CLI ブック 1：Cisco Secure Firewall ASA シリーズ 9.23 CLI コンフィギュレーション ガイド（一般的な操作）

最終更新：2025 年 11 月 12 日

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

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025 Cisco Systems, Inc. All rights reserved.

目 次

はじめに：

このマニュアルについて lxi

本書の目的 lxi

関連資料 lxi

表記法 lxi

通信、サービス、およびその他の情報 lxiii

第 I 部：

ASA の開始 65

第 1 章

Cisco Secure Firewall ASA の概要 1

ハードウェアとソフトウェアの互換性 1

VPN の互換性 1

新機能 1

ASA 9.23(1) の新機能 2

ファイアウォール機能の概要 5

セキュリティ ポリシーの概要 5

アクセス ルールによるトラフィックの許可または拒否 6

NAT の適用 6

IP フラグメントからの保護 6

HTTP、HTTPS、または FTP フィルタリングの適用 6

アプリケーション インスペクションの適用 6

QoS ポリシーの適用 6

接続制限と TCP 正規化の適用 7

脅威検出のイネーブル化 7

ファイアウォール モードの概要 7

ステートフル インスペクションの概要 8
VPN 機能の概要 9
セキュリティ コンテキストの概要 10
ASA クラスタリングの概要 11
特殊なサービスおよびレガシー サービス 11

第 2 章 はじめに 13
コマンドライン インターフェイス（CLI）のコンソールへのアクセス 13
ISA 3000 コンソールへのアクセス 13
Firepower 1000 、および Cisco Secure Firewall 1200/3100/4200 コンソールへのアクセス 15
Firepower 4100/9300 シャーシ 上の ASA コンソールへのアクセス 16
ASDM アクセスの設定 18
ASDM アクセスの工場出荷時のデフォルト設定の使用 18
ASDM アクセスのカスタマイズ 19
ASDM の起動 21
工場出荷時のデフォルト設定 23
工場出荷時のデフォルト設定の復元 24
ASA 仮想 導入設定の復元 26
Firepower 1010 のデフォルト設定 27
Firepower 1100 のデフォルト設定 29
Cisco Secure Firewall 1210/1220 のデフォルト設定 30
Secure Firewall 1230/1240/1250 のデフォルト設定 32
Cisco Secure Firewall 3100 デフォルト設定 33
Cisco Secure Firewall 4200 のデフォルト設定 34
Firepower 4100/9300 シャーシ デフォルト設定 35
ISA 3000 のデフォルト設定 36
ASA 仮想 による展開の設定 37
コンフィギュレーション作業 39
スタートアップ コンフィギュレーションおよび実行コンフィギュレーションについて 39
コンフィギュレーションの変更の保存 40
シングル コンテキスト モードでのコンフィギュレーションの変更の保存 40

マルチ コンテキスト モードでのコンフィギュレーションの変更の保存 41
スタートアップ コンフィギュレーションの実行コンフィギュレーションへのコピー 43
設定の表示 43
コンフィギュレーション設定のクリアおよび削除 43
オフラインでテキスト コンフィギュレーション ファイルの作成 45
接続の設定変更の適用 45
ASA のリロード 46

第 3 章 ライセンス：ISA 3000 の製品認証キーライセンス 47
PAK ライセンスについて 47
事前インストール済みライセンス 47
永続ライセンス 48
時間ベース ライセンス 48
時間ベース ライセンス有効化ガイドライン 48
時間ベース ライセンス タイマーの動作 48
永続ライセンスと時間ベース ライセンスの結合 48
時間ベース ライセンスのスタッキング 49
時間ベース ライセンスの有効期限 50
ライセンスに関する注意事項 50
Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス 51
その他の VPN ライセンス 51
合計 VPN セッション、全タイプ 51
VPN ロード バランシング 51
レガシー VPN ライセンス 52
暗号化ライセンス 52
合計 TLS プロキシ セッション 52
VLAN、最大 53
セキュアクライアント Premium 共有ライセンス（AnyConnect 3 以前） 53
フェールオーバー 54
フェールオーバー ライセンスの要件および例外 54

フェールオーバーライセンスの結合方法 54
フェールオーバーユニット間の通信の途絶 55
フェールオーバー ペアのアップグレード 55
ペイロード暗号化機能のないモデル 55
ライセンスの FAQ 56
PAK ライセンスのガイドライン 57
PAK ライセンスの設定 59
ライセンスの PAK の注文とアクティベーション キーの取得 59
高度暗号化ライセンスの取得 60
キーのアクティブ化または非アクティブ化 63
共有ライセンスの設定（セキュアクライアント 3 以前） 64
共有ライセンスについて 64
共有ライセンスのサーバーと参加システムについて 65
参加者とサーバーの間の通信問題 66
共有ライセンス バックアップ サーバーについて 66
フェールオーバーと共有ライセンス 67
参加者の最大数 69
共有ライセンス サーバーの設定 69
共有ライセンス バックアップ サーバーの設定（オプション） 70
共有ライセンス パーティシパントの設定 71
モデルごとにサポートされている機能のライセンス 72
モデルごとのライセンス 72
ISA 3000 ライセンスの各機能 73
PAK ライセンスのモニタリング 74
現在のライセンスの表示 74
共有ライセンスのモニタリング 83
PAK ライセンスの履歴 84

第 4 章 ライセンス：スマート ソフトウェア ライセンシング 93
スマート ソフトウェア ライセンスについて 93
Firepower 4100/9300 シャーシの ASA のスマート ソフトウェア ライセンシング 94

Smart Software Manager とアカウント 94
オフライン管理 95
パーマネント ライセンスの予約 95
Smart Software Manager オンプレミス 100
仮想アカウントごとに管理されるライセンスとデバイス 101
評価ライセンス 101
ライセンスについて（タイプ別） 102
Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス 103
その他の VPN ピア 103
合計 VPN ピア。全タイプの合計 103
暗号化ライセンス 103
キャリア ライセンス 105
合計 TLS プロキシ セッション 106
VLAN、最大 107
ボットネット トラフィック フィルタ ライセンス 107
フェールオーバーまたは ASA クラスタ ライセンス 108
ASAv のフェールオーバー ライセンス 108
Firepower 1010 のフェールオーバー ライセンス 108
Firepower 1100 のフェールオーバー ライセンス 108
Secure Firewall 1210/1220 のフェールオーバー ライセンス 110
Secure Firewall 1230/1240/1250 のフェールオーバー ライセンス 112
Secure Firewall 3100 のフェールオーバーライセンス 114
Secure Firewall 4200 のフェールオーバーライセンス 115
Firepower 4100/9300のフェールオーバーライセンス 117
Secure Firewall 3100 の ASA クラスタライセンス 118
Secure Firewall 4200 の ASA クラスタライセンス 120
ASAv の ASA クラスタライセンス 121
Firepower 4100/9300 の ASA クラスタライセンス 122
スマート ソフトウェア ライセンスの前提条件 124
Smart Software Manager 定期およびオンプレミスの前提条件 124

永続ライセンス予約の前提条件 124
スマート ソフトウェア ライセンスのガイドライン 125
スマート ソフトウェア ライセンスのデフォルト 125
ASA 仮想：スマート ソフトウェア ライセンスの設定 126
ASA 仮想：定期スマート ソフトウェア ライセンシングの設定 126
ASA 仮想：Smart Software Manager オンプレミスライセンシングの設定 133
ASA 仮想：ユーティリティ（MSLA）スマート ソフトウェア ライセンシングの設定 137
ASA 仮想：永続ライセンス予約の設定 144
ASA 仮想 永続ライセンスのインストール 144
（オプション）ASA 仮想 の永続ライセンスの返却 149
非フレキシブル PLR モードからフレキシブル PLR モードへの切り替え 150
回数変更可能な PLR モードから非 Flexible PLR モードへの切り替え 151
（オプション）ASA 仮想 の登録解除（定期およびオンプレミス） 152
（オプション）ASA 仮想 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス） 152
1000/1200/3100/4200：スマート ソフトウェア ライセンシングの設定 153
1000/1200/3100/4200：定期スマート ソフトウェア ライセンシングの設定 153
1000/1200/3100/4200：Smart Software Manager オンプレミス ライセンシングの設定 159
1000/1200/3100/4200：永久ライセンス予約の構成 164
1000/1200/3100/4200 永続ライセンスの インストール 164
（オプション）1000/1200/3100/4200 永続ライセンスの返却 167
（オプション） 1000/1200/3100/4200 の登録解除（定期およびオンプレミス） 168
（オプション）1000/1200/3100/4200 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス） 169
Firepower 4100/9300：スマート ソフトウェア ライセンスの設定 169
モデルごとのライセンス 172
ASA 仮想 172
Firepower 1010 178
Firepower 1100 シリーズ 179
Cisco Secure Firewall 1210、1220 180
Secure Firewall 1230、1240、1250 181
Secure Firewall 3100 シリーズ 183

Firepower 4100 185
Cisco Secure Firewall 4200 シリーズ 186
Firepower 9300 187
モデルごとのライセンス PID 188
スマート ソフトウェア ライセンシングのモニタリング 193
現在のライセンスの表示 194
スマート ライセンス ステータスの表示 194
UDI の表示 197
スマート ソフトウェア ライセンスのデバッグ 197
Smart Software Manager 通信 197
デバイスの登録とトークン 198
Smart Software Manager との定期的な通信 198
コンプライアンス逸脱状態 198
Smart Call Home インフラストラクチャ 199
スマート ライセンス証明書の管理 199
Smart Software Licensing の履歴 200

第 5 章 論理デバイス Firepower 4100/9300 205
インターフェイスについて 205
シャーシ管理インターフェイス 205
インターフェイス タイプ 206
FXOS インターフェイスとアプリケーション インターフェイス 209
論理デバイスについて 210
スタンドアロン論理デバイスとクラスタ化論理デバイス 210
のハードウェアとソフトウェアの要件と前提条件 210
論理デバイスに関する注意事項と制約事項 212
インターフェイスに関する注意事項と制限事項 212
一般的なガイドラインと制限事項 212
ハイアベイラビリティの要件と前提条件 212
インターフェイスの設定 213
物理インターフェイスの設定 213

EtherChannel（ポート チャネル）の追加 216
論理デバイスの設定 219
スタンドアロン ASA の追加 219
ハイ アベイラビリティ ペアの追加 225
ASA 論理デバイスのインターフェイスの変更 226
アプリケーションのコンソールへの接続 227
論理デバイスの履歴 229

第 6 章 トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード 231
ファイアウォール モードについて 231
ルーテッド ファイアウォール モードについて 231
トランスペアレント ファイアウォール モードについて 232
ネットワークでのトランスペアレント ファイアウォールの使用 232
管理 インターフェイス 233
ルーテッド モード機能のためのトラフィックの通過 233
ブリッジグループについて 233
ブリッジ仮想インターフェイス（BVI） 234
トランスペアレント ファイアウォール モードのブリッジグループ 234
ルーテッド ファイアウォール モードのブリッジグループ 235
ルーテッド モードで許可されないトラフィックの通過 236
レイヤ 3 トラフィックの許可 237
許可される MAC アドレス 237
BPDU 処理 237
MAC アドレスとルート ルックアップ 238
トランスペアレント モードのブリッジ グループのサポートされていない機能 239
ルーテッド モードのブリッジ グループのサポートされていない機能 240
デフォルト設定 241
ファイアウォール モードのガイドライン 242
ファイアウォール モードの設定 243
ファイアウォール モードの例 244
ルーテッド ファイアウォール モードで ASA を通過するデータ 244

内部ユーザーが Web サーバーにアクセスする 245
外部ユーザーが DMZ 上の Web サーバーにアクセスする 246
内部ユーザーが DMZ 上の Web サーバーにアクセスする 247
外部ユーザーが内部ホストにアクセスしようとする 248
DMZ ユーザーによる内部ホストへのアクセスの試み 249
トランスペアレント ファイアウォールを通過するデータの動き 249
内部ユーザーが Web サーバーにアクセスする 250
NAT を使用して内部ユーザーが Web サーバーにアクセスする 252
外部ユーザーが内部ネットワーク上の Web サーバーにアクセスする 253
外部ユーザーが内部ホストにアクセスしようとする 254
ファイアウォール モードの履歴 255

第 II 部： ハイ アベイラビリティとスケーラビリティ 259

第 7 章 マルチ コンテキスト モード 261
セキュリティ コンテキストについて 261
セキュリティ コンテキストの一般的な使用方法 261
コンテキスト コンフィギュレーション ファイル 262
コンテキスト コンフィギュレーション 262
システム設定 262
管理コンテキストの設定 262
ASA がパケットを分類する方法 263
有効な分類子基準 263
分類例 264
セキュリティ コンテキストのカスケード接続 266
セキュリティ コンテキストへの管理アクセス 267
システム管理者のアクセス 267
コンテキスト管理者のアクセス 268
インターフェイス使用率の管理 268
リソース管理の概要 268
リソース クラス 269

リソース制限値 269
デフォルト クラス 269
オーバーサブスクライブ リソースの使用 270
無限リソースの使用 271
MAC アドレスについて 272
マルチコンテキスト モードでの MAC アドレス 272
自動 MAC アドレス 272
VPN サポート 273
マルチ コンテキスト モードのライセンス 273
マルチ コンテキスト モードの前提条件 275
マルチ コンテキスト モードのガイドライン 275
マルチ コンテキスト モードのデフォルト 277
マルチ コンテキストの設定 277
マルチ コンテキスト モードの有効化または無効化 278
マルチ コンテキスト モードの有効化 278
シングルコンテキスト モードの復元 279
リソース管理用のクラスの設定 280
セキュリティ コンテキストの設定 285
コンテキスト インターフェイスへの MAC アドレスの自動割り当て 289
コンテキストとシステム実行スペースの切り替え 290
セキュリティ コンテキストの管理 291
セキュリティ コンテキストの削除 291
管理コンテキストの変更 292
セキュリティ コンテキスト URL の変更 292
セキュリティ コンテキストのリロード 294
コンフィギュレーションのクリアによるリロード 294
コンテキストの削除および再追加によるリロード 295
セキュリティ コンテキストのモニタリング 295
コンテキスト情報の表示 295
リソースの割り当ての表示 297
リソースの使用状況の表示 300

コンテキストでの SYN 攻撃のモニタリング 303
割り当てられた MAC アドレスの表示 305
システム設定での MAC アドレスの表示 305
コンテキスト内の MAC アドレスの表示 307
マルチ コンテキスト モードの例 307
マルチ コンテキスト モードの履歴 309

第 8 章 ハイ アベイラビリティのためのフェールオーバー 315
フェールオーバーについて 315
フェールオーバー モード 315
フェールオーバー のシステム要件 316
ハードウェア要件 316
ソフトウェア要件 317
ライセンス要件 317
フェールオーバー リンクとステートフル フェールオーバー リンク 318
フェールオーバー リンク 318
ステートフル フェールオーバー リンク 320
フェールオーバーの中断の回避とデータ リンク 321
フェールオーバー の MAC アドレスと IP アドレス 322
ステートレス フェールオーバーとステートフル フェールオーバー 325
ステートレス フェールオーバー 325
ステートフル フェールオーバー 325
フェールオーバーのブリッジ グループ要件 328
アプライアンス、ASAv のブリッジグループ必須要件 328
フェールオーバーのヘルス モニタリング 328
装置のヘルス モニターリング 329
ハートビートモジュールの冗長性 329
インターフェイス モニタリング 330
フェールオーバー 時間 332
設定の同期 333
コンフィギュレーションの複製の実行 333

ファイルの複製 334
コマンドの複製 335
設定同期の最適化 336
アクティブ/スタンバイ フェールオーバーについて 337
プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス 337
起動時のアクティブ装置の判別 337
フェールオーバー イベント 338
アクティブ/アクティブ フェールオーバーの概要 339
アクティブ/アクティブ フェールオーバーの概要 339
フェールオーバー グループのプライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス 340
起動時のフェールオーバー グループのアクティブ装置の決定 340
フェールオーバー イベント 340
フェールオーバーのライセンス 342
フェールオーバー のガイドライン 343
フェールオーバーのデフォルト 347
アクティブ/スタンバイ フェールオーバーの設定 347
アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定 347
アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定 352
アクティブ/アクティブ フェールオーバーの設定 353
アクティブ/アクティブ フェールオーバーのプライマリ装置の設定 353
アクティブ/アクティブ フェールオーバーのセカンダリ装置の設定 358
オプションのフェールオーバー パラメータの設定 359
フェールオーバー基準とその他の設定の構成 360
インターフェイス モニタリングの設定 364
非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブモード） 365
フェールオーバー の管理 369
フェールオーバーの強制実行 369
フェールオーバーのディセーブル化 370
障害が発生した装置の復元 371
コンフィギュレーションの再同期 372

フェールオーバー機能のテスト 372
リモート コマンドの実行 373
コマンドの送信 373
コマンド モードの変更 374
セキュリティに関する考慮事項 375
リモート コマンドの実行に関する制限事項 375
フェールオーバーのモニタリング 376
フェールオーバー メッセージ 376
フェールオーバーの syslog メッセージ 376
フェールオーバー デバッグ メッセージ 377
SNMP のフェールオーバー トラップ 377
フェールオーバー ステータスのモニタリング 377
フェールオーバーの履歴 378

第 9 章 パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー 383
パブリック クラウドでのフェールオーバーについて 383
アクティブ/バックアップ フェールオーバーについて 384
プライマリ/セカンダリの役割とアクティブ/バックアップ ステータス 384
フェールオーバー接続 385
ポーリングと Hello メッセージ 385
起動時のアクティブ装置の判別 385
フェールオーバー イベント 386
注意事項と制約事項 388
パブリック クラウドでのフェールオーバーのライセンス 389
パブリック クラウドでのフェールオーバーのデフォルト 389
Microsoft Azure での ASA 仮想 ハイアベイラビリティについて 390
Azure サービス プリンシパルについて 391
Azure での ASA 仮想 ハイアベイラビリティの設定要件 392
アクティブ/バックアップ フェールオーバーの設定 393
アクティブ/バックアップ フェールオーバーのプライマリ装置の設定 393
アクティブ/バックアップ フェールオーバーのセカンダリ装置の設定 394

オプションのフェールオーバー パラメータの設定 395
フェールオーバー基準とその他の設定の構成 395
Azure サービス プリンシパル用の認証クレデンシャルの設定 397
Azure ルート テーブルの設定 399
アクティブ/バックアップ フェールオーバーの有効化 400
アクティブ/バックアップ フェールオーバーのプライマリ装置の有効化 401
アクティブ/バックアップ フェールオーバーのセカンダリ装置の有効化 402
パブリック クラウドでのフェールオーバーの管理 403
フェールオーバーの強制実行 403
ルートの更新 403
Azure 認証の検証 404
パブリック クラウドでのフェールオーバーのモニター 405
フェールオーバー ステータス 405
フェールオーバー メッセージ 405
パブリック クラウドでのフェールオーバーの履歴 406

第 10 章 **Cisco Secure Firewall 3100/4200 の ASA クラスタ 407**
ASA クラスタリングの概要 407
クラスタをネットワークに適合させる方法 408
クラスタ メンバー 408
ブートストラップ設定 408
制御ノードとデータノードの役割 408
クラスタ インターフェイス 409
クラスタ制御リンク 409
コンフィギュレーションの複製 409
ASA クラスタ管理 409
管理ネットワーク 409
管理インターフェイス 410
制御ユニット管理とデータユニット管理 410
暗号キー複製 411
ASDM 接続証明書 IP アドレス不一致 411

サイト間クラスタリング 411
ASA クラスタリングのライセンス 412
ASA クラスタリングの要件と前提条件 414
クラスタリングに関するガイドライン 416
ASA クラスタリングの設定 422
ユニットのケーブル接続およびインターフェイスの設定 423
クラスタ インターフェイスについて 423
クラスタ ユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定 430
各ユニットでのクラスタ インターフェイス モードの設定 431
制御ノードでのインターフェイスの設定 432
ブートストラップ コンフィギュレーションの作成 439
制御ノードのブートストラップの設定 439
データノードのブートストラップの設定 445
クラスタリング動作のカスタマイズ 448
ASA クラスタの基本パラメータの設定 448
のヘルス モニタリングおよび自動再結合の設定 449
接続の再分散およびクラスタ TCP 複製の遅延の設定 453
サイト間機能の設定 454
分散型サイト間 VPN の設定 462
クラスタノードの管理 468
非アクティブノードになる 468
ノードの非アクティブ化 469
クラスタへの再参加 470
クラスタからの脱退 471
制御ノードの変更 472
クラスタ全体でのコマンドの実行 473
ASA クラスタのモニタリング 474
クラスタ ステータスのモニタリング 474
クラスタ全体のパケットのキャプチャ 478
クラスタリソースのモニタリング 478

クラスタ トラフィックのモニタリング 478
クラスタのルーティングのモニタリング 484
分散型サイト間 VPN のモニタリング 484
クラスタリングのロギングの設定 485
クラスタのインターフェイスのモニタリング 485
クラスタリングのデバッグ 485
分散型サイト間 VPN のトラブルシューティング 486
ASA クラスタリングの例 488
ASA およびスイッチのコンフィギュレーションの例 488
ASA の設定 488
Cisco IOS スイッチのコンフィギュレーション 490
スティック上のファイアウォール 491
トラフィックの分離 493
ルーテッド モード サイト間クラスタリングの OTV 設定 495
サイト間クラスタリングの例 498
個別インターフェイス ルーテッド モード ノースサウス サイト間の例 498
サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド EtherChannel ルーテッド モードの例 499
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例 501
スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例 502
クラスタリングの参考資料 503
ASA の各機能とクラスタリング 503
クラスタリングでサポートされない機能 503
クラスタリングの中央集中型機能 504
個々のノードに適用される機能 505
ネットワーク アクセス用の AAA とクラスタリング 506
接続設定とクラスタリング 506
FTP とクラスタリング 506
ICMP インスペクションとクラスタリング 506
マルチキャスト ルーティングとクラスタリング 507
NAT とクラスタリング 507

ダイナミック ルーティングおよびクラスタリング 509
SCTP とクラスタリング 512
SIP インスペクションとクラスタリング 512
SNMP とクラスタリング 512
STUN とクラスタリング 512
syslog および NetFlow とクラスタリング 512
Cisco TrustSec とクラスタリング 513
VPN とクラスタリング 513
パフォーマンス スケーリング係数 513
制御ノードの選定 513
クラスタ内のハイ アベイラビリティ 514
ノードヘルスモニタリング 514
インターフェイス モニタリング 515
障害後のステータス 515
クラスタへの再参加 516
データ パス接続状態の複製 516
クラスタが接続を管理する方法 517
接続のロール 517
新しい接続の所有権 520
TCP のサンプルデータフロー 520
ICMP および UDP のサンプルデータフロー 521
新しい TCP 接続のクラスタ全体での再分散 522
Cisco Secure Firewall 3100/4200 の ASA クラスタリングの履歴 522

第 11 章 **Firepower 4100/9300 の ASA クラスタ 525**
Firepower 4100/9300 シャーシのクラスタリングについて 525
ブートストラップ設定 526
クラスタ メンバー 526
クラスタ制御リンク 527
クラスタ制御リンクのサイジング 527
クラスタ制御リンクの冗長性 528

クラスタ制御リンクの信頼性 528
クラスタ制御リンク ネットワーク 529
クラスタ インターフェイス 529
冗長スイッチシステムへの接続 529
コンフィギュレーションの複製 529
Secure Firewall ASA クラスタの管理 529
管理ネットワーク 529
管理インターフェイス 530
制御ユニット管理とデータユニット管理 530
暗号キー複製 530
ASDM 接続証明書 IP アドレス不一致 531
スパンド EtherChannel（推奨） 531
サイト間クラスタリング 532
Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 533
でのクラスタリングのライセンス Firepower 4100/9300 シャーシ 535
クラスタリング ガイドラインと制限事項 537
でのクラスタリングの設定 Firepower 4100/9300 シャーシ 543
FXOS：ASA クラスタの追加 543
ASA クラスタの作成 543
クラスタ メンバの追加 554
ASA：ファイアウォール モードとコンテキスト モードの変更 555
ASA：データ インターフェイスの設定 555
ASA：クラスタ設定のカスタマイズ 558
ASA クラスタの基本パラメータの設定 559
のヘルス モニタリングおよび自動再結合の設定 562
接続の再分散およびクラスタ TCP 複製の遅延の設定 565
サイト間機能の設定 566
分散型サイト間 VPN の設定 574
FXOS：クラスタノードの削除 582
ASA：クラスタ メンバの管理 584
非アクティブなメンバーになる 584

ユニットの非アクティブ化 585
クラスタへの再参加 586
制御ユニットの変更 587
クラスタ全体でのコマンドの実行 588
ASA：での ASA クラスタのモニタリング Firepower 4100/9300 シャーシ 589
クラスタ ステータスのモニタリング 589
クラスタ全体のパケットのキャプチャ 593
クラスタリソースのモニタリング 593
クラスタ トラフィックのモニタリング 594
クラスタのルーティングのモニタリング 598
分散型 S2S VPN のモニタリング 599
クラスタリングのロギングの設定 599
クラスタリングのデバッグ 599
分散型 S2S VPN のトラブルシューティング 600
ASA クラスタリングの例 602
スティック上のファイアウォール 602
トラフィックの分離 603
ルーテッド モード サイト間クラスタリングの OTV 設定 603
サイト間クラスタリングの例 606
サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド EtherChannel ルーテッド モードの例 606
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例 608
スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例 610
クラスタリングの参考資料 611
ASA の各機能とクラスタリング 611
クラスタリングでサポートされない機能 611
クラスタリングの中央集中型機能 612
個々のユニットに適用される機能 613
ネットワーク アクセス用の AAA とクラスタリング 613
接続設定 614
FTP とクラスタリング 614

ICMP インスペクション 614
マルチキャスト ルーティングとクラスタリング 614
NAT とクラスタリング 614
ダイナミック ルーティングおよびクラスタリング 617
SCTP とクラスタリング 617
SIP インスペクションとクラスタリング 617
SNMP とクラスタリング 618
STUN とクラスタリング 618
syslog および NetFlow とクラスタリング 618
Cisco TrustSec とクラスタリング 618
Secure Firewall eXtensible オペレーティングシステム（FXOS）シャーシ上の VPN とクラスタリング 618
パフォーマンス スケーリング係数 619
制御ユニットの選定 619
クラスタ内のハイ アベイラビリティ 620
シャーシ アプリケーションのモニターリング 620
装置のヘルス モニターリング 620
インターフェイス モニタリング 621
デコレータ アプリケーションのモニタリング 621
障害後のステータス 622
クラスタへの再参加 622
データ パス接続状態の複製 623
クラスタが接続を管理する方法 623
接続のロール 623
新しい接続の所有権 626
TCP のサンプルデータフロー 626
ICMP および UDP のサンプルデータフロー 627
新しい TCP 接続のクラスタ全体での再分散 629
Firepower 4100/9300 上の ASA クラスタリングの履歴 629

第 12 章 **ASA クラスタのクラスタを展開する** 639

ASA 仮想クラスタリングについて 640
クラスタをネットワークに適合させる方法 640
クラスタ ノード 640
ブートストラップ設定 640
制御ノードとデータノードの役割 641
個々のインターフェイス 641
ポリシーベース ルーティング 642
等コスト マルチパス ルーティング 643
クラスタ制御リンク 643
クラスタ制御リンク トラフィックの概要 644
クラスタ制御リンクの障害 644
コンフィギュレーションの複製 644
ASA 仮想 クラスタの管理 645
管理ネットワーク 645
管理インターフェイス 645
制御ノードの管理対データノードの管理 645
暗号キー複製 646
ASDM 接続証明書 IP アドレス不一致 646
サイト間クラスタリング 646
ASA 仮想クラスタリングのライセンス 647
ASA 仮想クラスタリングの要件と前提条件 647
ASA 仮想クラスタリングに関するガイドライン 648
Day0 設定を使用した ASA 仮想 クラスタリングの設定 649
展開後のASA 仮想クラスタリングの設定 652
インターフェイスの設定 652
各ノードのでクラスタ インターフェイス モードを設定する 652
個々のインターフェイスの設定 654
ブートストラップ コンフィギュレーションの作成 657
制御ノードのブートストラップの設定 657
データノードのブートストラップの設定 663
クラスタリング動作のカスタマイズ 666

ASA クラスタの基本パラメータの設定 667
ヘルスモニタリングおよび自動再参加設定の設定 667
接続リバランスおよびクラスタ TCP 複製遅延の設定 671
サイト間機能の設定 672
ディレクタ ローカリゼーションの有効化 672
サイト冗長性の有効化 673
クラスタ フロー モビリティの設定 673
クラスタノードの管理 679
非アクティブノードになる 679
制御ノードからのデータノードの非アクティブ化 680
クラスタへの再参加 681
クラスタからの脱退 681
制御ノードの変更 682
クラスタ全体でのコマンドの実行 683
ASA 仮想クラスタのモニタリング 684
クラスタ ステータスのモニタリング 684
クラスタ全体のパケットのキャプチャ 688
クラスタリソースのモニタリング 688
クラスタ トラフィックのモニタリング 688
クラスタのルーティングのモニタリング 694
クラスタリングのロギングの設定 694
クラスタのインターフェイスのモニタリング 694
クラスタリングのデバッグ 695
ASA 仮想クラスタリングの例 695
個別インターフェイス ルーテッド モード ノースサウス サイト間の例 696
クラスタリングの参考資料 696
ASA の各機能とクラスタリング 697
クラスタリングでサポートされない機能 697
クラスタリングの中央集中型機能 697
個々のノードに適用される機能 698
ネットワーク アクセス用の AAA とクラスタリング 699

接続設定とクラスタリング 699
ダイナミック ルーティングおよびクラスタリング 699
FTP とクラスタリング 701
ICMP インスペクションとクラスタリング 701
マルチキャスト ルーティングとクラスタリング 701
NAT とクラスタリング 701
SCTP とクラスタリング 704
SIP インスペクションとクラスタリング 704
SNMP とクラスタリング 704
STUN とクラスタリング 704
syslog および NetFlow とクラスタリング 704
Cisco TrustSec とクラスタリング 705
VPN とクラスタリング 705
パフォーマンス スケーリング係数 705
制御ノードの選定 705
ASA 仮想クラスタ内のハイアベイラビリティ 706
ノードヘルスモニタリング 706
インターフェイス モニタリング 707
障害後のステータス 707
クラスタへの再参加 707
データ パス接続状態の複製 708
ASA 仮想クラスタが接続を管理する方法 709
接続のロール 709
新しい接続の所有権 711
TCP のサンプルデータフロー 711
ICMP および UDP のサンプルデータフロー 712
新しい TCP 接続のクラスタ全体での再分散 714
ASA 仮想クラスタリングの履歴 714

