフォルト設定値を設定するには、システム管理者権限またはネットワーク管理者権限が必要です。 レポートのデフォルト設定値の設定 （3598 ページ）を参照してください。
- 別のユーザーのスケジュールに対して、参照、イネーブル化またはディセーブル化、生成された結果の表示、または削除を行うには、システム管理者権限またはネットワーク管理者権限が必要です。次のトピックを参照してください。
  - レポート スケジュールの表示 （3603 ページ）
  - スケジューリングされたレポートの結果の表示 （3605 ページ）
  - レポート スケジュールのイネーブル化およびディセーブル化 （3606 ページ）
  - レポート スケジュールの削除 （3607 ページ）
- サーバーに設定されているすべてのカスタムレポートのリストの参照、または別のユーザーのカスタムレポートの削除を行うには、システム管理者権限またはネットワーク管理者権限が必要です。 カスタム レポートの管理 （3602 ページ）を参照してください。

ACS を使用して Security Manager へのアクセスを制御する場合、Report Manager へのユーザ アクセスを制御することもできます。ACS を使用する場合、次のようになります。

- View Report Manager 権限を使用して、Report Manager アプリケーションへのアクセスを制御できます。この権限を使用して、特定のユーザが Report Manager にアクセスできないようにしたり、Event Viewer へのアクセスを許可せずに Report Manager へのアクセスを許可するロールを作成したりすることができます。

- ユーザは、少なくともデバイスに対する表示権限がある場合にのみ、そのデバイスのレポートを表示できます。

Cisco Security Manager と Cisco Secure ACS との統合の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

Report Manager の概要

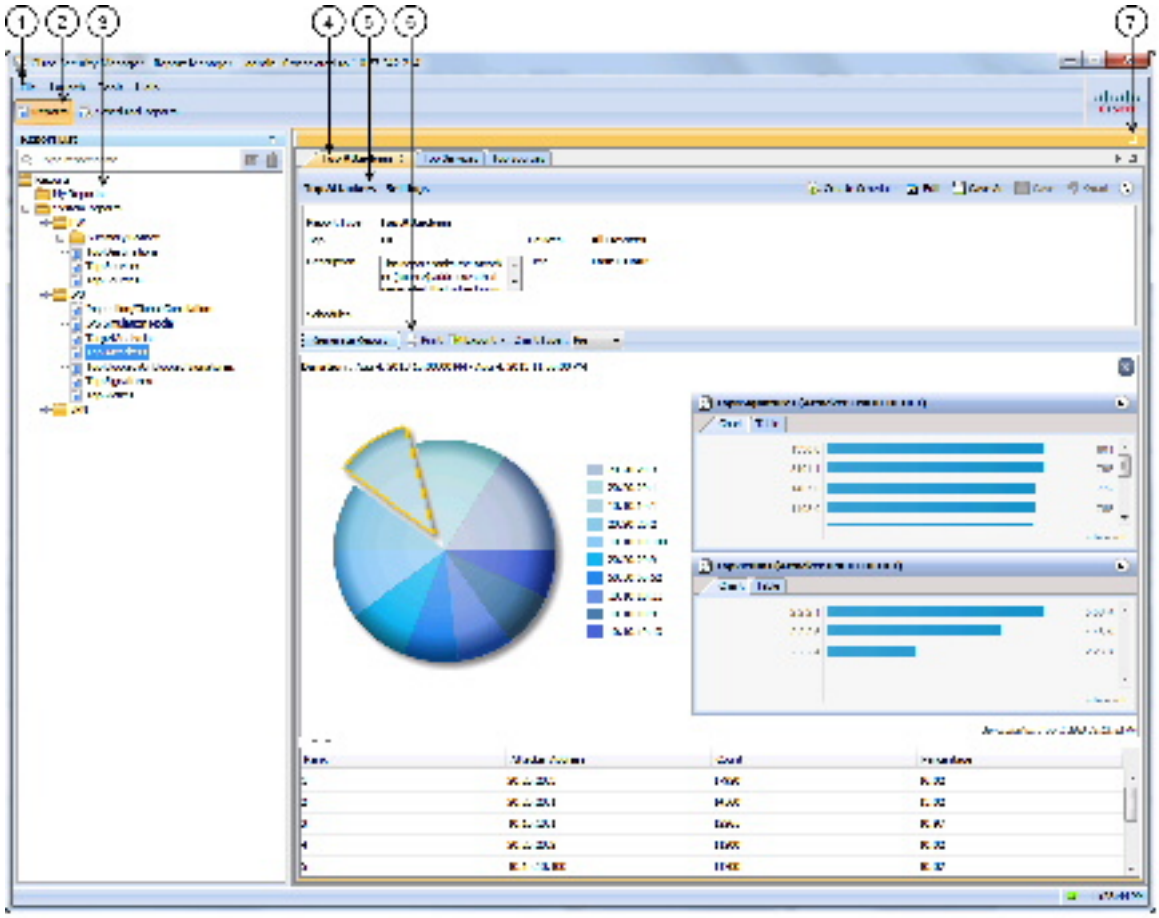
Report Manager を使用して、ASA デバイスと IPS デバイス、およびリモート アクセス IPsec と ASA デバイスでホストされる SSL VPN に関する、セキュリティおよび使用状況のレポートを作成します。サポートされるデバイス、および Report Manager を使用して生成できるレポートの詳細については、レポート管理について （3561 ページ）を参照してください。

Report Manager を開くには、次のいずれかを実行します。

- Windows のスタートメニューから [スタート（Start）] > [すべてのプログラム（All Programs）] > [Cisco Security Managerクライアント（Cisco Security Manager Client）] > [Report Manager] を選択するか（コマンドパスは異なる場合があります）、デスクトップの [Report Manager] アイコンをダブルクリックします。ログインを求められます。Cisco Security Manager クライアント アプリケーションの開始方法の詳細については、Security Manager へのログインおよび終了 （14 ページ）を参照してください。
- Configuration Manager アプリケーションまたはイベントビューア アプリケーションから **[起動（Launch）] > [Report Manager]** を選択します。他のアプリケーションへのログインに使用したアカウントと同じユーザ アカウントを使用して Report Manager が開きます。

次の図とその後のリストで、Report Manager の基本を説明します。

図 *65 : Report Manager* のメイン ウィンドウ



次のリストで、メイン Report Manager ウィンドウとそのコールアウトをさらに詳細に説明します。

- **メニューバー（1）**：Report Manager でアクションを実行するための一般的なコマンド。コマンドの説明については、Report Manager のメニュー （3571 ページ）を参照してください。
- **メインウィンドウのタブ（2）**：次のタブで構成されるメインウィンドウの領域：
  - [Reports]：[Reports] タブを使用して、オンデマンドでのレポートの生成、カスタム レポートの作成、およびその他のレポート指向タスクの実行を行います。上の図と、このトピックのほとんどの情報は、[Reports] タブに関連しています。[Reports] タブから実行できるタスクについては、Report Manager でのレポートの使用 （3585 ページ）を参照してください。
  - [Scheduled Reports]：[Scheduled Reports] タブを使用して、レポート スケジュールを表示および管理します。[Scheduled Reports] タブの詳細については、レポート スケジュールの表示 （3603 ページ）を参照してください。[Scheduled Reports] タブから実行でき

るタスクについては、レポートのスケジュール設定 （3603ページ）を参照してください。

- **レポートリスト（3）**：[レポート（Reports）] タブの左側のペインは、レポートのリストです。このリストはフォルダに編成されています。[System Reports] は事前定義レポートで、[My Reports] フォルダにはユーザが作成するカスタム レポートが含まれます。レポートをダブルクリックして開くか、レポートを選択して**[ファイル（File）]>[開く（Open）]**を選択するか、またはレポートを右クリックして [レポートを開く（Open Report）] を選択します。レポート リストの使用方法の詳細については、Report Manager のレポート リストについて （3572 ページ）を参照してください。
- **レポートペイン（4、5、6、7）**：[レポート（Reports）] タブの右側のペインには、開いているレポートが表示されます。開いている各レポートは別々のタブで表されます（開いているレポートは最大 5 つです）。このスペースにレポートを水平または垂直に配置可能で、別のウィンドウにレポートをフローティングすることも可能であることに注意してください。レポートの配置方法またはフローティング方法の詳細については、レポート ウィンドウの配置 （3599 ページ）を参照してください。

ペインの上の最大化コントロール（7）を使用して、そのペインがワークスペース全体を占めるようにする（レポートリストは非表示）ことができます。ペインの最大化後、コントロールはメイン ウィンドウを2つのペインで構成されるビューに戻すための復元コントロールに変わります。

右矢印と左矢印、および [Show List] アイコン ボタンを使用して、開いているレポート間のスクロール、またはレポートへの直接移動を行うことができます。ただし、目的のレポート名が表示されているタブをクリックすることが、レポートに移動する最も簡単な方法です。

レポート ペインには、開いている各レポートに対して次の領域が含まれています。

- - レポート設定ペイン（5）：レポートの上部には、レポートの生成に使用される基準であるレポート設定が表示されます。見出しをクリックするか、または展開/縮小アイコン ボタンをクリックすることにより、設定ペインを開閉できます。見出しには、レポートに対して実行できるコマンドが表示されているツールバーが含まれています。設定ペインの詳細については、レポート設定ペインについて （3573ページ）を参照してください。
  - 生成済みレポート ペインおよびレポート ツールバー（6）：設定ペインの下に、レポートデータの生成および操作に使用する追加のツールバーがあります。これらのコントロールを使用して、レポート設定で定義された基準を使用したレポートの生成、レポートの印刷、レポートの PDF 形式または CSV 形式へのエクスポート、またはレポートに表示されるグラフィックのタイプの変更を行います。

レポート ペインの下部は実際のレポートです。この領域は、[Generate Report] ボタンをクリックするまでは空です。レポートの上部には情報のグラフィカル表現が表示され、ページの下部には表形式のデータが表示されます。詳細については、「生成済みレポート ペインおよびツールバーについて （3575ページ）」および「レポートの起動と生成 （3586ページ）」を参照してください。

Report Manager のメニュー

次の表で、Report Manager のメニューのコマンドを説明します。

表 *979 : Report Manager* のメニューのリファレンス

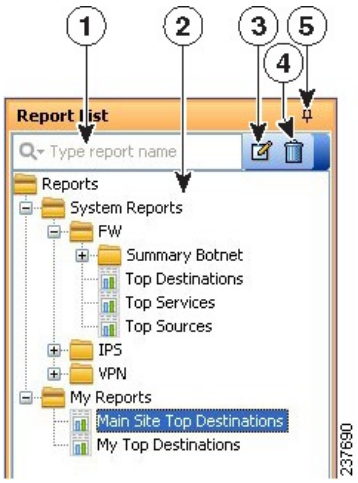
メニュー	コマンド	説明
ファイル（File）	オープン（Open）	[Reports] タブのレポートリストで選択されたレポートを開きます。レポートの起動と生成 （3586ページ）を参照してください。
	保存	レポート設定に対する変更内容を保存します。このコマンドは、カスタム レポートの場合にのみ使用できます。レポートの保存 （3600 ページ）を参照してください。
	名前を付けて保存	レポートを新規レポートとして保存します。このコマンドを使用して、既存のレポートから新規レポートを作成します。レポートの保存 （3600ページ）を参照してください。
	Close Report Close All Reports	アクティブな開いているレポートを閉じるか、または開いているレポートをすべて閉じます。レポート ウィンドウの終了 （3601 ページ）を参照してください。
	終了（Exit）	Report Manager を終了します。
ラウンチ	ダッシュボード 設定マネージャ（Configuration Manager） イベントビューア Health and Performance Monitor Image Manager	指定された Security Manager アプリケーションを開きます。
Tools	Default Report Settings	事前定義システム レポートのデフォルト設定を設定します。レポートのデフォルト設定値の設定 （3598ページ）を参照してください。
	Custom Report List	サーバに設定されているカスタム レポートを、ユーザが作成したものだけではなくすべて表示します。このウィンドウからレポートを管理できます。カスタム レポートの管理 （3602 ページ）を参照してください。

メニュー	コマンド	説明
ヘルプ	Help about this page	現在メイン ウィンドウに表示されているページに関連したトピックのオンライン ヘルプを開きます。
	About Report Manager	アプリケーションの著作権、バージョン、およびライセンス情報を表示します。

Report Manager のレポート リストについて

次の図に示すように、Report Manager の [Reports] タブの左側のペインには、使用可能なレポートのリストが表示されます。

図 *66 : Report Manager* のレポート リスト



レポート リストには、次のコントロールが含まれています（図のコールアウトで示されています）。

- **クイック フィルタ検索ボックス（1）**：クイックフィルタ検索ボックスを使用して、リスト内のレポートを検索します。入力すると、リストはフィルタリングされます。ただし、フォルダは自動的には開かれません。デフォルトでは、レポート名内の任意の位置にあるテキスト文字列を検索します。ただし、クイック フィルタ ボックスで下矢印をクリックすると、検索文字列の評価方法を変更するさまざまなオプションを選択できます。
- **レポートのリスト（2）**：このリストはフォルダに編成されています。システムレポートは事前定義レポート（Report Manager の事前定義システム レポートについて （3578 ページ）で説明）で、My Reports フォルダにはユーザが作成するカスタムレポートが含まれます。レポートをダブルクリックして開くか、またはレポートを選択して [ファイル（File）] > [開く（Open）] を選択します。詳細については、レポートの起動と生成 （3586 ページ）を参照してください。

- **右クリックのショートカットメニュー（表示されません）**：レポートを右クリックすると、レポートを開く、スケジュールを作成する、新規レポートとしてレポートを保存するなど、実行可能な追加のコマンドのリストが表示されます。
- **編集ボタン（3）**：[編集（Edit）]ボタンをクリックして、選択したカスタムレポートの名前を変更します。カスタム レポートのみを編集できます。詳細については、レポートの名前変更 （3601 ページ）を参照してください。
- **削除ボタン（4）**：[削除（Delete）]ボタンをクリックして、選択したカスタムレポートを削除します。カスタム レポートのみを削除できます。詳細については、レポートの削除（3602 ページ）を参照してください。
- **Push Pin ボタン（5）**：[プッシュピン（Push Pin）]アイコンをクリックして、レポートリストペインを開くか閉じるかを制御します。ピンが垂直である場合、レポートリストは開いたままです。ただし、レポートペイン（右側のペイン）を最大化する場合は除きます。ピンが水平である場合、レポート リストは左マージンに縮小され、リストを開くには左マージンでレポート リストの見出しをクリックする必要があります。

関連項目

- Report Manager の概要 （3568 ページ）
- レポート管理について （3561 ページ）
- Report Manager でのレポートの使用 （3585 ページ）
- レポート スケジュールの表示 （3603 ページ）
- レポートのスケジュール設定 （3603 ページ）
- レポート ウィンドウの配置 （3599 ページ）

レポート設定ペインについて

レポートが開いている場合、[Reports]タブの右側の上部にレポート設定が表示されます。これらの設定は、レポートの生成に使用する基準を定義します。次の図に、レポート設定ペインの例を示します。

図 *67 : Report Manager* のレポート設定

レポートリストには、次のコントロールが含まれています（図のコールアウトで示されています）。

- [レポート（Report）]タブ（3）：正確には設定の一部ではありませんが、各レポートは独自のタブに表示されます。これらの設定はタブの上部にあります。タブ自体を右クリックすると、レポート ウィンドウを配置できるようにするコマンドのメニューが表示されます。詳細については、レポート ウィンドウの配置 （3599 ページ）を参照してください。
- 見出しとツールバー（2）：設定ペインの上部には、見出し（たとえば、「Top Sources - Settings」）、および設定を操作するためのボタンの行が表示されています。見出しをクリックするか、またはツールバーの一番右側の上矢印ボタンをクリックすることにより、ペインを開閉できます。その他のボタンには、次の機能があります。
  - [Create Schedule] ボタン：これらの設定に基づいて自動的にレポートを生成する新規スケジュールを作成します。詳細については、レポート スケジュールの設定 （3604 ページ）を参照してください。

    [Edit] ボタン：レポート設定を編集します。詳細については、レポート設定の編集 （3589 ページ）を参照してください。
  - [Save As] ボタン：レポートを新規レポートとして保存します。事前定義システム レポートの設定を編集し、変更内容を保存する場合は、[Save As] を使用してカスタム レポートを作成する必要があります。詳細については、レポートの保存 （3600 ページ）およびカスタム レポートの作成 （3588 ページ）を参照してください。
  - [Save] ボタン：設定に対する変更内容を保存します。カスタム レポートの場合にのみ、変更内容を保存できます。詳細については、レポートの保存 （3600 ページ）を参照してください。
  - [Reset] ボタン：前回保存された値に設定をリセットします。
  - [Expand/Collapse] ボタン（二重の上矢印と下矢印）：レポート設定ペインの開閉を切り替えます。
- 設定表示（1）：見出しとツールバーの下には、レポート設定の概要が示されます。情報には、レポートのタイプ、レポートに含まれるデバイス、時間範囲、説明、レポートに定義されているスケジュール、およびレポートに固有のその他のプロパティが含まれます。

説明を変更するには、[Description] 編集ボックスに直接変更内容を入力します。

関連項目

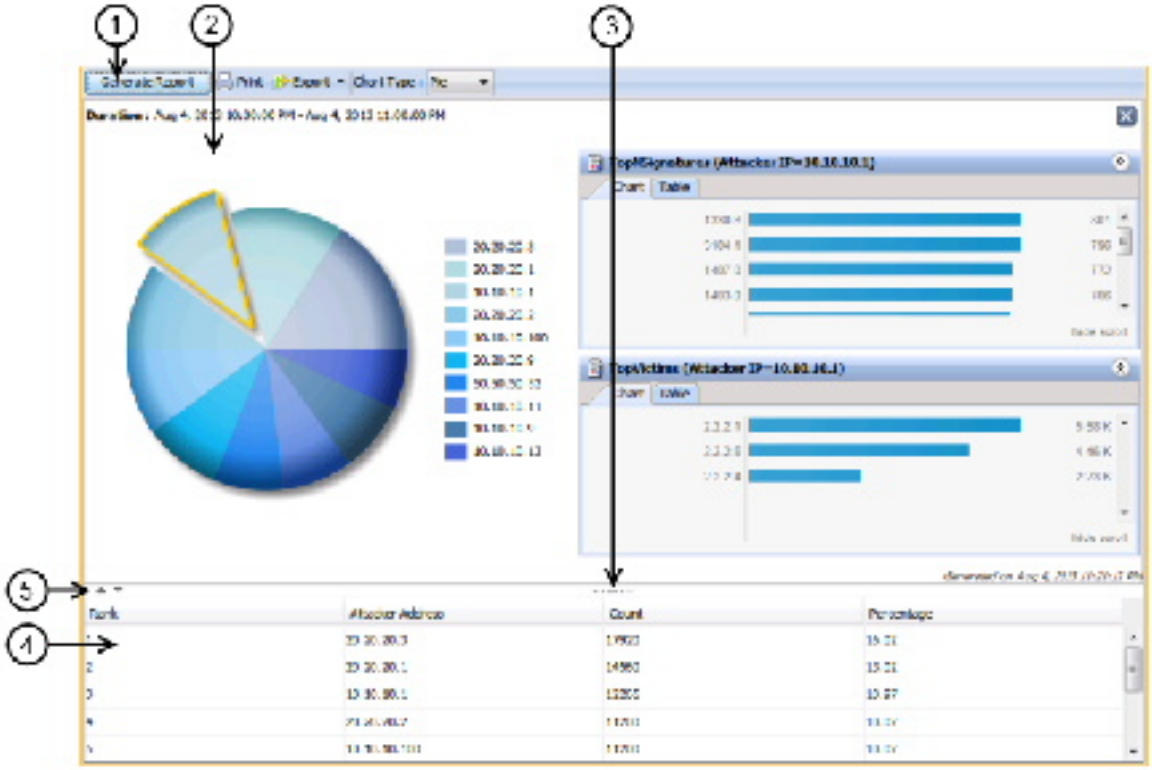
- レポートの起動と生成 （3586 ページ）
- 生成済みレポート ペインおよびツールバーについて （3575 ページ）
- Report Manager の概要 （3568 ページ）
- レポート管理について （3561 ページ）
- Report Manager でのレポートの使用 （3585 ページ）
- レポート スケジュールの表示 （3603 ページ）
- レポートのスケジュール設定 （3603 ページ）

生成済みレポート ペインおよびツールバーについて

レポートが開いている場合、[Reports] タブの右側の下部に生成済みレポートとレポート ツールバーが表示されます。このペインには、[Generate Report] ボタンをクリックした結果が表示されます。

次の図に、生成済みレポート ペインと関連ツールバーの例を示します。

図 *68 : Report Manager* の生成済みレポート ペインとツールバー



レポートリストには、次のコントロールが含まれています（図のコールアウトで示されています）。

- **レポートツールバー（1）**：生成済みレポートペインの上部に、レポートを生成および操作するためのコントロールの行があります。これらのコントロールには次の機能があります。
  - [Generate Report] ボタン：レポート設定（上部のペイン）で定義された基準に基づいてレポートを生成します。詳細については、レポートの起動と生成 （3586ページ）を参照してください。
  - [Print] ボタン：生成されたレポートを印刷します。詳細については、レポートの印刷（3595 ページ）を参照してください。
  - [Export] ボタン：レポートをエクスポートします。ボタンの下矢印をクリックして、作成するファイルのタイプを選択します。タイプは、[PDFとして（As PDF）]（Adobe Acrobat の場合）または [CSVとして（As CSV）]（カンマで区切られた値の場合）です。詳細については、レポートのエクスポート （3596ページ）を参照してください。
  - [Chart Type]：レポートの上部に表示されるグラフのタイプを決定します。一般には、円グラフ、棒グラフ、および XY（線形）グラフを使用できます。場合によっては、

一部のグラフ タイプを選択できないことがあります。詳細については、 レポートの起動と生成 （3586 ページ）を参照してください。

- **グラフィカルビュー（2、3、5）**：生成されたレポートの上部には、レポートデータが色分けされたグラフで表示され、また配色を示す凡例が含まれます。また、レポートが生成された日付と時刻も含まれています。

（注） 上位の宛先、上位のサービス、上位の送信元のファイアウォールレポートと上位の攻撃者、上位のシグネチャ、上位の被害者 IPS レポートでは、円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのデータポイントの詳細を表示できます。たとえば、上位のシグネチャレポートの円グラフのスライスをクリックすると、選択したシグネチャの上位の攻撃者と上位の被害者のレポートの詳細が表示されます。詳細については、 レポートデータへのドリルダウン （3593 ページ）を参照してください。

グラフィカル ビューの下部には、次のコントロールがあります。

- 上矢印と下矢印（5）：グラフィックの左側にあるこれらのアイコンボタンを使用すると、レポートのグラフィカル部分を開くこと、および閉じることができます。
- ウィンドウ サイズ コントロール（3）：ウィンドウの中央のグラフィックの下にある水平方向のダッシュの上にマウス ポインタを移動すると、ポインタをクリックして移動し、レポートのグラフィカル部分のサイズを変更できます。領域のサイズを拡大または縮小すると、グラフィックは自動的にサイズ変更されます。実際、テーブルの上部の任意の部分の上にマウス ポインタを移動すると、このコントロールにアクセスできます。
- **表形式のビュー（4）**：レポートの下部には、そのレポートに対して収集されたデータを表示するテーブルがあります。このデータはグラフィックの生成に使用されます。テーブルのカラムは、レポートのタイプによって異なります。

見出しをクリックして、テーブルをカラムでソートできます。3 つのソート順序があり、カラムの見出しをクリックすると、これらの順序が循環して切り替わります。矢印が、昇順（上矢印）、降順（下矢印）、およびソートなし（空）の、各ソート順序を示します。Ctrl を押した状態でクリックすると、別のカラムに別のソート順序を作成できます。これは、最初のソートカラムで1つ以上のエントリが繰り返される場合にのみ効果があります。番号は、そのカラムが 1 番め、2 番め、3 番めなどの、どのソート基準であるかを示しています。

関連項目

- レポート設定ペインについて （3573 ページ）
- Report Manager の概要 （3568 ページ）
- レポート管理について （3561 ページ）
- Report Manager でのレポートの使用 （3585 ページ）
- レポート スケジュールの表示 （3603 ページ）

- レポートのスケジュール設定 （3603 ページ）

Report Manager の事前定義システム レポートについて

Report Manager にはいくつかの事前定義システム レポートが組み込まれており、ネットワークの分析に使用できます。これらのレポートをカスタマイズして、特定のデバイスと期間の集合に焦点を当てたり、その他の設定可能パラメータに焦点を当てたりすることができます。

ここでは、次の内容について説明します。

- ファイアウォール トラフィック レポートについて （3578 ページ）
- ファイアウォール サマリー ボットネット レポートについて （3579 ページ）
- VPN 上位レポートについて （3580 ページ）
- 全般 VPN レポートについて （3581 ページ）
- IPS 上位レポートについて （3583 ページ）
- 全般 IPS レポートについて （3585 ページ）

ファイアウォール トラフィック レポートについて

Report Manager には、ファイアウォール ACL イベントの上位の宛先、サービス、およびソースの識別に使用できる事前定義システム レポートが組み込まれています。この統計情報は、Event Manager サービスで収集されるイベント（Event Viewer に表示されるイベント）に基づいています。

[システムレポート（System Reports）] > [FW] フォルダで、以下のレポートを使用できます。

- [上位の宛先（Top Destinations）]：このレポートでは、Cisco Security Manager によって受信されたすべての built/deny ファイアウォールイベントのセッションの宛先がランク付けされます。このレポートには、宛先 IP アドレス、各アドレスに対するイベント数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の宛先を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その宛先に関連付けられた上位の送信元と上位のサービスに関するレポート情報を表示できます（レポートデータへのドリルダウン （3593ページ）を参照）。
- [上位の送信元（Top Sources）]：このレポートでは、Cisco Security Manager によって受信されたすべての built/deny ファイアウォールイベントのセッションの送信元がランク付けされます。このレポートには、送信元 IP アドレス、各アドレスに対するイベント数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の送信元を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その送信元に関連付けられた上位の宛先と上位のサービスに関するレポート情報を表示できます（レポートデータへのドリルダウン （3593ページ）を参照）。

- [上位のサービス（Top Services）]：このレポートでは、Cisco Security Manager によって受信されたすべての built/deny ファイアウォールイベントの宛先サービスがランク付けされます。TCP サービスおよび UDP サービスにはポート番号が含まれています。このレポートには、サービス、各サービスに対するイベント数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定のサービスを表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのサービスに関連付けられた上位の宛先と上位の送信元に関するレポート情報を表示できます（レポートデータへのドリルダウン （3593 ページ）を参照）。

レポートに含めるアドレスまたはサービスの数およびレポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （3598 ページ）で説明されているようにシステム デフォルトで定義されます。

レポート設定の編集およびレポートのカスタムバージョンの作成を行うこともできます。次のトピックで説明されているように、レポートを絞り込んで、ソースアドレス、宛先アドレス、またはサービスの特定の集合に焦点を当てたり、アクションの許可または拒否のみに焦点を当てたり、ファイアウォールデバイスのサブセットに焦点を当てるようにレポートを制限したりすることができます。

- レポート設定の編集 （3589 ページ）
- カスタム レポートの作成 （3588 ページ）

ファイアウォール サマリー ボットネット レポートについて

Report Manager には、ボットネット トラフィック フィルタリングの分析に使用できる事前定義システム レポートが組み込まれています。この統計情報は、ブロックリストおよびグレーリストにあるサイトについて Event Manager サービスで収集されるボットネットイベント（Event Viewer に表示されるイベント）に基づいています。

ボットネットの詳細については、Botnet Traffic Filter について （1163 ページ）を参照してください。

[システムレポート（System Reports）] > [FW] > [サマリーボットネット（Summary Botnet）] フォルダで、次のレポートを使用できます。

- **上位感染ホスト（Top Infected Hosts）**：このレポートは、Security Manager によって受信されたすべてのボットネットイベントに基づいて、感染したホストからブラックリストまたはグレーリストのサイトへのトラフィックについて上位感染ホストをランク付けします。このレポートには、感染したホストの IP アドレスとそのイベントが検出されたファイアウォールインターフェイス名（カッコ内）、各アドレスについてブロックリストまたはグレーリストのサイトに記録された接続数のカウント、ボットネットトラフィックフィルタリングによってブロックされた（ドロップされた）接続数のカウント、およびレポート内のすべてのカウントの合計に比較したカウントのパーセンテージが表示されます。
- **上位マルウェアポート（Top Malware Ports）**：このレポートは、Security Manager によって受信されたすべてのボットネットイベントに基づいて、感染したホストからブラックリストまたはグレーリストのサイトへのトラフィックについて上位宛先ポートをランク付け

します。このレポートには、宛先マルウェアポート、各ポートについてブロックリストまたはグレーリストのサイトに記録された接続数のカウント、ボットネット トラフィック フィルタリングによってブロックされた（ドロップされた）接続数のカウント、およびレポート内のすべてのカウントの合計に比較したカウントのパーセンテージが表示されます。

- **上位マルウェアサイト（Top Malware Sites）**：このレポートは、Security Manager によって受信されたすべてのボットネットイベントに基づいて、すべてのインバウンドセッションとアウトバウンドセッションについて、上位ボットネットサイト（ブラックリストまたはグレーリストのサイト）をランク付けします。このレポートには、次の情報が表示されます。
  - IP アドレス（IP Address）：ボットネットイベントで悪意のあるホストとして示されている IP アドレス（ブロックリストまたはグレーリストのいずれか）。
  - マルウェア サイト（Malware Site）：動的なフィルタ データベースに登録されていて、トラフィックの宛先となったドメイン名または IP アドレス。
  - リストサイト（List Type）：サイトがブラックリストまたはグレイリストのどちらにあるか。
  - 記録された接続数（Connections Logged）：各サイトについて記録またはモニタされた接続数のカウント。
  - ブロックされた接続数（Connections Blocked）：各サイトについてボットネット トラフィック フィルタリングによってブロックされた（ドロップされた）接続数のカウント。
  - 脅威レベル（Threat Level）：サイトのボットネット脅威レベル（「非常に低い」から「非常に高い」まで、または「なし」）。
  - カテゴリ（Category）：ボットネットデータベースに定義されている、サイトが引き起こす脅威のカテゴリ（ボットネット、トロイの木馬、スパイウェアなど）。

レポート内のホスト数、ポート数、またはサイト数、およびレポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （3598ページ）で説明されているように、システムデフォルトで定義されています。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタム バージョンの作成を行うこともできます。

- レポート設定の編集 （3589 ページ）
- カスタム レポートの作成 （3588 ページ）

VPN 上位レポートについて

Report Manager には、帯域幅使用状況、ネットワークへの接続期間、およびデータ スループットに基づいて、上位のリモート アクセス VPN ユーザを識別するために使用される事前定義システム レポートが組み込まれています。ユーザによる接続のタイプに基づいて、別々のレポートが提供されます。

これらのレポートは、**AnyConnect（SSL）リモートアクセス VPN**、**Cisco VPN Client（IPsec）リモートアクセス VPN**、および**クライアントレス SSL VPN** の [システムレポート（System Reports）] > [VPN] フォルダで使用できます。

次のレポートは各フォルダで使用できます。各レポートはフォルダ名で示される接続タイプに固有です。接続タイプはレポート名のカッコ内にも含まれています。

- **帯域幅が上位のユーザー（Top Bandwidth Users）**：このレポートは、帯域幅消費量が最大である VPN ユーザーをランク付けします。このレポートには、ユーザ名、合計送受信バイト数での帯域幅、および報告された各ユーザによる使用帯域幅のパーセンテージが表示されます。
- **接続時間が上位のユーザー（Top Duration Users）**：このレポートは、ネットワークへの接続時間が最も長かった VPN ユーザーをランク付けします。このレポートには、ユーザー名、*days hours:minutes:seconds* という形式での接続時間、および報告された各ユーザーの期間のパーセンテージが表示されます。チャートには、期間は秒単位で表示されます。
- **スループットが上位のユーザー（Top Throughput Users）**：このレポートは、最高のスループットレートでデータを送受信した VPN ユーザーをランク付けします。このレポートには、ユーザ名、各ユーザのスループット（kbps 単位）、および報告された各ユーザのスループットのパーセンテージが表示されます。スループットは、8.0 *（バイト単位でのユーザの帯域幅）/（秒単位でのユーザの接続時間 * 1000.0）として計算されます。

レポートに含めるユーザ数およびレポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （3598ページ）で説明されているようにシステムデフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタム バージョンの作成（特定のユーザに焦点を当てることも含む）を行うこともできます。

- レポート設定の編集 （3589 ページ）
- カスタム レポートの作成 （3588 ページ）

全般 VPN レポートについて

Report Manager には、ネットワークにおける一般的なリモート アクセス VPN 使用状況の分析に使用できる事前定義システム レポートが組み込まれています。これらのレポートは、VPN で使用される接続タイプに固有ではありません。

[システムレポート（System Reports）] > [VPN] フォルダで、次のレポートを使用できます。

- **接続プロファイルレポート**：このレポートは、各リモートアクセス接続プロファイルのユーザ数、セッション、帯域幅使用率とスループット使用状況の概要を提供します。

デフォルトのレポートには、直前の 1 時間のすべてのデバイスに関するこの情報が含まれます。レポートは、さまざまな方法でカスタマイズできます（レポート設定の編集 （3589 ページ）を参照）。

- **ユーザレポート**：このレポートは、各リモートアクセス VPN ユーザの帯域幅使用率、接続時間、およびスループット使用状況の概要を提供します。このレポートには、ユーザ

名、合計送受信バイト数での帯域幅、*days hours:minutes:seconds* 形式での接続時間、および各ユーザのスループット（kbps）が表示されます。スループットは、8.0 *（バイト単位でのユーザの帯域幅）/（秒単位でのユーザの接続時間 * 1000.0）として計算されます。

Security Manager 4.7 以降、ユーザレポートは**ユーザレベルの詳細**と**セッション レベルの詳細**の両方を提供します。

- • **ユーザレベルの詳細**：**ユーザレベルの詳細**は、特定のユーザーについて、ユーザのすべてのセッションの合計値（ユーザー名、セッション合計数、帯域幅、期間、およびスループット）を表します: 。

（注） Cisco Security Manager 4.13 以降、パブリック IP および割り当てられた IP の詳細は、一般的な VPN レポートのユーザレベルの詳細の一部としても表示されます。

- • **セッションレベルの詳細**：ツリーを展開すると、特定のユーザが VPN 接続を持つ各セッションについて**セッションレベルの詳細**が表示されます。セッションレベルの詳細には、セッション ID、ログイン時間、ログアウト時間、帯域幅、スループット、およびセッションの期間が含まれます。（ここで、ログアウト時間は、式**ログアウト時間 = ログイン時間 + 期間**を使用して計算されます。)

デフォルト レポートには、すべての接続テクノロジーとすべてのユーザの情報が含まれています。単一のテクノロジー タイプまたは 1 つ以上の特定ユーザに焦点を当てるようにレポートをカスタマイズできます（ レポート設定の編集 （3589 ページ）を参照）。

ユーザレポートの [条件（Criteria）] セクションには、テクノロジー（すべて、クライアントレス、フルクライアント、および IPSec RA）、ユーザー名、およびユーザーセッション時間（<=、>= （時間））のフィルターがあります。

- **VPN デバイス使用率レポート**：このレポートは、リモートアクセス VPN 接続をホストする各デバイスの使用率の統計の概要を提供します。このレポートには、デバイス（Security Manager の表示名を使用）、レポート時間範囲内の任意の時点における VPN へのログインユーザの平均数、VPN のすべてのユーザの合計帯域幅（バイト）（送信および受信）、*days hours:minutes:seconds* 形式の合計接続時間、およびこのレポート期間内の任意の時点における平均スループット（ kbps）が表示されます。

デフォルト レポートには、すべての接続テクノロジーの情報が含まれています。単一のテクノロジー タイプに焦点を当てるようにレポートをカスタマイズできます（ レポート設定の編集 （3589 ページ）を参照）。

レポート期間の定義に使用されるパラメータは、 レポートのデフォルト設定値の設定 （3598 ページ）で説明されているようにシステムデフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタムバージョンの作成を行うこともできます。

- レポートのデフォルト設定値の設定 （3598 ページ）

- カスタム レポートの作成 （3588 ページ）

IPS 上位レポートについて

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Report Manager には、ネットワーク内の IPS アラートの攻撃者、攻撃対象、およびシグニチャの分析に使用できる事前定義システム レポートが組み込まれています。

[システムレポート（System Reports）] > [IPS] フォルダで、次のレポートを使用できます。

- [上位攻撃者（Top Attackers）]：このレポートは、記録された IPS アラート数が最も多い攻撃者（送信元）のアドレスをランク付けします。このレポートには、攻撃者 IP アドレス、各アドレスに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の攻撃者を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その攻撃者に関連した上位のシグニチャと上位の攻撃対象に関するレポート情報を表示できます（レポートデータへのドリルダウン （3593 ページ）を参照）。

デフォルト レポートには、ブロックされたアクションとブロックされなかったアクションの両方について、すべての攻撃者、攻撃対象、およびシグニチャの情報が含まれています。攻撃者、攻撃対象、またはシグニチャのサブセットに焦点を当てるようにレポートをカスタマイズしたり、ブロックされたアクションのみ、またはブロックされなかったアクションのみに分析を制限したりすることができます（ レポート設定の編集 （3589 ページ）を参照）。

- [上位攻撃対象（Top Victims）]：このレポートは、記録された IPS アラート数が最も大きい攻撃対象（宛先）のアドレスをランク付けします。このレポートには、攻撃対象アドレス、各アドレスに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定の攻撃対象を表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、その攻撃対象に関連した上位のシグニチャと上位の攻撃者に関するレポート情報を表示できます（レポートデータへのドリルダウン （3593 ページ）を参照）。

デフォルト レポートには、ブロックされたアクションとブロックされなかったアクションの両方について、すべての攻撃者、攻撃対象、およびシグニチャの情報が含まれています。攻撃者、攻撃対象、またはシグニチャのサブセットに焦点を当てるようにレポートをカスタマイズしたり、ブロックされたアクションのみ、またはブロックされなかったアクションのみに分析を制限したりすることができます（ レポート設定の編集 （3589 ページ）を参照）。

- [上位シグニチャ（Top Signatures）]：このレポートは、発行したアラートの数が最も大きいシグニチャをランク付けします。このレポートには、シグニチャ ID 番号、シグニチャの名前、各シグニチャに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。特定のシグニチャを表す円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのシ

グニチャに関連した上位の攻撃対象と上位の攻撃者に関するレポート情報を表示できます（レポートデータへのドリルダウン （3593 ページ）を参照）。

デフォルト レポートには、ブロックされたアクションとブロックされなかったアクションの両方について、すべての攻撃者、攻撃対象、およびシグニチャの情報が含まれています。攻撃者、攻撃対象、またはシグニチャのサブセットに焦点を当てるようにレポートをカスタマイズしたり、ブロックされたアクションのみ、またはブロックされなかったアクションのみに分析を制限したりすることができます（レポート設定の編集 （3589 ページ）を参照）。

- [上位ブロック/非ブロックシグニチャ（Top Blocked/Unblocked Signatures）]：このレポートは、ブロックした攻撃者の数が最も大きいシグニチャをランク付けします。このレポートには、シグニチャ ID 番号、シグニチャの名前、各シグニチャに対するアラート数のカウント、およびレポート内のすべてのカウントの合計と比較したそのカウントのパーセンテージが表示されます。

デフォルト レポートには、ブロックされたアクションのみが表示されます。ただし、ブロックされなかったアクションのみ、またはブロックされたアクションとブロックされなかったアクションの組み合わせを表示するように、レポートをカスタマイズできます（レポート設定の編集 （3589 ページ）を参照）。

特定の攻撃者または攻撃対象のアドレス、またはシグニチャのサブセットに制限されたブロック リストまたは非ブロック リストを表示する場合は、上位ブロック/非ブロック シグニチャ（Top Blocked/Unblocked Signatures）レポートではなく上位シグニチャ（Top Signatures）レポートを使用します。ブロックされたシグニチャのみ、またはブロックされなかったシグニチャのみを表示するようにレポートをカスタマイズします。

- [IPSターゲット分析（IPS Target Analysis）：このレポートは、シグニチャおよび攻撃の頻度による上位ターゲットを提示します。このレポートには、アラートを生成したシグニチャ、アラートの数、および攻撃対象 IP アドレスが表示され、[Top Signatures] レポートと [Top Victims] レポートの集約ビューに基づいています。このレポートには、最大で 10 個のシグニチャと 5 個の攻撃者が含まれています。情報は散布図にプロットされます。これは、そのレポートに対して使用できる唯一のグラフィカル表現です。

レポートに含めるアドレスまたはシグニチャの数およびレポート期間の定義に使用されるパラメータは、レポート スケジュールの設定 （3604 ページ）で説明されているようにシステム デフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタム バージョンの作成を行うこともできます。

- レポート設定の編集 （3589 ページ）
- カスタム レポートの作成 （3588 ページ）

全般 IPS レポートについて

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

Report Manager には、ネットワークにおける一般的な IPS アクティビティの分析に使用できる事前定義システム レポートが組み込まれています。

[システムレポート（System Reports）] > [IPS] フォルダで、次のレポートを使用できます。

- [検査/グローバル相関（Inspection/Global Correlation）]：このレポートでは、グローバル相関によって生成されたアラートと従来の IPS 検査によって生成されたアラートの比較が示されます。このレポートには、IPS 検査方式（グローバル相関または検査のいずれか）あたりのアラートの数およびパーセンテージが表示されます。
- [IPSシミュレーションモード（IPS Simulation Mode）]：このレポートでは、インライン（IPS）モードと無差別（IDS または IPS シミュレーション）モードのアラートの比較が示されます。このレポートには、モードに基づくアラートの数とパーセンテージが表示されます（非シミュレーション カウント（インライン）またはシミュレーション モード カウント（無差別）のいずれか）。IPS センサーは、無差別モードで発生する攻撃を直接ブロックすることはできません。

IPS イベントを処理する際、Cisco Security Manager の Report Manager コンポーネントはイベントを個別に報告します。 Cisco Security Manager のイベント ビューア コンポーネントにアラートが表示されます。イベント ビューア コンポーネントで、IPS Summarizer はイベントを単一のアラートにグループ化するため、IPS センサーが送信するアラートの数が減少します。

ヒント Cisco IPS Manager Express（IME）と Cisco Security Manager は、まったく同じ方法ではイベントを要約しません。

レポート期間の定義に使用されるパラメータは、レポートのデフォルト設定値の設定 （3598 ページ）で説明されているようにシステムデフォルトで定義されます。次のトピックで説明されているように、レポート設定の編集およびレポートのカスタムバージョンの作成を行うこともできます。

- レポート設定の編集 （3589 ページ）
- カスタム レポートの作成 （3588 ページ）

Report Manager でのレポートの使用

Report Manager アプリケーションを使用して、デバイス、およびリモート アクセス IPsec と SSL VPN に関する、セキュリティおよび使用状況のレポートを表示します。次のトピックで、

レポート作成の基本を説明します。レポート スケジュールの使用については、 レポートのスケジュール設定 （3603 ページ）を参照してください。

ここでは、次の内容について説明します。

- レポートの起動と生成 （3586 ページ）
- カスタム レポートの作成 （3588 ページ）
- レポート設定の編集 （3589 ページ）
- レポートデータへのドリルダウン （3593 ページ）
- レポートの印刷 （3595 ページ）
- レポートのエクスポート （3596 ページ）
- レポートのデフォルト設定値の設定 （3598 ページ）
- レポート ウィンドウの配置 （3599 ページ）
- レポートの保存 （3600 ページ）
- レポートの名前変更 （3601 ページ）
- レポート ウィンドウの終了 （3601 ページ）
- レポートの削除 （3602 ページ）
- カスタム レポートの管理 （3602 ページ）

レポートの起動と生成

レポートはスタティックではありません。レポートを開くと、そのレポートの生成に使用するデータを定義する設定は含まれていますが、レポートにデータは含まれていません。したがって、レポートを表示するには、レポートを開いてから生成する必要があります。この手順では、このプロセスを説明します。

関連項目

- Report Manager の概要 （3568 ページ）
- カスタム レポートの作成 （3588 ページ）
- レポート ウィンドウの配置 （3599 ページ）
- Report Manager のトラブルシューティング （3607 ページ）

ステップ 1 Report Manager で、次のいずれかを実行してレポートを開きます。

- レポート リスト（左側のペイン）内のレポートの名前をダブルクリックします。
- レポートリスト内のレポートを選択し、[ファイル（File）] > [開く（Open）] を選択します。

- レポートリスト内のレポートを右クリックし、[レポートを開く（Open Report）] を選択します。

レポート設定ペインが開いていてレポート コンテンツ領域が空の状態で、レポートが開きます。

ヒント 同時に開いていることができるレポートは、最大で 5 つです。設定ツールバーの任意の領域（別の機能を実行するボタンではない領域）をクリックすることにより、レポート設定ペインを縮小して、生成されたレポートを表示するための領域を増やすこともできます。

ステップ 2 （任意）レポート設定に目的の値（たとえば、レポートに対する目的の時間枠）が含まれていることを確認します。システム レポートの設定値は、システム デフォルト（レポートのデフォルト設定値の設定（3598 ページ）の説明に従って設定可能）に基づいています。カスタム レポートの設定値は、そのレポートに対して前回保存された設定値です。

設定を変更する必要がある場合は、設定ツールバーで [編集（Edit）] ボタンをクリックし、[設定の編集（Edit Settings）] ダイアログボックスで変更します。詳細については、レポート設定の編集 （3589 ページ）を参照してください。

ヒント 変更内容を永続的にする場合は、必ずその変更内容を保存してください。システム レポートの設定値を変更して保持する場合は、[Save As] を使用して新規カスタム レポートを作成する必要があります。システム レポートの設定値をデフォルト設定値から変更することはできません。

ステップ 3 設定ペインの下にある [レポートの生成（Generate Report）] ボタンをクリックして、レポートデータベースからレポートデータを取得し、取得した情報を表示します。この情報は次の 2 つの形式で表示されます。

- グラフィカル：レポートの上部に、データのグラフィカル表現が表示されます。レポートデータの上の [チャート（Chart）] メニューから、さまざまなタイプのグラフを選択できます（円グラフ、XY（線形グラフの場合）、または棒グラフ）。レポートに 10 項目よりも多い項目が含まれている場合（たとえば、25 個の値を表示するように上位レポートを設定した場合）、10 番目以降の値はすべて、チャートでは「others」として要約表示されます。

（注） 上位の宛先、上位のサービス、上位の送信元のファイアウォールレポートと上位の攻撃者、上位のシグネチャ、上位の被害者 IPS レポートでは、円グラフ、XY グラフ、または棒グラフのデータポイントをクリックして、そのデータポイントの詳細を表示できます。たとえば、上位のシグネチャレポートの円グラフのスライスをクリックすると、選択したシグネチャの上位の攻撃者と上位の被害者のレポートの詳細が表示されます。詳細については、レポートデータへのドリルダウン （3593 ページ）を参照してください。

IPS ターゲット分析（IPS Target Analysis）レポートなどの一部のレポートは、散布図を使用します。これらのレポートの場合、別のグラフィック タイプを選択するオプションはありません。

- 表形式：グラフィックの下のテーブルには、グラフィックの生成に使用されたデータがリストされます。テーブルのカラムは、レポートのタイプに基づいて異なります。以下に、いくつかの一般的なカラムを示します。各レポートの内容の詳細については、Report Manager の事前定義システム レポートについて （3578 ページ）を参照してください。
  - [Rank]：情報の順序は大きさ順。たとえば、ファイアウォール上位宛先レポートの場合、ランク 1 は、その宛先が評価対象イベントで最も使用されていることを示しています。

- （レポート対象の特性の名前）：レポートでターゲットとする特性に基づく名前を持つカラムが必ず存在します。たとえば、[Source/Destination]（IP アドレス）、[Service]（プロトコルおよびポート）、または [User]（ユーザ名）などです。
- [Count]：その項目がイベントまたは関連統計情報に現れる回数。
- [Percentage]：報告された特性の、レポート内のその特性の総計に対する比率。この比率は、レポートに含まれる数値のみが含まれます。したがって、たとえば、上位 10 件のレポートと上位 25 件のレポートで、同じ項目に対して異なるパーセンテージが得られる可能性があります。

ステップ 4 （任意）必要に応じて、レポートの印刷、または PDF ファイルまたは Comma-Separated Values（CSV; カンマ区切り値）ファイルへのエクスポートを行うことができます。

- レポートを印刷するには、[印刷（Print）] ボタンをクリックしてプリンタを選択します。詳細については、レポートの印刷 （3595 ページ）を参照してください。
- レポートをエクスポートするには、[エクスポート（Export）] ボタンをクリックしてファイルタイプ（PDF または CSV）を選択します。詳細については、レポートのエクスポート （3596 ページ）を参照してください。

ヒント レポートを閉じるときに、レポート データは保持されません。表示されている情報を保持する場合は、レポートを印刷またはエクスポートする必要があります。

カスタム レポートの作成

通常の分析または表現を必要とする特定の特性をターゲットとするカスタム レポートを作成できます。たとえば、さまざまなファイアウォール デバイスのグループに対して別々の上位宛先（Top Destination）ファイアウォール レポートを作成し、別々の物理サイトのアクティビティを別々に分析できるようにすることができます。カスタム レポートを使用して、通常は上位レポートに含まれないソース、宛先、またはサービスを分析することもできます。

ヒント 新規に作成されたカスタム レポートでデータを使用できるまでに最大 1 時間かかる可能性があります。レポートの作成後にレコードが見つからないというメッセージが表示される場合は、1 時間待ってから、レポートの期間が直前の 1 時間（Last 1 Hour）であることを確認してください。

関連項目

- レポートの起動と生成 （3586 ページ）
- Report Manager の概要 （3568 ページ）

ステップ 1 レポート リストで、カスタム レポートが基づくレポートを選択します。レポートをダブルクリックするか、レポートを選択して [ファイル（File）] > [開く（Open）] を選択するか、右クリックして [レポートを開く（Open Report）] を選択して、レポートを開きます。

ステップ 2 設定ツールバーで [編集（Edit）]（鉛筆）ボタンをクリックし、[設定の編集（Edit Settings）] ダイアログボックスを開きます。

（注） レポート リストの上の [Edit] ボタンはクリックしないでください。その [Edit] ボタンでは、レポートの名前のみを変更できます。

[Edit Settings] ダイアログボックスは、2 つのペインに分かれています。左側のペインには使用可能な設定ページがリストされ、右側のペインには左側のペインで選択されているページの設定が表示されます。

ステップ 3 目的のレポート パラメータを定義するように設定値を設定します。詳細については、レポート設定の編集（3589 ページ）を参照してください。

ステップ 4 設定ツールバーで [名前を付けて保存（Save As）] ボタンをクリックするか、[ファイル（File）] > [名前を付けて保存（Save As）] を選択します。

ステップ 5 レポートの名前と説明（任意）を入力し、[OK] をクリックします。

レポート名は最大 64 文字で、英数字、スペース、ハイフン（-）、および下線文字（_）を含みます。説明には、最大 1024 文字を使用できます。

レポート設定の編集

レポートの生成に使用する基準を定義する設定を変更できます。カスタム レポートの場合、変更内容を保存できます。

事前定義システム レポートの場合、変更内容を直接保存することはできません。代わりに、[Save As] を使用して、更新された設定を使用する新規カスタム レポートを作成できます。また、レポートのデフォルト設定値の設定 （3598ページ）で説明されているように、レポート設定を編集するのではなく、すべての事前定義システム レポートで使用されるデフォルト設定を変更することもできます。

関連項目

- レポートの起動と生成 （3586 ページ）
- Report Manager の概要 （3568 ページ）
- カスタム レポートの作成 （3588 ページ）
- Report Manager データ集約について （3565 ページ）
- レポート ウィンドウの配置 （3599 ページ）

ステップ 1 Report Manager で、設定を変更するレポートを開きます。レポートをダブルクリックして開くか、レポートをダブルクリックして[ファイル（File）]>[開く（Open）]を選択するか、またはレポートを右クリックして [レポートを開く（Open Report）] を選択します。

レポートの上部に設定ペインが開いた状態で、レポートが開きます。設定ペインには、レポートのタイプ、レポートに含まれるデバイス、時間範囲、説明、レポートに対して定義されているスケジュール、およびそのレポートに固有のその他のプロパティが表示されます。

ステップ 2 （任意）レポート設定ペインの [Description] 編集ボックスに入力することにより、説明を変更します。

ステップ 3 設定ツールバーで [編集（Edit）]（鉛筆）ボタンをクリックし、[設定の編集（Edit Settings）] ダイアログボックスを開きます。

（注） レポートリストの上の [Edit] ボタンはクリックしないでください。その [Edit] ボタンでは、レポートの名前のみを変更できます。

[Edit Settings] ダイアログボックスは、2 つのペインに分かれています。左側のペインには使用可能な設定ページがリストされ、右側のペインには左側のペインで選択されているページの設定が表示されます。

ステップ 4 次のように、目的のページで設定を編集します。

- [デバイス（Devices）]：レポートに含めるモニタ対象デバイスを変更します。デフォルトは[すべてのデバイス（All Devices）] です。

モニタ対象デバイスのサブセットをレポートに反映させる場合は、[デバイスのフィルタ（Filter Devices）] を選択し、リストから目的のデバイスを選択するか、コンテキストを作成します。デバイスがイタリック体である場合、そのデバイスが現在は Event Viewer でモニタ対象として選択されていないことを意味します。これらのデバイスを選択すると、そのデバイスが選択された期間にモニタリングされた場合はレポートにそのデバイスのデータが組み込まれます。フォルダを選択して、フォルダ内のすべてのデバイスを選択できます。

デバイス リストは、適切なタイプのデバイスのみを表示するように事前にフィルタリングされます。たとえば、ファイアウォール レポートの設定を編集している場合、IPS デバイスは選択可能なデバイスのリストに表示されません。

（注） Cisco Security Manager 4.10 以降では、ASA 9.5(2) 以降で作成されたすべてのコンテキストが [デバイスのフィルタ（Filter Devices）] の下にリストされます。

- [時間（Time）]：レポートに含めるイベントとデータの選択に使用する期間を変更します。時間は Security Manager サーバの時間に基づいています。次のいずれかのオプションを選択して、期間を定義します。
  - [Last 1 Hour]：00 分から始まる直前の 1 時間全体。たとえば、現在の時刻が午前 11:45 である場合、直前の 1 時間（Last 1 Hour）のレポートには 10:00 から 11:00 までのデータが表示されます。
  - [Last 1 Day]：直前の 1 日全体（0 時から 0 時まで）。たとえば、現在の日付が火曜日である場合、直前の 1 日（Last 1 Day）のレポートには月曜日のデータが表示されます。
  - [Last 1 Week]：前の月曜日から日曜日まで。

- [Last 1 Month]：前月。たとえば、現在の日付が 9 月 29 日である場合、直前の 1 か月（Last 1 Month）のレポートには 8 月のデータが表示されます。
- [Custom]：[Start Date] カレンダーと [End Date] カレンダーを使用して、そのレポートに対する目的の開始時刻と終了時刻を選択します。カレンダー ウィジェットで、下矢印をクリックして目的の日時を選択し、[OK] をクリックします。レポート可能なデータは 90 日間保持されます。したがって、90 日よりも前にさかのぼる日付は選択できません。さらに、5 日間を超えてさかのぼる開始日を選択すると、時刻を指定できません。開始日に現在の日付を選択する場合、開始日と終了日両方の分の値も指定できますが、レポート データは 15 分ごと（各正時からの時間で 00 分、15 分、30 分、および 45 分）に集約されるため、分のエントリはこれらの数値で最も近い値に丸められます。許可される時間選択は、Report Manager データ集約について （3565 ページ）で説明されているように、データの集約方法に基づいています。

- [基準（Criteria）]：レポートの定義に使用するその他の基準を変更します。[Criteria] 設定ページで使用可能な属性は可変です。場合により、選択可能な基準はありません。以下に、可能な基準のリストを示します。
  - [上位（Top）]（すべての「上位」レポート）：レポートに含める対象項目数。たとえば、[Top 10] ファイアウォール宛先は、設定されている時間範囲内のファイアウォール イベントについて最も頻度が高い 10 件の宛先を戻します。10、20、25、または 50 を選択します。
  - [Service]（ボットネット以外のファイアウォール レポート）：レポートに含めるサービス。サービスを指定するには、フィールドの横の [Edit] ボタンをクリックし、目的のサービス ポリシー オブジェクトを選択します。複数のオブジェクトを選択できます。
  - [Source IP]、[Destination IP]（ボットネット以外のファイアウォール レポート）：ソースと宛先の IP アドレス フィールドは分かれていますが、機能的には同じです。これらのフィールドは、レポートに含めるソースまたは宛先の IP アドレスを定義します。個々のアドレス（10.100.10.10 など）を入力することも、アドレスの範囲（10.100.10.10-10.100.10.20 など）を入力することもできます。IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。カンマで複数のアドレスを区切ります。

フィールドの横の [Edit] ボタンをクリックしてダイアログボックスを開き、そこでアドレスとアドレス範囲の複雑なリストをより簡単に作成できます。ただし、ネットワーク/ホスト オブジェクトを使用してアドレスを定義することはできません。

（注） [Service]、[Source IP]、および [Destination IP] の各基準の値をすべて単一レポートで指定することは行わないでください。レポートが基づく基準（たとえば、上位サービス（Top Services）レポートの場合は [Service]）と、その他の 1 つの基準を指定できます。3 つの値すべてを指定すると、そのレポートには常にデータが含まれません。

- [Permit/Deny]（ボットネット以外のファイアウォール レポート）：イベントで反映されるアクション。一致するトラフィックの許可（[Permit]）、一致するトラフィックの拒否（[Deny]）、またはその両方（[All]）のいずれか。デフォルトは [All] です。
- [Signature ID]（IPS 上位攻撃者、上位シグニチャ、上位攻撃対象）：レポートに含めるシグニチャ。シグニチャを指定するには、フィールドの横の [Edit] ボタンをクリックし、目的のシグニチャを選択します。フォルダを選択して、フォルダ内のすべてのシグニチャを選択できます。

（注） 事前定義システム レポートでは、[Signature ID]、[Attacker IP]、および [Victim IP] の各基準すべての値を指定することはできません。レポートのキー属性の値（たとえば、上位攻撃対象レポートの場合は [Victim IP]）と、その他の値を 1 つ指定できます。3 つの基準すべての値を設定する場合は、カスタム レポートを作成する必要があります。

- [Attacker IP]、[Victim IP]（IPS 上位攻撃者、上位シグニチャ、上位攻撃対象）：攻撃者と攻撃対象の IP アドレス フィールドは分かれていますが、機能的には同じです。これらのフィールドは、レポートに含める攻撃者（ソース）または攻撃対象（宛先）の IP アドレスを定義します。個々のアドレス（10.100.10.10 など）を入力することも、アドレスの範囲（10.100.10.10-10.100.10.20 など）を入力することもできます。IPv4 アドレスと IPv6 アドレスの両方が受け入れられます。カンマで複数のアドレスを区切ります。

フィールドの横の [Edit] ボタンをクリックしてダイアログボックスを開き、そこでアドレスとアドレス範囲の複雑なリストをより簡単に作成できます。ただし、ネットワーク/ホスト オブジェクトを使用してアドレスを定義することはできません。

- [Blocked]（IPS 上位攻撃者、上位ブロック/非ブロック シグニチャ、上位シグニチャ、上位攻撃対象）：イベントが、ドロップされたトラフィック（[Blocked]）、ドロップされなかったトラフィック（[Unblocked]）、または両方（[All]）の、どちらに起因するか。
- [ユーザー名（Username）]（接続プロファイル レポートおよびユーザー レポート）：レポートに含めるユーザの名前。デフォルトは空のリストで、すべてのユーザが含まれます。レポートで特定のユーザに焦点を当てる場合は、テーブルの下の [Add]（+）ボタン、[Edit]（鉛筆）ボタン、または [Delete]（ゴミ箱）ボタンを使用して、目的のユーザ リストを作成します。Security Manager のバージョン 4.7 以降、ユーザー名フィルタは大文字/小文字の区別、ワイルドカード文字、および「NOT」操作のサポートをサポートします。このトピックの最後の段落にある「**大文字/小文字の区別の有効化**」と「**ワイルドカードのサポートの無効化**」を参照してください。
- [テクノロジー（Technology）]（接続プロファイル レポート、ユーザ レポート、および VPN デバイス使用状況レポート）：レポートに含めるリモート アクセス テクノロジーのタイプ：すべて、クライアントレス（SSL VPN）、フルクライアント（SSL VPN）、IPsec RA（IPsec リモートアクセス VPN）。
- [接続プロファイル（Connection Profile）]（接続プロファイル レポート）：クライアントレス（SSL VPN）、フル クライアント（SSL VPN）、または IPsec RA（IPsec リモートアクセス VPN）トポロジの接続プロファイルを追加または編集することにより、Report Manager で接続プロファイル レポートをカスタマイズできます。詳細については、[Connection Profiles] ページ （1715 ページ）および接続プロファイルの設定（ASA、PIX 7.0+） （1713 ページ）を参照してください。Security Manager のバージョン 4.7 以降、接続プロファイル フィルタは大文字/小文字の区別、ワイルドカード文字、および「NOT」操作のサポートをサポートします。このトピックの最後の段落にある「**大文字/小文字の区別の有効化**」と「**ワイルドカードのサポートの無効化**」を参照してください。
- グループ ポリシー（接続プロファイル レポート）：フィルタで 1 つまたは複数のグループ ポリシーを指定して、指定したグループ ポリシーでログインしたユーザのレポートを生成することにより、Report Manager で接続プロファイル レポートをカスタマイズできます。詳細については、リモート アクセス VPN のグループ ポリシーの設定 （1740 ページ）を参照してください。Security Manager のバージョン 4.7 以降、グループ ポリシー フィルタは大文字/小文字の区別、ワイルドカード文字、および「NOT」操作のサポートをサポートします。このトピックの最後の段落にある「**大文字/小文字の区別の有効化**」と「**ワイルドカードのサポートの無効化**」を参照してください。

- ユーザーセッションの継続時間（接続プロファイルレポートおよびユーザレポート）：タイトルが示すように、ユーザーセッションの継続時間を <= または >= 時間として指定できます。