第 13 章 **パブリッククラウドにおける ASA Virtual の ASA クラスタ 717**
パブリッククラウドにおける ASA Virtual クラスタリングについて 718

クラスタをネットワークに適合させる方法 718
クラスタ ノード 719
ブートストラップ設定 719
制御ノードとデータノードの役割 719
個々のインターフェイス 719
クラスタ制御リンク 720
クラスタ制御リンク トラフィックの概要 720
クラスタ制御リンクの障害 721
コンフィギュレーションの複製 721
ASA 仮想 クラスタの管理 721
管理ネットワーク 721
管理インターフェイス 721
制御ノードの管理対データノードの管理 722
暗号キー複製 722
ASDM 接続証明書 IP アドレス不一致 723
ASA Virtual クラスタリングのライセンス 723
ASA Virtual クラスタリングの要件と前提条件 723
ASA Virtual クラスタリングのガイドライン 725
AWS でクラスタを展開する 726
AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ 726
トポロジの例 727
AWS で ASA Virtual クラスタを展開するためのエンドツーエンドのプロセス 729
テンプレート 731
AWS における GWLB を使用した ASA 仮想クラスタリングのターゲットフェールオーバーの設定 731
CloudFormation テンプレートを使用した AWS へのスタックの展開 733
自動スケーリングのパラメータ設定 740
スタックの更新による ASA Virtual クラスタリングでの IMDSv2 必須モードの設定 742
AWS でのクラスタの手動展開 742
AWS 向け Day 0 構成の作成 742
クラスタノードの展開 744

AWS での ASA virtual のターゲットフェールオーバーの有効化 745
Azure でクラスタを展開する 747
Azure でのクラスタ展開について 748
Azure Resource Manager テンプレートを使用したクラスタの展開 748
Azure でクラスタを設定する 754
Azure でクラスタを作成するための構成ファイルを準備する 754
構成ファイルを使用して手動でクラスタを設定する 756
Azure Function App を使用してクラスタを設定する 757
Azure における ASA Virtual クラスタのトラブルシューティング 759
ASA 仮想 Azure でのクラスタリングのオートスケール ソリューション 760
トポロジの例 761
Azure での ASA 仮想 クラスタリングの自動スケール ロジック 764
GitHub での展開とインフラストラクチャのテンプレート 765
入力パラメータ 766
ASA 仮想 Auto Scale の展開プロセスとリソースを備えたクラスター 773
Autoscale ソリューションを使用した ASA 仮想 クラスタの展開 774
Function App への Azure Cluster Autoscale 機能の展開 778
Azure Logic App の更新 779
クラスタリング動作のカスタマイズ 783
ASA クラスタの基本パラメータの設定 783
ヘルスモニタリングおよび自動再参加設定の設定 784
クラスタノードの管理 787
非アクティブノードになる 787
制御ノードからのデータノードの非アクティブ化 788
クラスタへの再参加 789
クラスタからの脱退 790
制御ノードの変更 791
クラスタ全体でのコマンドの実行 792
クラスタのモニタリング 792
クラスタ ステータスのモニタリング 792
クラスタ全体のパケットのキャプチャ 797

クラスタリソースのモニタリング 797
クラスタ トラフィックのモニタリング 797
クラスタのルーティングのモニタリング 802
クラスタリングのロギングの設定 803
クラスタのインターフェイスのモニタリング 803
クラスタリングのデバッグ 803
クラスタリングの参考資料 804
ASA の各機能とクラスタリング 804
クラスタリングでサポートされない機能 804
クラスタリングの中央集中型機能 805
個々のノードに適用される機能 806
ネットワーク アクセス用の AAA とクラスタリング 806
接続設定とクラスタリング 807
ダイナミック ルーティングおよびクラスタリング 807
FTP とクラスタリング 808
ICMP インスペクションとクラスタリング 808
マルチキャスト ルーティングとクラスタリング 808
NAT とクラスタリング 809
SCTP とクラスタリング 811
SIP インスペクションとクラスタリング 811
SNMP とクラスタリング 811
STUN とクラスタリング 811
syslog とクラスタリング 812
Cisco TrustSec とクラスタリング 812
VPN とクラスタリング 812
パフォーマンス スケーリング係数 812
制御ノードの選定 813
クラスタ内のハイアベイラビリティ 813
ノードヘルスモニタリング 814
インターフェイス モニタリング 814
障害後のステータス 814

クラスタへの再参加 815
データ パス接続状態の複製 815
クラスタが接続を管理する方法 816
接続のロール 816
新しい接続の所有権 818
TCP のサンプルデータフロー 819
ICMP および UDP のサンプルデータフロー 820
パブリッククラウドにおける ASA Virtual クラスタリングの履歴 821

第 III 部： インターフェイス 823

第 14 章 基本的なインターフェイス設定 825
基本的なインターフェイス設定について 825
Auto-MDI/MDIX 機能 826
管理インターフェイス 826
管理インターフェイスの概要 826
管理スロット/ポート インターフェイス 826
管理専用トラフィックに対する任意のインターフェイスの使用 827
トランスペアレント モードの管理インターフェイス 827
基本インターフェイスの設定のガイドライン 828
基本インターフェイスのデフォルト設定 829
物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 830
ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000） 833
Cisco Secure Firewall 3100/4200 のネットワークモジュールの管理 834
ブレークアウトポートの設定 835
ネットワークモジュールの追加 836
ネットワークモジュールの交換方法 836
ネットワークモジュールを別のタイプに交換する 838
ネットワーク モジュールの取り外し 839
インターフェイスのモニタリング 840
基本インターフェイスの例 840

物理インターフェイス パラメータの例 840
マルチ コンテキスト モードの例 841
基本インターフェイスの設定の履歴 841

第 15 章 Firepower 1010 と Cisco Secure Firewall 1210/1220 スイッチポートの基本インターフェイス設定 845
スイッチ ポートについて 845
スイッチポートおよびインターフェイスについて 845
Auto-MDI/MDIX 機能 847
スイッチポートの注意事項および制約事項 847
スイッチ ポートと Power Over Ethernet の設定 849
スイッチ ポート モードの有効化または無効化 849
VLAN インターフェイスの設定 850
スイッチ ポートのアクセス ポートとしての設定 851
スイッチ ポートのトランク ポートとしての設定 853
Power over Ethernet の設定 856
スイッチポートのモニタリング 858
スイッチポートの例 860
ルーテッドモードの例 860
トランスペアレントモードの例 860
ファイアウォール インターフェイス/スイッチポートの混合の例 861
統合ルーティングおよびブリッジングの例 862
フェールオーバーの例 863
スイッチポートの履歴 864

第 16 章 EtherChannel インターフェイスインターフェイス 865
EtherChannel インターフェイスについて 865
EtherChannel について 866
チャネル グループのインターフェイス 866
別のデバイスの EtherChannel への接続 866
Link Aggregation Control Protocol 868

ロード バランシング 868
EtherChannel MAC アドレス 869
EtherChannel インターフェイスのガイドライン 869
EtherChannel インターフェイスのデフォルト設定 872
EtherChannel の設定 872
EtherChannel へのインターフェイスの追加 872
EtherChannel のカスタマイズ（ISA 3000） 875
EtherChannel のモニタリング 877
EtherChannel の例 878
EtherChannel インターフェイスの履歴 879

第 17 章 ループバック インターフェイス 881
ループバック インターフェイスについて 881
ループバック インターフェイスの概要 882
ループバック インターフェイスの設定 882
ループバック インターフェイスへのトラフィックのレート制限 883
ループバック インターフェイスのモニタリング 884
ループバック インターフェイスの履歴 885

第 18 章 VLAN サブインターフェイス 887
VLAN サブインターフェイスについて 887
VLAN サブインターフェイスのライセンス 888
VLAN サブインターフェイスのガイドラインと制限事項 889
VLAN サブインターフェイスのデフォルト設定 890
VLAN サブインターフェイスと 802.1Q トランキングの設定 890
VLAN サブインターフェイスのモニタリング 892
VLAN のサブインターフェイスの例 892
VLAN サブインターフェイスの履歴 893

第 19 章 VXLAN インターフェイス 895
VXLAN インターフェイスの概要 895

カプセル化 895
VXLAN トンネル エンドポイント 896
VTEP 送信元インターフェイス 896
VNI インターフェイス 897
VXLAN パケット処理 897
ピア VTEP 898
VXLAN 使用例 899
VXLAN ブリッジまたはゲートウェイの概要 899
VXLAN ブリッジ 900
VXLAN ゲートウェイ（ルーテッド モード） 900
VXLAN ドメイン間のルータ 901
AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ 902
AWS ゲートウェイロードバランサおよび Geneve デュアルアームプロキシ 903
Azure ゲートウェイロードバランサおよびペアプロキシ 904
VXLAN インターフェイスの要件と前提条件 905
VXLAN インターフェイスのガイドライン 906
VXLAN インターフェイスのデフォルト設定 907
VXLAN インターフェイスの設定 907
VTEP 送信元インターフェイスの設定 908
VNI インターフェイスの設定 910
（オプション）VXLAN UDP ポートの変更 913
Geneve インターフェイスの設定 914
Geneve の VTEP 送信元インターフェイスの設定 914
Geneve の VNI インターフェイスの設定 915
ゲートウェイロードバランサのヘルスチェックの許可 917
VXLAN インターフェイスのモニタリング 919
VXLAN インターフェイスの例 921
トランスペアレント VXLAN ゲートウェイの例 922
VXLAN ルーティングの例 924
VXLAN インターフェイスの履歴 926

第 20 章 ルーテッド モードおよびトランスペアレント モードのインターフェイス 927

ルーテッドモードインターフェイスとトランスペアレントモードインターフェイスについて 927

セキュリティ レベル 928

デュアル IP スタック（IPv4 および IPv6） 929

31 ビット サブネット マスク 929

31 ビットのサブネットとクラスタリング 929

31 ビットのサブネットとフェールオーバー 929

31 ビットのサブネットと管理 929

31 ビットのサブネットをサポートしていない機能 929

ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項 930

ルーテッド モードのインターフェイスの設定 932

ルーテッド モードの一般的なインターフェイス パラメータの設定 933

PPPoE の設定 936

ブリッジグループ インターフェイスの設定 937

ブリッジ仮想インターフェイス（BVI）の設定 937

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定 940

トランスペアレント モードの管理インターフェイスの設定 942

IPv6 アドレスの設定 944

IPv6 について 944

IPv6 アドレッシング 944

Modified EUI-64 インターフェイス ID 945

IPv6 プレフィックス委任クライアントの設定 945

IPv6 プレフィックス委任の概要 945

IPv6 プレフィックス委任クライアントの有効化 948

グローバル IPv6 アドレスの設定 950

IPv6 ネイバー探索の設定 954

ルーテッド モードおよびトランスペアレント モードのインターフェイスのモニタリング 959

インターフェイス統計情報 959

DHCP Information 959
PPPoE 963
IPv6 ネイバー探索 963
ルーテッド モードおよびトランスペアレント モードのインターフェイスの例 964
2 つのブリッジグループを含むトランスペアレント モードの例 964
2 つのブリッジグループを含むスイッチド LAN セグメントの例 965
ルーテッド モードおよびトランスペアレント モードのインターフェイスの履歴 968

第 21 章 高度なインターフェイス設定 973
インターフェイスの詳細設定について 973
MAC アドレスについて 973
デフォルトの MAC アドレス 974
自動 MAC アドレス 974
MTU について 975
パス MTU ディスカバリ 976
デフォルト MTU 976
MTU とフラグメンテーション 976
MTU とジャンボ フレーム 976
TCP MSS について 977
デフォルト TCP MSS 977
TCP MSS の推奨最大設定 977
インターフェイス間通信 978
インターフェイス内通信（ルーテッド ファイアウォール モード） 978
MAC アドレスの手動設定 978
MAC アドレスの自動割り当て 979
MTUおよび TCP MSS の設定 980
同一のセキュリティ レベル通信の許可 982
インターフェイスの詳細設定の履歴 983

第 22 章 トラフィック ゾーン 985
トラフィック ゾーンの概要 985

ゾーン分割されていない動作 985
ゾーンを使用する理由 986
非対称ルーティング 986
紛失したルート 986
ロード バランシング 987
ゾーンごとの接続テーブルおよびルーティング テーブル 988
ECMP ルーティング 988
ゾーン分割されていない ECMP サポート 988
ゾーン分割された ECMP サポート 989
接続のロード バランス方法 989
別のゾーンのルートへのフォール バック 989
インターフェイスベースのセキュリティ ポリシーの設定 990
トラフィック ゾーンでサポートされるサービス 990
セキュリティ レベル 990
フローのプライマリおよび現在のインターフェイス 991
ゾーンの追加または削除 991
ゾーン内トラフィック 991
To-the-Box および From-the-Box トラフィック 991
ゾーン内の IP アドレスのオーバーラップ 992
トラフィック ゾーンの前提条件 992
トラフィック ゾーンのガイドライン 994
トラフィック ゾーンの設定 995
トラフィック ゾーンのモニタリング 996
ゾーン情報 996
ゾーン接続 997
ゾーン ルーティング 998
トラフィック ゾーンの例 999
トラフィック ゾーンの履歴 1002

第 IV 部： 基本設定 1003

第 23 章 基本設定 1005

ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 1005

日時の設定 1008

タイムゾーンと夏時間の日付の設定 1008

NTP サーバを使用した日付と時刻の設定 1010

手動での日時の設定 1012

Precision Time Protocol の設定（ISA 3000） 1013

マスター パスフレーズの設定 1015

マスター パスフレーズの追加または変更 1015

マスター パスフレーズの無効化 1018

マスター パスフレーズの削除 1019

DNS サーバーの設定 1020

ハードウェア バイパスおよびデュアル電源（Cisco ISA 3000）の設定 1023

ASP（高速セキュリティ パス）のパフォーマンスと動作の調整 1025

ルール エンジンのトランザクション コミット モデルの選択 1025

ASP ロード バランシングの有効化 1027

DNS キャッシュのモニタリング 1028

基本設定の履歴 1028

第 24 章 DHCP サービスと DDNS サービス 1033

DHCP サービスと DDNS サービスについて 1033

DHCPv4 サーバについて 1033

DHCP オプション 1033

DHCPv6 ステートレス サーバーについて 1034

DHCP リレー エージェントについて 1035

VTI での DHCP リレーサーバーのサポート 1035

DHCP サービスと DDNS サービスのガイドライン 1036

DHCP サーバーの設定 1038

DHCPv4 サーバーの有効化 1038

高度な DHCPv4 オプションの設定 1040

DHCPv6 ステートレス サーバーの設定 1042
DHCP リレー エージェントの設定 1044
DHCPv4 リレー エージェントの設定 1045
DHCPv6 リレー エージェントの設定 1047
ダイナミック DNS の設定 1048
DHCP および DDNS サービスのモニタリング 1054
DHCP サービスのモニタリング 1054
VTI を介した DHCP リレーのトラブルシューティング 1057
DDNS ステータスのモニタリング 1058
DHCP および DDNS サービスの履歴 1060

第 25 章 デジタル証明書 1063
デジタル証明書の概要 1063
公開キー暗号化 1064
証明書のスケーラビリティ 1065
キーペア 1065
トラストポイント 1066
認証登録 1066
SCEP 要求のプロキシ 1067
失効チェック 1067
サポート対象の CA サーバー 1067
CRL 1068
OCSP 1069
証明書とユーザー ログイン クレデンシャル 1070
ユーザー ログイン クレデンシャル 1071
証明書 1071
デジタル証明書のガイドライン 1072
デジタル証明書の設定 1075
キーペアの設定 1075
トラストポイントの設定 1078
トラストポイントの CRL の設定 1084

トラストポイント設定のエクスポートまたはインポート 1087
CA 証明書マップ ルールの設定 1089
参照 ID の設定 1091
手動での証明書の取得 1093
SCEP を使用した証明書の自動取得 1095
SCEP 要求のプロキシ サポートの設定 1096
特定の証明書タイプの設定方法 1099
CA 証明書 1099
CA サーバー管理 1099
証明書の有効期限アラートの設定（ID 証明書または CA 証明書用） 1101
デジタル証明書のモニタリング 1101
証明書管理の履歴 1104

第 26 章 **ARP インスペクションおよび MAC アドレス テーブル** 1109
ARP インスペクションと MAC アドレス テーブルについて 1109
ブリッジグループ トラフィックの ARP インスペクション 1109
MAC アドレス テーブル 1110
デフォルト設定 1111
ARP インスペクションと MAC アドレス テーブルのガイドライン 1111
ARP インスペクションとその他の ARP パラメータの設定 1111
スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ 1112
ARP インスペクションの有効化 1114
トランスペアレント モードのブリッジグループにおける MAC アドレス テーブルの 1114
ブリッジ グループのスタティック MAC アドレスの追加 1114
MAC アドレス タイムアウトを設定する 1115
MAC アドレスラーニングの設定 1115
ARP インスペクションと MAC アドレス テーブルのモニタリング 1116
ARP インスペクションと MAC アドレス テーブルの履歴 1117

第 V 部： **IP ルーティング** 1121

第 27 章 ルーティングの概要 1123
パスの決定 1123
サポートされるルート タイプ 1124
スタティックとダイナミックの比較 1124
シングルパスとマルチパスの比較 1125
フラットと階層型の比較 1125
リンクステートと距離ベクトル型の比較 1125
ルーティングでサポートされるインターネット プロトコル 1126
ルーティングテーブル 1127
ルーティング テーブルへの入力方法 1127
ルートのアドミニストレーティブ ディスタンス 1128
ダイナミック ルーロとフローティング スタティック ルートのバックアップ 1129
転送の決定方法 1129
ダイナミック ルーティングおよび フェールオーバー 1130
ダイナミック ルーティングおよびクラスタリング 1130
スパンド EtherChannel モードでのダイナミック ルーティング 1130
個別インターフェイス モードでのダイナミック ルーティング 1131
マルチ コンテキスト モードのダイナミック ルーティング 1133
ルートのリソース管理 1133
管理トラフィック用ルーティングテーブル 1134
管理インターフェイスの識別 1135
Equal-Cost Multipath（ECMP）ルーティング 1135
プロキシ ARP 要求のディセーブル化 1136
ルーティング テーブルの表示 1137
ルート概要の履歴 1138

第 28 章 スタティック ルートとデフォルト ルート 1139
スタティック ルートとデフォルト ルートについて 1139
デフォルトルート 1139
スタティック ルート 1140

不要なトラフィックをドロップするための null0 インターフェイスへのルート 1140
ルートのプライオリティ 1140
トランスペアレント ファイアウォール モードおよびブリッジ グループのルート 1141
スタティック ルート トラッキング 1141
スタティック ルートとデフォルト ルートのガイドライン 1142
デフォルト ルートおよびスタティック ルートの設定 1143
デフォルト ルートの設定 1143
スタティック ルートの設定 1145
スタティック ルート トラッキングの設定 1146
スタティック ルートまたはデフォルト ルートのモニタリング 1148
スタティック ルートまたはデフォルト ルートの例 1148
スタティック ルートおよびデフォルト ルートの履歴 1149

第 29 章 ポリシーベースルーティング 1151
ポリシーベース ルーティングについて 1151
ポリシーベース ルーティングを使用する理由 1152
同等アクセスおよび送信元依存ルーティング 1152
QoS 1152
コスト節約 1153
ロード シェアリング 1153
PBR の実装 1153
ポリシーベース ルーティングのガイドライン 1154
パスモニタリング 1156
パスモニタリングの設定 1157
ポリシーベース ルーティングの設定 1157
ポリシーベース ルーティングの例 1162
ルート マップ コンフィギュレーションの例 1162
PBR の設定例 1164
ソフトウェアデファインド WAN を使用したダイレクト インターネット アクセス 1165
アクションでのポリシーベース ルーティング 1168
ポリシーベース ルーティングの履歴 1172

第 30 章 ルート マップ 1175

ルート マップについて 1175

permit 句と deny 句 1176

match 句と set 句の値 1176

ルート マップのガイドライン 1177

ルート マップの定義 1177

ルート マップのカスタマイズ 1178

特定の宛先アドレスに一致するルートの定義 1178

ルート アクションのメトリック値の設定 1179

ルート マップの例 1180

ルート マップの履歴 1181

第 31 章 双方向フォワーディング検出ルーティング 1183

BFD ルーティングについて 1183

BFD 非同期モードおよびエコー機能 1183

BFD セッション確立 1184

BFD タイマー ネゴシエーション 1186

BFD 障害検出 1187

BFD 導入シナリオ 1187

BFD ルーティングのガイドライン 1188

BFD の設定 1188

BFD テンプレートの作成 1189

BFD インターフェイスの設定 1191

BFD マップの設定 1192

BFD のモニタリング 1193

BFD ルーティングの履歴 1194

第 32 章 BGP 1195

BGPについて 1195

BGP を使用する状況 1195

ルーティング テーブルの変更 1196
BGP パスの選択 1197
BGP マルチパス 1198
BGP のガイドライン 1199
BGP の設定 1200
BGP の有効化 1200
BGP ルーティング プロセスの最適なパスの定義 1202
ポリシー リストの設定 1203
AS パス フィルタの設定 1204
コミュニティ ルールの設定 1205
IPv4 アドレス ファミリの設定 1206
IPv4 ファミリの一般設定 1206
IPv4 ファミリ集約アドレスの設定 1209
IPv4 ファミリのフィルタリング設定 1210
IPv4 ファミリの BGP ネイバーの設定 1211
IPv4 ネットワークの設定 1218
IPv4 再配布の設定 1219
IPv4 ルート注入の設定 1220
IPv6 アドレス ファミリの設定 1221
IPv6 ファミリの一般設定 1221
IPv6 ファミリ集約アドレスの設定 1222
IPv6 ファミリの BGP ネイバーの設定 1224
IPv6 ネットワークの設定 1230
IPv6 再配布の設定 1231
IPv6 ルート注入の設定 1233
BGP のモニタリング 1234
BGP の例 1236
BGP の履歴 1239

第 33 章 **Open Shortest Path First（OSPF） 1241**
OSPF について 1241

fast hello パケットに対する OSPF のサポート 1243
Fast Hello パケットに対する OSPF サポートの前提条件 1243
fast hello パケットに対する OSPF のサポートについて 1243
OSPFv2 および OSPFv3 間の実装の差異 1244
OSPF のガイドライン 1245
OSPFv2 の設定 1249
認証用のキー チェーンの設定 1250
OSPFv2 ルータ ID の設定 1253
OSPF ルータ ID の手動設定 1253
移行中のルータ ID の挙動 1254
OSPF fast hello パケットの設定 1254
OSPFv2 のカスタマイズ 1255
OSPFv2 へのルートの再配布 1255
OSPFv2 にルートを再配布する場合のルート集約の設定 1257
ルート サマリー アドレスの追加 1257
OSPFv2 エリア間のルート集約の設定 1258
OSPFv2 インターフェイス パラメータの設定 1259
OSPFv2 エリア パラメータの設定 1263
OSPFv2 フィルタ ルールの設定 1264
OSPFv2 NSSA の設定 1265
クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3） 1266
スタティック OSPFv2 ネイバーの定義 1267
ルート計算タイマーの設定 1268
ネイバーの起動と停止のロギング 1268
認証用のキー チェーンの設定 1269
OSPFv3 の設定 1272
OSPFv3 の有効化 1272
OSPFv3 インターフェイス パラメータの設定 1273
OSPFv3 ルータ パラメータの設定 1279
OSPFv3 エリア パラメータの設定 1282
OSPFv3 受動インターフェイスの設定 1284

OSPFv3 アドミニストレーティブ ディスタンスの設定 1285
OSPFv3 タイマーの設定 1285
スタティック OSPFv3 ネイバーの定義 1288
OSPFv3 デフォルト パラメータのリセット 1288
Syslog メッセージの送信 1290
Syslog メッセージの抑止 1290
集約ルート コストの計算 1291
OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成 1291
IPv6 サマリー プレフィックスの設定 1292
IPv6 ルートの再配布 1293
グレースフル リスタートの設定 1295
機能の設定 1296
OSPFv2 のグレースフル リスタートの設定 1296
OSPFv2 の Cisco NSF グレースフル リスタートの設定 1297
OSPFv2 の IETF NSF グレースフル リスタートの設定 1297
OSPFv3 のグレースフル リスタートの設定 1298
OSPF のグレースフル リスタート待機タイマーの設定 1299
OSPFv2 設定の削除 1300
OSPFv3 設定の削除 1300
OSPFv2 の例 1301
OSPFv3 の例 1302
OSPF のモニタリング 1303
OSPF の履歴 1308

第 34 章 **IS-IS** 1311
IS-IS について 1311
NET について 1312
IS-IS ダイナミック ホスト名 1312
IS-IS での PDU のタイプ 1313
マルチアクセス回線での IS-IS の動作 1314
IS-IS での代表 IS の選択 1315

IS-IS LSPDB の同期 1316
IS-IS 最短パスの計算 1317
IS-IS シャットダウン プロトコル 1318
IS-IS の前提条件 1318
IS-IS のガイドライン 1319
IS-IS の設定 1319
IS-IS ルーティングのグローバルな有効化 1320
IS-IS 認証の有効化 1324
IS-IS LSP の設定 1329
IS-IS サマリー アドレスの設定 1333
IS-IS パッシブ インターフェイスの設定 1334
IS-IS インターフェイスの設定 1335
IS-IS インターフェイス hello パディングの設定 1340
IS-IS IPv4 アドレス ファミリの設定 1343
IS-IS IPv6 アドレス ファミリの設定 1349
IS-IS の監視 1354
IS-IS の履歴 1357
IS-IS の例 1357

第 35 章 EIGRP 1367
EIGRP について 1367
EIGRP のガイドライン 1369
EIGRP の設定 1370
EIGRP のイネーブル化 1371
EIGRP スタブ ルーティングのイネーブル化 1371
EIGRP のカスタマイズ 1373
EIGRP ルーティング プロセスのネットワークの定義 1373
EIGRP のインターフェイスの設定 1374
パッシブ インターフェイスの設定 1376
インターフェイスでのサマリー集約アドレスの設定 1377
インターフェイス遅延値の変更 1378

インターフェイスでの EIGRP 認証のイネーブル化 1379
EIGRP ネイバーの定義 1381
EIGRP へのルート再配布 1382
EIGRP でのネットワークのフィルタリング 1384
EIGRP Hello 間隔と保持時間のカスタマイズ 1385
自動ルート集約の無効化 1387
EIGRP でのデフォルト情報の設定 1387
EIGRP スプリット ホライズンのディセーブル化 1389
EIGRP プロセスの再始動 1390
EIGRPv6 プロセスの設定 1390
EIGRPv6 の有効化 1390
EIGRPv6 のフィルタルール 1391
EIGRPv6 のインターフェイスの設定 1392
EIGRPv6 のパッシブインターフェイスの設定 1393
EIGRPv6 へのルートの再配布 1394
EIGRPv6 ネイバーの定義 1395
EIGRP のモニタリング 1396
EIGRP の例 1397
EIGRP の履歴 1399

第 36 章 マルチキャスト ルーティング 1401
マルチキャスト ルーティングについて 1401
スタブ マルチキャスト ルーティング 1402
PIM マルチキャスト ルーティング 1402
PIM Source Specific Multicast のサポート 1402
PIM ブートストラップ ルータ（BSR） 1403
PIM ブートストラップ ルータ（BSR）の用語 1403
マルチキャスト グループの概念 1404
マルチキャスト アドレス 1404
クラスタ 1404
マルチキャスト ルーティングのガイドライン 1405

マルチキャスト ルーティングの有効化 1406
マルチキャスト ルーティングのカスタマイズ 1406
スタブ マルチキャスト ルーティングの設定と IGMP メッセージの転送 1407
スタティック マルチキャスト ルートの設定 1407
IGMP 機能の設定 1408
インターフェイスでの IGMP の有効化 1408
IGMP グループ メンバーシップの設定 1409
スタティック加入した IGMP グループの設定 1409
マルチキャスト グループへのアクセスの制御 1410
インターフェイスにおける IGMP 状態の数の制限 1411
マルチキャスト グループに対するクエリー メッセージの変更 1412
IGMP バージョンの変更 1413
PIM 機能の設定 1414
インターフェイスでの PIM の有効化またはディセーブル化 1414
スタティック ランデブー ポイント アドレスの設定 1415
指定ルータのプライオリティの設定 1415
PIM 登録メッセージの設定とフィルタリング 1416
PIM メッセージ間隔の設定 1416
PIM ネイバーのフィルタリング 1417
双方向ネイバー フィルタの設定 1418
BSR 候補としての ASA の設定 1419
マルチキャスト境界の設定 1420
PIM のモニタリング 1421
マルチキャスト ルーティングの例 1421
マルチキャスト ルーティングの履歴 1422

第 VI 部： AAA サーバーおよびローカル データベース 1425

第 37 章 AAA サーバーとローカル データベース 1427
AAA とローカル データベースについて 1427
認証 1427

認証 1428
アカウンティング 1428
認証、認可、アカウンティング間の相互作用 1428
AAA サーバーおよびサーバーグループ 1428
ローカル データベースについて 1430
フォールバック サポート 1431
グループ内の複数のサーバーを使用したフォールバックの仕組み 1432
ローカル データベースのガイドライン 1432
ローカル データベースへのユーザー アカウントの追加 1432
ローカル データベースのモニタリング 1435
ローカル データベースの履歴 1436

第 38 章 **AAA の RADIUS サーバー** 1441
AAA 用の RADIUS サーバーについて 1441
サポートされている認証方式 1441
VPN 接続のユーザー認証 1442
RADIUS 属性のサポートされるセット 1442
サポートされる RADIUS 認証属性 1443
サポートされる IETF RADIUS 認証属性 1452
RADIUS アカウンティング切断の理由コード 1453
AAA の RADIUS サーバーのガイドライン 1454
AAA 用の RADIUS サーバーの設定 1455
RADIUS サーバ グループの設定 1455
グループへの RADIUS サーバーの追加 1459
AAA 用の RADIUS サーバーのモニタリング 1462
AAA 用の RADIUS サーバーの履歴 1463

第 39 章 **AAA 用の TACACS+ サーバー** 1465
AAA 用の TACACS+ サーバーについて 1465
TACACS+ 属性 1465
AAA 用の TACACS+ サーバーのガイドライン 1467