ステップ 5 [設定の編集（Edit Settings）] ダイアログボックスで [OK] をクリックして、変更内容を実装します。

これで、[Generate Report] ボタンをクリックして設定で定義されたデータを取得し、レポートに表示できます。[Save] または [Save As] を使用して、変更内容を設定に永続的に保存することもできます。

大文字/小文字の区別を有効にする

Security Manager のバージョン 4.7 以降、ユーザー名フィルタ、接続プロファイルフィルタ、およびグループポリシーフィルタで、大文字/小文字を区別できます。大文字/小文字の区別はデフォルトで無効になっています。使用する場合は、次の手順に従って有効にする必要があります。これら 3 つのフィルタのいずれかに対して有効にすると、それら 3 つすべてに対して有効になることに注意してください。

1. reporting.properties ファイルを見つける。デフォルトの場所は NMSROOT/MDC/reports/config です。（NMSROOT のデフォルト値は C:\Program Files\CSCOpx です）
2. パラメータ reports.reportgeneration.vpnUserReport.casesensitive.enable=true を設定する
3. CsmReportServer である Report Manager サービスを再起動する。

ワイルドカードサポートの無効化

Security Manager のバージョン 4.7 以降、ユーザー名フィルタ、接続プロファイルフィルタ、およびグループポリシーフィルタで、ワイルドカードをサポートしています。ワイルドカードサポートは、デフォルトで有効になっています。使用したくない場合は、次の手順に従って無効にする必要があります。これら 3 つのフィルタのいずれかを無効にすると、3 つすべてが無効になることに注意してください。

1. reporting.properties ファイルを見つける。デフォルトの場所は NMSROOT/MDC/reports/config です。（NMSROOT のデフォルト値は C:\Program Files\CSCOpx です）
2. パラメータ reports.reportgeneration.vpnUserReport.wildcard.enable=false を設定します。
3. CsmReportServer である Report Manager サービスを再起動する。

レポートデータへのドリルダウン

上位の宛先、上位のサービス、上位の送信元ファイアウォールレポート、および上位の攻撃者、上位のシグネチャ、上位の攻撃対象 IPS レポートでは、レポートデータをドリルダウンできます。

ドリルダウン対応レポートの 1 つをドリルダウンするには、そのレポートの円グラフ、XY グラフ、または棒グラフのデータポイントをクリックします。たとえば、上位のシグネチャレポートの円グラフのスライスをクリックすると、選択したシグネチャの上位の攻撃者と上位の被害者のレポートの詳細が表示されます。

（注） レポートに使用するフィルタ条件は、関連するドリルダウンレポートで表示されるデータに影響します。レポートデータにフィルタを適用すると、レポートデータをドリルダウンするときに、1 つのドリルダウンレポートのみが表示されます。

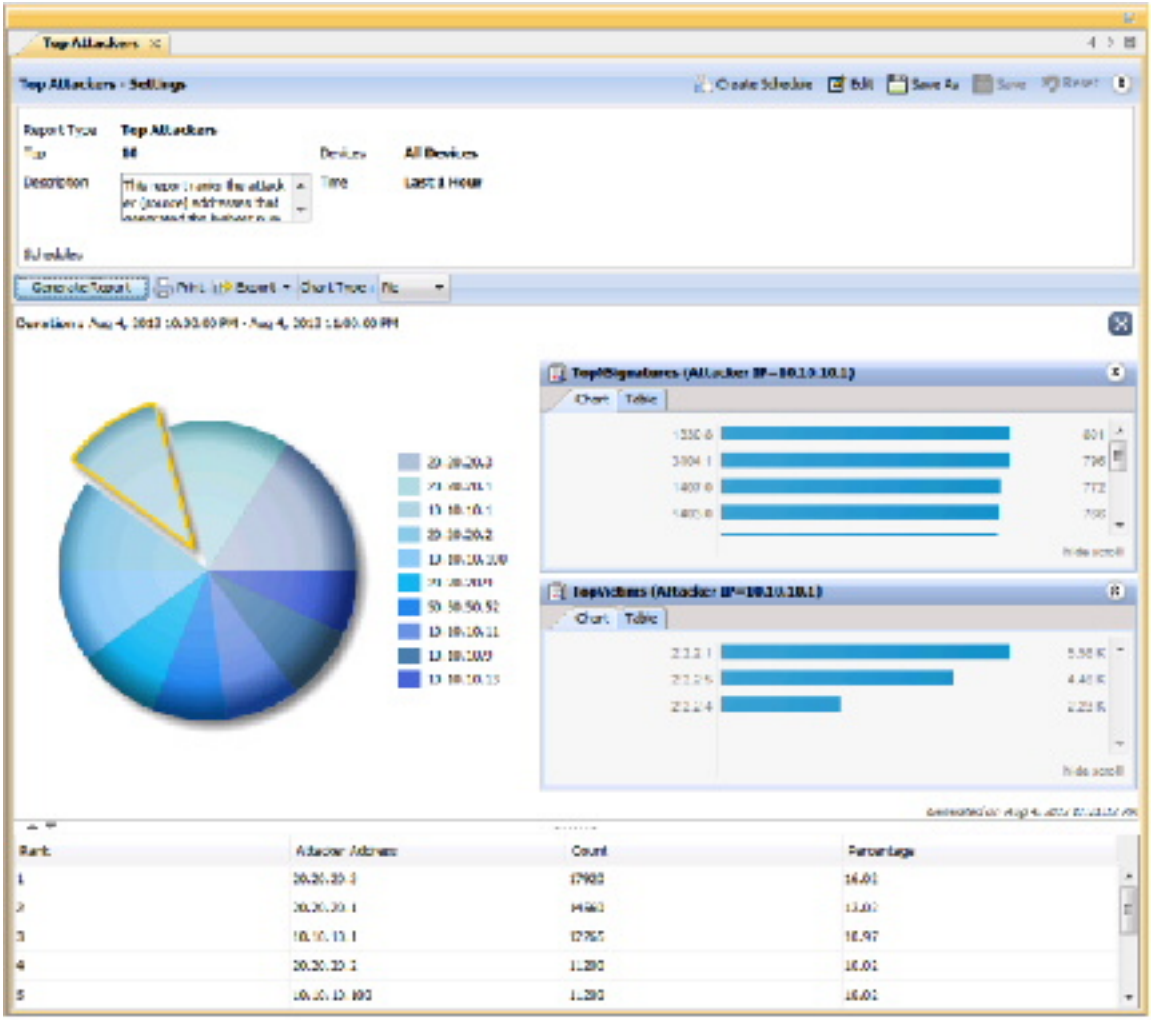
次の表は、サポートされているレポートタイプごとに表示されるドリルダウンレポートを示しています。

レポート名	表示されるドリルダウンレポート
Firewall	
上位ソース	上位宛先（Top Destinations）、上位サービス（Top Services）
上位接続先	上位送信元（Top Sources）、上位サービス（Top Services）
最上位サービス（Top Services）	上位送信元（Top Sources）、上位宛先（Top Destinations）
IPS	
上位シグニチャ（Top Signature）	上位攻撃者（Top Attackers）、上位攻撃対象（Top Victim）
上位攻撃者（Top Attackers）	上位攻撃者（Top Attackers）、上位攻撃対象（Top Victim）
上位攻撃対象（Top Victim）	上位シグニチャ（Top Signature）、上位攻撃者（Top Attackers）

ドリルダウンレポートごとに、ドリルダウンデータのグラフまたは表を表示できます。サポートされているレポートのいずれかで特定のデータポイントにドリルダウンした場合、ドリルダウンレポートのグラフと表形式のデータが、印刷したレポートとエクスポートしたレポートデータに含まれます。

次の図は、[上位攻撃者（Top Attackers）] レポートのドリルダウンレポートデータの例を示しています。

図 *69* : 上位の攻撃者のドリルダウン レポート



関連項目

- レポートの起動と生成 （3586 ページ）
- ASA および PIX 7.0+ デバイスのリモート アクセス VPN ポリシーの概要 （1706 ページ）

レポートの印刷

レポートの起動と生成 （3586ページ）の説明に従ってレポートを生成したあとで、そのレポートを印刷できます。

（注） 上位宛先、上位サービス、または上位送信元ファイアウォールレポート、または上位攻撃者、上位シグネチャ、または上位攻撃対象IPSレポートで特定のデータポイントのドリルダウンレポートを開いている場合、ドリルダウンレポートのグラフと表形式のデータは、印刷されたレポートに含まれます。詳細については、レポートデータへのドリルダウン （3593 ページ）を参照してください。

レポートを印刷するには、レポートの上にある[印刷（Print）]ボタンをクリックします。プリンタを選択するプロンプトが表示されます。

レポートのエクスポート

レポートの起動と生成 （3586ページ）の説明に従ってレポートを生成したあとで、そのレポートをAdobe Acrobat（PDF）ファイルまたはComma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートできます。

エクスポートされたファイルには、次の情報が含まれています。

- レポートの作成時刻。
- レポートの生成に使用した設定。
- （PDFのみ）レポートデータのグラフィカル表現。
- 表形式のレポートデータ。PDFでは、情報はテーブルとして表されます。CSVでは、情報はカンマ区切りで、最初の行がカラムの見出しになります。

（注） 上位宛先、上位サービス、または上位送信元ファイアウォールレポート、または上位攻撃者、上位シグネチャ、または上位攻撃対象IPSレポートで特定のデータポイントのドリルダウンレポートを開いている場合、ドリルダウンレポートのグラフと表形式のデータは、エクスポートに含まれます。詳細については、レポートデータへのドリルダウン （3593 ページ）を参照してください。

レポートをエクスポートするには、レポートの上の[エクスポート（Export）]ボタンで下矢印をクリックし、[PDFとして（As PDF）]または[CSVとして（As CSV）]のいずれかを選択します。レポートのフォルダを選択するプロンプトが表示されます。デフォルトのファイル名が指定されていますが、そのファイル名を変更できます。

レポートエクスポートエラーのトラブルシューティング

デバイスステータスレポートをエクスポートしようとすると、次のエラーが表示されます。

「Windowsは'acrord32'を見つけることができません。名前を正しく入力したことを確認してから、やり直してください。」

まず、サーバーに Adobe Reader がインストールされていない場合に上記のエラーが発生します。Adobe がインストールされていないため、Windows は acrord32.exe ファイルを見つけることができません。

次に、Adobe Reader がインストールされている場合でも、上記のエラーがスローされる場合があります。これは、Windows XP、Vista、7、8.1、および 10 に存在する問題です。これは、Adobe Reader の起動に失敗したことが原因です。これは既知のエラーであり、Adobe Reader だけでなく、すべてのアプリケーションで発生する可能性があります。Microsoft はまだこれに対するパッチを提供していません。

この問題が発生する可能性のある報告された理由は次のとおりです。

1) 破損したレジストリエントリ

2) Adobe のインストール中の問題

3) デフォルトの Adobe Reader の削除

<B>症状：</B>

デバイスステータスレポートをエクスポートしようとすると、次のエラーが表示されます。

「Windows は 'acrord32' を見つけることができません。名前を正しく入力したことを確認してから、やり直してください。」

<B>条件：</B>

まず、サーバーに Adobe Reader がインストールされていない場合に上記のエラーが発生します。Adobe がインストールされていないため、Windows は acrord32.exe ファイルを見つけることができません。

次に、Adobe Reader がインストールされている場合でも、上記のエラーがスローされる場合があります。これは、Windows XP、Vista、7、8.1、および 10 に存在する問題です。これは、Adobe Reader の起動に失敗したことが原因です。これは既知のエラーであり、Adobe Reader だけでなく、すべてのアプリケーションで発生する可能性があります。Microsoft はまだこれに対するパッチを提供していません。

<B>回避策：</B>

1) Adobe Reader がインストールされていない場合はインストールします

2) Adobe Reader がインストールされていてもエラーがスローされる場合は、ファイルが保存されている場所に移動して実行します

Adobe Reader アクションで開きます。エラーがスローされても、ファイルは作成されますが、フォーマットはなしになります。

形式）。そのため、PDF リーダーを使用して開くことができます。

<B>問題の詳細：</B>

レポートのデフォルト設定値の設定

Report Managerがシステム レポートに対して使用するデフォルト設定を制御できます。デフォルトを変更すると、すべてのシステム レポートの設定が自動的に変更されますが、変更内容はカスタム レポートとして保存したレポート（[My Reports] フォルダ内）には適用されません。これらの設定を変更するには、システム管理者権限またはネットワーク管理者権限が必要です。

レポートを表示している間に、任意のシステム レポートを編集してこれらの設定に別の値を指定できます。その目的は、レポートを表示している間の一時的な使用、または [My Reports] フォルダ内のカスタム レポートとしての保存のいずれかです。

（注） レポートの作成後はフィルタを適用できないため、[マイレポート（My Reports）] または [カスタムレポート（Custom Reports）] でレポートを作成する際には、レポートの作成時に必要なフィルタが適用されていることを確認してください。

ヒント システムレポートの設定を変更する場合、[レポート設定（Report Settings）] ツールバーで [リセット（Reset）] ボタンをクリックすると、レポートをデフォルト設定に戻すことができます。

ステップ 1 Report Manager で、[ツール（Tools）] > [デフォルトのレポート設定（Default Report Settings）] を選択し、[デフォルトのレポート設定（Default Report Settings）] ダイアログボックスを開きます。

ステップ 2 次のいずれかのオプションを設定します。

- [上位（Top）]：いずれかの「上位」レポートに表示される結果の数。上位レポートには、レポートがターゲットとするタイプの最新の発生項目が表示されます。たとえば、20 を選択すると、ファイアウォール上位宛先（Top Destinations）レポートには、Security Manager に報告されたイベント内で発生時刻が最新 20 個のトラフィック宛先が表示されます。デフォルトは 10 です。

各追加項目の詳細情報はレポートテーブルに表示されますが、10 よりも大きい値を選択すると、10 番目の後の項目はすべて、チャートでは「others」として要約表示されます。

- [時間範囲（Time Range）]：レポートに含めるイベントの時間枠：
  - [Last 1 Hour]：00 分から始まる直前の 1 時間全体。たとえば、現在の時刻が午前 11:45 である場合、直前の 1 時間（Last 1 Hour）のレポートには 10:00 から 11:00 までのデータが表示されます。
  - [Last 1 Day]：直前の 1 日全体（0 時から 0 時まで）。たとえば、現在の日付が火曜日である場合、直前の 1 日（Last 1 Day）のレポートには月曜日のデータが表示されます。
  - [Last 1 Week]：前の月曜日から日曜日まで。
  - [Last 1 Month]：前月。たとえば、現在の日付が 9 月 29 日である場合、直前の 1 か月（Last 1 Month）のレポートには 8 月のデータが表示されます。

時間範囲設定の意味の詳細については、Report Manager データ集約について （3565 ページ）を参照してください。

- [デフォルトの電子メールアドレス（Default Email Address）]：スケジューリングされたレポートのデフォルトの宛先として使用される電子メールアドレス。

インストール時のデフォルト値に戻す場合は、[デフォルトの復元（Restore Defaults）] をクリックします。

ステップ 3 [適用（Apply）] をクリックして変更内容を保存し、[閉じる（Close）] をクリックしてダイアログボックスを閉じます。

レポート ウィンドウの配置

同時に最大で 5 つのレポート ウィンドウを開いていることができます。レポートは、メイン Report Manager ウィンドウの右側のペインにタブ付きウィンドウとして開かれます。複数の領域がある場合は、最も最近に使用された領域（「タブ付きグループ」）に開かれます。次の図に示すように、レポート ウィンドウのタブを右クリックすると、ウィンドウを配置するためのコマンドが表示されます。

ユーザの要件に基づいてレポート ウィンドウを配置するための多数のオプションがあります。たとえば、2 つのレポートを横に並べて比較したり、レポートを閉じないでメイン ウィンドウから除去したりすることができます。

次の方法を使用してレポート ウィンドウを配置し、目的の表示にすることができます。

- レポートのフローティング：レポートを閉じずにメイン Report Manager ウィンドウから除去するには、レポートタブを右クリックし、[フローティング（Floating）] を選択します。レポートは独自のウィンドウに移動します。

すでにレポートをフローティングしている場合は、[フローティング先（Floating to）] を選択し、既にフローティングされているウィンドウの 1 つを選択します。レポートがそのウィンドウ内の新しいタブになります。

- レポートのドッキング：フローティングレポートをメイン Report Manager ウィンドウに戻すには、レポートタブを右クリックし、[ドッキング（Docking）] を選択します。
- 横に並べて比較するためのレポートの水平配置：レポートをフローティングせずに、簡単に比較できるようにするためにレポートを垂直または水平に配置するには、レポートタブ

を右クリックし、[新しい横方向グループ（New Horizontal Group）] または [新しい縦方向グループ（New Vertical Group）] を選択します。これらのコマンドは、現在のタブ付きグループを選択されたレイアウトに分割します。これらのコマンドを使用するには、少なくとも 2 つのレポートが開いている必要があります。レポートを 3 つ以上開いていて、それらすべてを別々のウィンドウに配置する場合は、コマンドを複数回使用する必要があります。

- 異なるタブ付きグループへのレポートの移動：開いているレポートが複数あり、それらのレポートが水平または垂直のグループに配置されている場合は、レポートタブを右クリックして [次のタブグループに移動（Move to Next Tab Group）] または [前のタブグループに移動（Move to Previous Tab Group）] を選択することにより、グループ間でレポートを移動できます。これらのコマンドは、移動できるような方法でレポートが配置されている場合にのみ表示されます。
- グループの向きの変更：レポートタブを右クリックし、[タブグループの方向を変更（Change Tab Groups Orientation）] を選択することにより、水平方向のレイアウトと垂直方向のレイアウトを切り替えることができます。

レポートの保存

レポートの設定を編集する場合、それらの変更内容を永続的にするにはレポートを保存する必要があります。ただし、事前定義システム レポートに対する変更内容を保存するには、レポートをカスタム レポートとして保存する必要があります。

ヒント　レポートを保存すると、そのレポートを定義している設定が保存されます。レポートの生成内容は保存されません。レポートの生成内容（つまり、グラフとレポート データ）を保存する場合は、レポートを保存するのではなくエクスポートする必要があります。

- カスタム レポートに対する変更内容を保存するには、Report Manager で次のいずれかを実行します。
  - メニューバーから **[ファイル（File）] > [保存（Save）]** を選択する。
  - レポート設定ツールバーで [名前を付けて保存（Save As）] ボタンをクリックする。
- 変更内容を新規カスタム レポートとして保存するには、次のいずれかを実行して、[Save Report As] ダイアログボックスを開きます。
  - メニューバーから **[ファイル（File）] > [名前を付けて保存（Save As）]** を選択する。
  - レポート設定ツールバーで [名前を付けて保存（Save As）] ボタンをクリックする。
  - レポートリストでレポートを右クリックして、[名前を付けて保存（Save As）] を選択する。

次に、レポートの名前とレポートの説明（任意）を入力し、[OK] をクリックします。レポートがレポート リストの [My Reports] フォルダに追加されます。

（注） レポート名は最大 64 文字で、英数字、スペース、ハイフン（-）、および下線文字（_）を含みます。説明には、最大 1024 文字を使用できます。

レポートの名前変更

カスタム レポートの名前は変更できますが、事前定義システム レポートの名前は変更できません。

関連項目

- Report Manager の概要 （3568 ページ）
- Report Manager のレポート リストについて （3572 ページ）

ステップ 1 Report Manager で、名前を変更するレポートをレポート リストから選択します。レポートを開く必要はありません。単にリスト内で選択します。

ステップ 2 レポートリストの上の [編集（Edit）]（鉛筆）ボタンをクリックしてダイアログボックスを開きます。そこで、レポート名を変更できます。

ステップ 3 新しい名前を入力し、[OK] をクリックします。

レポート名は最大 64 文字で、英数字、スペース、ハイフン（-）、および下線文字（_）を含みます。

レポート ウィンドウの終了

レポート タブの X アイコンをクリックすることにより、任意のレポートを閉じることができます。フロートしたレポートの場合、単にそのウィンドウのタイトルバーの [X] アイコンをクリックします。

ヒント レポートを閉じるときに、生成されたレポートデータは保持されません。生成されたデータを保持する場合は、レポート ウィンドウを閉じる前に、レポートを印刷またはエクスポートする必要があります。

次の方法を使用して、Report Manager を終了せずにレポート ウィンドウを閉じることもできます。

- レポートを閉じる：[ファイル（File）]>[レポートを閉じる（Close Report）] を選択して、現在表示されているウィンドウを閉じるか、または目的のレポートタブを右クリックして [閉じる（Close）] を選択します。

- すべてのレポートを閉じる：[ファイル（File）] > [すべてのレポートを閉じる（Close All Reports）] を選択するか、または任意のレポートタブを右クリックして [すべてを閉じる（Close All）] を選択します。
- 1 つのレポートを除いてすべてのレポートを閉じる：開いたままにしておくレポートのレポートタブを右クリックし、[他を閉じる（Close Others）] を選択します。

レポートの削除

カスタム レポートは削除できますが、事前定義システム レポートは削除できません。

カスタムレポートを削除するには、削除するレポートをレポートリストで選択し、レポートリストの上の [削除（Delete）]（ゴミ箱）ボタンをクリックします。削除の確認が求められます。

ヒント レポートを削除すると、そのレポートのスケジュールもすべて削除されます。

別のユーザのカスタムレポートを削除する必要がある場合は、カスタム レポートの管理 （3602 ページ）を参照してください。

カスタム レポートの管理

システム管理者権限またはネットワーク管理者権限がある場合は、この Security Manager サーバ上のすべての Report Manager ユーザによって作成されたカスタム レポートのリストを表示できます。

カスタムレポートのリストを表示するには、[ツール（Tools）] > [カスタムレポートリスト（Custom Report List）] を選択して [カスタムレポートの管理（Manage Custom Reports）] ダイアログボックスを開きます。リストには、レポート名、レポートのタイプ、レポートで分析されるデバイスのタイプ、カスタム レポートを作成したユーザのユーザ名が表示されます。

次のコントロールを使用して、このページのカスタム レポートを管理できます。

- **ページネーションコントロール**：多数のカスタムレポートがある場合、ページネーションコントロールを使用してリスト内を移動します。ボタンをクリックして、最初のページ、前のページ、次のページ、または最後のページに移動できます。または [Page X of Y] 編集ボックスにページ番号を入力できます。編集ボックスで下矢印をクリックして、ページ番号ではなくレコード番号で処理するように編集ボックスを変更することもできます。
- [削除（Delete）] ボタン：選択されたレポートを削除するには、このボタンをクリックします。そのレポートを使用するスケジュール（およびスケジュールの結果）もすべて削除されます。
- [リフレッシュ（Refresh）] ボタン：最新の情報を使用してリストを更新するには、このボタンをクリックします。

レポートのスケジュール設定

定期的に Report Manager からレポートを生成するようにスケジュールを作成できます。

ここでは、次の内容について説明します。

- レポート スケジュールの表示 （3603 ページ）
- レポート スケジュールの設定 （3604 ページ）
- スケジューリングされたレポートの結果の表示 （3605 ページ）
- レポート スケジュールのイネーブル化およびディセーブル化 （3606 ページ）
- レポートの削除 （3602 ページ）

レポート スケジュールの表示

Report Manager で設定されているレポート スケジュールのリストを表示できます。システム管理者権限またはネットワーク管理者権限がある場合、リストには、そのユーザが設定したか別のユーザが設定したかには関係なく、サーバで設定されているすべてのスケジュールが含まれています。それより低い権限を持つユーザは、自身のスケジュールのみを参照できます。

レポートスケジュールのリストを表示するには、[スケジュール設定されたレポート（Scheduled Reports）] タブを選択し、必要に応じて、[スケジュールリスト（Schedule List）] サブタブを選択します。リストには、スケジュール名、説明、スケジュールによって生成されるレポート、レポート生成の頻度、レポートの送信先電子メールアドレス（ある場合）、スケジュールがイネーブルまたはディセーブルのどちらであるか、およびスケジュールを作成したユーザのユーザ名が表示されます。

次のコントロールを使用して、このページのレポート スケジュールを管理できます。

- **ページネーション コントロール**：多数のスケジュールがある場合、ページネーション コントロール（テーブルの下の左側）を使用してリスト内を移動します。ボタンをクリックして、最初のページ、前のページ、次のページ、または最後のページに移動できます。または [Page X of Y] 編集ボックスにページ番号を入力できます。編集ボックスで下矢印をクリックして、ページ番号ではなくレコード番号で処理するように編集ボックスを変更することもできます。
- [追加（Add）] ボタン：新規スケジュールを追加するには、このボタンをクリックします。詳細については、 レポート スケジュールの設定 （3604 ページ）を参照してください。
- [編集（Edit）] ボタン：選択されたスケジュールを編集するには、このボタンをクリックします。詳細については、 レポート スケジュールの設定 （3604 ページ）を参照してください。
- [削除（Delete）] ボタン：選択されたスケジュールを削除するには、このボタンをクリックします。詳細については、 レポート スケジュールの削除 （3607 ページ）を参照してください。

- [リフレッシュ（Refresh）]ボタン：最新の情報を使用してリストを更新するには、このボタンをクリックします。
- [イネーブル（Enable）] ボタン：選択されたスケジュールをイネーブルにするには、このボタンをクリックします。このボタンは、選択されたスケジュールがディセーブルの場合にのみアクティブです。詳細については、レポート スケジュールのイネーブル化およびディセーブル化 （3606 ページ）を参照してください。
- [ディセーブル（Disable）]ボタン：選択されたスケジュールをディセーブルにするには、このボタンをクリックします。このボタンは、選択されたスケジュールがディセーブルの場合にのみアクティブです。詳細については、レポート スケジュールのイネーブル化およびディセーブル化 （3606 ページ）を参照してください。

レポート スケジュールの設定

設定された時刻に自動的にレポートを生成するようにスケジュールを作成できます。生成されたレポートは、指定された受信者に電子メールで送信され、また、Report Manager で表示できるように保管されます。レポートをスケジューリングすることにより、ネットワーク セキュリティおよび使用状況の定期的なマイルストーン ビューを簡単かつ効率的に作成できます。この手順では、レポートのスケジュールのセットアップ方法を説明します。

関連項目

- Report Manager の概要 （3568 ページ）
- レポートの起動と生成 （3586 ページ）
- レポート スケジュールの表示 （3603 ページ）
- Report Manager のトラブルシューティング （3607 ページ）

ステップ 1 Report Manager で、次のいずれかを実行します。

- [Reports] タブで、レポート リスト（左側のペイン）でレポートの名前ダブルクリックすることにより、新規スケジュールを作成するレポートを開きます。次に、レポート設定ツールバーで[スケジュールの作成（Create Schedule）] ボタンをクリックします。

（注） [Reports] タブから既存のスケジュールを編集することはできません。

- [レポート（Reports）]タブで、スケジュールを作成するレポートを右クリックし、[スケジュールの作成（Create Schedule）] を選択します。レポートがまだ開いていない場合は、開かれます。
- [スケジュール設定されたレポート（Scheduled Reports）] タブの [スケジュールリスト（Schedule List）] サブタブで、スケジュールのリストの下にある [追加（Add）] ボタンをクリックし、新規スケジュールを作成します。既存のスケジュールを編集するには、リストでレポートを選択して [編集（Edit）] ボタンをクリックします。

[Add or Edit Report Schedule] ダイアログボックスが開きます。

ステップ 2 ダイアログボックスで次のオプションを設定します。

- [スケジュール名（Schedule Name）]：スケジュールの名前（最大 64 文字）。
- [レポート名（Report Name）]：スケジュールで生成するレポートの名前を選択します。レポート設定ペインからスケジュールを作成する場合、名前は事前に選択されており、ユーザはその名前を変更できません。
- [スケジュール（Schedule）]：レポートの生成頻度（毎日、毎週（週に 1 回）、または毎月（月に 1 回））を選択します。次に、レポートを生成する日時を入力します。
  - [Daily schedules]：スケジュールが [Monday through Friday]（5 日間）または [Monday through Sunday]（7 日間全体）のどちらであるかを選択します。レポートを生成する時刻（24 時間表記）を入力します。
  - [Weekly schedules]：曜日を選択し、24 時間表記で時刻を入力します。
  - [Monthly schedules]：レポートの生成が、月の最初の日、最後の日、またはカスタムの、いずれであるかを選択します。[Custom] を選択する場合は、日付番号を入力します。次に、24 時間表記で時刻を入力します。
- [電子メールの送信先（Email To）]：レポートの送信先の電子メールアドレス。カンマで複数のアドレスを区切ります。レポートを電子メールで送信しない場合は、そのフィールドが空であることを確認してください。電子メールを正常に送信するには、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）で説明されているように、Security Manager サーバに SMTP を設定する必要があることに注意してください。

何らかの理由でレポートを生成できない場合、その失敗に関する通知がこれらの電子メール アドレスに送信されます。

- [レポート形式のエクスポート（Export Report Format）]：レポートを Adobe Acrobat（PDF）形式またはカンマ区切り値（CSV）形式で生成するかを指定します。PDF にはグラフィックが含まれますが、CSV には含まれません。エクスポート形式の詳細については、レポートのエクスポート （3596 ページ）を参照してください。
- [説明（Description）]：スケジュールの説明。
- [ステータス（Status）]：スケジュールが有効（レポートが生成される）または無効（レポートが生成されない）であるかを指定します。

ステップ 3 [OK] をクリックして、スケジュールを保存します。[Schedules] タブのスケジュール リストに新規スケジュールが追加されます。

スケジューリングされたレポートの結果の表示

通常、レポート スケジュールには生成されたレポートの送信先電子メール アドレスが含まれています。Report Manager でスケジュールから生成されたレポートを表示することもできま

す。システム管理者権限またはネットワーク管理者権限がある場合、他のユーザーのスケジュールによって生成された結果を表示できます。

ヒント　Report Manager は、スケジュールによって生成された最後のレポートのコピーを維持します。以前に生成されたレポートを取得することはできません。

関連項目

- Report Manager の概要　（3568 ページ）
- レポートの起動と生成　（3586 ページ）
- レポート スケジュールの表示　（3603 ページ）
- Report Manager のトラブルシューティング　（3607 ページ）

ステップ 1　Report Manager で、[スケジュール設定されたレポート（Scheduled Reports）] タブを選択します。

ステップ 2　[結果（Results）] サブタブを選択します。

表示する権限があるすべての結果が、このタブにリストされます。このリストには、スケジュール名、生成されたレポートの名前、レポート生成の頻度、前回のスケジュール実行（レポートが生成されたとき）の日時、レポート生成のステータス（[Success] または [Failed]）、生成されたレポート（[Last Report] カラム内）へのリンク、およびスケジュールを作成したユーザのユーザ名が表示されます。

ヒント　レポートのステータスが [Failed] である場合は、リンクをクリックして失敗の理由を参照します。

ステップ 3　[Last Report] カラムでレポートへのアイコン リンクをダブルクリックし、レポートを開きます。レポートを表示しているときに、そのレポートをワークステーションに保存できます。

探しているレポートが見つからない場合は、[リフレッシュ（Refresh）] ボタンをクリックして最新の情報でリストを更新します。

レポート スケジュールのイネーブル化およびディセーブル化

レポート スケジュールをイネーブルまたはディセーブルにして、スケジュールに基づいてレポートが生成されるかどうかを変更できます。スケジュールをディセーブルにすることにより、スケジュールを削除せずにレポートが生成されないようにすることができます。システム管理者権限またはネットワーク管理者権限がある場合、別のユーザのスケジュールをイネーブルまたはディセーブルにすることができます。

関連項目

- Report Manager の概要　（3568 ページ）
- レポート スケジュールの表示　（3603 ページ）

ステップ 1 Report Manager で、[スケジュール設定されたレポート（Scheduled Reports）] タブを選択し、必要に応じて、[スケジュールリスト（Schedule List）] サブタブを選択します。このタブには、現在定義されていて表示権限があるスケジュールがすべてリストされます。

ステップ 2 ステータスを変更するスケジュールを選択し、[有効（Enable）] ボタンまたは [無効（Disable）] ボタンのいずれかをクリックします。

レポート スケジュールの削除

レポート スケジュールが不要になったら、それらのスケジュールを削除できます。システム管理者権限またはネットワーク管理者権限がある場合、別のユーザーのスケジュールを削除できます。

ヒント スケジュールからレポートを生成しないが、スケジュール定義を保持しておく場合は、スケジュールをディセーブルにすることができます。ディセーブルになったスケジュールは、レポートを生成しません。

ステップ 1 Report Manager で、[Scheduled Reports] タブを選択し、必要に応じて、[Schedule List] サブタブを選択します。このタブには、現在定義されていて表示権限があるスケジュールがすべてリストされます。

ステップ 2 スケジュールを選択し、リストの下の [削除（Delete）] ボタンをクリックします。削除の確認が求められます。

スケジュールを削除すると、そのスケジュールの結果もすべてサーバから削除され、[Results] タブから除去されます。

Report Manager のトラブルシューティング

以下に、Report Manager アプリケーション使用時に発生する可能性があるいくつかの問題と、いくつかの問題解決方法を示します。

問題：Report Manager が開かず、「Not able to connect to server」というメッセージが表示される。

解決策：Report Manager で、csmReportServer プロセス、rptDbEngine プロセス、および rptDbMonitor プロセスを開始する必要があります。Report Manager は、Event Management サービス VmsEventServer にも依存しています。Security Manager サーバですべてのサービスが開始されており、正しく実行していることを確認してください。

プロセスの現在の状態を表示するには、http://SecManServer:1741（SecManServer はサーバーの DNS 名）を使用して Security Manager Web インターフェイスにログインします。Security

Management Suite ホームページから、[サーバー管理（Server Administration）] リンクをクリックして [管理（Admin）] ページで CiscoWorks Common Services を開きます。ウィンドウの左側の TOC で [プロセス（Processes）] をクリックして、現在の状態を表示するプロセスのリストを開きます。これらのプロセスを選択し、[開始（Start）] をクリックして開始します。必要に応じて、これらのプロセスを停止してから再起動することができます。プロセスが完全に再起動するまで待機してから、再度 Report Manager を開いてみます。

問題：レポートの生成時に、「No records found」というメッセージが表示される。

解決策：このメッセージは、そのレポートタイプと設定されている設定値に関連したイベントレコードがイベント データ ストレージ ロケーションに存在しないか、または必要な Report Manager 集約サイクルが完了していないことを示しています。以下を調べます。

- モニタするデバイスの選択 （3514ページ）の説明に従って、モニタリングに適したタイプのデバイスが選択されていることを確認します。
- これらのデバイスが Security Manager へのイベント送信用に適切に設定されていること、およびデバイスからのイベントが Event Viewer に表示されていることを確認します。デバイスと Security Manager が同じ syslog ポートを使用していることを確認します。デバイスの設定については、イベント管理のための ASA と FWSM デバイスの設定 （3506ページ）および イベント管理のための IPS デバイスの設定 （3508 ページ）を参照してください。Security Manager が使用している syslog ポートを確認するには、Configuration Manager の [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [イベント管理（Event Management）] ページの設定を表示します。
- IPS デバイスの場合、証明書が期限切れになっていないことを確認します。Configuration Manager で [管理（Manage）] > [IPS] > [IPS証明書（IPS Certificates）] を選択することにより証明書テーブルを確認し、必要な場合は証明書を再生成します。
- レポート設定で、レポート対象の集約データが存在しない期間が指定されている可能性があります。データは、15 分ごと、1 時間ごと（正時）、および 1 日ごと（0 時）に集約されます。レポートの時間のパラメータを変更してみてください。 レポート設定の編集（3589 ページ）を参照してください。以下の点に注意してください。
  - 直前の 1 時間（Last 1 Hour）のレポートを表示するには、最初に Event Manager サービスを開始したあとで時間の変更（正時）が発生している必要があります。たとえば、10:05 にサービスを開始する場合、毎時のレポートは 11:00 のあとでのみ使用できます。
  - 直前の 1 日（Last 1 Day）のレポートを表示するには、最初に Event Manager サービスを開始したあとで日付の変更が発生している必要があります。たとえば、10:05 にサービスを開始する場合、毎日のレポートを参照するには 0 時を過ぎるまで待つ必要があります。
  - 直前の 1 週間（Last 1 Week）のレポートを表示するには、すべての曜日のサイクルが少なくとも 1 回発生している必要があります。毎週のレポートは、毎日のレポートに基づいています。
  - 直前の 1 か月（Last 1 Month）のレポートを表示するには、サービス開始後に少なくとも 1 つの月全体が経過している必要があります。

- カスタム期間レポートを表示するには、その日付のサイクルが少なくとも 1 回発生している必要があります。

- 新規カスタム レポートを作成する場合、データを使用できるまでに最大 1 時間かかる可能性があります。また、レポートの経過時間が他の期間のデータに対して十分になるまでは、期間が直前の 1 時間（Last 1 Hour）であることを確認してください。

問題：特定のデバイスのレポートを取得できない。

解決策：以下を調査します。

- モニタするデバイスの選択 （3514 ページ）で説明されているように、そのデバイスがレポーティング時間フレームにおけるイベント管理用に選択されている必要があります。デバイスが選択されている場合でも、Report Manager が Event Viewer でサポートされるすべてのデバイスをサポートするとは限りません。サポートされるデバイス タイプについては、 レポート管理について （3561 ページ）を参照してください。

- レポート設定でそのデバイスが除外されている可能性があります。レポートですべてのデバイスを考慮するようにレポート設定が指定している場合を除き、デバイス選択にそのデバイスが含まれていることを確認します。 レポート設定の編集 （3589 ページ）を参照してください。

- レポート設定で、そのデバイスのデータが存在しない期間が指定されている可能性があります。レポートの時間のパラメータを変更してみてください。 レポート設定の編集 （3589 ページ）を参照してください。

- ユーザの組織で Cisco Secure ACS を使用してアプリケーションへのアクセスを制御している場合は、少なくともデバイスに対する表示権限がある場合にのみ、そのデバイスに関するレポートを表示できます。必要な権限があるかどうかを確認してください。

問題：シグニチャ、攻撃対象 IP、および攻撃者 IP のそれぞれに対して値を指定したあとで、特定の IPS 事前定義レポートのデータが表示されない。

解決策：上位攻撃者、上位攻撃対象、および上位シグニチャの各事前定義レポートには、シグニチャ、攻撃対象 IP アドレス、および攻撃者 IP アドレスの各基準が含まれています。ただし、3 つの基準すべてを事前定義レポート内で設定することはできません。代わりに、レポートが基づく基準（たとえば、上位攻撃対象レポートの攻撃対象 IP アドレス）と、残りの値を 1 つのみ設定できます。この制限は、[Blocked] や [Top] などの他の基準には適用されないことに注意してください。

問題：サービス、ソース IP、および宛先 IP のそれぞれに対して値を指定したあとで、特定のファイアウォール事前定義レポートのデータが表示されない。

解決策：上位宛先、上位サービス、および上位ソースの各事前定義レポートには、サービス、ソース IP アドレス、および宛先 IP アドレスの各基準が含まれています。ただし、3 つの基準すべてを事前定義レポート内で設定することはできません。代わりに、レポートが基づく基準（たとえば、上位サービス レポートのサービス）と、残りの値を 1 つのみ設定できます。この制限は、[Permit/Deny] や [Top] などの他の基準には適用されないことに注意してください。

問題：VPN レポートの統計情報を取得できない。

解決策：VPN 統計情報は、イベント データ ストレージ ロケーションに格納されているイベントからではなく、デバイスから直接部分的に取得されます。統計情報を取得するには、Report Manager がデバイスにログインして show コマンドを使用できる必要があります。ご使用の VPN デバイスのデバイス プロパティが、ログインするための正しいクレデンシャルを持っていることを確認してください。

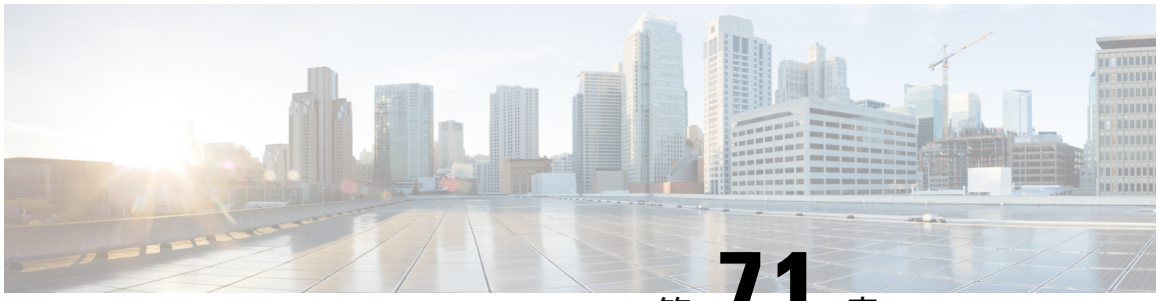
問題：スケジュール設定されたレポートが受信者に送信されない。

解決策：SMTP サーバーが正しく設定されていること、および Security Manager に対して有効なソース電子メールアドレスが設定されていることを確認してください。詳細については、電子メール通知用の SMTP サーバおよびデフォルト アドレスの設定 （34 ページ）を参照してください。

問題：デバイスステータスレポートをエクスポートすると、次のエラーが表示される。「Windows は 'acrord32' を見つけることができません。名前を正しく入力したことを確認してから、やり直してください。」

解決策：以下を実行します。

- サーバーに Adobe Reader をインストールします（まだインストールされていない場合）。Adobe Reader がインストールされていない場合、MS-Windows は acrord32.exe ファイルを見つけることができません。
- Adobe Reader がインストールされていても、Windows XP、Vista、7、8.1、または 10 を使用している場合は、エラーがスローされることがあります。これは Microsoft Windows の既知のエラーです。Microsoft は、このエラーに対するパッチをまだ提供していません。次の手順を実行します。
  - エクスポートされたレポートファイルが保存されている場所に移動します。右クリックして、[プログラムから開く] > [Adobe Reader] を選択します。エラーは発生していますが、ファイルは定義された形式なしで作成されます。そのため、PDF リーダーを使用して開くことができます。



第 71 章

ヘルスとパフォーマンスのモニタリング

Health and Performance Monitor（HPM）アプリケーションを使用すると、デバイスのステータスとトラフィック情報をネットワークレベルで可視化することで、ASA デバイス、IPS デバイス、および VPN サービスの主要な正常性データとパフォーマンスデータを監視できます。

すべてのデバイス、ファイアウォールデバイス、IPS デバイス、VPN サマリなど、さまざまなビューが提供され、独自のカスタマイズされたビューを作成できます。デバイスアラートの設定可能なリストも利用できます。

この機能を使用して、主要なネットワークとデバイスのメトリックを監視することで、ネットワーク内のデバイスの誤動作やボトルネックをすばやく検出して解決できます。

この章は次のトピックで構成されています。

- Health and Performance Monitor の概要 （3611 ページ）
- HPM アクセス制御 （3614 ページ）
- 正常性とパフォーマンスのモニタリングの準備 （3615 ページ）
- Health and Performance Monitor の起動 （3616 ページ）
- 監視対象デバイスの管理 （3616 ページ）
- HPM ウィンドウ （3617 ページ）
- デバイスのモニタリング （3637 ページ）
- アラートと通知 （3651 ページ）
- SNMP トラップ転送通知 （3666 ページ）

Health and Performance Monitor の概要

Health and Performance Monitor は、他のスタンドアロン Cisco Security Manager アプリケーション（ダッシュボード、Configuration Manager、イベントビューア、Report Manager、および Image Manager）から、または Windows のスタートメニューからアクセスする Cisco Security Manager クライアントのログイン画面から起動できるスタンドアロン アプリケーションです。

HPM アプリケーションは、イベントビューアおよび Report Manager アプリケーションを補完します。以下を参照してください。

- **イベントビューア**：ASA および FWSM デバイス、それぞれのセキュリティコンテキストの syslog（システムログ）イベント、さらに IPS デバイスおよび仮想センサーの Secure Device Event Exchange（SDEE）イベントを対象にネットワークをモニターします。対象イベントには、ファイアウォール トラフィック情報、NAT イベント、フェイルオーバーイベント、IPS アラートなどが含まれます。イベントビューアは、この情報を収集して表示し、さまざまなビューに編成します。詳細については、Event Viewer 機能の概要 （3473 ページ）を参照してください。
- **Report Manager**：ASA および IPS デバイス、リモートアクセス IPsec および SSL VPN のネットワーク使用状況とセキュリティ情報を収集、表示、およびエクスポートします。各レポートには、上位の送信元、宛先、攻撃者、被害者などのセキュリティデータ、および上位の帯域幅、期間、スループットユーザーなどのセキュリティ情報が集約されます。データは、時間別、日別、および月別の期間でも集約されます。詳細については、レポート管理について （3561 ページ）を参照してください。
- **Health and Performance Monitor**（HPM）：ネットワーク内の ASA および IPS デバイスの主要な正常性、パフォーマンス、および VPN データを監視および表示します。この情報には、メモリ使用量、インターフェイスステータス、ドロップされたパケット、トンネルステータスなど、重大な問題と重大ではない問題が含まれます。また、デバイスを通常または優先監視用に分類し、優先デバイスに異なるアラートルールを設定できます。

表示されたアラートにメモを追加したり、アラートを「確認」したり、削除したりできます。アラートがクリアされると、[アラート（Alerts）] の表示から削除されます。ただし、アラート情報はデータベースに 30 日間保持されます。メモの追加、アラートの確認とクリアの詳細については、アラート：確認応答とクリア （3664 ページ）を参照してください。

（注） アラート：履歴 （3665 ページ）の説明に従い、[アラート履歴（Alerts History）] ウィンドウを使用して、以前クリアされたアラートにアクセスして表示できます。

ここでは、次の内容について説明します。

- トレンド情報 （3612 ページ）
- マルチコンテキストのモニタリング （3613 ページ）

トレンド情報

Health and Performance Monitor は、監視対象デバイスを定期的にポーリングして、ステータスとパフォーマンスデータを取得します。この情報はアラートの生成に使用されるほか、集計データに基づいてリアルタイムビューと過去の傾向を表示するために使用されます。

特定のメトリックセットに関する傾向が、グラフで表示されます。現在選択されているデバイスの各傾向が、選択した時間間隔で生成されたグラフとして表されます。たとえば、CPU およびメモリ使用量の現在の値と週平均を比較することで、選択したデバイスの運用に関するコン

テキストが得られます。監視対象デバイスで利用可能な傾向の間隔は、1時間、24時間、および1週間です。

傾向の生成に使用される指標には、次のものがあります。

- CPU 使用率
- メモリ使用量（シングルコンテキスト デバイスのみ）
- 1 秒あたりの接続数（ファイアウォールデバイス）
- 1 秒あたりの翻訳数（ファイアウォールデバイス）
- インスペクションの負荷（IPS デバイス）
- 欠落したパケットの割合（IPS デバイス）
- VPN トンネルの数
- RA VPN セッションの数
- VPN の合計スループット
- ファイアウォールのスループット
- ドロップされたパケットの総数（ファイアウォール インターフェイス）

特定のデバイスのヘルスとパフォーマンスに関して、その他のグラフィック情報を確認するには、デバイス、クラスターノード、またはマルチコンテキストデバイスのシステムコンテキストのエントリを右クリックし、ポップアップメニューから [デバイスマネージャ（Device Manager）] を選択することで、関連するデバイスマネージャを起動できます。デバイスマネージャの詳細については、デバイス マネージャの起動 （3697 ページ）を参照してください。

マルチコンテキストのモニタリング

Health and Performance Monitor は、単一および複数のコンテキストの ASA デバイスをモニターできます。マルチコンテキストデバイスの場合、各コンテキストがモニターされ、個別のデバイスとして表示されます。

各コンテキストは、該当するすべてのメトリックに対して個別にポーリングされます。HPM は、任意のデバイスから一度に最大 5 つのコンテキストをポーリングします。5 つ以上のコンテキストを持つデバイスの場合、データは5つのコンテキストの連続する各バッチから取得され、各バッチは連続するポーリングサイクル中に徐々にポーリングされます。これは、すべてのコンテキストが同時に更新されない可能性があることを意味します。

マルチコンテキストデバイスの場合、基本的な Device Health（メモリ使用量、デバイスステータスなど）は物理デバイスでのみ（つまり、システムコンテキストから）モニターされますが、トラフィックデータ（接続数、変換数、ドロップされた数）は、コンテキストレベルでモニターされます。

仮想コンテキストの場合、CPU使用率データはパターン分析にのみ使用され、アラート生成には使用されません。仮想コンテキストについては、インターフェイス ステータス アラートのみが生成されます。

HPM アクセス制御

ユーザー名に対して割り当てられる権限により、Health and Performance Monitor で行うことができる操作が制御されます。ローカルユーザーまたは他のタイプの ACS 以外のアクセスコントロールを使用している場合は、すべてのユーザーが HPM にアクセスできます。ただし、次のアクセス制限が課されます。

- Security Manager でヘルスとパフォーマンスのモニタリングを有効または無効にするには、[Health and Performance Monitor] ページ （690 ページ）で説明されているように、システム管理者権限が必要です。
- デバイスを監視対象として選択または選択解除するためには、 監視対象デバイスの管理 （3616 ページ） で説明されているように、システム管理者、ネットワーク管理者、または承認者権限が必要です。
- アラートと通知を構成するには、 アラート：設定 （3654 ページ） で説明されているように、システム管理者、ネットワーク管理者、または承認者権限も必要です。

ACS を使用して Security Manager へのアクセスを制御する場合は、次も制御できます。

- [表示（View）] > [Health and Performance Monitor] 権限（ACS の Role Management の一部）を使用して、Health and Performance Monitor アプリケーションへのアクセスを制御できます。この権限を使用して、特定のユーザーが HPM にアクセスできないようにしたり、イベントビューアまたは Report Manager へのアクセスを許可せずに HPM へのアクセスを許可するロールを作成したりすることができます。すべてのデフォルトの ACS ロールは、Health and Performance Monitor アプリケーションの使用が許可されています。
- [変更（Modify）] > [ポリシー（Policy）] > [HPMモニタリング（HPM Monitoring）] 特権を使用して、監視対象のデバイスを選択および選択解除できるユーザーを制御したり（監視対象デバイスの管理 （3616 ページ）を参照）、アラートと通知を設定したり（アラート：設定 （3654 ページ）を参照）、アラートに注釈を付けて確認したり（アラート：確認応答とクリア （3664 ページ）を参照）することができます。ヘルプデスクとスーパー管理者を除くすべてのデフォルトの ACS ロールには、この権限があります。
- ユーザーは、少なくともデバイスの表示権限を持っている場合にのみ、デバイスの正常性とパフォーマンスの情報を表示できます。
- [Health and Performance Monitor] ページ （690 ページ）で説明されているように、HPM を有効化または無効化するヘルスとパフォーマンスのモニタリングの管理設定ページ（Security Manager の Configuration Manager 内）へのアクセスを制御できます。このページ（またはその他の管理設定ページ）にアクセスするには、ユーザーは[変更（Modify）]>[ポリシー（Policies）] > [HPM管理者（HPM Admin）] 権限を持っている必要があります。ヘルプデスクを除くすべてのデフォルト ACS ロールがこのページを表示できますが、設定を変更できるのはシステム管理者だけです。

Cisco Security Manager と Cisco Secure ACS との統合の詳細については、Cisco Security Manager インストレーションガイド [英語] を参照してください。

正常性とパフォーマンスのモニタリングの準備

Health and Performance Monitor（HPM）を使用するには、次のように Security Manager を設定し、HPM アプリケーションを有効にし、デバイスモニタリングを設定する必要があります。

- ACL ドロップパケット、スキャン脅威ドロップパケット、インスペクション ドロップ パケット、および SYN 攻撃ドロップパケットなどのメトリックを監視するには、基本脅威検出を ASA 8.0 以降のデバイスで有効にする必要があります（基本脅威検出は、デフォルトで有効になっています）。
- 電子メールでアラート通知を受信するには、Security Manager サーバーの [システム設定（System Preferences）] ページで、SMTP サーバーと管理者の電子メール ID を設定しておく必要があります。詳細については、『*Installation Guide for Cisco Security Manager*』を参照してください（Health and Performance Monitor アプリケーションからのアラート通知用電子メールアドレスの指定については、アラート：設定 （3654ページ）で説明されています）。
- [Health and Performance Monitor] ページ （690 ページ）で説明されているように、Security Manager で正常性とパフォーマンスのモニタリングを有効にする必要があります。
- 監視対象デバイスの管理 （3616ページ）で説明されているように、HPM で、通常モードと優先モードの両方でモニタリングするデバイスを指定します。

（注） ASA の読み取りタイムアウトを防ぐには、PIX ファイアウォール、ASA、および FWSM デバイスでの SSL（HTTPS）の設定 （74 ページ）で説明されているように、該当するデバイスが、サーバーとして動作するときに特定の SSL/TLS プロトコルバージョンのみを使用するように設定する必要があります。

- アラートと電子メール通知がトリガーされるタイミングを定義するデバイスのしきい値と状態変更ルールを有効にして設定します。このプロセスについては、アラート：設定 （3654 ページ）で説明します。

（注） また、タイミングの同期のため、Network Time Protocol（NTP）サーバーを使用するようにモニタリング対象デバイスを設定することをお勧めします。詳細については、[NTP] ページ （2624 ページ）を参照してください。

これらの手順を完了すると、HPM は指定されたデバイスのポーリングを開始し、正常性情報とアラートを表示します。

Health and Performance Monitor の起動

Health and Performance Monitor（HPM）を使用して、ネットワーク全体で監視対象のファイアウォールおよびIPSデバイスから収集されたステータス情報とアラートを表示します。モニタ対象のデバイスの選択の詳細については、監視対象デバイスの管理 （3616ページ）を参照してください。

HPM を起動するには、次のいずれかを実行します。

- Windows の [スタート] メニューから [すべてのプログラム] > [Cisco Security Manager Client] > [Cisco Security Manager Client] を選択し（コマンドパスは若干異なる場合があります）、ログイン時のデフォルトビューとして [Health and Performance Monitor] を選択します。
- Configuration Manager、イベントビューア、Image Manager、または Report Manager アプリケーションから、[起動（Launch）] > [Health and Performance Monitor] を選択します。
- Configuration Manager または Image Manager ウィンドウのクイック起動ツールバーにある [Health and Performance Monitor] ボタンをクリックします。

現在 Security Manager アプリケーションにログインしていない場合は、ログインするように求められます（Security Manager クライアント アプリケーションの起動とログインの詳細については、Security Manager へのログインおよび終了 （14 ページ）を参照してください）。それ以外の場合、他のアプリケーションへのログインに使用したのと同じユーザーアカウントを使用して、HPM ウィンドウ （3617 ページ）が開きます。

（注） 前述のように、HPM は他の Security Manager クライアント アプリケーションから「相互起動」できます。[起動（Launch）] メニューから目的のアプリケーションを選択するか、適切なクイック起動ボタンをクリックすることにより、Health and Performance Monitor から他のクライアント アプリケーションを同様に相互起動できます。

監視対象デバイスの管理

HPM デバイスセレクタは、「通常」と「優先」の両方の監視リストにデバイスを追加および削除するために使用されます。また、デバイスセレクタを使用して、2 つのリスト間でデバイスを転送できます。

（注） HPM でデバイスの監視を有効にした後、HPM パラメータの実際の値が [デバイスの概要（Device Summary）] に表示されるまで、優先デバイスの場合は最大 5 分、非優先デバイスの場合は 10 分かかることがあります。

HPM デバイスセレクタを使用するには、次の手順を実行します。

ステップ 1 [ツール（Tools）] メニューから [デバイスセレクタ（Device Selector）] を選択して、[デバイスセレクタ（Device Selector）] ウィンドウを開きます。デバイス管理画面が表示されます。

左側の [すべてのデバイス（All Devices）] セクションには、Cisco Security Manager インベントリ内の監視可能なすべての ASA デバイスと IPS デバイスが一覧表示されます。（例：HPM は、バージョン 7.0.1 以降の IPS センサーの監視のみをサポートします。以前の IPS バージョンはデバイスセレクタに表示されません）。

現在、通常監視リストと優先監視リストに割り当てられているすべてのデバイスが、ウィンドウの右側にある 2 つのセクションに表示されます。

ステップ 2 [通常（Normal）] リストにデバイスを追加するには、[すべてのデバイス（All Devices）] リストでデバイスを選択し、[すべてのデバイス（All Devices）] リストと [通常監視対象デバイス（Normal Monitored Devices）] リストの間にある [>] ボタンをクリックします。

デバイスを [優先監視対象デバイス（Priority Monitored Devices）] リストに移動する手順も同じです。[すべてのデバイス（All Devices）] リストと [優先監視対象デバイス（Priority Monitored Devices）] リストの間にある [>] ボタンを使用します。

ステップ 3 いずれかの [監視対象（Monitored）] リストからデバイスを削除して [すべてのデバイス（All Devices）] リストに戻すには、デバイスを選択して適切な [<] ボタンをクリックします。

ステップ 4 1 つの [監視対象（Monitored）] リストから別のリストにデバイスを転送するには、そのエントリを強調表示し、[上へ（Up）] または [下へ（Down）] ボタンをクリックして、上位または下位のリストに移動します。

ステップ 5 ウィンドウの下部にある [次へ（Next）] をクリックして、[VPNセレクタ（VPN-selector）] 画面を表示します。

すべての監視対象デバイスと個々のコンテキスト（ある場合）が一覧表示されます。各エントリには、リモートアクセス（RA）用のチェックボックスと、サイト間（S2S）VPN 選択用のチェックボックスが含まれています。

（注） Cisco Security Manager 4.10 以降、ASA 9.5(2) 以降のすべてのコンテキストがデバイスセレクタに一覧表示されます。デバイスセレクタで対応するチェックボックスをオンにすることで、すべてのユーザーコンテキストの RA およびサイト間 VPN を監視できるようになりました。

リストフィルターフィールドの使用 （3635 ページ）の説明に従い、このページの [リストフィルタ（List Filter）] フィールドを使用してリストをフィルタ処理できます。

ステップ 6 適切なボックスをオンにして、特定のデバイスで監視する VPN のタイプを選択します。

ステップ 7 [保存（Save）] をクリックして変更を保存して適用し、デバイスセレクタを閉じます。

HPM ウィンドウ

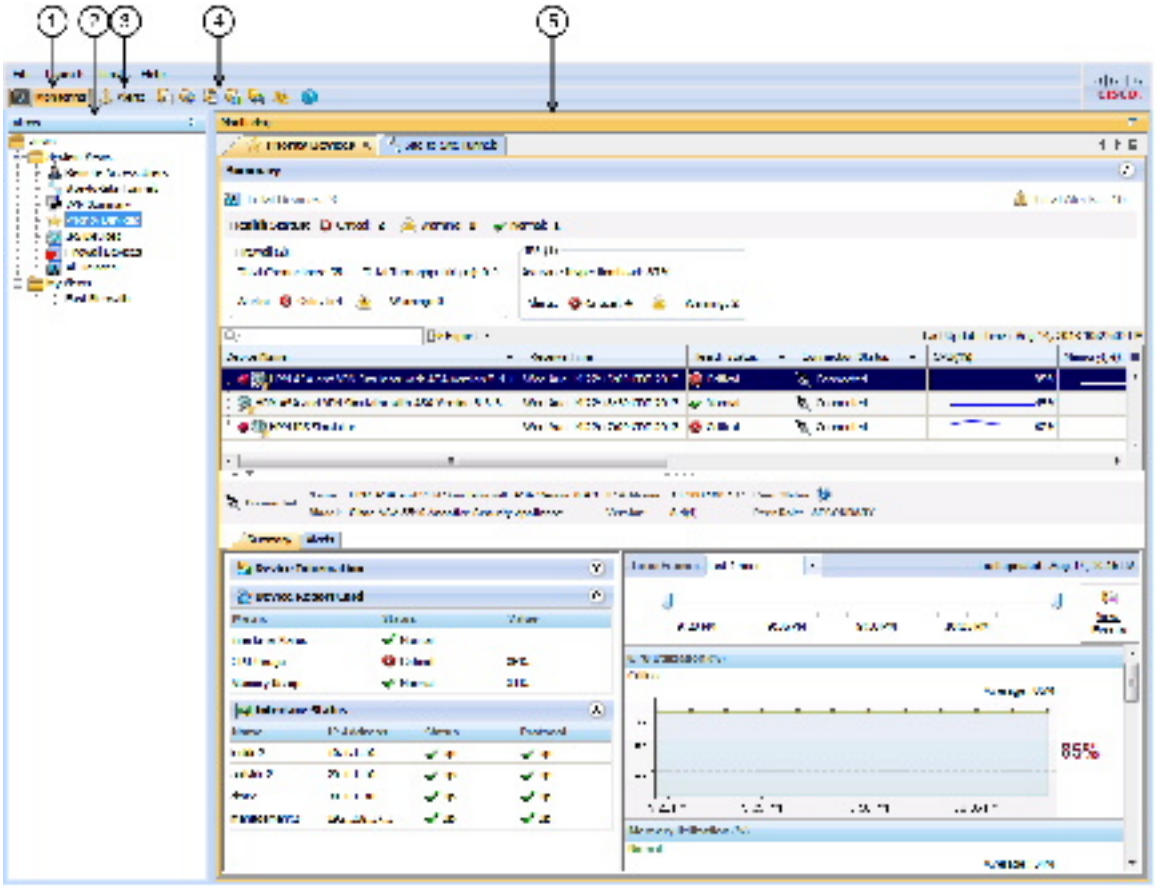
[ヘルスとパフォーマンスのモニタ（HPM）アプリケーション（Health and Performance Monitor (HPM) application）] ウィンドウでは、監視対象のファイアウォールおよび IPS デバイスから収

集されたステータス情報とアラート、およびネットワーク全体のリモートアクセス（RA）およびサイト間（S2S）VPN 情報を表示できます。

（注） 監視するデバイスの指定については、監視対象デバイスの管理 （3616ページ）を参照してください。

次の図は、[HPM] ウィンドウの主な機能を示しています。

図 *70 : [ヘルスとパフォーマンスのモニタ（Health and Performance Monitor）] ウィンドウ*



[ヘルスとパフォーマンスのモニタ（Health and Performance Monitor）] ウィンドウ

1	**モニタリングボタン。**	**4**	**クイック起動ボタン。**
2	ビュー	5	モニタリング/アラート表示エリア。
3	アラートボタン。		

[HPM] ウィンドウは、次の 3 つの主要な要素で構成されています。

- **監視ボタン（1）**：このボタンをクリックして、デバイスとVPNの正常性とパフォーマンスのデータを表示します。詳細については、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （3642 ページ）を参照してください。
- **ビュー（2）**：モニタリングビューでは、HPMメインウィンドウの左ペインに使用可能なビューのリストが表示されます。詳細については、デバイスビューの管理 （3637ページ）を参照してください。