TACACS+ サーバーの設定 1467
TACACS+ サーバー グループの設定 1468
グループへの TACACS+ サーバーの追加 1470
AAA 用の TACACS+ サーバーのモニタリング 1471
AAA 用の TACACS+ サーバーの履歴 1471

第 40 章 **AAA の LDAP サーバー** 1473
LDAP および ASA について 1473
LDAP での認証方法 1473
LDAP 階層 1474
LDAP 階層の検索 1474
LDAP サーバーへのバインド 1475
LDAP 属性マップ 1476
AAA の LDAP サーバーのガイドライン 1477
AAA の LDAP サーバーの設定 1478
LDAP 属性マップの設定 1478
LDAP サーバー グループの設定 1480
VPN の LDAP 認証の設定 1483
AAA の LDAP サーバーのモニタリング 1484
AAA の LDAP サーバーの履歴 1485

第 41 章 **AAA の RSA SecurID サーバー** 1487
RSA SecurID サーバーについて 1487
AAA の RSA SecurID サーバーのガイドライン 1487
AAA の RSA SecurID サーバーの設定 1488
RSA SecurID AAA サーバーグループの設定 1488
SDI サーバーグループへの RSA SecurID サーバーの追加 1489
SDI ノードシークレットファイルのインポート 1490
AAA の RSA SecurID サーバーのモニタリング 1491
AAA の RSA SecurID サーバーの履歴 1492

第 VII 部： システム管理 1493

第 42 章 管理アクセス 1495

管理リモート アクセスの設定 1495

SSH アクセスの設定 1495

SSH サーバーを有効化 1496

パスワード アクセス用の SSH の設定 1499

公開キー アクセス用の SSH の設定 1501

Telnet アクセスの設定 1505

ASDM、その他のクライアントの HTTPS アクセスの設定 1507

ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定 1510

VPN トンネルを介した管理アクセスの設定 1510

コンソール タイムアウトの変更 1512

CLI プロンプトのカスタマイズ 1512

ログイン バナーの設定 1513

管理セッション クォータの設定 1515

システム管理者用 AAA の設定 1516

管理認証の設定 1516

管理認証について 1516

CLIおよびASDM アクセス認証の設定 1518

enable コマンド認証の設定（特権 EXEC モード） 1519

ASDM 証明書認証の設定 1521

管理許可による CLI および ASDM アクセスの制限 1522

コマンド認可の設定 1525

コマンド認可について 1525

ローカル コマンド許可の設定 1527

TACACS+ サーバーでのコマンドの設定 1529

TACACS+ コマンド許可の設定 1532

ローカル データベース ユーザーのパスワード ポリシーの設定 1533

パスワードの変更 1536

ログインの履歴を有効にして表示する 1536
管理アクセス アカウンティングの設定 1537
ロックアウトからの回復 1538
デバイス アクセスのモニタリング 1540
管理アクセスの履歴 1542

第 43 章 ソフトウェアおよびコンフィギュレーション 1553
ソフトウェアのアップグレード 1553
ROMMON を使用したイメージのロード（ISA 3000） 1553
ROMMON イメージのアップグレード（ISA 3000） 1555
ソフトウェアのダウングレード 1557
ダウングレードに関するガイドラインおよび制限事項 1557
ダウングレード後に削除される互換性のない設定 1559
ASA アプライアンスのダウングレード 1560
Firepower 4100/9300 のダウングレード 1561
ISA 3000 のダウングレード 1562
ファイルの管理 1563
フラッシュ メモリ内のファイルの表示 1563
フラッシュ メモリからのファイルの削除 1564
フラッシュ ファイル システムの削除 1564
ファイル アクセスの設定 1565
FTP クライアント モードの設定 1565
ASA セキュアコピークライアントの設定 1565
ASA TFTP クライアントのパス設定 1567
ASA へのファイルのコピー 1568
スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー 1571
ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定 1573
コンフィギュレーションまたはその他のファイルのバックアップと復元 1577
完全なシステム バックアップまたは復元の実行 1577
バックアップまた復元を開始する前に 1577

システムのバックアップ 1579
バックアップの復元 1580
自動バックアップおよび復元の設定（ISA 3000） 1582
自動バックアップの設定（ISA 3000） 1582
自動復元の設定（ISA 3000） 1583
シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ 1585
フラッシュ メモリ内のコンテキスト コンフィギュレーションまたはその他のファイルのバック アップ 1586
コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ 1588
端末ディスプレイからのコンフィギュレーションのコピー 1588
export および import コマンドを使用した追加ファイルのバックアップ 1589
スクリプトを使用したファイルのバックアップおよび復元 1589
バックアップおよび復元スクリプトを使用する前に 1590
スクリプトを実行する 1590
サンプルスクリプト 1591
Cisco Secure Firewall 3100/4200 での SSD のホットスワップ 1596
USB ポートの無効化 1598
ソフトウェアとコンフィギュレーションの履歴 1600

第 44 章 システム イベントに対する応答の自動化 1603
EEM について 1603
サポートされるイベント 1603
イベント マネージャ アプレットのアクション 1604
出力先 1604
EEM のガイドライン 1605
EEM の設定 1605
イベント マネージャ アプレットの作成とイベントの設定 1606
アクションおよびアクションの出力先の設定 1608
イベント マネージャ アプレットの実行 1610
トラック メモリ割り当ておよびメモリ使用量 1610

EEM の例 1613
EEM のモニタリング 1614
EEM の履歴 1615

第 45 章 テストとトラブルシューティング 1617
イネーブル パスワードと Telnet パスワードの回復 1617
ISA 3000 でのパスワードの回復 1617
ASA 仮想 のパスワードまたはイメージの回復 1619
ISA 3000 ハードウェアのパスワード回復の無効化 1620
デバッグ メッセージの表示 1621
パケット キャプチャ 1622
パケット キャプチャのガイドライン 1622
パケットのキャプチャ 1623
パケット キャプチャの表示 1627
クラッシュ ダンプの表示 1629
コア ダンプの表示 1629
CPU 使用率とレポート 1629
の vCPU 使用率ASA 仮想 1629
CPU 使用率の例 1630
VMware の CPU 使用率のレポート 1630
ASA 仮想 と vCenter のグラフ 1631
Amazon CloudWatch CPU 使用率レポート 1631
ASA 仮想 と Amazon CloudWatch のグラフ 1632
Azure の CPU 使用率レポート 1632
ASA 仮想 と Azure のグラフ 1633
Hyper-V CPU 使用率レポート 1633
ASA Virtual と Hyper-V のグラフ 1634
OCI CPU 使用率レポート 1634
ASA 仮想 と OCI のグラフ 1635
設定のテスト 1635
基本接続のテスト：アドレス向けの ping の実行 1635

ping で実行可能なテスト 1636
ICMP ping と TCP ping の選択 1636
ICMP の有効化 1637
ホストの ping 1638
ASA 接続の体系的なテスト 1640
ホストまでのルートの追跡 1643
トレース ルート上の ASA の表示 1643
パケット ルートの決定 1645
パケット トレーサを使用したポリシー設定のテスト 1647
接続のモニタリング 1649
テストおよびトラブルシューティングの履歴 1650

第 VIII 部： モニタリング 1653

第 46 章 ロギング 1655
ロギングの概要 1655
マルチ コンテキスト モードでのロギング 1656
syslog メッセージ分析 1656
syslog メッセージ形式 1657
重要度レベル 1658
syslog メッセージ フィルタリング 1659
syslog メッセージ クラス 1659
カスタム メッセージ リスト 1662
クラスタ 1663
ロギングのガイドライン 1663
ロギングの設定 1665
ロギングの有効化 1665
出力先の設定 1666
外部 syslog サーバーへの syslog メッセージの送信 1666
内部ログ バッファへの syslog メッセージの送信 1670
電子メール アドレスへの syslog メッセージの送信 1672

ASDM への syslog メッセージの送信 1674
コンソール ポートへの syslog メッセージの送信 1675
SNMP サーバーへの syslog メッセージの送信 1675
Telnet または SSH セッションへの syslog メッセージの送信 1676
syslog メッセージの設定 1676
Syslog での無効なユーザー名の表示または非表示 1676
syslog メッセージに日付と時刻を含める 1677
syslog メッセージの無効化 1677
syslog メッセージの重大度の変更 1678
スタンバイ装置の syslog メッセージのブロック 1678
非 EMBLEM 形式の syslog メッセージにデバイス ID を含める 1679
カスタム イベント リストの作成 1680
ロギング フィルタの設定 1681
指定した出力先へのクラス内のすべての syslog メッセージの送信 1681
syslog メッセージの生成レートの制限 1682
ログのモニタリング 1682
ロギングの例 1683
ロギングの履歴 1684

第 47 章 SNMP 1689
SNMP について 1689
SNMP の用語 1690
MIB およびトラップ 1691
SNMP オブジェクト識別子 1693
物理ベンダー タイプ値 1696
MIB でサポートされるテーブルおよびオブジェクト 1696
サポートされるトラップ（通知） 1698
インターフェイスの種類と例 1704
SNMP バージョン 3 の概要 1705
セキュリティ モデル 1706
SNMP グループ 1706

SNMP ユーザー 1706
SNMP ホスト 1706
ASA と Cisco IOS ソフトウェアの実装の相違点 1707
SNMP syslog メッセージ 1707
アプリケーション サービスとサードパーティ ツール 1707
SNMP のガイドライン 1708
SNMP の構成 1712
SNMP エージェントおよび SNMP サーバーの有効化 1713
SNMP トラップの設定 1713
CPU 使用率のしきい値の設定 1715
物理インターフェイスのしきい値の設定 1715
SNMP バージョン 1 または 2c のパラメータの設定 1716
SNMP バージョン 3 のパラメータの設定 1717
ユーザーのグループの設定 1721
ネットワーク オブジェクトへのユーザーの関連付け 1722
SNMP モニタリング 1723
SNMP の例 1724
SNMP の履歴 1725

第 48 章 **Cisco Success Network とテレメトリデータ 1733**
Cisco Success Network について 1733
サポートされるプラットフォームと必要な設定 1734
ASA テレメトリデータが SSE クラウドに到達する仕組み 1734
Cisco Success Networkの有効化または無効化 1734
ASA テレメトリデータの表示 1735
Cisco Success Network - テレメトリデータ 1736
デバッグテレメトリデータ 1742

第 49 章 **Anonymous Reporting および Smart Call Home 1745**
Anonymous Reporting について 1745
DNS 要件 1746

Smart Call Home の概要 1746
アラート グループへの登録 1747
アラート グループの属性 1748
アラート グループによって Cisco に送信されるメッセージ 1748
メッセージ重大度しきい値 1751
サブスクリプション プロファイル 1752
Anonymous Reporting および Smart Call Home のガイドライン 1753
Anonymous Reporting および Smart Call Home の設定 1754
Anonymous Reporting の設定 1755
Smart Call Home の設定 1755
Smart Call Home のイネーブル化 1756
認証局のトラスト ポイントの宣言および認証 1757
環境およびスナップショット アラート グループの設定 1758
アラート グループ サブスクリプションの設定 1758
顧客連絡先情報の設定 1760
メール サーバーの設定 1761
トラフィック レートの制限の設定 1762
Smart Call Home 通信の送信 1763
宛先プロファイルの設定 1764
宛先プロファイルのコピー 1765
宛先プロファイルの名前の変更 1766
Anonymous Reporting および Smart Call Home のモニタリング 1767
Smart Call Home の例 1768
Anonymous Reporting および Smart Call Home の履歴 1769

第 IX 部： 参照先 1771

第 50 章 コマンドライン インターフェイスの使用 1773
ファイアウォール モードとセキュリティ コンテキスト モード 1773
コマンドのモードとプロンプト 1774
構文の書式 1775

コマンドの短縮形 1776
コマンドラインの編集 1776
コマンドの補完 1777
コマンドのヘルプ 1777
実行コンフィギュレーションの確認 1777
show コマンドおよび more コマンドの出力のフィルタリング 1778
show コマンド出力のリダイレクトと追加 1779
show コマンド出力の行数の取得 1780
コマンド出力のページング 1780
コメントの追加 1781
テキスト コンフィギュレーション ファイル 1781
テキスト ファイルでコマンドと行が対応する仕組み 1781
コマンド固有のコンフィギュレーション モード コマンド 1782
自動テキスト入力 1782
行の順序 1782
テキスト コンフィギュレーションに含まれないコマンド 1782
パスワード 1782
マルチセキュリティ コンテキスト ファイル 1783
サポートされている文字セット 1783

第 51 章 アドレス、プロトコル、およびポート 1785
IPv4 アドレスとサブネット マスク 1785
クラス 1785
プライベート ネットワーク 1786
サブネット マスク 1786
サブネットマスクの決定 1787
サブネットマスクに使用するアドレスの決定 1788
IPv6 アドレス 1789
IPv6 アドレスの形式 1789
IPv6 アドレス タイプ 1791
ユニキャスト アドレス 1791

マルチキャスト アドレス 1793
エニーキャスト アドレス 1795
必須アドレス 1795
IPv6 アドレス プレフィックス 1796
プロトコルとアプリケーション 1796
TCP ポートおよび UDP ポート 1797
ローカル ポートとプロトコル 1801
ICMP タイプ 1802

このマニュアルについて

ここでは、このガイドを使用する方法について説明します。

- 本書の目的 （lxi ページ）
- 関連資料 （lxi ページ）
- 表記法 （lxi ページ）
- 通信、サービス、およびその他の情報 （lxiii ページ）

本書の目的

このマニュアルは、コマンドライン インターフェイスを使用して Cisco Secure Firewall ASA シリーズの一般的な操作を設定する際に役立ちます。このマニュアルは、すべての機能を網羅しているわけではなく、ごく一般的なコンフィギュレーションの事例を紹介しています。

また、Web ベースの GUI アプリケーションである適応型セキュリティ デバイス マネージャ（ASDM）を使用して ASA を設定、監視することもできます。ASDM では、コンフィギュレーション ウィザードを使用して、いくつかの一般的なコンフィギュレーションを設定できます。また、あまり一般的ではない事例には、オンラインのヘルプが用意されています。

このマニュアルを通じて、「ASA」という語は、特に指定がない限り、サポートされているモデルに一般的に適用されます。

関連資料

詳細については、『*Navigating the Cisco ASA Series Documentation*』（http://www.cisco.com/go/asadocs）を参照してください。

表記法

このマニュアルでは、文字、表示、および警告に関する次の規則に準拠しています。

文字表記法

表記法	説明
boldface	コマンド、キーワード、ボタン ラベル、フィールド名、およびユーザー入力テキストは、**boldface**で示しています。メニューベース コマンドの場合は、メニュー項目を [ ] で囲み、コマンドのフル パスを示しています。
italic	ユーザーが値を指定する変数は、イタリック体で示しています。 イタリック体は、マニュアル タイトルと一般的な強調にも使用されています。
等幅	システムが表示するターミナル セッションおよび情報は、等幅文字で記載されます。
{x | y | z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
[ ]	システム プロンプトに対するデフォルトの応答も、角カッコで囲んで記載されます。
< >	パスワードなどの出力されない文字は、山カッコ（< >）で囲んで示しています。
!、#	コードの先頭に感嘆符（!）または番号記号（#）がある場合は、コメント行であることを示します。

読者への警告

このマニュアルでは、読者への警告に以下を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス	時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	「警告」の意味です。人身事故を予防するための注意事項が記述されています。

通信、サービス、およびその他の情報

- シスコからタイムリーな関連情報を受け取るには、Cisco Profile Manager でサインアップしてください。
- 重要な技術によって求めるビジネス成果を得るには、Cisco Services [英語] にアクセスしてください。
- サービス リクエストを送信するには、Cisco Support にアクセスしてください。
- 安全で検証済みのエンタープライズクラスのアプリケーション、製品、ソリューション、およびサービスを探して参照するには、Cisco DevNet にアクセスしてください。
- 一般的なネットワーキング、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。

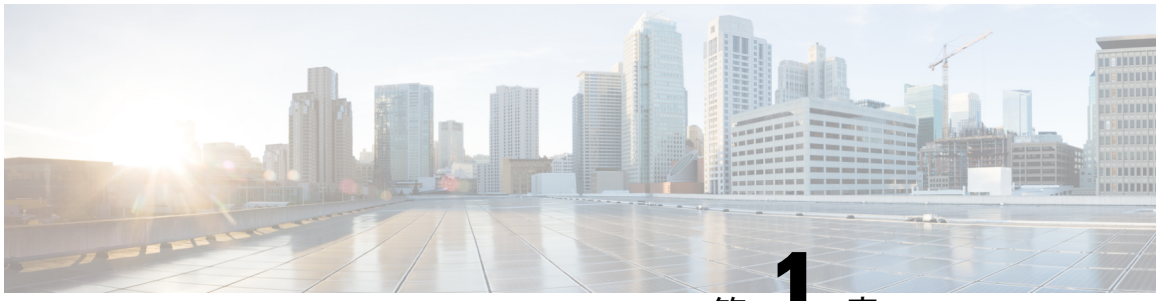
Cisco バグ検索ツール

Cisco Bug Search Tool（BST）は、シスコ製品とソフトウェアの障害と脆弱性の包括的なリストを管理する Cisco バグ追跡システムへのゲートウェイとして機能する、Web ベースのツールです。BST は、製品とソフトウェアに関する詳細な障害情報を提供します。

第 I 部

ASA の開始

- Cisco Secure Firewall ASA の概要 （1 ページ）
- はじめに （13 ページ）
- ライセンス：ISA 3000 の製品認証キーライセンス （47 ページ）
- ライセンス：スマート ソフトウェア ライセンシング （93 ページ）
- 論理デバイス Firepower 4100/9300 （205 ページ）
- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード （231 ページ）



第 1 章

Cisco Secure Firewall ASA の概要

Cisco Secure Firewall ASA は、高度なステートフル ファイアウォールおよび VPN コンセントレータ機能を 1 つのデバイスで提供します。ASA は、複数のセキュリティ コンテキスト（仮想ファイアウォールに類似）、クラスタリング（複数のファイアウォールを 1 つのファイアウォールに統合）、トランスペアレント（レイヤ 2）ファイアウォールまたはルーテッド（レイヤ 3）ファイアウォール オペレーション、高度なインスペクション エンジン、IPsec VPN、SSL VPN、クライアントレス SSL VPN サポートなど、多数の高度な機能を含みます。

- ハードウェアとソフトウェアの互換性 （1 ページ）
- VPN の互換性 （1 ページ）
- 新機能 （1 ページ）
- ファイアウォール機能の概要 （5 ページ）
- VPN 機能の概要 （9 ページ）
- セキュリティ コンテキストの概要 （10 ページ）
- ASA クラスタリングの概要 （11 ページ）
- 特殊なサービスおよびレガシー サービス （11 ページ）

ハードウェアとソフトウェアの互換性

サポートされるすべてのハードウェアおよびソフトウェアの一覧は、『Cisco ASA Compatibility』を参照してください。

VPN の互換性

『Supported VPN Platforms, Cisco ASA Series』を参照してください。

新機能

このセクションでは、各リリースの新機能を示します。

（注） syslog メッセージガイドに、新規、変更済み、および廃止された syslog メッセージを記載しています。

ASA 9.23(1) の新機能

リリース：**2025 年 3 月 5 日**

特長	説明
プラットフォーム機能	
Cisco Secure Firewall 1230/1240/1250	Cisco Secure Firewall 1230/1240/1250 は、1RU ラックマウント可能なファイアウォールです。
Cisco Secure Firewall 4200 の接続制限の引き上げ	最大接続数が引き上げられました。 • 4225：3,000 万 → **9,000 万** • 4245：6,000 万 → **18,000 万**
ファイアウォール機能	
RADIUS Message-Authenticator 属性のサポート。	Message-Authenticator 属性は、Blast- RADIUS 攻撃を防ぐために使用されます。メッセージオーセンティケータをサポートするようにRADIUSサーバーをアップグレードした場合は、このオプションを有効にして、Blast- RADIUS攻撃を防御できます。有効にする場合、すべての要求と応答にメッセージオーセンティケータが含まれている必要があります。含まれていない場合、認証は失敗します。 **message-authenticator-required** コマンドが追加されました。
新規 Umbrella API。	秘密キーを持つ API キーを使用する Cisco Umbrella オープンAPIを使用して、Cisco Umbrella を設定できるようになりました。 次のコマンドが追加されました。 **token-request-credential**
フロー オフロードは Secure Firewall 3100/4200 に対してデフォルトで有効です	フロー オフロードはデフォルトで有効です。 追加/変更されたコマンド： **flow-offload enable**
高可用性とスケーラビリティの各機能	

特長	説明
すべての Cisco Secure Firewall 1200 モデルでマルチ コンテキストをサポート	マルチ コンテキスト モードのサポートが追加されました。Cisco Secure Firewall 1210/1220 • Cisco Secure Firewall 1210CE-5 コンテキスト。 • Cisco Secure Firewall 1210CP：5 コンテキスト。 • Cisco Secure Firewall 1220CX：10 コンテキスト。 スイッチポートはマルチ コンテキスト モードではサポートされていません。マルチ コンテキスト モードに変換する前に、すべてのインターフェイスをルータ インターフェイスに変換する必要があります。 Cisco Secure Firewall 1230/1240/1250 も最初のリリースでマルチ コンテキスト モードをサポートしています。 • Cisco Secure Firewall 1230：25 コンテキスト。 • Cisco Secure Firewall 1240：25 コンテキスト。 • Cisco Secure Firewall 1250：25 コンテキスト。
クラスタ リダイレクト： Cisco Secure Firewall 4200 非対称クラスタ トラフィックのフロー オフロードのサポート	非対称フローの場合、クラスタリダイレクトにより、転送ノードはハードウェアにフローをオフロードできます。この機能はデフォルトで有効になっています。 既存のフローのトラフィックが別のノードに送信されると、そのトラフィックはクラスタ制御リンクを介してオーナー ノードにリダイレクトされます。非対称フローは、クラスタ制御リンクに大量のトラフィックを作成する可能性があるため、フォワーダにこれらのフローをオフロードさせると、パフォーマンスが向上します。 追加/変更されたコマンド：**flow-offload cluster-redirect**、**show conn**、**show flow-offload flow**, , **show flow-offload flow protocol**、**show flow-offload info**。
フェールオーバー中のロールスイッチ時間の短縮	フェールオーバーが発生すると、新しいアクティブデバイスが MAC アドレスエントリごとにマルチキャストパケットを生成して、すべてのブリッジ グループ インターフェイスに送信し、アップストリームスイッチにルーティングテーブルを更新させます。マルチキャストパケットを生成してブリッジインターフェイスに送信するこのタスクは、データプレーンで非同期に実行されるようになったため、コントロールプレーンでの重要なフェールオーバータスクを遅延なく続行できます。 この機能拡張により、フェールオーバー中のロールスイッチ時間が短縮され、ダウンタイムが短縮されます。
クラスタノード参加時の MTU ping テスト	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
インターフェイス機能	

特長	説明
Cisco Secure Firewall 1210CP IEEE 802.3bt のサポート（PoE++ および Hi-PoE）	IEEE 802.3bt のサポートに関連する次の改善を確認してください。 • PoE++ と Hi-PoE：ポートあたり最大 90 W。 • シングルシグネチャおよびデュアルシグネチャの受電デバイス（PD）。 • パワーバジェットが先着順で行われます。 • **show power inline** にパワーバジェットフィールドが追加されました。 新規/変更されたコマンド：**power inline**、**show power inline**
ライセンス機能	
ASA 仮想に対する柔軟な永続ライセンスの予約	ASA 仮想の場合、RAM と vCPU に関係なく、モデル固有のライセンスを永続ライセンス予約用に設定できます。ASA 仮想に割り当てられたメモリに関係なく、永続ライセンスの予約ライセンスを切り替えることができます。また、モデルライセンスを変更せずに、 ASA 仮想 に割り当てられたメモリと vCPU を変更することもできます。 ASA 仮想 の 9.23.1 より前のバージョンにダウングレードすると、ライセンスのステータスが [未登録（Unregistered）] になります。柔軟な永続ライセンス予約で ASA 仮想 をダウングレードしないことをお勧めします。 次のコマンドが追加されました。 **license smart flex-model**
管理、モニタリング、およびトラブルシューティングの機能	
TLS デバイス証明書に対する Automated Certificate Management Environment（ACME）プロトコル	ASA トラストポイントに自動証明書管理環境（ACME）プロトコルを設定して、TLS デバイス証明書を管理できます。ACME は、自動更新、ドメイン検証、および簡単な登録と失効によって、簡素化された証明書管理を可能にします。認証に Let's Encrypt CA サーバーを使用するか、他の ACME サーバーを使用するかを選択できます。ACME は認証に http01 方式を使用します。 変更されたコマンド **crypto ca trustpoint enrollment protocol crypto ca authenticate**
VPN 機能	
Secure Firewall 4200 のクラスタリングを使用した分散型サイト間 VPN	Firepower 4200 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ノードだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。 新規または変更されたコマンド：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn-mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show conn detail**、**show crypto ikev2 stats**

特長	説明
分散型サイト間 VPN モードの Cisco Secure Firewall 4200 のクラスタ制御リンクのトラフィックの IPsec フローのオフロード	分散型サイト間 VPN モードの非対称フローの場合、IPsec フロー オフロードにより、フローオーナーは、クラスタ制御リンクを介して転送されたハードウェア内の IPsec トラフィックを復号できます。この機能は構成可能ではありません。IPsec フローのオフロードを有効にすると常に使用できます。 追加/変更されたコマンド： **flow-offload-ipsec**、**show crypto ipsec sa detail**

ファイアウォール機能の概要

ファイアウォールは、外部ネットワーク上のユーザーによる不正アクセスから内部ネットワークを保護します。また、ファイアウォールは、人事部門ネットワークをユーザー ネットワークから分離するなど、内部ネットワーク同士の保護も行います。Web サーバーまたは FTP サーバーなど、外部のユーザーが使用できるようにする必要のあるネットワーク リソースがあれば、ファイアウォールで保護された別のネットワーク（非武装地帯（DMZ）と呼ばれる）上に配置します。ファイアウォールによってDMZに許可されるアクセスは限定されますが、DMZにあるのは公開サーバーだけのため、この地帯が攻撃されても影響を受けるのは公開サーバーに限定され、他の内部ネットワークに影響が及ぶことはありません。また、特定アドレスだけに許可する、認証または認可を義務づける、または外部の URL フィルタリング サーバーと協調するといった手段によって、内部ユーザーが外部ネットワーク（インターネットなど）にアクセスする機会を制御することもできます。

ファイアウォールに接続されているネットワークに言及する場合、外部ネットワークはファイアウォールの手前にあるネットワーク、内部ネットワークはファイアウォールの背後にある保護されているネットワーク、そして *DMZ* はファイアウォールの背後にあるが、外部ユーザーに制限付きのアクセスが許されているネットワークです。ASA を使用すると、数多くのインターフェイスに対してさまざまなセキュリティポリシーが設定できます。このインターフェイスには、多数の内部インターフェイス、多数のDMZ、および必要に応じて多数の外部インターフェイスが含まれるため、ここでは、このインターフェイスの区分は一般的な意味で使用するだけです。

セキュリティ ポリシーの概要

他のネットワークにアクセスするために、ファイアウォールを通過することが許可されるトラフィックがセキュリティポリシーによって決められます。デフォルトでは、内部ネットワーク（高セキュリティ レベル）から外部ネットワーク（低セキュリティ レベル）へのトラフィックは、自由に流れることが ASA によって許可されます。トラフィックにアクションを適用してセキュリティ ポリシーをカスタマイズすることができます。

アクセス ルールによるトラフィックの許可または拒否

アクセスルールを適用することで、内部から外部に向けたトラフィックを制限したり、外部から内部に向けたトラフィックを許可したりできます。ブリッジグループ インターフェイスでは、EtherType アクセス ルールを適用して、非 IP トラフィックを許可できます。

NAT の適用

NAT の利点のいくつかを次に示します。

- 内部ネットワークでプライベート アドレスを使用できます。プライベート アドレスは、インターネットにルーティングできません。
- NAT はローカル アドレスを他のネットワークから隠蔽するため、攻撃者はホストの実際のアドレスを取得できません。
- NAT は、重複 IP アドレスをサポートすることで、IP ルーティングの問題を解決できます。

IP フラグメントからの保護

ASA は、IP グラグメント保護を提供します。この機能は、すべての ICMP エラー メッセージの完全なリアセンブリと、ASA 経由でルーティングされる残りの IP フラグメントの仮想リアセンブリを実行します。セキュリティ チェックに失敗したフラグメントは、ドロップされログに記録されます。仮想リアセンブリはディセーブルにできません。

HTTP、HTTPS、または FTP フィルタリングの適用

アクセス リストを使用して、特定の Web サイトまたは FTP サーバーへの発信アクセスを禁止できますが、このような方法でWebサイトの使用方法を設定し管理することは、インターネットの規模とダイナミックな特性から、実用的とはいえません。

ASA でクラウド Web セキュリティを設定できます。ASA は、Cisco Web セキュリティ アプライアンス（WSA）などの外部製品とともに使用することも可能です。

アプリケーション インスペクションの適用

インスペクション エンジンは、ユーザーのデータ パケット内に IP アドレッシング情報を埋め込むサービスや、ダイナミックに割り当てられるポート上でセカンダリ チャネルを開くサービスに必要です。これらのプロトコルは、ASA によるディープ パケット インスペクションの実行を必要とします。

QoS ポリシーの適用

音声やストリーミング ビデオなどのネットワーク トラフィックでは、長時間の遅延は許容されません。QoS は、この種のトラフィックにプライオリティを設定するネットワーク機能です。QoS とは、選択したネットワーク トラフィックによりよいサービスを提供するネットワークの機能です。

接続制限と TCP 正規化の適用

TCP 接続、UDP 接続、および初期接続を制限することができます。接続と初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。ASA では、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

TCP 正規化は、正常に見えないパケットをドロップするように設計された高度な TCP 接続設定で構成される機能です。

脅威検出のイネーブル化

スキャン脅威検出と基本脅威検出、さらに統計情報を使用して脅威を分析する方法を設定できます。

基本脅威検出は、DoS 攻撃などの攻撃に関係している可能性のあるアクティビティを検出し、自動的にシステム ログ メッセージを送信します。

典型的なスキャン攻撃では、あるホストがサブネット内の IP アドレスにアクセスできるかどうかを 1 つずつ試します（サブネット内の複数のホストすべてを順にスキャンするか、1 つのホストまたはサブネットの複数のポートすべてを順にスイープする）。スキャン脅威検出機能は、いつホストがスキャンを実行するかを判別します。トラフィック署名に基づく IPS スキャン検出とは異なり、ASA のスキャニング脅威検出機能は、スキャン アクティビティに関して分析できるホスト統計を含む膨大なデータベースを維持します。

ホスト データベースは、不審なアクティビティを追跡します。このようなアクティビティには、戻りアクティビティのない接続、閉じているサービス ポートへのアクセス、脆弱な TCP 動作（非ランダム IPID など）、およびその他の多くの動作が含まれます。

攻撃者に関するシステム ログ メッセージを送信するように ASA を設定できます。または、自動的にホストを排除できます。

ファイアウォール モードの概要

ASA は、次の 2 つのファイアウォール モードで動作します。

- ルーテッド
- Transparent

ルーテッド モードでは、ASA は、ネットワークのルータ ホップと見なされます。

トランスペアレント モードでは、ASA は「Bump In The Wire」または「ステルス ファイアウォール」のように動作し、ルータ ホップとは見なされません。ASA は「ブリッジグループ」の内部および外部インターフェイスと同じネットワークに接続します。

トランスペアレント ファイアウォールは、ネットワーク コンフィギュレーションを簡単にするために使用できます。トランスペアレント モードは、攻撃者からファイアウォールが見えな

いようにする場合にも有効です。トランスペアレントファイアウォールは、他の場合にはルーテッドモードでブロックされるトラフィックにも使用できます。たとえば、トランスペアレントファイアウォールでは、EtherTypeアクセスリストを使用するマルチキャストストリームが許可されます。

ルーテッドモードでブリッジグループの設定、およびブリッジグループと通常インターフェイスの間のルートの設定を行えるように、ルーテッドモードではIntegrated Routing and Bridgingをサポートしてます。ルーテッドモードでは、トランスペアレントモードの機能を複製できます。マルチコンテキストモードまたはクラスタリングが必要ではない場合、代わりにルーテッドモードを使用することを検討してください。

ステートフル インスペクションの概要

ASAを通過するトラフィックはすべて、アダプティブセキュリティアルゴリズムを使用して検査され、通過が許可されるか、またはドロップされます。単純なパケットフィルタは、送信元アドレス、宛先アドレス、およびポートが正しいかどうかはチェックできますが、パケットシーケンスまたはフラグが正しいかどうかはチェックしません。また、フィルタはすべてのパケットをフィルタと照合してチェックするため、処理が低速になる場合があります。

（注） TCPステートバイパス機能を使用すると、パケットフローをカスタマイズできます。

ただし、ASAのようなステートフルファイアウォールは、パケットの次のようなステートについて検討します。

- 新規の接続かどうか。

  新規の接続の場合、ASAは、パケットをアクセスリストと照合してチェックする必要があり、これ以外の各種のタスクを実行してパケットの許可または拒否を決定する必要があります。このチェックを行うために、セッションの最初のパケットは「セッション管理パス」を通過しますが、トラフィックのタイプに応じて、「コントロールプレーンパス」も通過する場合があります。

  セッション管理パスで行われるタスクは次のとおりです。

  - アクセスリストとの照合チェック
  - ルートルックアップ
  - NAT変換（xlates）の割り当て
  - 「ファストパス」でのセッションの確立

  ASAは、TCPトラフィックのファストパスに転送フローとリバースフローを作成します。ASAは、高速パスも使用できるように、UDP、ICMP（ICMPインスペクションがイネーブルの場合）などのコネクションレス型プロトコルの接続状態の情報も作成するので、これらのプロトコルもファストパスを使用できます。

（注） SCTP などの他の IP プロトコルの場合、ASA はリバース パス フローを作成しません。そのため、これらの接続を参照する ICMP エラー パケットはドロップされます。

レイヤ7インスペクションが必要なパケット（パケットのペイロードの検査または変更が必要）は、コントロール プレーン パスに渡されます。レイヤ 7 インスペクション エンジンは、2 つ以上のチャネルを持つプロトコルで必要です。2 つ以上のチャネルの 1 つは周知のポート番号を使用するデータ チャネルで、その他はセッションごとに異なるポート番号を使用するコントロール チャネルです。このようなプロトコルには、FTP、H.323、および SNMP があります。

- 確立済みの接続かどうか。

  接続がすでに確立されている場合は、ASA でパケットの再チェックを行う必要はありません。一致するパケットの大部分は、両方向で「ファースト」パスを通過できます。高速パスで行われるタスクは次のとおりです。

  - IP チェックサム検証
  - セッション ルックアップ
  - TCP シーケンス番号のチェック
  - 既存セッションに基づく NAT 変換
  - レイヤ 3 ヘッダー調整およびレイヤ 4 ヘッダー調整

  レイヤ7インスペクションを必要とするプロトコルに合致するデータ パケットも高速パスを通過できます。

  確立済みセッション パケットの中には、セッション管理パスまたはコントロール プレーン パスを引き続き通過しなければならないものがあります。セッション管理パスを通過するパケットには、インスペクションまたはコンテンツ フィルタリングを必要とする HTTP パケットが含まれます。コントロール プレーン パスを通過するパケットには、レイヤ 7 インスペクションを必要とするプロトコルのコントロール パケットが含まれます。

VPN 機能の概要

VPN は、TCP/IP ネットワーク（インターネットなど）上のセキュアな接続で、プライベートな接続として表示されます。このセキュアな接続はトンネルと呼ばれます。ASA は、トンネリング プロトコルを使用して、セキュリティ パラメータのネゴシエート、トンネルの作成および管理、パケットのカプセル化、トンネルを通したパケットの送信または受信、パケットのカプセル化の解除を行います。ASA は、双方向トンネルのエンドポイントとして機能します。たとえば、プレーン パケットを受信してカプセル化し、それをトンネルのもう一方のエンドポイントに送信することができます。そのエンドポイントで、パケットはカプセル化を解除され、最終的な宛先に送信されます。また、セキュリティ アプライアンスは、カプセル化されたパ

ケットを受信してカプセル化を解除し、それを最終的な宛先に送信することもできます。ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

ASA は、次の機能を実行します。

- トンネルの確立
- トンネル パラメータのネゴシエーション
- ユーザーの認証
- ユーザー アドレスの割り当て
- データの暗号化と復号化
- セキュリティ キーの管理
- トンネルを通したデータ転送の管理
- トンネル エンドポイントまたはルータとしての着信と発信のデータ転送の管理

ASA は、これらの機能を実行するためにさまざまな標準プロトコルを起動します。

セキュリティ コンテキストの概要

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、さまざまな機能がサポートされています。ただし、サポートされていない機能もあります。詳細については、機能に関する各章を参照してください。

マルチ コンテキスト モードの場合、ASA には、セキュリティ ポリシー、インターフェイス、およびスタンドアロン デバイスで設定できるほとんどのオプションを識別するコンテキストごとのコンフィギュレーションが含まれます。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただし、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。

ASA クラスタリングの概要

ASA クラスタリングを利用すると、複数の ASA をグループ化して、1 つの論理デバイスにすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ユニット上でのみ実行します。コンフィギュレーションは、メンバーユニットに複製されます。

特殊なサービスおよびレガシー サービス

一部のサービスのマニュアルは、主要な設定ガイドおよびオンライン ヘルプとは別の場所にあります。

特殊なサービスに関するガイド

特殊なサービスを利用して、たとえば、電話サービス（Unified Communications）用のセキュリティ プロキシを提供したり、ボットネット トラフィック フィルタリングを Cisco アップデート サーバーのダイナミック データベースと組み合わせて提供したり、Cisco Web セキュリティ アプライアンス用の WCCP サービスを提供したりすることにより、ASA と他のシスコ製品の相互運用が可能になります。これらの特殊なサービスの一部については、別のガイドで説明されています。

- 『Cisco ASA Botnet Traffic Filter Guide』
- 『Cisco ASA NetFlow Implementation Guide』
- 『Cisco ASA Unified Communications Guide』
- 『Cisco ASA WCCP Traffic Redirection Guide』
- 『SNMP Version 3 Tools Implementation Guide』

レガシー サービス ガイド

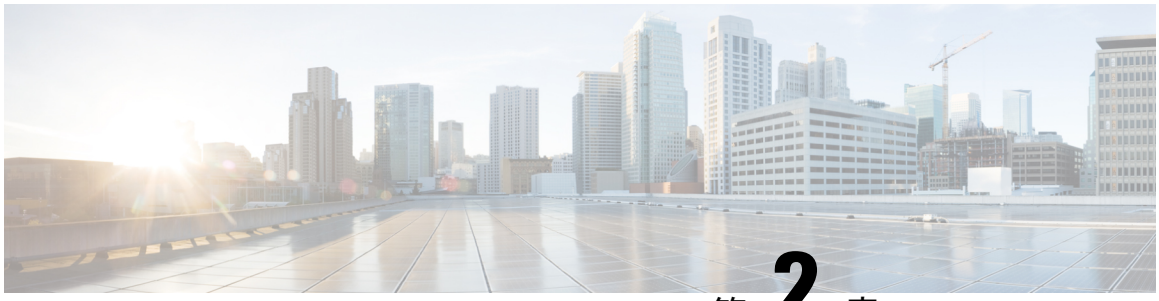
レガシー サービスは現在も ASA でサポートされていますが、より高度なサービスを代わりに使用できる場合があります。レガシー サービスについては別のガイドで説明されています。

『Cisco ASA Legacy Feature Guide』

このマニュアルの構成は、次のとおりです。

- RIP の設定
- ネットワーク アクセスの AAA 規則

- IP スプーフィングの防止などの保護ツールの使用（**ip verify reverse-path**）、フラグメント サイズの設定（**fragment**）、不要な接続のブロック（**shun**）、TCP オプションの設定（ASDM 用）、および基本 IPS をサポートする IP 監査の設定（**ip audit**）。
- フィルタリング サービスの設定



第 2 章

はじめに

この章では、ASA の使用を開始する方法について説明します。

- コマンドライン インターフェイス（CLI）のコンソールへのアクセス （13 ページ）
- ASDM アクセスの設定 （18 ページ）
- ASDM の起動 （21 ページ）
- 工場出荷時のデフォルト設定 （23 ページ）
- コンフィギュレーション作業 （39 ページ）
- 接続の設定変更の適用 （45 ページ）
- ASA のリロード （46 ページ）

コマンドラインインターフェイス（CLI）のコンソールへのアクセス

初期設定を行うには、コンソール ポートから直接 CLI にアクセスします。その後、管理アクセス （1495 ページ）に従って Telnet または SSH を使用して、リモート アクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソール ポートにアクセスするとシステムの実行スペースに入ります。

コンソールポートに接続したときに、読み取れない文字が表示される場合は、ポートの設定を確認してください。設定が正しい場合は、同じ設定を使用して別のデバイスでそのケーブルを試します。ケーブルに問題がない場合は、コンソールポートのハードウェアを交換する必要がある可能性があります。別のワークステーションでの接続を試みることも検討してください。

（注） ASA 仮想 のコンソールアクセスについては、ASA 仮想 のクイックスタートガイドを参照してください。

ISA 3000 コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

手順

ステップ 1 付属のコンソール ケーブルを使用してコンピュータをコンソール ポートに接続します。ターミナル エミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2 **Enter** キーを押して、次のプロンプトが表示されることを確認します。

```
ciscoasa>
```

このプロンプトは、ユーザー EXEC モードで作業していることを示します。ユーザー EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

Firepower 1000 、および Cisco Secure Firewall 1200/3100/4200 コンソールへのアクセス

Firepower 1000、およびCisco Secure Firewall 1200/3100/4200 コンソールポートを使用して、ASA CLI に接続します。ASA CLI から、トラブルシューティングのために Telnet を使用して FXOS CLI に接続できます。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。ご使用のオペレーティングシステムに必要なシリアルドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ASA CLIに接続します。デフォルトでは、コンソールアクセスに必要なユーザー クレデンシャルはありません。

ステップ 2 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

ASA で設定したイネーブルパスワードは、FXOS **管理者**のユーザーパスワードでもあり、ASA の起動に失敗した場合は、FXOS フェールセーフ モードに移行します。

設定以外のすべてのコマンドは、特権EXECモードで使用できます。特権EXECモードからコンフィギュレーション モードに入ることもできます。

特権 EXEC モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit**、**quit**、または **end** コマンドを入力します。

ステップ 4 （任意） FXOS CLI に接続します。

connect fxos [**admin**]

- **admin**：管理者レベルのアクセスを提供します。このオプションを指定しないと、ユーザーのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

FXOS 内では、**scope security/show audit-logs** コマンドを使用してユーザーアクティビティを表示できます。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Firepower 4100/9300 シャーシ 上の ASA コンソールへのアクセス

初期設定の場合、Firepower 4100/9300 シャーシ スーパバイザに（コンソール ポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイスにアクセスし、ASA セキュリティ モジュールに接続します。

手順

ステップ 1 Firepower 4100/9300 シャーシ スーパバイザ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* {**console** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

初めてモジュールにアクセスするときは、FXOS モジュールの CLI にアクセスします。その後 ASA アプリケーションに接続する必要があります。

connect asa

例：

```
Firepower# connect module 1 console
Firepower-module1> connect asa

asa>
```

ステップ 2 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
asa# configure terminal
asa(config)#
```

グローバル コンフィギュレーション モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 4 **Ctrl-a、d** と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

ステップ 5 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

ASDM アクセスの設定

ここでは、デフォルト設定で ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

ASDM アクセスの工場出荷時のデフォルト設定の使用

工場出荷時のデフォルトコンフィギュレーションでは、ASDM接続はデフォルトのネットワーク設定で事前設定されています。

手順

次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
  - Firepower 1010、Secure Firewall 1210/1220：管理用ネットワークインターフェース1/1（IPアドレス：192.168.45.1）、または内部イーサネットインターフェース1/2～1/8（1010および1210）または1/10（1220）（IPアドレス：192.168.1.1）。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
  - Firepower 1100、 Secure Firewall 1230/1240/1250/、3100、4200：内部イーサネット1/2（192.168.1.1）または管理用ポート1/1（DHCP経由）を使用。内部ホストは 192.168.1.0/24 ネットワークに限定されます。管理ホストは任意のネットワークからアクセスできます。
  - Firepower 4100/9300：展開時に定義された管理タイプ インターフェイスと IP アドレス。管理ホストは任意のネットワークからアクセスできます。
  - ASA 仮想：管理 0/0（展開時に設定）。管理ホストは管理ネットワークに限定されます。
  - ISA 3000：管理 1/1（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。

（注）
マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理コンテキストから ASDM にアクセスできるようになります。

関連トピック

工場出荷時のデフォルト設定 （23 ページ）
マルチ コンテキスト モードの有効化または無効化 （278 ページ）
ASDM の起動 （21 ページ）

ASDM アクセスのカスタマイズ

次の条件に *1* つ以上当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- 管理 IP アドレスを変更したい。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングル ルーテッド モードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理IPアドレスを設定できるオプションを備えた工場出荷時のデフォルトコンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ（トランスペアレント モードやマルチ コンテキスト モードの設定など）がある場合や、他の設定を維持する必要がある場合にのみ使用してください。

（注） ASAv の場合、導入時にトランスペアレント モードを設定できるため、この手順は、設定をクリアする必要がある場合など、導入後に特に役立ちます。

手順

ステップ 1 コンソール ポートで CLI にアクセスします。

ステップ 2 （オプション）トランスペアレント ファイアウォール モードをイネーブルにします。

このコマンドは、設定をクリアします。

firewall transparent

ステップ 3 管理インターフェイスを設定します。

```
interface interface_id
   nameif name
   security-level level
```

```
no shutdown
ip address ip_address mask
```

例：

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

ステップ 4 （直接接続された管理ホスト用）管理ネットワークの DHCP プールを設定します。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例：

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

その範囲にインターフェイス アドレスが含まれていないことを確認します。

ステップ 5 （リモート管理ホスト用）管理ホストへのルートを設定します。

route *management_ifc management_host_ip mask gateway_ip* **1**

例：

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

ステップ 6 ASDM の HTTP サーバーをイネーブルにします。

http server enable

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

http *ip_address mask interface_name*

例：

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

write memory

ステップ 9 （オプション）モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

関連トピック

工場出荷時のデフォルト設定の復元 （24 ページ）
ファイアウォール モードの設定 （243 ページ）
ISA 3000 コンソールへのアクセス （13 ページ）
ASDM の起動 （21 ページ）

ASDM の起動

ASDM-IDM ランチャを使用して ASDM を起動します。ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合、ランチャを再度ダウンロードする必要はありません。

ASDM では、管理のために別の ASA IP アドレスを選択できます。

ここでは、まず ASDM に接続する方法について説明し、次にランチャ

ASDM はローカルの \Users\<user_id>\.asdm ディレクトリ内にキャッシュ、ログ、設定などのファイルを保存し、Temp ディレクトリ内にも セキュアクライアント プロファイルなどのファイルを保存します。

手順

ステップ 1 ASDM クライアントとして指定したコンピュータで次の URL を入力します。

https://*asa_ip_address*/**admin**

（注）
http:// や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。ASA は、HTTP 要求を HTTPS に自動的に転送しません。

次のボタン

ASDM Launcher のインストール

ステップ 2 ランチャをダウンロードして、ASDM を起動するには、次の手順を実行します。

a) **[ASDM をインストールして、** をクリックします。

図 *1 : ASDM Launcher* のインストール

b) ユーザー名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。

HTTPS 認証が設定されていない場合は、ユーザー名および**イネーブル**パスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDM にログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定（1005 ページ）を参照してください。**注**：HTTPS 認証をイネーブルにした場合、ユーザー名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力すると、ASDM によってローカル データベースで一致がチェックされます。

c) インストーラをコンピュータに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
d) 管理IPアドレス、および同じユーザー名とパスワード（新規インストールの場合は空白）を入力し、[OK] をクリックします。

工場出荷時のデフォルト設定

工場出荷時のデフォルト設定とは、シスコが新しい ASA に適用したコンフィギュレーションです。

- Firepower 1010：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部スイッチ ポートから ASDM を使用して管理できます。
- Firepower 1100：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Secure Firewall 1210/1220：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部スイッチ ポートから ASDM を使用して管理できます。
- Secure Firewall 1230/1240/1250：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、管理インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Secure Firewall 3100：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、Management 1/1 インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Secure Firewall 4200：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、Management 1/1 インターフェイスまたは内部インターフェイスから ASDM を使用して管理できます。
- Firepower 4100/9300 シャーシ：ASA のスタンドアロンまたはクラスタを展開する場合、管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- ASA 仮想：ハイパーバイザによっては、展開の一環として、展開設定（初期の仮想展開設定）によって管理用のインターフェイスが設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。フェールオーバー IP アドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。
- ISA 3000：工場出荷時のデフォルト設定は、同じネットワーク上のすべての内部および外部インターフェイスを使用した、ほぼ完全なトランスペアレント ファイアウォール モー

ド設定です。ASDM を使用して管理インターフェイスに接続し、ネットワークの IP アドレスを設定できます。ハードウェアバイパスは2つのインターフェイスペアに対して有効になっていて。

アプライアンスの場合、工場出荷時のデフォルト設定は、工場出荷時のデフォルト設定がトランスペアレントモードでのみ使用可能な ISA 3000 を除き、ルーテッド ファイアウォール モードとシングルコンテキストモードのみで使用できます。ASA 仮想 および Firepower 4100/9300 シャーシ の場合、展開時にトランスペアレントモードまたはルーテッドモードを選択できます。

（注） イメージ ファイルと（隠された）デフォルト コンフィギュレーションに加え、log/、crypto_archive/、および coredumpinfo/coredump.cfg がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージ ファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

工場出荷時のデフォルト設定の復元

この項では、工場出荷時のデフォルトコンフィギュレーションを復元する方法について説明します。ASA 仮想 では、この手順を実行することで展開設定が消去され、次の設定が適用されます。

```
interface management 0/0
  ip address 192.168.1.1 255.255.255.0
  nameif management
  security-level 100
  no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

（注） Firepower 4100/9300 では、工場出荷時のデフォルト設定を復元すると単に設定が消去されるだけです。 デフォルト設定を復元するには、スーパバイザから ASA をもう一度展開する必要があります。

始める前に

この機能は、ISA 3000 を除き、ルーテッドファイアウォールモードでのみ使用できます（ISA 3000 では、このコマンドはトランスペアレントモードでのみサポートされます）。さらに、こ

の機能はシングルコンテキストモードでのみ使用できます。コンフィギュレーションがクリアされたASAには、この機能を使用して自動的に設定する定義済みコンテキストがありません。

手順

ステップ 1 工場出荷時のデフォルト コンフィギュレーションを復元します。

configure factory-default [*ip_address* [*mask*]]

例：

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

ip_address を指定する場合は、デフォルトのIPアドレスを使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスのIPアドレスを設定します。*ip_address* オプションで設定されているインターフェイスについては、次のモデルのガイドラインを参照してください。

- Firepower 1010：**管理**インターフェイスの IP アドレスを設定します。
- Firepower 1100：**内部**インターフェイスの IP アドレスを設定します。
- Secure Firewall 1210/1220：**管理**インターフェイスの IP アドレスを設定します。
- Secure Firewall 1230/1240/1250：**内部**インターフェイスの IP アドレスを設定します。
- Secure Firewall 3100：**内部**インターフェイスの IP アドレスを設定します。
- Secure Firewall 4200：**内部**インターフェイスの IP アドレスを設定します。
- Firepower 4100/9300：効果はありません。
- ASA 仮想：**管理**インターフェイスの IP アドレスを設定します。
- ISA 3000：**管理**インターフェイスの IP アドレスを設定します。

http コマンドでは、ユーザーが指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定した IP アドレスよりも大きい使用可能なすべてのアドレスで構成されます。たとえば、サブネットマスク 255.255.255.0 で 10.5.6.78 を指定した場合、DHCP アドレスの範囲は 10.5.6.79 ～ 10.5.6.254 になります。

Firepower 1000、および Secure Firewall 1200, 3100, 4200の場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

その他すべてのモデルの場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。**boot system** コマンドを使用すると、特定のイメージから起動できます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュ メモリの最初のイメージからブートします。内部フラッシュ メモリにイメージがない場合、ASA はブートしません。

例：

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
WARNING: The new maximum-session limit will take effect after the running-config is saved
 and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

ステップ 2 デフォルト コンフィギュレーションをフラッシュ メモリに保存します。

write memory

このコマンドでは、事前に **boot** config コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップ コンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションがクリアされると、このパスもクリアされます。

ASA 仮想 導入設定の復元

この項では、ASA 仮想 の導入（0 日）設定を復元する方法について説明します。

手順

ステップ 1 フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイ ユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブ ユニットをリロードし、フェールオーバー リンクを

介して再接続すると、古い設定は新しいアクティブユニットから同期し、必要な導入コンフィギュレーションが消去されます。

ステップ 2 リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

write erase

（注）
ASA 仮想 が現在の実行イメージをブートするため、元のブート イメージには戻りません。元のブート イメージを使用するには、**boot image** コマンドを参照してください。

コンフィギュレーションは保存しないでください。

ステップ 3 ASA 仮想 をリロードし、導入設定をロードします。

reload

ステップ 4 フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

Firepower 1010 のデフォルト設定

Firepower 1010 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェア スイッチ**：イーサネット 1/2 ～ 1/8 は VLAN 1 に属しています。
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
```

```
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
```

```
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 1100 のデフォルト設定

Firepower 1100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
```

```
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 1210/1220 のデフォルト設定

Cisco Secure Firewall 1210/1220 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェアスイッチ**：Ethernet 1/2 ～ 1/8 または 1/2 ～ 1/10（1220）は VLAN 1 に属しています。
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
```

```
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
! 1220
interface Ethernet1/9
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
! 1220
interface Ethernet1/10
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
```

```
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Secure Firewall 1230/1240/1250 のデフォルト設定

Cisco Secure Firewall 1230/1240/1250 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス、内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
```

```
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 3100 デフォルト設定

Cisco Secure Firewall 3100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
```

```
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 4200 のデフォルト設定

Cisco Secure Firewall 4200 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
```

```
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Firepower 4100/9300 シャーシ デフォルト設定

Firepower 4100/9300 シャーシ 上に ASA を展開した場合、ASDM を使用して管理インターフェイスへの接続が可能になる多くのパラメータを事前設定できます。一般的な構成には次の設定があります。

- 管理インターフェイス：
  - Firepower 4100/9300 シャーシ スーパバイザ上で定義された任意の管理タイプ インターフェイス
  - 名前は「management」
  - 任意の IP アドレス
  - セキュリティ レベル 0
  - 管理専用
- 管理インターフェイス内のデファルト ルート
- ASDM アクセス：すべてのホストが許可されます。

スタンドアロン ユニットの設定は、次のコマンドで構成されます。クラスタ ユニットの追加の設定については、ASA クラスタの作成 （543 ページ） を参照してください。

```
interface <management_ifc>
  management-only
  ip address <ip_address> <mask>
  ipv6 address <ipv6_address>
  ipv6 enable
  nameif management
  security-level 0
  no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
```

```
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- **トランスペアレントファイアウォールモード**：トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。
- **1 ブリッジ仮想インターフェイス**：すべてのメンバーインターフェイスは同じネットワーク内に存在しています（**IP アドレスは事前設定されていません。ネットワークと一致するように設定する必要があります**）：GigabitEthernet 1/1 （outside1）、GigabitEthernet 1/2（inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての**内部および外部**インターフェイスは相互通信できます。
- **管理 1/1** インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する **DHCP**。
- **ASDM** アクセス：管理ホストに許可されます。
- **ハードウェアバイパス**は、次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4

（注） ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのは上記のインターフェイスペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASA がフローを引き継ぐため、接続が短時間中断されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
```

```
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management
```

ASA 仮想 による展開の設定

ASA 仮想 を導入すると、ASDM を使用して、Management 0/0 インターフェイスへの接続を可能にする多数のパラメータをプリセットできます。一般的な構成には次の設定があります。

- ルーテッド ファイアウォール モードまたはトランスペアレント ファイアウォール モード
- Management 0/0 インターフェイス：
  - 名前は「management」
  - IP アドレスまたは DHCP
  - セキュリティ レベル 0
- 管理ホスト IP アドレスのスタティック ルート（管理サブネット上にない場合）
- HTTP サーバーの有効または無効
- 管理ホスト IP アドレス用の HTTP アクセス

- （オプション）GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、Management0/0 のスタンバイ IP アドレス
- DNS サーバー
- スマート ライセンス ID トークン
- スマートライセンスのスループットレベルおよびEssentials機能階層
- スマートトランスポート URL（https://smartreceiver.cisco.com/licservice/license）およびポート 80。
- （オプション）Smart スマート トランスポート プロキシ URL およびポート
- （オプション）SSH 管理設定：
  - クライアント IP アドレス
  - ローカル ユーザー名とパスワード
  - ローカル データベースを使用する SSH に必要な認証
- （オプション）REST API の有効または無効

（注） Cisco Licensing Authority に ASA 仮想 を正常に登録するには、ASA 仮想 にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

スタンドアロン ユニットについては、次の設定例を参照してください。

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http managemment_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
```

（注） Essentials ライセンスは、以前は「標準」ライセンスと呼ばれていました。

フェールオーバー ペアのプライマリ ユニットについては、次の設定例を参照してください。

```
nameif management
  security-level 0
  ip address ip_address standby standby_ip

  no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http managemment_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip
```

コンフィギュレーション作業

この項では、コンフィギュレーションを処理する方法について説明します。この項で説明する内容は、特に指定がない限り、シングル モードとマルチ モードの両セキュリティ コンテキストに適用されます。

スタートアップコンフィギュレーションおよび実行コンフィギュレーションについて

スタートアップ コンフィギュレーション

ASAは、起動時に、「スタートアップ コンフィギュレーション」と呼ばれるコンフィギュレーションをテキストファイルからロードします。このファイルは、デフォルトでは隠しファイルとして内部フラッシュ メモリに常駐しています。ただし、表示されるファイルシステムに存在するスタートアップ コンフィギュレーションに別のファイルを指定することができます。新しいスタートアップ コンフィギュレーションを指定するには、次のコマンドを使用します。

boot config {**disk0:/** | **disk1:/**} [*path/*]*filename*

新しい場所を保存します。

write memory

次に例を示します。

```
ciscoasa (config)# boot config disk0:/startup.cfg
ciscoasa (config)# write memory
```

大規模な設定の使用

隠しスタートアップディレクトリの容量は限られています。設定が非常に大きい場合（たとえば、16 MB を超える場合）、スタートアップ コンフィギュレーションを保存できません。この場合は、**boot config** コマンドを使用して、表示されるファイルシステムにスタートアップ コンフィギュレーションを保存する必要があります。たとえば、大規模な設定を実行メモリにロードして保存するために **write memory** コマンドを入力した場合、設定が大きすぎると、次のエラーメッセージが表示されることがあります。

```
%Error writing. nvram:/startup-config (No space left on device:)
```

この場合は、ASA をリロードする前に、必ず、実行コンフィギュレーションを新しいファイルの場所に再保存してください。そうしないと、ASA が完全な設定をロードしない可能性があります。

実行コンフィギュレーション

コマンドを入力すると、メモリ上の実行コンフィギュレーションに対してだけ変更が適用されます。変更内容をリロード後も維持するには、実行コンフィギュレーションを手動でスタートアップ コンフィギュレーションに保存する必要があります。

コンフィギュレーションの変更の保存

この項では、コンフィギュレーションを保存する方法について説明します。

シングル コンテキスト モードでのコンフィギュレーションの変更の保存

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存するには、次の手順を実行します。

手順

実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

（注）

copy running-config startup-config コマンドは、**write memory** コマンドに相当します。

マルチ コンテキスト モードでのコンフィギュレーションの変更の保存

各コンテキスト（およびシステム）コンフィギュレーションを個別に保存することも、すべてのコンテキスト コンフィギュレーションを同時に保存することもできます。

各コンテキストとシステムの個別保存

システムまたはコンテキストのコンフィギュレーションを保存するには、次の手順を使用します。

手順

コンテキストまたはシステム内から、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

マルチ コンテキスト モードでは、コンテキストのスタートアップ コンフィギュレーションを外部サーバーに置くことができます。この場合、ASA は、コンテキスト URL で指定したサーバにコンフィギュレーションを戻して保存します。ただし HTTP URL および HTTPS URL の場合は例外で、サーバにコンフィギュレーションを保存できません。

（注）
copy running-config startup-config コマンドは、**write memory** コマンドに相当します。

すべてのコンテキスト コンフィギュレーションの同時保存

すべてのコンテキスト コンフィギュレーションとシステム コンフィギュレーションを同時に保存するには、次の手順を使用します。

手順

システム実行スペースから、すべてのコンテキストとシステム コンフィギュレーションの実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory all [**/noconfirm**]

/noconfirm キーワードを入力しない場合、次のプロンプトが表示されます。