次の図に示します。

- **アラートボタン（3）**：このボタンをクリックすると、ウィンドウの表示エリアにアラートのテーブルが表示されます。詳細については、HPM ウィンドウ：アラートディスプレイ （3652 ページ）を参照してください。
- **クイック起動ボタン（4）**：任意のボタンをクリックして、関連するSecurity Managerクライアント アプリケーションを相互起動します。
- **モニタリング/アラート表示エリア（5）**：ウィンドウのこのセクションには、デバイスとVPNのモニタリング情報、またはモニタリング対象デバイスによって生成されたアラートのテーブルが表示されます。[モニタリング（Monitoring）] ボタンと [アラート（Alerts）] ボタンを使用して、これら 2 つの表示を切り替えることができます。

テーブル列の操作

HPM に表示されるさまざまな情報テーブルは、次のようにカスタマイズできます。

- 特定の列のエントリが昇順または降順になるようにテーブルをソートします。
  - 列の見出しで、ドロップダウンメニューボタン以外の任意の場所をクリックすると、列のエントリが昇順になるようにテーブルがソートされます（小さな灰色の上矢印で示されます）。
  - 見出しを再度クリックすると、エントリが降順にソートされます（小さな灰色の下矢印で示されます）。
  - 見出しを再度クリックすると、テーブルが元の表示順序に戻ります（矢印アイコンが削除されます）。
- さまざまな列を表示したり非表示にします。表示できる列は各テーブルで異なります。
- 列にフィルタを適用します。つまり、指定した条件に一致するエントリのみがテーブルに表示されるようにします。

ここでは、次の内容について説明します。

- テーブル列の表示と非表示 （3620 ページ）
- 列ベースのフィルタリング （3632 ページ）

テーブル列の表示と非表示

情報のさまざまな列を非表示および表示することで、HPM に表示される各種テーブルをカスタマイズできます。表示可能な列はテーブルごとに異なります。

（注） 列見出しは、列ベースのフィルタリング （3632ページ）で説明されているように、選択したパラメータに従ってエントリを非表示または表示することにより、テーブルをさらにフィルタ処理するために使用できるメニューです。

テーブルに表示される特定の列を表示または非表示にするには、次の手順を実行します。

1. 列見出しの右側にある[列（Columns）]ボタンをクリックして、[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開きます。

現在のビューで使用できるすべての列が一覧表示されます。

1. 表示および非表示にする列を選択または選択解除します。
2. [OK] をクリックして、ダイアログボックスを閉じます。

このテーブルには、選択した列のみが表示されます。

次のトピックでは、さまざまなテーブルで使用できる個々の列について説明します。

- テーブル列：デバイス関連のビュー （3620 ページ）
- テーブル列：VPN 関連のビュー （3626 ページ）
- アラートテーブル列 （3631 ページ）

テーブル列：デバイス関連のビュー

情報のさまざまな列を非表示および表示することにより、デバイス関連のビューの [モニタリング（Monitoring）]ペインに表示されるテーブルをカスタマイズできます。表示可能な列は、ビューごとに異なります。

[表示する列を選択（Choose Columns to Display）] ダイアログボックスのエントリの順序には、列の表示順序が反映されています（ただし、次の表の行の順序には、列の表示順序が必ずしも反映されていません）。[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開く方法については、テーブル列の表示と非表示 （3620 ページ）を参照してください。

次の表は、デバイス関連のモニタリングビュー（[優先デバイス（Priority Devices）]、[IPS デバイス（IPS Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[すべてのデバイス（All Devices）]）およびこれらのシステムビューに基づくすべてのカスタムビューで使用可能なすべてのデータ列を示します。リストされている列の一部は、そこに示されているように、特定のビューでは使用できません。

表 *980* : デバイス関連のビューで使用可能なテーブル列

列名	ビューで使用可能	説明
デバイス名（Device Name）	IPS、ファイアウォール	デバイスに割り当てられている名前（つまり、[デバイスのプロパティ（Device Properties）] ウィンドウの [デバイスのプロパティ（Device Properties）]：[全般（General）] ページ （137 ページ）で定義されているホスト名）。 列ベースのフィルタリング （3632 ページ）を利用できます。 名前の前にデバイスタイプを示すアイコンが付いています。このアイコンの前にデバイスアラートインジケータが表示される場合もあります。赤色のドットは 1 つ以上の重大なアラート（および、場合によっては警告）を示し、黄色のドットは 1 つ以上の警告のみを示します。このエリアは、アラートのないデバイスの場合は空白になります。 ドットにマウスのポインタを合わせると、そのデバイスに関する重大なアラートの数と警告の数を表示するポップアップが表示されます。 デバイスアイコン自体に金色の星が付加されている場合は、優先監視対象デバイスであることを示しています。
Receive Time	IPS、ファイアウォール	このエントリのポーリング日時（形式：曜日 MMM DD HH:MM:SS タイムゾーン YYYY）。
IPアドレス	IPS、ファイアウォール	このデバイスの IP アドレス。 列ベースのフィルタリング （3632 ページ）を利用できます。
ヘルス ステータス	IPS、ファイアウォール	デバイスの現在の全体的な正常性（[クリティカル（Critical）]、[警告（Warning）]、または [正常（Normal）]）。 列ベースのフィルタリング （3632ページ）を利用できます。 （注） 全体的な正常性は、正常性メトリックの中で最も重要なメトリックで定義されます。たとえば、デバイスで選択されたメトリックが、1 つのクリティカルを除いてすべて正常であっても、全体的な Device Health はクリティカルになります。

列名	ビューで使用可能	説明
接続ステータス	IPS、ファイアウォール	HPM がデバイスに接続可能またはデバイスをポーリング可能かどうかを示します（[接続済み（Connected）]、[認証エラー（Authentication Error）]、[証明書の不一致エラー（Certificate Mismatch Error）]、[接続エラー（Connection error）]、[読み取り操作中のタイムアウト（Timeout during Read operation）]、または [サービスが利用できません（Service unavailable）]）。列ベースのフィルタリング （3632 ページ）を利用できます。 （注） デバイスが HPM（[ツール（Tools）] > [デバイスセレクタ（Device Selector）]）で通常または優先監視対象デバイスとして選択されていない場合、このステータスは適用されません。監視対象デバイスの選択に対する変更が有効になり、画面に反映されるまで数分かかる場合があります。 「接続済み」ではないデバイスについて表示される情報は、接続が失敗する前の、示されている受信時間のものです。
[メモリ（%）（Memory (%)）]	IPS、ファイアウォール	メモリの総使用可能容量に対する使用率。
[CPU（%）]	IPS、ファイアウォール	CPU の総使用可能容量に対する使用率。
モデル	IPS、ファイアウォール	デバイスのタイプとモデル番号。ASA 5510、IPS 4270 などです。
バージョン	IPS、ファイアウォール	このデバイスで実行されているソフトウェアのバージョン。列ベースのフィルタリング （3632 ページ）を利用できます。
[検査負荷（%）（Inspection Load (%)）]	IPS	ポーリング時のデバイスの検査負荷（パーセンテージ）。
[受信できなかったパケット（%）（Missed Packet(%)）]	IPS	検査されたパケットの総数に対するドロップされたパケットの割合。
[センサーアプリケーションのステータス（Sensor App Status）]	IPS	現在のセンサーアプリ（分析エンジン）のステータス（[稼働（Up）]または [ダウン（Down）]）。列ベースのフィルタリング （3632 ページ）を利用できます。

列名	ビューで使用可能	説明
[メインアプリのステータス（Main App Status）]	IPS	現在のメインアプリのステータス（[稼働（Up）]または [ダウン（Down）]）。列ベースのフィルタリング（3632 ページ）を利用できます。
[コラボレーションアプリケーションのステータス（Collaboration App Status）]	IPS	現在のコラボレーションアプリのステータス（[稼働（Up）] または [ダウン（Down）]）。
[ライセンス有効期限ステータス（License Expiration Status）]	IPS	センサーに設定されている赤色および黄色のしきい値に基づくセンサーのライセンスステータス（[正常（Normal）]、[警告（Warning）]、または [クリティカル（Critical）]）。列ベースのフィルタリング （3632 ページ）を利用できます。
[バイパスモード状態（In Bypass Mode）]	IPS	センサーでバイパスモードが有効になっているかどうか（[はい（Yes）] または [いいえ（No）]）。列ベースのフィルタリング （3632ページ）を利用できます。
[イベント取得ステータス（Event Retrieval Status）]	IPS	IPS イベント取得のステータス（[正常（Normal）]、[警告（Warning）]、または [クリティカル（Critical）]）。列ベースのフィルタリング （3632 ページ）を利用できます。
[グローバル相関ステータス（Global Correlation Status）]	IPS	グローバル相関に参加しているセンサーの場合、その更新ステータス（[正常（Normal）]（前回の更新が成功）、[警告（Warning）]（過去 1 日間つまり 86,400 秒以内に更新が成功していない）、または [クリティカル（Critical）]（過去 3 日間つまり 259,200 秒以内に更新が成功していない））。列ベースのフィルタリング （3632 ページ）を利用できます。
シグニチャ アップデート	IPS	このセンサーに適用された最新のシグニチャアップデートの数（たとえば、S574）。列ベースのフィルタリング （3632 ページ）を利用できます。
ファイアウォールモード	Firewall	このデバイスの動作モード（[ルーテッド（Routed）]、[トランスペアレント（Transparent）]、または [混合（Mixed）]）。列ベースのフィルタリング （3632ページ）を利用できます。
コンテキスト モード	Firewall	このデバイスのコンテキストモード（[シングル（Single）] または [マルチ（Multiple）]）。列ベースのフィルタリング （3632 ページ）を利用できます。

列名	ビューで使用可能	説明
接続（Connections）	Firewall	デバイスがポーリングされたときのアクティブな接続の数。
Xlates	Firewall	アドレス変換カウンタ。
[接続数/秒（Connections/second）]	Firewall	1 秒あたりの確立された接続の数。
[変関数/秒（Translations/second）]	Firewall	1 秒あたりの変換数。
フェールオーバー ステータス	Firewall	このデバイスがフェールオーバーペアの一部である場合、その現在の状態（[アクティブ（Active）] または [スタンバイ（Standby）]）。列ベースのフィルタリング （3632 ページ）を利用できます。
[フェールオーバー ホスト ロール（Failover Host Role）]	Firewall	このデバイスがフェールオーバーペアの一部である場合、その現在のロール（[プライマリ（Primary）] または [セカンダリ（Secondary）]）。列ベースのフィルタリング （3632 ページ）を利用できます。
[フェールオーバーピア ロール（Failover Peer Role）]	Firewall	このデバイスがフェールオーバーペアの一部である場合、そのピアデバイスの現在のロール（[プライマリ（Primary）] または [セカンダリ（Secondary）]）。列ベースのフィルタリング （3632 ページ）を利用できます。
[フェールオーバー ピア ステータス（Failover Peer Status）]	Firewall	このデバイスがフェールオーバーペアの一部である場合、そのピアの現在のステータス（[アクティブ（Active）] または [スタンバイ準備完了（Standby Ready）]）。列ベースのフィルタリング （3632 ページ）を利用できます。
Used Memory (MB)	Firewall	デバイスがポーリングされたときのメモリ使用容量（メガバイト単位）。列ベースのフィルタリング （3632 ページ）を利用できます。
[空きメモリ（MB）（Free Memory (MB)）]	Firewall	デバイスがポーリングされたときのメモリ使用可能容量（メガバイト単位）。列ベースのフィルタリング （3632 ページ）を利用できます。
[最大接続数（Max. Connections）]	Firewall	接続のピーク数。ASA グループでは使用できません。

列名	ビューで使用可能	説明
[Xlate の最大数（Max. Xlates）]	Firewall	アドレス変換のピーク数。ASA グループでは使用できません。
Throughput (Kbps)	Firewall	デバイスの平均スループット（キロビット/秒単位）。ASA 9.0 以降のクラスタの場合、これはグループに含まれるすべてのインターフェイスの総スループットです。
[ACL ドロップパケット（ACL Dropped Packets）]	Firewall	アクセス制御リストルールに違反したためにドロップされたパケットの数。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[スキャン脅威ドロップパケット（Scanning Threat Dropped Packets）]	Firewall	スキャン脅威検出が有効になっている場合、スキャン脅威インスペクションに失敗したためにドロップされたパケットの数。有効になっていない場合は、[適用なし（NA）] と表示されます。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[インスペクション ドロップ パケット（Inspection Dropped Packets）]	Firewall	アプリケーションインスペクションが有効になっている場合、アプリケーションインスペクションに不合格になったためにドロップされたパケット数。有効になっていない場合は、[適用なし（NA）] と表示されます。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[SYN 攻撃ドロップパケット（Syn Attack Dropped Packets）]	Firewall	SYN フラッディングのためにドロップされたパケットの数。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。
[総インターフェイス ドロップ パケット（Total Interface Dropped Packets）]	Firewall	すべてのインターフェイスでドロップされたパケットの総数。ASA クラスタではクラスタレベルでのみ使用できます。個別のノードでは使用できません。 （注） インターフェイスごとのドロップされたパケットの数は、選択したデバイスの [詳細（detail）] セクションに表示されるタブ付きの [インターフェイス（Interface）] パネルで確認できます。
[分析エンジンメモリ（%）（Analysis Engine Memory (%)）]	IPS	現在使用中の分析エンジンに割り当てられているメモリの割合。

列名	ビューで使用可能	説明
[グループでのロール（Role in Group）]	Firewall	ASA ロードバランシンググループのこのメンバーのロール（[グループ（Group）]、[制御（Control）]、または [データ（Data）]）。 グループは、複数のノードを持つ単一のデバイスとして Security Manager によって管理されます。そのため、各グループは HPM に単一のエントリとして表示されます。これを展開するとノードのリストを表示できます。
* これらの列はすべて、[すべてのデバイス（All Devices）] ビューと [優先デバイス（Priority Devices）] ビューで使用できます。		

テーブル列：VPN 関連のビュー

情報のさまざまな列を非表示および表示することにより、VPN 関連のビューの [モニタリング（Monitoring）]ペインに表示されるテーブルをカスタマイズできます。表示可能な列は、ビューごとに異なります。

[表示する列を選択（Choose Columns to Display）] ダイアログボックスのエントリの順序には、列の表示順序が反映されています（ただし、次の表の行の順序には、列の表示順序が必ずしも反映されていません）。[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開く方法については、テーブル列の表示と非表示 （3620 ページ）を参照してください。

次の表に、VPN 関連のモニタリングビューで使用可能なすべてのデータ列を示します。[リモートアクセスユーザー（RA）（Remote Access Users (RA）]、[サイト間トンネル（S2S）（Site-to-Site Tunnels (S2S)）]、[VPNサマリー（VPN Summary）]、およびこれらのシステムビューに基づくすべてのカスタムビュー。表示されている列の一部は、示されているように、特定のビューでは使用できません。

デバイスがトラップメッセージを送信すると、Cisco Security Manager はトラップをキャプチャし、Health and Performance Monitoring アプリケーションの [サイト間トンネル（Site to Site Tunnels）] ページに送信します。Cisco Security Manager バージョン 4.16 までは、IPv4 経由でのみトラップメッセージを送信するためにデバイスが使用されていました。Cisco Security Manager 4.17 以降、SNMP トラップは IPv6 を使用してキャプチャされるため、Cisco Security Manager はトラップメッセージを受信します。また、デバイスの IPv6 アドレスをデバイスの詳細にマッピングし、Health and Performance Monitoring アプリケーションの [サイト間トンネル（Site to Site Tunnels）] ページにトラップに関するアラートを表示します。ステータスは、数回の更新サイクルの後、Health and Performance Monitoring アプリケーションに表示されます。

（注） Cisco Security Manager バージョン 4.9 以降、Health and Performance Monitoring アプリケーションは、IPv4 ベースのトンネルに加えて、IPv6 アドレスが設定されているサイト間トンネルを監視および表示します。また、電子メールとトラップの通知には、IPv4 アドレスに加えて IPv6 アドレスが含まれるようになりました。

表 *981 : VPN* 関連のビューで使用可能なテーブル列

列名	ビューで使用可能	説明
Receive Time	RA、S2S、VPNサマリー（VPN Summary）	このエントリのポーリング日時（形式：曜日 MMM DD HH:MM:SS タイムゾーン YYYY）。
ファイアウォール名（Firewall Name）	RA、S2S、VPNサマリー（VPN Summary）	Cisco Security Manager インベントリで提供されるこのデバイスの名前。列ベースのフィルタリング （3632 ページ）を利用可能。
ユーザー名	RA	このセッションを確立するために使用されるユーザーログイン名。列ベースのフィルタリング （3632 ページ）を利用可能。
ユーザーグループポリシー（User Group Policy）	RA	このユーザーが属する ASA VPN ユーザーグループの名前。 列ベースのフィルタリング （3632 ページ）を利用可能。
ゲートウェイ	RA	ユーザーが接続している VPN ゲートウェイの IP アドレス。列ベースのフィルタリング （3632 ページ）を利用可能。
割り当てられている IP	RA	このセッションのリモートクライアントに割り当てられたプライベート IP アドレス。「内部」または「仮想」IP アドレスとも呼ばれています。
Public IP	RA	クライアントに割り当てられた、公開されているルーティング可能な IP アドレス。 列ベースのフィルタリング （3632ページ）を利用可能。
接続開始時間（Connection Initiation Time）	RA	接続が開始された日時（HH:MM:SS 曜日 MMM DD YYYY）。時刻は 24 時間形式の協定世界時（UTC）で表示されます。
期間	RA	セッションの開始から最新のデバイスポーリングまでの経過時間（HH:MM:SS）。

列名	ビューで使用可能	説明
クライアントバージョン（Client Version）	RA	リモートピアで実行されている VPN クライアントソフトウェアとバージョン。AnyConnect Windows 3.0、Mozilla 4.0 など。列ベースのフィルタリング （3632 ページ）を利用可能。
エンドポイントOS（EndPoint OS）	RA	リモートピアで使用中のオペレーティングシステム。Windows、Windows NT など。列ベースのフィルタリング （3632ページ）を利用可能。
認証方式	RA	ユーザーパスワード、証明書、または事前共有キー。列ベースのフィルタリング （3632 ページ）を利用可能。
暗号化（Encryption）	RA、S2S	このセッションが使用しているデータ暗号化アルゴリズム。列ベースのフィルタリング （3632 ページ）を利用可能。
トンネル タイプ	RA、VPNサマリー（VPN Summary）（[タイプ（Type）] のみ）	トンネルまたは接続のタイプ。クライアントレス、IPsec、および AnyConnect が含まれます。列ベースのフィルタリング （3632ページ）を利用可能。
Throughput (Kbps)	RA、S2S	受信バイト数と送信バイト数（キロビット/秒）。
セッションID（Session ID）	RA	このセッションに割り当てられた識別子。
非アクティブ時間（Inactive Time）	RA	このセッションが非アクティブだった時間。
IPアドレス	S2S、VPNサマリー（VPN Summary）	このデバイスの IP アドレス。列ベースのフィルタリング （3632 ページ）を利用可能。
Local Endpoint	S2S	ローカル トンネル インターフェイスの IP アドレス。
リモートエンドポイント	S2S	リモート トンネル インターフェイスの IP アドレス。
ローカルサブネット（Local Subnet）	S2S	ローカルで保護されたサブネットのアドレス。
リモートサブネット（Remote Subnet）	S2S	リモートで保護されたサブネットのアドレス。

列名	ビューで使用可能	説明
アップタイム（Uptime）	S2S	このトンネルの現在の継続時間。
[接続時間（Connection Time）]	S2S	接続が開始された日時（HH:MM:SS 曜日 MMM DD YYYY）。時刻は 24 時間形式の協定世界時（UTC）で表示されます。
ステータス	S2S	トンネル接続ステータス。[アップ（Up）] または [ダウン（Down）] になります。トンネルが指定された回数ダウンすると、アラートが発行されます。詳細については、列ベースのフィルタリング （3632 ページ）を参照してください。 **ヒント** [ステータス（Statu）] 列の [ダウン（Down）] 通知ハイパーリンクをクリックして、イベントビューアでそのデバイスの IPSec VPN イベントを表示できます。イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。
ヘルス ステータス	VPNサマリー（VPN Summary）	基礎となるデバイスの現在の全体的な正常性：[クリティカル（Critical）]、[警告（Warning）]、または [正常（Normal）]。列ベースのフィルタリング （3632 ページ）を利用可能。 （注） 全体的な正常性は、正常性メトリックの中で最も重要なメトリックで定義されます。たとえば、デバイスで選択されたすべてのメトリックが、重要なメトリックを除いて正常である場合、全体的な Device Health がクリティカルになります。
接続ステータス	VPNサマリー（VPN Summary）	リモート接続ステータス。常に [接続済み（Connected）] になります（HPM は以前の接続に関する情報を表示できません）。列ベースのフィルタリング （3632 ページ）を利用可能。

列名	ビューで使用可能	説明
モニタリングタイプ（Monitoring Type）	VPNサマリー（VPN Summary）	監視されている VPN 接続のタイプ。 列ベースのフィルタリング （3632ページ）を利用可能。
アクティブセッション（Active Sessions）	VPNサマリー（VPN Summary）	現在アクティブなセッション（S2S、IPSec RA、クライアントベースの SSL RA、およびクライアントレス SSL RA）。
ピークセッション数（Peak Sessions）	VPNサマリー（VPN Summary）	同時セッションのピーク数（S2S、IPSec RA、クライアントベースの SSL RA、およびクライアントレス SSL RA）。
ユーザ総数	VPNサマリー（VPN Summary）	現在のリモートユーザーの合計（S2S、IPSec RA、クライアントベースの SSL RA、およびクライアントレス SSL RA）。
非アクティブセッション	VPNサマリー（VPN Summary）	非アクティブセッションの数。
合計VPNスループット（Kbps）（Total VPN Throughput (Kbps)）	VPNサマリー（VPN Summary）	すべての VPN トラフィックの合計。つまり、RA と S2S のスループット値の合計（キロビット/秒）。列ベースのフィルタリング （3632ページ）を利用可能。
ACL Name	サイト間トンネル（Site-to-Site Tunnels）	バージョン 4.9 以降、Cisco Security Manager では、選択したサイト間トンネルに関連付けられているアクセス制御リスト（ACL）名を表示できます。この列名はデフォルトで選択されています。 （注） Health and Performance アラートの表示で、トンネルアップ/ダウンアラートの [説明（Description）] 列に ACL 名も表示されるようになりました。同様に、電子メールおよびトラップ通知の [説明（Description）] 列にも ACL 名が表示されます。
備考	サイト間トンネル（Site-to-Site Tunnels）	（任意）この列には、[ACL名（ACL Name）] に対応する注釈が表示されます。 （注） アラート、電子メール、およびトラップ通知には、説明フィールドの一部として [注釈（Remarks）] は含まれていません。

列名	ビューで使用可能	説明
制限事項： Cisco Security Manager Daemon Manager サービスが開始されると、HPM アプリケーションは Configuration Archive の最新の構成を使用して、サイト間 VPN トンネルに関連付けられた [ACL名（ACL Name）] と [注釈（Remarks）] を抽出します。VPN トンネルが HPM によって識別されると、抽出されたデータを使用して、S2S ビューに [ACL名（ACL Name）] と [注釈（Remarks）] の列が表示されます。HPM でデータが使用可能になる前に VPN トンネルが起動した場合、次の UI 更新まで、 [ACL名（ACL Name）] と [注釈（Remarks）] の列にデータが表示されないことがあります。同様に、HPM によってデータが抽出される前にアラートが生成された場合、アラートの表示の [説明（Description）] 列に [ACL名（ACL Name）] が表示されないことがあります。これは、以前のバージョンから Cisco Security Manager バージョン 4.9 へのアップグレード中に発生する可能性があります。次回のポーリングで同じアラートが表示された場合、[ACL名（ACL Name）] が [説明（Description）] に追加されます。 **ヒント**： [注釈（Remarks）] 列の内容に相違がある場合があります。Configuration Archive の最新の構成に [注釈（Remarks）] が含まれているか確認します。アウトオブバンドの変更により [注釈（Remarks）] が追加または更新された場合は、デバイスを再検出する必要があります。		

アラートテーブル列

情報のさまざまな列を非表示または表示することにより、アラートテーブルをカスタマイズできます。

[表示する列を選択（Choose Columns to Display）] ダイアログボックスのエントリの順序には、表示される際の列の順序が反映されています（ただし、次の表の行の順序には、表示される列の順序が必ずしも反映されていません）。[表示する列を選択（Choose Columns to Display）] ダイアログボックスを開く方法については、テーブル列の表示と非表示 （3620ページ）を参照してください。

表 *982*：アラートテーブルで使用可能なデータ列

列名	説明
デバイス名（Device Name）（常に選択）	このアラートがトリガーされたデバイスの名前で、Cisco Security Manager インベントリで提供されます。列ベースのフィルタリング （3632ページ）で利用可能。
ノード	このアラートが ASA ロードバランシングクラスタのメンバーによって生成された場合のノード名です。列ベースのフィルタリング （3632ページ）で利用可能。
デバイスタイプ	デバイスのタイプ：ASA または IPS。列ベースのフィルタリング （3632ページ）で利用可能。

列名	説明
重大度	アラートの重大度：[クリティカル（Critical）]、[警告（Warning）]、または[正常（Normal）]。列ベースのフィルタリング （3632 ページ）で利用可能。
ステータス	現在のデバイスステータス：アクティブまたは確認済み。列ベースのフィルタリング （3632 ページ）で利用可能。
説明	アラートの説明。例、「Device Health がクリティカル」または「デバイスポーリング：認証エラー」など。
最初の確認	このアラートが最初に記録された日時（day-of-week MMM DD、YYYY HH:MM:SS AM/PM）。時間はユーザーのタイムゾーンに基づいています。列ベースのフィルタリング （3632 ページ）で利用可能。
最後の確認日時	このアラートが最後に記録された日時（day-of-week MMM DD、YYYY HH:MM:SS AM/PM）。時間はユーザーのタイムゾーンに基づいています。列ベースのフィルタリング （3632 ページ）で利用可能。
注記	アラートの確認時に、注釈を付けることができます。すべての注釈はこのフィールドに表示されます。詳細については、アラート：確認応答とクリア （3664 ページ）を参照してください。

列ベースのフィルタリング

特定の列の内容に基づいて HPM 内のさまざまなテーブルをフィルタ処理できます。列フィルタを適用すると、その列に指定された基準を持つエントリのみが含まれるようにテーブルがフィルタ処理されます。

（注） テーブルの表示を変更する他の方法については、テーブル列の操作 （3619ページ）参照してください。

ヒント

- 列フィルタは累積的です。フィルタ処理されたテーブルにエントリが表示されるには、すべての列フィルタ基準を満たす必要があります。論理和を取った列フィルタのセットは作成できません。
- すべてではありませんが、ほとんどのカラムの内容に対してフィルタリングできます。カラムに下矢印がない場合は、そのカラムに対してはフィルタリングできません。たとえば、[すべてのデバイス（All Devices）] ビューの [受信時間（Receive Time）] ではフィルタ処理できません。
- フィルタアイコン（じょうご）はフィルタリングされたカラムの見出しに表示されます。

- 使用可能なカラムの詳細については、テーブル列の表示と非表示 （3620ページ）を参照してください。

特定の列パラメータに従ってテーブルをフィルタ処理するには、次の手順を実行します。

列の見出しの下向き矢印をクリックし、ドロップダウンメニューから次のいずれかを選択します。

- [すべて（All）]：この列からフィルタを削除または「元に戻す」には、[すべて（All）]を選択します。テーブルが更新され、このパラメータのすべてのエントリが表示されます。たとえば、[アラート（Alerts）]テーブルの [重大度（Severity）] 列をフィルタ処理して [クリティカル（Critical）] アラートのみを表示した場合、このオプションを選択すると、すべての [クリティカル（Critical）] アラートと [警告（Warning）] アラートが再表示されます。
- [カスタム（Custom）]：[カスタム（Custom）] を選択すると、その列の情報に基づいてカスタムフィルタを作成できる [カスタムフィルタ（Custom Filter）] ダイアログボックスが開きます。詳細については、カスタムフィルタ処理 （3633 ページ）を参照してください。
- 特定のエントリ：ドロップダウンメニューには、列に関連するすべての値が含まれています。1 つの値を選択して、そのエントリのグループのみを表示します。たとえば、[アラート（Alerts）]テーブルの [重大度（Severity）] 列から [クリティカル（Critical）] を選択して、テーブルをフィルタ処理し、[クリティカル（Critical）] アラートのみ表示します。

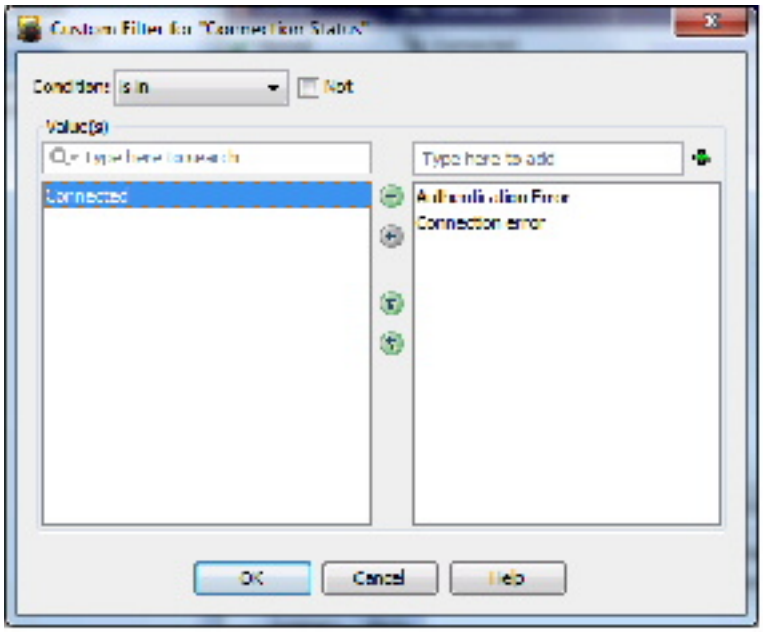
カスタムフィルタ処理

次の手順では、列のドロップダウンリストから単純に値を選択しない、カスタム列ベースのフィルタを作成する方法について説明します。他の列ベースのフィルタリングオプションについては、HPM ウィンドウ：アラートディスプレイ （3652 ページ）を参照してください。

ステップ 1 列の見出しの下向き矢印をクリックし、ドロップダウンメニューから [カスタム（Custom）] を選択します。

選択した列に対して [カスタムフィルタ（Custom Filter）] ダイアログボックスが開きます。

ステップ 2 [Custom Filter] ダイアログボックスで目的の値を選択します。次の図に、このダイアログボックスの一般的な例を示します。



以下は、[カスタムフィルタ（Custom Filter）]ダイアログボックスに表示される可能性のあるコントロールです（すべてのインスタンスにすべてのコントロールが表示されるわけではありません）。

- [条件（Condition）]：選択した [値（Values）] に適用される条件を選択します。

通常、これは **is in** です。つまり、選択した各 [値（Values）] は、そのエントリがフィルタ処理されたテーブルに表示されるためには、列に「含まれている」必要があります。

- [否定（Not）]：負の条件を作成するには、このボックスをオンにします。

is in が条件として選択されている場合、選択された [値（Values）] が列に存在できないことを意味します。つまり、列にこれらの [値（Values）] を持つエントリが表示されないように、テーブルがフィルタ処理されます。

- [値（Values）] リスト：ダイアログボックスのいくつかのインスタンスには、選択する [値（Values）] の 1 つのリストが表示されるので、目的のオプションをオンにします。

使用可能な [値（Values）] と選択された [値（Values）] のリスト：ほとんどの場合、ダイアログボックスには、前の図に示すように 2 つの [値（Values）] のリストが表示されます。カスタムフィルタの値を選択するには、列で使用可能な値が含まれている左側のリストでその値を強調表示し、右矢印をクリックして右側の選択された値のリストに追加します。複数の値を選択できます。

使用可能な [値（Values）] リストの項目は、送信元テーブルの選択した列に現在表示されている値によって決定されます。

使用可能な値が多数ある場合は、リストの上にある [リストフィルタ（List Filter）] フィールドに特定の値を入力して検索できます。詳細については、リストフィルターフィールドの使用 （3635 ページ）を参照してください。

次の方法を使用して、値の選択または選択解除をすることもできます。

- 選択した [値（Values）] リストの上にあるテキストフィールドに値の名前を入力し、[+] ボタンをクリックします。選択した [値（Values）] にその値が追加されます。この方法は、使用可能な [値（Values）] が多数ある場合、または使用可能な [値（Values）] リストにない値をフィルタ処理する場合に役立ちます。
- 他方のリストに移動する、一方のリストの項目をダブルクリックします。
- いずれかの二重矢印ボタンをクリックして、選択した値に関係なく、すべての項目を 1 つのリストから別のリストに移動します。

ステップ 3 [OK] をクリックして、ダイアログボックスを閉じます。

テーブルが更新され、現在適用されているすべてのフィルタを満たすエントリのみが表示されます。

リストフィルターフィールドの使用

[リストフィルタ（List Filter）] フィールドは、[モニタリング（Monitoring）] 画面のデバイスおよびVPN リストの上、[アラート（Alerts）] 画面のアラートテーブルの上、デバイス セレクタの [VPN] ページのデバイスリストの上、および [クリアされたアラートの表示（View Cleared Alerts）] ウィンドウにあります。いずれの場合も、[リストフィルタ（List Filter）] フィールドを使用して、指定したテキスト文字列を含む関連テーブル内のエントリをすばやく見つけることができます。

（注） 見つかったテキストは、エントリに関連付けられたデータフィールドの一部にすることができます。たとえば、[アラートリストフィルタ（Alerts List Filter）] フィールドに「ライセンス（license）」と入力すると、アラートテーブルがフィルタリングされ、差し迫ったライセンスの期限切れに関連するアラートのみが表示されます。（関連するデータカラム（この例では [詳細（Detail）]）が表示されていなくても、一致したエントリが一覧表示されるため、混乱が生じる可能性があります。テーブルのカラムを非表示にする方法の詳細については、テーブル列の表示と非表示 （3620ページ）を参照してください）。

図 *71* : ヘルスとパフォーマンスの監視：*[リストフィルタ（List Filter）]* フィールド

1	[フィルタパラメータ（Filter-parameters）] ボタン	2	[Clear] ボタン

デバイスリスト、VPNリスト、アラートテーブル、または[クリアされたアラートの表示（View Cleared Alerts）]ウィンドウで特定のテキスト文字列を検索するには、次の手順を実行します。

- [リストフィルタ（List Filter）]フィールドをクリックしてテキストカーソルを置き、入力を開始します。

これらは「ライブフィルター」フィールドです。つまり、各文字を入力すると、現在のテキスト文字列を含まないエントリがリストまたはテーブルから削除されます。たとえば、アラートの広範なリストに「Device Health Critical,」のステータスが 1 つあり、他のアラートには、*hea* という文字を含むテキスト文字列が含まれていないとします。[リストフィルタ（List Filter）]フィールドを使用して、その 1 つのアラートをすばやく見つけたいので、「health」という単語の入力を開始します。最初の 3 文字を入力した後に表示されるのは、そのアラートだけです。

[リストフィルタ（List Filter）] フィールドをクリアするには：

- フィールドの右側にある [クリア（clear）] ボタンをクリックします。

このボタンは、フィールドへの入力を開始すると表示されます。（文字を強調表示して、キーボードの Delete キーまたは Backspace キーを押すこともできます）。

[リストフィルタ（List Filter）]フィールドをクリアすると、リスト内のすべてのエントリが再び表示されます。

検索する情報（カラム）を指定し、大文字と小文字を区別するか区別しないかを選択し、ワイルドカードまたは正規表現を許可し、返される文字列のどこに文字を配置すべきかを指定することにより、フィルタ結果を調整できます。

リストフィルタ条件を変更するには、次の手順を実行します。

1. [リストフィルター（List Filer）] フィールドの左側にある [filter-parameters] ボタン（虫眼鏡）をクリックして、パラメータメニューを開きます。
2. オプションを選択します。

メニューは 4 つのセクションで構成されています。

- 使用可能なすべての情報タイプのリスト：これらのエントリは、その特定のリストまたはテーブルに表示できるカラムに対応しています。[すべて（All）]を選択するか、個別のエントリを選択することができます。
- [大文字と小文字を区別する（Case sensitive）]および[大文字と小文字を区別しない（Case insensitive）]：いずれかを選択します。[大文字と小文字を区別する（Case sensitive）]を選択した場合、見つかったテキストは、入力した文字だけでなく、大文字と小文字も入力されたものと一致する必要があります。

- [ワイルドカードを使用する（Use wildcards）] および [正規表現を使用する（Use regular expression）] : いずれかを選択します。次のワイルドカードが認識されます。
- *****（アスタリスク）：文字列内のその位置にある 0 個以上の文字に一致します。
- **?**（疑問符）：文字列内のその位置にある 1 文字に一致します。
- [最初から一致（Match from start）]、[完全一致（Match exactly）]、および [一部が一致（Match anywhere）] : 1 つを選択します。[最初から一致（Match from start）]とは、入力した文字列がエントリの先頭で見つかる必要があることを意味します。ただし、より大きな文字セットの一部でも可能です。[完全一致（Match exactly）] では、入力した文字列がカラムエントリ全体と完全に一致する必要があります。[一部が一致（Match anywhere）] とは、文字列がエントリ内のどこかで見つかることを意味し、より大きな文字セットの一部でも可能です。
- 別のパラメータを変更するには、手順 1 と 2 を繰り返します。

デバイスのモニタリング

[HPM] ウィンドウ：[モニタリング（Monitoring）]ディスプレイ （3642 ページ）で説明するように、HPM モニタリング画面には、ビュー制御、ビューパネル、現在選択されているデバイスに関する詳細情報が表示されます。

モニタリング画面に切り替えるには、次の手順を実行します。

- HPM メニューバーの下にある [モニタリング（Monitoring）] ボタンをクリックします。

([アラート（Alerts）]画面に戻るには、[アラート（Alerts）] ボタンをクリックします。)

（注） 監視するデバイスの指定については、デバイスビューの管理 （3637 ページ）を参照してください。

ここでは、次の内容について説明します。

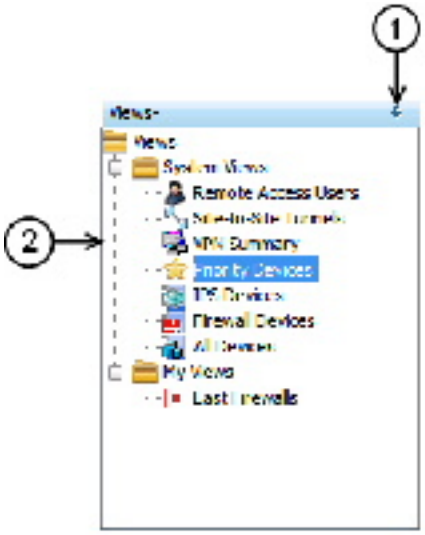
- デバイスビューの管理 （3637 ページ）
- [HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （3642 ページ）

デバイスビューの管理

「ビュー」は、HPM アプリケーションの [モニタリング（Monitoring）] ペインに表示される情報をフィルタ処理および整理するための手段を提供します。すべてのデバイス、ファイアウォールデバイス、リモートアクセスユーザーの詳細など、さまざまなシステムビューが提供されます。また、カスタムビューを作成して、地理的なデバイスの場所など、その他の方法で情報を整理することもできます。

HPM のメインウィンドウの左ペインには、次の図に示すように使用可能なビューのリストが表示されます。

図 *72 : Health and Performance Monitor* : *[ビュー（Views）]* ペイン *[ビュー（Views）]* ペインには、次のコントロールが含まれています。



- **(1) プッシュピンボタン**：ビューリストの表示を制御するには、プッシュピンボタンをクリックします。リストが HPM ウィンドウのペインとして表示されている場合（ピンが垂直）、このボタンをクリックするとペインがウィンドウの左端に折りたたまれ、ラベルの付いたタブが残ります。[モニタリング（Monitoring）] ペインが展開され、HPM ウィンドウ全体に表示されます。

タブの上にマウスポインタを合わせると、ビューリストを「ポップアウト」表示にできます。ポインタがタブまたはリスト領域にある限り、リストは表示されたままになります（ピンは水平）。また、タイトルバーの任意の場所（ピン自体を除く）をクリックして、リストを「ポップアウト」表示のままにすることもできます。

ピンをもう一度クリックすると、ビューリストが開いたペインとして再確立されます。[モニタリング（Monitoring）] ペインが縮小し、リストのための場所が確保されます。

- (2) ビューのリスト：リストは、[システムビュー（System Views）] と [マイビュー（My Views）] のフォルダに整理されます。ビュー：開閉 （3639 ページ）で説明されているように、いずれかのフォルダのエントリをクリックすると、そのビューが [モニタリング（Monitoring）] ウィンドウで開きます。[マイビュー（My Views）] フォルダに新しいビューを作成する方法については、ビュー：カスタム （3641 ページ）を参照してください。
- 右クリック ショートカット メニュー : [ビュー（Views）] リストのエントリを右クリックすると、ビュー関連のコマンドのポップアップメニューにアクセスできます。
  - [編集（Edit）] : 既存のカスタムビューの名前と説明を編集します。ビュー：カスタム （3641 ページ）を参照してください。

- [名前を付けて保存（Save As）]：ビューを新しいカスタムビューとして保存します。ビュー：カスタム （3641 ページ）を参照してください。
- [削除（Delete）]：そのカスタムビューを削除します。
- [デフォルトのビューとして設定（Set as default view）]：HPM アプリケーションを起動するたびに常に表示されるビューを指定するには、このコマンドを使用します。

ここでは、次の内容について説明します。

- ビュー：開閉 （3639 ページ）
- ビュー：水平または垂直方向に並べて表示 （3640 ページ）
- ビュー：フローティングとドッキング （3641 ページ）
- ビュー：カスタム （3641 ページ）

ビュー：開閉

使用可能なすべてのビューは、HPM ウィンドウの左側にある [ビュー（Views）]ペインに一覧表示されます。[モニタリング（Monitoring）]ペインには、開いているビューが表示されます。各ビューは個別のタブ付きパネルとして表示されます（このウィンドウの詳細については、[HPM] ウィンドウ：[モニタリング（Monitoring）]ディスプレイ （3642 ページ）を参照してください）。

（注） ビューを切り離して、別のウィンドウに「フロート」できます。詳細については、ビュー：フローティングとドッキング （3641 ページ）を参照してください。

[モニタリング（Monitoring）]ペインに新しいビューを表示するには、次の手順を実行します。

- [ビュー（Views ）] リストで目的のエントリをクリックします。

ビューは [モニタリング（Monitoring）] ペインにタブ付きパネルとして表示されます。また、自動的に選択されて表示されます

開いている別のビューに切り替えるには、次の手順を実行します。

- [モニタリング（Monitoring）] ペインで目的のタブをクリックすると、そのビューが表示されます。
- 任意のタブを右クリックし、[次へ（Next）] または [前へ（Previous）] を選択して、そのタブ付きビューの右側または左側にビューを表示します。
- タブの右側にある [スクロールバック（Scroll Back）] ボタンと [スクロールフォワード（Scroll Forward）] ボタンをクリックして、現在のビューの左側または右側にビューを表示します

ビューを閉じるには、次の手順を実行します。

- 該当タブの [閉じる（Close）] ボタンをクリックします。
- タブを右クリックし、[閉じる（Close）] を選択します。
- タブを右クリックし、[その他を閉じる（Close Others）]を選択して、右クリックしたビュー以外の開いているすべてのビューを閉じます。
- 任意のタブを右クリックし、[すべて閉じる（Close All）] を選択して、開いているすべてのビューを閉じます。

ビュー：水平または垂直方向に並べて表示

[モニタリング（Monitoring）] ペイン全体に 1 つのビューを表示するのではなく、簡単に比較できるように、2 つ以上のビューを水平または垂直に並べて表示できます。

たとえば、2 つのビューを水平に並べて表示すると、一方のビューが [モニタリング（Monitoring）]ペインの上半分に表示され、もう一方のビューが下半分に表示されます。同様に、2 つのビューを垂直に並べると、ペインの左半分が 1 つのビューで占められ、もう一方のビューによって右半分が占められます。さらに、3 つ以上のビューを並べて表示することもできます。ペインは、ビューごとに均等に分割されます。

2 つの水平または垂直のタイルを作成するには：

- いずれかのタブを右クリックし、[新規水平グループ（New Horizontal Group）] または [新規垂直グループ（New Vertical Group）] を選択します。

選択したビューとその他のビューは、[モニタリング（Monitoring）] ペインを均等に共有するように、選択に応じて水平または垂直に配置されます。

これらのコマンドのいずれかを選択したときに3つ以上のビューが開いている場合は、選択されているビューがタイルとして表示され、タブ付きビューの残りのグループがもう一方のタイルとして表示されることに注意してください。その後必要に応じて、残りのタブ付きビューでこのプロセスを繰り返し、表示されるタイルの数を増やすことができます。

既存のタイルを別のタイルに移動することもできます。

- タブを右クリックし、[次のタググループに移動（Move to Next Tab Group）] または [前のタブグループに移動（Move to Previous Tab Group）] を選択します。

選択したビューは、次のタイル（タイルの向きに応じて下または右）または前のタイル（上または左）に追加されます。これらのコマンドは、このような移動が可能なようにビューが配置されている場合にのみ使用できます。

ビューの方向を水平から垂直に、またはその逆に切り替えて変更するには：

- 任意のタブを右クリックし、[タブグループの方向を変更（Change Tab Groups Orientation）] を選択します。

このコマンドは、2 つ以上のビューが並べて表示されている場合にのみ使用できます。

ビュー：フローティングとドッキング

タブ付きビューを切り離し、別個のウィンドウとして「フローティング」させたり、フローティングビューを「ドッキング」し、タブ付きビューとして [モニタリング（Monitoring）] ペインに戻したりすることができます。

ビューをフローティングウィンドウとして切り離すには：

- タブを右クリックし、[フローティング（Floating）] を選択します。

標準ウィンドウが開き、選択したビューが表示されます。

[モニタリング（Monitoring）] ペインから、すでに開いているフローティング ビュー ウィンドウに別のタブ付きビューを移動するには、次の手順を実行します。

- タブを右クリックし、[フローティングの移動先（Floating to）] サブメニューからウィンドウを選択します。

右クリックしたビューは、別のタブ付きパネルとして既存のウィンドウに追加されます。

フローティングビューを [モニタリング（Monitoring）] ペインにタブ付きパネルとして戻すには：

- ウィンドウでビューのタブを右クリックし、[ドッキング（Docking）] を選択します。

フローティングビューが [モニタリング（Monitoring）] ペインに戻ります。

（注） 標準ウィンドウとして、他のウィンドウと同様に、フローティングビューを最小化、最大化したり、閉じたりすることができます。

ビュー：カスタム

Health and Performance Monitor には、7 つのシステムビューがあります。さらに、既存のビューに基づいたカスタムビューをいくつでも作成できます。カスタムビューを編集および削除することもできます。

さまざまなビューが [モニタリング（Monitoring）] 画面の [ビュー（View）] ペインに表示され、[システムビュー（System Views）] と [マイビュー（My Views）]（後者のフォルダにはカスタムビューが含まれています）という 2 つのフォルダに編成されています。[モニタリング（Monitoring）] 画面については、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （3642 ページ） で説明しています。

新しいカスタムビューを作成するには、次の手順に従います。

1. [ビュー（View）] リストで、新しいビューの基になるビューを選択します。

システムビューまたは既存のカスタムビューを、基になるビューにすることができます。

1. [ファイル（File）] メニューの [名前を付けて保存（Save As）] を選択して、[ビューに名前を付けて保存（Save View As）] ダイアログボックスを開きます。

選択したビューを右クリックし、ポップアップメニューから [名前を付けて保存（Save As）] を選択してダイアログボックスを開くこともできます。

1. [名前（Name）] に新しいビューの名前を指定し、オプションで [説明（Description）] に説明を入力します。
2. このビューでモニターするデバイスを指定します。ダイアログボックスのデバイスセレクタ領域のエントリをオンまたはオフにします。
3. [保存（Save）] をクリックしてダイアログボックスを閉じ、新しいビューを [マイビュー（My View）] フォルダに追加します。

既存のカスタム ビューを編集するには、次の手順に従います。

1. [マイビュー（My View）] で、ビューを選択します。
2. [ファイル（File）] メニューの [編集（Edit）] を選択して、[ビューに名前を付けて保存（Save View As）] ダイアログボックスを開きます。

選択したビューを右クリックして、ポップアップメニューから [編集（Edit）] を選択することもできます。

1. [名前（Name）] と [説明（Description）] を編集します。
2. このビューでモニターされるデバイスを変更するには、デバイスセレクタのエントリをオンまたはオフにします。
3. [Save] をクリックして、ダイアログボックスを閉じます。

既存のカスタム ビューを削除するには、次の手順に従います。

1. [マイビュー（My View）] で、ビューを選択します。
2. [ファイル（File）] メニューから [削除（Delete）] を選択します。

選択したビューを右クリックして、ポップアップメニューから [削除（Delete）] を選択することもできます。

1. ビューを削除することを確認します。

該当するビューは、[ビュー（Views）] リストから削除されます。

[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ

[HPM] ウィンドウには、モニタリングと警告という 2 つの異なる情報が表示されます。[モニタリング（Monitoring）] ボタンをクリックして、[モニタリング（Monitoring）] ディスプレイにアクセスします。

[モニタリング（Monitoring）] ディスプレイは、[ビュー（Views）] と [モニタリング（Monitoring）] という 2 つの主要なペインで構成されています。[ビュー（Views）] ペインに

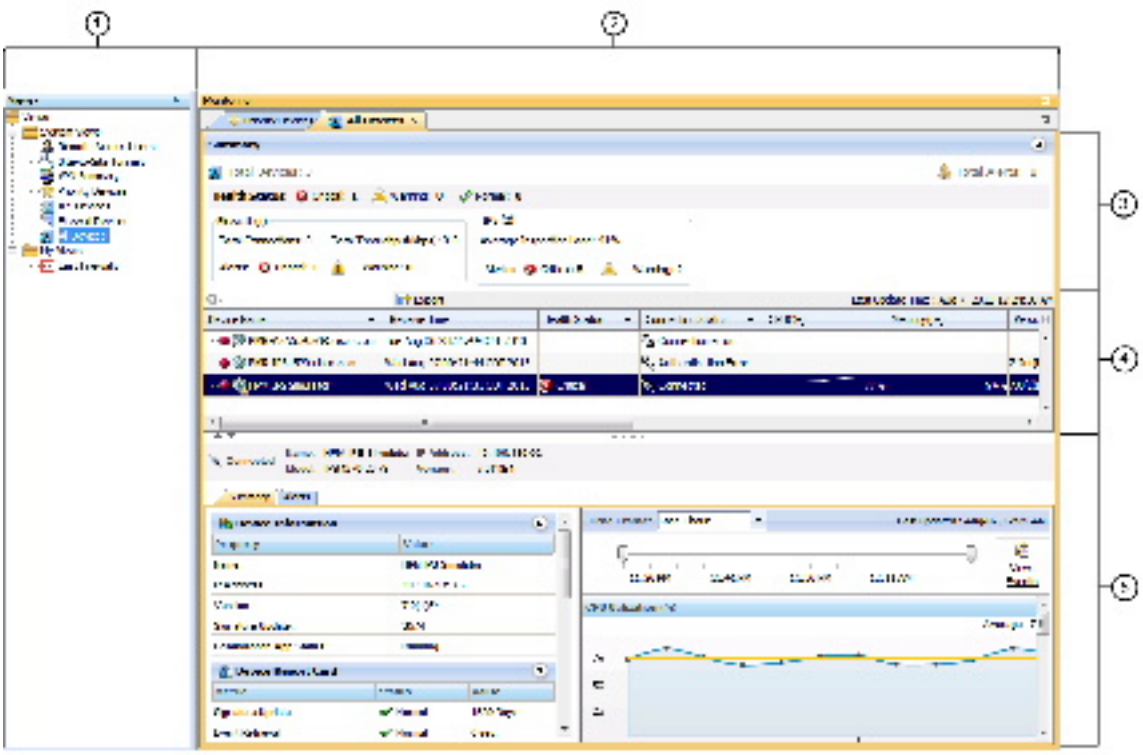
は、使用可能なビューのリストが表示されます。このリストのエントリをクリックして、そのビューを [モニタリング（Monitoring）] ペインのタブ付きパネルとして開きます。

[モニタリング（Monitoring）] ペインには複数のタブ付きビューが表示され、そのほとんどに複数のセクションが表示されます。タブをクリックすると、そのビューが前面に表示されます。

（注） モニタリングビュー：VPN、RA および S2S （3649 ページ）で説明されているように、[リモートアクセスユーザー（Remote Access Users）] ビューと [サイト間トンネル（Site-to-Site Tunnels）] ビューには、それぞれ情報のテーブルが 1 つだけ表示されます。以下の説明は、主にその他の利用可能なシステムビューに焦点を当てています。

次の図は、[モニタリング（Monitoring）] ディスプレイとパネルセクションの主な機能を示しています。

図 *73 : Health and Performance Monitor*：*[モニタリング（Monitoring）] ディスプレイ*



1	**[ビュー（Views）] リスト。**	4	**デバイスまたは VPN のステータス。**
2	[モニタリング（Monitoring）] ビューのコントロール。	5	選択したデバイスの詳細情報。
3	全デバイスの概要。		

[モニタリング（Monitoring）] ディスプレイは、5 つの主な要素で構成されています。

- [ビュー（Views）] リスト（1）：このペインには、使用可能なすべてのビューが一覧表示されます。このリストのエントリをクリックすると、そのビューが [モニタリング（Monitoring）] ペインで開きます。このビューは、Health and Performance Monitor の一部として提供される [システムビュー（System Views）] と、ユーザーが作成したカスタムビューである [マイビュー（My Views）] で編成されます。[ビュー（Views）] ペインについてはデバイスビューの管理 （3637ページ）、カスタムビューの管理についてはビュー：カスタム （3641 ページ）を参照してください。
- [モニタリング（Monitoring）] ビューのコントロール（2）：開いている各ビューのラベル付きタブがここに表示されます。任意のタブをクリックすると、そのビューが前面に表示されます。[後ろにスクロール（Scroll Backward）] ボタンと [前にスクロール（Scroll Forward）] ボタンを使用して、タブ付きビューから別のタブ付きビューへと前後に移動することもできます。または、右側の [リストの表示（Show List）] ドロップダウンメニューを開き、ラベルを選択してアクティブビューにします。
- 全デバイスまたは VPN の概要（3）：このビューに表示されるすべてのデバイスまたは VPN の集約情報を提供します。このセクションを展開するか折りたたむには、右側のボタンをクリックします。デバイス概要セクションについては、モニタリングビュー：デバイスまたは VPN サマリー （3644 ページ）で詳しく説明されています。
- デバイスステータスリスト（4）：このビューに含まれるすべてのデバイスまたは VPN がここに一覧表示されます。このリストの詳細については、モニタリングビュー：デバイスまたは VPN ステータスリスト （3645 ページ）を参照してください。 リストフィルターフィールドの使用 （3635ページ）で説明されているように、このセクションの [リストフィルタ（List Filter）] フィールドを使用してリストをフィルタリングします。
- 選択されたデバイスまたは VPN の詳細（5）：このセクションには、デバイスリストで現在強調表示されているデバイスまたは VPN に関する詳細情報が表示されます。詳細セクションについては、モニタリングビュー：デバイスまたは VPN の詳細 （3646ページ）で詳しく説明されています。

ここでは、次の内容について説明します。

- モニタリングビュー：デバイスまたは VPN サマリー （3644 ページ）
- モニタリングビュー：デバイスまたは VPN ステータスリスト （3645 ページ）
- モニタリングビュー：デバイスまたは VPN の詳細 （3646 ページ）
- モニタリングビュー：VPN、RA および S2S （3649 ページ）
- HPM データのエクスポート （3650 ページ）

モニタリングビュー：デバイスまたは VPN サマリー

HPM モニタリング画面には、タブ付きのビューが表示されます。各ビューには、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （3642ページ）で説明されているように、現在選択されているデバイスまたは VPN に関する詳細情報が表示されます。ここで説明され

ているように、すべてのデバイス関連ビュー（つまり、リモートアクセスユーザーとサイト間トンネルビューを除くすべて）には、概要セクションが含まれています。

このデバイスサマリー（VPNサマリー）は、タイトルバーの右側にあるボタンをクリックして表示または非表示にすることができ、現在のビューに関連するすべてのデバイスまたは VPN のヘルスステータスとアラートステータスを集約したスナップショットを表示します。たとえば、[ファイアウォールデバイス（Firewall Devices）] パネルを表示している場合、ステータスの概要は、監視対象のすべてのファイアウォールデバイスについてのみ表示されます。

モニタリングビュー：デバイスまたは VPN ステータスリスト

[HPM] ウィンドウ：[モニタリング（Monitoring）]ディスプレイ （3642 ページ）には、（特定のデバイスビューまたは [VPNサマリー（VPN Summary）] ビューで）現在選択されているデバイスまたはVPN に関する詳細情報が表示されます。すべてのデバイス関連ビューと [VPNサマリー（VPN Summary）] ビューには、現在のビューに関連する監視対象デバイスまたは VPN のテーブルが含まれています。

このテーブルには、すべての監視対象デバイスまたは VPN の「概要」ステータス情報が表示されます。それぞれ、このテーブルのエントリで表されます。ASA クラスタは展開可能なエントリとして表示されます。クラスタエントリの前にある [+] アイコンをクリックして展開し、各クラスタノードのインデントされたエントリを表示します。

この場合もやはり、リストには、現在のビューに関連する要素のみが含まれています。たとえば、[ファイアウォールデバイス（Firewall Devices）] ビューのリストには、IPS デバイスのエントリは含まれません。[リモートアクセスユーザー（Remote-Access Users）] および [サイト間トンネル（Site-to-Site Tunnels）] ビューには、このステータス表示は含まれません。

テーブルの列のサイズを変更したり、列の表示と非表示を切り替えたりできます。列の見出しは、選択したパラメータに従ってデバイスを非表示または表示することで、テーブルをフィルタ処理するために使用できるメニューです。これらのオプションの詳細については、テーブル列の表示と非表示 （3620 ページ）を参照してください。

このリストのエントリを選択すると、モニタリングビュー：デバイスまたはVPN の詳細 （3646 ページ）で説明されているように、そのデバイスの詳細情報がテーブルの下のデバイス詳細領域に表示されます。

ヒント [すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[IPSデバイス（IPS Devices）]、および [優先デバイス Priority Devices）] ビュー（および任意のカスタムデバイス関連ビュー）では、強調表示されたエントリを右クリックし、ポップアップメニューから [デバイスマネージャ（Device Manager）] を選択して、そのデバイスに適切な外部デバイスマネージャ（つまり、ASA の ASDM と IPS センサーの IDM）を開き、そのデバイスの正常性データとパフォーマンスデータを「ドリルダウン」できます。デバイスマネージャの詳細については、デバイスマネージャの起動 （3697 ページ）を参照してください。

モニタリングビュー：デバイスまたは VPN の詳細

[HPM] ウィンドウ：[モニタリング（Monitoring）]ディスプレイ （3642 ページ）には、現在選択されているデバイスまたは VPN に関するビューと詳細情報が表示されます。すべてのデバイス関連ビューと VPN サマリービューには、その上のデバイス ステータス テーブルで現在選択されている、個々のデバイスまたは VPN に関する詳細情報の 3 つまたは 4 つのタブ付きパネルが表示されます（[リモートアクセスユーザー（Remote-Access Users）] および [サイト間トンネル（Site-to-Site Tunnels）] ビューには、この詳細パネルは表示されません）。

ビューのタイプごとに表示される情報は次のとおりです。

[すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、[IPS デバイス（IPS Devices）]、[優先デバイス（Priority Devices）]、およびカスタムデバイス関連のビューの場合、タブ付きパネルは次のとおりです。

- [概要（Summary）]：[概要（Summary）] タブは、デバイスとデバイスのステータスに関する情報を提供する 4 つのセクションで構成されています。
  - [デバイス情報（Device Information）]：このセクションには、デバイス名、IP アドレス、デバイスタイプ、モデル番号などのデバイス固有の情報の読み取り専用リストが表示されます。フェイルオーバー情報の読み取り専用リストも表示されます。ASA クラスタが選択されている場合、[フェールオーバー（Failover）] リストはクラスタ関連情報のリストに置き換えられます。
  - [デバイスレポートカード（Device Report Card）]：このセクションには、デバイスの現在のステータスを示す一連のメトリックが表示されます。ここに表示されるメトリックの詳細については、テーブル列：デバイス関連のビュー （3620 ページ）を参照してください。
  - [インターフェイスステータス（Interface Status）]：このセクションには、デバイスで定義されているすべてのインターフェイスのリストと、現在のステータス情報が表示されます。
  - [デバイス正常性グラフ（Device Health Graphs）]：このセクションは、CPU やメモリの使用量などの特定のメトリックのグラフィック表示を使用して、デバイスステータスの「スナップショット」を提供します。また、デバイス固有のトラフィック情報、たとえば、ファイアウォールデバイスの平均接続数と変換数（最新のポーリング期間中）、IPS センサーの平均検査負荷と欠落したパケットの割合（最新のポーリング期間中）も表示されます。これらのグラフに使用する期間（過去 1 時間、過去 24 時間、または過去 7 日間）を [期間（Time Frame）] リストから指定できます。グラフの上にあるスライダバーを使用して、特定の期間に注目するできます。選択したデバイスのイベントを表示するには、[イベントの表示（View Events）] ボタンをクリックします。Event Viewer が開き、[イベントモニタリング（Event Monitoring ）] ウィンドウに、選択したデバイスでフィルタリングされたイベントと、スライダバーで指定された期間が一覧表示されます。

（注） IPSデバイスの場合、特定の正常性メトリックのしきい値を、個々のデバイス（つまり、HPM の外部）で個別に設定する必要があります。したがって、たとえば HPM に何も表示されないまま、IPSデバイスの正常性が重大な状態になる可能性があります。詳細については、アラート設定：IPS （3656 ページ）を参照してください。

- [アラート（Alerts）]：[アラート（Alerts）]タブには、選択したデバイスのすべてのアラートが一覧表示されます。アラートごとに、情報のさまざまな列を表示または非表示にすることができます。アラートの詳細については、アラートと通知 （3651 ページ）を参照してください。このタブ内のフィールドの詳細については、HPM ウィンドウ：アラートディスプレイ （3652 ページ）を参照してください。

[すべてのデバイス（All Devices）]、[ファイアウォールデバイス（Firewall Devices）]、および [優先デバイス（Priority Devices）] の場合、タブ付きパネルは次のとおりです。

- [概要（Summary）]：[概要（Summary）] タブは、デバイスとデバイスのステータスに関する情報を提供する 4 つのセクションで構成されています。
  - [デバイス情報（Device Information）]：このセクションには、デバイス名、IP アドレス、デバイスタイプ、モデル番号などのデバイス固有の情報の読み取り専用リストが表示されます。フェールオーバー情報の読み取り専用リストも表示されます。ASA クラスタが選択されている場合、[フェールオーバー（Failover）] リストはクラスタ関連情報のリストに置き換えられます。
  - [デバイスレポートカード（Device Report Card）]：このセクションには、デバイスの現在のステータスを示す一連のメトリックが表示されます。ここに表示されるメトリックの詳細については、テーブル列：デバイス関連のビュー （3620ページ）を参照してください。
  - [インターフェイスステータス（Interface Status）]：このセクションには、デバイスで定義されているすべてのインターフェイスのリストと、現在のステータス情報が表示されます。
  - [デバイス正常性グラフ（Device Health Graphs）]：このセクションは、CPU やメモリの使用量などの特定のメトリックのグラフィック表示を使用して、デバイスステータスの「スナップショット」を提供します。また、デバイス固有のトラフィック情報、たとえば、ファイアウォールデバイスの平均接続数と変換数（最新のポーリング期間中）、IPS センサーの平均検査負荷と欠落したパケットの割合（最新のポーリング期間中）も表示されます。これらのグラフに使用する期間（過去 1 時間、過去 24 時間、または過去 7 日間）を [期間（Time Frame）] リストから指定できます。グラフの上にあるスライダバーを使用して、特定の期間に焦点を合わせることができます。選択したデバイスのイベントを表示するには、[イベントの表示（View Events）] ボタンをクリックします。イベントビューアが開き、[イベントモニタリング（Event Monitoring）] ウィンドウに、選択したデバイスでフィルタリングされたイベントと、スライダバーで指定された期間が一覧表示されます。

（注） IPSデバイスの場合、特定の正常性メトリックのしきい値を、個々のデバイス（つまり、HPM の外部）で個別に設定する必要があります。したがって、たとえば HPM に何も表示されないまま、IPSデバイスの正常性が重大な状態になる可能性があります。詳細については、アラート設定：IPS （3656 ページ）を参照してください。

- [アラート（Alerts）] : [アラート（Alerts）] タブには、選択したデバイスのすべてのアラートが一覧表示されます。アラートごとに、複数の列の情報を表示または非表示にすることができます。アラートの詳細については、アラートと通知 （3651ページ）を参照してください。このタブ内のフィールドの詳細については、HPM ウィンドウ：アラートディスプレイ （3652 ページ）を参照してください。
- [フローオフロード（Flow-offload）] : [フローオフロード（Flow-offload）] タブには、オフロードエンジンに関する基本情報、オフロードコアの負荷率、アクティブなオフロードフローに関する情報（作成されたオフロードフローの数、オフロードアクティブフロー、それらの書き換えルールおよびデータ）が表示されます。
- [フローオフロード統計（Flow-offload Statistics）] : [フローオフロード統計（Flow-offload Statistics）] タブには、送信、受信、およびドロップされたパケットの数と、使用された仮想 NIC の統計が表示されます。

[VPNサマリー（VPN Summary）] ビューの場合、タブ付きパネルは次のとおりです。

- [VPNの使用状況（VPN Usage）] : アクティブなサイト間トンネル、アクティブなリモートアクセスセッション、合計スループットなどの情報を示すいくつかのグラフ。これには、アクティブなサイト間トンネル、アクティブ IPSec リモートアクセスユーザー、アクティブ SSL VPN クライアントレスユーザー、およびアクティブ SSL VPN とそのクライアントユーザーの履歴傾向情報が含まれます。
- [クラスタリソースの使用状況（Cluster Resource Usage）] : クラスタリソースの使用状況の詳細（リソース名、その現状、ピーク、および使用制限）を表示します。拒否されたパケットとコンテキストの数も表示します。この機能は、Cisco Firepower 9K デバイスにのみ適用されます。
- [クラスタ分散の詳細（Cluster Distribution Details）] : VPN のクラスタモードを表示します。集中型の場合、接続先モードが VPN 分散型ではないことを示すエラーメッセージが表示されます。分散されている場合は、メンバー I およびメンバー II の詳細が個別に表示されます。この機能は、Cisco Firepower 9K デバイスにのみ適用されます。
- [ライセンス情報（License Information）] : 上のテーブルでの選択に応じて、VPN タイプ別のライセンス情報の読み取り専用リスト、または IPSec および SSL ライセンスと負荷情報のリスト。マルチモードデバイスのシステムコンテキストの場合、VPN ライセンスと割り当てが表示されます。個々のコンテキストについて、VPN 割り当ての制限と VPN ライセンスの使用状況が表示されます。
- [その他の詳細（Other Details）] : 証明書とトラストポイントの詳細のリスト。

VPN モニタリングの対象デバイスの選択に関する詳細については、監視対象デバイスの管理（3616 ページ）を参照してください。

モニタリングビュー：VPN、RA および S2S

HPM モニタリングディスプレイには、[HPM] ウィンドウ：[モニタリング（Monitoring）] ディスプレイ （3642 ページ）で説明されているように、さまざまなデバイスおよび VPN に関連したデータビューが表示されます。これには、リモート アクセス ユーザー ビューとサイト間トンネルビューが含まれます。これらのビューは、他のビューとは異なり、単に現在のユーザーとトンネルのテーブルです。

VPN モニタリングの対象デバイスの選択に関する詳細については、監視対象デバイスの管理（3616 ページ）を参照してください。

両方のビューで、テーブルの列のサイズを変更したり、列の表示と非表示を切り替えたりできます。列の見出しは、選択したパラメータに従ってエントリを非表示または表示することにより、テーブルをフィルタリングするために使用できるメニューです。これらのオプションの詳細については、テーブル列の表示と非表示 （3620 ページ）を参照してください。

リモート アクセス ユーザー ビューには、HPM によってモニタリングされているデバイスを使用してネットワーク リソースに現在ログインしているリモートアクセスユーザーが一覧表示されます。リモートアクセスユーザー情報は、他のビューの標準である 5 分ではなく、20 分ごとに更新されることに注意してください（通常のモニタリングの場合、優先モニタリングの間隔は 15 分です）。また、リモートアクセスユーザーは履歴データやトレンド分析データを利用できません。

さらに、VPN サマリービューとリモート アクセス ユーザー ビューの RA ユーザー数が一致しない場合があります。これは、VPN サマリーが 10 分/5 分（通常/優先）間隔で更新されるためです。

ヒント リモート アクセス ユーザー ビューで、ユーザーエントリを右クリックし、ポップアップメニューから [ユーザーのログオフ（Log Off User）] を選択して、リモートアクセス接続を終了できます。

サイト間トンネルビューは、すべてのモニタリング対象デバイスを使用した現在の VPN トンネル情報を提供します。デバイスまたはコンテキストのトンネルアップ/ダウンアラートを有効にするには、[SNMP Credentials] ダイアログボックス （147 ページ）で説明されているように、デバイスで SNMPv3 を設定する必要があることに注意してください。

ヒント サイト間トンネルビューで、[ステータス（Statu）] 列の [ダウン（Down）] 通知ハイパーリンクをクリックして、イベントビューアでそのデバイスの IPSec VPN イベントを表示できます。イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。

ASA 9.0+ デバイスのクラスタの場合、VPN 処理はノード間でロードバランシングされず、クラスタ内の集中サポートに限定されるため、ディレクタデバイスのみの情報が表示されます。

（注） VPN ポーリングは一定の時間間隔で行われるため、その時間間隔内のステータスの変更をログに記録することはできません。たとえば、サイト間トンネルがポーリングの直後にダウンし、次のポーリングの直前に復旧した場合、そのステータスの変化は検出できません。

HPM データのエクスポート

現在のビューに含まれるデバイスステータス情報の「スナップショット」を PDF、HTML、または CSV（カンマ区切り値）ファイルとして保存できます。

（注） Security Manager バージョン 4.9 以降、PDF、HTML、または CSV 形式でエクスポートされたデータには、IPv6 トンネル情報も含まれます。

次に、現在のビューデータを PDF、HTML、または CSV ファイルにエクスポートする手順について説明します。

関連項目

- HPM ウィンドウ （3617 ページ）
- テーブル列の表示と非表示 （3620 ページ）

ステップ 1 適切なタブをクリックして、エクスポートするビュー（[優先デバイス（Priority Devices）]、[VPNサマリー（VPN Summary）]、[すべてのデバイス（All Devices）] など）を表示します。

ヒント 特定のビューに含まれるエントリすべてのサブセットのデータをエクスポートするには、目的のデバイスのみを含むカスタムビューを作成します。詳細については、ビュー：カスタム （3641 ページ）を参照してください。

ステップ 2 [リストフィルタ（List Filter）] フィールド（デバイスまたは VPN ステータスリストの上）の横にある [エクスポート（Export）] ボタンの横にある下矢印をクリックし、ドロップダウンメニューから [PDF形式（As PDF）]、[HTML形式（As HTML）]、または [CSV形式（As CSV）] を選択します。

[エクスポート（Export）] ダイアログボックスが開きます。

ステップ 3 ダイアログボックスの該当する列をオンにして、エクスポートする特定の情報を選択します。

次のトピックでは、さまざまなビューで使用できる個々の列について説明します。

- テーブル列：デバイス関連のビュー （3620 ページ）
- テーブル列：VPN 関連のビュー （3626 ページ）

ステップ 4 [エクスポート（Export）] ドロップダウンリストから [PDF形式（As PDF）] を選択した場合、[エクスポート（Export）] ダイアログボックスの下部で、PDF ファイルの目的の [ページサイズ（Page Size）]（A1、A2、A4、レター、またはリーガル）を選択できます。

PDF ファイルのページが選択したサイズになり、表示される情報はそれに応じて書式設定されます。

ステップ 5 [エクスポート（Export）] ドロップダウンリストから [CSV形式（As CSV）] を選択した場合、Security Manager は、必要に応じて保存できる CSV ファイルに情報をエクスポートします。バージョン 4.8 以降、Security Manager には、[トレンドチャートのエクスポート（Export Trend Charts）] チェックボックスが用意されています。これを選択すると、トレンド情報をCSVファイル形式でエクスポートできます。チェックボックスの選択後、過去 1 時間、過去 24 時間、過去 7 日間の利用可能な時間範囲からタイムフレームを選択できます。

ステップ 6 [エクスポート（Export）] をクリックすると、[エクスポート（Export）] ダイアログボックスが閉じます。

[ファイルの保存（File Save）] ダイアログボックスが開きます。

ステップ 7 ファイルの名前を入力し、保存する場所を指定します。

デフォルトのファイル名は、現在のシステム時刻（長整数型）です。これを説明的な名前に変更することもできます。Windows システムの場合、デフォルトの場所は My Documents です。任意の場所を指定できます。

ステップ 8 [保存（Save）] をクリックして [保存（Save）] ダイアログボックスを閉じ、選択したデータをエクスポートします。

アラートと通知

Health and Performance Monitor（HPM）では、監視対象デバイスのパフォーマンスと正常性に関するトレンド情報、アラート、および通知が提供されます。個々のデバイスおよびデバイスグループのステータスを迅速にスキャンすることにより、ネットワークユーザーとデバイスリソースの使用率を含む、ネットワークの全体的な正常性を監視できます。

特定のデバイスレベルのトレンド情報は、毎時、毎日、および毎週の間隔で利用できます。アラートは目立つように表示され、関連する HPM データに簡単にナビゲートできます。個々のアラートを確認して注釈を付けることもできます。

（注） クラスタのノードが削除され、そのクラスタが Cisco Security Manager で再検出されると、そのノードはHPMのモニタリング対象から除外されます（現在有効になっている場合）。ただし、そのノードで生成されたアラートは引き続き HPM に表示されます。アラートは手動で HPM からクリアする必要があります。

それらのアラートは、設定したしきい値と状態変更ルールに基づいています。さまざまなメトリックの [クリティカル（Critical）]、[警告（Warning）]、および [正常（Normal）] のレベルを定義するしきい値を指定し、インターフェイス障害など、特定の状態変更のルールを設定できます。

さらに、デバイスモニタリングには2つのレベルがあります。最初は、すべてのデバイスが監視されていません。ただし、監視対象のデバイスを「通常」レベルまたは「優先度」レベルで指定できます。レベルごとに個別のアラート定義のセットを定義します。優先デバイスはより頻繁にポーリングおよびレポートされ(「通常の」デバイスの場合は10分間隔であるのに対して5分間隔)、障害パラメータはより厳格です。

また、電子メールアラート通知を有効にできます。設定されている場合、アラートが生成されるたびに、指定されたアドレスに電子メールが送信されます。アラートのカテゴリ（ファイアウォールおよびIPS）ごとに複数のアドレスを指定できます。

（注） 電子メール通知は、アラートが初めて記録されたとき、およびアラートの重大度が[警告（Warning）]から[クリティカル（Critical）]に変更されたときに送信されます（逆の場合は送信されません）。デバイスが[正常（Normal）]の状態に戻っても、通知は発行されません。

ここでは、次の内容について説明します。

- HPM ウィンドウ：アラートディスプレイ （3652 ページ）
- アラート：設定 （3654 ページ）
- アラート：表示 （3663 ページ）
- アラート：表示 （3663 ページ）

HPM ウィンドウ：アラートディスプレイ

HPM ウィンドウには、モニタリングと警告という 2 つの異なる情報が表示されます。[アラート（Alerts）]ボタンをクリックして[アラート（Alerts）]画面にアクセスします。

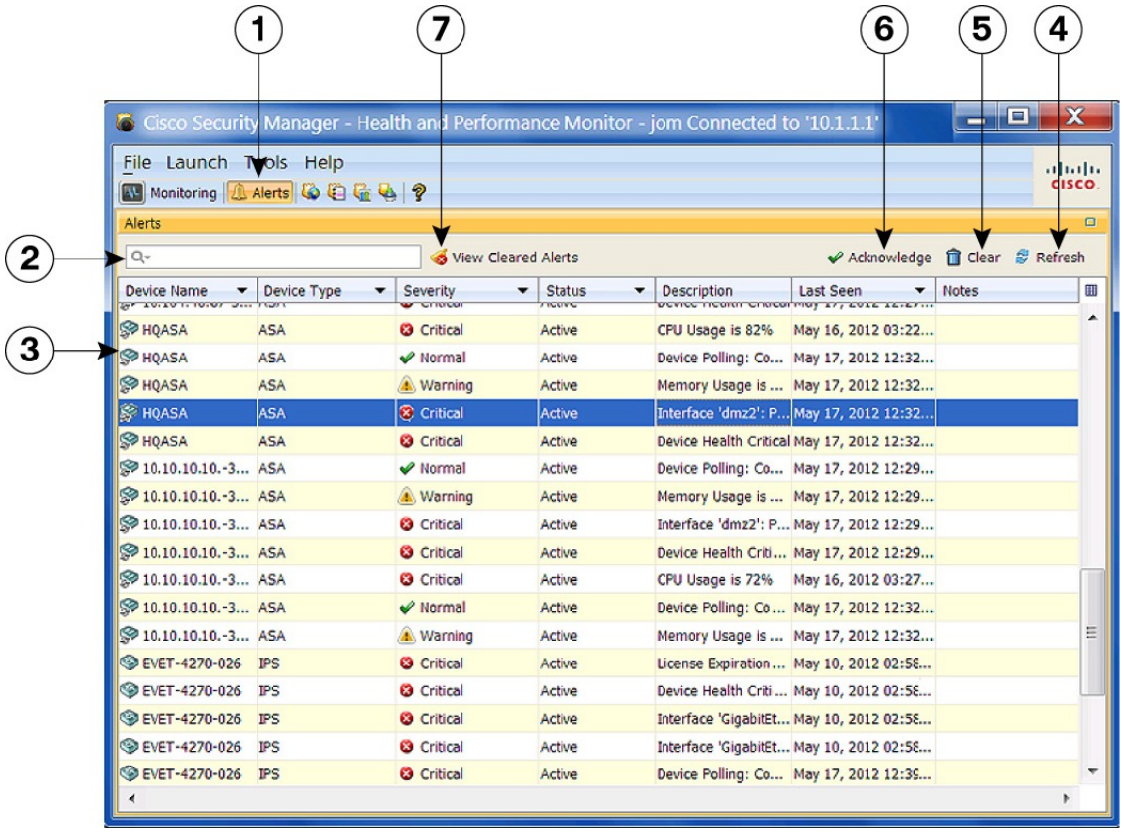
（注） アラートデータのデバイス固有のビューは、特定のデバイスの詳細情報を表示するときに[アラート（Alerts）]タブで使用できます（モニタリングビュー：デバイスまたはVPNの詳細 （3646ページ）を参照）。いくつかの例外を除き、デバイス固有のアラートビューでは、プライマリ[アラート（Alerts）]画面と同じ機能の多くを実行できます。

次の図は、[アラート（Alerts）]画面の主な機能を示しています。

関連項目

- アラート：設定 （3654 ページ）

図 *74 : [*ヘルスとパフォーマンスのモニタ（***Health and Performance Monitor***）*]* : *[*アラート（***Alerts***）*]*画面



1	**[アラート（Alerts）] ボタン**	5	**[クリア（Clear）] ボタン**
2	[リストフィルタ（List Filter）] フィールド	6	[確認（Acknowledge）] ボタン
3	[アラート（Alerts）] テーブル	7	[クリアされたアラートの表示（View Cleared Alerts）] ボタン
4	[更新（Refresh）] ボタン		

[アラート（Alerts）] 画面は、次の 7 つの主要要素で構成されています。

（注） これらの要素については、[リストのフィルタ（List Filter）] フィールドと [クリアされたアラートの表示（View Cleared Alerts）] ボタンを除き、特定デバイスの詳細情報を表示するときに [アラート（Alerts）] タブで同じ要素を使用できます（モニタリングビュー：デバイスまたは VPN の詳細 （3646 ページ）を参照）。

- [アラート（Alerts）] ボタン（1）：HPM ウィンドウには、デバイスおよび VPN の監視情報か、監視対象デバイスによって生成されたアラートのテーブルが表示されます。アラートテーブルを表示するには、この [アラート（Alerts）] ボタンをクリックしてください。

- [リストのフィルタ（List Filter）] フィールド（2）：このフィールドを使用すると、テーブルに表示されるアラートをフィルタ処理できます。指定されたテキストを含むアラートのみがリストされます。詳細については、リストフィルターフィールドの使用 （3635ページ）を参照してください。
- [アラート（Alerts）] テーブル（3）：このテーブルには、現在監視されているすべてのデバイスに関するすべてのアラートがリストされます。表示されるアラートは、[リストのフィルタ（List Filter）] フィールドを使用してフィルタ処理できます。また、アラートごとに、複数の列の情報を表示または非表示にすることもできます。詳細については、アラートと通知 （3651 ページ）を参照してください。
- [更新（Refresh）] ボタン（4）：通常のポーリングサイクルより前にすべてのアラートを更新するには、このボタンをクリックします。
- [クリア（Clear）] ボタン（5）：1 つ以上のアラートが選択されている場合、このボタンをクリックして [クリア（Clear）] ダイアログボックスを開くことができます。ダイアログボックスを閉じて、強調表示されたアラートをテーブルからクリアするには、ダイアログボックスの [クリア（Clear）] ボタンをクリックします。

（注） アラートのクリアと確認の詳細については、アラート：確認応答とクリア （3664ページ）を参照してください。

- [確認（Acknowledge）] ボタン（6）：1 つ以上のアラートが選択されている場合、このボタンをクリックして [クリア（Acknowledge）] ダイアログボックスを開くことができます。必要に応じて、選択したアラートに適用されるメモを入力できます。ダイアログボックスを閉じて、強調表示されたすべてのアラートを確認済みとしてマークするには、[確認（Acknowledge）] ボタンをクリックします。

ヒント 以前に確認したアラートにメモを追加できます。そのアラートの [メモ（Note）] フィールドをクリックして、[メモの入力（Enter Notes）] ダイアログボックスを開きます。これは、[メモの入力（Enter Notes）] ダイアログボックスにアクセスする唯一の方法です。

- [クリアされたアラートの表示（View Cleared Alerts）] ボタン（7）：このボタンをクリックすると、[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウが開き、以前にクリアされたアラートにアクセスして確認することができます。対象のデバイスと時間範囲を指定してください。このウィンドウの使用方法の詳細については、アラート：履歴 （3665 ページ）を参照してください。

アラート：設定

HPM によって提供されるアラートと電子メール通知は、[アラート設定（Alerts Configuration）] ダイアログボックスで設定するしきい値と状態変更ルールに基づいています。

[アラート設定（Alerts Configuration）] ダイアログボックスは、3 つのタブ付きパネルで構成されています。IPS センサー関連のアラートの場合は [IPS]、ファイアウォール関連のアラートの場合は [FW]、トンネルステータスアラートの場合は [VPN] です。各パネルには、セクションのオプションのグループが表示されます。特定のセクションを表示または非表示にするには、展開/折りたたみボタンを使用します。

（注） 該当するセクションを展開せずに、特定のアラートを有効または無効にすることができます。セクションの見出しの前にあるボックスをオンまたはオフにするだけです。現在の設定が使用および保持されます。

デバイスモニタリングには、通常または「標準」の優先順位と「アクティブ」な優先順位の 2 つのレベルがあります。アクティブな優先順位のデバイスはより頻繁にポーリングされて報告され、障害パラメータはより厳格になります。すべてのモニタリング対象デバイスの最大 10% を優先モニタリング対象として指定できます。デバイス選択の詳細については、監視対象デバイスの管理 （3616 ページ）を参照してください。

次の手順に従って、標準デバイスと優先デバイス両方のアラートレポートと通知を設定します。

ステップ 1 [ツール（Tools）] メニューから [アラート設定（Alert Configuration）] を選択して、[アラート設定（Alert Configuration）] ダイアログボックスを開きます。

ステップ 2 [IPS] パネルで、IPS 関連のアラートを設定します。必要に応じて、[IPS] タブをクリックしてパネルを表示します。

1. IPS アラートが生成された場合の電子メール通知を有効にするには、[電子メールアドレス（Email Addresses）] フィールドに 1 つ以上の有効なアドレスを入力します。複数のアドレスはコンマで区切ります。
2. セクション見出しのチェックボックスを使用して、特定のアラートを有効または無効にします。セクションを展開して、アラート定義を更新します。IPS パラメータについては、アラート設定：IPS （3656 ページ）で説明されています。

（注） 電子メール通知は、アラートが初めて記録されたとき、およびアラートの重大度が警告から重大に変更されたときに送信されます（逆の場合は送信されません）。デバイスが通常の状態に戻った場合、通知は発行されません。

ステップ 3 [FW] パネルで、ファイアウォール関連のアラートを設定します。[FW] タブをクリックしてパネルを表示します。

1. ファイアウォールアラートが生成された場合の電子メール通知を有効にするには、[電子メールアドレス（Email Addresses）] フィールドに 1 つ以上の有効なアドレスを入力します。複数のアドレスはコンマで区切ります。
2. セクション見出しのチェックボックスを使用して、特定のアラートを有効または無効にします。セクションを展開して、アラート定義を更新します。FW パラメータについては、アラート設定：ファイアウォール （3658 ページ）で説明されています。

ステップ 4 [VPN] パネルで、トンネルステータスアラートを設定します。[VPN] タブをクリックしてパネルを表示します。

1. トンネルダウンアラートが生成された場合の電子メール通知を有効にするには、[電子メールアドレス（Email Addresses）] フィールドに 1 つ以上の有効なアドレスを入力します。複数のアドレスはコンマで区切ります。
2. セクション見出しのチェックボックスを使用して、トンネルステータスアラートを有効または無効にします。セクションを展開して、アラート定義を更新します。VPN パラメータについては、アラート設定：VPN （3660 ページ）で説明されています。

（注） デバイスまたはコンテキストに対してこれらのトンネルステータスアラートを有効にするには、S2S ポーリングのための SNMP の設定 （3661 ページ）で説明されているように、まずデバイスで SNMP を設定する必要があります。

ステップ 5 [保存（Save）] をクリックして変更を保存し、ダイアログボックスを閉じます。

アラート設定：IPS

（注） バージョン 4.17 以降、Cisco Security Manager は IPS デバイスをサポートしていません。

モニタリング対象の IPS デバイスから収集されるアラートとステータス情報は、[アラート設定（Alerts Configuration）] ダイアログボックスの [IPS] パネルで設定されます。ダイアログボックスの開き方、IPS パネルへのアクセス、IPS 関連の通知用の電子メールアドレスの指定については、アラート：設定 （3654 ページ）を参照してください。

IPS アラートの設定パラメータは、展開したり折りたたんだりできるセクションにグループ化されています。各セクションには、見出しの横にチェックボックスがあります。このチェックボックスを使用して、アラートを有効または無効にします。各セクションを展開すると、アラートの定義に使用される設定にアクセスできます。

次の表で、IPS アラートおよびステータスの設定パラメータについて説明します。各パラメータは、優先デバイスと標準デバイスに対して個別に設定できます（優先モニタリングと標準モニタリングの対象となるデバイスの指定については、監視対象デバイスの管理 （3616ページ）で説明しています）。

（注） 次に挙げる一部のアラート設定では、モニタリング対象の IPS センサー自体で特定の関連パラメータを設定する必要があります。たとえば、特定のセンサーで **license-expiration-policy**（**health-monitor** コマンド）が有効になっていない場合、ライセンス有効期限メッセージはそのセンサーによって生成されないため、HPM はそのセンサーに関するアラートを集計しません。

表 *983 : IPS* アラートの設定

設定	説明
[コラボレーションアプリケーションのステータス（Collaboration App Status）]	コラボレーション アプリケーションによって生成されたエラーが集計されます。アラートと通知は、集計されたエラーの数が指定された発生回数の値に達すると生成されます。
[センサーアプリケーションのステータス（Sensor App Status）]	センサーアプリケーションによって生成されたエラーが集計されます。アラートと通知は、イベントの数が指定された発生回数の値に達すると生成されます。
[バイパスモード（Bypass Mode）]	バイパスモードがトリガーされるたびに、この設定に関する発生回数1が記録されます。アラートと通知は、発生回数が指定された値に達すると生成されます。
インターフェイス ステータス	有効になっている各インターフェイスのステータスは定期的にポーリングされます。任意のインターフェイスに対するポーリング結果「ダウン」は、そのインターフェイスでの発生回数1として記録されます。アラートと通知は、発生回数が指定された値に達すると生成されます。
ライセンスの期限切れ	ライセンスの期限切れのしきい値は、各 IPS センサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。
メモリ使用率	メモリ使用率のしきい値は、各IPSセンサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。 メモリ使用率メッセージごとに発生回数 1 が記録されます。アラートと通知は、発生回数がここで指定された値に達すると生成されます。
[受信できなかったパケット数（Missed Packets）]	受信できなかったパケット数のしきい値は、各IPSセンサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。 受信できなかったパケットメッセージごとに発生回数1が記録されます。アラートと通知は、発生回数がここで指定された値に達すると生成されます。
[検査負荷（Inspection Load）]	トラフィック検査負荷のしきい値は、各 IPS センサーで設定でき、このしきい値を超えると、ステータスメッセージが発行されます。 負荷超過メッセージごとに発生回数1が記録されます。アラートと通知は、発生回数が指定された値に達すると生成されます。

アラート設定：ファイアウォール

モニタリング対象のファイアウォールデバイスから収集されるアラートおよびステータス情報は、[アラート設定（Alerts Configuration）] ダイアログボックスの [FW] パネルで設定されます。ダイアログボックスを開く方法、[FW] パネルにアクセスする方法、セクションを展開する方法と折りたたむ方法、およびFW関連の通知用電子メールアドレスを提供する方法については、監視対象デバイスの管理 （3616 ページ）を参照してください。

ファイアウォールアラートの設定パラメータは、展開したり折りたたんだりできるセクションにグループ化されています。各セクションには、見出しの横にチェックボックスがあります。このチェックボックスを使用して、アラートを有効または無効にします。各セクションを展開すると、アラートの定義に使用される設定にアクセスできます。

一部のセクションの見出しには、[デバイスの正常性を判断する際に考慮（Consider for Device Health）]チェックボックスも含まれています。これらのボックスのいずれかをオンにすると、各デバイスの全体的な正常性を判断するときに、その特定の情報が考慮されるようになります。

次の表で、FW アラートおよびステータスの設定パラメータについて説明します。

表 *984* : ファイアウォールアラートの設定

設定	説明
フェールオーバーピアのステータス	デバイスのフェールオーバーピアへのリンクのステータスは、定期的にポーリングされます。送信試行の失敗は、それぞれ発生回数1として集計されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）]を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。
インターフェイス ステータス	有効になっている各インターフェイスのステータスは定期的にポーリングされます。任意のインターフェイスに対するポーリング結果「ダウン」は、そのインターフェイスでの発生回数1として記録されます。このモニタリングは、スタンドアロンデバイスごと、およびASAクラスタのノードごとに実行されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）]を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。 （注） デバイスの正常性の計算にこれらのデータを含めるには、ヘッダーの [デバイスの正常性を判断する際に考慮（Consider for Device Health）] をオンにします。

マスターの変更	発生回数は、ASA クラスタの制御ユニットノードとして指定されたデバイスが変更されるたびに集計されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）] を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。
クラスタノードのステータス	発生回数は、ASA クラスタノードの接続ステータスが変更（起動または停止）されるたびに集計されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 優先デバイスと標準デバイスの場合：[重大（Critical）] または [警告（Warning）] を選択して生成されるアラートのタイプを指定してから、アラートのトリガーに必要な発生回数を指定します。
CPU 使用率	発生回数は、CPU 使用率が指定されたしきい値のパーセンテージを超えるたびに集計されます。これはスタンドアロンデバイスごと、シングル コンテキスト クラスタのノードごとに実行されます。またマルチコンテキストクラスタのノードごとに（システムコンテキストに関してのみ）実行されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 （注） デバイスの正常性の計算にこれらのデータを含めるには、ヘッダーの [デバイスの正常性を判断する際に考慮（Consider for Device Health）] をオンにします。 優先デバイスと標準デバイスでは、CPU 使用率の [重大（Critical）] アラートと [警告（Warning）] アラートのいずれかまたは両方を有効にすることができます。 **1.** 該当するボックスをオンにして、[しきい値（Threshold）] フィールドと [発生回数（Occurrence）] フィールドを有効にします。 **2.** 上矢印または下矢印をクリックするか、既存の値を強調表示したり数値を入力したりすることで、[しきい値（Threshold）] のパーセンテージを指定します。 **3.** [発生回数（Occurrence）] フィールドで、指定したしきい値を超えてから重大アラートまたは警告アラートが発行される回数を指定します。

メモリ使用率	発生回数は、メモリ使用率が指定されたしきい値のパーセンテージを超えるたびに集計されます。これはスタンドアロンデバイスごと、シングル コンテキスト クラスタのノードごとに実行されます。またマルチコンテキストクラスタのノードごとに（システムコンテキストに関してのみ）実行されます。発生回数がここで指定した値に達すると、アラートと通知が生成されます。 （注） デバイスの正常性の計算にこれらのデータを含めるには、ヘッダーの [デバイスの正常性を判断する際に考慮（Consider for Device Health）] をオンにします。 優先デバイスと標準デバイスでは、メモリ使用率の [重大（Critical）] アラートと [警告（Warning）] アラートのいずれかまたは両方を有効にすることができます。 1. 該当するボックスをオンにして、[しきい値（Threshold）] フィールドと [発生回数（Occurrence）] フィールドを有効にします。 2. 上矢印または下矢印をクリックするか、既存の値を強調表示したり数値を入力したりすることで、[しきい値（Threshold）] のパーセンテージを指定します。 3. [発生回数（Occurrence）] フィールドで、指定したしきい値を超えてから重大アラートまたは警告アラートが発行される回数を指定します。

アラート設定：VPN

監視対象デバイスおよびコンテキストでのサイト間（S2S）トンネルのアラートの生成は、[アラート設定（Alerts Configuration）] ダイアログボックスの [VPN] パネルで有効化し、設定します。ダイアログボックスを開く方法、VPN パネルにアクセスする方法、および VPN 関連の通知用電子メールアドレスを提供する方法については、アラート：設定 （3654ページ）を参照してください。

ヒント VPNアラートが有効になっている場合、HPMは、通常/優先順位の指定に従って、監視対象のデバイスとコンテキストを通常間隔および優先間隔（それぞれ 10 分と 5 分）でポーリングします。また、トラップの処理直後にHPMトンネルのステータスを更新するSNMPモニタリングを有効にすることもできます。HPM の SNMP 処理を有効にする方法の詳細については、S2S ポーリングのための SNMP の設定 （3661ページ）を参照してください。

トンネルステータスの設定パラメータは、展開したり折りたたんだりできるセクションにグループ化されています。展開すると、アラート設定にアクセスできます。見出しの横にあるチェックボックスを使用して、アラートを有効または無効にします。

使用可能な VPN アラートパラメータについては、以下の表で説明します。

表 *985 : VPN* アラートの設定

設定	説明

Tunnel Status	監視対象の各 S2S トンネルのステータスは、定期的なポーリングまたは SNMP トラップ処理に基づいて、起動または停止するたびに更新されます。任意のトンネルに対するポーリング結果「ダウン」は、発生回数 1 として記録されます。発生回数がここで指定した値に達すると、アラートが生成されます。 優先デバイスと標準デバイスで、重大と警告の両方のトンネルダウンアラートを個別に設定できます。[重大（Critical）] または [警告（Warning）] を選択して、生成されるアラートのタイプを指定し、[発生回数（Occurrence）] フィールドで、クリティカルまたは警告アラートが発行される前に、ポーリングされたときにトンネルがダウンする回数を指定します。

S2S ポーリングのための SNMP の設定

正常性とパフォーマンスのモニタリング（HPM）アプリケーションは、SNMP を使用して、アップ/ダウンステータス更新のためサイト間（S2S）VPN トンネルをポーリングします。監視対象デバイスおよびコンテキストでのサイト間（S2S）トンネルのアラートの生成は、[HPMアラート設定（HPM Alerts Configuration）] ダイアログボックスの [VPN] パネルで設定します。ダイアログボックスを開く方法、VPN パネルにアクセスする方法、および VPN 関連の通知用 E メールアドレスを提供する方法については、アラート：設定 （3654 ページ）を参照してください。

ここでは、S2S ポーリングを提供するために Security Manager で SNMP を設定する方法について概説します。基本的な手順は以下のとおりです。

1. デバイスまたは個々のコンテキストに対して [SNMP] ページ （2519 ページ） で SNMP を有効にして設定します。具体的には、[SNMPサーバーを有効にする（Enable SNMP Servers）] をオンにして、[読み取りコミュニティ文字列（Read Community String）] を指定して確認します。
2. [SNMP Trap Configuration] ダイアログボックス （2522 ページ） で、[その他（Other）] パネルの [IPSECの開始（IPSEC Start）] および [IPSECの停止（IPSEC Stop）] を確認します。
3. [SNMPホストアクセスエントリの追加/編集（Add/Edit SNMP Host Access Entry）] ダイアログボックス （2527 ページ） で、インターフェイス名、IP アドレス、コミュニティ文字列を指定（および確認）し、SNMP バージョン（1 または 2c）を選択します。

バージョン 1、2c、および 3 は S2S ポーリングでサポートされていますが、次のセクションで説明するように、バージョン 3 は個別に設定する必要があります。

1. [SNMP Credentials] ダイアログボックス （147 ページ） で、デバイスまたは個々のコンテキストの SNMP ログイン情報を設定します。

バージョン 1 および 2c の場合は、RO コミュニティ文字列を指定して確認します。

バージョン 3 の場合、Security Manager は 3 つのモードをサポートします。どれを使用するかは、入力に応じて決まります。

- noauthnopriv（認証なし、プライバシーなし）：ユーザ名は必須ですが、その他は任意。

- authnopriv（認証あり、プライバシーなし）：ユーザ名、パスワード、認証アルゴリズム、およびエンジン ID が必要。
- authpriv（認証あり、プライバシーあり）：ユーザ名、パスワード、認証アルゴリズム、プライバシーパスワード、プライバシーアルゴリズム、およびエンジン ID が必要。

ここでも、次のセクションで説明するように、SNMP v3 の設定は個別に実行されます。

Security Manager デバイスの SNMP v3 の設定

Security Manager で SNMP v3 を直接設定することはできません。 CLI コマンドを使用するか、FlexConfig を設定する必要があります。手順は次のとおりです。

1. SNMP サーバーグループを設定します。

```
snmp-server group group-name v3 [auth | noauth | priv]
```

auth キーワードは、パケット認証を有効にします。noauth キーワードは、パケット認証や暗号化が使用されていないことを示します。priv キーワードは、パケット暗号化と認証を有効にします。auth または priv キーワードには、デフォルト値がありません。

1. 新しい SNMP ユーザを定義します。

```
snmp-server user username group-name{v3 [encrypted]
[auth {md5 | sha]} auth-password
[priv [des | 3des | aes] [128 | 192 | 256] priv-password]
```

v3 キーワードは、SNMP バージョン 3 のセキュリティモデルを使用することを指定し、encrypted、priv、および auth キーワードの使用を有効化します。encrypted キーワードは、パスワードが暗号化された形式であることを示します。暗号化されたパスワードは、16進数の形式である必要があります。

auth キーワードは、使用する認証レベル（md5 または sha）を指定します。

priv キーワードは、暗号化レベルを指定します。auth または priv キーワードには、デフォルト値がありません。

暗号化アルゴリズムには、des、3des、または aes を指定できます。また、使用する AES 暗号化アルゴリズムのバージョンとして、128、192、256 のいずれかを指定することもできます。auth-password は、認証ユーザ パスワードを指定します。priv-password は、暗号化ユーザ パスワードを指定します。

1. SNMP 通知の受信者を指定します。

```
snmp-server host interface {hostname | ip_address} [version 3 username]
```

トラップの送信元となるインターフェイスを示します。デバイスに接続できる NMS または SNMP マネージャの名前と IP アドレスを指定します。

関連項目

- SNMP の設定 （2516 ページ）

アラート：表示

監視対象デバイスに対して生成されたすべてのアラートは、HPM ウィンドウの代替画面に表として表示されます。デバイスがステータス情報をポーリングされると、アラートテーブルが自動的に更新されます。右側のテーブルの上にある [更新（Refresh）] ボタンをクリックして、テーブルを更新することもできます。

これらのアラートは、設定したしきい値と状態変更ルールに基づいています。詳細については、 アラート：設定 （3654 ページ）を参照してください。

（注） 監視対象デバイスの指定については、監視対象デバイスの管理 （3616ページ）を参照してください。

[アラート（Alerts）] 画面に切り替えるには、次の操作を実行します。

- HPM メニューバーの下にある [アラート（Alerts）] ボタンをクリックします

（[モニタリング（Monitoring）] ボタンをクリックするとモニタリング画面に戻ります）。

（注） 特定のデバイスの詳細を表示しているときに、[アラート（Alerts）] タブから特定のデバイスに適用されるアラートを表示することもできます（ モニタリングビュー：デバイスまたは VPN の詳細 （3646 ページ）を参照）。

アラートリストは、行と列で構成される基本的なテーブルであり、各行は特定のデバイスからの 1 つのアラートを表します。各列には、そのアラートに関する特定の情報（デバイス名、アラートの重大度、記録時間など）が表示されます（アラート画面の詳細については、HPM ウィンドウ：アラートディスプレイ （3652 ページ）を参照してください）。

（注） 列見出しは、選択したパラメータに従ってアラートを非表示または表示することにより、テーブルをフィルタ処理するために使用できるメニューです。たとえば、特定のデバイスのアラートのみを表示してから、そのデバイスの重大なアラートのみを選択することができます。詳細については、テーブル列の操作 （3619ページ）を参照してください。

ヒント　トンネルアップ/ダウンアラートの [説明（Description）] 列のハイパーリンクをクリックして、イベントビューアでそのデバイスの IPSec VPN イベントを表示できます。イベントビューアには、デバイスのポーリング間隔に応じた時間範囲内におけるデバイスの IPSec VPN イベントが表示されます。優先デバイスの場合、時間範囲は最初のアップ/ダウン通知の受信前と受信後の 5 分間です。非優先デバイスの場合、時間範囲は 5 分ではなく +/- 10 分になります。

アラートテーブルでは、スクロールだけでなく、特定のアラートのセットを表示することもできます。

- このテーブルの上にある [リストをフィルタ処理（List Filter）] フィールドを使用して、リストをフィルタリングします。詳細については、リストフィルターフィールドの使用（3635 ページ）を参照してください。
- [クリアされたアラートの表示（View Cleared Alerts）] ウィンドウを使用して、指定した時間範囲で選択された一連のデバイスについて、以前にクリアされたアラートを表示します。詳細については、アラート：履歴 （3665 ページ）を参照してください。

また、アラートの確認、アラートのクリア、アラートノートの編集を行うこともできます。

- アラート：確認応答とクリア （3664 ページ）で説明されているように、アラートを確認またはクリアできます。
- 既存のアラートメモに追加するには、テーブル内の該当するエントリの [メモ（Notes）] フィールドをクリックして、[メモの入力（Enter Notes）] ダイアログボックスを開きます。このダイアログボックスは、メモを表示してアラートに追加するために使用します。テーブルで既存のメモを含む単一のアラートが選択されている場合にのみ使用できます。

アラート：確認応答とクリア

アラート：表示 （3663 ページ）で説明されているように、監視対象デバイスに対して生成されたすべてのアラートが [アラート（Alerts）] テーブルに表示されます。個々のアラートにメモを追加したり、アラートを個別またはグループで確認または消去したりできます。

アラートを選択するには、[アラート（Alerts）] テーブルでそのエントリをクリックします。Shift キーを押しながら別のアラートをクリックして、2 つの間のグループを選択できます。また、Ctrl キーを押しながらさまざまな行をクリックして、連続していない複数のアラートを選択できます。

テーブルでアラートを選択すると、次のことができます。

- [確認（Acknowledge）] ボタンをクリックして [アラートの確認（Acknowledge Alert）] ダイアログボックスを開きます。これを使用してメモを追加し、選択したアラートを確認済みとしてマークします。一度に複数のアラートを確認できます。

このダイアログ ボックスの [メモ（Notes）] フィールドにテキストを入力し（これはオプションです）、[OK] をクリックします。ダイアログボックスが閉じ、アラートが確認済みとしてマークされ、[メモ（Notes）] カラムにタイムスタンプが表示されます。

- [クリア（Clear）] ボタンをクリックして [アラートのクリア（Clear Alert）] ダイアログボックスを開き、メモを追加し、選択したエントリを [アラート（Alerts）] テーブルから削除します。

このダイアログ ボックスの [メモ（Notes）] フィールドにテキストを入力し（これはオプションです）、[OK] をクリックします。ダイアログボックスが閉じ、選択したアラートが [アラート（Alerts）] テーブルから削除されます。

（注） 関連するしきい値を変更すると、アラートは HPM によって自動的にクリアされます。クリアしたアラートと同様に、これらのアラートは [クリアされたアラートの表示（View Cleared Alerts）] ウィンドウで確認できます（アラート：履歴 （3665 ページ）を参照）。

クリアされたアラートに関するメモやその他の情報は、[アラート（Alerts）] データベースに 30 日間保存されます。

アラート：履歴

モニタリング対象デバイスに対して生成されたすべてのアラートは、[HPM] ウィンドウに表として表示されます。アラート：表示 （3663 ページ）で説明されているように、表示されている列パラメータでテーブルをフィルタリングできます。

[クリアされたアラートの表示（View Cleared Alerts）] ボタンを使用して、以前にクリアされたアラートにアクセスして確認することができます。対象となるデバイスのセットと時間範囲を指定してください（アラートのクリアについては、アラート：確認応答とクリア （3664 ページ）で説明されています）。

（注） クリアされたアラートに関するメモやその他の情報は、アラートデータベースに 30 日間保持されます。生成から 30 日を超えたアラートにはアクセスできません。

[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウを開いて使用するには、次の手順に従います。

1. [アラート（Alerts）] 画面で、[リストフィルタ（List Filter）] フィールドの横にある [クリアされたアラートの表示（View Cleared Alerts）] ボタンをクリックして、[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウを開きます（[HPM] ウィンドウの [アラート（Alerts）] 画面へのアクセスに関する詳細については、アラート：表示 （3663 ページ）を参照してください）。
2. アラートの表示設定を指定します。これらの設定により、表示するアラートのセットが定義されます。

- 対象のデバイスを指定します。[すべて（All）] のデバイスがデフォルトで選択されています。特定のデバイスセットを選択するには：
- [選択（Select）] ボタンをクリックして、[デバイスの選択（Select Device）] ダイアログボックスを開きます。
- 目的のデバイスを選択します。除外するデバイスの選択を解除します。
- [OK] をクリックして [デバイスの選択（Select Devices）] ダイアログボックスを閉じます。
- 表示するアラートのタイプを指定します。[重大（Critical）]、[警告（Warning）]、[正常（Normal）] を選択または選択解除します。
- [開始（From）] の日時および [終了（To）] の日時を選択して、目的の [時間範囲（Time Range）] を定義します。この範囲内に [最初の確認（First Seen）] 時刻が入っているすべてのアラートが表示されます。

[開始（From）] と [終了（To）] にはそれぞれ、月と日の選択に使用される標準のドロップダウンカレンダーが表示されます。

各カレンダーの下の時間フィールドを使用して、正確な開始時刻または終了時刻をそれぞれ指定します。数字を強調表示して上矢印または下矢印をクリックするか、目的の数字を入力します。[現在（Now）] ボタンをクリックして、現在の時刻を指定することもできます。

1. [検索（Search）] ボタンをクリックして、定義済みのアラートセットを表示します。

[クリアされたアラートの表示（View Cleared Alerts）] ウィンドウには、クリアされたアラートの表示をフィルタリングするために使用できる [リストフィルタ（List Filter）] フィールドがあることに注意してください。このフィールドの使用方法については、リストフィルターフィールドの使用 （3635 ページ）で説明されています。

このテーブルをフィルタリングする他の方法については、テーブル列の操作 （3619ページ）を参照してください。

SNMP トラップ転送通知

4.6 以前のバージョンの Security Manager では、ASA、IPS、および VPN に関して Health and Performance Monitor のアラートが生成されると、電子メール通知がユーザーに送信されていました。

このフレームワークは、Security Manager 4.7 で、電子メール通知に加えて SNMP トラップ通知を送信するように拡張されました。Security Manager 4.7 はアラートをトラップに変換し、それらを中央 SNMP トラップサーバーに送信します。SNMP v1、v2c、および v3 がサポートされています。アラートが最初に生成されるとトラップが生成され、重大度が増加するとトラップが再生成されます。その結果、電子メール通知の場合と同様に、トラップが最大 2 回生成されます。

SNMP トラップ転送通知には、次の前提条件があります。

1. SNMP トラップ受信者（サーバー）を使用できる。また、特定の Security Manager インストールに複数のサーバーを使用できる。
2. ASA デバイスを使用できる。
3. IPS 7.0.x 以降を実行する IPS センサーを使用できる。
4. Health and Performance Monitor が有効になっている。

ヒント　Health and Performance Monitor が有効になっていることを確認するには、[Configuration Manager] > [ツール（Tools）] > [Security Manager 管理（Security Manager Administration...）] > [Health and Performance Monitor] に移動します。

1. Health and Performance Monitor で ASA デバイスおよび IPS センサーデバイスの通常または優先監視が有効になっている。
2. ファイアウォール、IPS、および VPN のアラート設定が有効になっている。

ヒント　ファイアウォール、IPS、および VPN のアラート設定を有効にするには、[Health and Performance Monitor] > [ツール（Tools）] > [アラート設定（Alert Configuration）] に移動します。

MIB ドキュメント

ここでは、Security Manager がトラップ通知の送信に使用する MIB と、特定のアラート情報を取得するためにユーザーが検索する必要がある OID について説明します。

SNMP トラップの場合、Security Manager は「CISCO-DEVICE-EXCEPTION-REPORTING-MIB」を使用します。

次のリストには、OID の詳細とそれに含まれる情報が示されています。

- iso.org.dod.internet.mgmt.mib-2.system.sysUpTime.0（HPM サーバーの稼働時間を示します）：「システム稼働時間 = 現在の Security Manager サーバー時間 - HPM サービス起動時間」で計算されます。
- snmpTrapOID（1.3.6.1.4.1.9.9.224.2.0.1）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.2（「memory usage」のようなアラートルール名をリストします）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.3（定数値 1、IP アドレスタイプを示します）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.4（デバイス表示名：デバイスタイプおよびクラスタノード（存在する場合）とデバイスの名前）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.5（アラートの重大度）

- .1.3.6.1.4.1.9.9.224.1.1.5.1.6（アラートのタイムスタンプ）：現在の Security Manager サーバー時間 - アラートが最初に生成された時間
- .1.3.6.1.4.1.9.9.224.1.1.5.1.7（アラートを説明する最大 1024 文字の文字列）
- .1.3.6.1.4.1.9.9.224.1.1.5.1.8（Security Manager サーバー名）

ここでは、次の内容について説明します。

- [SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックス （3668 ページ）
- [SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックス （3669 ページ）

[SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックス

SNMP トラップ転送通知の開始点として [SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックスを使用します。

ナビゲーション パス

Health and Performance Monitor で、[ツール（Tools）] メニューから [SNMPトラップの設定（SNMP Trap Configuration）] を選択します。[SNMPトラップエントリ（SNMP Trap Entries）] ダイアログボックスには、次の領域が含まれています。

- 現在設定されているトラップを表示する [設定（Settings）] テーブル。
- SNMP トラップエントリを操作するための追加、編集、およびその他のオプション。

フィールド リファレンス

表 *986 : [SNMP*トラップエントリ（*SNMP Trap Entries***）*]* ダイアログボックスの *[*設定（***Settings***）*]* テーブルとその他のオプション**

フィールド	説明
[トラップの転送先（Forward Trap To）] テーブル	
[ステータス（Status）] 列	[Enabled] と [Disabled] があります。常に最大 5 つのトラップ転送ホストを有効にできます。
[IP/ホスト（IP/Host）]列	中央 SNMP トラップサーバーの IP アドレスまたはホスト名。パフォーマンスの問題を避けるため、ローカルホストおよび Security Manager サーバーは、両方とも SNMP サーバーとして使用できません。
[ポート（Port）] 列	中央 SNMP トラップサーバーが使用するポート

フィールド	説明
[SNMPバージョン（SNMP Version）] 列	v1、v2c、または v3。デフォルトは v2c です。
[Username] カラム	SNMP サーバーに対する認証用のユーザ名
[認証アルゴリズム（Authentication Algorithm）] 列	MD5 または SHA
[暗号化アルゴリズム（Encryption Algorithm）] 列	DES、3DES、AES128、AES192、および AES256
追加（Add）	新しい設定の追加に使用します。[追加（Add）] ボタンをクリックすると、[トラップ設定の追加（Add Trap Settings）] ダイアログボックスが開きます。
Edit	既存の設定の編集に使用します。[編集（Edit）] ボタンをクリックすると、[トラップ設定の編集（Edit Trap Settings）] ダイアログボックスが開きます。
設定のコピー（Copy Settings）	既存の構成のすべての設定をコピーするために使用されます。[設定のコピー（Copy Settings）] ボタンをクリックすると、[SNMPトラップ設定のコピー（Copy SNMP Trap Settings）] ダイアログボックスが開きます。
削除（Delete）	既存の設定の削除に使用します。
有効	既存の設定の有効化に使用します。
無効	既存の設定の無効化に使用します。

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックス

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックスを使用して、SNMP トラップを追加、編集、およびその他の方法で操作および設定します。

ナビゲーション パス

ヘルスとパフォーマンスのモニターで、[ツール（Tools）] メニューから [SNMPトラップの設定（SNMP Trap Configuration）] を選択します。次に、[追加（Add）]、[編集（Edit）]、または [設定のコピー（Copy Settings）] を選択します。

[SNMPトラップエントリの追加/編集/コピー（Add/Edit/Copy SNMP Trap Entries）] ダイアログボックスには、次のエリアがあります。

- IP/ホストおよびポートエリア
- FW アラート、IPS アラート、および VPN アラートのトラップ設定エリア
- SNMP オプションのトラップ設定エリア

フィールド リファレンス

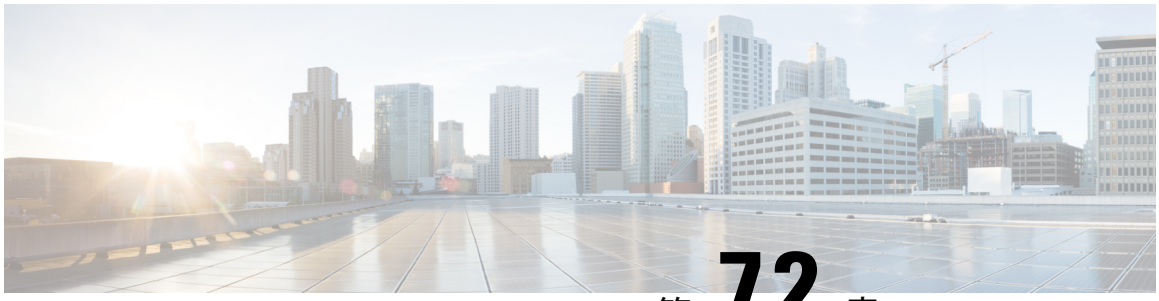
表 *987 : [SNMP*トラップエントリの追加/編集/コピー（*Add/Edit/Copy SNMP Trap Entries*）*]* ダイアログ ボックスの *[*トラップ設定（*Trap Settings*）*]* エリアおよびその他のオプション

フィールド	説明
トラップの設定	次のトピックで説明されている、FW、IPS、および VPN のすべてまたは選択したアラートのみを選択するために使用されます。 • アラート設定：ファイアウォール （3658ページ） • アラート設定：IPS （3656 ページ） • アラート設定：VPN （3660 ページ）
SNMP オプション	
RO Community String （SNMP バージョン V1 と V2C のみ）	SNMP バージョン v1 または v2c で認証に使用されるパスワード。
グループ タイプ （SNMP バージョン v3 のみ）	NOAUTH、AUTH、または PRIV。
エンジンID（Engine ID） （SNMP バージョン v3 のみ）	v3 で認証に使用される SNMPEngineID 識別子。
ユーザー名 （SNMP バージョン v3 のみ）	SNMP サーバーに対する認証用のユーザー名
認証パスワード（Authentication Password） （SNMP バージョン v3 のみ）	SNMP サーバーに対する認証用のパスワード
認証プロトコル（Authentication Protocol） （SNMP バージョン v3 のみ）	MD5 または SHA。
Encryption Password （SNMP バージョン v3 のみ）	MD5 または SHA 暗号化のパスワード。

フィールド	説明
暗号化プロトコル（Encryption Protocol） （SNMP バージョン v3 のみ）	DES、3DES、AES128、AES192、およびAES256。

注：AES192、AES256、または 3DES を使用するには、次の手順に従う必要があります。

1. http://www.oracle.com/technetwork/ > [ダウンロード（Downloads）] > [Java SE] > [JDK/JRE 7用Java暗号拡張（ JCE）無制限の強度の司法管轄権ポリシーファイル（Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files for JDK/JRE 7）] から、無制限の強度の暗号ポリシー .jar ファイルをダウンロードします。（[ダウンロード（download）] ボタンをクリックして、ライセンス契約に同意し、ファイルをダウンロードします。）
2. Security Manager サーバーの CSCOpx\MDC\vms\jre\lib\security フォルダにある local_policy.jar および US_export_policy.jar を置き換えます。
3. Security Manager サーバーを再起動します。



第 72 章

外部モニタリング、トラブルシューティング、および診断ツールの使用方法

大規模な企業やサービスプロバイダーでは、高いネットワーク可用性が求められます。ネットワーク管理者は、ネットワーク可用性を維持するうえでさまざまな課題に直面しています。課題には、予定外のダウンタイム、専門知識の不足、不十分なツール、複雑なテクノロジー、ビジネス統合、競争の激しい市場などがあります。これらの課題に対応して解決するには、ネットワークモニタリング、問題診断、およびトラブルシューティングが不可欠です。

モニタリングでは、ネットワークアクティビティおよびデバイスのステータスを調査して、異常なイベントおよび動作を識別します。ネットワークおよびシステムの障害（停止や低下など）を迅速に診断および修正することによりサービスアベイラビリティが向上するため、問題を切り分け、分析、および修正するためのツールが不可欠です。

デバイスイベントをモニタリングするための主なSecurity Managerツールは、ヘルスとパフォーマンスのモニタ（第71章「ヘルスとパフォーマンスのモニタリング」を参照）とイベントビューア（第69章「イベントの表示」を参照）です。

ヘルスとパフォーマンスのモニタ、およびイベントビューアに加え、次のトピックでは、Security Managerで使用できるその他のモニタリング、トラブルシューティング、および診断ツールについて説明します。

- ダッシュボードの概要 （3674 ページ）
- CSM Mobile （3692 ページ）
- インベントリ ステータスの表示 （3694 ページ）
- デバイス マネージャの起動 （3697 ページ）
- Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）
- Packet Tracer を使用した ASA または PIX の設定の分析 （3709 ページ）
- ping、トレースルート、またはNSルックアップツールを使用した接続問題の分析 （3713 ページ）
- Packet Capture Wizard の使用 （3718 ページ）
- IPインテリジェンス（IP Intelligence） （3723 ページ）
- CS-MARS と Security Manager の統合 （3727 ページ）

ダッシュボードの概要

バージョン4.5以降、Security Managerクライアントには新しい起動ポイント（構成可能なダッシュボード）があります。このトピックでは、このダッシュボードについての概要を説明します。

このダッシュボードは、Security Manager クライアントの起動時にデフォルトのクライアント アプリケーションとして選択できる 6 つのクライアント アプリケーションの 1 つです（他には、Configuration Manager、Event Viewer、Report Manager、Health and Performance Manager、Image Manager があります。CSM Mobile と呼ばれるモバイルデバイス用に設計されたアプリケーションもあります）。このダッシュボードを使用することによって、Security Manager の他の領域にある、IPS Health Monitor ページ、Report Manager、Health and Performance Monitor および IP Intelligence 設定などのタスクを 実行できます。

ダッシュボードには、次の表に示すウィジェットが含まれています。ウィジェットは、IPS、ファイアウォール、またはその両方の各用途別に分類されています（これらのウィジェットのすべてがデフォルトで表示されるわけではありません）。元のダッシュボードに加えて、新規ダッシュボードや追加のダッシュボードを作成して、タブとして表示できます。元のダッシュボードと、作成した新規や追加のダッシュボードの両方は、すべてカスタマイズ可能です。ダッシュボードをカスタマイズするには、使用可能なウィジェットのリストから任意のダッシュボードにウィジェットをドラッグアンドドロップします。

表 ***988 : IPS***、ファイアウォール、およびその両方に使用するウィジェット

IPS 用ウィジェット	• **IPSインスペクション負荷トレンド（IPS Inspection Load Trends）** • **IPS 攻撃者、攻撃対象、およびシグニチャに関する上位10のレポート（Top 10 Reports for IPS Attackers, Victims, and Signatures）** • **IPS欠落パケットトレンド（IPS Missed PacketTrends）** • **IPSライセンス（IPS License）** • **IPS更新パッケージ（IPS Update Packages）** • **古いIPSセンサー（IPS Sensors Out of Date）**
ファイアウォール用ウィジェット	• ファイアウォールの送信元、宛先、サービスに関する上位 10 のレポート（Top 10 Reports for Firewall Sources, Destinations, and Services） • ボットネットマルウェアサイト、ポート、ホストに関する上位10のレポート（Top 10 Reports for Botnet Malware Sites, Ports, and Hosts） • ファイアウォールCPU使用率トレンド（Firewall CPU Usage Trends）

IPS 用ウィジェット	• **IPSインスペクション負荷トレンド（IPS Inspection Load Trends）** • **IPS 攻撃者、攻撃対象、およびシグニチャに関する上位10のレポート（Top 10 Reports for IPS Attackers, Victims, and Signatures）** • **IPS欠落パケットトレンド（IPS Missed PacketTrends）** • **IPSライセンス（IPS License）** • **IPS更新パッケージ（IPS Update Packages）** • **古いIPSセンサー（IPS Sensors Out of Date）**
IPSおよびファイアウォールの両方に使用するウィジェット	• デバイスの健全性の概要（Device Health Summary） • メモリ使用量トレンド（Memory Usage Trends） • 展開 • IPインテリジェンス（IP Intelligence）

ダッシュボードとそのウィジェットの使用方法は、Security Manager を使用する目的によって異なります。たとえば、次の4つのウィジェットを使用して、デバイスの正常性の傾向を観察できます。

- IPSインスペクション負荷トレンド（IPS Inspection Load Trends）
- IPS欠落パケットトレンド（IPS Missed PacketTrends）
- メモリ使用量トレンド（Memory Usage Trends）
- ファイアウォールCPU使用率トレンド（Firewall CPU Usage Trends）

個々のウィジェットについて、次の表で説明します。主要なウィジェットの 1 つは、[デバイスの健全性の概要（Device Health Summary）] ウィジェットです。重要であることの理由の 1 つは、モバイルデバイス用に特別に設計された CSM Mobile を介してアクセスできる情報と同じ情報を提供することです。CSM Mobile の詳細については、CSM Mobile （3692 ページ）を参照してください。CSM Mobile の有効化または無効化については、[CSM Mobile] ページ （653 ページ）を参照してください。