```
Are you sure [Y/N]:
```

Y を入力すると、ASA によってシステム コンフィギュレーションと各コンテキストが保存されます。コンテキストのスタートアップ コンフィギュレーションは、外部サーバーに配置できます。この場合、ASA は、コンテキスト URL で指定したサーバーにコンフィギュレーションを戻して保存します。ただし HTTP URL および HTTPS URL の場合は例外で、サーバーにコンフィギュレーションを保存できません。

ASA によって各コンテキストが保存された後、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーのためにコンテキストが保存されない場合もあります。エラーについては、次の情報を参照してください。

- メモリ不足のためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unavailability of resources
  ```

- リモートの宛先に到達できないためにコンテキストが保存されない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to non-reachability of destination
  ```

- コンテキストがロックされているために保存されない場合は、次のメッセージが表示されます。

  ```
  Unable to save the configuration for the following contexts as these contexts are
  locked.
  context 'a' , context 'x' , context 'z' .
  ```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存している場合、またはコンテキストを削除している場合のみです。

- スタートアップ コンフィギュレーションが読み取り専用であるために（たとえば、HTTP サーバで）コンテキストが保存されない場合は、他のすべてのメッセージの最後に次のメッセージ レポートが出力されます。

  ```
  Unable to save the configuration for the following contexts as these contexts have
  read-only config-urls:
  context 'a' , context 'b' , context 'c' .
  ```

- フラッシュ メモリのセクターが壊れているためコンテキストを保存できない場合は、次のメッセージが表示されます。

  ```
  The context 'context a' could not be saved due to Unknown errors
  ```

スタートアップコンフィギュレーションの実行コンフィギュレーションへのコピー

新しいスタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーするには、次のいずれかのコマンドを使用します。

- **copy startup-config running-config**

  スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

- **reload**

  ASA をリロードします。その結果、スタートアップ コンフィギュレーションがロードされ、実行コンフィギュレーションが破棄されます。

- **clear configure all**、続いて then**copy startup-config running-config**

  スタートアップ コンフィギュレーションをロードし、実行コンフィギュレーションを破棄します。リロードは不要です。

設定の表示

実行コンフィギュレーションとスタートアップ コンフィギュレーションを表示するには、次のコマンドを使用します。

- **show running-config**

  実行コンフィギュレーションを表示します。

- **show running-config** *command*

  特定のコマンドの実行コンフィギュレーションを表示します。

- **show startup-config**

  スタートアップ コンフィギュレーションを表示します。

コンフィギュレーション設定のクリアおよび削除

設定を消去するには、次のいずれかのコマンドを入力します。

- **clear configure** *configurationcommand* [*level2configurationcommand*]

  指定されたコマンドのすべてのコンフィギュレーションをクリアします。コマンドの特定バージョンのコンフィギュレーションだけをクリアする場合は、*level2configurationcommand* に値を入力します。

たとえば、すべての **aaa** コマンドのコンフィギュレーションをクリアするには、次のコマンドを入力します。

```
ciscoasa(config)# clear configure aaa
```

aaa authentication コマンドのコンフィギュレーションだけをクリアするには、次のコマンドを入力します。

```
ciscoasa(config)# clear configure aaa authentication
```

- **no** *configurationcommand* [*level2configurationcommand*] *qualifier*

  コマンドの特定のパラメータまたはオプションをディセーブルにします。この場合、**no** コマンドを使用して、*qualifier* で識別される特定のコンフィギュレーションを削除します。

  たとえば、特定の **access-list** コマンドを削除するには、それを一意に特定するのに十分なコマンドを入力します。コマンド全体を入力しなければならない場合もあります。

```
ciscoasa(config)# no access-list abc extended permit icmp any any object-group
obj_icmp_1
```

- **write erase**

  スタートアップ コンフィギュレーションを消去します。

（注） ASA 仮想 の場合、このコマンドはリロード後に導入設定を復元します。コンフィギュレーションを完全に消去するには、**clear configure all** コマンドを使用します。

- **clear configure all**

  実行コンフィギュレーションを消去します。

（注） マルチ コンテキスト モードでは、システム コンフィギュレーションから **clear configure all** を入力すると、すべてのコンテキストを削除し、実行中のコンフィギュレーションを停止することにもなります。コンテキスト コンフィギュレーション ファイルは消去されず、元の場所に保持されます。

（注） Firepower 1000、および Secure Firewall 1200, 3100, 4200の場合：このコマンドは、残りの設定とともに **boot system** コマンドをクリアします（存在する場合）。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

その他すべてのモデルの場合：このコマンドは、残りの設定とともに**boot system** コマンドをクリアします（存在する場合）。**boot** system コマンドは、外部フラッシュ メモリ カードのイメージを含む、特定のイメージからの起動を可能にします。ASA を次回リロードすると、内部フラッシュ メモリの最初のイメージから起動します。内部フラッシュ メモリにイメージがない場合、ASA は起動しません。

オフラインでテキスト コンフィギュレーション ファイルの作成

このガイドは、CLI を使用した ASA の設定方法について説明します。コマンドを保存すると、変更がテキスト ファイルに書き込まれます。一方、CLI を使用する代わりに、テキスト ファイルをコンピュータで直接編集して、コンフィギュレーション モードのコマンドライン プロンプトから、コンフィギュレーションを全部または1行ずつペーストすることができます。別の方法として、ASA 内部フラッシュ メモリにテキスト ファイルをダウンロードします。ASA への設定ファイルのダウンロードについては、ソフトウェアおよびコンフィギュレーション（1553 ページ） を参照してください。

ほとんどの場合、このマニュアルで説明するコマンドには、CLI プロンプトが先行します。次の例でのプロンプトは「ciscoasa(config)#」です。

```
ciscoasa(config)# context a
```

コマンドの入力が要求されないテキスト コンフィギュレーション ファイルの場合は、プロンプトは次のように省略されます。

```
context a
```

ファイルのフォーマットの詳細については、コマンドライン インターフェイスの使用 （1773 ページ）を参照してください。

接続の設定変更の適用

コンフィギュレーションに対してセキュリティ ポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティ ポリシーが使用されます。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。古い接続に対する **show** コマンドの

出力は古いコンフィギュレーションを反映しており、場合によっては古い接続に関するデータが含まれないことがあります。

たとえば、インターフェイスから QoS **service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている QoS カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のコマンドを入力します。

- **clear conn**[**all**] [**protocol** {**tcp** |**udp**}] [**address** *src_ip* [*-src_ip*] [**netmask** *mask*] [**port** *src_port* [*-src_port*] [**address** *dest_ip* [*-dest_ip*] [**netmask** *mask*] [**port** *dest_port* [*-dest_port*]

  このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

  引数を指定しないと、このコマンドはすべての through-the-box 接続をクリアします。to-the-box 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。

ASA のリロード

ASA をリロードするには、次の手順を実行します。

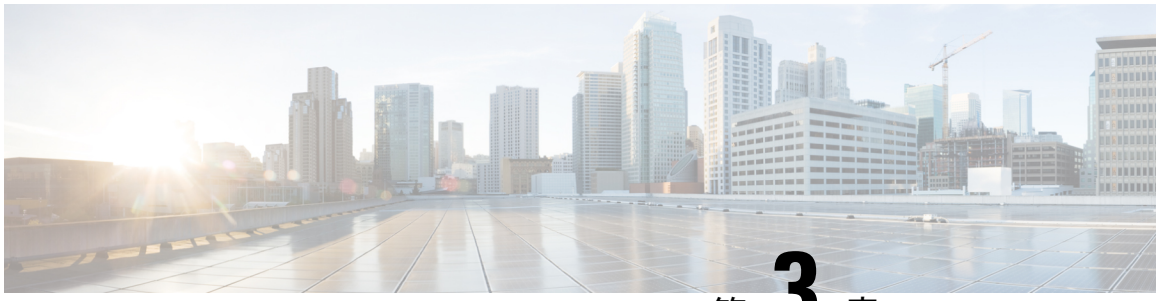
reload コマンドは、クラスタリング用のデータノードやフェールオーバー用のスタンバイ/セカンダリユニットには複製されません。

マルチ コンテキスト モードでは、システム実行スペース以外からはリロードできません。

手順

ASA をリロードします。

reload



第 3 章

ライセンス：ISA 3000 の製品認証キーライセンス

ライセンスでは、特定の ASA 上でイネーブルにするオプションを指定します。このマニュアルでは、ISA 3000 の製品認証キー（PAK）のライセンスについて説明します。その他のモデルについては、ライセンス：スマート ソフトウェア ライセンシング （93 ページ）を参照してください。

- PAK ライセンスについて （47 ページ）
- PAK ライセンスのガイドライン （57 ページ）
- PAK ライセンスの設定 （59 ページ）
- 共有ライセンスの設定（セキュアクライアント 3 以前） （64 ページ）
- モデルごとにサポートされている機能のライセンス （72 ページ）
- PAK ライセンスのモニタリング （74 ページ）
- PAK ライセンスの履歴 （84 ページ）

PAK ライセンスについて

ライセンスでは、特定の ASA 上でイネーブルにするオプションを指定します。ライセンスは、160 ビット（32 ビットのワードが 5 個、または 20 バイト）値であるアクティベーション キーで表されます。この値は、シリアル番号（11 文字の文字列）とイネーブルになる機能とを符号化します。

事前インストール済みライセンス

デフォルトでは、ASA は、ライセンスがすでにインストールされた状態で出荷されます。このライセンスは、注文した内容およびベンダーがインストールした内容に応じて、ライセンスを追加できる基本ライセンスの場合と、すべてのライセンスがすでにインストールされている場合があります。

関連トピック

PAK ライセンスのモニタリング （74 ページ）

永続ライセンス

永続アクティベーション キーを 1 つインストールできます。永続アクティベーション キーは、1 つのキーにすべてのライセンス機能を格納しています。時間ベース ライセンスもインストールすると、ASA は永続ライセンスと時間ベース ライセンスを 1 つの実行ライセンスに結合します。

関連トピック

永続ライセンスと時間ベース ライセンスの結合 （48 ページ）

時間ベース ライセンス

永続ライセンスに加えて、時間ライセンスを購入したり、時間制限のある評価ライセンスを入手したりできます。たとえば、SSL VPN の同時ユーザの短期増加に対処するために時間ベースの セキュアクライアント Premium ライセンスを購入したり、

時間ベース ライセンス有効化ガイドライン

- 複数の時間ベース ライセンスをインストールし、同じ機能に複数のライセンスを組み込むことができます。ただし、一度にアクティブ化できる時間ベース ライセンスは、1 機能につき 1 つだけです。非アクティブのライセンスはインストールされたままで、使用可能な状態です。たとえば、1000 セッション セキュアクライアント Premium ライセンスと 2500 セッション セキュアクライアント Premium ライセンスをインストールした場合、これらのライセンスのうちいずれか 1 つだけをアクティブにできます。
- キーの中に複数の機能を持つ評価ライセンスをアクティブにした場合、そこに含まれている機能のいずれかに対応する時間ベース ライセンスを同時にアクティブ化することはできません。

時間ベース ライセンス タイマーの動作

- 時間ベース ライセンスのタイマーは、ASA 上でライセンスをアクティブにした時点でカウント ダウンを開始します。
- タイムアウト前に時間ベース ライセンスの使用を中止すると、タイマーが停止します。時間ベース ライセンスを再度アクティブ化すると、タイマーが再開します。
- 時間ベース ライセンスがアクティブになっているときに ASA をシャットダウンすると、タイマーはカウント ダウンを停止します。時間ベース ライセンスでは、ASA が動作している場合にのみカウント ダウンします。システム クロック設定はライセンスに影響しません。つまり、ASA 稼働時間ではライセンス継続期間に対してのみカウントします。

永続ライセンスと時間ベース ライセンスの結合

時間ベース ライセンスをアクティブにすると、永続ライセンスと時間ベース ライセンスに含まれる機能を組み合わせた実行ライセンスが作成されます。永続ライセンスと時間ベース ライ

センスの組み合わせ方は、ライセンスのタイプに依存します。次の表に、各機能ライセンスの組み合わせルールを示します。

（注） 永続ライセンスが使用されていても、時間ベース ライセンスがアクティブな場合はカウントダウンが続行されます。

表 *1*：時間ベース ライセンスの組み合わせルール

時間ベース機能	結合されたライセンスのルール
セキュアクライアント Premium セッション	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。たとえば、永続ライセンスが 1000 セッション、時間ベース ライセンスが 2500 セッションの場合、2500 セッションがイネーブルになります。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。
Unified Communications Proxy セッション	時間ベース ライセンスのセッションは、プラットフォームの制限数まで永続セッションに追加されます。たとえば、永続ライセンスが 2500 セッション、時間ベース ライセンスが 1000 セッションの場合、時間ベース ライセンスがアクティブである限り、3500 セッションがイネーブルになります。
その他	時間ベース ライセンスまたは永続ライセンスのうち、値の高い方が使用されます。ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。数値ティアを持つライセンスの場合、高い方の値が使用されます。通常は、永続ライセンスよりも機能の低い時間ベース ライセンスをインストールすることはありませんが、そのようなインストールが行われた場合は永続ライセンスが使用されます。

関連トピック

PAK ライセンスのモニタリング （74 ページ）

時間ベース ライセンスのスタッキング

多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。

すでにインストールされているのと同じ時間ベースライセンスをインストールすると、それらのライセンスは結合され、有効期間は両者を合わせた期間になります。

次に例を示します。

1. 8 週 1000 セッションの セキュアクライアント Premium ライセンスをインストールし、これを 2 週間使用します（残り 6 週）。
2. 次に、別の 8 週 1000 セッションのライセンスをインストールすると、これらのライセンスは結合され、14 週（8 + 6 週）1000 セッションのライセンスになります。

これらのライセンスが同一でない場合（たとえば、1000 セッション セキュアクライアント Premium ライセンスと 2500 セッションライセンス）、これらのライセンスは結合されません。1 つの機能につき時間ベース ライセンスを 1 つだけアクティブにできるので、ライセンスのうちいずれか 1 つだけをアクティブにすることができます。

同一でないライセンスは結合されませんが、現在のライセンスの有効期限が切れた場合、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。

関連トピック

キーのアクティブ化または非アクティブ化 （63 ページ）
時間ベース ライセンスの有効期限 （50 ページ）

時間ベース ライセンスの有効期限

機能に対応する現在のライセンスが期限切れになると、同じ機能のインストール済みライセンスが使用可能であれば、ASA はそのライセンスを自動的にアクティブにします。その機能に使用できる時間ベース ライセンスが他にない場合は、永続ライセンスが使用されます。

その機能に対して複数の時間ベース ライセンスを追加でインストールした場合、ASA は最初に検出されたライセンスを使用します。どのライセンスを使用するかは、ユーザーが設定することはできず、内部動作に依存します。ASA がアクティブ化したライセンスとは別の時間ベース ライセンスを使用するには、目的のライセンスを手動でアクティブにする必要があります。

たとえば、2500 セッションの時間ベース セキュアクライアント Premium ライセンス（アクティブ）、1000 セッションの時間ベース セキュアクライアント Premium ライセンス（非アクティブ）、500 セッションの永続 セキュアクライアント Premium ライセンスを所有しているとします。2500 セッション ライセンスの有効期限が切れた場合、ASA は 1000 セッション ライセンスを有効化します。1000 セッション ライセンスの有効期限が切れた後、ASA は 500 セッション永久ライセンスを使用します。

関連トピック

キーのアクティブ化または非アクティブ化 （63 ページ）

ライセンスに関する注意事項

次の項で、ライセンスに関する追加情報について説明します。

Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス

Secure Client Advantageまたは Premier ライセンスは、ライセンスが指定するユーザープールを共有するすべての複数の ASA に適用できる同時使用ライセンスです。Secure Client VPN のみライセンスは、特定の ASA に適用されます。https://www.cisco.com/go/license を参照し、各 ASA に個別に PAK を割り当てます。ASA に取得したアクティベーション キーを適用すると、VPN 機能が最大許容数に切り替わりますが、ライセンスを共有するすべての ASA 上の実際の一意のユーザー数はライセンス限度を超えることはできません。詳細については、以下を参照してください。

- Cisco セキュアクライアント 発注ガイド
- セキュアクライアント ライセンスに関するよくある質問（FAQ）

（注） マルチコンテキストモードでサポートされている唯一の Secure Client Premier ライセンスは Secure Client Premier ライセンスです。さらに、マルチ コンテキスト モードでは、フェールオーバーペアの各ユニットにこのライセンスを適用する必要があります。ライセンスは集約されません。

その他の VPN ライセンス

その他の VPN ピアには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN セッション、全タイプ

- 合計 VPN ピアは、セキュアクライアント とその他の VPN ピアを合算した、許可される VPN ピアの最大数となります。たとえば、合計が 1000 の場合はセキュアクライアント とその他の VPN ピアを 500 ずつ、または セキュアクライアント を 700 とその他の VPN ピア 300 を同時に許可できます。あるいは、1000 すべてを セキュアクライアント に使用することも可能です。合計 VPN ピアが最大数を超えた場合は、ASA をオーバーロードして、適切なネットワークのサイズに設定してください。

VPN ロード バランシング

VPN ロード バランシングには、強力な暗号化（3DES/AES）ライセンスが必要です。

レガシー VPN ライセンス

ライセンスに関するすべての関連情報については、『Supplemental end User License Agreement for セキュアクライアント』を参照してください。

（注） Secure Client Premier ライセンスは、マルチコンテキストモードでサポートされる唯一のセキュアクライアントライセンスであり、デフォルトライセンスやレガシーライセンスは使用できません。

暗号化ライセンス

高度暗号化を有効にしている場合、DES を使用することはできません。

合計 TLS プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザー数が 250 未満のライセンス）では、TLS プロキシセッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザー数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 次に例を示します。

```
interface gigabitethernet 0/0.100
vlan 100
```

セキュアクライアント Premium 共有ライセンス（AnyConnect 3 以前）

（注） ASA の共有ライセンス機能は、AnyConnect 4 以降のライセンスではサポートされていません。セキュアクライアントライセンスは共有されるため、共有サーバーまたは参加者ライセンスは必要ありません。

共有ライセンスを使用すると、多数の セキュアクライアント Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いずれかの ASA を共有ライセンス サーバーとして、残りを共有ライセンス参加システムとして設定します。

フェールオーバー

いくつかの例外を除き、フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。以前のバージョンについては、お使いのバージョンに該当するライセンシングマニュアルを参照してください。

フェールオーバー ライセンスの要件および例外

モデル	ライセンス要件
ISA 3000	両方のユニットの Security Plus ライセンス。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、ISA 3000 で、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

フェールオーバーライセンスの結合方法

フェールオーバーペアでは、各ユニットのライセンスが結合されて 1 つの実行クラスタライセンスとなります。ユニットごとに別のライセンスを購入した場合は、結合されたライセンスには次のルールが使用されます。

- 数値ティアを持つライセンスの場合は（セッション数など）、各ユニットのライセンスの値が合計されます。ただし、プラットフォームの制限を上限とします。使用されているライセンスがすべて時間ベースの場合は、ライセンスのカウント ダウンは同時に行われます。

  たとえば、フェールオーバーの場合は次のようになります。

  - 2 つの ASA があり、それぞれに 10 個の TLS プロキシ セッションが設定されている場合、ライセンスは結合され、合計で 20 個の TLS プロキシ セッションになります。
  - 1 つの ASA には 1000 の TLS プロキシセッションがあり、もう 1 つには 2000 のセッションがあるとします。プラットフォームの限度は 2000 であるため、結合されたライセンスは 2000 の TLS プロキシセッションに対応できます。

- ライセンスのステータスがイネーブルまたはディセーブルの場合、イネーブル ステータスのライセンスが使用されます。
- イネーブルまたはディセーブル状態（かつ数値ティアを持たない）の時間ベース ライセンスの場合、有効期間はすべてのライセンスの期間の合計となります。最初にプライマリ/制御ユニットのライセンスがカウントダウンされ、期限切れになると、セカンダリ/データユニットのライセンスのカウントダウンが開始し、以下も同様です。

関連トピック

PAK ライセンスのモニタリング （74 ページ）

フェールオーバーユニット間の通信の途絶

ユニットの通信が途絶えてからの期間が 30 日を超えた場合は、各ユニットにはローカルにインストールされたライセンスが適用されます。30 日の猶予期間中は、結合された実行ライセンスが引き続きすべてのユニットで使用されます。

30 日間の猶予期間中に通信が復旧した場合は、時間ベースライセンスについては、経過した時間がプライマリ/制御ライセンスから差し引かれます。プライマリ/制御ライセンスが期限切れになるまでは、セカンダリ/データライセンスのカウントダウンが開始することはありません。

30 日間の期間が終了しても通信が復旧しなかった場合は、時間ベース ライセンスについては、その時間がすべてのユニットのライセンスから差し引かれます（インストールされている場合）。これらはそれぞれ別のライセンスとして扱われ、ライセンスの結合によるメリットはありません。経過時間には 30 日の猶予期間も含まれます。

フェールオーバー ペアのアップグレード

フェールオーバーペアでは、両方の装置に同一のライセンスがインストールされている必要はないので、ダウンタイムなしに各装置に新しいライセンスを適用できます。リロードが必要な永続ライセンスを適用する場合、リロード中に他の装置へのフェールオーバーを実行できます。両方の装置でリロードが必要な場合は、各装置を個別にリロードするとダウンタイムは発生しません。

関連トピック

キーのアクティブ化または非アクティブ化 （63 ページ）

ペイロード暗号化機能のないモデル

ペイロード暗号化機能のないモデルを購入することができます。輸出先の国によっては、ASA シリーズでペイロード暗号化をイネーブルにできません。ASA ソフトウェアは、ペイロード暗号化なしモデルを検出し、次の機能をディセーブルにします。

- ユニファイド コミュニケーション
- VPN

このモデルでも管理接続用に高度暗号化（3DES/AES）ライセンスをインストールできます。たとえば、ASDM HTTPS/SSL、SSHv2、Telnet、および SNMPv3 を使用できます。

ライセンスを表示すると、VPN およびユニファイド コミュニケーションのライセンスはリストに示されません。

関連トピック

PAK ライセンスのモニタリング （74 ページ）

ライセンスの FAQ

セキュアクライアント Premium とボットネット トラフィック フィルタなど、。

はい。一度に使用できる時間ベースライセンスは、1 機能につき 1 つです。

複数の時間ベースライセンスを「スタック」し、時間制限が切れると自動的に次のライセンスが使用されるようにできますか。

はい。ライセンスが同一の場合は、複数の時間ベースライセンスをインストールすると、時間制限が結合されます。ライセンスが同一でない場合（1000 セッション セキュアクライアント Premium ライセンスと 2500 セッションライセンスなど）、ASA はその機能に対して検出された次の時間ベースライセンスを自動的にアクティブにします。

アクティブな時間ベースライセンスを維持しながら、新しい永続ライセンスをインストールできますか。

はい。永続ライセンスをアクティブ化しても、時間ベースライセンスには影響しません。

フェールオーバーのプライマリ装置として共有ライセンスサーバを、セカンダリ装置として共有ライセンス バックアップ サーバを使用できますか。

いいえ。セカンダリ装置は、プライマリ装置と同じ実行ライセンスを使用します。共有ライセンスサーバには、サーバライセンスが必要です。バックアップサーバには、参加ライセンスが必要です。バックアップサーバは、2 つのバックアップサーバの別々のフェールオーバーペアに配置できます。

フェールオーバーペアのセカンダリ装置用に、同じライセンスを購入する必要がありますか。

いいえ。バージョン 8.3(1) から、両方の装置に同一のライセンスをインストールする必要はなくなりました。一般的に、ライセンスはプライマリ装置で使用するために購入されます。セカンダリ装置は、アクティブになるとプライマリライセンスを継承します。セカンダリ装置に別のライセンスを持っている場合は（たとえば、8.3 よりも前のソフトウェアに一致するライセンスを購入した場合）、ライセンスは実行フェールオーバー クラスタ ライセンスに結合されます。ただし、モデルの制限が最大数になります。

AnyConnect Premium（共有）ライセンスに加えて、時間ベースまたは永続の セキュアクライアント Premium ライセンスを使用できますか。

はい。ローカルにインストールされたライセンス（時間ベースライセンスまたは永続ライセンス）のセッション数を使い果たした後、共有ライセンスが使用されます。

（注） 共有ライセンスサーバーでは、永続セキュアクライアントライセンスは使用されません。ただし、共有ライセンスサーバーライセンスと同時に時間ベースライセンスを使用することはできます。この場合、時間ベースライセンスのセッションは、ローカルのセキュアクライアント Premium セッションにだけ使用できます。共有ライセンスプールに追加して参加システムで使用することはできません。

PAK ライセンスのガイドライン

コンテキスト モードのガイドライン

マルチ コンテキスト モードでシステム実行スペース内にアクティベーション キーを適用します。

フェールオーバーのガイドライン

フェールオーバー （54 ページ）を参照してください。

モデルのガイドライン

- スマートライセンシングは、ASA 仮想 でのみサポートされます。
- 共有ライセンスは、ASA 仮想、ASA 5506-X、ASA 5508-X、および ASA 5516-X ではサポートされません。
- ASA 5506-X および ASA 5506W-X は、時間ベース ライセンスをサポートしません。

アップグレードとダウングレードのガイドライン

任意の旧バージョンから最新バージョンにアップグレードした場合、アクティベーション キーの互換性は存続します。ただし、ダウングレード機能の維持には問題が生じる場合があります。

- バージョン 8.1 以前にダウングレードする場合：アップグレード後に、*8.2* よりも前に導入された機能のライセンスを追加でアクティブ化すると、ダウングレードした場合でも旧バージョンに対するアクティベーション キーの互換性は存続します。ただし、*8.2* 以降で導入された機能ライセンスをアクティブ化した場合は、アクティベーション キーの下位互換性がなくなります。互換性のないライセンス キーがある場合は、次のガイドラインを参照してください。
  - 以前のバージョンでアクティベーション キーを入力した場合は、ASA はそのキーを使用します（バージョン 8.2 以降でアクティブ化した新しいライセンスがない場合）。
  - 新しいシステムで、以前のアクティベーション キーがない場合は、旧バージョンと互換性のある新しいアクティベーション キーを要求する必要があります。

- バージョン 8.2 以前にダウングレードする場合：バージョン 8.3 では、よりロバストな時間ベース キーの使用およびフェールオーバー ライセンスの変更が次のとおり導入されました。
  - 複数の時間ベースのアクティベーション キーがアクティブな場合、ダウングレード時には一番最近アクティブ化された時間ベース キーのみがアクティブになれます。他のキーはすべて非アクティブ化されます。最後の時間ベース ライセンスが 8.3 で導入された機能に対応している場合、そのライセンスは旧バージョンでの使用はできなくても、アクティブ ライセンスのままです。永続キーまたは有効な時間ベース キーを再入力してください。
  - フェールオーバーペアに不一致のライセンスがある場合、ダウングレードによりフェールオーバーはディセーブルになります。キーが一致した場合でも、使用するライセンスは、結合されたライセンスではなくなります。
  - 1 つの時間ベース ライセンスをインストールしているが、それが 8.3 で導入された機能に対応している場合、ダウングレードの実行後、その時間ベース ライセンスはアクティブなままです。この時間ベース ライセンスをディセーブルにするには、永続キーを再入力する必要があります。

その他のガイドライン

- アクティベーション キーは、コンフィギュレーション ファイルには保存されません。隠しファイルとしてフラッシュ メモリに保存されます。
- アクティベーション キーは、デバイスのシリアル番号に関連付けられます。機能ライセンスは、デバイス間で転送できません（ハードウェア障害の発生時を除く）。ハードウェア障害が発生したためにデバイスを交換する必要があり、このことが Cisco TAC によってカバーされている場合は、シスコのライセンス チームに連絡して、既存のライセンスを新しいシリアル番号に転送するよう依頼してください。シスコのライセンス チームから、製品認証キーの参照番号と既存のシリアル番号を求められます。
- ライセンシングで使うシリアル番号は、 **show version** 出力。このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。
- 購入後に、返金またはアップグレードしたライセンスのためにライセンスを返却できません。
- 1 つのユニット上で、同じ機能の 2 つの別個のライセンスを加算することはできません。たとえば、25 セッション SSL VPN ライセンスを購入した後で 50 セッション ライセンスを購入しても、75 個のセッションを使用できるわけではなく、使用できるのは最大 50 個のセッションです。（アップグレード時に、数を増やしたライセンスを購入できることがあります。たとえば 25 セッションから 75 セッションへの増加です。このタイプのアップグレードは、2 つのライセンスの加算とは別のものです）。
- すべてのライセンス タイプをアクティブ化できますが、機能によっては、機能どうしの組み合わせができないものがあります。AnyConnect Essentials ライセンスの場合、次のライ

センスとは互換性がありません。AnyConnect Premium ライセンス、AnyConnect Premium（共有）ライセンス、および Advanced Endpoint Assessment ライセンス。デフォルトでは、AnyConnect Essentials ライセンスをインストールした場合（使用中のモデルで利用できる場合）、このライセンスが前述のライセンスの代わりに使用されます。 **webvpn**、次に **no anyconnect-essentials** コマンドを使用して、設定で AnyConnect Essentials ライセンスを無効にし、他のライセンスを使用できます。

PAK ライセンスの設定

この項では、アクティベーション キーを取得する方法とそれをアクティブ化する方法について説明します。また、キーを非アクティブ化することもできます。

ライセンスの PAK の注文とアクティベーション キーの取得

ASA にライセンスをインストールするには製品認証キーが必要です。その後、それを Cisco.com に登録してアクティベーション キーを取得することができます。次に、ASA のアクティベーション キーを入力できます。機能ライセンスごとに個別の製品認証キーが必要になります。PAK が組み合わせられて、1 つのアクティベーション キーになります。デバイス発送時に、すべてのライセンス PAK が提供されている場合もあります。ASA には基本ライセンスまたは Security Plus ライセンスがプリインストールされ、ご使用資格を満たしている場合には Strong Encryption（3DES/AES）ライセンスも提供されます。無料の Strong Encryption ライセンスを手動でリクエストする必要がある場合は、http://www.cisco.com/go/license を参照してください。

始める前に

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager では、組織のマスター アカウントを作成できます。

手順

ステップ 1 追加ライセンスを購入するには、http://www.cisco.com/go/ccw を参照してください。次の セキュアクライアント 発注ガイドおよび FAQ を参照してください。

- Cisco セキュアクライアント 発注ガイド
- セキュアクライアント ライセンスに関するよくある質問（FAQ）

ライセンスを購入した後、製品認証キー（PAK）が記載された電子メールを受け取ります。セキュアクライアント ライセンスの場合、ユーザーセッションの同じプールを使用する複数の

ASA に適用できるマルチユース PAK を受け取ります。場合によっては、PAK が記載された電子メールを受け取るまで数日かかることがあります。

ステップ 2 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカル サポートで使用され、ライセンスには使用されません。

ステップ 3 アクティベーション キーを取得するには、以下のライセンス Web サイトに移動します。

http://www.cisco.com/go/license

ステップ 4 プロンプトが表示されたら、次の情報を入力します。

- 製品認証キー（キーが複数ある場合は、まず 1 つを入力します。キーごとに個別のプロセスとして入力する必要があります）
- ASA のシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。時間ベース ライセンスの場合は、ライセンスごとに個別のアクティベーション キーがあります。

ステップ 5 さらに追加の製品認証キーがある場合は、製品認証キーごとにこの手順を繰り返します。すべての製品認証キーを入力した後、最後に送信されるアクティベーションキーには、登録した永続機能がすべて含まれています。

ステップ 6 キーのアクティブ化または非アクティブ化 （63 ページ）に基づいて、アクティベーション キーをインストールします。

高度暗号化ライセンスの取得

ASDM（および他の多数の機能）を使用するには、高度暗号化（3DES/AES）ライセンスをインストールする必要があります。ASA に高度暗号化ライセンスがプリインストールされていない場合は、ライセンスを無料で入手できます。高度暗号化ライセンスに関するそれぞれ国の資格を満たす必要があります。

手順

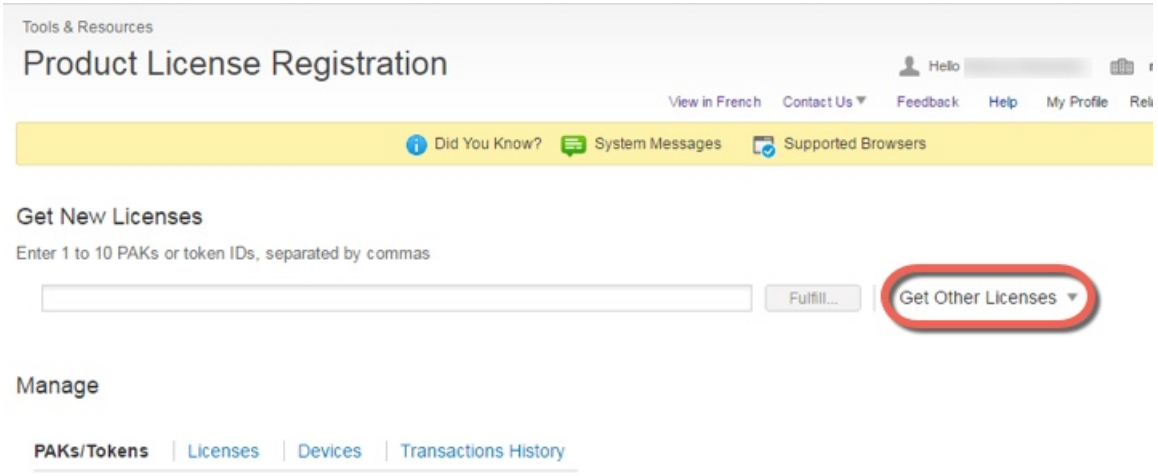
ステップ 1 次のコマンドを入力して、ASA のシリアル番号を取得します。

show version | grep Serial

このシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。

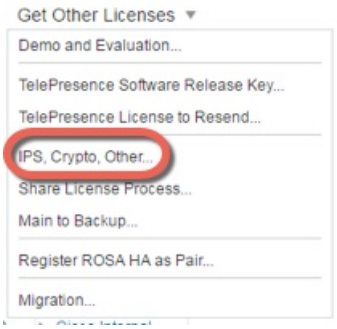
ステップ 2 Https://www.cisco.com/go/license を参照し、[Get Other Licenses] をクリックしてください。

図 *2*：他のライセンスの取得



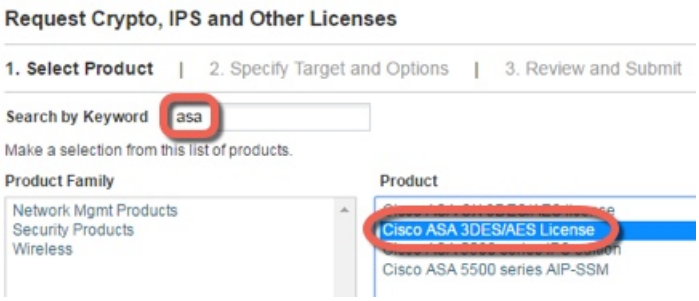
ステップ 3 [IPS、Crypto、その他（IPS, Crypto, Other）] を選択します。

図 *3*：*IPS*、*Crypto*、その他



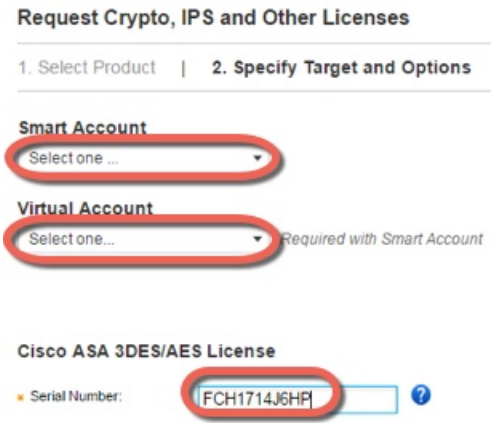
ステップ 4 [キーワード検索（Search by Keyword）] フィールドに **asa** と入力し、[Cisco ASA 3DES/AES License] を選択します。

図 *4 : Cisco ASA 3DES/AES* ライセンス



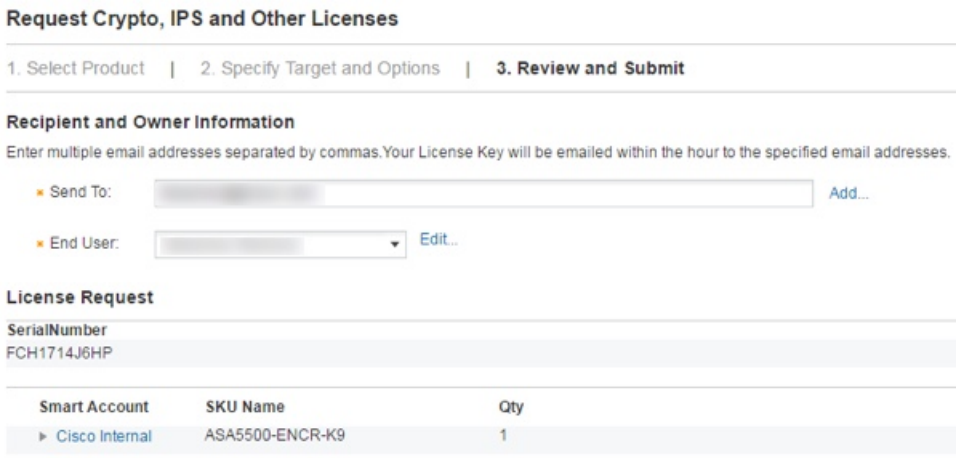
ステップ 5 [スマートアカウント（Smart Account）]、[バーチャルアカウント（Virtual Account）] を選択し、ASA の [シリアルナンバー（Serial Number）] を入力して、[次へ（Next）] をクリックします。

図 *5 :* スマート アカウント、バーチャル アカウント、シリアル番号



ステップ 6 送信先の電子メールアドレスとエンドユーザー名は自動的に入力されます。必要に応じて追加の電子メールアドレスを入力します。[同意する（I Agree）] チェックボックスをオンにして、[送信（Submit）] をクリックします。

図 *6 :* 送信



ステップ 7 その後、アクティベーション キーの記載された電子メールが届きますが、**[管理（Manage）]**> **[ライセンス（Licenses）]** エリアからキーをすぐにダウンロードすることもできます。

ステップ 8 キーのアクティブ化または非アクティブ化（63 ページ）に基づいて、アクティベーションキーを適用します。

キーのアクティブ化または非アクティブ化

この項では、新しいアクティベーション キーの入力と、時間ベース キーのアクティブ化および非アクティブ化の方法について説明します。

始める前に

- すでにマルチ コンテキスト モードに入っている場合は、システム実行スペースにこのアクティベーション キーを入力します。
- 一部の永続ライセンスでは、アクティブ化後に ASA をリロードする必要があります。次の表に、リロードが必要なライセンスを示します。

表 *2 :* 永続ライセンスのリロード要件

モデル	リロードが必要なライセンス アクション
すべてのモデル	暗号化ライセンスのダウングレード

手順

ステップ 1 アクティベーション キーを ASA に適用します。

activation-key *key* [**activate** | **deactivate**]

例：