表 *989:*個々のウィジェットの説明 ダッシュボードウィジェット ダッシュボード内の ***IPS***用ウィジェット ダッシュボード内のファイアウォール用ウィジェット

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS** デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
IPS 攻撃者、攻撃対象、およびシグニチャに関する上位10のレポート（Top 10 Reports for IPS Attackers, Victims, and Signatures）	

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	ネットワーク内の IPS アラートの上位攻撃者、攻撃対象、およびシグニチャの分析に使用できる事前定義システムレポート。 **クリック可能なリンク**：[上位攻撃者（Top Attackers）] ウィジェットでは、IP アドレスはアクティブなハイパーリンクです。クリックすると IP インテリジェンスが表示されます。Security Manager の IP インテリジェンスの詳細については、 IP インテリジェンス（IP Intelligence） （3723 ページ）を参照してください。 **クリック可能なリンク**：[上位シグニチャ（Top Signature）] ウィジェットでは、シグニチャ ID はアクティブなハイパーリンクです。クリックすると、シグニチャ情報が表示されます。 これらのレポートを使用するには、Report Manager を使用します（[起動（Launch）] > [Report Manager...]）。 これらの上位 10 レポートのいずれかから Event Viewer をクロス起動するには、特定の攻撃者、攻撃対象、またはシグニチャを選択し、発生数をクリックします。デフォルトでは、過去 24 時間の発生数がリストされます。必要に応じて、過去 1 時間に変更できます。 （注） Event Viewer をクロス起動すると、サマリーダッシュボードでは過去 24 時間または過去 1 時間であっても、Event Viewer のイベントクエリ時間は過去 10 分として表示されます。ドロップダウンリストを使用して、Event Viewer のイベントクエリ時間を過去 10 分間から別の値に変更できます。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
IPS欠落パケットトレンド（IPS Missed PacketTrends）	IPS欠落パケットトレンドの測定。欠落パケットのトレンドデータは、欠落したパケットに基づくアラートがある場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 （デバイスビューのIPSデバイス）[プラットフォーム（Platform）]>[デバイス管理（Device Admin）]>[ヘルスモニター（Health Monitor）]の[IPSヘルスモニター（IPS Health Monitor）]ページでモニタリングパラメータを設定できます。
IPSライセンス（IPS License）	ライセンスが 30 日または 60 日で期限切れになる IPS デバイスを表示します（ドロップダウンリストを使用して、30 日または 60 日を選択します）。 ライセンスが 30 日または 60 日（選択した方）で期限切れになると、このウィジェットにはライセンスの有効期限が表示されます。
IPS更新パッケージ（IPS Update Packages）	Cisco.com またはローカル ダウンロード サーバーに存在するが、Security Manager サーバーにはダウンロードされていないセンサーの更新およびシグニチャの更新を表示します。 このような更新が多数ある場合、このウィジェットには最新の10件の更新のみが表示されます。
古いIPSセンサー（IPS Sensors Out of Date）	シグネチャの更新が必要なセンサー。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
ファイアウォールの送信元、宛先、サービスに関する上位 10 のレポート（Top 10 Reports for Firewall Sources, Destinations, and Services）	ファイアウォールACLイベントの上位の宛先、サービス、および送信元の識別に用できる事前定義システムレポート。この統計情報は、Event Manager サービスで収集されるイベント（Event Viewer に表示されるイベント）に基づいています。 これらのレポートを使用するには、Report Managerを使用します（[起動（Launch）] > [Report Manager...]）。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
ボットネットマルウェアサイト、ポート、ホストに関する上位10のレポート（Top 10 Reports for Botnet Malware Sites, Ports, and Hosts）	ボットネットトラフィックフィルタリングの分析に使用できる事前定義システムレポート。この統計情報は、ブロックリストおよびグレーリストにあるサイトについて Event Manager サービスで収集されるボットネットイベント（Event Viewer に表示されるイベント）に基づいています。 これらのレポートを使用するには、Report Manager（**[**起動（**Launch**）**]** > **[Report Manager]**）を使用します。
ファイアウォールCPU使用率トレンド（Firewall CPU Usage Trends）	ファイアウォールの CPU 使用率トレンドの測定。CPU 使用率トレンドデータは、ファイアウォールが CPU 使用率のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
デバイスの健全性の概要（Device Health Summary）	

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS** デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ **（デバイスビューの IPS デバイス）[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ヘルスモニター（Health Monitor）] の [IPSヘルスモニター（IPS Health Monitor）] ページでモニタリングパラメータを設定できます。**
	HPM によって生成された、現在の重大度の高いまたは中程度のアクティブなアラートを表示します。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。 **クリック可能なリンク**：デバイス名はアクティブなハイパーリンクです。クリックすると、ダッシュボードに [デバイスの概要（Device Summary）] ダイアログボックスが表示されます。このリンクは、[_____ でグループ化（Group by _____）] ドロップダウンリストのすべてのオプション（[アラート（Alert）]、[カテゴリ（Category）]、[デバイス（Device）]、または [テクノロジー（Technology）]）で機能します。 これらのアラートを構成するには、HPM（[起動（Launch）] > [Health and Performance Monitor...]）を使用します。 （注） HPM でデバイスの監視をイネーブルにした後、実際の値が [デバイスの健全性の概要（Device Health Summary）] に表示されるまで、優先デバイスの場合は最大 5 分、非優先デバイスの場合は 10 分かかることがあります。 **アラートの確認**：アラートを確認するには、次の手順に従います。 **1.** [_____ でグループ化（Group by _____）] ドロップダウンリストを使用して、[アラート（Alert）]、[カテゴリ（Category）]、[デバイス（Device）]、または [テクノロジー（Technology）]）を選択します。。 **2.** 関心のあるアラート、カテゴリ、デバイス、またはテクノロジーを展開しま

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	す。これを行うと、Security Manager で監視している各デバイスのアラート、カテゴリ、デバイス、またはテクノロジーが表示されます。 **3.** [詳細（Detail）] アイコン（このトピックの最後に示しています）をクリックします。これにより、[アラート（Alert）] ダイアログボックスが開きます。 **4.** [アラートを確認（Acknowledge Alert）] をクリックします。 **アラートのクリア**：アラートをクリアするには、次の手順に従います。 **1.** [_____ でグループ化（Group by _____）] ドロップダウンリストを使用して、[アラート（Alert）]、[カテゴリ（Category）]、[デバイス（Device）]、または [テクノロジー（Technology）]）を選択します。。 **2.** 関心のあるアラート、カテゴリ、デバイス、またはテクノロジーを展開します。これを行うと、Security Manager で監視している各デバイスのアラート、カテゴリ、デバイス、またはテクノロジーが表示されます。 **3.** [詳細（Detail）] アイコン（このトピックの最後に示しています）をクリックします。これにより、[アラート（Alert）] ダイアログボックスが開きます。 **4.** [アラートのクリア（Clear Alert）] をクリックします。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	モバイルデバイスからもデバイス健全性の概要情報にアクセスできます。これを行うには、CSM Mobile アプリケーションを使用します。CSM Mobile から入手できる情報は、[デバイスの健全性の概要（Device Health Summary）] ウィジェットで入手できるものと同じです。CSM Mobile の有効化または無効化については、[CSM Mobile] ページ （653 ページ）を参照してください。
メモリ使用量トレンド（Memory Usage Trends）	IPS 健全性ステータスまたはファイアウォール健全性トレンドの測定。 IPS デバイスの場合、（デバイスビューの IPS デバイス）[プラットフォーム（Platform）] > [デバイス管理（Device Admin）] > [ヘルスモニター（Health Monitor）] の [IPS ヘルスモニター（IPS Health Monitor ）] ページでモニタリングパラメータを設定できます。
展開	過去 24 時間のすべてのデバイスの展開ステータスを表示します。 Deployment Manager（[Configuration Manager] > [管理（Manage ）] > [展開（Deployments）]）を使用して展開ステータスを監視することもできます。 。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
IPインテリジェンス（IP Intelligence）	次の事項に関連する、IP アドレスについての情報。 • IP 位置情報 • DNS リバースルックアップによる FQDN • WHOIS 情報 Security Manager の IP インテリジェンス設定については、[Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [IPインテリジェンス設定（IP Intelligence Settings）] に移動します。

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
CSM モニター	

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS**デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**] の [IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	サーバー情報を次の 3 つのカテゴリで表示します。 • CSMサーバー統計情報。この情報は、その名が示す通りです。たとえば、オペレーティングシステムの起動時間が表示されます。 • CSMユーザ関連情報。この情報には、ログインしているユーザ数という 1 つの項目のみが含まれます。 • CSM DB バックアップ関連情報。この情報は、[CMSモニター（CSM Monitor）] ウィジェットが未解決のバックアップロックファイルを検出したかどうかを示します。 未解決のバックアップロックファイルがあるかどうかを知ることは、次の理由で重要です。CSM バックアップを実行すると、次のようなエラーで失敗します。「ERROR(383): C:\PROGRA~2\CSCOpx\backup.LOCK file exists.」 次のような解決策が考えられます。Security Manager は、バックアップを開始する前に、バックアップディレクトリに新しいロックファイル（backup.LOCK)）を作成します。バックアップが中断または失敗した場合、このファイルはクリーンアップされません。Security Manager サーバーから現在の backup.LOCK ファイルを削除してから、バックアッププロセスを再度実行する必要があります。 [CMSモニター（CSM Monitor）] ウィジェットを使用すると、未解決のバックアップロック ファイルをより迅速かつ便利に検出できます。 詳細については、次の URL にある Cisco TAC のドキュメントを参照してくださ

IPSインスペクション負荷トレンド（**IPS Inspection Load Trends**）	**IPS**インスペクション負荷トレンドの測定。インスペクション負荷トレンドデータは、**IPS** デバイスがインスペクション負荷のためにアラートを発行した場合にのみこのウィジェットに表示され、アラートがクリアされるとデータは消えます。 センサーが使用しているトラフィックインスペクション容量を示します。**0**はトラフィックのバックアップがないことを示し、**100**はバッファが完全にバックアップされていることを示します。インスペクション負荷は、次の要因の影響を受けます。 • インスペクションが必要なトラフィックの割合 • 検査の対象となるトラフィックの種類 • 検査の対象となるアクティブな接続の数 • **1** 秒あたりの新規接続の割合 • 検出される攻撃の割合 • センサーでアクティブなシグニチャ • センサーで作成されたカスタムシグニチャ （デバイスビューの **IPS** デバイス）**[**プラットフォーム（**Platform**）**] > [**デバイス管理（**Device Admin**）**] > [**ヘルスモニター（**Health Monitor**）**]** の **[IPS**ヘルスモニター（**IPS Health Monitor**）**]** ページでモニタリングパラメータを設定できます。
	い。 http://www.cisco.com/en/US/products/ps6498/products_tech_note09186a0080c13cdd.shtml

（注） 場合によっては、上位の感染ホストなどのダッシュボードレポートの外観が、 Report Managerによって生成されたレポートとわずかに異なります。これは並べ替えの違いによるものですが、データは同一です。このようなケースは、ダッシュボードレポートの複数のエントリに同じカウントがある場合に発生します。

ダッシュボードの基本的な操作を次の表に示します。

表 *990 :* ダッシュボードの基本操作ダッシュボードの操作

ダッシュボードの起動	**Configuration Manager** またはその他の **Security Manager** クライアントアプリケーション**>[**起動（**Launch**）**]>[**ダッシュボード（**Dashboard**）**]**
新しいダッシュボードの追加	[ファイル（File）] > [新規ダッシュボード（New Dashboard）]

ダッシュボードの起動	**Configuration Manager** またはその他の **Security Manager** クライアントアプリケーション**>[**起動（**Launch**）**]>[**ダッシュボード（**Dashboard**）**]**
デフォルトビューのダッシュボードタブを再配置する	ダッシュボードのタブを再配置して、デフォルトビューを設定できます。たとえば、[IPS] タブを最初（左端） にしたい場合があります。 **1.** [サマリー（Summary）]、[ファイアウォール（Firewall）]、[IPS] など、関心のあるタブをクリックします。 **2.** 目的のタブが選択されたままの状態で右クリックすると、コンテキスト メニュー オプション [左に移動（Move to Left）]、[右に移動（Move to Right）]、[最初に移動（Move to First）]、[最後に移動（Move to Last）] が表示されます。 **3.** 選択する項目をクリックします。 **4.** 変更を保存する必要はありません。また、変更は永続的です。個々のダッシュボードタブは、次回ダッシュボードを起動したときに同じように配置されます。
別のダッシュボードを表示する	[サマリー（Summary）]、[ファイアウォール（Firewall）]、[IPS] など、目的のダッシュボードのタブをクリックします。
ウィジェットの表示または非表示	[ファイル（File）] > [ウィジェットを表示（Show Widgets）] または [ファイル（File）] > [ウィジェットを非表示（Hide Widgets）]
ウィジェットの追加	ドラッグアンドドロップによる方法： **1.** [ファイル（File）] > [ウィジェットを表示（ Show Widgets）] に移動します。 **2.** 目的のウィジェットを、ダッシュボードにドラッグアンドドラッグします。 メニューによる方法： **1.** [ファイル（File）] > [ウィジェットを表示（ Show Widgets）] に移動します。 **2.** 目的のウィジェットをクリックして選択します。 **3.** 説明バーで [追加（Add）] をクリックします。 **4.** 説明バーで [完了（Done）] をクリックします。 （**注**） メニューによる方法を使用すると、ウィジェットはダッシュボードの左上隅に追加されます。必要に応じて、すべてのウィジェットをドラッグアンドドロップして並べ替えることができます。

ダッシュボードの起動	**Configuration Manager** またはその他の **Security Manager** クライアントアプリケーション**>[**起動（**Launch**）**]>[**ダッシュボード（**Dashboard**）**]**
ウィジェットの削除	削除するウィジェットのタイトルバーにある [削除（Remove）] アイコンをクリックします。
ウィジェットの展開	ダッシュボードにウィジェットが表示されている場合は、下矢印で展開できます。ウィジェットのタイトルバーの右側にマウスポインタを合わせると、下矢印が表示されます。下矢印のツールチップには、「展開（Expand）」というラベルが付いています。 （注） ウィジェットを折りたたんで、ダッシュボードを終了し、ダッシュボードを再度起動したときは、特別な操作が必要となります。この場合、ウィジェットは引き続き折りたたまれていますが、（通常は展開に使用される）下矢印は表示されません。上矢印 （通常は折りたたむために使用）のみが表示されます。この場合、ウィジェットを展開するには、上矢印をクリックします。下矢印が再び表示されますので、通常どおり下矢印をクリックします。
ウィジェットを折りたたむ	ダッシュボードにウィジェットが表示されている場合は、上矢印で折りたたむことができます。ウィジェットのタイトルバーの右側にマウスポインターを合わせると、上矢印が表示されます。上矢印のツールチップには、「展開（Expand）」というラベルが付いています (「折りたたむ（Collapse）」ではありません）。
_____ でグループ化 （[デバイスの健全性の概要（Device Health Summary）] ウィジェットのみ）	次の選択肢を提供するドロップダウンリスト： • アラートでグループ化 • カテゴリでグループ化 • デバイスでグループ化 • テクノロジーでグループ化 （注） [_____でグループ化（Group by _____）] ドロップダウンリストで、デバイスの表示名（ハイパーリンクであることを示すために下線が引かれています）をクリックして、メモリやその他のパラメータについて、デバイスの健全性に関する情報ボックスを表示できます。情報ボックスにはアドレスフィールドがあります。アドレスは Host.Domain または IP アドレスのいずれかです。Host.Domain が構成されている場合、その情報が表示されます。それ以外の場合は、IPアドレスが表示されます。

ダッシュボードの多くのアイコンは、クリックすることで更新やダッシュボードの追加などの特定のアクションを実行できます。これらのクリック可能なアイコンのほとんどには、アイコンをクリックすると実行されるアクションを説明するツールチップがありますが、いくつかの

アイコンにはツールチップがありません。ダッシュボード内のツールチップのないクリック可能アイコンを次の表に示します。

表 *991* : ダッシュボード内のツールチップがないクリック可能アイコン ダッシュボードアイコン ダッシュボード内のツールチップがないアイコン

アイコン	表示	ウィジェット	説明
	三角形の黄色の背景に黒い感嘆符。	[展開（Deployment）] ウィジェット	[展開中（Deploying）] アイコン。 ジョブが展開中の状態であることを示します。このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）
	赤と黄色のドットが付いた白い長方形（ドキュメント）。	[展開（Deployment）] ウィジェット	[ステータスレポート（Status Report）] アイコン。 このアイコンをクリックして、詳細な展開ステータスレポートを表示します。
	灰色の縁取りのある緑の円の中に白いチェックマーク。	[展開（Deployment）] ウィジェット	[成功（Succeeded）] アイコン ジョブが成功状態であることを示します。このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）

アイコン	表示	ウィジェット	説明
	灰色の縁取りの赤い円の中に白い「X」。	[展開（Deployment）] ウィジェット	[失敗（Failed）] アイコン。 ジョブが失敗した状態であることを示します。このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）
	紙に注釈を付けている鉛筆とクリップボード。	[デバイスの健全性の概要（Device Health Summary）] ウィジェット	[詳細（Details）] アイコン このアイコンをクリックして、次のジョブの説明を開閉します。 • 作成された日付と時刻 • ジョブ名 • 説明 • ステータス • ユーザー（User） • ジョブ タイプ（Job Type）

CSM Mobile

バージョン 4.5 以降、Cisco Security Manager には CSM Mobile と呼ばれるアプリケーションがあります。

CSM Mobile では、モバイル デバイスからのデバイスのヘルスに関するサマリー情報にアクセスできます。この方法で入手できる情報は、[デバイスの健全性の概要（Device Health Summary）] ウィジェットで入手可能な情報と同じで、ヘルスとパフォーマンスのモニタによって生成される現在のシビラティ（重大度）が高または中程度のアクティブなアラートです。アラートは、Alert-Description、Predefined-Category、Device または Alert Technology 別にグループ化できます。ダッシュボードのデバイスの健全性の概要情報の詳細については、ダッシュボードの概要（3674 ページ）を参照してください。

CSM Mobile のプリンシパル ユーザは、Apple iPad、Apple iPhone、Google Chrome ブラウザ、Apple Safari ブラウザを使用するユーザであることが想定されています。

CSM Mobile を使用するには、有効にする必要があります。CSM Mobile の有効化または無効化については、[CSM Mobile] ページ （653 ページ）を参照してください。

（注） CSM Mobile 機能が有効になっていない場合は、デフォルトの Security Manager ログイン ページ（CiscoWorks Common Services フレームワーク ソフトウェアによって提供される）にリダイレクトされます。エラーメッセージは表示されません。

CSM Mobile のホームページには、次のアラートカテゴリがあります。

- Device Not Reachable
- Interface Down
- Overall Device Health Alerts
- メモリ使用率が高い（High Memory Utilization）
- Firewall—High CPU Utilization
- IPS—High Inspection Load
- IPS—High Missed Packets
- IPS—Bypass Mode
- Other Alerts

CSM Mobile のナビゲーションおよびその他のタスクは、いくつかのシンプルな画面とアイコンを使用して実行できます。

- [ログイン（Login）]：「Cisco Security Manager Mobile - バージョン 4.5.0」と書かれた画面に、ユーザー名とパスワードのフィールドと、ログイン用のボタンがあります。
- [ログアウト（Logout）]：CSM Mobile ホームページ上にある、青色の背景の白い [X] アイコン。このアイコンは左上隅にあります。
- [更新（Refresh）]：CSM Mobile ホームページ上にある、青色の背景の白い円形の矢印アイコン。このアイコンは右上隅にあります。
- [アラートの詳細（Alert Detail）]：CSM Mobile ホームページのアラートタイプごとに、アラートカウントの右側にある灰色の矢印アイコン。
- CSM モバイルの [戻る（Back）] ボタン：各アラートの詳細ページにある、青い五角形の背景に白い角形矢印[アラートの詳細ページでのみ使用可能]。CSM Mobile の [戻る（Back）] ボタンは、ブラウザの戻るボタンと機能的に同等です。

（注） CSM Mobile の表示は自動的に更新されません。最新のアラートデータを取得するには、更新ボタンを手動でクリックする必要があります。

インベントリ ステータスの表示

表示することを許可されているすべてのデバイスのデバイス プロパティの概要を表示できます。概要には、デバイス アクセス情報およびすべてのデバイス設定が含まれています。概要では、どの設定がローカルであり、どの設定が共有ポリシーを使用しているかが示され、また有効なポリシー オブジェクト オーバーライドも示されます。デバイスへの設定展開のステータスを表示することもできます。

レポートは表形式であり、フィルタリング、ソート、並べ替え、およびカラムの削除によって情報を整理できます。また、表の内容を Security Manager サーバ上の Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートすることもできます。

ステップ 1 デバイスビューで、[ツール（Tools）]>[インベントリステータス（Inventory Status）] を選択して、[Inventory Status] ウィンドウ （3695 ページ）を開きます。

ステップ 2 上部の表で、詳細なステータスを表示するデバイスを選択します。詳細情報が下部のペインのタブに表示されます。情報はフォルダに整理されています。[+] または [-] アイコンをクリックして、フォルダを開いたり閉じたりします。または、フォルダ名をダブルクリックします。次のタブを使用できます。

- [インベントリ（Inventory）]：選択したデバイスのデバイスプロパティ、展開方法、デバイス グループ メンバーシップ、およびモジュールの親デバイスに関する概要情報が表示されます。
- [Policy]：選択したデバイスに対して設定できるポリシーの現在のステータスが表示されます。ポリシーのステータスは、未割り当て（未定義）、ローカル ポリシー、または共有ポリシーです。
- [Policy Object Overrides]：選択したデバイスに対して定義されたオーバーライドを持つポリシー オブジェクトが表示されます。
- [ステータス（Status）]：選択したデバイスの Security Manager 展開ジョブからのステータスメッセージを、イベントタイプごとに整理して一覧表示します。

イベントは、管理対象のデバイスまたはコンポーネントが異常な状態になったことを示す通知です。1 つのモニタ対象デバイスまたはサービス モジュールで複数のイベントが同時に発生する場合もあります。

Security Manager では、各タイプの最近のイベントだけが表示されます。過去のステータス情報を表示するには、Deployment Manager を使用します。

ステップ 3 [閉じる（Close）] をクリックして、[インベントリステータス（Inventory Status）] ウィンドウを閉じます。

[Inventory Status] ウィンドウ

[Inventory Status] ウィンドウを使用して、表示することを許可されているデバイスのデバイス プロパティおよびステータスを表示します。このウィンドウでは、個々のデバイスごとにデバイス プロパティを開かなくても済むように、デバイス情報の概要が示されます。

デバイス プロパティ情報に加え、各デバイスのポリシーの設定方法（ローカル、共有、または未設定）および各デバイスのオーバーライドを持つポリシー オブジェクトに関する概要情報を表示できます。デバイスへの設定展開のステータスを表示することもできます。

[Inventory Status] ウィンドウには、2 つのペインがあります。上部のペインを使用して、すべてのデバイスの一覧を表示したり、属性をデバイスでソートしたり、特定のデバイスを除外したりします。下部のペインを使用して、上部のペインで選択したデバイスのデバイス プロパティの詳細を表示します。

ナビゲーション パス

[ツール（Tools）] > [インベントリステータス（Inventory Status）] を選択します。

関連項目

- インベントリ ステータスの表示 （3694 ページ）
- テーブルのフィルタリング （64 ページ）
- テーブル カラムおよびカラム見出しの機能 （66 ページ）

フィールド リファレンス

表 992 : [Inventory Status] ウィンドウ

要素	説明
すべてのデバイスのデバイス概要情報（上部のペイン）	
[Export] ボタン	インベントリを Comma-Separated Values（CSV; カンマ区切り値）ファイルとしてエクスポートするには、このボタンをクリックします。ファイル名を指定して、Security Manager サーバ上のフォルダを選択するように求められます。エクスポート ファイルは参照または分析に使用できます。
表示名	Security Manager に表示されるデバイス名。
展開	デバイスの設定展開のステータス。
OS タイプ	デバイスで実行されているオペレーティング システムのファミリ。IOS、IPS、ASA、FWSM、PIX など。
実行中 OS のバージョン	デバイスで実行されているオペレーティング システムのバージョン。

要素	説明
ターゲットOSバージョン	設定を適用するターゲットOSバージョン。設定は、このバージョンでサポートされているコマンドに基づきます。
Host Name.Domain Name	デバイスの DNS ホスト名および DNS ドメイン名。
IP Address	デバイスの管理 IP アドレス。
デバイスタイプ	デバイスのタイプ。
選択したデバイスの詳細（下部のペイン） 詳細情報が下部のペインのタブに表示されます。情報はフォルダに整理されています。[+]または[-]アイコンをクリックして、フォルダを開いたり閉じたりします。または、フォルダ名をダブルクリックします。	
インベントリ	選択したデバイスのデバイスプロパティ、展開方法、デバイスグループメンバーシップ、およびモジュールの親デバイスに関する概要情報が表示されます。
ポリシー	選択したデバイスに対して設定できるポリシーの現在のステータスが表示されます。ポリシーのステータスは、未割り当て（未定義）、ローカル ポリシー、または共有ポリシーです。
Policy Object Overrides	選択したデバイスに対して定義されたオーバーライドを持つポリシー オブジェクトが表示されます。ポリシー オブジェクト オーバーライドの詳細については、ポリシー オブジェクト オーバーライドのページ （154 ページ）を参照してください。
ステータス	選択したデバイスに対する展開ステータスメッセージが表示されます。 イベントはイベントタイプ別に整理されています。イベントの詳細には、タイムスタンプ、説明、および推奨するアクションが含まれています。タイムスタンプは、デバイスの最新のポーリング時刻ではなく、デバイスのステータスが最後に変更された時刻です。 ステータスメッセージの最も高い重大度レベルも表示されます。
ナビゲーション ボタン	インベントリ リスト内を移動するには、ナビゲーション ボタンをクリックします。ボタンの意味は、左から右の順で、リスト内の最初のデバイスに移動、前のデバイスに移動、次のデバイスに移動、最後のデバイスに移動です。中央のフィールドに、現在選択されているデバイスが行番号で示されます（たとえば、5/10は、リスト内の10個のデバイスのうちの5番めを意味します）。

デバイス マネージャの起動

デバイスマネージャを起動して、Security Manager からデバイスの設定とステータスを表示できます。ASA、ASA-SM、PIX、FWSM、IPS、およびIOS の各デバイスのデバイス マネージャを起動できます。

各デバイス マネージャには、デバイス上で実行されているサービスに関する情報およびシステムの全体的なヘルスのスナップショットを提供する複数のモニタリングおよび診断機能が含まれています。これらのデバイス マネージャを使用して、既存のデバイス設定の表示および現在のステータスのモニタを行うことができますが、デバイスに設定変更を適用することはできません。

（注） IPS 仮想センサーに対してデバイス マネージャを起動することはできません。

（注） Cisco Security Manager 4.16 では、JRE 1.7 ビルド 161 のアップグレードにより、一部の古いアプレットへのサポートが廃止されました。したがって、Cisco Security Manager 4.16 以降、PIX 6.3、IDS/IPS バージョン 5.x ～ 7.x、および FWSM 2.x を直接起動することはできません。

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

デバイスマネージャを起動するには、デバイスビューでデバイスを選択し、右クリックして [デバイスマネージャ（Device Manager）] を選択します。**[起動（Launch）] > [デバイスマネージャ（Device Manager）]** を選択してデバイスマネージャを起動することもできます。（これらのコマンドは、ASA CX デバイスを選択するとディセーブルになり、**Prime Security Manager** のコマンドがイネーブルになります。Cisco Prime Security Manager は、ASA CX デバイスの設定と管理に使用されます。詳細については、Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ） を参照してください）。

Security Manager からデバイス マネージャを起動すると、デバイス マネージャ実行ファイルがクライアント システムにダウンロードされます。ネットワーク デバイスにデバイス マネージャをインストールする必要はありません。デバイス マネージャを最初に起動するときは、ソフトウェアをワークステーションにダウンロードするのに時間がかかります（経過表示バーが表示されます）（問題が発生した場合は、デバイス マネージャのトラブルシューティング （3699 ページ）のヒントを確認してください）。

Security Manager によって、ネットワーク デバイス上で実行されているオペレーティング システムに基づいて、最適なデバイス マネージャ バージョンが選択されます。選択されたデバイ

スとのその後の通信は、ユーザにはまったく意識されません。接続はSecurity Managerサーバーを介して行われます。つまり、Security Manager サーバーはプロキシサーバーとして機能します。Security Manager からデバイス マネージャを起動することによって、クライアント システムとモニタ対象デバイスとの間で HTTPS 接続を開く必要がなくなります。

ヒント　デバイスマネージャ セッションを開始すると、Security Managerによって、デバイスで実行されているオペレーティング システム ソフトウェア バージョンに適切なマネージャのバージョンが開かれます（詳細については、「ASA and ASDM Compatibility Per Model」を参照してください）。ただし、使用している Security Manager バージョンのリリースよりもあとに新しいデバイスマネージャ バージョンがリリースされた場合、Security Managerによって、利用できる最新のデバイス マネージャ バージョンが開かれない場合があります。デバイスマネージャを起動するときは、そのバージョンを確認してください（たとえば、デバイスマネージャ ウィンドウで **[ヘルプ（Help）] > [バージョン情報（About）]** を選択します）。必要な機能を備えた、さらに新しいデバイスマネージャが使用可能な場合、その新機能を使用するには、Security Manager 以外でそのデバイスマネージャをインストールして使用する必要があります。

デバイスで実行されている外部デバイスマネージャを使用してデバイス設定を直接変更する場合、これらの変更は Security Manager によってアウトオブバンドと見なされ、次に Security Manager から設定を展開するときに上書きされる場合があることに注意してください。アウトオブバンド変更の詳細と、アウトオブバンド変更の識別および再作成については、次の項を参照してください。

- アウトオブバンド変更の処理方法について （494 ページ）
- アウトオブバンド変更の検出および分析 （537 ページ）

Security Manager では、デバイスごとにデバイスマネージャのインスタンスが 1 つだけ起動されます。Security Managerを終了するか、アイドルセッションのタイムアウト時間が過ぎると、デバイスマネージャは終了します。複数のデバイス マネージャ ウィンドウを（異なるデバイスに接続して）同時に開くことができます。

次の表に、Security Manager から起動できるデバイス マネージャの概要を示します。

表 *993 : Security Manager* で使用可能なデバイス マネージャ

Device Manager	説明
IDM	IPS Device Manager（IDM）を使用すると、Security Manager インベントリの一部である IPS センサーおよびモジュールをモニタできます。 このデバイスマネージャの使用方法の詳細については、IDM のマニュアルを参照してください。

Device Manager	説明
PDM	PIX Device Manager（PDM）を使用すると、PIX 6.x デバイスおよび初期の FWSM（つまり、シングル コンテキスト モードまたはマルチ コンテキスト モードの FWSM リリース 1.1、2.2、および 2.3）をモニタできます。 このデバイスマネージャの使用方法の詳細については、PDM のマニュアルを参照してください。
ASDM	Adaptive Security Device Manager（ASDM）を使用すると、ASA、ASA-SM、PIX 7.x 以降、および FWSM 3.x 以降のデバイスをモニターできます。 このデバイスマネージャの使用方法の詳細については、ASDM のマニュアルを参照してください。
SDM	Security Device Manager（SDM）を使用すると、Cisco IOS ベースのリソースをモニタできます。SDM では、シスコ デバイスまたは Cisco コマンドライン インターフェイス（CLI）に関するこれまでの経験は必要ありません。Cisco SDM では、広範囲の Cisco IOS ソフトウェア リリースがサポートされます。 このデバイスマネージャの使用方法の詳細については、SDM のマニュアルを参照してください。

次の項では、デバイスマネージャのトラブルシューティングおよび使用について詳細に説明します。

- デバイス マネージャのトラブルシューティング （3699 ページ）
- デバイス マネージャからのアクセス ルールの検索 （3701 ページ）
- ASDM からアクセス ルールへのナビゲート （3702 ページ）
- SDM からアクセス ルールへのナビゲート （3704 ページ）

デバイス マネージャのトラブルシューティング

設定をデバイスに正常に展開できた場合、Security Manager でデバイスとのデバイス マネージャ セッションを開くことができます（デバイス マネージャの起動 （3697 ページ）を参照）。

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

ただし、接続の確立または開かれたセッションの使用に問題がある場合は、次のトラブルシューティングに関するヒントを考慮してください。ヒントは、基本的なヒントと複数のデバイスマネージャの使用に関するヒントに分かれています。

デバイス マネージャのトラブルシューティングに関する基本的なヒント

- 一般に、Security Managerインベントリでデバイス用に設定されているクレデンシャルが、デバイスマネージャの起動に使用されます。ただし、SDMのいくつかのバージョンでは、デバイスマネージャの起動時にユーザ名およびパスワードを入力する必要があります。デバイスのクレデンシャルがないか、または有効ではないというエラーが表示された場合は、デバイスにログインできるユーザ名およびパスワードを使用して、[Device Properties Credentials] ページを更新します。デバイスビューで、デバイスを右クリックして、[デバイスプロパティ（Device Properties）] を選択します。詳細については、デバイス プロパティの表示または変更 （136 ページ）および[Device Credentials] ページ （143 ページ）を参照してください。

- CiscoWorks Common Services ロールのいずれかに関連付けられているすべてのユーザには、Security Manager からデバイス マネージャを起動する権限があります。ただし、Help Desk ロールと、定義済みのすべての Cisco Secure ACS ロールを除きます。適切な権限があることを確認してください。

- Security Manager とデバイス間のセキュアな通信を実現するには、SSL/HTTPS がターゲット デバイスでイネーブルである必要があります。デバイスで SSL がイネーブルになっていない場合、エラー メッセージが表示されます。詳細については、デバイスの通信要件について （71 ページ）を参照してください。

- デバイスマネージャサービス（**xdm-launcher.exe**）を起動するには、Security Manager システムおよびワークステーションで、Cisco Security Agent またはその他のアンチウイルスやネットワーク ファイアウォール ソフトウェアの変更が必要となる場合があります。

- ターゲット デバイスへのアクセスおよび通信に関して Security Manager が正しく設定されていることを確認します。特に、アイデンティティ、オペレーティング システム、クレデンシャルなどのデバイスのプロパティを確認します。目的のデバイスを選択し、右クリックして [デバイスプロパティ（Device Properties）] を選択します。[General] および [Credentials] ページで設定を確認します。[クレデンシャル（Credentials）] タブを選択して [接続のテスト（Test Connectivity）] をクリックすることにより、Security Manager がデバイスに接続できるかどうかをテストできます（デバイス接続のテスト （573 ページ）を参照）。

（注） [デバイスプロパティ（Device Properties）] の [全般（General）] タブの [オペレーティングシステム（Operating System）] フレームにある [実行中のOSのバージョン（Running OS Version）] フィールドが空白のときにパケットトレーサーを実行すると、CSMは、[実行中のOSのバージョン（Running OS Version）] フィールドを使用してデバイスのライブネスを正しくチェックできず、ASA デバイスが停止していると見なします。

- デバイス マネージャは、トランスペアレント モード（レイヤ 2 ファイアウォール）またはルーテッド モード（レイヤ 3 ファイアウォール）で実行されており、1 つのセキュリ

ティ コンテキストまたは複数のセキュリティ コンテキストをサポートしている FWSM および ASA に対して起動できます。複数のセキュリティ コンテキストを実行している FWSM および ASA デバイスの場合、セキュリティ コンテキストごとに一意の管理 IP アドレスを定義する必要があります。

- プラットフォームがデバイス マネージャの起動に対してサポートされていないというメッセージが表示されたが、このガイドの情報ではプラットフォームはサポートされている場合、デバイスで実行されているオペレーティング システムのバージョンと、使用している Security Manager ソフトウェアのバージョンを考慮してください。最近のオペレーティング システムを使用しているが、比較的古いバージョンの Security Manager を使用している場合は、Security Manager をアップグレード（またはサービス パックを適用）するか、Cisco Technical Support に問い合わせるか、あるいは最新のデバイス マネージャをネットワーク デバイスにインストールして Security Manager 以外で使用する必要があることがあります。Security Manager 以外でデバイス マネージャを使用する前に、デバイス マネージャの起動（3697 ページ）でアウトオブバンド変更に関する情報を確認してください。

複数のデバイス マネージャ セッションのトラブルシューティングに関するヒント

- 複数のデバイス マネージャを起動すると、Security Manager サーバとクライアントの両方のパフォーマンスに影響することがあります。クライアントでは、メモリ要件およびパフォーマンスへの影響は、起動されるデバイス マネージャの数に比例します。サーバでは、デバイス マネージャの起動またはデバイスからの最新情報の取得に対する大量の要求が、パフォーマンスに悪影響を及ぼす可能性があります。
- すべてのクライアントから 1 つのデバイスに対して確立できる永続的な HTTPS 接続の最大数は、デバイスのタイプおよびモデルによって異なります。この制限を超えようとすると、エラー メッセージが表示されます。

たとえば、1 つの PIX 6.x では、複数のクライアントがそれぞれ 1 つのブラウザ セッションを開くことができ、最大 16 個の同時 PDM セッションがサポートされます。FWSM（1.1、2.2、または 2.3）では、モジュール全体で最大 32 個の PDM セッションと、コンテキストごとに最大 5 つの同時 HTTPS 接続が許可されます。

個別の制限については、該当するデバイスの資料を参照してください。

デバイス マネージャからのアクセス ルールの検索

アクセス ルールのセットが、各デバイス インターフェイスに関連付けられています。これらのルールは、順序が付けられたリストまたは表の形式で提供されます。このリストは Access-Control List（ACL; アクセス コントロール リスト）と呼ばれ、リスト内の各ルールは Access-Control Entry（ACE; アクセス コントロール エントリ）と呼ばれます。パケットを転送するかドロップするかを決定するときに、デバイスは、リストされている順序で各アクセス ルールに照らしてパケットをテストします。ルールが一致した場合、デバイスは指定されたアクションを実行します。その後の処理のためにデバイスへのパケットを許可するか、エントリを拒否します。パケットがどのルールとも一致しない場合、パケットは拒否されます。

ファイアウォールまたはルータでのアクティビティは、syslog メッセージを使用してモニタできます。デバイスでロギングがイネーブルの場合、syslog メッセージを生成するように設定されたアクセス ルールが一致すると（たとえば、拒否されている IP アドレスから接続が試行された場合）、ログ エントリが生成されます。

（注） デバイスでログ エントリを生成するには、デバイスでロギングをイネーブルにする必要があります（ASA/PIX デバイスの場合は [Logging Setup] ページ （2656 ページ）、IOS デバイスの場合はロギング ポリシー（Cisco IOS ルータにおけるロギング （3269 ページ）を参照））。また、一致した場合にログ メッセージを生成するように個々のアクセス ルールを設定する必要があります（ [Advanced]/[Edit Options] ダイアログボックス （936 ページ）を参照）。

Security Manager から起動するデバイスマネージャで syslog メッセージをモニタリングできます。一部のデバイスマネージャでは、特定のメッセージを生成した Security Manager のアクセスルールをモニタリングウィンドウから検索できます。syslog エントリをトリガーしたアクセス ルールは、複数の一致があった場合でも、最初に一致したものが Security Manager で強調表示されます。

このアクセスルール検索は、IOS を実行しているすべての管理対象ルータの場合は SDM で使用可能であり、管理対象 PIX およびバージョン 8.0(3) 以降の ASA デバイス（ASA-SM を含む）、および FWSM バージョン 3.1 以降を実行しているデバイスの場合は ASDM で使用可能です。

次の項では、デバイス マネージャから Security Manager のアクセス ルールを検索する方法について説明します。

- ASDM からアクセス ルールへのナビゲート （3702 ページ）
- SDM からアクセス ルールへのナビゲート （3704 ページ）

ASDM からアクセス ルールへのナビゲート

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

Security Manager から起動された ASDM デバイス マネージャでは、[Real-time Log Viewer] ウィンドウおよび [Log Buffer] ウィンドウでシステム ログ メッセージをモニタできます。いずれかのウィンドウで表示された syslog メッセージを選択し、メッセージをトリガーした Security Manager のアクセス コントロール ルールにナビゲートして、必要に応じてルールを更新できます。

[Real-time Log Viewer] は、syslog メッセージが記録されたときにそれを表示できる独立したウィンドウです。独立した [Log Buffer] ウィンドウでは、syslog バッファ内に存在するメッセージを表示できます。

次の syslog メッセージ ID に関連付けられたアクセス ルールを検索できます。

- 106023：アクセス ルールによって IP パケットが拒否されたときに生成されます。このメッセージは、ルールに対してロギングがイネーブルになっていない場合にも表示されます。
- 106100：一致したアクセス ルールに対してロギングがイネーブルの場合（[Advanced]/[Edit Options] ダイアログボックス （936 ページ）を参照）、このメッセージは、設定されているパラメータに応じて、トラフィック フローに関する情報を提供します。このメッセージは、拒否されたパケットだけを記録するメッセージ 106023 よりも多くの情報を提供します。

次の手順では、ASDM の [Real-time Log Viewer] または [ログバッファ（Log Buffer）] ウィンドウから Security Manager のアクセスルールを検索する方法について説明します。

関連項目

- デバイス マネージャからのアクセス ルールの検索 （3701 ページ）
- SDM からアクセス ルールへのナビゲート （3704 ページ）

ステップ 1 Security Manager デバイス インベントリで、PIX、ASA、ASA-SM または FWSM を選択します。

ステップ 2 [起動（Launch）] > [デバイスマネージャ（Device Manager）] を選択して ASDM を開始します。デバイス マネージャの起動の詳細については、 デバイス マネージャの起動 （3697 ページ）を参照してください。

（注） バージョン 4.21 以降、Cisco Security Manager は、ASA 9.14(1) 以前のデバイスの ASDM の相互起動をサポートしています。ただし、この機能を利用するには、CLI `http server basic-auth-client Java` が ASA で手動で設定されていることを確認してください。

ステップ 3 [ASDM] ウィンドウで、[モニタリング（Monitoring）] ボタンをクリックして [モニタリング（Monitoring）] パネルを表示します。左側のペインで [ロギング（Logging）] をクリックして、ログ表示オプションにアクセスします。

ステップ 4 [Real-time Log Viewer] または [ログバッファ（Log Buffer）] を選択します。

ステップ 5 [表示（View）] ボタンをクリックして、選択したログ表示ウィンドウを開きます。

（注） デバイスでロギングがイネーブルになっていない場合、[View] ボタンは表示されません。

ウィンドウに表示される各 syslog メッセージには、メッセージ ID 番号、メッセージが生成された日時、ロギング レベル、およびパケットが送受信されたネットワーク アドレスまたはホスト アドレスが含まれています。

ステップ 6 特定の syslog メッセージをトリガーしたアクセス ルールを表示するには、メッセージを選択し、ASDM ツールバーの [ルールの表示（Show Rule）] ボタンをクリックします（または、メッセージを右クリックして、ポップアップメニューから [CSMのルールに移動（Go to Rule in CSM）] を選択します）。

Security Manager クライアント ウィンドウがアクティブになり、[Access Rules] ページが表示されます。このページでは、ルール テーブル内のルールが強調表示されます。syslog エントリが現在の Security Manager アクティビティで参照されていないアクセス ルールによってトリガーされた場合、エラー メッセージが表示されます。

SDM からアクセス ルールへのナビゲート

Security Manager から起動された SDM デバイス マネージャでは、[Logging] ウィンドウの [Syslog] タブで、セキュリティ レベルで分類されたイベントのログを表示できます。syslog メッセージを選択し、メッセージをトリガーした Security Manager のアクセス コントロール ルールにナビゲートして、必要に応じてルールを更新できます。

SDM の [Monitor] > [Logging] オプションには、4 つのログ タブがあります。そのうち [Syslog] だけに、Security Manager アクセス ルール検索オプションがあります。ルータには、重大度レベルで分類されたイベントのログが含まれています。ログ メッセージが syslog サーバに転送されている場合でも、[Syslog] タブにはルータ ログが表示されます。

Cisco IOS デバイスでは、syslog メッセージは **log** または **log-input** キーワードを使用して設定されたアクセスルール用に生成されます。**log** キーワードでは、パケットがルールと一致したときにメッセージが生成されます。**log-input** キーワードでは、パケットの送信元および宛先 IP アドレスとポートに加えて、入力インターフェイスおよび送信元 MAC アドレスを含むメッセージが生成されます。同一のパケットが一致すると、メッセージは、直近の 5 分間に許可または拒否されたパケット数によって、5 分間隔で更新されます。

次の手順では、SDM の [ロギング（Logging）] パネルの [Syslog] タブから Security Manager のアクセスルールを検索する方法について説明します。

関連項目

- デバイス マネージャからのアクセス ルールの検索 （3701 ページ）
- ASDM からアクセス ルールへのナビゲート （3702 ページ）

ステップ 1 Security Manager デバイス インベントリで、IOS ルータを選択します。

ステップ 2 [起動（Launch）] > [デバイスマネージャ（Device Manager）] を選択して ASDM を開始します。デバイス マネージャの起動の詳細については、デバイス マネージャの起動 （3697 ページ）を参照してください。

ステップ 3 [SDM] ウィンドウで、[モニタリング（Monitoring）] ボタンをクリックして [モニタリング（Monitoring）] パネルを表示します。左側のペインで [ロギング（Logging）] をクリックして、ログ表示オプションにアクセスします。

[Syslog] タブが表示された [Logging] ペインが表示されます。

ステップ 4 特定の syslog メッセージをトリガーしたアクセスルールを表示するには、メッセージを選択し、ログメッセージの表の上にある [CSMのルールに移動（Go to Rule in CSM）] ボタンをクリックします。

Security Manager クライアント ウィンドウがアクティブになり、[Access Rules] ページが表示されます。このページでは、ルール テーブル内のルールが強調表示されます。syslog エントリが現在の Security Manager

アクティビティで参照されていないアクセスルールによってトリガーされた場合、エラーメッセージが表示されます。

Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動

ASA CX は、高度なコンテキスト認識型セキュリティを実現する適応型セキュリティアプライアンス モジュールであり、ASA プラットフォームを拡張して、アプリケーションの可視性と制御（「誰が、何を、どこで、いつ、どのように」についての詳細）を提供します。ASA FirePOWER モジュールは、次世代 IPS（NGIPS）、Application Visibility and Control（AVC）、URL フィルタリング、および高度なマルウェア防御（AMP）などの次世代ファイアウォールサービスを提供します。

ASA CX デバイスは Cisco Prime Security Manager（PRSM）アプリケーションによって管理され、ASA FirePOWER モジュールは FireSIGHT Management Center アプリケーションによって管理されます。Cisco Security Manager で直接管理することはできません。とはいえ、Security Manager が拡張され、ASA デバイスでこれらのモジュールの存在を検出できるようになりました。Configuration Manager アプリケーションから PRSM と FireSIGHT Management Center を「クロス起動」したり、Security Manager と PRSM の間でポリシーオブジェクトデータを共有したりすることができます。

（注） PRSM と FireSIGHT Management Center はブラウザベースのアプリケーションです。つまり、ブラウザウィンドウ内で起動および動作します。そのため、Configuration Manager クライアントから PRSM または FireSIGHT Management Center をクロス起動すると、ホストシステムのデフォルトブラウザが開き、管理アプリケーションが開始されます。ただし、一部のブラウザは PRSM または FireSIGHT Management Center で認定されていないため、クロス起動の前に Security Manager クライアントのホストシステムでデフォルトのブラウザを変更しなければならない場合があります。詳細については、PRSM または FireSIGHT Management Center インストールガイドの「ブラウザ要件」を参照してください。

はじめる前に

PRSM または FireSIGHT Management Center を相互起動するには、Security Manager がモジュールの存在を認識している必要があります。そのような認識は、新しい ASA デバイス、または既存の ASA に追加されたモジュールのいずれかを検出することによって達成されます。このプロセスについては、ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）で概説されています。

また、「シングルサインオン」（SSO）を有効にして設定すると、Security Manager ユーザーがアプリケーションに別個にログインすることなく、PRSM または FireSIGHT Management Center に直接アクセスできるようになります。これを可能にするには、両方のアプリケーションで適切なユーザーログイン情報を定義する必要があります（PRSM または FireSIGHT Management

Center の相互起動に SSO は必要ないことに留意してください）。詳細については、Security Manager の [シングルサインオンの設定（Single Sign-on Configuration）] ページ （735 ページ）と、『*User Guide for ASA CX and Cisco Prime Security Manager*』（『Cisco ASA CX Context-Aware Security End-User Guides』）の「Configuring Single Sign-On for Cisco Security Manager」を参照してください。

関連項目

- [シングルサインオンの設定（Single Sign-on Configuration）] ページ （735 ページ）
- ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）
- PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有 （3708 ページ）

ASA CX デバイスまたは FirePOWER モジュールをモニタリングおよび管理するには、PRSM または FireSIGHT Management Center をクロス起動します。

ステップ 1 Configuration Manager のデバイスビューで、デバイスセレクタツリーまたはコンテンツ領域のデバイスのテーブルで、以前に検出された ASA CX デバイスまたは ASA with FirePOWER モジュールを選択します。

繰り返しになりますが、Security Manager での ASA CX デバイスまたは FirePOWER モジュールの検出については、 ASA CX モジュールおよび FirePOWER モジュールの検出 （3707 ページ）で説明しています。

ステップ 2 選択したデバイスを右クリックし、ポップアップメニューから [Prime Security Manager] または [FireSIGHT Management Center] を選択します。または、Configuration Manager の [起動（Launch）] メニューからも [Prime Security Manager] や [FireSIGHT Management Center] を選択できます（これらのコマンドは、ASA CX、または FirePOWER モジュールを備えた ASA を選択した場合にのみ使用できます）。

ブラウザベースの PRSM または FireSIGHT Management Center のウィンドウが表示され、選択したデバイスのデバイス画面が表示されます。

（注） Security Manager が PRSM を起動するために使用する URL には、CX モジュールの管理 IP アドレス（デバイス検出中に取得）が組み込まれており、文字列 /admin/mgmt?rtp が含まれています。相互起動中に、このタイプの要求は、適切な PRSM 中央サーバーが存在する場合、そのサーバーにリダイレクトされます。それ以外の場合は、PRSM の「オンボックス」バージョンが起動されます（オンボックスバージョンの PRSM を自分で直接起動するには、ブラウザのアドレスフィールドに **https://**<*management_IP_address*> と入力する必要があります。ここで <*management_IP_address*> は、目的の CX モジュールの管理アドレスです）。

PRSM の使用に関する情報は、cisco.com の『Cisco ASA CX Context-Aware Security End-User Guides』ページにあり、FireSIGHT Management Center の使用に関する情報は、cisco.com の『Cisco FireSIGHT Management Center』ページにあります。

ASA CX モジュールおよび FirePOWER モジュールの検出

Security Manager と PRSM の間でポリシーオブジェクトデータを共有し、Configuration Manager から PRSM または FireSIGHT Management Center を相互起動するには、Security Manager がモジュールを確実に認識している必要があります。

デバイス インベントリへのデバイスの追加 （94 ページ）で説明しているように、新規デバイスウィザードで関連するオプションを選択して新しいASAデバイスを検出すると、CXモジュールまたは FirePOWER モジュールの検出が自動的に行われます。

すでにインベントリにある ASA デバイスに CX モジュールまたは FirePOWER モジュールを追加すると、次のように、ホスト ASA の既存のポリシーに影響を与えずに新しいモジュールを検出できます。

1. Configuration Manager のデバイスセレクタツリーで 1 つ以上の ASA デバイスを選択します。

   一度に複数のモジュールを検出できます。ASA ではないデバイス、または CX または FirePOWER モジュールを含まない ASA であるデバイスが選択されている場合、それらは無視されます。

2. 選択したデバイスを右クリックし、ポップアップメニューから [ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）] を選択します。

   [検出タスクの作成（Create Discovery Task）] ダイアログボックスまたは [バルク再検出（Bulk Rediscovery）] ダイアログボックスが表示され、[ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）] オプションが選択されています。他の検出オプションは使用できません。

   このダイアログボックスの使用方法の詳細は、[Create Discovery Task] および [Bulk Rediscovery] ダイアログボックス （231 ページ）を参照してください。

3. [検出タスクの作成（Create Discovery Task）] ダイアログボックスで [OK] をクリックするか、[バルク再検出（Bulk Rediscovery）] ダイアログボックスで [完了（Finish）] をクリックしてダイアログボックスを閉じ、モジュールの検出を開始します。

   検出によって既存のポリシーが置き換えられるという警告が表示される場合があります。[はい（Yes）] をクリックして警告を閉じ、続行できます。

   [検出ステータス（Discovery Status）] ダイアログボックスが自動的に開き、検出の進行状況が表示されます。このプロセスの詳細については、ポリシー検出タスクのステータスの表示 （237 ページ）を参照してください。

CX モジュールまたは FirePOWER モジュールが ASA で検出されると、モジュール自体の管理 IP アドレスが取得され、[デバイスのプロパティ（Device Properties）] ウィンドウの [ASA-CX/FirePOWERモジュール（ASA-CX/FirePOWER Module）] セクションが更新されます。[デバイスのプロパティ（Device Properties）]：[全般（General）] ページ （137 ページ）を参照してください。管理 IP アドレスは、PRSM または FireSIGHT Management Center を相互起動するために使用されます。（Cisco Prime Cisco Security Manager または FireSIGHT Management Center の起動 （3705 ページ）で説明しているように、Cisco Prime Security Manager（PRSM）は

ASA CX デバイスの設定と管理に使用されるアプリケーションであり、FireSIGHT Management Center は ASA FirePOWER モジュールの設定と管理に使用されるアプリケーションです）。

（注） Security Manager が PRSM を起動するために使用する URL には、CX モジュールの管理 IP アドレス（デバイス検出中に取得）が組み込まれており、文字列 /admin/mgmt?rtp が含まれています。相互起動中に、このタイプの要求は、適切な PRSM 中央サーバーが存在する場合、そのサーバーにリダイレクトされます。それ以外の場合は、PRSM の「オンボックス」バージョンが起動されます。（オンボックスバージョンの PRSM を自分で直接起動するには、ブラウザのアドレスフィールドに **https://**<*management_IP_address*> と入力する必要があります。ここで <*management_IP_address*> は、目的の CX モジュールの管理アドレスです。）

検出プロセスが完了すると、CX モジュールがインストールされているすべての ASA は、さまざまな Security Manager 画面に、次の PRSM アイコンを提示したり含めたりして示されます。

。たとえば、デバイスセレクタでは、次の ASA CX アイコンが使用されます。

注意 また、選択したデバイスの右クリックメニューから[デバイス上のポリシーを検出（Discover Policies on Device(s)）] を選択するか、[ポリシー（Policy）] メニューから [デバイス上のポリシーを検出（Discover Policies on Device）] を選択して、既存の ASA における CX モジュールまたは FirePOWER モジュールの存在を検出することもできます。選択したデバイスの数と選択したコマンドに応じて、[検出タスクの作成（Create Discovery Task）] ダイアログボックスまたは [バルク再検出タスク（Bulk Rediscovery Task）] ダイアログボックスが開き、すべての検出、再検出オプションが使用可能になります。つまり、選択したデバイスですでに確立されている共有ポリシーを上書する可能性があります。既存のポリシーを確実に再検出する場合を除き、[ASA-CX/FirePOWERモジュールの検出（Detect ASA-CX/FirePOWER Module）] を除くすべてのオプションの選択を解除してください。詳細については、Security Manager にすでに存在するデバイス上のポリシーの検出 （227 ページ）を参照してください。

PRSM とのデバイスインベントリおよびポリシーオブジェクトの共有

Cisco Security Manager の定義に従い Cisco Prime Security Manager（PRSM）にインポートするために、現在のデバイスインベントリおよびポリシーオブジェクトのセットをエクスポートできます。

デバイス インベントリのエクスポート

Cisco Security Manager デバイスインベントリを PRSM と共有するには、デバイス インベントリのエクスポート（605 ページ）の説明に従い、インベントリをカンマ区切り値（CSV）ファイルとしてエクスポートします。エクスポートファイルのフォーマットタイプには、必ず「Cisco Security Manager」を指定してください。

ネットワーク/ホストおよびサービスポリシーオブジェクトのエクスポート

PRSM にインポートするために、Cisco Security Manager ポリシーオブジェクト、具体的にはネットワーク/ホストオブジェクト、またはサービスオブジェクトをエクスポートするには、Cisco Security Manager サーバーホストで Perl スクリプトを実行して CSV ファイルを作成する必要があります（PRSM はポートリストオブジェクトをサポートしていません）。

Perl スクリプトは Cisco Security Manager サーバーのインストールに含まれており、その使用方法については、ポリシー オブジェクトのインポートおよびエクスポート （318 ページ）を参照してください。基本的な手順は次のとおりです。

1. Cisco Security Manager サーバーを実行しているコンピュータにログインし、Cmd ウィンドウを開き、Perl スクリプトの場所に移動してから、コマンドプロンプトで Perl スクリプトコマンドを実行します。

ネットワーク/ホストオブジェクトをエクスポートするために使用されるコマンドの例を次に示します。perl PolicyObjectImportExport.pl -u *user* -p *password* -o export -t network -f C:\CSM_Net_objects.csv -e true

1. CSV ファイルを PRSM クライアントシステムにコピーします。

このファイルは、必要に応じて編集できます。

1. PRSM を起動し、CSV ファイルをインポートします。このプロセスの詳細については、PRSM ユーザーガイドの「Managing Policy Objects」の章にある「Importing Objects」セクションを参照してください。

Packet Tracer を使用した ASA または PIX の設定の分析

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き PIX の機能をサポートしていますが、バグ修正や拡張機能はサポートしていません。

パケットトレーサは、ルーテッドモードで稼働していない、バージョン 7.2.1 以降を実行している ASA および PIX セキュリティアプライアンス用のポリシーデバッグツールです。

パケットトレーサは、アプライアンスで現在実行されているアクティブなポリシーを検査します。実際のトラフィックを生成しなくても、2 つのアドレス間でトラフィックがセキュリティアプライアンスをどのように通過するか（ドロップまたは許可）を分析できます。結果が予期

しないものである場合は、問題がある場所を判別し、Security Manager で対応するポリシーを更新して解決できます。

パケットトレーサは、セキュリティアプライアンスのアクティブな設定による、シミュレートされたパケットの処理方法を段階的に分析します。また、ルートルックアップ、アクセスリスト、NAT 変換、VPN など、アクティブなファイアウォールモジュールを通過するパケットのフローをトレースします。アクティブなモジュールのセットは、設定されているパケットのタイプとアクティブな設定に基づいて変わります。たとえば、VPN ポリシーが設定されていない場合、VPN モジュールは評価されません。

ネットワークトラフィックを生成する代わりに、シミュレートされたパケットの通過を検査し、syslog メッセージを有効にして、生成される syslog メッセージを手動で確認できます。Packet Tracer では、パケットでアクティブな設定によって実施されたアクションが詳細に示されます。コンフィギュレーション コマンドによってパケットがドロップされた場合、「Drop-reason: (telnet-not-permitted) Telnet not permitted on least secure interface」などの理由が示されます。

セキュリティアプライアンスを通過するシミュレートされたパケットの寿命をトレースして、パケットの動作が予期したとおりかどうかを確認できます。Packet Tracer の用途は、次のとおりです。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用されるすべてのルール（ルールを定義する CLI を含む）を表示します。
- データ パス内でのパケット変化を時系列で表示する。
- データ パスでパケットをトレースします。
- 明示的なアクセスルールによってパケットがブロックまたは許可されている場合、ルールを編集できるように、ショートカットを使用してポリシーに移動できます。

ヒント：

- Packet Tracer は ASDM アプリケーションおよび ASA コマンドラインでも使用でき、Security Manager のバージョンは ASDM のバージョンと同じです。ASDM および CLI からパケットトレーサを使用して設定を分析する例については、「PIX/ASA 7.2(1) 以降：インターフェイス内通信」を参照してください。
- デバイスに対して Packet Tracer を使用する前に、デバイスをインベントリに追加したあとで少なくとも 1 回はポリシー変更を送信する必要があります。
- Packet Tracer では、デバイスで実行されているアクティブな設定だけが分析されます。このため、提案された設定がデバイスに展開されて実行される前に、Packet Tracer を使用してテストすることはできません。設定変更が保留中のデバイスで Packet Tracer を使用しないでください。変更を展開してから Packet Tracer を使用して、Packet Tracer の結果が有効になるようにしてください。

Packet Tracer を使用するには、次の手順を実行します。

ステップ 1 （デバイスビュー）ASA または PIX 7.2.1 以降のデバイスを右クリックし、ショートカットメニューで [パケットトレーサ（Packet Tracer）] を選択して [パケットトレーサ（Packet Tracer）] ウィンドウを開きます。

ステップ 2 [インターフェイス（Interfaces）] リストから、テストするインターフェイスを選択します。このリストには、デバイスで定義されているすべてのインターフェイスが含まれています。

ステップ 3 次のフィールドを設定して、トレースするパケットをモデル化します。

- [パケットタイプ（Packet Type）]：トレースするパケット（TCP、UDP、ICMP、IP、または ESP）を選択します。

（注） 4.16 以降、Cisco Security Manager は ASA 9.9.1 デバイスからの ESP パケットのトレースをサポートしています。

- [送信元、宛先IPアドレス（Source, Destination IP Address）]：次のアドレスタイプから選択し、通信（送信元から宛先へ）の両端のホスト IP アドレスを入力します。
  - ホストの IP アドレスIPv4 または IPv6 アドレスを使用できます。IPv6 を使用したパケットトレーサは、8.4(2) より前の ASA ソフトウェアバージョンを実行しているデバイスではサポートされていません。
  - ユーザ（送信元のみ）。例：DOMAIN\Administrator。ユーザーにマップされた IP アドレスがトレースに使用されます。このタイプのアドレスを使用するには、アイデンティティ オプションを設定することにより、アイデンティティ対応のファイアウォールを有効にする必要があります。
  - ホストの FQDN、つまり完全修飾ドメイン名。例：host.example.com。このタイプのアドレスを使用するには、DNS を設定する必要があります。
  - セキュリティ名（ASA 9.x 以降のみ）。
  - セキュリティタグ（ASA 9.x 以降のみ）。
- [送信元、宛先ポート（TCPおよびUDPのみ）（Source, Destination Port (TCP and UDP only)）]：トラフィックタイプを表すポート番号を入力（または選択）します。選択リストでは、指定アプリケーションの標準ポート番号と一致する名前が使用されています。たとえば、**http** を選択することと、**80** を入力することは同じです。
- [タイプ、コード、 ID（ICMPのみ）（Type, Code, ID (ICMP only)）]：ICMP パケットをモデル化する場合、次のフィールドすべてに値を入力する必要があります。
  - [タイプ（Type）]：ICMP パケットタイプを選択するか、同等の番号を入力します。リストには、主要な ICMP タイプがすべて含まれています。タイプと関連するコードの一覧については、http://www.ietf.org/rfc/rfc1700.txtで RFC 1700 を参照し、「ICMP Type Numbers」を検索してください。
  - [コード（Code）]：ゼロ以外のコードを持つパケットタイプをモデル化している場合以外は、**0** を入力します。これらは、宛先到達不能（タイプ 3、コード 0 ～ 12）、リダイレクト（タイプ 5、コード 0 ～ 3）、時間超過（タイプ 11、コード 0 ～ 1）、およびパラメータの問題（タイプ 12、コード 0 ～ 2）です。コードの説明については、RFC 1700 を参照してください。追加のコードが他の RFC に導入されている場合がある点に注意してください。

- [ID]：限定された数のメッセージタイプに対してのみフィールドが使用される場合でも、ID の値を入力する必要があります。ID は、要求および応答バージョン（エコー、エコー要求など）を含む ICMP タイプに対して、応答を要求に一致させるために使用されます。値は 1 ～ 255 です。

- [プロトコル（IPのみ）Protocol (IP only)]：次のレベルのプロトコルを示す番号を入力します。プロトコルコードの一覧については、 http://www.ietf.org/rfc/rfc1700.txt で RFC 1700 を参照し、「Protocol Numbers」を検索してください。この項の執筆時点では、番号 1 ～ 54 および 61 ～ 100 が、許容範囲である 0 ～ 255 から実際のプロトコルに割り当てられている値を表しています。

- VLAN ID（1 ～ 4096）：フローの VLAN ID を入力します。VLAN ID は、パケットが属する VLAN を決定します。Cisco Security Manager により、ID 範囲が 1 ～ 4096 であることが検証されます。

（注） バージョン 4.13 以降、Cisco Security Manager パケットトレーサは透過的な FW デバイスをサポートします。VLAN ID は、デバイス 9.7.1 以降でパケットトレーサをサポートするためにバージョン 4.13 で導入された新しいパラメータです。

- 宛先 MAC：フローの宛先 MAC アドレスを入力します。Cisco Security Manager により、MAC アドレスのフォーマットが検証されます。

- [SPIの入力（ESPのみ）（Enter the SPI (ESP only)）]：セキュリティ パラメータ インデックスを入力します。これは、受信側のセキュリティ アソシエーションを識別するために（宛先 IP アドレスとともに）使用される任意の値です。0 ～ 4294967295 の数値を入力します。

ステップ 4 [パケットのトレース（Tracing Packet）] ドロップダウンリストから、該当するオプションを選択します。

- bypass-checks：シミュレートされたパケットのセキュリティチェックをすべてバイパスする
- decrypted：シミュレートされたパケットを復号された IPSec/SSL VPN として扱う
- persist：長期トレースを有効にし、クラスタでトレースを追跡する
- transmit：シミュレートされたパケットをデバイスから送信できるようにする

ステップ 5 トレースの経過を表示するには、[アニメーションの表示（Show animation）] を選択します。選択しない場合、トレースが完了するまでウィンドウは結果によって更新されません。

ステップ 6 [Start] をクリックして、パケットをトレースします。

ポリシーが検査され、結果がウィンドウの下部にグラフィカル情報と詳細情報という 2 つの形式で表示されます。グラフィカルビューには、パケットのパスで評価されたフェーズの概要が示されます。チェックマークはパケットがフェーズに合格したことを示し、赤い X はパケットがそのポイントでドロップされたことを示します。

詳細情報では、フェーズに対応するフォルダで結果が整理されます。[Action] カラムにフェーズの結果が示されます（合格した場合はチェックマーク、ドロップされた場合は赤い X）。フォルダを開くには、その見出しをクリックします。詳細情報には、評価された特定のコンフィギュレーション コマンドおよび**show** コマンドから取得されたデータを含めることができます。Result という名前の最後のフォルダでは、トレース結果の概要が示されます。

ヒント：

- 明示的なアクセス ルールによってパケットが許可または拒否される場合、そのルールにジャンプできます。Access-List フォルダを選択して開き、セクションの一番上にある [アクセスルールの表示（Show access rule）] リンクをクリックします。Access Rule ポリシーが表示され、そのルールが強調表示されます。必要に応じてルールを編集できます。暗黙的な廃棄ルールによってパケットがドロップされる場合、ルールがポリシー テーブルに存在しないため、[Show access rule] リンクは使用できません。
- 分析中にネットワーク障害によってデバイスがシャットダウンされるかデバイスに到達できない場合、「Device Connectivity is Failed」というエラーメッセージが表示されます。
- 新しいトレースを開始すると、表示されていた情報は自動的にクリアされます。[クリア（Clear）] をクリックしてもクリアできます。

ping、トレースルート、または NS ルックアップツールを使用した接続問題の分析

ping またはトレース ルートのツールを使用して、ネットワークの設定および接続の調査およびトラブルシューティングを行うことができます。通常は、Security Manager 内から特定の起動ポイントとパラメータを指定して、デバイスのこれらのコマンドを実行します。これにより、Security Manager で対応するコマンドが生成されます。一方、NS ルックアップは通常、Security Manager クライアントから実行します。

（注） バージョン 4.13 以降、Cisco Security Manager のトレースルートは IPv6 アドレスをサポートします。ASA バージョン 9.7.1 以降、IPv6 アドレスのトレースルートがサポートされています。

表 *994 : Ping*、トレースルート、および *NS* ルックアップ トラブルシューティング コマンドのプロファイル

Tool	Profile
Ping	ping を使用すると、特定のホストが IP ネットワーク上で到達可能かどうかをテストし、ローカルホストから宛先のコンピュータに送信されたパケットのラウンドトリップ時間を測定します。これには、ICMP メッセージを使用するローカルホスト独自のインターフェイスの測定も含まれる場合があります。 このツールの使用方法の詳細については、ping を使用した設定の分析 （3714 ページ）を参照してください。

Tool	Profile
トレース ルート	トレース ルートを使用すると、IP ネットワーク上でパケットが通過するルートが表示されます。システムは、行われたホップ数と通過した各デバイスのアドレスを返します。 このツールの使用方法の詳細については、TraceRoute を使用した設定の分析（3716 ページ）を参照してください。
NS ルックアップ	NS ルックアップ（ネームスペース ルックアップ）を使用すると、デバイスから NS ルックアップ コマンドを発行するため、問い合わせされたデバイスが使用する DNS サーバの内容をテストできます。 このツールの使用方法の詳細については、NS ルックアップを使用した設定の分析 （3718 ページ）を参照してください。

適用性

ping ツールは、ASA（7.0 ～ 8.3）、PIX（6.3(1-5) ～ 8.0(2-4)）、FWSM（2.2(1) ～ 4.1(1)）、およびすべての IOS のデバイスで適用可能です。IPS には適用できません。

トレース ルート ツールは、ASA（7.2(1) 以降）、PIX（6.3(1-5) ～ 8.0(2-4)）、およびすべての IOS のデバイスで適用可能です。これは FWSM にも IPS にも適用できません。

NS ルックアップツールは、Cisco Security Manager によって管理されるどのデバイスでもサポートされず、Windows API を使用して Cisco Security Manager クライアントから実行します。

ping を使用した設定の分析

ping ツールは、デフォルトで ICMP エコー要求およびエコー応答メッセージを使用して、リモート システムへの到達可能性をテストします。また、ping の実行に TCP を使用するように選択できます。一番簡単な形式で、ping は単純に IP パケットが宛先 IP アドレスに送信されて戻ってくることを確認します。ping が IP アドレスに送信されると、応答が返されます。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。Security Manager 内から、ping コマンドの発行元のネットワーク デバイスと、エコー要求のターゲットの両方を指定できます。このツールは、一般に 2 つの情報を返します。送信元が宛先に到達可能かどうか（推測によるこの逆への到達可能性も）と Round-Trip Time（RTT; ラウンドトリップ時間、ミリ秒単位）です。

ping 診断ツールは、次のようにさまざまな方法で使用できます。

- **セキュリティアプライアンスに対する ping の実行**：他のセキュリティアプライアンス上のインターフェイスに ping を実行して、インターフェイスが起動していて応答することを検証します。
- **2 つのインターフェイス間のループバックテスト**：同じセキュリティアプライアンス上の一方のインターフェイスから相手側のインターフェイスに ping を、外部ループバックテストとして起動して、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証します。

- **セキュリティアプライアンスを介した ping の実行**：ping ツールから発信した ping パケットは、デバイスとの中間にあるセキュリティアプライアンスをパススルーする場合があります。エコーパケットが返されるときも、そのインターフェイスのうち2つをパススルーします。これを使用して、中間にある装置のインターフェイス、動作、応答時間についての基本的なテストを実行できます。
- **中間の通信をテストするための ping の実行**：正しく機能していてエコー要求を返すことがわかっているネットワークデバイスに対して、セキュリティ アプライアンス インターフェイスから ping を開始します。エコーを受信した場合、物理的な接続と任意の中間デバイスの正常な動作を確認します。

ヒント　Event Manager 内から、イベントを右クリックし、ping ツールを開いて関連デバイスに ping を実行します。

ステップ 1　デバイスビューで、[ツール（Tools）] > [Ping、トレースルートおよびNSルックアップ...（Ping, TraceRoute and NS Lookup . . .）] を選択します。**...**.

[Ping, TraceRoute and NS Lookup] ダイアログが表示されます。

ステップ 2　デバイスセレクタから、**Ping** コマンドの発行元にするデバイスを選択します。

選択したデバイスがダイアログボックスの右上に表示されます。

（注）　ping に TCP を使用するには、[Packet Type] で [TCP] を選択します（デフォルトのパケット タイプは ICMP です）。

ステップ 3　[Hostname/IPv4address] に ping の送信先にするホスト ネットワーク/ホスト ポリシー オブジェクトの IP アドレスを入力します。

または、[選択（Select）] をクリックして、ping の送信先にするホストネットワーク/ホストポリシーオブジェクトを定義するホストネットワーク/ホストオブジェクトを選択します。

ステップ 4　タイムアウト値を入力します（任意）。

ステップ 5　[Ping] をクリックします。

ウィンドウ下部の領域に結果が表示されます。

ping の実行結果の例：

例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping の実行結果が失敗の場合の例：

例：

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
```

```
?????
Success rate is 0 percent (0/5)
```

[出力をクリア（Clear Output）] をクリックすると、ping の結果領域から以前の応答を削除できます。

ping コマンドの詳細については、Cisco.com の「Troubleshooting TCP/IP」を参照してください。

TraceRoute を使用した設定の分析

Traceroute ツールを使用して、パケットが宛先に到着するまでのルートを判断できます。このツールは、送信される各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。

Traceroute は、ネットワーク全体の TCP/IP 接続に関して役立つ情報を返します。次の表に、Traceroute ユーティリティによって返されるコードとその考えられる原因を示します。

表 *995 : Traceroute* の出力記号

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。
!A	ICMP が管理者によって禁止されています。
?	原因不明の ICMP エラーが発生しました。

ステップ 1 デバイスビューで、[ツール（Tools）] > [Ping、トレースルートおよびNSルックアップ...（Ping, TraceRoute and NS Lookup . . .）] を選択します。. . .

[Ping, TraceRoute and NS Lookup] ダイアログが表示されます。

ヒント Event Manager 内から、イベントを右クリックし、[TraceRoute] ページを開いて関連デバイスのルートをトレースします。

ステップ 2 [ルートのトレース（Trace Route）] タブを選択します。

[Trace Route] ページが表示されます。

ステップ 3 デバイス セレクタから、ルートのトレース元にするホストを選択します。

ステップ 4 [IPv4アドレス/ホスト名（IPv4 Address/Hostname）] を入力して、ルートのトレース先にするホストのアドレスまたは名前を指定します。

または、[選択（Select）] をクリックして、IP アドレスを定義するホストネットワーク/ホストオブジェクトを選択します。

（注） バージョン 4.13 以降、Cisco Security Manager のトレースルートは IPv6 アドレスをサポートします。バージョン 4.12 まで、syslog サーバーは IPv4 アドレスを持つデバイスで構成されていました。デバイスバージョン 9.7.1 以降、IPv6 アドレスのトレースルートがサポートされています。syslog サーバーは、IPv6 アドレスを持つデバイスで IPv6 syslog アドレスを使用して設定できます。

ステップ 5 必要に応じて、次のフィールドの値を指定します。

表 996 : Traceroute フィールド

フィールド	説明
[タイムアウト（Timeout）] :（任意）	接続がタイムアウトになるまでの応答の待機時間（秒単位）。デフォルトは 3 秒です。
[ポート（Port）]（任意）	UDP プローブ メッセージで使用される宛先ポート。デフォルトは 33434 です。
[ホップごとのプローブ数（Probes per hop）]（任意）	TTL の各レベルで送信するプローブの数。デフォルトは 3 です。
[TTL最小値（TTL Min）]（任意）	最初のプローブの TTL の最小値（デフォルトは 1 です）。
[TTL最大値（TTL Max）]（任意）	最初のプローブの TTL の最大値（デフォルトは 30 です）。

ステップ 6 必要に応じて、[送信元インターフェイスまたはIPアドレスの指定（Specify Source Interface or IP Address）] を選択してから次のいずれかを実行します。

- ドロップダウンリストから送信元の [インターフェイス（Interface）] を選択します。

（注） [IPアドレス/ホスト名（IP Address/ Hostname）] フィールドに IPv6 アドレスが指定されている場合、送信元の [インターフェイス（Interface）] フィールドは適用されません。

- [IPアドレス（IP Address）] を入力します。

ステップ 7 必要に応じて、[逆解決（Reverse Resolve）] を選択して、アドレスとホスト名の表示を入れ替えます。

ステップ 8 必要に応じて、[ICMP] を選択して、IP ではなくプロトコルを使用します。

ステップ 9 [トレース（Trace）] をクリックします。

tracerouteは、パケットが宛先に到達するか、またはTTLの最大値に達すると終了します。行われたホップおよび各ホップに対応するデバイスアドレスが表示されます。

NS ルックアップを使用した設定の分析

NS ルックアップ ツールを使用して、ホスト名を使用している場合はリモート ホスト アドレスを検索し、アドレスを使用している場合はホスト名を検索します。

ping ツールおよび Traceroute ツールとは異なり、NS ルックアップは、Security Manager クライアント上で実行されます。

ステップ 1 デバイスビューで、[ツール（Tools）] > [Ping、トレースルートおよびNSルックアップ...（Ping, TraceRoute and NS Lookup . . .）] を選択します。. . .

[Ping, TraceRoute and NS Lookup] ダイアログが表示されます。

ステップ 2 [NSルックアップ（NS Lookup）] タブを選択します。

ステップ 3 [IPv4Address/Hostname] にアドレスまたはホスト名を入力します。

または、[選択（Select）] をクリックして、IP アドレスを定義するホストネットワーク/ホストオブジェクトを選択します。

ステップ 4 必要に応じて、検索に特定の DNS サーバーを使用するには、DNS サーバーのサーバー名またはアドレスを入力します。

ステップ 5 [検索（Lookup）] をクリックします。

システムでは、検索に使用する DNS サーバだけでなく、特定のアドレス/ホスト名のペアも表示されます。

Packet Capture Wizard の使用

Packet Capture Wizard を使用して、エラーのトラブルシューティングを行うために、キャプチャを設定、実行、表示、および保存できます。事前設定されたアクセス リストを使用するか、または 1 つ以上のインターフェイス上の送信元および宛先のアドレス/ポートなどのパケット パラメータの一致基準を使用して、キャプチャを実行できます。このウィザードは、入出力インターフェイスのそれぞれでキャプチャを 1 回実行します。キャプチャを Cisco Security Manager クライアント コンピュータに保存して、パケット アナライザによるキャプチャの検査が可能です。

Packet Capture Wizard は、ASA クラスタでのパケットキャプチャもサポートしています。ASA クラスタの制御ユニットで Packet Capture Wizard を実行すると、選択したデバイスのみまたはクラスタ内のすべてのデバイスのデータをキャプチャするオプションが提供されます。クラスタのキャプチャを実行したら、クラスタのサマリー情報を表示したり、クラスタ内の特定デバイスのキャプチャバッファを表示またはダウンロードすることができます。

（注） ディレクタが変更されている場合は、Packet Capture Wizard を実行する前に Security Manager でディレクタを更新する必要があります。それを行わないと、メンバーのキャプチャにエラーが含まれます。[デバイスのプロパティ（Device Properties）]>[クラスタ情報（Cluster Information）]ページの [デバイスから取得（Retrieve From Device）] ボタンを使用すると、クラスタのディレクタを更新できます。詳細については、[グループ情報（Group Information）] ページ （149 ページ）を参照してください。

事前設定されたアクセス リストを使用するか、または 1 つ以上のインターフェイス上の送信元および宛先のアドレス/ポートなどのパケット パラメータの一致基準を使用して、キャプチャを実行できます。

次の点に注意してください。

- Packet Capture Wizard は、ファイアウォール デバイス（PIX、ASA、または FWSM）だけで使用できます。
- パケットの一致基準に基づいたパケット キャプチャは、ASA バージョン 7.2(3) 以降を実行するデバイスだけでサポートされます。他のデバイスについては、パケット キャプチャをアクセス リストに基づいて実行できるだけです。

Packet Capture Wizard を使用するには、次の手順に従います。

ステップ 1 次のいずれかの方法を使用して、Packet Capture Wizard を起動します。

- [ツール（Tools）] > [Packet Capture Wizard] を選択します。
- （デバイスビュー）ASA、PIX、または FWSM のデバイスを右クリックし、ショートカットメニューで [パケットキャプチャ（Packet Capture）] を選択します。ステップ 3 （3719 ページ）に進みます。
- （イベントビューア）ASA、PIX、または FWSM のデバイスのイベントを右クリックし、ショートカットメニューで [パケットキャプチャ（Packet Capture）] を選択します。ステップ 3 （3719 ページ）に進みます。

ステップ 2 [ツール（Tools）] メニューから Packet Capture Wizard を起動した場合は、パケットをキャプチャするデバイスを選択します。[Security Devices] リストには、パケット キャプチャが実行可能なデバイスだけが含まれています。

ステップ 3 ASA クラスタのディレクタユニットであるデバイスを選択した場合は、選択したデバイスについてのみキャプチャを実行するかクラスタ全体についてキャプチャを実行するかを指定し、[次へ（Next）] をクリックします。

ステップ 4 ドロップダウン リストから入力インターフェイスを選択します。

（注） 同じウィザードでは、同じインターフェイスを入力と出力の両方として選択できません。

ステップ 5 インターフェイスによって送信されたクラスタ コントロール プレーン パケットをキャプチャするには、[クラスタインターフェイスで制御パケットをキャプチャする（Capture control packets on cluster interface）] チェックボックスをオンにします。

（注） このオプションのフィールドは、クラスタ コントロール プレーン パケットのみをキャプチャするために、ASA 9.12.1 以降のデバイス用に Cisco Security Manager 4.19 で導入されました。この情報は、特にマルチコンテキストモードでクラスタでの問題をトラブルシューティングするときに役立ちます。

ステップ 6 [Packet Match Criteria] 領域で、次のいずれかの操作を実行します。

- パケットの照合に使用するアクセスリストを指定するには、[アクセスリスト（Access-List）] オプションボタンを選択して、ドロップダウンリストからアクセスリストを選択します。
- パケットパラメータを指定するには、[パケットパラメータ（Packet Parameters）] オプションボタンを選択して、次のフィールドを入力します。
  - [Source Host / Network] フィールドおよび [Destination Host / Network] フィールドに、それぞれ送信元および宛先を指定します。次のいずれかを使用して、送信元または宛先を指定できます。
  - [送信元ホスト/ネットワークオブジェクト（Source Host/ Network object）]。オブジェクトの名前を入力するか、または [選択（Select）] をクリックしてリストから名前を選択します。選択リストから、新しいネットワーク/ホスト オブジェクトを作成することもできます。

（注） Cisco Security Manager 4.18 以降、パケットパラメータは All-Address（any）、All-IPv4-Address（any4）、および All-IPv6-Address（any6）でサポートされます。

- ホスト IP アドレス（10.10.10.100 など）。
- ネットワーク アドレスとサブネット マスク。形式は 10.10.10.0/24 または 10.10.10.0/255.255.255.0。
- キャプチャするプロトコル タイプをドロップダウン リストから選択します。指定できるキャプチャのプロトコル タイプは、ah、eigrp、esp、gre、icmp、icmp6、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、snp、tcp、または udp です。

プロトコルが ICMP の場合は、ドロップダウン リストから ICMP タイプを選択します。指定できるタイプは、ALL、alternate-address、conversion-error、echo、echo-reply、information-reply、information-request、mask-reply、mask-request、mobile-redirect、parameter-problem、redirect、router-advertisement、router-solicitation、source-quench、time-exceeded、timestamp-reply、timestamp-request、traceroute、または unreachable です。

プロトコルが TCP または UDP の場合は、送信元および宛先のポート サービスを指定します。指定できるオプションは次のとおりです。

- すべてのサービスを含めるには、[All Services] を選択します。
- 特定のサービスを指定するには、ドロップダウン リストから適切な演算子（=、!=、>、<、または range）を選択してから、aol、bgp、chargen、cifs、citrix-ica、ctiqbe、daytime、discard、domain、echo、exec、finger、ftp、ftp-data、gopher、h323、hostname、http、https、ident、imap4、irc、kerberos、klogin、kshell、ldap、ldaps、login、lotusnotes、lpd、netbios-ssn、nfs、nntp、pcanywhere-data、pim-auto-rp、pop2、pop3、pptp、rsh、rtsp、sip、smtp、sqlnet、ssh、sunrpc、tacacs、talk、telnet、uucp、whois、または www のいずれかを選択します。>、<、および range の演算子は、選択したサービスに割り当てられたポート番号に基づいて機能します。

range 演算子を使用する場合は、別のドロップダウン リストがイネーブルになります。2 つのドロップダウン リストを使用して、指定する範囲の開始サービスと終了サービスを選択します。対応するポート番号が小さい方のサービスを最初のドロップダウン リストに選択し、対応するポート番号の大きい方のサービスを 2 番めのドロップダウン リストに選択する必要があります。

ステップ 7 [次へ（Next）] をクリックして、[出力インターフェイスの選択（Select egress interface）] ステップに進みます。

ステップ 8 ドロップダウン リストから出力インターフェイスを選択します。

（注） 同じウィザードでは、同じインターフェイスを入力と出力の両方として選択できません。

ステップ 9 インターフェイスによって送信されたクラスタ コントロール プレーン パケットをキャプチャするには、[クラスタインターフェイスで制御パケットをキャプチャする（Capture control packets on cluster interface）] チェックボックスをオンにします。

（注） このオプションのフィールドは、クラスタ コントロール プレーン パケットのみをキャプチャするために、ASA 9.12.1 以降のデバイス用に Cisco Security Manager 4.19 で導入されました。この情報は、特にマルチコンテキストモードでクラスタでの問題をトラブルシューティングするときに役立ちます。

ステップ 10 [Packet Match Criteria] 領域で、次のいずれかの操作を実行します。

（注） 入力インターフェイスに選択した [Packet Match Criteria] オプション（アクセス リストまたはパケット パラメータ）は、出力インターフェイスにも使用されます。また、入力インターフェイスでの照合にパケット パラメータを使用した場合は、使用したプロトコル定義が出力インターフェイスにも使用されます。

- アクセス リストを使用してパケットを照合している場合は、ドロップダウン リストからアクセス リストを選択します。
- パケット パラメータを使用してパケットを照合している場合、入力に使用されるパラメータは、出力にも使用されます。

ステップ 11 [次へ（Next）] をクリックして、[バッファパラメータの設定（Set buffer parameters）] ステップに進みます。

ステップ 12 次のフィールドを設定して、バッファ パラメータを指定します。

[Buffer Parameters] 領域で、バッファ サイズとパケット サイズを指定します。バッファ サイズは、キャプチャがパケットを保存するために使用可能なメモリの最大容量です。パケット サイズは、キャプチャが保持できる最長のパケットです。できる限り多くの情報をキャプチャするため、最長パケット サイズを使用することを推奨します。

- [10 秒ごとにキャプチャバッファを読み取る（Read capture buffer every 10 seconds）]：このオプションを選択にすると、10 秒ごとにキャプチャデータを自動的に取得します。このオプションを選択する場合は、循環バッファを使用する必要があります。
- [循環バッファを使用（Use a circular buffer）]：このオプションを選択すると、バッファが一杯になった後もパケットのキャプチャを継続します。この設定を選択すると、すべてのバッファ ストレージが使用されている場合、キャプチャは最も古いパケットへの上書きを始めます。

- [バッファサイズ（Buffer Size）]：キャプチャがパケットを保存するために使用可能なバイト数（1534 ～ 33554432）を入力します。
- [最大パケットサイズ（Maximum Packet Size）]：キャプチャが単一のパケットを保存するために使用可能なバイト数（14 ～ 1522）を入力します。最大値の 1522 を使用すると、可能な限り多くの情報をキャプチャします。

ステップ 13 [次へ（Next）] をクリックして [サマリー（Summary）] ステップに進みます。入力したトラフィックセレクタとバッファパラメータが表示されます。

ステップ 14 [次へ（Next）] をクリックして、[実行、表示、保存（Run, View & Save）] ステップに進みます。

ステップ 15 [Run, View & Save] ステップからは、次の操作を実行できます。

- パケットのキャプチャを開始するには、[キャプチャを開始（Start Capture）] をクリックします。
- パケットのキャプチャを停止するには、[キャプチャを停止（Stop Capture）] をクリックします。
- キャプチャされたパケットの次のセットを取得するには、次のいずれかを実行します。
  - 個別のデバイスの場合は、[キャプチャパケットの表示（Display Capture Packets）] をクリックして、キャプチャされたパケットの次のセットをデバイスから取得し、バッファステータスバーを更新します。このボタンは、[Set buffer parameters] ステップで [Read capture buffer every 10 seconds] オプションが選択されなかった場合だけイネーブルになります。
  - クラスタの場合は、[クラスタキャプチャサマリーの取得（Get Cluster Capture Summary）] をクリックして、キャプチャされたパケットの次のセットをクラスタ内のデバイスから取得し、バッファステータスバーを更新します。このボタンは、[Set buffer parameters] ステップで [Read capture buffer every 10 seconds] オプションが選択されなかった場合だけイネーブルになります。
- ASA クラスタのキャプチャを実行する場合、クラスタ内のデバイスのキャプチャバッファを操作するために次のオプションを使用できます。
  - クラスタ内のデバイスからキャプチャされたパケットを表示するには、[キャプチャバッファの取得（Get Capture Buffer）] の下にある [デバイス名（Device Name）] リストでデバイスを選択し、[キャプチャバッファの取得（Get Capture Buffer）] をクリックします。

選択したデバイスのキャプチャ情報が表示されます。このデータに対して実行できるアクションについては、このリストの他のオプションを参照してください。

- クラスタ内の特定デバイスまたはすべてのデバイスに関するキャプチャの内容を削除し、バッファに別のパケットをキャプチャするスペースを確保するには、[キャプチャバッファのクリア（Clear Capture Buffer）] の下にある [デバイス名（Device Name）] フィールドでデバイスを選択するか [-- すべて --（--All--）] を選択し、[キャプチャバッファのクリア（Clear Capture Buffer）] をクリックします。

（注） デバイスバッファをクリアする前に、キャプチャを保存することを推奨します。デバイスバッファをクリアする前にキャプチャを保存しないと、キャプチャされたデータは消失します。

- 外部パケット分析ツールを使用して対応する入力キャプチャまたは出力キャプチャを表示するには、[入力キャプチャ（Ingress Capture）] ウィンドウまたは [出力キャプチャ（Egress Capture）] ウィンド

ウの上にある [Network Sniffer を起動（Launch Network Sniffer）] ボタンをクリックします。パケットアナライザがインストールされていて、*.pcap ファイル拡張子に関連付けられている必要があります。

- パケットキャプチャデータを大きなウィンドウに並べてを表示するには、[データを大きなウィンドウで表示（View Data in Larger Window）] をクリックします。
- [キャプチャを保存（Save captures）] をクリックして、[キャプチャを保存（Save Capture）] ダイアログボックスを表示します。キャプチャしたパケットに含める形式として、ASCII または PCAP を選択します。入力キャプチャまたは出力キャプチャを保存するオプションがあります。
- 現在のパケットの内容を削除して、バッファに別のパケットをキャプチャするスペースを確保するには、[デバイスバッファのクリア（Clear Device Buffer）] をクリックします。

（注） デバイスバッファをクリアする前に、キャプチャを保存することを推奨します。デバイスバッファをクリアする前にキャプチャを保存しないと、キャプチャされたデータは消失します。

- クラスタ内のデバイスに関してキャプチャされたパケットの次のセットを取得し、バッファステータスバーを更新するには、[キャプチャバッファのリフレッシュ（Refresh Capture Buffers）] をクリックして、

ステップ 16 [Finish] をクリックして、ウィザードを終了します。

IPインテリジェンス（IP Intelligence）

Cisco Security Manager によって管理されるネットワーク セキュリティ デバイスは、攻撃者または被害者のマシン、あるいはその両方の IP アドレス情報を含む大量のセキュリティログとセキュリティイベントを生成します。

IP アドレスに関する有用な詳細は、まとめて IP インテリジェンスと呼ばれ、ping、トレースルート、NS ルックアップなどのツールを使用して検出できます。ただし、これらのツールはやや初歩的なので、より高度なツールで補強することが望ましい場合がよくあります。

バージョン 4.5 以降、Security Manager は、IP アドレスに関する重要な詳細をリアルタイムで提供する、または生成されたレポートで提供する高度なツールを備えています。Security Manager では、これらの重要な詳細を次のカテゴリで提供しています。

- 逆引き DNS（FQDN）ルックアップサービス
- GeoIP ルックアップサービス
- Whois ルックアップサービス

（注） IPv6 アドレスの IP インテリジェンスはサポートされていません。

これらの IP インテリジェンスカテゴリについて、次の表で説明します。

表 *997 : IP* インテリジェンスカテゴリ

IP ルックアッププロバイダー	情報源	リアルタイムまたは手動/制限
逆引き DNS（FQDN）ルックアップサービス	DNS サーバー	リアルタイム （注） 外部 DNS 設定は設定可能な追加オプションですが、個々の状況を評価する必要があります。
GeoIP ルックアップサービス	外部のサードパーティ コマーシャル ベンダー	リアルタイム、Cisco Security Manager バージョン 4.18 まで。 GeoIP ルックアップサービスのデータベースは GeoIP2 にアップグレードされましたが、 Cisco Security Manager はまだアップグレードされていません。したがって、Cisco Security Manager の以前のバージョンの GeoIP の自動更新と、Cisco Security Manager 4.19 のデフォルトの GeoIP パッケージには、2018 年 12 月のデータベースのみが含まれます。

IP ルックアッププロバイダー	情報源	リアルタイムまたは手動/制限
Whois ルックアップサービス	サードパーティの Web サーバーである無料の whois サーバーによって提供されます。	リアルタイム 制限事項： • Whois は、クエリおよび応答プロトコルであり、登録されたユーザーやインターネットリソース（ドメイン名、IP アドレスブロック、自律システムなど）の割り当て先を保存するデータベースに照会するために幅広く使用されます。5 つの地域インターネットレジストリ（RIR）組織が IP アドレスの割り当てと登録を管理しています。 • ARIN（American Registry for Internet Numbers）、RIPE（Réseaux IP Européens Network Coordination Centre）、および APNIC（Asia-Pacific Network Information Centre）は、Security Manager が直接クエリを実行するために使用する 3 つの RIR であり、参照 URL も提供します。RIPE および APNIC では、解析エラーがある場合、直接の URL リンクのみが表示されます。 • 指定された URL をクリックすると、指定された IP アドレスの詳細が Web ブラウザに表示されます。IP アドレスが LACNIC（Latin America and Caribbean Network Information Centre）または AfriNIC（African Network Information Centre）に属している場合、Web ブラウザはそれぞれの RIR のホームページを表示します。 • 場合によっては（DNS クエリが Windows ファイアウォールによってブロックされている、または無効なプロキシが cco 設定ページで構成されているなど）、Whois が有効になっていても機能しないことがあります。そのような場合、「フェイルセーフ」メソッドとして、参照された URL のみを提供します。

IP インテリジェンスの検索を開始する前に、[Configuration Manager] > [ツール（Tools）] > [Security Manager管理（Security Manager Administration）]...> [IPインテリジェンス設定（IP Intelligence Settings）] で必要なサービスを有効にする必要があります。[IPインテリジェンス設定（IP Intelligence Settings）] ページ （696 ページ） を参照してください。

IP インテリジェンス ルックアップは、次のいずれかの方法を使用して実行できます。

- [IPインテリジェンス（IP Intelligence）] ダイアログボックスを使用します。[Configuration Manager] > [ツール（Tools）] > [IPインテリジェンス（IP Intelligence）]... に移動し、表示される [IPインテリジェンス（IP Intelligence）] ダイアログボックスの検索フィールドに有

効な IPv4 アドレスを入力します（IP アドレスを入力した後、Enter キーを押す必要があります）。

- Security Managerインターフェイスで有効なIPv4アドレスにマウスのカーソルを合わせて、「クイック起動」を使用します。これはイベントビューアなどで行うことができ、通常、IPアドレスが表示されるデータの一部であるすべてのGUIテーブルで実行できます。GUIテーブルの 1 つのセルに複数の IP アドレスが表示されている場合は、最初の IP アドレスのみが表示されます。

（注） クイック起動を使用した場合、GUI に [IPインテリジェンス（IP Intelligence）] オプションが表示されるまで、1 ～ 2 秒の遅延が発生する場合があります。

（注） [Configuration Manager] > [ツール（Tools）] > [IPインテリジェンス（IP Intelligence）] の [IPインテリジェンス（IP Intelligence）]... ダイアログボックスで [クイック起動の有効化（Enable Quick Launch）] チェックボックスをオンまたはオフにすることで、クイック起動を有効または無効にすることができます。 。

- ダッシュボードで IP インテリジェンス ウィジェットを使用します（[起動（Launch）] > [ダッシュボード（Dashboard）]... 。この方法は、前述の [IPインテリジェンス（IP Intelligence）] ダイアログボックスを使用する場合と同等です。
- Report Manager（**[起動（Launch）] > [Report Manager]...**）を使用して、次のいずれかのレポートで IP インテリジェンスを確認します。
  - [FW/サマリーボットネット（FW/Summary Botnet）]：上位の感染ホスト
  - [FW/サマリーボットネット（FW/Summary Botnet）]：上位のマルウェア サイト
  - [FW]：上位の宛先
  - [FW]：上位のソース
  - [IPS]：ターゲット分析
  - [IPS]：上位の攻撃者
  - [IPS]：上位の被害者

（注） これらのレポートにはいくつかの注意点があります。1）Whois 情報は含まれません。2）**[Configuration Manager] > [ツール（Tools）] > [Security Manager管理（Security Manager Administration）]... > [IP インテリジェンス設定（IP Intelligence Settings）]** ですべてのプロバイダーを無効にしている場合、レポートには IP インテリジェンス関連の列が表示されません。3）すべてのサービスを有効にすると、逆引き DNS（FQDN）と GeoIP の詳細のみがレポートに表示されます。4）1 つのサービスのみを有効にすると、そのサービスのみがレポートに表示されます。

（注） PDF 形式と CSV 形式の両方で生成されたレポートには、IP インテリジェンスの詳細が含まれます。

（注） これらのすべてのレポートでは、必要なサービスが有効化されている必要があります。「[IPインテリジェンス設定（IP Intelligence Settings）] ページ （696 ページ）」を参照してください。

CS-MARS と Security Manager の統合

Cisco Security Manager では、ネットワーク内のセキュリティ ポリシーおよびデバイス設定を集中管理できます。一方、Cisco Security Monitoring, Analysis and Response System（CS-MARS）は、デバイスをモニタしてイベント情報（syslog メッセージや NetFlow トラフィック レコードなど）を収集する別のアプリケーションであり、Security Manager よりも広範なネットワーク モニタリング機能を備えています。CS-MARS では、大量のネットワークおよびセキュリティ データが、使いやすい形式で集約および提供されます。CS-MARS レポートから取得された情報に基づいて、セキュリティ脅威に対抗するために Security Manager でデバイス ポリシーを編集できます。

特に、Security Manager を使用してファイアウォール アクセス ルールおよび IPS シグニチャを設定する場合、それらのポリシーに関連する情報を収集して Security Manager ユーザに対して使用可能にするように、CS-MARS を設定できます。CS-MARS サーバを Security Manager に登録することによって、ユーザは特定のアクセス ルールまたは IPS シグニチャから直接 CS-MARS レポート ウィンドウにナビゲートできます。このウィンドウには、そのルールまたはシグニチャのクエリー基準があらかじめ読み込まれています。

同様に、CS-MARS ユーザは、特定の CS-MARS イベントに関連する Security Manager ポリシーを表示できます。特定のイベントとそれをトリガーしたポリシーとの双方向マッピングと、ポリシーを即時に変更する機能を結合することによって、大規模または複雑なネットワークの設定およびトラブルシューティングに要する時間を大幅に削減できます。

この相互通信をイネーブルにするには、CS-MARS サーバを Security Manager に登録し、Security Manager サーバを CS-MARS サーバに登録する必要があります。また、特定のデバイスを各アプリケーションに登録する必要もあります。これにより、デバイスのファイアウォール アクセス ルールまたは IPS シグニチャを操作するときに、Security Manager ユーザは、そのルールまたはシグニチャに関連するリアルタイムおよび過去のイベント情報を迅速に表示できます。

次の項では、CS-MARS と Security Manager の相互通信をイネーブルにして使用する方法について説明します。

- CS-MARS と Security Manager を統合するためのチェックリスト （3728 ページ）
- Security Manager ポリシーの CS-MARS イベントの検索 （3734 ページ）
- CS-MARS イベントからの Security Manager ポリシーの検索 （3740 ページ）

CS-MARS と Security Manager を統合するためのチェックリスト

CS-MARS と Security Manager 間の相互通信（CS-MARS と Security Manager の統合 （3727 ページ）を参照）をイネーブルにするには、アプリケーションを相互に識別させ、両方のアプリケーションによって管理されるデバイスが適切に設定されるようにする必要があります。次の表に、統合の手順を示します。

相互通信について問題がある場合は、CS-MARS クエリーのトラブルシューティングに関するヒント （3732 ページ）を参照してください。

表 *998 : CS-MARS と Security Manager* の統合

タスク	説明
Security Manager および CS-MARS にデバイスを追加する	Security Manager へのデバイスの追加については、デバイス インベントリへのデバイスの追加 （94 ページ）を参照してください。CS-MARS インベントリへのデバイスの追加については、Cisco Security MARS のデバイス設定ガイドを参照してください。 デバイスに相互通信を提供するには、デバイスが両方のアプリケーションによってサポートされている必要があります。サポートされているデバイス タイプは、一般に、[Firewall] > [Access Rules] または [IPS] > [Signatures] ポリシーを提供するデバイス タイプです（PIX、ASA および FWSM アプライアンス、Cisco IOS ルータ、Cisco IPS センサーとモジュール、Cisco Catalyst スイッチなどがあります）。
必要に応じてアプリケーションごとにデバイスを設定する	Security Manager の基本的な設定要件については、デバイスの通信要件について （71 ページ）を参照してください。CS-MARS の広範な要件については、Cisco Security MARS のデバイス設定ガイドを参照してください。

タスク	説明
Security Manager を CS-MARS に登録する	Security Manager と通信するための CS-MARS の設定については、Cisco Security MARS Local Controller および Global Controller のユーザ ガイドを参照してください。 Security Manager とのリンク専用の CS-MARS ユーザ アカウントを作成する場合があります。 CS-MARS ポリシー クエリーに応答するための Security Manager サーバの設定 （3729 ページ）を参照してください。
CS-MARS コントローラを Security Manager に登録する	CS-MARS コントローラの Security Manager への登録については、Security Manager での CS-MARS サーバの登録 （3730 ページ）を参照してください。
Security Manager で CS-MARS コントローラをデバイスにリンクする	Security Manager で、デバイスの [デバイスのプロパティ（Device Properties）] ページで [CS-MARSの検出（Discover CS-MARS）] をクリックして、特定のデバイスをモニターする CS-MARS コントローラをプロアクティブに検出できます（ デバイスの CS-MARS コントローラの検出または変更 （3731 ページ）を参照）。そのようにしない場合は、ユーザがデバイスのイベントを検索しようとしたときに、適切なコントローラが自動的に検出されます（複数のコントローラがデバイスをモニタしている場合、ユーザはコントローラを選択するように求められます）。

関連項目

- アクセス ルールの CS-MARS イベントの表示 （3735 ページ）
- IPS シグニチャの CS-MARS イベントの表示 （3738 ページ）
- Security Manager ポリシーの CS-MARS イベントの検索 （3734 ページ）

CS-MARS ポリシー クエリーに応答するための Security Manager サーバの設定

CS-MARS は、ポリシー検索クエリーを実行してポリシー情報を取得できるように、Security Manager サーバへのアクセスを許可されている必要があります。

- サーバで Common Services AAA 認証を使用している場合（Cisco Secure ACS など）、CS-MARS が Security Manager サーバにクライアント アクセスできるように、管理アクセス設定を更新する必要があります。
- Security Manager で CS-MARS がクエリーの実行に使用できるユーザ アカウントを定義します。Security Manager サーバで特定の監査証跡を提供するために、別個のアカウントを作成することを推奨します。このアカウントを次の Common Services ロールの 1 つに割り当てる必要があります。
  - 承認者

- Network Operator
- ネットワーク管理者
- システム管理者（System Administrator）

Help Desk セキュリティ レベルのユーザは、CS-MARS 内のポリシー検索テーブルの表示だけを行うことができます。つまり、Security Manager をクロス起動してポリシーを変更することはできません。

（注） Security Manager サーバを CS-MARS に登録するときに、ポリシー テーブル検索のために Security Manager クレデンシャルを求める場合、認証用に Common Services で別の CS-MARS アカウントを用意する必要がなくなることがあります。

Common Services でのユーザーの追加およびロールの関連付けの詳細については、『*User Guide for CiscoWorks Common Services*』を参照してください。

関連項目

- Security Manager での CS-MARS サーバの登録 （3730 ページ）
- デバイスの CS-MARS コントローラの検出または変更 （3731 ページ）

Security Manager での CS-MARS サーバの登録

CS-MARS と Security Manager を同時に使用する場合は、 CS-MARS と Security Manager を統合するためのチェックリスト （3728 ページ）の説明に従って、CS-MARS コントローラを Security Manager に登録し、これらのアプリケーション間の相互通信をイネーブルにする必要があります。

これにより、ユーザがデバイスのイベントを検索するときに、Security Manager によって、そのデバイスのイベントを収集している CS-MARS コントローラが識別されます。複数の CS-MARS コントローラによってデバイスのイベントが収集されている場合、ユーザは使用する CS-MARS コントローラを選択できます。各デバイスの [Device Properties] ウィンドウで、使用する正しい CS-MARS コントローラを指定することもできます（詳細については、デバイスの CS-MARS コントローラの検出または変更 （3731 ページ）を参照してください）。

（注） Security Manager で明示的にサポートされている CS-MARS バージョンについては、製品の該当するバージョンの『Release Notes for Cisco Security Manager』を参照してください。明示的にはサポートされていないバージョンを使用する場合、4.3.4 または 5.3.4 よりも前の CS-MARS バージョンは使用できません。

ステップ 1 [ツール（Tools）] > [Security Manager管理（Security Manager Administration）] を選択し、コンテンツテーブルで [CS-MARS] を選択して、[CS-MARS] ページ （650 ページ）を表示します。

ステップ 2 [追加（Add）] ボタンをクリックして、CS-MARS サーバーを追加します。[New CS-MARS Device] ダイアログボックスが開きます（詳細については、[New CS-MARS Device]/[Edit CS-MARS Device] ダイアログボックス （652 ページ）を参照してください）。

ステップ 3 [New CS-MARS Device] ダイアログボックスで、サーバの IP アドレスまたは完全修飾 DNS ホスト名と、サーバにログインするためのユーザ名およびパスワードを入力します。ローカル コントローラを追加する場合、入力するユーザ名はローカル アカウントとグローバル アカウントのいずれかです。[User Type] リストからアカウントのタイプを選択します。

ヒント CS-MARS Global Controller を使用している場合は、個別の Local Controller ではなく Global Controller を追加します。Global Controller を追加することによって、各 Local Controller を追加しなくても、Security Manager でデバイスの正しい Local Controller を識別できます。Global Controller を追加する場合は、Global Controller によってモニタされる個別の Local Controller を追加しないでください。

[デバイスから取得（Retrieve From Device）] をクリックして、サーバーの認証証明書を取得します。証明書が提示されたら、[承認（Accept）] をクリックします。

完了したら、[OK] をクリックします。[New CS-MARS Device] ダイアログボックスが閉じて、サーバが CS-MARS デバイス リストに追加されます。

ステップ 4 [CS-MARSの起動タイミング（When Launching CS-MARS）] リストから、ユーザーがイベントステータスを要求したときに CS-MARS サーバーにログインするように求められるようにするか、またはユーザーが Security Manager にログインしたときに提供されたクレデンシャルを使用して Security Manager が CS-MARS に自動的にログインするかを選択します。

Security Manager クレデンシャルの使用を選択した場合は、必要なユーザ アカウントを CS-MARS で設定する必要があります。詳細については、CS-MARS のマニュアルを参照してください。

ステップ 5 [CS-MARS] ページで [保存（Save）] をクリックして変更を保存します。

デバイスの CS-MARS コントローラの検出または変更

Cisco Security Monitoring, Analysis and Response System（CS-MARS）コントローラを使用してデバイスをモニタする場合、このコントローラを Security Manager に登録することにより、個々のデバイスのファイアウォール アクセスまたは IPS シグニチャ ルールに関連する syslog およびイベントを表示できます。

ルールに関連するイベントを表示しようとすると、Security Manager によって、デバイスをモニタする CS-MARS コントローラを自動的に検出できます。複数のコントローラによってデバイスがモニタされている場合は、使用するコントローラの選択を求められます。

デバイスの CS-MARS コントローラを、そのデバイスの [Device Properties] ウィンドウでプロアクティブに選択することもできます。同様に、デバイスに割り当てられている CS-MARS コントローラを変更する必要がある場合は、[Device Properties] ウィンドウで選択内容を変更できま

す。次の手順では、デバイスの CS-MARS コントローラをそのデバイスの [Device Properties] ウィンドウで検出または変更する方法について説明します。

はじめる前に

デバイスをモニターする CS-MARS コントローラが、[CS-MARS] 管理ページ（[ツール（Tools）] > [Cisco Security Manager管理（Security Manager Administration）] > [CS-MARS]）で Cisco Security Manager に登録されている必要があります。詳細については、Security Manager での CS-MARS サーバの登録 （3730 ページ）を参照してください。

ステップ 1 デバイス ビューのデバイス セレクタで次のいずれかを実行し、[Device Properties] ダイアログボックスを開きます。

- デバイスをダブルクリックします。
- デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
- デバイスを選択して、[ツール（Tools）] > [デバイスのプロパティ（Device Properties）] の順に選択します。

ステップ 2 目次で [全般（General）] をクリックして、[全般（General）] プロパティページを開きます（[デバイスのプロパティ（Device Properties）] : [全般（General）] ページ （137 ページ）を参照）。

ステップ 3 [CS-MARSモニタリング（CS-MARS Monitoring）] グループで、[CS-MARSの検出（Discover CS-MARS）] をクリックします。Security Manager によって、デバイスをモニタしている登録済みコントローラが判別されます（存在する場合）。複数ある場合は、使用する CS-MARS コントローラを選択するように求められます。

CS-MARS クエリーのトラブルシューティングに関するヒント

CS-MARS と Security Manager を一緒に使用しているときに発生する可能性がある問題を識別して解決するには、次のトラブルシューティングに関するヒントを使用します。

- Security Manager サーバと CS-MARS 間の通信には、HTTPS が必要です。
- インターフェイス名は、Security Manager では大文字と小文字が区別されませんが、CS-MARS では区別されます。たとえば、「outside」と「Outside」は CS-MARS アプライアンスでは排他的と見なされますが、Security Manager では同一です。さらに、syslog メッセージでは、すべてのインターフェイス名に小文字が使用されます。その結果、CS-MARS で生成されたイベントから Security Manager ポリシーのクエリーを実行する場合、syslog イベントに記録されるインターフェイス名は、Security Manager のそのポリシーでのインターフェイス名と一致しない場合があります。この問題を回避するには、すべてのインターフェイス名、インターフェイス ロールの定義、CS-MARS で小文字を使用します。
- Security Manager ポリシーから CS-MARS イベントを照会するには、Security Manager クライアントが、ネットワーク アドレス変換（NAT）境界について、CS-MARS アプライアンスおよび Security Manager サーバと同じ側にある必要があります。

同様に、CS-MARS クライアントが NAT 境界について CS-MARS アプライアンスおよび Security Manager サーバと同じ側にない場合は、Security Manager ポリシーを検索できますが、読み取り専用モードになります。読み取り専用ポリシー検索テーブルからは Security Manager クライアントを起動できません。Security Manager クライアントを CS-MARS から起動して、一致したポリシーを変更する場合、クライアントは NAT 境界について CS-MARS アプライアンスおよび Security Manager サーバと同じ側にある必要があります。

- 複数の独立したセキュリティ コンテキストが存在する FWSM、PIX、および ASA デバイスの場合、CS-MARS イベントを照会するには、セキュリティ コンテキストごとに Security Manager で一意の管理 IP アドレスを定義する必要があります。また、各仮想コンテキストのホスト名およびレポート IP アドレスが、CS-MARS に追加される前に設定されている必要があります。設定されていないと、これらのコンテキストのポリシーからのイベント検索は失敗します。
- すべての IPS デバイスおよびサービス ポリシーについて、IPS ポリシーを検出しない場合、または設定済みのポリシーをデバイスから削除する場合は、デフォルトのシグニチャ ポリシーがデバイスに割り当てられます。デフォルトのシグニチャからイベント検索を実行しようとすると、「Policy not found」というエラーメッセージが表示されます。ただし、デフォルトのシグニチャを編集して保存すると、CS-MARS でイベントにナビゲートできます。
- Security Manager で定義されたアクセス ルールに対してオブジェクト グループ化またはルール最適化がイネーブルであり、デバイス上の関連付けられた access-list コマンドが最適化されたルールと一致しない場合、CS-MARS でイベントは表示されません。
- アクセス ルールに対してロギングがイネーブルになっていない場合は、警告メッセージが表示され、それらのルールのトラフィック フロー イベントだけを検索できます。
- デバイスでサポートされている場合は、Access-Control Entry（ACE; アクセス コントロール エントリ）によって生成された syslog メッセージについて CS-MARS を照会するときに、Security Manager によって ACE ハッシュコードが追加キーワードとして使用されます。大きな Access-Control List（ACL; アクセス コントロール リスト）には、このようなハッシュコードが数千含まれる場合もあります。キーワードの数か、または ACE やシグニチャの送信元、宛先、およびプロトコルの合計数がクエリー制限の 150 を超えた場合は、エラー メッセージが表示されます。エラー メッセージには、考えられる原因と推奨アクションが示されます。
- 次の状況で、ルールとレポートされるイベントとの間で同期の問題が発生する場合があります。
  - デバイスが Security Manager に追加されましたが、それに対する設定または変更がデータベースに保存されていません。これは、デバイスが CS-MARS に追加されて以降に変更されたが展開されていないアクセス ルールの場合に特に該当します。
  - Security Manager 内に対応するルールがないアクセス ルールがデバイス上に存在するか、またはその逆です。すべてのデバイスが Security Manager に追加され、Security Manager を使用してデバイス上にアクセス ルールが設定されるようにします。

- ルールが定義されていない、イベントをトリガーしている「間違った」方向のトラフィック。たとえば、インバウンド トラフィック ルールだけが定義されている高いセキュリティ レベルのインターフェイスでのアウトバウンド トラフィックがあります。

- CS-MARS からポリシー検索を実行し、Security Manager クライアントがアクティブである場合、クエリーは、開かれているアクティビティまたは設定セッション内のすべてのポリシーと、データベースに保存されているポリシー（コミットされた設定）に対して実行されます。Security Manager クライアントがアクティブではない場合は、コミットされたポリシーだけが考慮されます。

関連項目

- CS-MARS と Security Manager を統合するためのチェックリスト （3728 ページ）
- Security Manager ポリシーの CS-MARS イベントの検索 （3734 ページ）
- Security Manager での CS-MARS サーバの登録 （3730 ページ）

Security Manager ポリシーの CS-MARS イベントの検索

CS-MARS と Security Manager を統合したあと、特定のファイアウォール アクセス ルールまたは IPS シグニチャに関連する CS-MARS 内のイベントを検索できます。

CS-MARS がイベントを受信すると、イベントは解析され、「セッション化」されて、イベントバッファに書き込まれてから、データベースに書き込まれます。セッション化には2つの形式があります。セッション指向プロトコル（TCP など）では、セッションには初期ハンドシェイクから接続のティアダウンまでが含まれます。セッションレス プロトコル（UDP など）では、セッションの開始時刻と終了時刻は、制限された時間内で追跡される最初と最後のパケットに基づきます。時間外のパケットは、他のセッションの一部と見なされます。

新しく受信したデータと完全に処理されたデータには違いがあるため、リアルタイムイベントまたは過去イベントのいずれも検索できます。

- [リアルタイム（Real-time）]：イベントをキャッシュ内に最大2分間保持するためセッション化には時間がかかります。そのため、リアルタイム イベント クエリを使用して解析直後にイベントを表示し、受信した最新データへのアクセスを可能にします。

リアルタイム イベントを照会すると、クエリーは Security Manager から取得されたポリシー値に基づいて自動的に実行され、結果は CS-MARS の [Query Results] ウィンドウに表示されます。このリアルタイム イベント ビューアを使用して、未処理イベントがセッション化される前の CS-MARS へのストリーミング中に、最大 5 秒の遅延で、CS-MARS トラフィックをほぼリアルタイムでモニタできます。セッション化されたイベントストリームの表示を選択することもできます。そのためには、[クエリ結果（Query Results）] ウィンドウで [編集（Edit）] をクリックし、[リアルタイム（Realtime）] ドロップダウンメニューから [セッション化されたイベント（Sessionized events）] を選択します。セッション内のイベント数が多い場合には、遅延が長くなる可能性があります。

- [履歴（Historical）]：過去のイベントのレポートは、リアルタイムモニタリングで可能な期間よりも長期にわたる傾向を識別するのに役立ちます。過去のイベントを照会すると、CS-MARS の [Query Criteria: Result] ウィンドウが開きます。クエリをすぐに実行するか、あとで実行するために基準を「レポート」として保存できます。過去のイベントの場合、[Result Format] は [All Matching Events] オプションであり、[Filter By Time] 値は過去 10 分に設定されます。

次の項では、イベント検索についてより詳細に説明します。

- アクセス ルールの CS-MARS イベントの表示 （3735 ページ）
- IPS シグニチャの CS-MARS イベントの表示 （3738 ページ）

アクセス ルールの CS-MARS イベントの表示

Security Manager の **[ファイアウォール（Firewall）] > [アクセスルール（Access Rules）]** ポリシーから、アクセスルールを選択し、CS-MARSの関連するイベント情報を表示できます。ルールと一致するリアルタイム イベントまたは過去のイベント、トラフィック フロー、送信元アドレス、または宛先アドレスを表示できます。アクセス ルールをサポートする任意のデバイス（ASA、PIX、FWSM、ルータ、スイッチなど）のイベントを表示できます。

ファイアウォール アクセス ルールは、順序が付けられたリストまたは表の形式で提供されます。展開されると、このポリシーはAccess-Control List（ACL; アクセス コントロール リスト）となります。リスト内の各エントリは、Access-Control Entry（ACE; アクセス コントロール エントリ）と呼ばれます（詳細については、アクセス ルールについて （913 ページ）を参照してください）。

パケットを転送するかドロップするかを決定するときに、デバイスは、リストされている順序で各アクセス ルールに照らしてパケットをテストします。アクセス ルールに対してロギングをイネーブルにすると、テストの結果はルールごとのログ設定に従って記録されます。ASA などの一部のデバイスでは、ロギングを明示的に設定しない場合でも、拒否されたアクセスのログ エントリが生成されます。ロギング オプションを含むアクセス ルールの作成の詳細については、アクセス ルールの設定 （920 ページ）を参照してください。

次のタイプのトラフィックのアクセス ルールに関連するリアルタイム イベントまたは過去のイベントについて、CS-MARS を照会できます。コマンドを使用するには、ルールを右クリックしてコンテキスト メニューから選択します。

- [フロー（Flow）]：トラフィックフローは、ルールの送信元と宛先のIPアドレス、プロトコル、およびポートによって定義されます。レポートされるフローイベントには、接続の設定およびティアダウンが含まれます。この情報を記録するには、アクセスルールに対してロギングをイネーブルにする必要があります。

フロー関連のイベントを表示するには、次の右クリック コマンドを使用します。

- **[MARSイベントを表示（Show MARS Events）] > [リアルタイム（Realtime）] > [このフローに一致（Matching this Flow）]**：このトラフィックフローと一致するイベントについて CS-MARS でリアルタイムクエリーの結果を表示します。いつでも CS-MARS ウィンド

ウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- **[MARSイベントを表示（Show MARS Events）] > [過去（Historical）] > [このフローに一致（Matching this Flow）]**：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、選択したルールのトラフィックフローに基づいて読み込まれます。必要に応じてルールパラメータとクエリー基準を編集し、[適用（Apply）] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。

- [ルール（Rule）]：ルールに対してロギングがイネーブルの場合（[Advanced]/[Edit Options] ダイアログボックス （936 ページ）を参照）、イベントをログに記録するために、（デバイスが CS-MARS によってモニタされていると想定する場合は）デバイスから CS-MARS に syslog メッセージが送信されます。このクエリーには、使用可能なキーワード情報などのアクセス ルール パラメータが含まれています。レポートされるイベントには、接続の設定およびティアダウンは含まれません。

ルール関連のイベントを表示するには、次の右クリック コマンドを使用します。

- **[MARSイベントを表示（Show MARS Events）] > [リアルタイム（Realtime）] > [このルールに一致（Matching this Rule）]**：このルール（フローパラメータおよびキーワード）と一致するイベントについて、CS-MARS でリアルタイムクエリーの結果を表示します。結果は 5 秒以内にスクロールを開始します。いつでも CS-MARS ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- [MARSイベントを表示（Show MARS Events）] > [過去（Historical）] > [このフローに一致（Matching this Flow）]：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、アクセルルール（フローパラメータおよびキーワード）に基づいて読み込まれます。必要に応じてルールパラメータとクエリー基準を編集し、[適用（Apply）] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。

- [送信元または宛先（Source or Destination）]：アクセスルールエントリの [送信元（Source）] セルまたは [宛先（Destination）] セルを右クリックした場合、ルールの送信元または宛先の IP アドレスと一致するリアルタイムイベントまたは過去のイベントを表示するように選択することもできます。

送信元または宛先アドレスのイベントを表示するには、[Source] セルまたは [Destination] セルのアドレスを右クリックし、次のコマンドのいずれかを選択します（選択するセルによってコマンドは異なります）。

- **[MARSイベントを表示（Show MARS Events）] > [リアルタイム（Realtime）] > [この送信元/宛先に一致（Matching this Source/Destination）]**：送信元または宛先アドレスが一致するイベントについて、CS-MARS でリアルタイムクエリーの結果を表示します。いつでも CS-MARS ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- **[MARSイベントを表示（Show MARS Events）] > [過去（Historical）] > [この送信元/宛先に一致（Matching this Source/Destination）]**：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、アクセスルールの送信元または宛先アドレスに基づいて読み込まれます。必要に応じてルールパラメータとクエリー基準を編集し、[適用（Apply）] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。

トラフィック フローまたはアクセス ルール イベント クエリーの基準として、Security Manager から CS-MARS に次の情報が提供されます。

- [Device details]：ホスト名、ドメイン名、管理 IP アドレス、表示名などのデバイスに関する一般情報。
- [Source addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの送信元アドレス。
- [Destination addresses]：ホストおよび IP アドレスのネットワークまたは集合を表示するために拡張されたネットワーク/ホスト オブジェクトの宛先アドレス。
- [Service]：プロトコルおよびポート情報。
- [イベントタイプ（Event Type）]：許可ルールの場合は「構築/ティアダウン/許可された IP 接続」、拒否ルールの場合は「セキュリティポリシーによってパケットを拒否」。
- [Keyword]（ルール イベントだけ。トラフィック フロー クエリーには提供されない）：論理演算子 OR で接続された ACL 名および ACE ハッシュコード（使用可能な場合）。

バージョン 7.0 以降の PIX および ASA デバイスでは、各アクセス ルールには MD5 ハッシュコードが割り当てられます。これは、そのルールによって生成される syslog に含まれています。大規模な ACL には数千のアクセス ルールを含めることができます。クエリーのキーワードとして使用すると、これらのハッシュコードは、より正確なイベント一致を生成するのに役立ちます。デバイスでハッシュコードがサポートされていない場合、キーワードがあいまいであるためクエリー結果が不正確な可能性があるという警告が表示されます。クエリーを続行し、クエリー キーワード リストを編集して送信し直します。

ヒント：

- 一度に照会できるアクセス ルールは 1 つだけです。
- セキュリティ デバイスで NAT または PAT が設定されている場合、送信元アドレスと宛先アドレスは変換前および変換後のアドレスにマッピングされ、Security Manager から CS-MARS にクエリーが送信されるときは変換後のアドレスが使用されます。インバウンド アクセス ルールの場合、宛先アドレスは変換前アドレスと見なされ、アウトバウンド アクセス ルールの場合、送信元アドレスは変換後アドレスと見なされます。
- デバイスが複数の CS-MARS コントローラによってモニタされている場合は、使用する CS-MARS インスタンスを選択するように要求されます。

- システムでのクレデンシャル検証の設定方法によっては、CS-MARS にログインするように要求される場合があります。詳細については、 Security Manager での CS-MARS サーバの登録 （3730 ページ）を参照してください。

関連項目

- [Access Rules] ページ （924 ページ）
- CS-MARS イベントからの Security Manager ポリシーの検索 （3740 ページ）
- アクセス ルールの CS-MARS イベントの表示 （3735 ページ）

IPS シグニチャの CS-MARS イベントの表示

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

着信トラフィックを設定済みのシグニチャと比較することにより、IPS または IOS IPS デバイスによってネットワーク侵入が検出およびレポートされると、デバイス上で syslog メッセージが生成されます。デバイスが CS-MARS によってモニタされている場合、シグニチャに関連付けられたログがデバイスから取得されたあと、CS-MARS でインシデントが生成されます。特定のシグニチャに関連付けられたイベントを検索すると、攻撃を迅速に識別し、デバイス設定を調整して侵入を最小限に抑えるか、または防止できます。

レポートされたネットワーク侵入イベントを CS-MARS で表示するには、Security Manager のデバイスの Signatures ポリシーで 1 つ以上のエントリを選択し、CS-MARS の [Query] ページにナビゲートしてリアルタイム イベントおよび過去のイベントを表示します。

シグニチャのリアルタイム イベントを検索すると、クエリーが自動的に実行され、結果が CS-MARS に表示されます。ただし、シグニチャの過去のイベントを検索すると、Security Manager から CS-MARS に送信される値が、クエリー フィールドへの読み込みに使用されます。必要に応じてクエリーフィールドを変更し、クエリーを実行するか、あとで使用するために保存できます。

クエリー基準として、Security Manager から CS-MARS に次のシグニチャ情報が提供されます。

- [Device details]：ホスト名、ドメイン名、管理 IP アドレス、表示名などのデバイスに関する一般情報。
- [Keyword]：シグニチャ ID、サブシグニチャ ID、および仮想センサー名（該当する場合）。

仮想センサーの場合、センサーの名前がキーワード基準として他のデバイス情報およびシグニチャ パラメータとともに含まれます。

関連項目

- CS-MARS イベントからの Security Manager ポリシーの検索 （3740 ページ）

• アクセス ルールの CS-MARS イベントの表示 （3735 ページ）

ステップ 1 （デバイスビュー）IPS または IOS IPS デバイスを選択して、[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）] を選択し、 [Signatures] ページ （2169 ページ）を表示します。

ステップ 2 シグニチャテーブルで目的のエントリを右クリックするか、または複数のエントリを選択してそのうちの 1 つを右クリックし、[MARS イベントの表示（Show MARS Events）] メニューから次のコマンドのいずれかを選択します。

- [リアルタイム（Realtime）]：このシグニチャと一致するイベントについて CS-MARS でリアルタイム クエリーの結果を表示します。5 秒以内にこの結果のスクロールが開始されます。CS-MARS へのストリーミング中の未処理イベントを表示するには、このオプションを使用します。

いつでも CS-MARS の [Query Results] ウィンドウでクエリー基準を変更し、新しいパラメータを適用して、リアルタイムの結果を変更できます。

- [履歴（Historical）]：CS-MARS で過去のクエリー基準ページを開きます。フィールドは、シグニチャ パラメータに基づいて読み込まれます。必要に応じてパラメータとクエリー基準を編集し、[Apply] をクリックして続行します。次に、[Query] ウィンドウで、クエリーを送信するか、または保存してあとで送信したり再利用したりできます。クエリーは編集でき、あとで再度実行する場合はレポートとして保存できます。

ヒント：

- シグニチャがディセーブルの場合、警告が表示され、イベント検索に進むかどうかが確認されます。
- デバイスが複数の CS-MARS コントローラによってモニタされている場合は、使用する CS-MARS インスタンスを選択するように要求されます。
- システムでのクレデンシャル検証の設定方法によっては、CS-MARS にログインするように要求される場合があります。詳細については、 Security Manager での CS-MARS サーバの登録 （3730 ページ）を参照してください。
- カスタムシグニチャはすべて、CS-MARS では「Unknown Device Event Type」イベントとして分類されます。
- IPS デバイスを Security Manager インベントリに追加するとき、または設定済みの IPS ポリシーをデバイスから削除するときに、IPS ポリシーを検索しない場合は、デフォルトのシグニチャがデバイスに割り当てられます。デフォルトのシグニチャからイベントを検索しようとすると、「Policy not found」というエラーメッセージが表示されます。ただし、デフォルトのシグニチャを編集して保存すると、CS-MARS で関連するイベントを照会できます。
- タイプが Packet Data および Context Data のイベントはシグニチャ ルールによってトリガーされないため、これらのイベントはクエリー結果に表示されません。

CS-MARS イベントからの Security Manager ポリシーの検索

『User Guide for Cisco Security MARS Local and Global Controllers』には、CS-MARS に表示されているイベントに基づいてポリシーを検索する方法についての詳細情報が記載されています。この情報には、起こりうる問題を解決するのに役立つ広範なトラブルシューティング情報と、相互作用をイネーブルにするために CS-MARS で設定する必要がある項目のチェックリストが含まれています。

ポリシー検索を実行する主な理由は、ポリシーが生成しているイベントに基づいてポリシーを調整することです。たとえば、アクセスルールにより、実際には許可すべきトラフィックがドロップされることがあります。イベントが表示中であるため、そのイベントを発生させているポリシーがあることがわかります。数回のクリックで、そのイベントから再設定する必要があるポリシーにたどり着くことができます。

デバイスで生成されたイベントに基づいてポリシーを検索するための一般的なプロセスは次のとおりです。ポリシー検索を実行するには、Security Manager クライアントがシステムにインストールされている必要があることに注意してください。

関連項目

- アクセス ルールの CS-MARS イベントの表示　（3735 ページ）
- IPS シグニチャの CS-MARS イベントの表示　（3738 ページ）

ステップ 1　CS-MARS の [Query Results] または [Incident Details] ページでイベントを検索します。

アクセス ルールの照会に使用できる syslog および NetFlow イベントの詳細については、次の項を参照してください。

- ポリシー検索に対してサポートされるシステム ログ メッセージ　（3741 ページ）
- CS-MARS での NetFlow イベント レポート　（3743 ページ）

ステップ 2　イベントの [Reporting Device] セルにある [Security Manager] アイコンをクリックします。CS-MARS の設定によっては、Security Manager へのログインを求められる場合があります。

Security Manager で複数のデバイスがイベントの特性と一致する場合は、デバイスを選択するように求められます。

ステップ 3　詳細情報が Security Manager から取得され、イベントがアクセス ルールに関するものか、または IPS シグニチャに関するものかに応じて表示されます。

- **アクセルルール**：アクセスルールが CS-MARS の読み取り専用ウィンドウに表示され、イベントと一致するルールが強調表示されます。

ルールを編集する場合は、ルール番号をクリックします。Security Manager クライアントの Access Rule ポリシーにルールが表示されます。ルールを編集して保存し、設定を展開できます。変更内容を展開するまで、デバイスに対して変更は行われません。

アクセス ルールの設定の詳細については、 アクセス ルールの設定　（920 ページ）を参照してください。

- **IPS シグニチャ**：シグニチャ詳細が CS-MARS の読み取り専用ウィンドウに表示されます。

シグニチャを編集するには、[シグニチャの編集（Edit Signature）] をクリックします。シグニチャポリシーにシグニチャが表示され、変更できるようになります。詳細については、シグニチャ パラメータの編集（シグニチャの調整） （2196 ページ）を参照してください。

特定のアクションをイベントから削除するか、またはイベントを完全に削除してセンサーが処理できないようにする場合は、[フィルタの追加（Add Filter）] をクリックします。Security Manager で [Add Event Filter] ダイアログボックスが開き、イベント フィルタを設定できます。詳細については、[Add Filter Item]/[Edit Filter Item] ダイアログボックス （2222 ページ）を参照してください。

アクセス ルールと同様に、変更内容は、新しい設定を展開するまで有効になりません。

ポリシー検索に対してサポートされるシステム ログ メッセージ

セキュリティ アプライアンスおよび IOS デバイスでアクセス ルールを設定するときに、[Advanced]/[Edit Options] ダイアログボックス （936 ページ）で、システム ログ（syslog）メッセージを生成するロギング オプションを設定できます。複数のコンテキストを持つデバイスでは、各セキュリティ コンテキストに独自のロギング設定が含まれ、独自のメッセージが生成されます。Security Manager が CS-MARS と相互に機能するように設定されている場合、これらのメッセージは CS-MARS にレポートされ、レポートされた情報をルールごとに照会できます。

これらのメッセージ ID の詳細については、該当する製品マニュアルの『System Message Guide』を参照してください。

セキュリティ アプライアンス メッセージ

セキュリティ アプライアンス syslog メッセージはパーセント記号（%）で始まり、その構造は次のとおりです。