```
ciscoasa# activation-key 0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

キーは、5 つのエレメントからなる 16 進文字列です。各エレメントは 1 つのスペースで区切られます。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。

1 つの永続キーおよび複数の時間ベース キーをインストールできます。新しい永続キーを入力した場合、すでにインストール済みのキーが上書きされます。

activate および **deactivate** キーワードは、時間ベース キーだけに使用できます。値を入力しない場合は、**activate** がデフォルトです。特定の機能に対して最後にアクティブ化した時間ベース キーがアクティブになります。アクティブな時間ベース キーを非アクティブにするには、**deactivate** キーワードを入力します。キーの初回入力時で、**deactivate** を指定した場合、キーは ASA に非アクティブ ステートでインストールされます。

ステップ 2 （場合によって必須）ASA をリロードします。

reload

永続ライセンスによっては、新しいアクティベーション キーの入力後に ASA をリロードする必要があります。リロードが必要な場合は、次のメッセージが表示されます。

```
WARNING: The running activation key was not updated with the requested key.
The flash activation key was updated with the requested key, and will become
active after the next reload.
```

関連トピック

時間ベース ライセンス （48 ページ）

共有ライセンスの設定（セキュアクライアント 3 以前）

（注） ASA の共有ライセンス機能は、セキュアクライアント 4 以降のライセンスではサポートされていません。セキュアクライアントライセンスは共有されるため、共有サーバーまたは参加者ライセンスは必要ありません。

この項では、共有ライセンス サーバーと参加システムを設定する方法について説明します。

共有ライセンスについて

共有ライセンスを使用すると、多数の セキュアクライアント Premium セッションを購入し、それらのセッションを ASA のグループ間で必要に応じて共有できます。そのためには、いず

れかの ASA を共有ライセンス サーバーとして、残りを共有ライセンス参加システムとして設定します。

共有ライセンスのサーバーと参加システムについて

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバーのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバーを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバーとして指定します。バックアップ サーバには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバに必要なのは参加ライセンスのみです。

4. 共有ライセンス サーバ上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
5. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバーに登録します。

（注） 参加者は IP ネットワークを経由してサーバと通信できる必要がありますが、同じサブネット上にある必要はありません。

6. 共有ライセンス サーバは、参加者がサーバにポーリングするべき頻度の情報で応答します。
7. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバに 50 セッション単位で追加セッションの要求を送信します。
8. 共有ライセンス サーバは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンス サーバーは、共有ライセンス プールに参加することもできます。参加には参加ライセンスもサーバ ライセンスも必要ありません。

1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバは使用可能な限りのセッション数で応答します。

2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバが要求に適切に対応できるまで続けます。

9. 参加者の負荷が減少した場合、参加者はサーバに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバーと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバーの間の通信問題

参加者とサーバ間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔3倍の時間が経過した後で、サーバはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバに到達できない場合、参加者はサーバから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24 時間を経過しても参加者がまだライセンス サーバと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバに再接続したが、サーバが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバは、参加者に再割り当てできる限りのセッション数で応答します。

共有ライセンス バックアップ サーバーについて

共有ライセンス バックアップ サーバは、バックアップの役割を実行する前にメインの共有ライセンス サーバへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバは共有ライセンス情報に加えてサーバ設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバとバックアップ サーバは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバはリロード後でもバックアップの役割を実行できます。

メイン サーバがダウンすると、バックアップ サーバがサーバ動作を引き継ぎます。バックアップ サーバは継続して最大30日間動作できます。30日を超えると、バックアップ サーバは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバが復旧した場合、メイン サーバはバックアップ サーバと同期してから、サーバ動作を引き継ぎます。

バックアップ サーバがアクティブでないときは、メインの共有ライセンス サーバの通常の参加者として動作します。

（注） メインの共有ライセンス サーバの初回起動時には、バックアップ サーバは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバがその後短時間でもダウンした場合、バックアップ サーバの動作制限は日ごとに減少します。メイン サーバが復旧した場合、バックアップ サーバは再び日ごとに増加を開始します。たとえば、メイン サーバが 20 日間ダウンしていて、その期間中バックアップ サーバがアクティブであった場合、バックアップ サーバには、10 日間の制限のみが残っています。バックアップ サーバは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

フェールオーバーと共有ライセンス

ここでは、共有ライセンスとフェールオーバーの相互作用について説明します。

フェールオーバーと共有ライセンス サーバー

この項では、メイン サーバーおよびバックアップ サーバーと、フェールオーバーとの相互作用について説明します。共有ライセンス サーバーでは、VPN ゲートウェイやファイアウォールなど、ASA としての通常機能も実行されます。このため、メインとバックアップの共有ライセンス サーバーにフェールオーバーを設定して、信頼性を高めることをお勧めします。

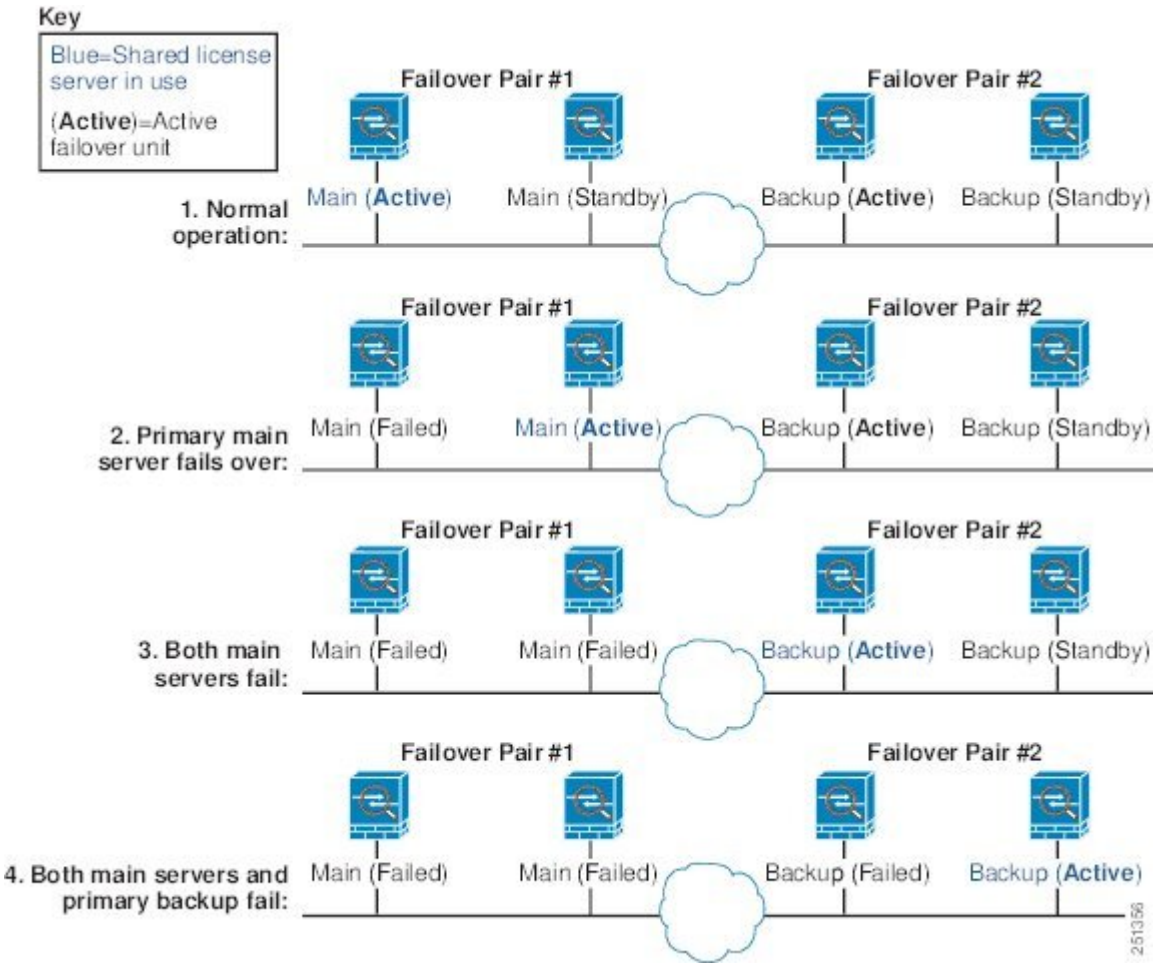
（注） バックアップ サーバー メカニズムとフェールオーバーは異なりますが、両者には互換性があります。

共有ライセンスはシングル コンテキスト モードでだけサポートされるため、アクティブ/アクティブ フェールオーバーはサポートされません。

アクティブ/スタンバイ フェールオーバーでは、プライマリ装置が主要な共有ライセンス サーバーとして機能し、スタンバイ装置はフェールオーバー後に主要な共有ライセンス サーバーとして機能します。スタンバイ装置は、バックアップの共有ライセンス サーバーとしては機能しません。必要に応じて、バックアップ サーバーとして機能する装置のペアを追加します。

たとえば、2 組のフェールオーバー ペアがあるネットワークを使用するとします。ペア #1 にはメインのライセンス サーバーが含まれます。ペア #2 にはバックアップ サーバーが含まれます。ペア #1 のプライマリ装置がダウンすると、ただちに、スタンバイ装置が新しくメイン ライセンス サーバーになります。ペア #2 のバックアップ サーバーが使用されることはありません。ペア #1 の装置が両方ともダウンした場合だけ、ペア #2 のバックアップ サーバーが共有ライセンス サーバーとして使用されるようになります。ペア #1 がダウンしたままで、ペア #2 のプライマリ装置もダウンした場合は、ペア #2 のスタンバイ装置が共有ライセンス サーバーとして使用されるようになります（次の図を参照）。

図 7: フェールオーバーと共有ライセンス サーバー



スタンバイ バックアップ サーバーは、プライマリ バックアップ サーバーと同じ動作制限を共有します。スタンバイ装置がアクティブになると、その時点からプライマリ装置のカウントダウンを引き継ぎます。

関連トピック

共有ライセンス バックアップ サーバーについて （66 ページ）

フェールオーバーと共有ライセンス参加システム

参加システムのペアについては、両方の装置を共有ライセンス サーバーに登録します。登録時には、個別の参加システム ID を使用します。アクティブ装置の参加システム ID は、スタンバイ装置と同期されます。スタンバイ装置は、アクティブに切り替わるときに、この ID を使用して転送要求を生成します。この転送要求によって、以前にアクティブだった装置から新しくアクティブになる装置に共有セッションが移動します。

参加者の最大数

ASA では、共有ライセンスの参加システム数に制限がありません。ただし、共有ネットワークの規模が非常に大きいと、ライセンス サーバーのパフォーマンスに影響する場合があります。この場合は、参加システムのリフレッシュ間隔を長くするか、共有ネットワークを2つ作成することをお勧めします。

共有ライセンス サーバーの設定

この項では、ASA を共有ライセンス サーバーとして設定する方法について説明します。

始める前に

サーバーが共有ライセンス サーバー キーを持っている必要があります。

手順

ステップ 1 共有秘密を設定します。

license-server secret *secret*

例：

```
ciscoasa(config)# license-server secret farscape
```

secret は、4 ～ 128 文字の ASCII 文字の文字列です。この秘密を持つ参加システムが、ライセンス サーバーを使用できます。

ステップ 2 （オプション）更新間隔を設定します。

license-server refresh-interval *seconds*

例：

```
ciscoasa(config)# license-server refresh-interval 100
```

間隔は 10 ～ 300 秒です。この値が、サーバーと通信する頻度として参加システムに設定されます。デフォルトは 30 秒です。

ステップ 3 （オプション）サーバーが参加ユニットからのSSL接続をリッスンするポートを設定します。

license-server port *port*

例：

```
ciscoasa(config)# license-server port 40000
```

port は 1 ～ 65535 です。デフォルトは、TCP ポート 50554 です。

ステップ 4 （オプション）バックアップ サーバーの IP アドレスとシリアル番号を指定します。

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]

例：

```
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

バックアップ サーバーがフェールオーバー ペアの一部である場合は、スタンバイ装置のシリアル番号も指定します。1 つのバックアップ サーバーとそのオプションのスタンバイ ユニットのみを指定できます。

ステップ 5 このユニットを共有ライセンス サーバーとしてイネーブルにします。

license-server enable *interface_name*

例：

```
ciscoasa(config)# license-server enable inside
```

参加システムがサーバーと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

共有ライセンス バックアップ サーバーの設定（オプション）

この項では、共有ライセンスのメイン サーバーがダウンした場合にバックアップ サーバーとして機能する参加システムをイネーブルにします。

始める前に

バックアップ サーバーには、共有ライセンス参加キーが必要です。

手順

ステップ 1 共有ライセンス サーバーの IP アドレスと共有秘密を指定します。

license-server address *address* **secret** *secret* [**port** *port*]

例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

デフォルト ポートをサーバー コンフィギュレーションで変更した場合は、同じポートをバックアップ サーバーにも設定します。

ステップ 2 このユニットを共有ライセンス バックアップ サーバーとしてイネーブルにします。

license-server backup enable *interface_name*

例：

```
ciscoasa(config)# license-server backup enable inside
```

参加システムがサーバーと通信するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

例

次に、ライセンス サーバーと共有秘密を指定し、このユニットを内部インターフェイスと dmz インターフェイス上のバックアップ共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

共有ライセンス パーティシパントの設定

この項では、共有ライセンス サーバーと通信する共有ライセンス参加システムを設定します。

始める前に

参加システムが共有ライセンス参加キーを持っている必要があります。

手順

ステップ 1 共有ライセンス サーバーの IP アドレスと共有秘密を指定します。

license-server address *address* **secret** *secret* [**port** *port*]

例：

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
```

デフォルト ポートをサーバー コンフィギュレーションで変更した場合は、同じポートを参加システムにも設定します。

ステップ 2 （オプション）バックアップ サーバーを設定した場合は、バックアップ サーバーのアドレスを入力します。

license-server backup address *address*

例：

```
ciscoasa(config)# license-server backup address 10.1.1.2
```

例

次に、ライセンス サーバーの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバーの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

モデルごとにサポートされている機能のライセンス

この項では、各モデルに使用できるライセンスと、ライセンスに関する特記事項について説明します。

モデルごとのライセンス

この項では、各モデルに使用できる機能のライセンスを示します。

イタリック体で示された項目は、基本ライセンス（または Security Plus など）ライセンス バージョンを置換できる個別のオプション ライセンスです。オプション ライセンスは、混在させることも統一することもできます。

（注） 一部の機能は互換性がありません。互換性情報については、個々の機能の章を参照してください。

ペイロード暗号化機能のないモデルの場合は、次に示す機能の一部がサポートされません。サポートされない機能のリストについては、ペイロード暗号化機能のないモデル （55 ページ）を参照してください。

ライセンスの詳細については、ライセンスに関する注意事項 （50 ページ）を参照してください。

ISA 3000 ライセンスの各機能

次の表に、ISA 3000 のライセンス機能を示します。

ライセンス	基本ライセンス		Security Plus ライセンス	
ファイアウォール ライセンス				
Botnet Traffic Filter	サポートなし		サポートなし	
ファイアウォールの接続、同時	20,000		50,000	
キャリア	サポートなし		サポートなし	
合計 TLS プロキシセッション	160		160	
VPN ライセンス				
セキュアクライアントピア	無効	オプション*Secure Client Advantage*、*Secure Client Premier*、*Secure Client VPN* のみライセンス：最大 *25*	無効	オプション*Secure Client Advantage*、*Secure Client Premier*、*Secure Client VPN* のみライセンス：最大 *25*
その他の VPN ピア	10		50	
合計 VPN ピア。全タイプの合計	25		50	
VPN ロードバランシング	サポートなし		サポートなし	
一般ライセンス				
暗号化	基本（DES）	オプションライセンス：強化（*3DES/AES*）	基本（DES）	オプションライセンス：強化（*3DES/AES*）
フェールオーバー	サポートなし		アクティブ/スタンバイ	

ライセンス	基本ライセンス	Security Plus ライセンス
セキュリティ コンテキスト	サポートなし	サポートなし
クラスタ	サポートなし	サポートなし
VLAN、最大	5	25

PAK ライセンスのモニタリング

この項では、ライセンス情報の表示方法について説明します。

現在のライセンスの表示

この項では、現在のライセンスと、時間ベース アクティベーション キーの残り時間を表示する方法について説明します。

始める前に

ペイロード暗号化機能のないモデルでライセンスを表示すると、VPN および Unified Communications ライセンスは一覧に示されません。詳細については、「ペイロード暗号化機能のないモデル （55 ページ）」を参照してください。

手順

永続ライセンス、アクティブな時間ベース ライセンス、および実行ライセンスを表示します。実行ライセンスとは、永続ライセンスとアクティブな時間ベース ライセンスの組み合わせです。

show activation-key [**detail**]

detail キーワードを使用すると、非アクティブな時間ベース ライセンスも表示されます。

フェールオーバーまたはクラスタ ユニットでは、このコマンドは、すべてのユニットの結合キーである「クラスタ」ライセンスも示します。

例

例 1：show activation-key コマンドのスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、およびアクティブな各時間ベース ライセンスを示す、スタンドアロン ユニットの **show activation-key** コマンドの出力例を示します。

```
ciscoasa# show activation-key

Serial Number:  JMX1232L11M
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Running Timebased Activation Key: 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2

Licensed features for this platform:
Maximum Physical Interfaces       : Unlimited      perpetual
Maximum VLANs                     : 150            perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
VPN-DES                           : Enabled        perpetual
VPN-3DES-AES                      : Enabled        perpetual
Security Contexts                 : 10             perpetual
GTP/GPRS                          : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Enabled        perpetual
  Shared AnyConnect Premium Peers : 12000          perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 12             62 days
Total UC Proxy Sessions           : 12             62 days
Botnet Traffic Filter             : Enabled        646 days
Intercompany Media Engine         : Disabled       perpetual

This platform has a Base license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter        : Enabled    646 days

0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2 0xyadayad2
Total UC Proxy Sessions      : 10         62 days
```

例 2：show activation-key detail のスタンドアロン ユニットの出力

次に、実行ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）、および永続ライセンスとインストールされている各時間ベース ライセンス（アクティブおよび非アクティブ）を示す、スタンドアロン ユニットの **show activation-key detail** コマンドの出力例を示します。

```
ciscoasa# show activation-key detail

Serial Number:  88810093382
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
```

```
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5512-X Security Plus license.

Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : 8              perpetual
VLANs                          : 20             DMZ Unrestricted
Dual ISPs                      : Enabled        perpetual
VLAN Trunk Ports               : 8              perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Standby perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 25             perpetual
Total VPN Peers                   : 25              perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        39 days
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    39 days

Inactive Timebased Activation Key:
0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3 0xyadayada3
AnyConnect Premium Peers                   : 25     7 days
```

例 3：show activation-key detail に対するフェールオーバー ペアのプライマリ ユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセン

スです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。

- プライマリ ユニットの永続ライセンス。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000171
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c
Running Timebased Activation Key: 0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 12             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers       : 4           perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.
```

```
Running Permanent Activation Key: 0xce06dc6b 0x8a7b5ab7 0xa1e21dd4 0xd2c4b8b8 0xc4594f9c

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xa821d549 0x35725fe4 0xc918b97b 0xce0b987b 0x47c7c285
Botnet Traffic Filter           : Enabled    33 days

Inactive Timebased Activation Key:
0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3 0xyadayad3
Security Contexts               : 2          7 days
AnyConnect Premium Peers                   : 100        7 days

0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4 0xyadayad4
Total UC Proxy Sessions         : 100        14 days
```

例 4：show activation-key detail に対するフェールオーバー ペアのセカンダリ ユニット出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key detail** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリ ユニットの永続ライセンス。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  P3000000011
Running Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
GTP/GPRS                       : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 2              perpetual
Total UC Proxy Sessions        : 2              perpetual
Botnet Traffic Filter          : Disabled       perpetual
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Failover cluster licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Enabled        perpetual
Security Contexts              : 10             perpetual
GTP/GPRS                       : Enabled        perpetual
AnyConnect Premium Peers          : 4              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions        : 4              perpetual
Total UC Proxy Sessions        : 4              perpetual
Botnet Traffic Filter          : Enabled        33 days
Intercompany Media Engine      : Disabled       perpetual

This platform has an ASA 5520 VPN Plus license.

Running Permanent Activation Key: 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1 0xyadayad1

Licensed features for this platform:
Maximum Physical Interfaces    : Unlimited      perpetual
Maximum VLANs                  : 150            perpetual
Inside Hosts                   : Unlimited      perpetual
Failover                       : Active/Active  perpetual
VPN-DES                        : Enabled        perpetual
VPN-3DES-AES                   : Disabled       perpetual
Security Contexts              : 2              perpetual
```

```
GTP/GPRS                        : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 750            perpetual
Total VPN Peers                   : 750            perpetual
Shared License                    : Disabled        perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions         : 2              perpetual
Total UC Proxy Sessions         : 2              perpetual
Botnet Traffic Filter           : Disabled       perpetual
Intercompany Media Engine       : Disabled       perpetual

The flash permanent activation key is the SAME as the running permanent key.
```