```
%{ASA | PIX | FWSM}-Level-Message_number: Message_text
```

次に例を示します。

```
%ASA-2-302013: Built outbound TCP connection 42210
for outside:9.1.154.12/23 (9.1.154.12/23) to inside:2.168.154.12/4402 (192.168.154.12/4402)
```

これらのメッセージの前に追加情報（日付やタイムスタンプなど）が付加されることに注意してください。具体的な追加情報は、デバイスのタイプによって異なります。

各メッセージは一意の 6 桁の数字（前の例では 302013）によって識別されます。Security Manager から CS-MARS へのクエリーでは、次のセキュリティ アプライアンス syslog メッセージ ID がサポートされます。セキュリティ アプライアンスのロギング レベルを変更した場合、これらのメッセージは新しいレベルで生成されます。

メッセージ ID	メッセージ
106023	IP パケットがアクセス ルールによって拒否されました。このメッセージは、ルールに対してロギングがイネーブルにされていない場合でも記録されます。これは、デフォルトのロギング オプションです。
106100	IP パケットがアクセス ルールによって許可または拒否されました。[Advanced]/[Edit Options] ダイアログボックス （936 ページ）でルールに対して定義されているロギング レベルに基づいて、追加情報が提供されます。
302013	2 つのホスト間の TCP 接続が確立されました。
302014	2 つのホスト間の TCP 接続がティアダウンされました。
302015	2 つのホスト間の UDP 接続が確立されました。
302016	2 つのホスト間の UDP 接続がティアダウンされました。
302020	2 つのホスト間の ICMP 接続が確立されました。
302021	2 つのホスト間の ICMP 接続がティアダウンされました。

ルータ メッセージ

Cisco IOS ルータでも、アクセス ルールに対して syslog メッセージが生成されます。アクセス リストをトリガーする最初のパケットによって、即座にロギング メッセージが生成され、後続パケットは表示または記録されるまで 5 分間隔で収集されます。各ロギング メッセージには、アクセス リスト番号、パケットが許可されたか拒否されたか、パケットの送信元 IP アドレス、および前の 5 分間隔で許可または拒否されたその送信元からのパケットの数が含まれます。

Security Manager から CS-MARS へのクエリーでは、次の IOS syslog メッセージ ID がサポートされます。

%SEC-6-IPACCESSLOGP	特定のアクセス リストのログ基準と一致するパケットが検出されました（TCP および UDP）。
%SEC-6-IPACCESSLOGS	特定のアクセス リストのログ基準と一致するパケットが検出されました（IP アドレス）。
%SEC-6-IPACCESSLOGDP	特定のアクセス リストのログ基準と一致するパケットが検出されました（ICMP）。
%SEC-6-IPACCESSLOGNP	特定のアクセス リストのログ基準と一致するパケットが検出されました（その他のすべての IPv4 プロトコル）。

（注） 過剰な数の syslog が生成されて CS-MARS にレポートされている場合は、[Advanced]/[Edit Options] ダイアログボックス （936ページ）を使用して、最も多くのメッセージを生成しているアクセス ルールのロギング レベルを変更します。生成されるメッセージのタイプを制限するために、デバイスのロギング ポリシーの変更を考慮することもできます。

CS-MARS での NetFlow イベント レポート

CS-MARS でのイベント レポートに、ASA 8.1+ デバイスからの NetFlow イベントを含めることができます。

NetFlow Security Event Logging では、高性能環境でセキュリティ テレメトリを効率的に配信するために、NetFlow バージョン 9 のフィールドおよびテンプレートが使用されます。NetFlow Security Event Logging は、syslog メッセージングよりも拡張性が高く、記録されるイベントについて同様に詳細な情報を提供します。ASA NetFlow 実装では、定期的な間隔でフローに関するデータがエクスポートされるのではなく、フローの寿命の中で重大なイベントだけがエクスポートされます。次のフロー イベントがエクスポートされます。

- フロー作成
- フロー ティアダウン
- アクセス ルールによって拒否されたフロー

ASA は syslog メッセージもエクスポートしますが、これには同じ情報が含まれています。デバイスで NetFlow をイネーブルにする場合、同等の syslog メッセージをディセーブルにすることを検討できます。同等の syslog メッセージをディセーブルにすると、同じイベントを表す NetFlow レコードと syslog メッセージの両方を生成および処理することによりパフォーマンスが低下する可能性を回避できます。次の表に、syslog メッセージおよび同等の NetFlow イベントを示します。NetFlow イベント ID および拡張イベント ID も示します。NetFlow と同等の syslog メッセージをディセーブルにする方法については、[Server Setup] ページ （2664ページ）を参照してください。

syslog ID	syslog の説明	NetFlow イベント ID	拡張イベント ID
302013302015302017302020	TCP、UDP、GRE、および ICMP 接続の作成。	1 = フロー作成	0 = 無視
302014302016302018302021	TCP、UDP、GRE、および ICMP 接続のティアダウン。	2 = フロー削除	0 = 無視、または > 2000 = ASP ドロップ理由
710003	デバイスインターフェイスへの接続の試行が拒否されました。	3 = フロー拒否	1003 = 設定により To-the-box フローが拒否されました。

syslog ID	syslog の説明	NetFlow イベント ID	拡張イベント ID
106015	最初のパケットがSYNパケットではなかったため、TCP フローが拒否されました。	3 = フロー拒否	1004 = 最初のパケットがTCP SYN パケットではなかったため、フローが拒否されました。
313001	デバイスへの ICMP パケットが拒否されました。	3 = フロー拒否	1003 = 設定により To-the-box フローが拒否されました。
313008	デバイスへの ICMP v6 パケットが拒否されました。	3 = フロー拒否	1003 = 設定により To-the-box フローが拒否されました。
106023	アクセス グループ コマンドでインターフェイスに付加されたアクセス リストによってフローが拒否されました。	3 = フロー拒否	1001 = フローが入力 ACL によって拒否されました。1002 = フローが出力 ACL によって拒否されました。
106100	アクセスルールがヒットしました。	1 = フローが作成されました（ACL がフローを許可した場合）。3 = フローが拒否されました（ACL がフローを拒否した場合）。	0 = フローが ACL によって許可されている場合。1001 = フローが入力 ACL によって拒否されました。1002 = フローが出力 ACL によって拒否されました。

Flow Denied NetFlow イベントの場合、次の表に示すように、拡張イベント ID によって拒否の理由が示されます。

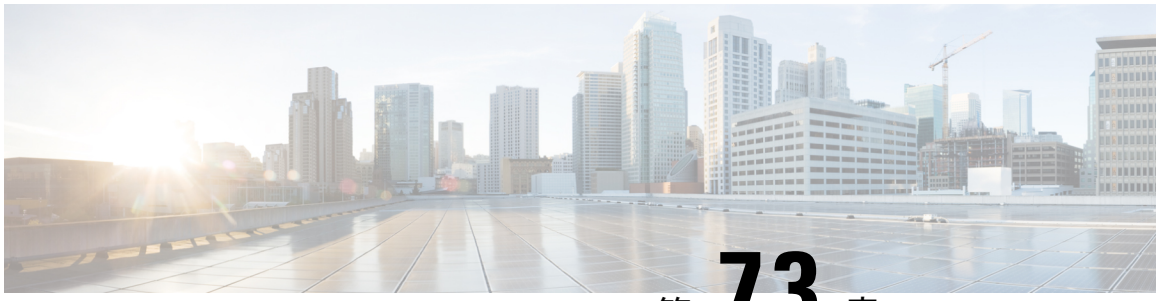
拡張イベント ID	イベント	説明
1001	フロー拒否	フローが入力 ACL によって拒否されました。
1002	フロー拒否	フローが出力 ACL によって拒否されました。

拡張イベント ID	イベント	説明
1003	フロー拒否	インターフェイス サービスへの接続の試みがセキュリティ アプライアンスによって拒否されました。たとえば、このメッセージは、セキュリティ アプライアンスが、権限のない SNMP 管理ステーションからの SNMP 要求を受信したときに（サービス SNMP とともに）表示されます。
1004	フロー拒否	最初のパケットが TCP SYN パケットではなかったため、フローが拒否されました。
> 2000	フロー削除	2000 を超える値は、フローが終了したさまざまな理由を表します。

第 VIII 部

イメージ管理

• Image Manager の使用 （3749 ページ）



第 73 章

Image Manager の使用

Image Manager は、ネットワークの内部およびエッジファイアウォールデバイスでのイメージの配布と管理を簡素化するツールです。このツールにより、次のことが可能になります。

さまざまなタイプおよびバージョンのイメージのリポジトリをダウンロードして維持する

イメージを評価する

ネットワーク内のデバイスへのイメージのアップグレードの影響を分析する

アップグレードを準備し計画する

組み込みフォールバックおよびリカバリメカニズムを十分に使用した信頼性の高い方法でデバイスをアップグレードし、ネットワークのダウンタイムを最小限にする

この章は次のトピックで構成されています。

- イメージ マネージャの使用開始　（3749 ページ）
- イメージの操作　（3759 ページ）
- バンドルの操作　（3764 ページ）
- デバイスの使用　（3767 ページ）
- Image Manager を使用したデバイスでのイメージの更新について　（3773 ページ）
- ジョブの操作　（3789 ページ）
- イメージ管理のトラブルシューティング　（3794 ページ）

イメージ マネージャの使用開始

Image Manager には、イメージの管理、更新が必要なデバイスの操作、およびそれらのデバイスにおけるイメージのインストールの実行に使用されるセクションが含まれています。

Image Manager 上の該当する領域の詳細については、次の項目を参照してください。

- イメージの操作　（3759 ページ）
- バンドルの操作　（3764 ページ）
- デバイスの使用　（3767 ページ）

- ジョブの操作 （3789 ページ）

Image Manager を使用する前に、次のセクションを確認する必要があります。

- この機能でサポートされているプラットフォーム
- 機能の動作を制御するために変更可能な設定
- デバイスが Image Manager と連動するように設定されていることを確認するために必要な手順

ここでは、次の内容について説明します。

- Image Manager のサポートされるプラットフォームおよびバージョン （3750 ページ）
- Image Manager によってサポートされるデバイス設定 （3753 ページ）
- Image Manager でサポートされるイメージタイプ （3754 ページ）
- Image Manager での管理設定 （3756 ページ）
- Image Manager 用のデバイスのブートストラップ （3758 ページ）

Image Manager のサポートされるプラットフォームおよびバージョン

注意 バージョン 4.18 以降、Cisco Security Manager では、ASA 5512、ASA 5506、ASA 5506H、および ASA 5506W モデルの ASA 9.10(1) 以降の SFR はサポートされないため、Image Manager を介して 9.10(1) にアップグレードすると、既存の SFR 設定が失われます。

Image Manager は、ASA デバイスでのみ使用できます。次のデバイスは、Image Manager をサポートしています。

- すべてのレガシー ASA モデル：ASA 5505/10/20/40/50/80
- ASA 5585
- ASA 5515/25/35/45/55
- Catalyst 6000 の ASA-SM モジュール
- 5516-X
- 適応型セキュリティ仮想アプライアンス（ASAv）

Cisco Security Manager 4.20 以降、Image Manager は、ASA 9.13(1) 以降のデバイスで実行されている、アプライアンスモードで動作する次の Firepower デバイスをサポートしています。

- Cisco Firepower 1140 セキュリティ アプライアンス
- Cisco Firepower 1150 セキュリティ アプライアンス

- Cisco Firepower 1010 セキュリティアプライアンス
- Cisco Firepower 2140 セキュリティアプライアンス
- Cisco Firepower 2120 セキュリティアプライアンス
- Cisco Firepower 1120 セキュリティ アプライアンス
- Cisco Firepower 2110 セキュリティアプライアンス
- Cisco Firepower 2130 セキュリティアプライアンス

次のデバイスはサポートされておらず、Image Manager の統合ビューのデバイスタブでは除外されます。

- PIX ファイアウォール
- FWSM ブレード
- AUS によって管理される ASA デバイス
- Security Manager で管理されていないデバイス
- その他のデバイスタイプ：IPS およびルーター

Image Manager は、バージョン 7.x 以降の ASA デバイスのイメージアップグレードをサポートしています。アップグレードに使用できる対象イメージのバージョンに制限はありません。Security Manager 4.4 でサポートされている最新バージョンの ASA（ASA バージョン 9.0(1) および 9.1(1)）へのイメージアップグレードがテストされています。

4.9 より前のバージョンの Image Manager アプリケーションでは、サポートされているデバイスタイプのすべてのイメージがリストされていました。そこで、必要なイメージを選択してダウンロードしていました。バージョン 4.9 以降の Image Manager アプリケーションでは、特定のバージョンのイメージのみがリストされます。

Image Manager には ASDM、†リモートアクセスプラグイン、およびホストスキャンの最新のイメージがリストされます。AnyConnect バージョン 3.x および 4.x では、最新のイメージがリストされます。

ASA デバイスでは、次のイメージがリストされます。

ASA デバイスのモデル	Image Manager にリストされる ASA イメージ
5512-x、5515-x、5525-x、5545-x、5585x	9.4.1 9.3.3 9.3.2 9.3.1.SMP 9.2.3.SMP 9.2.2.4.SMP 9.2.1.SMP.ED 9.1.4.SMP.ED 9.1.5.SMP.ED 9.1.6.SMP.ED 9.1.2.SMP.ED 9.0.4.SMP.ED 8.4.6.SMP.ED
5580-x	9.1.6.SMP 9.1.5.SMP.ED 9.1.4.SMP.ED 9.1.2.SMP.ED 9.0.4.SMP.ED 8.4.6.SMP.ED
5555-x	9.4.1 9.3.3 9.3.2 9.3.1.SMP 9.2.3.SMP 9.2.2.4.SMP 9.2.1.SMP.ED 9.1.2.SMP.ED 9.0.4.SMP.ED

ASA デバイスのモデル	Image Manager にリストされる ASA イメージ
5505、5510、5520、5540、5550	9.1.6 9.1.5.ED 9.1.4.ED 9.1.2.ED 9.0.4.ED 8.4.6.ED
5506-X	9.4.1、9.3.3、9.3.2
5506H-X	9.4.1
5506W-X	9.4.1
5516-X	9.4.1
適応型セキュリティ仮想アプライアンス（ASAv）	9.3.1、9.3.2、9.4.1

（注） Image Manager の ASA イメージアップグレードは、Firepower シリーズのアプライアンスモード デバイスでサポートされます。

危険 イメージのダウングレードは制限されていませんが、ユーザー責任で実施してください。ダウングレードでは Image Manager による検証は実行されません。

Image Manager によってサポートされるデバイス設定

スタンドアロン ASA デバイスでのイメージ更新のサポートに加えて、Image Manager は、ファイルシステムを管理し、高可用性と拡張性を目指して特別に設定された ASA デバイスのシームレスなイメージ更新をサポートします。次の構成がサポートされています。

- [マルチコンテキストモード（Multiple context mode）]：単一の ASA を複数の仮想デバイス/ファイアウォールに分割できるマルチコンテキストモードの ASA。http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_contexts.html [英語] を参照してください。該当する各仮想ファイアウォールは、Security Manager では独立したデバイスとして扱われます。Image Manager が、これらの仮想デバイスをホストする物理ユニットのイメージを更新すると、すべての仮想デバイスのデバイスプロパティが新しいイメージ情報で更新されます。
- [フェールオーバー構成（Failover configuration）]：高可用性のためにフェールオーバーするように設定された 2 台の同一の ASA デバイス。これらのデバイスは、アクティブ/アク

ティブまたはアクティブ/スタンバイフェールオーバーになるように構成できます。http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_overview.html [英語] を参照してください。アクティブ/アクティブ フェールオーバー ペアでのイメージの更新は、Image Manager ではサポートされていません。Image Manager を使用してアクティブ/アクティブ フェールオーバー ペアのイメージを更新するには、1 つのユニットですべてのフェールオーバーグループをアクティブにし、他方のユニットで対応するフェールオーバーグループをスタンバイにすることによって、アクティブ/アクティブ フェールオーバー ペアを一時的にアクティブ/スタンバイに変換する必要があります。アップグレード後に、フェールオーバーペアをアクティブ/アクティブに戻すことができます。

- [クラスタ構成（Cluster configuration）]：複数の ASA（最大 8 つの ASA）を**クラスタ**と呼ばれる単一の論理ユニットとしてグループ化して、スループットと冗長性を向上させることができます。デバイスをクラスタリングする目的は、管理を簡素化し、処理速度を向上させることです。クラスタを使用することで、接続を負荷分散するために連携して動作する多数の同時接続に拡張できます。クラスタリング機能は、ASA バージョン 9.0(1) から導入されました。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa91/configuration/general/ha_cluster.html [英語] を参照してください。

（注） クラスタリングは ASA 5580 と SSA 5585 のみでサポートされています。

リリース 4.4 以降、Security Manager はクラスタリングをサポートしています。Configuration Manager と Image Manager では、クラスタまたはフェールオーバーペアのすべてのデバイス/メンバーが単一のデバイスとして管理されます。つまり、制御ユニットの設定を変更すると、その変更はクラスタ内のすべてのデバイスに対して自動的に実行されます。同様に、Image Manager は、フェールオーバーまたはクラスタの一部である各物理ユニットのイメージを 1 回の操作で更新します。

マルチコンテキスト ASA のイメージ管理

バージョン 4.12 以降、Image Manager のデバイスツリービューには、ASA ソフトウェアバージョン 9.6(2) 以降を実行しているマルチコンテキスト ファイアウォール デバイスのすべてのユーザーコンテキスト（管理コンテキストとユーザーコンテキスト）が表示されます。

ユーザーコンテキストを選択し、選択したコンテキストの storage-url 情報を [ストレージ（Storage）] タブで表示できます。

[互換性のあるイメージ（Compatible Images）] タブでは、選択したユーザーコンテキストの AnyConnect イメージのみを表示できます。ただし、システムコンテキストについては、すべてのイメージタイプが表示されます。

Image Manager でサポートされるイメージタイプ

Image Manager は、次のタイプのイメージをサポートしています。

- ASA システムソフトウェア
- ASDM イメージ
- VPN イメージ（Cisco Secure Desktop（CSD）、AnyConnect、および Hostscan を含む）
- SSLVPN プラグインのイメージ（例：RDP、SSH、ICA など）

Image Manager は、ASA システムソフトウェアと ASA デバイス上の ASDM イメージを完全に管理します。つまり、イメージのロード、設定の変更によるイメージのアクティブ化、さらには、イメージのアップグレードプロセスを完了するために必要なデバイスのリロードを実行します。

ユーザー コンテキスト デバイスの場合、Security Manager は、コピーおよびインストール用の AnyConnect イメージのみをサポートします。

Image Manager は ASA–CX イメージをサポートしていません。これには、asacx-sys-9.1.1-1.pkg などのシステムイメージと、asacx-5500x-boot-9.1.1-1.img などのブートイメージの両方が含まれます。Image Manager を使用して CX イメージを Image Manager リポジトリに追加したり、CX イメージをデバイスにプッシュしたりすることはできません。

SSL VPN イメージの取り扱い

Image Manager は、SSL VPN イメージを ASA デバイスに確実にコピーすることだけを行います。Image Manager によって SSL VPN イメージに設定コマンドまたはアクティベーションコマンドが追加されることはありません。イメージの設定は、Configuration Manager を使用して行う必要があります。

次のファイルは Image Manager では管理されないため、以前のバージョンの Security Manager と同様に、Configuration Manager から設定および展開する必要があります。

- CSD コンフィギュレーション XML
- AnyConnect クライアント プロファイル ファイル
- DAP コンフィギュレーション XML
- フルカスタマイズ XML ファイル

Image Manager を使用して SSL VPN イメージをデバイスにコピーした後、これらのイメージを使用できるように、Configuration Manager でリモートアクセス VPN ポリシーを設定する必要があります。設定する必要があるリモートアクセス VPN ポリシーは、Configuration Manager の次のパスにあります。

- CSD パッケージ：[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] > [Cisco Secure Desktop] グループボックス
- HostScan パッケージ：[リモートアクセスVPN（Remote Access VPN）] > [ダイナミックアクセス（Dynamic Access）] > [Cisco Secure Desktop] グループボックス
- Anyconnect イメージ：[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] > [クライアント設定（Client Settings）] タブ

- プラグイン：[リモートアクセスVPN（Remote Access VPN）] > [SSL VPN] > [その他の設定（Other Settings）] > [プラグイン（Plug-in）] タブ

SSL VPN バイナリファイルは、VPN ポリシーで参照する前にデバイスフラッシュに存在している必要があります。そうでない場合、Security Manager は、設定を展開する前に、Image Manager を使用してこれらのファイルをデバイスに確実にプッシュする設定についてユーザーに通知する、アクティビティ検証警告を表示します。ユーザーがアクティブ化の警告を無視して続行すると、Configuration Manager はデフォルトで古い動作に戻り、これらのファイルを参照する構成を展開する前に、以前のバージョンの Security Manager で実行されていたように、イメージまたはファイルをプッシュします。ただし、ユーザーは、Image Manager を使用してこれらのファイルをコピーした場合に得られる次の利点を活用できません。

1. disk1 のような外部ディスクを使用してファイルをコピーする機能。Configuration Manager は、ファイルを disk0 にのみコピーし、外部ディスクを認識またはサポートしません。
2. Image Manager は、選択したイメージをコピーするのに十分な空き領域がディスク上にあることを検証することにより、イメージコピー中のエラーを未然に防ぎ、イメージをコピーするための十分な領域がない限り、ジョブの作成を許可しません。ユーザーは、Image Manager を使用して不要なイメージを削除することでスペースを空けることができます。

（注） Image Manager は、ASA にプッシュされる SSL VPN ファイルの互換性を検証しません。ただし、リモートアクセス VPN ポリシーで互換性のないファイルが参照されている場合、Configuration Manager はエラーを示します。

Image Manager での管理設定

Image Manager には、新しい管理設定が導入されました。これらの管理設定は、Configuration Manager の一部として設定する必要があります。

Cisco.com 証明書の設定

バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理 （620 ページ）を参照してください。

Image Manager の管理設定をするには、次の手順を実行します。

ステップ 1 [Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] に移動します。

Cisco Security Manager - [管理（Administration）] ページが表示されます。

ステップ 2 Workflow を設定します。

ヒント Workflow 制御設定については、Configuration Manager のマニュアルを参照してください。

a) [Workflow] を選択します。

b) インストールジョブをデバイスにインストールする前に、割り当てられた承認者がインストールジョブを明示的に承認するよう要求するには、[展開とインストールイメージの承認が必要（Require Deployment & Install Image Approval）] を選択します。このオプションを選択する場合は、適切な電子メール通知を設定してください。詳細については、『 [Workflow] ページ （745 ページ）』を参照してください。

（注） 送信者が展開ジョブを承認できるようにするには、[送信者が展開ジョブを承認可能（Submitter can Approve Deployment Job）] を選択します。

c) [保存（Save）] をクリックします。

ステップ 3 デバッグの設定をします。

a) [デバッグオプション（Debug Options）] を選択し、[Image Manager のデバッグレベル（ Image Manager Debug Level）] のドロップダウンリストから、必要なデバッグレベルを選択します。

ヒント レベルには、重大、エラー、警告、情報、およびデバッグが含まれます。デフォルトのログレベルはエラーです。

（注） ログファイルは次のように保存されます。

- サーバーログは、**%NMSROOT%\MDC\log\operation\vmssharedsvcs.log** および **%NMSROOT%\MDC\tomcat\logs\stdout.log** にあります。
- クライアントログは **<Client Install Dir>\logs*.log** にあります。

b) [保存（Save）] をクリックします。

ステップ 4 Cisco.com のログイン情報を設定します。

a) [Image Manager] を選択します。

[Image Manager] ページが表示されます。

b) [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [IPSの更新（IPS Updates）] > [サーバーの更新（Update Server）] ですでに設定されている Cisco.com に接続するためのログイン情報があり、それを Image Manager で再利用する場合は、[IPS更新設定を使用（Use IPS Updates Settings）] チェックボックスをオンにします。これはデフォルトの動作です。

（注） Cisco.com のみがサポートされ、ローカルサーバーはサポートされません。

c) [Image Manager] ページで、Image Manager のログイン情報のセットを明示的に指定する場合は、[IPS更新設定を使用（Use IPS Updates Settings）] チェック ボックスをオフにします。

[Image Manager] ページのフィールドが操作可能になります。

d) 次のフィールドに入力します。

- ユーザ名
- パスワード
- 確認

e) 必要に応じて、プロキシサーバー設定を完了して、プロキシを設定します。

1. [プロキシの有効化（Enable Proxy）] チェックボックスをオンにします。
2. 次のフィールドに入力して、プロキシを定義します。
3. IP またはホスト名（IP or Hostname）
4. ポート
5. ユーザ名
6. パスワード
7. （パスワードの）確認

f) [テスト接続（Test Connection）] をクリックして、設定した Cisco.com への接続をテストします。
g) [保存（Save）] をクリックします。

ステップ 5 イメージインストールジョブのパージ間隔の設定

a) [Image Manager] を選択します。
b) [これより古いジョブをパージ（Purge Jobs Older Than）] フィールドにパージ値を入力して、パージとパージの間に経過すべき日数を指定します。

（注） [今すぐパージ（Purge Now）] ボタンを押すと、パージ間隔基準を満たすイメージインストールジョブが即座にパージされます。

ステップ 6 イメージバックアップを設定します。

a) [Image Manager] を選択します。
b) 標準バックアップの一部としてリポジトリを含めるには、[リポジトリを含める（Include Repository）] を選択します。

注意 イメージファイルは多くの容量を消費するため、Security Manager サーバーに十分なハードディスク容量があることを確認してください。

（注） [リセット（Reset）] ボタンをクリックすると、値を、現在の変更の前に最後に保存された値にリセットできます。

c) [保存（Save）] をクリックします。

ステップ 7 [閉じる（Close）] をクリックして管理ウィンドウを閉じます。

Image Manager 用のデバイスのブートストラップ

Image Manager でのブートストラップは、ASA デバイスに対して Configuration Manager で実行するものと本質的に同じです。

イメージ管理のためにデバイスをブートストラップするには、次の手順を実行します。

ステップ 1 デバイスで HTTPS を設定して、Security Manager で ASA を管理します。

a) HTTP サーバがイネーブルであることを確認します。

b) デバイスでの HTTP 管理のために、Security Manager サーバーの IP アドレスを許可ホストとして追加します。

ステップ 2 コンフィギュレーション レジスタの設定が、実行コンフィギュレーションのイメージリストを使用してブートするように設定されていることを確認します。

a) レジスタ値：0x1、0x3、0x5、0x7、0x9

（注） レジスタ値：0x1 が推奨設定です。

b) **rommon** モードで起動するように設定しないでください（設定すると、デバイスは再起動されず、イメージのアップグレードは中止されます）。

ステップ 3 Security Manager で、[ツール（Tools）] > [Security Manager管理（Security Manager Administration）] > [デバイス通信（Device Communication）] > [SSL証明書パラメータ（SSL Certificate Parameters）] に移動します。[SSL証明書パラメータ（SSL Certificate Parameters）] 領域で、[PIX/ASA/FWSMデバイス認証証明書（PIX/ASA/FWSM Device Authentication Certificates）] を [証明書認証を使用しない（Do not use certificate authentication）] に設定します。

ステップ 4 デバイスのフラッシュメモリに、ロードするイメージを保持するための十分なスペースがあることを確認します。

ヒント 必要に応じて、使用する予定のない他のイメージをデバイスから削除できます。

ステップ 5 次のように、ASA のブートイメージ/設定ポリシーを管理対象外にすることをお勧めします。

a) Security Manager で、[ツール（Tools）] > [管理（Administration）] > [ポリシー管理（Policy Management）] に移動します。

b) [ブートイメージ（Boot Image）]/[設定ポリシー（Configuration policy）] の選択をオフにします

（注） Image Manager は、イメージインストールジョブの一部としてブートイメージと ASDM イメージを構成します。したがって、ブートイメージ/構成ポリシーが管理対象外ではない場合、イメージのインストール後に設定を展開すると、Image Manager によって追加されたこれらのブートコマンドが削除されます。これを防ぐには、ブートイメージ/設定ポリシーを Security Manager で管理対象外にする必要があります。これは、[Security Managerの管理設定（Security Manager administration settings）] -> [デバイス例外設定（Device Exception Settings）] -> [ファイアウォールポリシー（Firewall Policies）] ノードから実行できます。

ステップ 6 デバイスを HPM の優先監視対象デバイスとして設定しないことをお勧めします。

ステップ 7 デバイスのすべての設定変更が送信され、展開されていることを確認します。

イメージの操作

Image Manager は、Cisco.com 上のイメージへのアクセスに加え、ネットワーク上のイメージへのアクセスも提供します。イメージにリポジトリの場所が示されている場合は、そのイメージ

がすでにダウンロードされていることを意味します（Cisco.com またはローカルファイルシステムから）。逆に、場所が Cisco.com であることが示されているイメージは、リポジトリにダウンロードされていません。セレクタの[イメージ（Images）]セクションで[リポジトリイメージ（ Repository Images）] に移動すると、すべてのイメージが示されたリストを調べることができます。利用可能なイメージをフィルタリング、並べ替え、検索することもできます。特に、フィルタリングは、Image Manager 内の移動に使えるため便利です。すべてのイメージを始め、メインリポジトリビューの見出しを使用して、名前、バージョン、タイプなどのさまざまな属性でイメージを見つけることができます。

Image Manager は ASA-CX イメージを管理しません。Cisco.com で入手可能な CX イメージは、ダウンロード用に Image Manager に表示されません。また、ファイルシステムから CX イメージを追加することもできません。

（注） イメージリポジトリにダウンロードされたイメージのみを、イメージ アップグレード ジョブに使用できます。

（注） Security Manager リリース 4.4 以降、Security Manager が Cisco.com に接続してイメージを更新するか、イメージの更新が利用可能かどうかを確認するときに、追加の証明書検証が実行されます。最新の証明書を受け入れていない場合、更新またはダウンロードは失敗します。他の操作を続行する前に、最新の証明書を取得、表示、および受け入れる必要があります。証明書の詳細については、デバイス通信設定および証明書の管理 （576 ページ）を参照してください。

ここでは、次の内容について説明します。

- すべてのイメージの表示 （3760 ページ）
- イメージのリポジトリへのダウンロード （3762 ページ）

すべてのイメージの表示

最初に Image Manager を開いたとき、またはセレクタから [すべてのイメージ（All Images）] を選択したとき、システムはイメージの完全なリストを表示します。このリストには、リポジトリ内のイメージと Cisco.com 上のイメージ（まだダウンロードされていない）の両方が含まれています。一部の VPN イメージファイルは、Security Manager のインストールにバンドルされており、最初からリポジトリに表示されます。Image Manager クライアントが最初に起動したとき、またはクレデンシャルが Image Manager の Security Manager 管理設定で設定されるまで、Image Manager はクレデンシャルが設定されていないことに関する警告を表示します。

（注） Security Managerの以前のリリースでは、Image Managerリポジトリにすでに存在するパッケージ済みの SSL-VPN イメージのみが表示されていました。Security Manager リリース 4.4 以降、新しくインストールされた Security Manager でリポジトリに接続していない場合、Image Manager は、リポジトリ内の事前にパッケージ化された SSL-VPN イメージを表示するだけでなく、Cisco.com で利用可能なサポート対象の ASA イメージも一覧表示します。事前にパッケージ化されたファイルは、CSMRoot>\MDC\athena\ccometadata で入手できます。したがって、Cisco.com への初期接続を実行していない場合でも、Security Managerのリリース時点で利用可能になっていた最新のイメージを表示できます。Cisco.com で最新の更新を確認するか、Cisco.com からイメージをダウンロードするか、またはその両方を行うには、Cisco.com への接続が必要であり、Cisco.com へのクレデンシャルを設定する必要があります。イメージの可用性に関する事前にパッケージ化されたこの情報により、Cisco.com に接続していないユーザーでも、Cisco.com で入手可能な最新のイメージ（少なくとも Security Manager リリースによって Cisco.com で公開されたもの）を表示できます。この機能により、特定のデバイスタイプ/プラットフォームに互換性のあるイメージを表示することもできます。

（注） CSMは、サポートされているすべての最新のイメージを[すべてのイメージ（All Images）]ウィンドウに一覧表示します。インストールエラーやデバイスのシャットダウンを回避するには、デバイスのリストから適切なイメージインストールを使用する必要があります。

このビューは、リストされているイメージ属性のいずれかを基準にして並べ替えることができます。たとえば、イメージをサイズ別に一覧表示できます。並べ替えの基準にできる属性は次のとおりです。

- ダウンロード状態：これは最初の列であり、アイコンとして表示されます。アイコンは操作可能で、この列のアイコンをダブルクリックして、Cisco.com からのイメージのダウンロードを開始したり、進行中のイメージのダウンロードを中止したり、リポジトリからイメージを削除したりできます。これらのアクションのたびにアイコンが変化することに留意してください（緑色の矢印はCisco.com上の画像を示し、赤色の十字はすでにダウンロードされている画像を示し、別のアイコンはダウンロードが進行中であることを示しています）。
- イメージ（名前）
- タイプ（Type）
- バージョン
- 参照先
- Size
- 説明

- コメント（イメージについてのコメントを追加および編集できます）。

すべてのイメージを表示するには、次の手順を実行します。

ステップ 1 Cisco.com で利用可能な新しいイメージを確認します。

a) [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] > [Image Manager] に移動して、Cisco.com にアクセスするためのクレデンシャルを設定します。
b) 右上隅にある二重矢印の [更新の確認（Check for Updates）] アイコンをクリックします。
c) CCO アカウントに暗号化イメージをダウンロードする権限があることを確認します。権限がない場合は、リンクに移動して契約に同意してから、操作を再試行してください。

更新をチェックしている間、システムには「**Updating（更新中）**」と表示されます。完了すると、「**Last updated at: <timestamp>（最終更新日時：<timestamp>）**」と表示され、[すべてのイメージ（All Images）] ビューで利用可能な新しいイメージを表示できるようになります。

ステップ 2 最近発行された Cisco.com 証明書をまだ承認していない場合、システムは、Image Manager による Cisco.com との通信が発生する前に、最新の証明書を取得、表示、および承認する必要があることを通知します。

ステップ 3 セレクタで [すべてのイメージ（All Images）] をクリックします。

イメージリストが表示されます。

ステップ 4 リストを並べ替えるには、いずれかの列見出しをクリックします。

イメージのリストは、選択した属性に従って並べ替えられます。

ステップ 5 リストをフィルタリングするには、Image Manager の検索ウィンドウを使用してキー文字列を入力します。たとえば、バージョン番号の数字を入力できます。

（注） また、一部の列見出しのフィルタ設定を使用して、表示されるリストをフィルタリングすることもできます。

イメージのリポジトリへのダウンロード

Cisco.com またはローカルファイルシステムからリポジトリにイメージをダウンロードできます。

（注） バージョン 4.4 以降、Security Manager には証明書信頼管理機能があります。この機能は、Cisco.com 証明書の処理改善に役立ちます。この機能の詳細については、証明書信頼管理（620 ページ）を参照してください。続行するには、Cisco.com のイメージダウンロードサイトからの最新の証明書を承認している必要があります。イメージをダウンロードするサイトの証明書は、イメージに関する最新のメタデータ情報を取得するために「更新の確認」のために接続されるサイトとは異なる場合があります。そのため、「Image Meta-data Locator」URL からの証明書を承認した場合でも、イメージダウンロード URL の証明書を承認する際にエラーが発生して、イメージのダウンロードに失敗する場合があります。イメージのダウンロードを続行するには、エラーメッセージに示されたダウンロード URL からの証明書を取得して承認する必要があります。

（注） バージョン 4.9 以降、Security Manager では、cisco.com からイメージをダウンロードする前に、エンドユーザライセンス契約（EULA）を読んで同意することが義務付けられています。

ヒント イメージは、[互換イメージ（Compatible Images）] タブからダウンロードすることもできます。詳細については、デバイス上のイメージの管理 （3770 ページ）を参照してください。

イメージファイルを Security Manager リポジトリに追加するには、次の手順を実行します。

ステップ 1 Cisco.com からイメージをダウンロードするには、次の手順を実行します。

a) [すべてのイメージ（All Images）] ビューで、最初の列にある [ダウンロードの開始（Start Download）] アイコンをダブルクリックします。

ヒント Cisco.com へのログイン情報が設定されており、イメージをダウンロードする権限があることを確認してください。

（注） ダウンロードするイメージがリポジトリにすでに存在する場合、Image Manager はエラーメッセージを表示します。ファイル名とチェックサムが同じ場合、システムはダウンロードをスキップします。

ダウンロードの進行状況を示す [ダウンロード（Downloads）] ウィンドウが表示されます。

ヒント ダウンロードの進行に応じて、進行状況アイコンが変化する場合があります。緑色のチェックアイコンに [展開済み（Deployed）] という単語が付いている場合、成功を示します。赤い X アイコンは失敗を示します。失敗した場合は、[ダウンロード（Downloads）] ウィンドウでそのイメージの失敗の原因を表示できます。メッセージをダブルクリックして、エラーの完全な詳細を表示できます。

b) 完了したら、[リポジトリイメージ（Repository Images）] を選択し、リストにイメージを表示します。

ヒント 複数のイメージを選択して、それらを右クリックしてコンテキストメニューを使用して一度にダウンロードすることもできます。

ヒント 更新時刻でリストをソートすることで、最新のイメージを簡単に見ることができます。

ステップ 2 ローカルファイルシステムからイメージをダウンロードするには、次の手順を実行します。

a) [リポジトリイメージ（Repository Images）] ビューのツールバーから、[イメージをファイルシステムからダウンロード（Download image from file system）] アイコン（左端）をクリックします。

[ファイルシステムからダウンロード（Download from File System）] ダイアログボックスが表示されます。

b) 参照機能を使用して、インポート場所を選択し、インポートするイメージを選択します。

c) [OK] をクリック

d) [イメージをファイルシステムからダウンロード（Download image from file system）] ダイアログボックスで [OK] をクリックします。

e) ダウンロードの経過表示を監視します。

（注） ダウンロードするイメージがリポジトリにすでに存在する場合、システムはエラーを表示します。

f) 完了したら、Security Manager でデバイスグループを選択し、リストのイメージを表示します。

ヒント 更新時刻でリストをソートすることで、最新のイメージを簡単に見ることができます。

g) または、ドラッグアンドドロップ方法を使用してイメージファイルをダウンロードすることもできます。たとえば、1つまたは複数のファイルをデスクトップからドラッグして、Image Manager アプリケーションにドロップするだけです。

バンドルの操作

バンドルとは、ユーザーが定義する互換性のあるイメージのグループです。バンドルを使用すると、事前に検証されたイメージをグループ化して論理グループとしてまとめて機能させることで、反復的な操作を簡素化できます。たとえば、ASA と ASDM のペアを反映するバンドルを定義して、1 回の操作で両方のタイプを展開することができます。次のタイプのイメージをバンドルの一部にすることができます。

- ASA システムソフトウェア
- ASDM イメージ
- VPN イメージ（csd、AnyConnect、Hostscan を含む）
- プラグイン（rdp、ssh、ica、owa などを含む）

複数のシステム ソフトウェア イメージを同じバンドルに含めることはできません。

注意 Image Manager は、バンドルの一部として互換性のないイメージを追加することを阻止しません。この互換性はユーザーが判断する必要があります。ASA と ASDM の互換性マトリックスは、http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html#wp42231 にあります。

ヒント Image Manager 全体で、1 つのイメージ、複数のイメージ、または（事前定義された）イメージのバンドルを適用するように選択できる操作があります。

ここでは、次の内容について説明します。

- バンドルの作成 （3765 ページ）
- バンドル別のイメージの表示 （3766 ページ）
- バンドルの名前変更 （3766 ページ）
- バンドルの削除 （3767 ページ）
- バンドルからのイメージの削除 （3767 ページ）

バンドルの作成

イメージのバンドルを定義して、 Image Managerを簡素化できます。バンドルは、定期的に操作するイメージのグループがある場合に特に便利です。

バンドルを作成するには、次の手順を実行します。

ステップ 1 セレクタの [バンドル（Bundles）] 見出しから、[バンドルの追加（Add Bundle）]（プラス記号）アイコンをクリックします。

ステップ 2 表示される [バンドルの作成（Create Bundle）] ダイアログボックスに、新しいバンドルの名前を入力します。

ステップ 3 [OK] をクリック

バンドルは、セレクタの [バンドル（ Bundles）] 見出しの下に一覧表示されます。

ステップ 4 セレクタの [イメージ（Images）] セクションから、バンドルするイメージを選択します。次に、[リリースノート（Release Notes）] タブをクリックします。最後に、該当するリリースノートの互換性テーブルを調べて、バンドルする他のイメージとの競合がないことを確認します。

注意 Image Manager は、バンドルの一部として互換性のないイメージを追加することを阻止しません。この互換性を判断するのはユーザの責任です。ASA と ASDM の互換性マトリックスは、http://www.cisco.com/en/US/docs/security/asa/compatibility/asamatrx.html#wp42231 にあります。

ステップ 5 互換性を判断したら、各イメージをバンドルにドラッグアンドドロップします。

（注） 複数のシステム ソフトウェア イメージを同じバンドルに含めることはできません。

ヒント ドラッグアンドドロップするイメージの範囲を選択するには、範囲の最初のイメージを選択し、Shift キーを押しながら範囲の最後のイメージを選択します。Ctrl キーを押しながらイメージをクリックすると、複数の画像を選択できます。イメージの範囲を選択してから、Ctrl キーを使用して選択した範囲にイメージを追加することもできます。複数のイメージを 1 つのバンドルに移動するには、マウスの右ボタンを使用してドラッグします。

バンドル別のイメージの表示

バンドルに追加されたイメージを表示できます。

バンドル内のイメージを表示するには、次のいずれかを実行します。

ステップ 1 すべてのバンドルに含まれるイメージを表示するには、次のように操作します。

a) セレクタの [バンドル（Bundles）] 見出しの下で、最上位の [バンドル（Bundles）] フォルダをクリックします。

すべてのバンドルが、それぞれに含まれるイメージとともにリストされます。

b) バンドルを展開したり折りたたんだりして、見やすくすることができます。すべてのバンドルを展開するか、すべてのバンドルを折りたたむには、メインウィンドウの上部にある [すべて展開（Expand All）] ボタンと [すべて折りたたむ（Collapse All）] ボタンを使用します。

ステップ 2 特定のバンドルの画像を表示するには、次のように操作します。

a) セレクタの [バンドル（Bundles）] 見出しの下で、バンドルを選択します。

選択したバンドルのイメージの一覧がメインウィンドウに表示されます。

ステップ 3 特定のバンドルを表示するには、次のように操作します。

a) セレクタの [バンドル（Bundles）] セクションで、[検索（Search）]（拡大鏡のアイコン）をクリックします。

b) [バンドル（Bundles）] バナーの下の検索フィールドにバンドル名を入力します。

バンドルのリストには、指定されたバンドルのみが表示されます。

バンドルの名前変更

バンドルの名前を簡単に変更して、編成を改善したり、バンドルの内容をより正確に反映したりできます。

バンドルの名前を変更するには、次の手順を実行します。

ステップ 1 セレクタの [バンドル（Bundles）] 見出しから、バンドルを選択します。

ステップ 2 バンドル名を右クリックし、ドロップダウンリストから [バンドル名の変更（Rename Bundle）] を選択します。

[名前の変更（Rename）] ダイアログボックスが表示されます。

ステップ 3 新しいバンドル名を入力します。

ステップ 4 [OK] をクリックします。

バンドルの下のセレクタに新しいバンドル名が表示されます。

バンドルの削除

不要になったバンドルは削除できます。

バンドルを削除するには、次の手順を実行します。

ステップ 1 バンドルを選択します。

ステップ 2 セレクタの [バンドル（Bundles）] 見出しから、[削除（Delete）]（赤い X アイコン）をクリックします。または、選択したバンドルを右クリックして、[バンドルの削除（Delete Bundle）] を選択します。

バンドルからのイメージの削除

バンドルの内容を変更する場合は、バンドルの一部として定義されているイメージを削除できます。

バンドルからイメージを削除するには、次の手順を実行します。

ステップ 1 バンドルを選択します。

ステップ 2 削除するイメージを右クリックします。

ステップ 3 [バンドルからイメージを削除（Delete Image from Bundle）] を選択します。または、テーブルの最上部にある [削除（Delete）] ボタンをクリックします。

デバイスの使用

次のトピックでは、Image Manager でのデバイスの操作方法について説明します。

（注） クラスタの場合、ストレージからのファイルのダウンロードをサポートしているのは制御ユニットだけです。

ここでは、次の内容について説明します。

- デバイス インベントリの表示 （3768 ページ）
- デバイス上のイメージの管理 （3770 ページ）
- デバイスメモリの表示 （3771 ページ）
- イメージのインストール場所の設定 （3772 ページ）

デバイス インベントリの表示

[デバイスの概要（Device Summary）] ページを使用して、ネットワーク上のデバイスとその属性をすばやく表示できます。

左側のセレクターパネル内には、[デバイス（Devices）] と呼ばれる領域があります。その領域から、[すべて（All）] を選択すると、すべてのデバイスを表示できます（または、定義した場所またはデバイスのグループを選択できます）。デバイス選択の範囲を選択すると、対応するデバイスが [デバイスの概要（Device Summary）] ページの上部パネルに表示されます。[デバイスの概要（Device Summary）] ページの上部ウィンドウには、必要に応じて、各デバイスの次の属性が表示されます。

- デバイスの表示名
- モード（たとえば、スタンドアロン、アクティブ-アクティブ。アクティブ-スタンバイ、クラスタ）
- システムの SW バージョン
- ASDM のバージョン
- AnyConnect のバージョン
- セキュアデスクトップのバージョン
- Hostscanのバージョン

[デバイスの概要（Device Summary）] テーブルには、[モード（Mode）] 列が含まれます。この列では、クラスタ、スタンドアロン、アクティブ-アクティブ、アクティブ-スタンバイなどのモードを指定します。

フェールオーバーやクラスタ設定のように、複数の物理デバイスがグループ化されている設定の場合、各物理ユニット/メンバーには独自のファイルシステムがあります。また、これらのファイルシステムは異なる場合があります。各物理デバイス/メンバーのファイルシステムの詳細は、Image Manager 内で表示できます。

ストレージやイメージのステータスなど、個々のクラスタメンバーの詳細は、Security Manager ユーザーインターフェイスに表示されます。イメージ管理インベントリデータの検出中に、各クラスタメンバーのストレージに関する詳細と実行中のイメージの詳細が検出されます。

[デバイスの概要（Device Summary）]ページでフェールオーバーまたはクラスタデバイスを選択すると、グループ内の個々の物理メンバーが中央のデバイスビューテーブルに表示されます。クラスタデバイスのデバイスビューテーブルには、クラスタメンバーに関する次の情報が表示されます。

- [名前（Name）]：デバイスまたはクラスタメンバーの名前。
- [ID]：クラスタメンバー ID。
- [ステータス（Status）]：クラスタ内のメンバーのロール。たとえば、クラスタコントロールまたはクラスタデータ。
- [シリアル番号（Serial Number）]：クラスタデバイスのシリアル番号。
- [実行中のOSバージョン（Running OS Version）]：特定のメンバーの OS のバージョン。
- [CCL IP]：クラスタリンクの IP アドレス。
- [CCL MAC]：クラスタリンクの MAC アドレス。
- [サイトID（Site ID）]：クラスタデバイスのサイト ID。

フェールオーバーデバイスのデバイスビューテーブルには、名前、ステータス（スタンバイまたはアクティブなど）、シリアル番号、RAM サイズ、および実行中の OS バージョンを含む列があります。フェールオーバー デバイス テーブルには、フェールオーバー ペア ノードのプライマリデバイスとセカンダリデバイスごとにこれらの要素が一覧表示されます。

[デバイスの概要（device summary）] ページで特定のデバイスを選択すると、下部のウィンドウに、そのデバイスの詳細に関する次のタブ付きページが表示されます。

- [概要（Summary）]：表示名、デバイスタイプ、IP アドレス、ホスト名、ドメイン名、シリアル番号、実行中の OS バージョン、ターゲット OS バージョン、RAM、フェイルオーバーモード、イメージのインストール場所
- [互換性のあるイメージ（Compatible Images）]：デバイスと互換性のあるオメージ（イメージ、タイプ、バージョン、場所、サイズ、説明、コメント）。
- [履歴（History）]：デバイスで実行されたイメージのインストールジョブおよび設定展開ジョブの時系列ビュー（ジョブ名、変更者、状態、最後のアクション、チケット）

中央の [デバイスビュー（Device View）] でフェールオーバーまたはクラスタデバイスの特定のメンバーを選択すると、下部のウィンドウに、その物理デバイスに関する次のタブ付きの詳細が表示されます。

- [概要（Summary）]：実行中の OS バージョン、ターゲット OS バージョン、RAM
- [ストレージ（Storage）]：フラッシュメモリユニットの数とキャパシティ。名前、サイズ、パス、タイプ、ディスク使用量

- [実行中のイメージ（Running Images）]：現在動作中のイメージ。名前、タイプ、バージョン、パス、サイズ

デバイス上のイメージの管理

[イメージ管理（Image Management）] ツールを使用して、選択した ASA デバイス上のイメージを確認、ダウンロード、および削除できます。

デバイス上の ASA イメージを確認、ダウンロード、または削除するには、次の手順を実行します。

ステップ 1 セレクタパネルの [デバイス（Devices）] 領域でデバイスグループを選択します。

メインウィンドウにデバイスの概要が表示されます。デバイスの概要には、デバイスおよび関連するシステムソフトウェアのバージョンが一覧表示されます。

ヒント または、[デバイス（Devices）] バナーから検索機能（虫眼鏡アイコン）を選択し、表示される検索フィールドにデバイス名を入力することもできます。

ステップ 2 [デバイスの概要（Device Summary）] ページの上部ペインから、デバイスを選択します。

（注） 特定のデバイスがクラスタの一部である場合、クラスタ内を移動してデバイスの詳細を表示できます。

下部ペインに、選択したデバイスの詳細が表示されます。

ステップ 3 下部ペインで [ストレージ（Storage）] タブを選択し、[ディスク使用量（Disk Usage）] に表示される空き容量を確認します。

（注） 特定のデバイスがクラスタの一部である場合、クラスタ内を移動してストレージの詳細を表示できます。

ヒント デバイスには、disk1 などの複数のストレージ領域がある場合があります。 下にスクロールして、セカンダリ（フラッシュ）ストレージ容量を確認してください。

ステップ 4 デバイスで使用可能なディスク領域を確認します。

ステップ 5 デバイスから 1 つまたは複数のイメージを削除してスペースを解放するには、[ストレージ（Storage）] タブで 1 つまたは複数の画像を選択し、[ストレージ（Storage）] タブの上部にある [削除（Delete）] をクリックします。

ヒント または、1 つまたは複数のイメージを選択し、右クリックして [削除（Delete）] をクリックします。

ヒント 現在アクティブであり参照されているイメージを削除すると、Image Manager に警告メッセージが表示されます。

ステップ 6 デバイスからイメージをダウンロードするには、イメージを選択し、[ストレージ（Storage）] タブの上部にある [ダウンロード（Download）] をクリックします。イメージのダウンロード先のローカルファイルシステム上の場所を選択し、[OK] をクリックします。

（注） クラスタデバイスの場合、イメージのダウンロードは制御ユニットでのみサポートされます。同様に、フェールオーバーデバイスの場合、イメージのダウンロードは、ペアのアクティブデバイスでのみサポートされます。

デバイスからのダウンロードの進行状況を示すダイアログが表示されます。ダウンロードが完了すると、ダウンロードしたイメージがエクスプローラに表示されます。

ステップ 7 下のペインで [互換性のあるイメージ（Compatible Images）] タブを選択します。

デバイスと互換性のあるイメージが表示されます。

ステップ 8 互換性のあるイメージをデバイスにインストールするには、次の手順を実行します。

a) デバイスに追加するイメージを選択します。

b) ダウンロードアイコンをダブルクリックします。

イメージがリポジトリにダウンロードされます。

c) イメージを選択し、コンテキストメニューから [インストール（Install）] を選択します。

インストールウィザードが表示され、イメージがインストールされます。詳細については、互換性のあるイメージのデバイスへのインストール （3786 ページ）を参照してください。

デバイスメモリの表示

Image Manager を使用して、ネットワーク内のデバイスのメモリ容量とアプリケーションを判断できます。

（注） メモリ容量は物理デバイスのみで表示でき、クラスタでは表示できません。

デバイスのメモリの詳細を表示するには、次の手順を実行します。

ステップ 1 セレクタパネルの [デバイス（Devices）] 領域から、調べるデバイスを選択します。

選択したデバイスの詳細は、[デバイスの概要（Device Summary）] ページの上部のウィンドウに表示されます。

ステップ 2 上部のパネルで、RAM のリストを調べます。

注意 新しいイメージをロードするのに十分な RAM がデバイスに存在しない場合、Image Manager は警告を表示します。ただし、システムはそのようなイメージアップグレードの実行を停止しません（これは、RAM が不足している場合に展開ジョブが停止する設定展開とは対照的です）。

イメージのインストール場所の設定

ASA デバイスには、すべてのイメージが存在するデフォルトのフラッシュ（disk0）があります。デフォルトでは、Image Manager はイメージを ASA デバイスの disk0 にコピーします。ASA デバイスが外部ディスク（つまり、disk1）で構成されている場合、Image Manager では、ASA デバイスにイメージをロードするときに、2 つのディスク（disk0 または disk1）のいずれかを選択できます。

（注） 外部ディスクにイメージをロードする機能は、AnyConnect 用や CSD 用などの大きなイメージを保存する場合に非常に役立ちます。これは、これらの大きなイメージがいくつかあるだけで disk0 の領域がすぐに不足する可能性があるためです。

外部ディスクを使用するように Image Manager を設定するには、次の手順を実行します。

ステップ 1 セレクタの [デバイス（Devices）] 領域でデバイスを選択します。

ステップ 2 右側のペインには、概要情報が表示されます。

デバイスで使用可能なディスクは、[イメージのインストール場所（ Image Install Location）] ドロップダウンリストに表示されます。外部ディスクを備えたデバイスの場合、disk0 と disk1 がリストされます。

ステップ 3 [イメージのインストール場所（ Image Install Location）] ドロップダウンリストから外部ディスク disk1 を選択し、[適用（Apply）] をクリックします。ユーザコンテキスト デバイスの場合、共有ラベルまたはプライベートラベルを選択して、デフォルトのインストール場所を適用できます。

このデバイスの今後のすべてのイメージインストールジョブでは、イメージは disk1 にロードされます。

ヒント 外部ディスクの構成は、イメージインストール操作を実行することで確認できます。ジョブが完了したら、Image Managerで、デバイスの [ストレージ（Storage）] タブの disk1 の内容を確認します。新しくインストールされたイメージが一覧表示されます。

（注） クラスタデバイスとフェールオーバーデバイス、およびマルチコンテキストデバイスの場合、一部の物理メンバーデバイスに、イメージのインストール場所として選択されたディスクがない場合、イメージをコピーまたはインストールしようとすると、検証エラーが発生します。イメージのコピーまたはインストールを続行するには、すべてのメンバーデバイスに存在するディスクをイメージのインストール場所として選択する必要があります。

Image Manager を使用したデバイスでのイメージの更新について

Image Manager が ASA デバイスのイメージを更新する仕組み

Image Manager は、標準の文書化された手順に従って、信頼性の高いイメージアップグレードを保証するためのいくつかの組み込みチェックを使用して、スタンドアロン ASA デバイスをアップグレードします。イメージのアップグレード手順については、http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008067e9f9.shtml#maintask2 を参照してください。

（注） Image Manager が cisco.com に接続できるようにするには、最新の Cisco.com 証明書を受け入れている必要があります。イメージのダウンロードを正常に開始するには、「イメージメタデータロケータ」サイトとイメージのダウンロードサイトの両方からの証明書を受け入れる必要があります（[Image Manager] ページ （695 ページ）を参照）。

Image Manager は、HTTPS プロトコルを使用してイメージを ASA デバイスにコピーし、設定変更を実行して新しいイメージをアクティブ化し（エラーが発生した場合の古いイメージへのフォールバックを保証）、最後に、必要に応じて新しいイメージでデバイスをリロードします。

Image Manager がフェールオーバー用に設定された ASA のイメージを更新する仕組み

アクティブ/スタンバイ フェールオーバー ペアのイメージを更新するには、ペアのアクティブ デバイスでイメージ アップグレード ジョブを作成し、そのイメージ アップグレード ジョブを実行します。

アクティブ/アクティブ フェールオーバー ペアでのイメージの更新は、Image Manager ではサポートされていません。アクティブ/アクティブ フェールオーバー ペアの場合は、一方のユニットですべてのフェールオーバーグループをアクティブにし、他方のユニットで対応するフェールオーバーグループをスタンバイにすることによって、アクティブ/スタンバイに変換する必要があります。その後にのみ、Image Manager は、デバイスのペアのイメージを更新できます。

アクティブ/アクティブ フェールオーバー ペアのデバイスをアップグレードするには、次の手順を実行します。

1. すべてのフェールオーバーグループを一方のデバイスで**アクティブ**にし、他方のデバイスで**スタンバイ**にすることによって、ペアをアクティブ/スタンバイに手動で変換します。

（注） Security Manager でデバイスを検出しないでください。

（注） アクティブ/アクティブ フェールオーバー ペアをアクティブ/スタンバイに変換する方法の詳細については、http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b20f35.shtml#Actact を参照してください。

2. ペアのアクティブデバイスでイメージアップグレードジョブを作成し、そのイメージアップグレード ジョブを実行します。
3. アップグレードの実行後に、必要なフェールオーバーグループを一方のユニットでアクティブにし、残りのフェールオーバーグループを他方の物理ユニットでアクティブにして、アップグレード前と同じように、ペアを手動でアクティブ/アクティブ構成に戻します。
4. Security Manager で、スタンバイに変換したユニットのデバイスインベントリのみを再検出します。

Image Manager は、http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a0080b20f35.shtml で説明されているアップグレード手順に従います。イメージが両方のユニットにコピーされ、設定変更が実行されて、両方のユニットに同期されたイメージがアクティブ化されます。最初に、スタンバイがアクティブユニットを介してリロードされ、スタンバイが新しいバージョンに正常にアップグレードされたことが確認された後に、現在のアクティブがリロードされます。両方のユニットが新しいバージョンにアップグレードされると、フェールオーバーペアまたはクラスタのアップグレードは成功とマークされます。

（注） 現在のアクティブのリロード中は、スタンバイ ASA が引き継ぐまで、フェールオーバーペアを通過するトラフィックが影響を受けます。

フェールオーバー ASA ペアでのイメージアップグレードには制限があります。Image Manager を使用してフェールオーバー ASA ペアまたはクラスタでイメージアップグレードを実行するときは、次の制限が満たされていることの確認をお勧めします。

- フェールオーバー コンフィギュレーション内の 2 つの装置は、メジャー（最初の番号）およびマイナー（2 番目の番号）のソフトウェア バージョンが同じになるようにします。
- **メンテナンスリリース**：任意のメンテナンスリリースを、マイナーリリース内の他のメンテナンスリリースにアップグレードできます。たとえば、中間のメンテナンス リリースをあらかじめインストールしなくても、7.0（1）から 7.0（4）にアップグレードできます。
- **マイナーリリース**：マイナーリリースから次のマイナーリリースにアップグレードできます。**マイナー リリースはスキップできません。**たとえば、7.0 から 7.1 にアップグレードできます。ただし、ゼロダウンタイム アップグレードでは 7.0 から 7.2 への直接のアップグレードはサポートされておらず、まず 7.1 にアップグレードする必要があります。

- **メジャーリリース**：前のバージョンの最後のマイナーリリースから次のメジャーリリースにアップグレードできます。たとえば、7.9 が 7.x リリースの最後のマイナー バージョンであれば、7.9 から 8.0 にアップグレードできます。

Image Manager が ASA クラスタのイメージを更新する仕組み

イメージの更新では、ヒットレスアップグレードのために以前に確立された手順に従います。これにより、確実に、トラフィックフローに影響を与えることなく、クラスタのすべてのメンバーが 1 回のユーザー操作で新しいバージョンにアップグレードされます。イメージのアップグレード時には、次のような動作が実行されます。

- クラスタのデータユニットには、最初に、制御ユニットから新しいイメージがロードされます。制御ユニットのみに接続されている場合、イメージがクラスタのすべてのメンバーにコピーされます。クラスタを介したそのような伝播では、各デバイスのスイッチオーバーによってユニットのステータスを制御する必要がないため、トラフィックの中断が最小限に抑えられます。
- 新しいイメージをロードする起動コマンドを追加するために、制御ユニットで設定が変更されます。制御ユニットで設定が変更されると、すべてのデータユニットで自動的に同期されます。
- すべてのデータユニットが、制御ユニットを介して新しいイメージで順番に再起動します。
- すべてのデータユニットがオンラインになり、クラスタに再参加します。
- その後、制御ユニットがデータユニットになります（次のデータユニットが制御ユニットの役割を引き継ぎます）。
- 新しい制御ユニットを介して、古い制御ユニットに新しいイメージが再ロードされます。

Image Manager がこのイメージ更新手順に従うことで、スイッチオーバーが最小限になり、トラフィックの中断が最小限になります。

イメージ更新中および更新後のデバイス状態の変化

イメージのアップグレードは重要な操作であるため、すべてのイメージ更新操作が視覚的に表現され、ユーザーに通知される必要があります。そのため、次の 3 つの新しいデバイス状態が導入されました。

- [アップグレード中（Upgrade In Progress）]：デバイスでイメージインストールジョブが開始されるたびに、デバイスはこの状態になります。デバイスでイメージ更新操作が完了すると、この状態はシステムによって自動的にリセットされます。
- [メンテナンス（Maintenance）]：デバイスでイメージインストールジョブが失敗し、イメージインストール操作後にデバイスに到達できなくなると、デバイスはメンテナンス状態になります。アップグレードによって発生した問題を手動で修正するかイメージをロールバックすることによって、デバイスをオンラインに戻すために必要な手順を実行した後に、この状態を手動で正常/動作状態にリセットする必要があります。

- [設定が必要（Configuration Required）]：特定のケースのイメージアップグレード（ASA 8.2 から ASA 8.3 など）では、イメージアップグレードの一部としてデバイス設定が大幅に変更されるため、Security Manager のポリシー設定モデルがデバイス設定との互換性をなくします。このような場合は、イメージアップグレード操作が成功しても、アップグレード後に Security Manager の設定ポリシーモデルとデバイス設定が連携していることを確認するために、デバイスの再検出などのいくつかの操作を実行する必要があります。そのため、イメージのアップグレード後に、デバイスを動作させるために Configuration Manager で追加の設定が必要である場合、デバイスは [設定が必要（Configuration Required）] 状態になります。Image Manager を使用して VPN イメージが展開されている場合でも、ユーザーは Configuration Manager を使用して VPN ポリシーでこれらのイメージを設定する必要があるため、デバイスは [設定が必要（Configuration Required）] 状態になります。[設定が必要（Configuration Required）] 状態は、イメージ更新操作後にデバイスを Security Manager で機能させるために Configuration Manager で変更を行う必要があることを示しています。提示される変更を行うことができ、設定の変更に問題がないことを確認できたら、デバイスを手動で [動作（Operational）] 状態に戻すことができます。

（注） デバイスを [設定が必要（Configuration Required）] モードにできる他のシナリオについては、イメージ管理のトラブルシューティング （3794 ページ）を参照してください。

デバイスの状態がこれらの 3 つの状態のいずれかに変化するたびに、その状態がデバイスセレクタに明示的なアイコンで示されます。このデバイス状態の変化は、Configuration Manager と Image Manager の両方で確認できます。デバイスでイメージ更新操作がないときのデバイスの正常な状態は [動作（Operational）] 状態です。

ヒント デバイスの状態を正常な状態（つまり、[動作（Operational）]状態）に手動でリセットするには、Configuration Manager または Image Manager のデバイスセレクタでデバイスを選択し、右クリックして、[デバイスを動作させる（Make Device Operational）] を選択します。

ここでは、次の内容について説明します。

- デバイスで提案されたイメージの更新を検証する （3777 ページ）
- Image Installation ウィザードを使用してデバイスにイメージをインストールする （3780 ページ）
- バンドルされたイメージをデバイスにインストールする （3786 ページ）
- 互換性のあるイメージのデバイスへのインストール （3786 ページ）
- 選択したデバイスにイメージをインストールする （3788 ページ）

デバイスで提案されたイメージの更新を検証する

実際に実行する前に、1 つ以上のデバイスでイメージ更新ジョブを検証できます。次のリストは、実行されるさまざまな検証の詳細を示しています。

- ASA デバイスに選択したイメージを収容するための十分なディスクスペースがありません。

この場合、エラーが表示されます。そのデバイスの [ストレージ（Storage）] タブに移動し、1 つ以上のイメージを削除してスペースを確保する必要があります。次に、アップグレードの検証操作を再試行します。

（注） クラスタ内の各メンバー、およびフェールオーバー内のアクティブユニットとスタンバイユニットの両方のディスクスペースについて、選択されたイメージを収容するのに十分なスペースがあるかどうかが評価されます。1 つのメンバーまたはデバイスに十分なスペースがない場合、エラーが表示され、そのデバイスでのジョブの作成に進むことができません。その特定のメンバーの [ストレージ（Storage）] タブに移動し、1 つ以上の不要なイメージを削除してスペースを確保する必要があります。

- デバイスで新しいイメージを実行するのに十分な RAM がありません（Cisco ASA 5500 シリーズ 8.4(x) のリリースノートでの推奨による）。

（注） 新しいイメージをロードするのに十分な RAM がデバイスにない場合、Image Manager は警告を表示します。ただし、これによってイメージのアップグレードの実行が停止することはありません。これとは対照的に、設定展開では RAM が不足している場合に展開ジョブが停止します。

- イメージのインストール場所として選択されたフラッシュデバイス（disk0 または disk1）が、クラスタ/フェールオーバー セットアップのデバイス/メンバーのいずれにも存在しない場合、エラーが表示され、ジョブは中止されます。
- 送信されたがまだデバイスに展開されていない設定変更。これらの変更は、イメージ更新ジョブを開始する前に展開する必要があります。そうしないと、設定の変更とデバイス上のアップグレードされたイメージバージョンの互換性がなくなる可能性があります。
- 選択したイメージがデバイスタイプと互換性がない場合、たとえば、非 SMP イメージが ASA 5585 デバイスタイプに選択されている場合、警告を行います。

（注） この警告は、ドラッグアンドドロップ方法を使用している場合にのみ発生します。他のフローの場合、互換性のないイメージ/デバイスは、イメージインストール ウィザードのステップ 2 で除外されます。

（注） Cisco Security Manager 4.3 では、MDF ID と互換性のある Cisco.com 上のイメージに関するメタデータ情報が利用できないことが原因で更新のチェックが実行されない場合、この検証はスキップされていました。Cisco Security Manager 4.4 では、メタデータ情報は Cisco Security Manager のインストールに事前にパッケージ化されているため、更新のチェックが実行されていない場合でも、イメージマネージャーはデバイスタイプのイメージの互換性を検証し、互換性のないイメージとデバイスの組み合わせが選択された場合は、ユーザーに警告します。

- デバイスが Security Manager でサポートされていないバージョンに更新されている場合、警告を行います。
- 新しいイメージバージョンがデバイスで実行されているバージョンと同じまたはそれより低い場合、警告を行います。
- 下位バージョンから ASA バージョン 8.3 へのイメージアップグレードでは、デバイスを Security Manager で再検出する必要があります。ASA バージョン 8.3 で導入された NAT 設定では、以前の ASA バージョンと互換性のない大きな変更が加えられています。同様に、バージョン 8.3 の Security Manager では、NAT ポリシーモデルが大きく変更されています。したがって、デバイスが ASA 8.3 にアップグレードされると、そのデバイスは設定が必要な状態になり、デバイスを動作させるには Configuration Manager でいくつかの変更を加える必要があることが、 Configuration ユーザーに示されます。Security Manager でデバイスを再検出した後、デバイスツリーでデバイスを右クリックし、[デバイスを動作させる（Make Device Operational）] を選択して、デバイスを通常の状態に戻すことができます。
- ASA バージョン 8.3.x から 8.4.2 以降のバージョンへのイメージアップグレードでも、ASA バージョン 8.4.2 の PAT 設定の変更に互換性がないため、Security Manager でデバイスを再検出する必要があります。この場合も、イメージのアップグレード後にデバイスの状態が設定が必要な状態に変更されます。
- ASA バージョン 8.x から 9.0.1 以降へのイメージアップグレードでは、ユニファイドアクセスルール、インスペクション、および NAT ルールの変更に互換性がないため、Security Manager でデバイスを再検出する必要があります。
- ASA バージョン 7.x から 8.x へのイメージアップグレードにより、デバイスと Security Manager の両方の SSLVPN 設定に大きな変更が導入されます。これらの変更に互換性がないため、イメージのアップグレード後にデバイスを Security Manager から削除してから、再度追加する必要があります。デバイスは設定が必要な状態になり、これらの警告に対処するようにユーザーに通知されます。
- AnyConnect、CSD、または Hostscan イメージなどの VPN イメージが Image Manager を使用してロードされる場合、既存の VPN イメージが現在のデバイスまたは他のデバイスに割り当てられている共有ポリシーの一部であると、ユーザーに警告が発行されます。新しいイメージを共有ポリシーが割り当てられているすべてのデバイスにもコピーするよう警告が発行されます。そうすることで、ポリシー共有を失うことなく、すべてのデバイスに対して共有ポリシーをシームレスに更新できるようになります。

- フェールオーバーペアのスタンバイユニットに到達できない場合、警告を行います。これは、ジョブの中止を引き起こすエラーです。
- アクティブ/スタンバイ フェールオーバー ペアのアップグレードに関する警告。アップグレードされるバージョンは、ASA/PIX：CLIを使用してフェールオーバーペアのソフトウェアイメージをアップグレードする方法[英語]の推奨事項に準拠している必要があります。

（注） 同じ警告は、クラスタ設定の ASA にも当てはまります。

- アクティブ/アクティブ フェールオーバー ペアのアップグレードに関する警告。ペアがアクティブ/スタンバイに変換されない限り（つまり、1 つの物理ユニットですべてのフェールオーバーグループがアクティブである場合）、イメージ更新ジョブが中止されます。

（注） 指定された制御ユニットである「デバイス」には、追加の検証が必要です。アクティブ/スタンバイフェールオーバーの場合と同様のチェックに加えて、クラスタイメージがサポートされているプラットフォームと互換性があるかどうかもチェックします。クラスターを 9.x 未満のバージョンにダウングレードすることはできません。

イメージのインストールを検証するには、次の手順を実行します。

ステップ 1 [ファイル（File）] メニューの [検証（Validate）] を選択します。

[イメージ割り当ての検証（Validate Image Assignments）] ウィンドウが開きます。

ステップ 2 [ロール割り当ての追加（Add role assignment）] をクリックします。

[イメージの割り当て（Image Assignments）] ウィンドウが開きます。

ステップ 3 [イメージの割り当て（Image Assignments）] ウィンドウで、ドロップダウンリストから次のいずれかを選択します。

- イメージを選択してデバイスに割り当て（Select Images and Assign to Devices）
- デバイスを選択してイメージに割り当て（Select Devices and Assign to Images）

ヒント イメージをデバイスに割り当てても、デバイスをイメージに割り当てても、得られる結果は同じです。

ステップ 4 1 つ以上のアイテム（イメージまたはデバイス）を右側のウィンドウに移動して選択します。

ヒント [バンドル（Bundles）] をクリックしてバンドルを選択すると、イメージではなく事前定義されたバンドルを使用できます。

ステップ 5 [次へ（Next）] をクリックして、他の項目（イメージまたはデバイス）を割り当てます。

[割り当ての確認（Confirm Assignments）] ウィンドウが表示されます。

ステップ 6 指定した割り当てを確認し、確定します。

ヒント 必要に応じて、引き続き割り当てを追加または削除できます。

ステップ 7 [終了（Finish）] をクリックします。

[割り当ての検証（Validate Assignments）] ウィンドウが表示されます。

ステップ 8 [検証の開始（Start Validation）] をクリックします。

割り当ての検証ステータスは、[検証（Validation）] 列に表示されます。警告、成功、またはエラーのいずれかが表示されます。

ステップ 9 警告、成功、またはエラーの表示をクリックします。

ウィンドウの下側ペインが開きます。

ステップ 10 検証ステータスに従って、次のいずれかを実行します。

- [エラー（Error）]：エラーの考えられる原因を調べ、必要に応じて修正します。
- [警告（Warning）]：警告の潜在的な理由を調べ、必要に応じて修正します。
- 成功 — 対処不要です。

ヒント 右側のウィンドウスライダーバーを使用して、すべてのエラーまたは警告を表示して確認してください。

ステップ 11 表示された警告またはエラーに対処したら、[イメージのインストール（Image Install）] ウィザードを使用してジョブの作成に進むことができます。

ステップ 12 必要に応じて、[イメージ割り当ての検証（Validate Image Assignments）] ウィンドウで割り当て要素を右クリックし、続行する前に変更または削除できます。

ステップ 13 割り当てを右クリックして、[テーブルのコピー（Copy Table）] を選択することもできます。これにより、割り当ての詳細および検証ステータスとメモがコピーされます。その後、その内容をメモ帳などのプログラムに CSV ファイルとして貼り付けて、参照することができます。

Image Installation ウィザードを使用してデバイスにイメージをインストールする

この機能を使用して、デバイスにイメージを割り当ててインストールするジョブを作成できます。割り当ては、インストールジョブを定義するイメージとデバイスの単純な関連付けです。

（注） ワークフロー機能をイネーブルにしている場合は、インストールを完了する前に、説明されている追加の手順を実行して承認を取得する必要があります。

（注） 任意のデバイス セットを操作するように選択できます。

デバイスにイメージをインストールするジョブを作成するには、次の手順を実行します。

ステップ 1 [ファイル（Files）] > [イメージのインストールウィザードを開く（Open Image Installation Wizard）] に移動します。

イメージのインストール（Image Installation）ウィザードが表示されます。

ヒント イメージのインストール（Image Installation）ウィザードは、いくつかの方法で呼び出すことができます。ここで説明したメニューからのウィザードの呼び出しに加えて、次のいずれかを実行するときにウィザードを呼び出すことができます。（1）ドラッグアンドドロップによるイメージのインストール。（2）デバイスまたはバンドルを右クリックする。または（3）デバイスを選択し、[互換性のあるイメージ（Compatible Image）] タブに移動し、テーブルから 1 つ以上のイメージを選択して右クリックし、[インストール（Install）] オプションを選択する。

ステップ 2 左下の [割り当ての追加（Add Assignment）] をクリックします。

[イメージの割り当て（Image Assignments）] ダイアログボックスが表示されます。

ステップ 3 上部のドロップダウンリストから、イメージをデバイスに割り当てるか、デバイスにイメージを割り当てるかを選択します。

ステップ 4 項目（デバイスまたはイメージ）を左側のリストから右側の選択済みアイテムのリストに移動します。次に、[次へ（Next）] をクリックします。[バンドル（Bundles）] タブをクリックして、イメージの代わりにバンドルを選択することもできます。

ヒント 割り当てを定義するためにイメージとデバイスをペアリングする場合、イメージの後にデバイスを、またはデバイスの後にイメージを操作できます。この選択の順序は重要ではありません。

ステップ 5 [割り当ての確認（Confirm Assignments）] ダイアログボックスで割り当ての定義を確認し、[完了（Finish）] をクリックします。

ヒント この時点で、必要に応じて、[割り当ての追加（Add Assignment）] をクリックして、割り当てペアをさらに追加することもできます。

ステップ 6 割り当ての定義が終了したら、[検証の開始（Start Validation）] をクリックします。[検証の完了（Validation Complete）] が表示されるまで待ちます。

ステップ 7 [ウィザード（Wizard）] ダイアログボックスの [割り当て（Assignments）] タブにある [検証（Validation）] 列のステータスを調べます。警告、成功、またはエラーのいずれかが表示されます。

ステップ 8 ステータスに応じて必要な手順を決定します。

- エラー — エラーの考えられる原因を調べ、必要に応じて修正します。
- 警告 — 警告の潜在的な理由を調べ、必要に応じて修正します。
- 成功 — 対処不要です。

ステップ 9 その他のオプションについては、割り当てを右クリックします。

- [上に移動（Move Up）]/[下に移動（Move Down）]：デバイスが更新される順序を変更する場合は、複数デバイスのジョブに対してこれらのオプションを選択します。[イメージをデバイスにインストール（Install Images to Devices）] ジョブオプションが [逐次（Sequential）] に設定されている場合、この機能を使用して、デバイスの順序付けを行うことができます。
- [削除（Delete）]/[すべて削除（Delete All）]：これらのオプションを選択して、1 つまたはすべてのデバイスをイメージ アップグレード ジョブから削除します。
- [テーブルをコピー（Copy Table）]：これを使用して、警告メッセージをテキストエディタまたはスプレッドシートプログラムにコピーして参照します。
- [ファイルコピーのテスト（Test File copy）]：このオプションを使用して、https プロトコルを使用して Security Manager イメージリポジトリと ASA デバイスのフラッシュの間でファイルをコピーできるかどうかを確認します。

ヒント 右側のウィンドウスライダバーを使用して、すべてのエラーまたは警告を表示して確認してください。

ステップ 10 特定の時刻にインストール ジョブをスケジュールする場合は、[スケジュール（Schedule）] タブを選択し、日付と時刻を指定します。

ステップ 11 インストールジョブのプロパティを設定するには、[プロパティ（Properties）] タブを選択します。

a) 必要に応じて、[名前（Name）] を編集します（デフォルトは Image install Job—<timestamp>）。

b) 必要に応じて、[説明（Description）] を追加します。

c) 必要に応じて、[チケットID（Ticket ID）] を選択します。

ヒント リリース 4.4 以降、Image Manager の [チケットID（Ticket ID）] フィールドは Config Manager から切り離されました。現在は単なる「タグ」であり、任意の文字列にすることができます。[チケットID（Ticket ID）] フィールドは、Image Manager と Configuration Manager の両方で以前に作成されたチケットを表示するオートコンプリート機能付きの編集可能なコンボ ボックスです。また、[チケットID（Ticket ID）] フィールドについては、Configuration Manager のチケットモードに依存しません。[チケットID（Ticket ID）] はオプションのフィールドで、空白のままにすることができます。Configuration Manager のグローバル検索は、Image Manager で使用されるチケットもサポートし、チケットが関連付けられているイメージインストールジョブを一覧表示します。

d) [エラー時（On Error）] オプションを設定します（デフォルトは [インストールの停止（Stop Installation）]、代替は [操作の続行（Continue Operation）] です）。

e) [現在のイメージをバックアップ（Backup Current Image）] オプションを設定します（デフォルトは [はい（Yes）]、代替は [いいえ（No）] ）。

ヒント これは、システム ソフトウェア イメージにのみ適用されます。

f) [イメージをデバイスにインストールする方法（Install images to devices in）] オプションを設定します（デフォルトは [並列（Parallel）]、代替は [逐次（Sequential）]）。

g) 次の 3 つの操作のいずれかを選択します。

- イメージのインストールとデバイスの再起動
- イメージをインストールするが、デバイスを再起動しない
- イメージのデバイスへのコピーのみ
  - [非侵入型：フェールオーバーをトリガーしない（Non-Intrusive: Does not trigger failover）] チェックボックスをオンにして、フェールオーバー デバイスを切り替えずにイメージをコピーします。

h) ワークフローを使用している場合は、オプションで次の承認オプションを構成できます。

ヒント これらは、ジョブのジョブプロパティの上部フレームにあります。

- [アクション（Action）] :
- 承認（Approve）
- 拒否（Reject）
- [展開（Deploy）]
- 送信

ジョブを拒否すると、ステータスは [拒否（Rejected）] に設定され、その後ジョブは破棄されます。ジョブを破棄すると、ステータスは [破棄（Discarded）] として表示され、ジョブのすべてのアクションボタンが無効になります。

ジョブを承認すると、ステータスは [承認済み（Approved）] に設定されます。次に、[展開（Deploy）] をクリックして、イメージ アップグレード ジョブを開始する必要があります。

i) バージョン 4.12 以降、Security Manager には、ソフトウェアバージョン 9.6(2) 以降を実行している ASA マルチコンテキストデバイスのストレージ URL を選択するオプションが用意されています。選択したユーザコンテキストに対して、共有またはプライベートの ストレージ URL を選択できます。デフォルトでは、[共有（Shared）] が選択されています。

ヒント [詳細（Details）]タブを選択して [進行状況を表示（Show Progress）] をクリックすると、実行中の状況を確認できます。

ジョブを展開すると、ジョブのステータスが [展開済み（Deployed）] または [失敗（Failed）] として表示されます。下部ペインの [履歴（History）] タブ（選択したジョブの情報）のみが WF モードでアクティブ化され、次の 2 つのジョブアクションフローのいずれかが表示されます。

- 作成/編集中/送信済み/却下済み/破棄済み
- 作成/編集中/送信済み/承認済み/展開中/展開済み（または失敗）
- [ジョブを送信（Submit the job）] : これはデフォルトでオンになっています
- [承認者の電子メール（Approver email）] : 承認者の電子メールアドレスリスト
- [送信元の電子メール（Submitter email）] : ジョブを送信する担当者の電子メールアドレス。

j) [編集（Edit）] をクリックして、ジョブのプロパティを変更できます。
k) その他のジョブ表示オプションについては、インストールジョブの表示 （3790 ページ）を参照してください。

ステップ 12 [Install（インストール）] をクリックします。

[ジョブ（Jobs）] ページが表示され、インストールジョブのステータスが [展開中（Deploying）] として表示されます。

（注） ジョブのスケジュールが選択されている場合、ジョブの状態は[スケジュール済み（Scheduled）] と表示されます。ジョブはスケジュールされた時刻に展開を開始し、その時点でジョブの状態が [展開中（Deploying）] に変わります。

（注） イメージインストールジョブに対してワークフローがイネーブルになっている場合、ジョブの状態は [送信済み（Submitted）] または [編集中（Edit-in-Use）] のいずれかに変更されます。このモードでは、承認された後にのみジョブを展開できます。ワークフローモードでのジョブの状態については、イメージインストールジョブの承認ワークフロー （3793 ページ）を参照してください。

ヒント [中断（Abort）] をクリックすると、ジョブを中断できます。インストールジョブの中断に関する重要な情報については、イメージインストールジョブの中止 （3791 ページ）を参照してください。[破棄（Discard）] をクリックすると、スケジュールされた実行時間の前にジョブを破棄できます。

ステップ 13 ジョブの展開が開始されると、Configuration Manager および Image Manager のデバイスツリーで、デバイスの状態が [更新処理中（Update in progress）] 状態に変化することに注意してください。デバイスツリーのデバイスの横に、緑色の進行状況アイコンが表示されます。

ステップ 14 ジョブが展開中の状態の間、ジョブの詳細と進行状況を表示します。詳細については、インストールジョブの表示 （3790 ページ）を参照してください。

ステップ 15 ジョブが完了するまで待ちます。

すべてのデバイスが正常に更新されると、ジョブの状態が [展開済み（Deployed）] に変わります。ジョブの 1 つ以上のデバイスが失敗した場合、ジョブの状態は [失敗（Failed）] に変更されます。

ステップ 16 ジョブが完了した後、デバイスツリー内のデバイスの状態の変化に注目してください。

イメージの更新が成功し、Configuration Manager でそれ以上の構成変更が必要ない場合、デバイスは [動作中（Operational）] 状態に戻ります。更新後にデバイスで構成の変更が必要な場合、デバイスは [構成が必要（Configuration Required）] 状態に移行します。デバイスツリーでデバイスをクリックすると、状態の詳細とデバイスの状態を [動作中（Operational）] に戻すために実行する必要があるアクションを含むバルーンヒントが表示されます。デバイスでイメージの更新が失敗し、イメージの更新中にデバイスが到達不能状態になった場合、デバイスは [メンテナンス（Maintenance）] 状態になります。

ステップ 17 イメージの更新を検証します。

a) Image Manager のデバイスツリーでデバイスをクリックします。
b) [概要（Summary）] タブに移動して、更新された実行中の OS バージョンを表示します。
c) [実行中のイメージ（Running Images）] タブに移動して、イメージ更新後の新しい実行中のイメージを表示します。

d) Configuration Manager でデバイスを選択します。
e) デバイスを右クリックして、[デバイスのプロパティ（Device Properties）] を選択します。
f) [実行中のOSバージョン（Running OS Version）] フィールドで、更新された新しいイメージバージョンを確認します。
g) [Configuration Manager] > [管理（Manage）] > [構成アーカイブ（Configuration Archive）] に移動します。
h) デバイス CLI から、**sh ver** と入力します。

   更新された OS バージョンが表示されます。

i) 左側のデバイスツリーでデバイスを選択します。
j) 右側のペインで構成アーカイブのバージョンを表示し、アーカイブソースが Image Manager である最新のエントリを確認します。
k) アーカイブされたエントリを選択し、[View（表示）] をクリックします。
l) このエントリを以前のアーカイブバージョンと比較して、イメージの更新中に Image Manager によって行われた構成の変更を表示します。新しい ASA システム ソフトウェア イメージの先頭に追加されているブートコマンドや、新しい ASDM イメージに追加されている ASDM イメージコマンドを表示できます。
m) Image Manager の管理設定で電子メール通知が設定されている場合、イメージアップグレードジョブのステータスが含まれた電子メール通知が、設定された受信者に送信されます。

ステップ 18 イメージの更新操作後にデバイスが [構成が必要（Configuration Required）] または [メンテナンス（Maintenance）] の状態に設定されている場合は、次の手順に従って Configuration Manager でイメージ更新後に必要な操作を完了して、デバイスが機能するようにします。

a) Configuration Manager または Image Manager のデバイスツリーでデバイスをクリックします。

   デバイス情報を示すバルーンヒントが表示されます。

b) バルーンヒントの内容を確認します。デバイスが [構成が必要（Configuration Required）] または [メンテナンス（Maintenance）] 状態に設定されている理由を確認します。推奨される措置も確認します。
c) 推奨される処置を実行します。
d) デバイスツリーでデバイスを右クリックし、[デバイスを動作状態にする（Make Device(s) Operational）] を選択します。

   デバイスは [動作中（Operational）] 状態に移行し、デバイスツリーのデバイスの横にあるアイコンが削除されます。

   （注） アプライアンスモードで動作している Cisco Firepower 1000 および 2000 シリーズ デバイスのインストールジョブを開始する前に、[プロパティ（Properties）] パネルの [現在のイメージをバックアップ（Backup Current Image）] フィールドで [いいえ（No）] オプションを選択する必要があります。

バンドルされたイメージをデバイスにインストールする

Image Manager ツールを使用して、バンドルとしてグループ化された互換性のあるイメージを割り当ててインストールできます。バンドルによって、反復操作が簡素化されるとともに、デバイスのグループでの一貫したアクションの実行を可能にします。

デバイスまたはデバイスグループにイメージバンドルを選択的にインストールするには、次の手順を実行します。

ステップ 1 バンドルをデバイスまたはデバイスグループにドラッグアンドドロップします。

[デバイスにイメージをインストール（Install images on devices）] ダイアログボックスが表示され、バンドル内のデバイスとイメージが事前に割り当てられます。バンドルをデバイスグループにドロップすると、グループ内のすべてのデバイスが自動的に選択され、バンドル内のイメージに割り当てられます。

ステップ 2 [デバイスにイメージをインストール（Install images on devices）] ダイアログボックスに表示されている割り当て検証エラーまたは警告を調査します。

ヒント ジョブをスケジュールし、ジョブのデフォルトプロパティを変更することもできます。ジョブのスケジュール設定とジョブプロパティの設定の詳細については、Image Installation ウィザードを使用してデバイスにイメージをインストールする （3780 ページ）を参照してください。

ステップ 3 警告が修正されたら（または警告が重要ではないと判断したら）、[インストール（Install）] をクリックします。

（注） または、バンドルを右クリックして [インストール（Install）] を選択し、バンドルが事前に選択された状態でイメージインストールウィザードを起動することもできます。次に、デバイスを選択し、[インストール（Install）] をクリックして、選択したデバイスにバンドルをインストールします。

互換性のあるイメージのデバイスへのインストール

Image Manager を使用して、互換性のあるイメージをデバイスにインストールできます。

デバイスまたはデバイスグループに 1 つ以上の互換性のあるイメージを選択的にインストールするには、次の手順を実行します。

ステップ 1 セレクタの [デバイス（Devices）] 領域でデバイスを選択し、[互換性のあるイメージ（Compatible Images）] タブに移動します。

ステップ 2 [互換性のあるイメージ（Compatible Images）] タブで、 リポジトリイメージを 1 つ以上選択します。

ステップ 3 選択したイメージを右クリックして、[インストール（Install）] をクリックします。

イメージのインストール（Image Installation）ウィザードが表示されます。選択したイメージが事前に割り当てられているか、[イメージの選択（Select Image）] ページの右側のペインに移動されています。

ステップ 4 [次へ（Next）] をクリックします。

ウィザードの [デバイスの選択（Select Devices）] ページが表示されます。

ステップ 5 インストール先のデバイスを選択し、[次へ（Next）] をクリックします。

ウィザードの [割り当ての確認（Confirm Assignments）] ページが表示されます。

ステップ 6 デバイスとイメージの割り当てを確認し、[完了（Finish）] をクリックします。

[選択したデバイスにイメージをインストール（Install images on selected devices）] ダイアログボックスが表示されます。デバイスとイメージが割り当てられています。

ステップ 7 [割り当て（Assignments）] タブの右上隅にある [検証の開始（Start Validation）] をクリックします。[デバイスにイメージをインストール（Install images on devices ）] ダイアログボックスに表示されている割り当て検証エラーまたは警告を調査します。

バージョン 4.9 以降の Security Manager には、デバイスにイメージをインストールするための拡張された検証手順があります。

- Image Manager を使用して CCO からイメージをダウンロードした場合は、イメージをデバイスにインストールする前に、デバイスのシリアル番号がサービス契約に対して検証されます。デバイスに有効なサービス契約がある場合、イメージのインストールまたはアップグレードプロセスが続行されます。デバイスに有効なサービス契約がない場合、イメージのインストールまたはアップグレードプロセスは続行されません。
- ローカルファイルシステムから Image Manager にイメージをコピーした場合、サービス契約の検証はデバイスに対して実行されず、デバイスへのイメージのインストールに進むことができます。

ヒント ジョブをスケジュールできます。また、ジョブのデフォルトプロパティを変更することもできます。ジョブのスケジュール設定とジョブプロパティの設定の詳細については、 Image Installation ウィザードを使用してデバイスにイメージをインストールする （3780 ページ）を参照してください。

ステップ 8 警告が修正されたら（または警告が重要ではないと判断したら）、[インストール（Install）] をクリックします。

イメージのインストールジョブが作成されます。ジョブの進行状況を監視し、イメージの更新を確認するための残りの手順については、 Image Installation ウィザードを使用してデバイスにイメージをインストールする （3780 ページ）を参照してください。

（注） または、デバイスまたはデバイスグループに 1 つ以上のイメージをインストールするには、リポジトリビューから複数のイメージをドラッグし、デバイスまたはデバイスグループにドロップします。次に、[インストール（Install）] をクリックして、選択したイメージを選択したデバイスにインストールします。

選択したデバイスにイメージをインストールする

Image Manager を使用して、選択した一連のデバイスのイメージをアップグレードできます。

選択した一連のデバイスにイメージをインストールするには、次の手順を実行します。

ステップ 1 セレクタの [デバイス（Devices）] 領域でデバイスグループを選択します。

ステップ 2 右側のペインにグループ内のデバイスのリストを表示します。

ステップ 3 リストから 1 つ以上のデバイスを選択します。

ヒント 複数のデバイスを選択するには、Shift キーと Ctrl キーを使用します。

ステップ 4 選択したデバイスを右クリックして、[インストール（Install）] をクリックします。

Image Installation ウィザードが表示されます。選択したデバイスが事前に割り当てられているか、[デバイスの選択（Select Devices）] ページの右側のペインに移動されています。

ステップ 5 [次へ（Next）] をクリックします。

ウィザードの [イメージの選択（Select Images）] ページが表示されます。

ステップ 6 インストールするイメージを選択し、[次へ（Next）] をクリックします。

ヒント [バンドル（Bundles）] タブでバンドルを選択することもできます。

ウィザードの [割り当ての確認（Confirm Assignments）] ページが表示されます。

ステップ 7 デバイスとイメージの割り当てを確認し、[完了（Finish）] をクリックします。

[選択したデバイスにイメージをインストール（Install Images on selected devices）] ダイアログボックスが表示されます。デバイスとイメージが割り当てられています。

ステップ 8 [割り当て（Assignments）] タブの右上隅にある [検証の開始（Start Validation）] をクリックします。[デバイスにイメージをインストール（Install images on devices ）] ダイアログボックスに表示されている割り当て検証エラーまたは警告を調査します。

ヒント ジョブをスケジュールできます。また、ジョブのデフォルトプロパティを変更することもできます。ジョブのスケジュール設定とジョブプロパティの設定の詳細については、 Image Installation ウィザードを使用してデバイスにイメージをインストールする （3780 ページ）を参照してください。

ステップ 9 警告が修正されたら（または警告が重要ではないと判断したら）、[インストール（Install）] をクリックします。

イメージのインストールジョブが作成されます。ジョブの進行状況を監視し、イメージの更新を確認するための残りの手順については、 Image Installation ウィザードを使用してデバイスにイメージをインストールする （3780 ページ）を参照してください。

ジョブの操作

このセクションでは、イメージのインストールジョブの実行を支援する一連の機能について詳しく説明します。イメージのインストールジョブは、すぐに実行することも、指定した日時に実行するようにスケジュールすることもできます。Image Manager のジョブは時間がかかる傾向があるため、ジョブ管理機能を使用すると、これらの操作をバックグラウンドで実行できます。Image Manager には、一意のチケット ID を使用してジョブを簡単に検索できるオプションのチケットシステムが組み込まれています。

特定のジョブの詳細は、実行前に定義および検証されることを理解しておく必要があります。

ここでは、次の内容について説明します。

- イメージインストールジョブの概要の表示 （3789 ページ）
- インストールジョブの表示 （3790 ページ）
- イメージインストールジョブの中止 （3791 ページ）
- 失敗したイメージインストールジョブの再試行 （3791 ページ）
- 展開されたジョブをロールバックする （3792 ページ）
- イメージインストールジョブの承認ワークフロー （3793 ページ）

イメージインストールジョブの概要の表示

Image Manager ツールを使用して、イメージのインストールおよび展開ジョブを監視できます。Image Manager が実行したジョブの履歴とステータス、および特定のジョブの概要、詳細、または履歴を表示できます。

（注） ジョブの状態変更の包括的な詳細は、Configuration Manager で確認できます（ Workflow 以外のモードでのジョブの状態 （485 ページ）または Workflow モードでのジョブの状態 （487 ページ）を参照）。監査レポートの場合は、[Configuration Manager] > [管理（Manage）] > [監査レポート（Audit Report）] に移動します。

イメージインストールジョブの概要を表示するには、次の手順を実行します。

ステップ 1 セレクタの [ジョブ（Jobs）] で、[ジョブのインストール（Install Jobs）] をクリックします。

メイン ウィンドウの上部ペインに [ジョブ（Jobs）] リストが表示されます。

ステップ 2 [ジョブ（Jobs）] リストの詳細を調べます。次の項目が含まれる可能性があります。

- [名前（Name）]：ジョブの名前。デフォルトでは、名前にタイムスタンプが含まれています。
- [最後のアクション（Last Action）]：最後のアクションの日付。

- [ステータス（Status）]：ジョブのステータス（展開済み、失敗、または進行中）。
- [変更者（Changed By）]：ジョブを開始したユーザー。
- [説明（Description）]：ジョブの説明。
- [スケジュール（Schedule）]：ジョブスケジュール。
- [チケットID（Ticket ID(s)）]：チケットは、変更を追跡するために Image Manager ジョブに添付されるタグです。チケットは、Configuration Manager で作成されたチケットである可能性もあります。

ステップ 3 必要に応じて、1 つのジョブを見つけて選択し、そのジョブに関する詳細情報を下部のペインに表示できます。次の機能が含まれています。

- [概要（Overview）]
- 詳細（Details）
- 履歴（History）

ヒント 下部のペインにある [詳細（Details）] タブを表示しているときに、デバイスを選択し、右下部のペインでジョブのログを表示できます。

（注） それらはドッキング可能なウィンドウです。デフォルトのビューはカスタマイズできます。

インストールジョブの表示

特定のイメージ管理ジョブに関連付けられた詳細を表示できます。

ジョブに関連付けられた詳細を表示するには、次の手順を実行します。

ステップ 1 セレクタの [ジョブ（Jobs）] で、[ジョブのインストール（Install Jobs）] をクリックします。

ヒント ジョブセレクタの [ステータス（Status）] 列には、ジョブのステータス（[送信済み（Submitted）]、[承認済み（Approved）]、[展開済み（Deployed）]、[進行中（In Progress）]、または [失敗（Failed）]）が表示されます。

メイン ウィンドウの上部ペインに [ジョブ（Jobs）] リストが表示されます。

ステップ 2 調べるジョブを選択します。

ヒント 特定のジョブを見つける場合、[名前（Name）]、[最後のアクション（時系列）（Last Action (chronology)）]、[ステータス（Status）]（[展開済み（Deployed）]、[失敗（Failed）] など）、[説明（Description）] など、いずれかの列見出しで [ジョブ（Jobs）] リストをソートできます。検索ウィンドウを使用してフィルタリング文字列を入力し、特定のジョブを検索することもできます。

（注） ジョブフォルダの場所は、CSM-ROOT\files\vms\jobs ディレクトリです。

ステップ 3 下部のペインで [概要（Summary）] をクリックして、ジョブの概要情報を調べます。

下部のペインには、[イメージ管理ジョブ名（Image Management Job Name）]、[展開されるデバイス（Devices to be Deployed）]、[正常に展開されたデバイス（Devices Deployed Successfully）]、[展開時にエラーが発生したデバイス（Devices Deployed with Errors）] など、ジョブの概要情報が表示されます。

ステップ 4 下部のペインで [詳細（Details）] をクリックして、ジョブの概要の詳細を調べます。

デバイスの詳細、新しいイメージ、古いイメージ、およびデバイスステータスが表示されます。

ステップ 5 右端にある縦の [注釈（Commentary）] タブをクリックして、ジョブのデバイスに関する注釈を調べます。注釈には、デバイスでのイメージインストール操作の進行状況が示されます。

ステップ 6 右端にある縦の [トランスクリプト（Transcript）] タブをクリックして、ジョブ内のデバイスのトランスクリプトを調べます。トランスクリプトには、デバイスで実行されたコマンドとその応答が時系列で示されます。

ステップ 7 下部のペインで [履歴（History）] をクリックして、ジョブ履歴の詳細を調べます。ジョブの状態遷移の履歴が示されます。

（注） この情報は、Workflow モードでのみ表示されます。

イメージインストールジョブの中止

[ジョブ（Jobs）] ページで [中止（Abort）] をクリックすると、イメージインストールジョブを中止できます。このオプションは、マルチデバイスジョブに対してのみ有効です。

（注） ジョブに1つのデバイスが含まれる場合、ジョブの開始後に停止しても効果がなく、ジョブは必ず完了するまで実行されます。

- [順次（Sequential）] オプションが選択されている場合、ジョブがまだ開始されていないすべてのデバイスが中止されます。
- [並列（Parallel）] が選択されている場合、そのバッチまでのすべてのデバイスでイメージのアップグレードが行われます。次のバッチ以降のすべてのデバイスは中止されます。

失敗したイメージインストールジョブの再試行

1つ以上のデバイスにイメージを展開しようとして失敗した場合は、ジョブを再試行できます。ただし、失敗したステップから単純に続行しようとしないでください。ジョブ全体を再試行する必要があります。

失敗したジョブを再試行するには、次の手順を実行します。

ステップ 1 インストールジョブが失敗したことを確認するには、セレクタの [ジョブ（Jobs）] セクションに移動し、[インストールジョブ（Install Jobs）] をクリックします。

[ジョブ（Jobs）] ページが表示されます。

ステップ 2 [ステータス（Status）] 列を調べて、問題のジョブのステータスを判断します。

ヒント 緑色のチェックアイコンに [展開済み（Deployed）] という単語が付いている場合、成功を示します。赤い X アイコンは失敗を示します。

ステップ 3 ジョブが失敗した考えられる原因を調査します。

ステップ 4 ジョブリストから失敗したイメージインストールジョブを選択し、上部ペインのツールバーから [再試行（Retry）] をクリックします。

[デバイス（Devices）] ウィンドウにインストールイメージが表示されます。通常のインストールジョブの場合と同様に、検証警告を確認できます。

ステップ 5 必要に応じて、使用するイメージ、デバイス、スケジュール、またはジョブのプロパティを変更できます。

ステップ 6 [デバイスにイメージをインストール（Install Images on Devices）] ウィンドウで、[インストール（Install）] をクリックします。

ステップ 7 新しく作成されたジョブを観察して、再試行が成功したことを確認します。

展開されたジョブをロールバックする

展開されたイメージインストールジョブから変更をロールバックできます。

展開されたジョブをロールバックするには、次の手順を実行します。

ステップ 1 ジョブリストから、ロールバックするイメージインストールジョブを選択し、上部ペインのツールバーから [ロールバック（Rollback）] をクリックします。

[デバイス（Devices）] ウィンドウにインストールイメージが表示されます。通常のインストールジョブの場合と同様に、検証警告を確認できます。

ステップ 2 必要に応じて、ロールバックで使用するイメージ、デバイス、スケジュール、またはジョブのプロパティを変更できます。

ステップ 3 [デバイスにイメージをインストール（ Install Images on Devices）] ウィンドウで、[インストール（Install ）] をクリックします。

ステップ 4 新しく作成されたジョブをモニタリングして、ロールバックの試行が成功したことを確認します。

イメージインストールジョブの承認ワークフロー

イメージの更新は、デバイスやネットワークのダウンタイムを引き起こす可能性のある重要な操作です。そのため、イメージインストール操作の変更制御と管理は非常に重要です。イメージインストールジョブの変更管理は、Configuration Manager の展開ワークフローフレームワークを使用して行われます。これにより、すべてのイメージインストールジョブについて、実行または展開前の承認の必要性が確保されます。

イメージインストールジョブでワークフローを使用するには、次の手順を実行します。

ステップ 1 イメージインストールジョブのワークフローを有効にします。

a) Configuration Manager で、[ツール（Tools）] > [Security Manager の管理（Security Manager Administration）] > [ワークフロー（Workflow）] を選択します。

b) ワークフローがまだ有効になっていない場合は、[ワークフローの有効化（Enable Workflow）] を選択します。

c) [イメージの展開およびインストールに承認が必要（Require Deployment & Install Image Approval）] を選択します。

d) [ジョブ/スケジュール承認者（Job/Schedule Approver）] フィールドで、イメージインストールジョブを承認する担当者の電子メールアドレスを設定します。詳細については、[Workflow] ページ （745 ページ）を参照してください。

e) [保存（Save）] をクリックし、[閉じる（Close）] をクリックします。

f) Image Manager を起動し、[ジョブのインストール（Install Jobs）] に移動します。メニューバーで、ワークフローモードにおいてジョブの状態を変更するための新しいボタン（[送信（Submit）]、[承認（Approve）]、[拒否（Reject）]、[展開（Deploy）]）が使用可能になります。

ステップ 2 ワークフローを有効にしてイメージインストールジョブを作成して実行するには、次の手順を実行します。

a) 以前に説明した手順のいずれかを使用して、イメージインストールジョブを作成します。Image Manager を使用したデバイスでのイメージの更新について （3773 ページ）を参照してください。

（注） [プロパティ（Properties）] タブには、ジョブを送信するための追加のオプションがあります。ジョブの作成後に承認のためにジョブを自動送信するには、このオプションをオンにします。

b) イメージインストールジョブを作成したら、イメージインストール ジョブ ビューでジョブの状態を確認します。

c) ジョブの作成時に自動送信オプションが選択されていない場合は、ジョブを選択し、[送信（Submit）] をクリックして承認のためにジョブを送信します。

ジョブ承認者（承認者のロール/権限を持つユーザー）は、ジョブを承認するための電子メール通知を受信します。

d) 承認者は、Security Manager にログインし、Image Manager を起動して、ジョブに移動できます。

e) 承認者は、アップグレードの詳細（アップグレードに使用されるイメージ、ジョブのプロパティ、スケジュールなど）を確認した後、[承認（Approve）] をクリックしてジョブを承認します。

ジョブの状態が [承認済み（Approved）] に変更されます。ジョブの作成者は、ジョブが承認されたことを通知する電子メールを受信します。これでジョブを展開できます。

f) 承認者がジョブの詳細を確認し、納得できない場合は、[拒否（Reject）] をクリックしてジョブを拒否できます。

ジョブの状態が [拒否（Rejected）] に変更されます。ジョブの作成者は、ジョブが拒否されたことを通知する電子メールを受信します。拒否されたジョブは展開されません。

（注） 拒否されたジョブは展開されません。編集して承認のために再送信することができます。または、破棄します。

g) ジョブが承認されたら、[展開（Deploy）] をクリックしてジョブを展開できます。

ジョブの状態が [展開中（Deploying）] に変更され、イメージインストールジョブの実行が開始されます。

h) ジョブが拒否された場合またはジョブに追加の変更を加える必要がある場合は、[編集（Edit）] をクリックしてジョブを編集できます。

ウィザードの [イメージの割り当て（Image Assignments）] ページが表示され、すべてのデバイスおよびイメージが示されます。ユーザーは、ジョブのプロパティを変更したり、イメージへのデバイスの割り当てをスケジュール（場合によっては削除）したり、[送信（Submit）] をクリックして承認のためにジョブを再送信することができます。

i) ジョブの実行が開始されていない場合、ユーザーは、[破棄（Discard）] をクリックしてジョブを破棄できます。

ジョブの状態が [破棄（Discarded）] に変更されます。破棄されたジョブは実行されず、編集したり他の状態に変更することもできません。

j) 承認者は、変更されたジョブが受け入れ可能である場合、そのジョブを承認できます。前述のように、このジョブは展開できます。

k) ジョブの展開が完了すると、イメージのインストールが成功した場合は状態が [展開済み（Deployed）] に変更され、イメージのインストールが失敗した場合は状態が [失敗（Failed）] に変更されます。

イメージ管理のトラブルシューティング

このセクションでは、特定の症状に応じてイメージ管理をトラブルシューティングするために実行できる手順について説明します。

設定されている再起動時間が原因で、イメージインストールジョブに失敗したと表示される場合があります。

クラスタデバイスとフェールオーバーデバイスの場合、スタンバイデバイスとプライマリデバイスの間の再起動時間は、デフォルトで 15 分に設定されています。デバイスの構成が大規模な場合、設定されている再起動時間が原因で、イメージインストールジョブに失敗したと表示されることがあります。設定の完了後、デバイスはイメージを使用して更新されます。ところが、再起動時間の不一致により、Security Manager はジョブを失敗として表示します。

再起動時間を変更するには、次の手順を実行します。

プライマリデバイスまたはクラスタデバイスの ##MAX_RELOAD_WAIT_TIME

#デフォルトの時間は 15 分（15*60*1000）

reloadTime = 900000

Security Manager のアップグレード後、Image Manager にはデバイスのデータが存在しません。デバイスに対して最初に実行される次の操作のいずれかによって、デバイスのイメージインベントリが収集されます。

- デバイスインベントリのみを検出することを選択してデバイスを再検出する
- デバイスへのライブ展開を実行する
- デバイスへのイメージインストール操作を実行する

Cisco.com からのイメージのダウンロードに失敗する

- [Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] に移動します。
- [Image Manager] を選択します。
- [接続のテスト（Test Connection）] をクリックして、サーバーに到達できることを確認します。
- [%NMSROOT%/MDC/athena/config/****-CCOMetaData.xml] で、特定の MDF ID のメタデータ情報をダウンロードした際のエラーを確認してください。

証明書の不一致、使用不能であること、有効期限、またはその他の原因により、更新またはイメージのダウンロードが失敗します。

- エラーメッセージに示されている推奨アクションを実行します。エラーメッセージで、ダウンロードに失敗した URL を使用して証明書を取得します。
- [%NMSROOT%/MDC/certificates/*.ser] に保存されている証明書を表示します（シリアル化されたオブジェクトやファイルの内容は判読不能であり、どのエディタでも表示できません）。

Cisco.com からのイメージのダウンロード時に次のメッセージが表示されて失敗する：「ユーザーにはファイルをダウンロードする権限がありません（User not authorized to download file）」

- [Configuration Manager] > [ツール（Tools）] > [Security Managerの管理（Security Manager Administration）] に移動します。
- [Image Manager] を選択します。
- [接続のテスト（Test Connection）] をクリックして、サーバーに到達できることを確認します。
- Cisco Encryption Software Usage Handling and Distribution Policy への同意を登録してください。

ヒント　このポリシーは、http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y で閲覧できます。

Cisco.com からのイメージのダウンロードが遅い

- プロキシが設定されていることを確認します。
- Security Manger から Cisco.com へのルートをトレースします。

更新の確認に失敗する

Security Manager の管理設定ページに移動し、Cisco.com への接続をテストします。[%NMSROOT%/MDC/athena/config/****-CCOMetaData.xml] で、特定の MDF ID のメタデータ情報をダウンロードした際のエラーを確認してください。

メッセージ：「ユーザーにはファイルをダウンロードする権限がありません（User not authorized to download file）」Security Manager の管理設定ページに移動し、Cisco.com への接続をテストします。http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y で、暗号化についての合意事項を承認してください。

外部ファイルシステムまたはネットワークファイル共有からのイメージのダウンロードが失敗する

- 外部ファイルシステムまたはファイル共有への適切なアクセス権限/ログイン情報があることを確認します。
- クライアントでファイル共有を開き、イメージをドラッグして Image Manager にドロップします。

Image Install ウィザードに互換性のあるイメージが表示されない

- Image Manager は、Cisco.com の情報を使用して MDF ID のイメージの互換性を判断します。[更新の確認（Check for Updates）] を実行して、Cisco.com で入手可能な最新のイメージをダウンロードしてください。イメージが Cisco.com で入手可能で、プラットフォームとの互換性があると表示されている場合は、デバイスの該当するイメージが Image Install ウィザードおよびデバイスの [互換性のあるイメージ（Compatible Images）] タブに表示されるようになりました。
- デバイスの [互換性のあるイメージ（Compatible Images）] タブに、デバイスと実際に互換性のある一部のイメージが表示されないこともあります。
- Cisco.com に接続していないか、Cisco.com で該当するプラットフォーム向けにイメージが更新されていないため、依然として Install ウィザードにイメージが表示されない場合は、デバイス上でドラッグアンドドロップを使用してイメージをインストールできます。イメージに互換性がないという警告が表示される可能性がありますが、操作を続行し、イ

メージをデバイスにドラッグアンドドロップしてジョブを作成することで、イメージをインストールできます。

イメージコピーの失敗：「HTTP 413 エラー（HTTP 413 Error）」

- [Image Manager] > [テストファイルをデバイスにコピー（Test File Copy To Device）] で [デバイス（Device）] を右クリックします。
- vmssharedsvcs.log のエラーメッセージを確認します。
- HTTP 413 エラーが発生した場合は、ジョブを分割して、1 つのジョブに含まれるイメージの数を減らします

イメージコピーの失敗：「ディスクに十分な容量がありません（Not enough space on disk）」

- [デバイス（Device）] > [ストレージビュー（Storage View）] をチェックして、デバイス上のファイルと、イメージのインストール場所の空き容量を確認します。
- [デバイス（Device）] > [ストレージビュー（Storage View）] にファイルが表示されている場合は、ストレージからファイルを削除して容量を確保し、再試行します。
- ファイルが新規のデバイスであるか、Security Manager アップグレードセットアップであるために、[デバイス（Device）] > [ストレージビュー（Storage View）] にファイルが表示されない場合は、デバイス上のデバイスインベントリのみを再検出し、その後 [ストレージビュー（Storage View）] からファイルを削除して容量を確保します。

イメージインストールジョブの失敗：エラー：「フラッシュデバイスが無効です（Invalid flash device）」

- デバイスにフラッシュが存在するかどうかを確認します。
  - [IM] > [テストファイルをデバイスにコピー（Test File Copy To Device）] でデバイスを右クリックします。
  - デバイスに接続し、それが Security Manager でシングル コンテキスト デバイスとして管理されているマルチコンテキスト デバイスかどうかを確認します。
  - [システムコンテキスト（System Context）] の検出を選択しているデバイスを再検出します。その後、イメージインストールジョブを再試行します。

アクティブ/スタンバイペアのイメージ アップグレード ジョブが失敗する

- エラー：「このホストはフェールオーバーペアの「アクティブ」デバイスではありません（This host is not the 'active' device in the failover pair）」。フェールオーバーペアが、スタンバイデバイスの IP アドレスではなく、フェールオーバーペアのアクティブデバイスの IP アドレスを使用して Security Manager で管理されていることを確認します。
- エラー：「セカンダリデバイスがスタンバイ準備完了状態になっていません（Secondary device is not in standby-ready state）」。フェールオーバーペアのデバイスが稼働しており、

スタンバイデバイスがスタンバイ準備完了状態になっていることを確認します。スタンバイデバイスに障害が発生している場合、ジョブは中止されます。

イメージインストールジョブの失敗：エラー：「SWIM1114：アップグレード後にデバイスに到達できませんでした（SWIM1114: Device could not be reached after upgrade）」

- デバイスに到達可能かどうかを手動で確認します。解決策：イメージのアップグレード後、デバイスをSecurity Managerに再度追加するか、管理オプションを[証明書の認証を確認しない（Do not check certificate authentication）]に変更する必要があります。
- [ツール（Tools）]>[管理（Admin）]>[デバイス通信（Device Communication）]>[SSL証明書パラメータ（SSL Certificate Parameters）]>[PIX/ASA/FWSMデバイス認証証明書（PIX/ASA/FWSM Device Authentication Certificates）]が[デバイスの追加中に再取得（Retrieve while adding devices）]に設定されているかどうか確認します。
- イメージのアップグレード後、デバイスがSecurity Managerに再度追加されていることを確認します。それ以外の場合は、管理オプションを[証明書の認証を確認しない（Do not check certificate authentication）]に変更します。

（注） Image Managerがcisco.comに接続できるようにするには、最新のCisco.com証明書を受け入れている必要があります。イメージのダウンロードを正常に開始するには、「イメージメタデータロケータ」サイトとイメージのダウンロードサイトの両方からの証明書を受け入れる必要があります（[Image Manager] ページ （695 ページ）を参照）。

Security Managerのアップグレード後、Image Managerにデバイスのデータが存在しない

- デバイスインベントリのみを検出することを選択してデバイスを再検出します。
- デバイスへのライブ展開を実行します。
- デバイスへのイメージインストール操作を実行します。

ジョブを再試行またはロールバックしようとすると失敗する

- ジョブ内のいずれかのデバイスがSecurity Managerから削除されているかどうかを確認します。
- 再試行またはロールバックするすべてのイメージがSecurity Managerで使用できるかどうかを確認します。イメージをSecurity Managerリポジトリに追加して、操作を再試行します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。