例 5：show activation-key に対する、フェールオーバー ペアでの ASA サービス モジュールのプライマリ ユニット出力

次に、プライマリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- プライマリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- プライマリ ユニットのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。

```
ciscoasa# show activation-key

erial Number:  SAL144705BF
Running Permanent Activation Key: 0x4d1ed752 0xc8cfeb37 0xf4c38198 0x93c04c28 0x4a1c049a
Running Timebased Activation Key: 0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880

Licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
Security Contexts                 : 25             perpetual
GTP/GPRS                          : Enabled        perpetual
Botnet Traffic Filter             : Enabled        330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces                : 1024           perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Active  perpetual
DES                               : Enabled        perpetual
3DES-AES                          : Enabled        perpetual
```

```
Security Contexts                : 50 perpetual
GTP/GPRS                         : Enabled        perpetual
Botnet Traffic Filter            : Enabled        330 days
This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.

The flash permanent activation key is the SAME as the running permanent key.

Active Timebased Activation Key:
0xbc07bbd7 0xb15591e0 0xed68c013 0xd79374ff 0x44f87880
Botnet Traffic Filter           : Enabled    330 days
```

例 6：show activation-key に対する、フェールオーバー ペアでの ASA サービス モジュールのセカンダリ ユニット出力

次に、セカンダリ フェールオーバー ユニットの **show activation-key** コマンドの出力例を示します。

- セカンダリ ユニット ライセンス（永続ライセンスと時間ベース ライセンスの組み合わせ）。
- プライマリおよびセカンダリ装置のライセンスの組み合わせである、「フェールオーバー クラスタ」ライセンス。これは、ASA で実際に実行されているライセンスです。プライマリおよびセカンダリ ライセンスの組み合わせを反映したこのライセンスの値は、太字になっています。
- セカンダリのインストール済みの時間ベース ライセンス（アクティブおよび非アクティブ）。このユニットには時間ベース ライセンスはないため、この出力例には何も表示されません。

```
ciscoasa# show activation-key detail

Serial Number:  SAD143502E3
Running Permanent Activation Key: 0xf404c46a 0xb8e5bd84 0x28c1b900 0x92eca09c 0x4e2a0683

Licensed features for this platform:
Maximum Interfaces               : 1024           perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
DES                              : Enabled        perpetual
3DES-AES                         : Enabled        perpetual
Security Contexts                : 25             perpetual
GTP/GPRS                         : Disabled       perpetual
Botnet Traffic Filter            : Disabled       perpetual

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.


Failover cluster licensed features for this platform:
Maximum Interfaces               : 1024           perpetual
Inside Hosts                     : Unlimited      perpetual
Failover                         : Active/Active  perpetual
DES                              : Enabled        perpetual
3DES-AES                         : Enabled        perpetual
Security Contexts                : 50 perpetual
GTP/GPRS                         : Enabled perpetual
Botnet Traffic Filter            : Enabled 330 days

This platform has an WS-SVC-ASA-SM1 No Payload Encryption license.
```

```
The flash permanent activation key is the SAME as the running permanent key.
```

例 7：クラスタでの show activation-key の出力

```
ciscoasa# show activation-key
 Serial Number: JMX1504L2TD
 Running Permanent Activation Key: 0x4a3eea7b 0x54b9f61a 0x4143a90c 0xe5849088 0x4412d4a9


 Licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 2 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 2 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 2 perpetual
 Total UC Proxy Sessions : 2 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 Failover cluster licensed features for this platform:
 Maximum Physical Interfaces : Unlimited perpetual
 Maximum VLANs : 100 perpetual
 Inside Hosts : Unlimited perpetual
 Failover : Active/Active perpetual
 Encryption-DES : Enabled perpetual
 Encryption-3DES-AES : Enabled perpetual
 Security Contexts : 4 perpetual
 GTP/GPRS : Disabled perpetual
 AnyConnect Premium Peers : 4 perpetual
 AnyConnect Essentials : Disabled perpetual
 Other VPN Peers : 250 perpetual
 Total VPN Peers : 250 perpetual
 Shared License : Disabled perpetual
 AnyConnect for Mobile : Disabled perpetual
 AnyConnect for Cisco VPN Phone : Disabled perpetual
 Advanced Endpoint Assessment : Disabled perpetual
 UC Phone Proxy Sessions : 4 perpetual
 Total UC Proxy Sessions : 4 perpetual
 Botnet Traffic Filter : Disabled perpetual
 Intercompany Media Engine : Disabled perpetual
 Cluster : Enabled perpetual

 This platform has an ASA 5585-X base license.

 The flash permanent activation key is the SAME as the running permanent key.
```

共有ライセンスのモニタリング

共有ライセンスをモニターするには、次のいずれかのコマンドを入力します。

- **show shared license** [**detail** | **client** [*hostname*] | **backup**]

  共有ライセンス統計情報を表示します。オプション キーワードはライセンス サーバーだけに使用できます。**detail** キーワードを使用すると、参加システムごとの統計情報が表示されます。表示内容を 1 台の参加システムに限定するには、**client** キーワードを使用します。**backup** キーワードを使用すると、バックアップ サーバーに関する情報が表示されます。

  共有ライセンスの統計情報をクリアするには、**clear shared license** コマンドを入力します。

  次に、ライセンス参加ユニットでの **show shared license** コマンドの出力例を示します。

```
ciscoasa>  show shared license
Primary License Server : 10.3.32.20
  Version              : 1
  Status               : Inactive

Shared license utilization:
  SSLVPN:
    Total for network :     5000
    Available         :     5000
    Utilized          :        0
  This device:
    Platform limit    :      250
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
```

  次に、ライセンス サーバー上での **show shared license detail** コマンドの出力例を示します。

```
ciscoasa>  show shared license detail
Backup License Server Info:

Device ID           : ABCD
Address             : 10.1.1.2
Registered          : NO
HA peer ID          : EFGH
Registered          : NO
  Messages Tx/Rx/Error:
    Hello           : 0 / 0 / 0
    Sync            : 0 / 0 / 0
    Update          : 0 / 0 / 0

Shared license utilization:
  SSLVPN:
    Total for network :      500
    Available         :      500
    Utilized          :        0
  This device:
    Platform limit    :      250
```

```
    Current usage     :        0
    High usage        :        0
  Messages Tx/Rx/Error:
    Registration    : 0 / 0 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0


Client Info:

  Hostname          : 5540-A
  Device ID         : XXXXXXXXXXX
  SSLVPN:
    Current usage   : 0
    High            : 0
  Messages Tx/Rx/Error:
    Registration    : 1 / 1 / 0
    Get             : 0 / 0 / 0
    Release         : 0 / 0 / 0
    Transfer        : 0 / 0 / 0
...
```

- **show activation-key**

  ASA にインストールされているライセンスを表示します。**show version** コマンドでもライセンス情報が表示されます。

- **show vpn-sessiondb**

  VPN セッションのライセンス情報を表示します。

PAK ライセンスの履歴

機能名	プラットフォーム リリース	説明
接続数と VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA5510 Base ライセンス接続は 32000 から 5000 に、VLAN は 0 から 10 に増加。 • ASA5510 Security Plus ライセンス接続は 64000 から 130000 に、VLAN は 10 から 25 に増加。 • ASA5520 接続は 130000 から 280000 に、VLAN は 25 から 100 に増加。 • ASA5540 接続は 280000 から 400000 に、VLAN は 100 から 200 に増加。
SSL VPN ライセンス	7.1(1)	SSL VPN ライセンスが導入されました。

機能名	プラットフォーム リリース	説明
SSL VPN ライセンスの追加	7.2(1)	5000 ユーザーの SSL VPN ライセンスが ASA 5550 以降に対して導入されました。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。
VLAN 数の増加	7.2(2)	ASA 5505 上の Security Plus ライセンスに対する VLAN 最大数が、5（3 つのフル機能インターフェイス、1 つのフェールオーバー インターフェイス、1 つのバックアップ インターフェイスに制限されるインターフェイス）から 20 のフル機能インターフェイスに増加されました。また、トランク ポート数も 1 から 8 に増加されました。フル機能のインターフェイスの数が 20 になり、バックアップ ISP インターフェイスを停止するために backup interface コマンドを使用する必要がなくなりました。つまり、バックアップ ISP インターフェイス用にフル機能のインターフェイスを使用できるようになりました。backup interface コマンドは、これまでどおり Easy VPN 設定用に使用できます。 VLAN の制限値も変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、Security Plus ライセンスを使用する Ethernet 0/0 および 0/1 ポート用にギガビット イーサネット（1000 Mbps）をサポートしています。基本ライセンスでは、これらのポートは引き続きファスト イーサネット（100 Mbps）ポートとして使用されます。いずれのライセンスに対しても、Ethernet 0/2、0/3、および 0/4 はファスト イーサネット ポートのままです。 （注） インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。 **speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。

機能名	プラットフォーム リリース	説明
Advanced Endpoint Assessment ライセンス	8.0(2)	Advanced Endpoint Assessment ライセンスが導入されました。Cisco AnyConnect またはクライアントレス SSL VPN 接続の条件としてリモートコンピュータでスキャン対象となる、アンチウイルスアプリケーションやアンチスパイウェア アプリケーション、ファイアウォール、オペレーティングシステム、および関連アップデートの種類が、大幅に拡張されました。また、任意のレジストリエントリ、ファイル名、およびプロセス名を指定してスキャン対象にすることもできます。スキャン結果をASA に送信します。ASA は、ユーザー ログイン クレデンシャルとコンピュータ スキャン結果の両方を使用して、ダイナミック アクセス ポリシー（DAP）を割り当てます。 Advanced Endpoint Assessment ライセンスを使用すると、バージョン要件を満たすように非準拠コンピュータのアップデートを試行する機能を設定して、Host Scan を拡張できます。 シスコは、Host Scan でサポートされるアプリケーションとバージョンの一覧に、Cisco Secure Desktop とは異なるパッケージで、タイムリーなアップデートを提供できます。
ASA 5510 の VPN ロード バランシング	8.0(2)	VPN ロード バランシングが ASA 5510 Security Plus ライセンスでサポートされるようになりました。
AnyConnect for Mobile ライセンス	8.0(3)	AnyConnect for Mobile ライセンスが導入されました。これにより、Windows モバイルデバイスはセキュアクライアント を使用して ASA に接続できます。
時間ベース ライセンス	8.0(4)/8.1(2)	時間ベース ライセンスがサポートされるようになりました。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。

機能名	プラットフォーム リリース	説明
Unified Communications Proxy セッション ライセンス	8.0(4)	UC Proxy セッション ライセンスが導入されました。電話プロキシ、Presence Federation Proxy、および Encrypted Voice Inspection アプリケーションでは、それらの接続に TLS プロキシ セッションが使用されます。各 TLS プロキシ セッションは、UC ライセンスの制限に対してカウントされます。これらのアプリケーションは、すべて UC Proxy として包括的にライセンスされるので、混在させたり、組み合わせたりできます。 この機能は、バージョン 8.1 では使用できません。
ボットネット トラフィック フィルタ ライセンス	8.2(1)	ボットネット トラフィック フィルタ ライセンスが導入されました。ボットネット トラフィック フィルタでは、既知の不正なドメインや IP アドレスに対する接続を追跡して、マルウェア ネットワーク アクティビティから保護します。

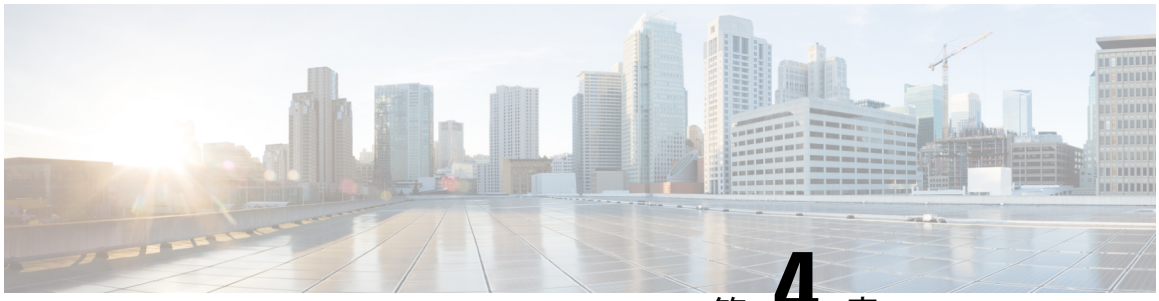
機能名	プラットフォーム リリース	説明
AnyConnect Essentials ライセンス	8.2(1)	AnyConnect Essentials ライセンスが導入されました。このライセンスにより、AnyConnect VPN クライアントは ASA にアクセスできるようになります。このライセンスでは、ブラウザベースの SSL VPN アクセスまたは Cisco Secure Desktop はサポートされていません。これらの機能に対しては、AnyConnect Essentials ライセンスの代わりに AnyConnect Premium ライセンスがアクティブ化されます。 （注） AnyConnect Essentials ライセンスを所有する VPN ユーザーは、Web ブラウザを使用してログインし、セキュアクライアント をダウンロードおよび起動（WebLaunch）できます。 このライセンスか AnyConnect Premium ライセンスでイネーブル化されたかに関係なく、セキュアクライアント ソフトウェアには同じクライアント機能のセットが装備されています。 特定の ASA では、AnyConnect Premium ライセンス（全タイプ）または Advanced Endpoint Assessment ライセンスを、AnyConnect Essentials ライセンスと同時にアクティブにすることはできません。ただし、同じネットワーク内の異なる ASA で、AnyConnect Essentials ライセンスと AnyConnect Premium ライセンスを実行することは可能です。 デフォルトでは、ASA は AnyConnect Essentials ライセンスを使用しますが、**webvpn** を使用し、次に **no anyconnect-essentials** コマンドを使用すると、AnyConnect Essentials ライセンスを無効にして他のライセンスを使用できます。
SSL VPN ライセンスの AnyConnect Premium SSL VPN Edition ライセンスへの変更	8.2(1)	SSL VPN ライセンスの名前が AnyConnect Premium SSL VPN Edition ライセンスに変更されました。
SSL VPN の共有ライセンス	8.2(1)	SSL VPN の共有ライセンスが導入されました。複数の ASA で、SSL VPN セッションのプールを必要に応じて共有できます。
モビリティ プロキシ アプリケーションでの Unified Communications Proxy ライセンス不要化	8.2(2)	モビリティ プロキシに UC Proxy ライセンスが必要なくなりました。

機能名	プラットフォーム リリース	説明
ASA 5585-X（SSP-20）用 10 GE I/O ライセンス	8.2(3)	ASA 5585-X（SSP-20）の 10 GE I/O ライセンスを導入し、ファイバ ポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-60 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 （注） ASA 5585-X は 8.3(x) ではサポートされていません。
ASA 5585-X（SSP-10）用 10 GE I/O ライセンス	8.2(4)	ASA 5585-X（SSP-10）の 10 GE I/O ライセンスを導入し、ファイバ ポートでの 10 ギガビット イーサネットの速度をイネーブルにしました。SSP-40 は、デフォルトで 10 ギガビット イーサネットの速度をサポートします。 （注） ASA 5585-X は 8.3(x) ではサポートされていません。
同一でないフェールオーバー ライセンス	8.3(1)	フェールオーバー ライセンスが各ユニット上で同一である必要がなくなりました。両方のユニットで使用するライセンスは、プライマリ ユニットおよびセカンダリ ユニットからの結合されたライセンスです。 **show activation-key** および **show version** の各コマンドが変更されました。
スタック可能な時間ベース ライセンス	8.3(1)	時間ベース ライセンスがスタッカブルになりました。多くの場合、時間ベース ライセンスは更新の必要があり、旧ライセンスから新しいライセンスへシームレスに移行する必要があります。時間ベース ライセンスだけで使用される機能では、新しいライセンスが適用される前に、ライセンスの有効期限が切れてしまわないことが特に重要です。ASA では時間ベース ライセンスをスタックできるので、ライセンスの有効期限が切れたり、新しいライセンスを早めにインストールしたために時間が無駄になったりする心配はありません。
Intercompany Media Engine ライセンス	8.3(1)	IME ライセンスが導入されました。
複数の時間ベース ライセンスの同時アクティブ化	8.3(1)	時間ベース ライセンスを複数インストールできるようになり、同時に機能ごとに 1 つのアクティブなライセンスを保持できるようになりました。 **show activation-key** および **show version** の各コマンドが変更されました。

機能名	プラットフォーム リリース	説明
時間ベース ライセンスのアクティブ化と非アクティブ化の個別化	8.3(1)	コマンドを使用して、時間ベース ライセンスをアクティブ化または非アクティブ化できるようになりました。 **activation-key** [**activate** | **deactivate**] コマンドが変更されました。
AnyConnect Premium SSL VPN Edition ライセンスの AnyConnect Premium SSL VPN ライセンスへの変更	8.3(1)	AnyConnect Premium SSL VPN Edition ライセンスの名前が AnyConnect Premium SSL VPN ライセンスに変更されました。
輸出用のペイロード暗号化なしイメージ	8.3(2)	ASA 5505 ～ 5550 にペイロード暗号化機能のないソフトウェアをインストールした場合、Unified Communications、強力な暗号化VPN、強力な暗号化管理プロトコルをディセーブルにします。 （注） この特殊なイメージは 8.3(x) でのみサポートされます。8.4(1) 以降で暗号化機能のないソフトウェアをサポートするには、ASA の特別なハードウェア バージョンを購入する必要があります。
ASA 5550、5580、および 5585-X でのコンテキストの増加	8.4(1)	ASA 5550 および ASA 5585-X（SSP-10）では、コンテキストの最大数が 50 から 100 に引き上げられました。ASA 5580 および 5585-X（SSP-20）以降では、コンテキストの最大数が 50 から 250 に引き上げられました。
ASA 5580 および 5585-X での VLAN 数の増加	8.4(1)	ASA 5580 および ASA 5585-X では、VLAN の最大数が 250 から 1024 に引き上げられました。
ASA 5580 および 5585-X での接続数の増加	8.4(1)	ファイアウォール接続の最大数が次のように引き上げられました。 • ASA 5580-20：1,000,000 から 2,000,000 へ。 • ASA 5580-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-10：750,000 から 1,000,000 へ。 • ASA 5585-X with SSP-20：1,000,000 から 2,000,000 へ。 • ASA 5585-X with SSP-40：2,000,000 から 4,000,000 へ。 • ASA 5585-X with SSP-60：2,000,000 から 10,000,000 へ。

機能名	プラットフォーム リリース	説明
AnyConnect Premium SSL VPN ライセンスの AnyConnect Premium ライセンスへの変更	8.4(1)	AnyConnect Premium SSL VPN ライセンスの名前が AnyConnect Premium ライセンスに変更されました。ライセンス情報の表示が「SSL VPN ピア」から「AnyConnect Premium ピア」に変更されました。
ASA 5580 での AnyConnect VPN セッション数の増加	8.4(1)	AnyConnect VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
ASA 5580 での AnyConnect 以外の VPN セッション数の増加	8.4(1)	AnyConnect 以外の VPN セッションの最大数が 5,000 から 10,000 に引き上げられました。
IKEv2 を使用した IPsec リモート アクセス	8.4(1)	AnyConnect Essentials ライセンスおよび AnyConnect Premium ライセンスに IKEv2 を使用した IPsec リモート アクセス VPN が追加されました。 （注） ASA での IKEv2 のサポートに関して、重複するセキュリティ アソシエーションがサポートされていないという制約が現在あります。 Other VPN ライセンス（以前の IPsec VPN）には IKEv2 サイトツーサイト セッションが追加されました。Other VPN ライセンスは基本ライセンスに含まれています。
輸出用のペイロード暗号化なしハードウェア	8.4(1)	ペイロード暗号化機能のないモデルでは（ASA 5585-X など）、特定の国に ASA を輸出できるよう、ASA ソフトウェアのユニファイド コミュニケーションと VPN 機能を無効にしています。
デュアル SSP（SSP-20 および SSP-40）	8.4(2)	SSP-40 および SSP-60 の場合、同じシャーシでレベルが同じ 2 つの SSP を使用できます。レベルが混在した SSP はサポートされていません（たとえば、SSP-40 と SSP-60 の組み合わせはサポートされていません）。各 SSP は個別のコンフィギュレーションおよび管理を持つ独立したデバイスとして動作します。必要に応じて 2 つの SSP をフェールオーバー ペアとして使用できます。2 個の SSP をシャーシで使用する場合、VPN はサポートされません。しかし、VPN がディセーブルになっていないことに注意してください。
ASA 5512-X ～ ASA 5555-X での IPS モジュール ライセンス	8.6(1)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、および ASA 5555-X での IPS SSP ソフトウェア モジュールには IPS モジュール ライセンスが必要です。

機能名	プラットフォーム リリース	説明
ASA 5580 および ASA 5585-X のクラスタリング ライセンス。	9.0(1)	クラスタリング ライセンスが ASA 5580 および ASA 5585-X に対して追加されました。
ASASM での VPN のサポート	9.0(1)	ASASM は、すべての VPN 機能をサポートするようになりました。
ASASM でのユニファイド コミュニケーションのサポート	9.0(1)	ASASM は、すべてのユニファイド コミュニケーション機能をサポートするようになりました。
SSP-10 および SSP-20 に対する ASA 5585-X デュアル SSP サポート（SSP-40 および SSP-60 に加えて）、デュアル SSP に対する VPN サポート	9.0(1)	ASA 5585-X は、すべての SSP モデルでデュアル SSP をサポートするようになりました（同一シャーシ内で同じレベルの SSP を 2 つ使用できます）。デュアル SSP を使用するときに VPN がサポートされるようになりました。
ASA 5500-X でのクラスタリングのサポート	9.1(4)	ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X および ASA 5555-X が 2 ユニット クラスタをサポートするようになりました。2 ユニットのクラスタリングは、基本ライセンスではデフォルトでイネーブルになります。ASA 5512-X では Security Plus ライセンスが必要です。
ASA 5585-X の 16 のクラスタ メンバのサポート	9.2(1)	ASA 5585-X が 16 ユニット クラスタをサポートするようになりました。
ASAv4 および ASAv30 の標準およびプレミアム モデル ライセンスの導入	9.2(1)	シンプルなライセンス方式で ASAv が導入されました（標準またはプレミアム レベルの ASAv4 および ASAv30 永続ライセンス）。アドオン ライセンスは使用できません。



第 4 章

ライセンス：スマート ソフトウェア ライセンシング

スマート ソフトウェア ライセンシングによって、ライセンスを購入し、ライセンスのプールを一元管理することができます。製品認証キー（PAK）ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンス キーを管理しなくても、簡単に ASA を導入したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。

（注） プラットフォーム別のスマートライセンスの機能と動作の詳細については、「Smart Enabled Product Families」を参照してください。

- スマート ソフトウェア ライセンスについて （93 ページ）
- スマート ソフトウェア ライセンスの前提条件 （124 ページ）
- スマート ソフトウェア ライセンスのガイドライン （125 ページ）
- スマート ソフトウェア ライセンスのデフォルト （125 ページ）
- ASA 仮想：スマート ソフトウェア ライセンスの設定 （126 ページ）
- 1000/1200/3100/4200：スマート ソフトウェア ライセンシングの設定 （153 ページ）
- Firepower 4100/9300：スマート ソフトウェア ライセンスの設定 （169 ページ）
- モデルごとのライセンス （172 ページ）
- モデルごとのライセンス PID （188 ページ）
- スマート ソフトウェア ライセンシングのモニタリング （193 ページ）
- Smart Software Manager 通信 （197 ページ）
- Smart Software Licensing の履歴 （200 ページ）

スマート ソフトウェア ライセンスについて

シスコ スマート ライセンシングは、シスコ ポートフォリオ全体および組織全体でソフトウェアをより簡単かつ迅速に一貫して購入および管理できる柔軟なライセンス モデルです。また、

これは安全です。ユーザーがアクセスできるものを制御できます。スマートライセンスを使用すると、次のことが可能になります。

- **簡単なアクティベーション**：スマートライセンスは、組織全体で使用できるソフトウェアライセンスのプールを確立します。PAK（製品アクティベーションキー）は不要です。
- **管理の統合**：My Cisco Entitlements（MCE）は、使いやすいポータルですべてのシスコ製品とサービスの完全なビューを提供するので、取得したもの、使用しているものを常に把握できます。
- **ライセンスの柔軟性**：ソフトウェアはハードウェアにノードロックされていないため、必要に応じてライセンスを簡単に使用および転送できます。

スマートライセンシングを使用するには、まず Cisco Software Central（software.cisco.com）でスマートアカウントを設定する必要があります。

シスコライセンスの概要については詳しくは、cisco.com/go/licensingguide を参照してください。

Firepower 4100/9300 シャーシの ASA のスマート ソフトウェア ライセンシング

Firepower 4100/9300 シャーシ 上の ASA では、スマート ソフトウェア ライセンシングの設定は、Firepower 4100/9300 シャーシ スーパバイザと ASA に分割されています。

- Firepower 4100/9300 シャーシ：Smart Software Manager との通信に使用するパラメータなど、すべてのスマート ソフトウェア ライセンシング インフラストラクチャをシャーシで設定します。Firepower 4100/9300 シャーシ 自体の動作にライセンスは必要ありません。ライセンスの手順については、『FXOS 構成ガイド』を 参照してください。

（注） シャーシ間クラスタリングでは、クラスタ内の各シャーシで同じスマート ライセンス方式を有効にする必要があります。

- ASA アプリケーション：ASA のすべてのライセンスの権限付与を設定します。

Smart Software Manager とアカウント

デバイスの 1 つ以上のライセンスを購入する場合は、Cisco Smart Software Manager で管理します。

https://software.cisco.com/#module/SmartLicensing

Smart Software Manager では、組織のマスター アカウントを作成できます。

（注） まだアカウントをお持ちでない場合は、このリンクをクリックして新しいアカウントをセットアップしてください。Smart Software Manager を使用すると、組織のマスター アカウントを作成できます。

デフォルトでは、マスターアカウントにあるデフォルトの仮想アカウントにライセンスが割り当てられます。アカウント管理者は、必要に応じて仮想アカウントを追加できます。たとえば、地域、部門、または支社用にアカウントを作成できます。複数の仮想アカウントがあることで、大量のライセンスやデバイスを簡単に管理できます。

オフライン管理

デバイスにインターネットアクセスがなく、Smart Software Manager に登録できない場合は、オフライン ライセンスを構成する必要があります。

パーマネント ライセンスの予約

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、各 ASA の永続ライセンスを要求できます。永続ライセンスでは、Smart Software Manager への定期的なアクセスは必要ありません。PAK ライセンスの場合と同様にライセンスを購入し、ASA のライセンス キーをインストールします。PAK ライセンスとは異なり、ライセンスの取得と管理に Smart Software Manager を使用します。通常のスマート ライセンス モードと永続ライセンスの予約モード間で簡単に切り替えることができます。

（注） ASA は特定のライセンス予約（SLR）をサポートしていません。SLR では、特定の機能権限が永続的に有効になっています。ASA は、すべての機能が永続的に有効になっている PLR のみをサポートします。

ASA Virtual 永久ライセンス予約

（注） 永久ライセンス予約は、VMware と KVM のみでサポートされます。

次のすべての機能を有効にするモデル固有のライセンスを取得できます。

- 使用中のモデルの最大スループット
- Essentials 層
- 高度暗号化（3DES および AES）ライセンス（スマート ライセンシング アカウントで有効にしている場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

（注） セキュアクライアントの機能を使用するには、セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

Cisco では、 ASA 仮想に 2 つの永続ライセンスの予約モードを用意しています。

- メモリおよび vCPU に基づく永続ライセンスの予約モード
- 柔軟なパーマネント ライセンスの予約モード

メモリおよび vCPU に基づく永続ライセンスの予約モード

ASA 仮想に割り当てられた RAM と vCPU に基づいて、モデル固有のライセンスを設定できます。たとえば、8 GB RAM と 4 つの vCPU を搭載した ASA 仮想 の場合、 では常に 2G のスループットを備えた ASAv30 ライセンスを使用します。

vCPU およびメモリとライセンスの関係は次のとおりです。

- 2 GB、1 vCPU：ASAv5（100 M）（**license smart set_plr5** コマンドを実行する必要があります。それ以外の場合は、ASAv10 ライセンスが 1 G のスループットを可能にするように割り当てられます）。

（注） バージョン 9.13 で、ASAv5 の RAM 要件が 2 GB に増加しました。ASA は、割り当てられたメモリをチェックし、2 GB の RAM が ASAv5 ではなく ASAv10 であると判断していたため、この増加により、ASAv5 の永久ライセンスが機能しなくなっています。ASAv5 の永久ライセンスを機能させるために、このモデルの追加メモリを認識するように ASA を設定できます。

- 2 GB、1 vCPU：ASAv10（1G）
- 8 GB、4 vCPU：ASAv30（2G）
- 16 GB、8 vCPU：ASAv50（10G）
- 32 GB、16 vCPU：ASAv100（20G）
- 64 GB、32 vCPU：ASAvU
- 128 GB、64 vCPU：ASAvU

後でモデル レベルを変更したい場合は、現在のライセンスを返却し、変更後のモデル レベルに対応する新規ライセンスを要求する必要があります。展開済みの ASA 仮想 のモデルを変更するには、新しいモデルの要件に合わせるために、ハイパーバイザから vCPU と DRAM の設

定を変更します。これらの値については、『*ASA 仮想 Virtual Getting Started Guide*』を参照してください。

ライセンスの使用を停止した場合、ASA 仮想 で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

柔軟なパーマネント ライセンスの予約モード

ASA 仮想に割り当てられた RAM および vCPU に関係なく、モデル固有のライセンスを設定できます。

指定するモデルライセンスにより、ASA 仮想のスループットレベルが設定されます。ASA 仮想 のメモリにより、最大セキュアクライアント セッション、TLS プロキシ セッション、最大同時ファイアウォール接続数および VLAN が決定されます（モデルライセンスではありません）。ただし、ASA 仮想 メモリプロファイルを小さくすると、セッションと機能の実際の数が制限されます。

たとえば、ASA 仮想 に 8 GB の RAM があり、ASAV_50_UNIVERSAL に登録されている場合、セキュアクライアント に割り当てられる最大セッション数は 750 です。セッションがこの制限を超えると、接続はドロップされます。

永続ライセンス予約ライセンスモードのその他の利点は次のとおりです。

- ASA 仮想に割り当てられたメモリに関係なく、永続ライセンスの予約ライセンスを切り替えることができます。ただし、ASA 仮想 に 16 を超える vCPU がある場合は、ASAvU（無制限）ライセンスのみを設定できます。
- モデル ライセンスを変更せずに、ASA 仮想 に割り当てられたメモリと vCPU を変更できます。

ライセンスの使用を停止した場合、ASA 仮想 で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

永続ライセンス予約の設定の詳細については、ASA 仮想：永続ライセンス予約の設定 （144 ページ）を参照してください。

Firepower 1010 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- Security Plus
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

  セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

（注） また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 1100 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

  セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

（注） また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Secure Firewall 1210/1220 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

  セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

（注） また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Secure Firewall 1230/1240/1250 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

  セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

（注） また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Secure Firewall 3100/4200 永続ライセンスの予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層
- 最大セキュリティコンテキスト数
- キャリア ライセンス
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

  セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にするセキュアクライアントライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

（注） また、ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。

ライセンスの使用を停止した場合、ASA で戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Firepower 4100/9300 シャーシ永久ライセンス予約

すべての機能を有効にするライセンスを取得できます。

- Essentials 層。
- 最大セキュリティコンテキスト数
- キャリア ライセンス
- 高度暗号化（3DES/AES）ライセンス（アカウントが適格の場合）
- プラットフォームの上限まで有効化される セキュアクライアント の機能

  セキュアクライアント の機能を使用するには、セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入する必要があります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

（注） ライセンスは Firepower 4100/9300 シャーシ上で管理されますが、それに加えて ASA の設定で権限付与を要求することにより、ASA でそれらを使用できるようにする必要があります。ライセンスを管理するには、『FXOS 構成 ガイド』を参照します。

ライセンスの使用を停止した場合、Firepower 4100/9300 シャーシで戻りコードを生成し、そのコードを Smart Software Manager に入力して、ライセンスを返却する必要があります。使用していないライセンスの料金の支払うことのないように、返却プロセスに正確に従ってください。

Smart Software Manager オンプレミス

デバイスがセキュリティ上の理由でインターネットにアクセスできない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager オンプレミスサーバー（旧「Smart Software サテライトサーバー」）をインストールできます。Smart Software Manager オンプレミスは、Smart Software Manager の機能の一部を提供します。これにより、すべてのローカルデバイスに不可欠なライセンシングサービスを提供できます。ライセンスの使用状況を同期するためにメインの Smart Software Manager に定期的に接続する必要があるのは、Smart Software Manager オンプレミスだけです。スケジュールに沿って同期するか、または手動で同期できます。

Smart Software Manager オンプレミスでは、次の機能を実行できます。

- ライセンスの有効化または登録
- 企業ライセンスの表示
- 会社のエンティティ間でのライセンス移動

詳細については、『Cisco Smart Software Manager オンプレミスのデータ シート』を参照してください。

仮想アカウントごとに管理されるライセンスとデバイス

ライセンスとデバイスは仮想アカウントごとに管理されます。つまり、その仮想アカウントのデバイスのみが、そのアカウントに割り当てられたライセンスを使用できます。新たにライセンスを追加する必要がある場合は、別の仮想アカウントから未使用のライセンスを譲渡できます。仮想アカウント間でデバイスを転送することもできます。

Firepower 4100/9300 シャーシ 上で動作する ASA の場合：シャーシのみがデバイスとして登録される一方で、シャーシ内の ASA アプリケーションはそれぞれ固有のライセンスを要求します。たとえば、3 つのセキュリティ モジュールを搭載した Firepower 9300 シャーシでは、全シャーシが 1 つのデバイスとして登録されますが、各モジュールは合計 3 つのライセンスを別個に使用します。

評価ライセンス

ASA 仮想

ASA 仮想 は、評価モードをサポートしません。Smart Software Manager への登録の前に、ASA 仮想 は厳しいレート制限状態で動作します。

Firepower 1000

Firepower 1000 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 1000 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Firepower 2100

Firepower 2100 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 2100 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Cisco Secure Firewall 3100/4200

Cisco Secure Firewall 3100/4200 は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。デフォルトの権限のみが有効になります。この期間が終了すると、Cisco Secure Firewall 3100/4200 はコンプライアンス違反の状態になります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録する必要があります。

Firepower 4100/9300 シャーシ

Firepower 4100/9300 シャーシ は、次の 2 種類の評価ライセンスをサポートしています。

- シャーシレベル評価モード：Firepower 4100/9300 シャーシ は、Smart Software Manager への登録の前に 90 日間（合計使用時間）評価モードで動作します。このモードでは、ASA は固有の権限付与を要求できません。デフォルトの権限のみが有効になります。この期間が終了すると、Firepower 4100/9300 シャーシはコンプライアンス違反の状態になります。
- 権限付与ベースの評価モード：Firepower 4100/9300 シャーシ が Smart Software Manager に登録された後、ASA に割り当て可能な時間ベースの評価ライセンスを取得できます。ASA で、通常どおりに権限付与を要求します。時間ベースのライセンスの期限が切れると、時間ベースのライセンスを更新するか、または永続ライセンスを取得する必要があります。

（注） 高度暗号化（3DES/AES）の評価ライセンスを受け取ることはできません。高度暗号化（3DES/AES）ライセンスを有効にするエクスポートコンプライアンス トークンを受け取るには、Smart Software Manager に登録して永続ライセンスを取得する必要があります。

ライセンスについて（タイプ別）

ここでは、ライセンスに関する追加情報をタイプ別に説明します。

Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス

セキュアクライアントライセンスはASAに直接適用されません。ただし、ASAをセキュアクライアントヘッドエンドとして使用する権利を保証するには、ライセンスを購入してスマートアカウントに追加する必要があります。

- Secure Client Advantage および Secure Client Premier ライセンスの場合は、スマートアカウントのすべての ASA で使用する予定のピアの数を合計し、その多くのピア用にライセンスを購入します。
- Secure Client VPN のみの場合は、ASA ごとに 1 つのライセンスを購入します。複数の ASA で共有できるピアのプールを提供する他のライセンスとは異なり、Secure Client VPN のみライセンスはヘッドエンド単位です。

詳細については、以下を参照してください。

- Cisco セキュアクライアント 発注ガイド
- セキュアクライアント ライセンスに関するよくある質問（FAQ）

その他の VPN ピア

その他の VPN ピアには、次の VPN タイプが含まれています。

- IKEv1 を使用した IPsec リモート アクセス VPN
- IKEv1 を使用した IPsec サイトツーサイト VPN
- IKEv2 を使用した IPsec サイトツーサイト VPN

このライセンスは基本ライセンスに含まれています。

合計 VPN ピア。全タイプの合計

- 合計 VPN ピアは、セキュアクライアント とその他の VPN ピアを合算した、許可される VPN ピアの最大数となります。たとえば、合計が 1000 の場合はセキュアクライアント とその他の VPN ピアを 500 ずつ、または セキュアクライアント を 700 とその他の VPN ピア 300 を同時に許可できます。あるいは、1000 すべてを セキュアクライアント に使用することも可能です。合計VPNピアが最大数を超えた場合は、ASAをオーバーロードして、適切なネットワークのサイズに設定してください。

暗号化ライセンス

高度暗号化：ASA 仮想

Smart Software Manager または Smart Software Manager オンプレミスサーバーに接続する前に、管理接続に高度暗号化（3DES/AES）を使用できるため、ASDM を起動して Smart Software Manager に接続することが可能です。（VPN などの）高度暗号化を必要とする through-the-box

トラフィックの場合、Smart Software Manager に接続して高度暗号化ライセンスを取得するまで、スループットは厳しく制限されます。

スマート ソフトウェア ライセンシング アカウントから ASA 仮想 の登録トークンを要求する場合、[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（お使いのアカウントでその使用が許可されている必要があります）。ASA 仮想 が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA 仮想 はライセンスを保持し、レート制限状態に戻ることはありません。ASA 仮想 を再登録し、エクスポート コンプライアンスが無効になっている場合、または ASA 仮想 を工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度暗号化なしで ASA 仮想 を登録し、後で高度暗号化を追加する場合は、新しいライセンスを有効にするために ASA 仮想 をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：Firepower 1000、Cisco Secure Firewall 1200/3100/4200

ASA には、管理アクセスのみを対象にした 3DES 機能がデフォルトで含まれているので、Smart Software Manager に接続でき、すぐに ASDM を使用することもできます。後に ASA で SSH アクセスを設定する場合は、SSH および SCP を使用することもできます。高度な暗号化を必要とするその他の機能（VPN など）では、最初に Smart Software Manager に登録する必要がある高度暗号化が有効になっている必要があります。

（注） 登録する前に高度な暗号化を使用できる機能の設定を試みると（脆弱な暗号化のみ設定している場合でも）、HTTPS 接続はそのインターフェイスでドロップされ、再接続できません。このルールの例外は、管理 1/1 などの管理専用インターフェイスに接続されている場合です。SSH は影響を受けません。HTTPS 接続が失われた場合は、コンソール ポートに接続して ASA を再設定するか、管理専用インターフェイスに接続するか、または高度暗号化機能用に設定されていないインターフェイスに接続することができます。

スマート ソフトウェア ライセンシング アカウントから ASA の登録トークンを要求する場合、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにして、高度暗号化（3DES/AES）のライセンスが適用されるようにします（ご使用のアカウントでその使用が許可されている必要があります）。ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。ASA を再登録し、エクスポート コンプライアンスが無効になっていても、ライセンスは有効なままです。ASA を工場出荷時の設定に復元すると、ライセンスは削除されます。

最初に高度な暗号化なしで ASA を登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA をリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

高度暗号化：Firepower 4100/9300 シャーシ

ASA を論理デバイスとして展開すると、すぐに ASDM を起動できます。高度暗号化ライセンスに接続して取得するまで、（VPN などの）高度暗号化を必要とする through the box トラフィックは許可されません。

スマート ソフトウェア ライセンシング アカウントからシャーシの登録トークンを要求する場合、[このトークンに登録した製品でエクスポート制御機能を許可する（Allow export-controlled functionality on the products registered with this token）] チェックボックスをオンにして、高度暗号化（3DES/AES）ライセンスが適用されるようにします（お使いのアカウントでその使用が許可されている必要があります）。

ASA が後でコンプライアンス違反になった場合、エクスポート コンプライアンス トークンが正常に適用されていれば、ASA は引き続き through the box トラフィックを許可します。シャーシを再登録し、エクスポートコンプライアンスが無効になっている場合、またはシャーシを工場出荷時の設定に復元した場合、ライセンスは削除されます。

最初に高度な暗号化なしでシャーシを登録し、後で高度な暗号化を追加する場合は、新しいライセンスを有効にするために ASA アプリケーションをリロードする必要があります。

永続ライセンス予約のライセンスの場合、アカウントに使用資格があれば、高度暗号化（3DES/AES）ライセンスが有効になります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。

DES：すべてのモデル

高度暗号化を有効にしている場合、DES を使用することはできません。

キャリア ライセンス

キャリア ライセンスでは、以下のインスペクション機能が有効になります。

- Diameter：Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。
- GTP/GPRS：GPRS トンネリングプロトコルは、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS、および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変

更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザ データ パケットの伝送にもトンネリング メカニズムを使用します。

- M3UA：MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバープロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザパート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。
- CTP：SCTP（Stream Control Transmission Protocol）は RFC 4960 で説明されています。プロトコルは IP 経由のテレフォニー シグナリング プロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャにおける複数のインターフェイス用の転送プロトコルでもあります。

合計 TLS プロキシ セッション

Encrypted Voice Inspection の各 TLS プロキシ セッションは、TLS ライセンスの制限に対してカウントされます。

TLS プロキシセッションを使用するその他のアプリケーション（ライセンスが不要な Mobility Advantage Proxy など）では、TLS 制限に対してカウントしません。

アプリケーションによっては、1 つの接続に複数のセッションを使用する場合があります。たとえば、プライマリとバックアップの Cisco Unified Communications Manager を電話に設定した場合は、TLS プロキシ接続は 2 つ使用されます。

TLS プロキシの制限は、**tls-proxy maximum-sessions** コマンドまたは ASDM で [Configuration] > [Firewall] > [Unified Communications] > [TLS Proxy] ペインを使用して個別に設定できます。モデルの制限を表示するには、**tls-proxy maximum-sessions ?** コマンドを入力します。デフォルトの TLS プロキシ制限よりも高い TLS プロキシライセンスを適用する場合、ASA では、そのライセンスに一致するように TLS プロキシの制限が自動的に設定されます。ライセンスの制限よりも TLS プロキシ制限が優先されます。TLS プロキシ制限をライセンスよりも少なく設定すると、ライセンスですべてのセッションを使用できません。

（注） 「K8」で終わるライセンス製品番号（たとえばユーザー数が 250 未満のライセンス）では、TLS プロキシセッション数は 1000 までに制限されます。「K9」で終わるライセンス製品番号（たとえばユーザー数が 250 以上のライセンス）では、TLS プロキシの制限はコンフィギュレーションに依存し、モデルの制限が最大数になります。K8 と K9 は、エクスポートについてそのライセンスが制限されるかどうかを示します。K8 は制限されず、K9 は制限されます。

（たとえば **clear configure all** コマンドを使用して）コンフィギュレーションをクリアすると、TLS プロキシ制限がモデルのデフォルトに設定されます。このデフォルトがライセンスの制限よりも小さいと、**tls-proxy maximum-sessions** コマンドを使用したときに、再び制限を高めるようにエラー メッセージが表示されます（ASDM の [TLS Proxy] ペインを使用）。フェールオーバーを使用して、**write standby** コマンドを入力するか、または ASDM でプライマリ装置に対して [File] > [Save Running Configuration to Standby Unit] を使用して強制的にコンフィギュレーションの同期を行うと、セカンダリ装置で **clear configure all** コマンドが自動的に生成され、セカンダリ装置に警告メッセージが表示されることがあります。コンフィギュレーションの同期によりプライマリ装置の TLS プロキシ制限の設定が復元されるため、この警告は無視できます。

接続には、SRTP 暗号化セッションを使用する場合もあります。

- K8 ライセンスでは、SRTP セッション数は 250 までに制限されます。
- K9 ライセンスでは、制限はありません。

（注） メディアの暗号化/復号化を必要とするコールだけが、SRTP 制限に対してカウントされます。コールに対してパススルーが設定されている場合は、両方のレッグが SRTP であっても、SRTP 制限に対してカウントされません。

VLAN、最大

VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 次に例を示します。

```
interface gigabitethernet 0/0.100
vlan 100
```

ボットネット トラフィック フィルタ ライセンス

ダイナミック データベースをダウンロードするには、強力な暗号化（3DES/AES）ライセンスが必要です。

フェールオーバーまたは ASA クラスタ ライセンス

ASAv のフェールオーバー ライセンス

スタンバイ ユニットにはプライマリ ユニットと同じモデル ライセンスが必要です。

Firepower 1010 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

両方の Firepower 1010 ユニットは、Smart Software Manager または Smart Software Manager オンプレミスサーバーに登録する必要があります。フェールオーバーを設定する前に、両方のユニットでEssentialsライセンスと Security Plus ライセンスを有効にする必要があります。

通常は、ユニットの登録時に両方のユニットが強力な暗号化トークンを取得する必要があるため、ASA で強力な暗号化（3DES/AES）機能ライセンスを有効にする必要もありません。登録トークンを使用する場合、両方のユニットに同じ暗号化レベルが設定されている必要があります。

スマートアカウントで強力な暗号化が許可されていないが、強力な暗号化の使用が許可されているとシスコが判断した場合、強力な暗号化ライセンスをアカウントに手動で追加できます。この場合、フェールオーバーを有効にした後、アクティブユニットで有効にします。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブユニットのみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となり、高度暗号化トークンを使用する場合は、高度暗号化（3DES/AES）機能ライセンスを必要とする機能の設定変更を行えなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 1100 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

アクティブユニットのみサーバからライセンスを要求します。ライセンスは、フェールオーバーペアで共有される単一のフェールオーバーライセンスに集約されます。セカンダリユニットに追加費用はかかりません。

アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブフェールオーバーでは、フェールオーバーグループ1がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

（注） フェールオーバーペアを形成する場合は、各ASAに同じ暗号化ライセンスが必要です。スマート ライセンシング サーバに ASA を登録すると、高度暗号化ライセンスは、登録トークンを適用するときに、対象となるお客様の場合に自動的に有効化されます。この要件のため、フェールオーバーで高度暗号化トークンを使用する場合は、次の2つのライセンスを選択できます。

- フェールオーバーを有効にする前に、両方のユニットをスマート ライセンシング サーバに登録します。この場合、両方のユニットに高度暗号化が適用されます。次に、フェールオーバーを有効にした後、アクティブユニットでライセンス権限の設定を続行します。フェールオーバーリンクの暗号化を有効にすると、AES/3DES（高度暗号化）が使用されます。
- アクティブユニットをスマートライセンシングサーバに登録する前に、フェールオーバーを有効にします。この場合、両方のユニットに高度暗号化はまだ適用されません。次に、ライセンス権限を設定し、アクティブユニットをスマート ライセンシング サーバに登録します。両方のユニットが集約ライセンスから高度暗号化を取得します。フェールオーバーリンクで暗号化を有効にした場合、ユニットが高度暗号化を取得する前にフェールオーバーリンクが確立されているため、DES（脆弱な暗号化）が使用されます。リンクでAES/3DESを使用するには、両方のユニットをリロードする必要があります。1つのユニットだけをリロードすると、そのユニットはAES/3DESを使用しようとしますが、元のユニットはDESを使用するため、両方のユニットがアクティブになります（スプリットブレイン）。

各アドオンライセンスタイプは次のように管理されます。

- Essentials：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Essentials ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトでEssentialsライセンスには2のコンテキストが含まれ、これは両方のユニットにあります。各ユニットのEssentialsライセンスの値と、アクティブな装置のContextライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。

- アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1120 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 3 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 7 つのコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が 5 なので、結合されたライセンスでは最大 5 つのコンテキストのみ許可されます。この場合、アクティブな Context ライセンスを 1 つのコンテキストとしてのみ設定することになる場合があります。
- アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1140 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 4 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 8 つのコンテキストが含まれています。たとえば、一方のユニットが 5 コンテキストを使用し、他方が 3 コンテキストを使用しますが、障害中には 1 ユニットが 8 のすべてを使用します。ユニットごとのプラットフォームの制限が 10 なので、結合されたライセンスでは最大 10 のコンテキストが許可されます。8 コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 1210/1220 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、フェールオーバーを有効にする前に、ライセ

ンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、フェールオーバーリンクの暗号化に関する問題も発生します。

データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス構成では、Essentials ライセンスは両方のユニットで常にデフォルトで有効になっています。アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

各アドオンライセンスタイプは次のように管理されます。

- Essentials：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Secure Firewall 1210 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 5 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには9つのコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が 5 なので、結合されたライセンスでは最大 5 つのコンテキストのみ許可されます。この場合、アクティブな Context ライセンスを 1 つのコンテキストとしてのみ設定することになる場合があります。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Secure Firewall 1220 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 5 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 9 のコンテキストが含まれています。一方のユニットが 5 コンテキストを使用でき、他方が 4 コンテキストを使用できます。次に例を示します。ただし、障害発生時には、1 つのユニットですべての 9 を使用します。ユニットごとのプラットフォームの制限が 10 なので、結合されたライセンスでは最大 10 のコンテキストが許可されます。9 コンテキストは制限の範囲内です。
- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンス

をアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 1230/1240/1250 のフェールオーバー ライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、フェールオーバーを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、フェールオーバーリンクの暗号化に関する問題も発生します。

フェールオーバー機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス構成では、Essentials ライセンスは両方のユニットで常にデフォルトで有効になっています。アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

各アドオンライセンスタイプは次のように管理されます。

- Essentials：各ユニットには、サーバーからのEssentialsのライセンスが必要です。

- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Secure Firewall 1230 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 25 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 29 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 25 であるため、結合されたライセンスでは最大 25 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 21 のコンテキストのみを設定できます。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Secure Firewall 1230 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 14 のコンテキストが含まれています。たとえば、一方のユニットが 5 コンテキストを使用し、他方が 3 コンテキストを使用しますが、障害中には 1 ユニットが 8 のすべてを使用します。ユニットごとのプラットフォームの制限が 25 であるため、結合されたライセンスでは最大 25 のコンテキストが許容されます。14 コンテキストは制限の範囲内です。
- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 3100 のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、フェールオーバーを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、フェールオーバーリンクの暗号化に関する問題も発生します。

フェールオーバー機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス構成では、Essentials ライセンスは両方のユニットで常にデフォルトで有効になっています。アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

各アドオンライセンスタイプは次のように管理されます。

- Essentials：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - アクティブ/スタンバイ：Essentialsライセンスには2つのコンテキストが含まれています。2 つの Secure Firewall 3130 ユニットの場合、それらのライセンスで最大 4 つのコンテキストが追加されます。アクティブ/スタンバイペアのアクティブな装置に 100 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには104のコンテキストが含まれています。ただし、ユニットごとのプラットフォームの制限が 100 であるため、結合されたライセンスでは最大 100 のコンテキストのみが許容されます。この場合では、アクティブな Context ライセンスとして 95 のコンテキストのみを設定できます。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Firepower 1140 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに10Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには14のコンテキストが含まれています。たとえば、一方のユニットが 5 コンテキストを使用し、他方が 3 コンテキストを使用しますが、障害中には 1 ユニットが 8 のすべてを使用します。ユニットごとのプラットフォームの制限が 100 であるため、結合された

ライセンスでは最大100のコンテキストが許容されます。14 コンテキストは制限の範囲内です。

- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 4200 のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、フェールオーバーを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、フェールオーバーリンクの暗号化に関する問題も発生します。

フェールオーバー機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス構成では、Essentials ライセンスは両方のユニットで常にデフォルトで有効になっています。アクティブ/スタンバイフェールオーバーのフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイユニットに複製されますが、スタンバイユニットは設定を使用しません。この設定はキャッシュの状態のままになります。集

約されたライセンスは、スタンバイユニットにキャッシュされ、将来アクティブユニットになる場合に使用されます。

各アドオンライセンスタイプは次のように管理されます。

- Essentials：各ユニットがサーバから標Essentials準ライセンスを要求します。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには 2 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Secure Firewall 4215 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/スタンバイペアのアクティブな装置に 250 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 254 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 246 のコンテキストのみを設定できます。
  - アクティブ/スタンバイ：Essentials ライセンスには 2 つのコンテキストが含まれています。2 つの Secure Firewall 4215 ユニットの場合、これらのライセンスは最大 4 つのコンテキストを追加します。アクティブ/アクティブペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 14 のコンテキストが含まれています。たとえば、一方のユニットが 9 コンテキストを使用し、他方が 5 コンテキストを使用しますが、障害中には 1 ユニットが 14 のすべてを使用します。ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。14 コンテキストは制限の範囲内です。
- 高度な暗号化（3DES/AES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更（つまり、追加コンテキストの追加）を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300のフェールオーバーライセンス

Smart Software Manager Regular およびオンプレミス

フェールオーバーを設定する前に、両方の Firepower 4100/9300 は、Smart Software Manager または Smart Software Manager オンプレミスサーバーに登録する必要があります。セカンダリ ユニットに追加費用はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

アクティブ/スタンバイフェールオーバーの ASA ライセンス設定のフェールオーバーを有効にした後は、アクティブユニットにのみスマートライセンシングを設定できます。アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブになっている装置にのみスマートライセンシングを設定できます。設定はスタンバイ ユニットに複製されますが、スタンバイ ユニットは設定を使用しません。この設定はキャッシュの状態のままになります。アクティブな装置のみサーバーからライセンスを要求します。ライセンスは単一のフェールオーバーライセンスにまとめられ、フェールオーバーのペアで共有されます。この集約ライセンスはスタンバイ ユニットにもキャッシュされ、将来アクティブなユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Essentials：アクティブな装置のみがサーバにこのライセンスを要求しますが、スタンバイ装置にはデフォルトで有効になっている Essentials ライセンスがあります。その使用のためにサーバに登録を行う必要はありません。
- Context：このライセンスはアクティブな装置のみが要求します。ただし、デフォルトで Essentials ライセンスには 10 のコンテキストが含まれ、これは両方のユニットにあります。各ユニットの Essentials ライセンスの値と、アクティブな装置の Context ライセンスの値はプラットフォームの上限まで加算されます。次に例を示します。
  - アクティブ/スタンバイ：Essentialsライセンスは 10 のコンテキストを含みます。2 つユニットの場合、合計で 20 のコンテキストが加算されます。アクティブ/スタンバイ ペアのアクティブな装置に 250 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 270 のコンテキストが含まれています。しかし、ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。この場合では、アクティブな Context ライセンスとして 230 コンテキストを設定する必要があります。
  - アクティブ/スタンバイ：Essentialsライセンスは 10 のコンテキストを含みます。2 つユニットの場合、合計で 20 のコンテキストが加算されます。アクティブ/アクティブ ペアのプライマリユニットに 10 Context ライセンスを設定します。この場合、集約されたフェールオーバーライセンスには 30 のコンテキストが含まれています。たとえば、一方のユニットが 17 コンテキストを使用し、他方が 13 コンテキストを使用しま

すが、障害中には 1 ユニットが 30 のすべてを使用します。ユニットごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。30 コンテキストは制限の範囲内です。

- キャリア：アクティブのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

フェールオーバーの後には、新しいアクティブ装置は集約ライセンスを引き続き使用します。キャッシュされたライセンス設定を使用し、サーバーに権限付与を再要求します。古いアクティブ装置がペアにスタンバイとして参加した場合、ライセンス権限を解放します。アカウントに充分なライセンスがない場合、スタンバイ装置が権限を解放する前に、新しいアクティブ装置のライセンスがコンプライアンス違反状態になることがあります。フェールオーバーのペアは集約ライセンスを 30 日間使用できますが、この猶予期間以降もコンプライアンス違反となる場合は、特殊なライセンスを必要とする機能の設定変更を行なえなくなります。動作には影響しません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで35秒ごとに権限承認更新要求を送信します。フェールオーバーのペアを解消した場合は、アクティブな装置は権限を解放し、両方のユニットはライセンス設定をキャッシュ状態にして保持します。ライセンスを再アクティベートするには、各ユニットの設定をクリアし、再設定する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、フェールオーバーを設定する前にライセンスを有効にする必要があります。

Secure Firewall 3100 の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、Essentialsライセンスはすべてのユニットで常にデフォルトで有効になっています。制御ユニットにのみスマートライセンスを設定できます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しませ

ん。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Essentials：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは2のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタ内に 6 つの Secure Firewall 3100 があります。Essentialsライセンスは 2 のコンテキストを含みます。6ユニットの場合、合計で12のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは32のコンテキストを含みます。シャーシごとのプラットフォームの制限が 100 であるため、結合されたライセンスでは最大 100 のコンテキストが許容されます。32コンテキストは制限の範囲内です。したがって、制御ユニット上で最大32コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して 32 コンテキストを持つことになります。
  - クラスタ内に 3 つの Secure Firewall 3100 があります。Essentialsライセンスは 2 のコンテキストを含みます。3 ユニットの場合、合計で 6 のコンテキストが加算されます。制御ユニット上で追加の 100 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 106 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 100 であるため、統合されたライセンスでは最大 100 のコンテキストが許容されます。106 コンテキストは制限を超えています。したがって、制御ユニット上で最大100のコンテキストのみを設定できます。各データユニットも、設定の複製を介して100のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして 94 のコンテキストのみを設定する必要があります。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。ライセンス要求

が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

Secure Firewall 4200 の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、Essentialsライセンスはすべてのユニットで常にデフォルトで有効になっています。制御ユニットにのみスマートライセンスを設定できます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の1つが将来制御ユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Essentials：各ユニットには、サーバーからのEssentialsのライセンスが必要です。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは2のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタ内に 6 つの Secure Firewall 4200 があります。Essentialsライセンスは 2 のコンテキストを含みます。6ユニットの場合、合計で12のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは32のコンテキストを含みます。シャーシごとのプラットフォームの制限が 250 であるため、結合されたライセンスでは最大 250 のコンテキストが許容されます。32コンテキストは制限の範囲内です。したがって、制御ユニット上で最大32コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して 32 コンテキストを持つことになります。

- クラスタ内に 3 つの Secure Firewall 4200 があります。Essentialsライセンスは 2 のコンテキストを含みます。3 ユニットの場合、合計で 6 のコンテキストが加算されます。制御ユニット上で追加の 250 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 256 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大 250 のコンテキストが許容されます。256 コンテキストは制限を超えています。したがって、制御ユニット上で最大 250 のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して 250 のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして 244 のコンテキストのみを設定する必要があります。

- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

ASAv の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、同じスループットライセンスと同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます:

- Essentials：制御ユニットのみがサーバーからEssentialsライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。
- スループット：各ユニットには、サーバからの各自のスループットライセンスが必要です。
- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

永続ライセンスの予約

永続ライセンスを予約するには、ユニットごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

Firepower 4100/9300 の ASA クラスタライセンス

Smart Software Manager Regular およびオンプレミス

クラスタリング機能自体にライセンスは必要ありません。強力な暗号化およびその他のオプションのライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシ がライセンス機関または Smart Software Manager の通常およびオンプレミスサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンスタイプは次のように処理されます:

- Essentials：制御ユニットのみがサーバーからEssentialsライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは10のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタに 6 台の Firepower9300 モジュールがある場合を考えます。Essentialsライセンスは 10 のコンテキストを含みます。6 つユニットの場合、合計で 60 のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 80 のコンテキストを含みます。モジュールごとのプラットフォーム制限は250であるため、統合されたライセンスに最大250のコンテキストが許容されます。80のコンテキストは制限範囲内です。したがって、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して80コンテキストを持つことになります。
  - クラスタに Firepower 4112 が 3 台あるとします。Essentialsライセンスは 10 のコンテキストを含みます。3つユニットの場合、合計で30のコンテキストが加算されます。制御ユニット上で追加の250コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 280 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大 250 のコンテキストが許容されます。280 コンテキストは制限を超えています。したがって、制御ユニット上で最大250のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して250のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして220のコンテキストのみを設定する必要があります。
- キャリア：分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- 高度な暗号化（3DES）：2.3.0 以前の Cisco Smart Software Manager オンプレミス展開の場合。またはスマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されていると Cisco が判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセン

ス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

スマート ソフトウェア ライセンスの前提条件

Smart Software Manager 定期およびオンプレミスの前提条件

Firepower 4100/9300

ASA ライセンス資格を設定する前に、Firepower 4100/9300 シャーシでスマート ソフトウェア ライセンス インフラストラクチャを設定します。

他のすべてのモデル

- デバイスからのインターネットアクセス、HTTP プロキシアクセス、Smart Software Manager オンプレミスサーバーへのアクセスを確保します。
- デバイスが Smart Software Manager の名前を解決できるように DNS サーバーを設定します。
- デバイスのクロックを設定します。
- Cisco Smart Software Manager でアカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のアカウントを作成できます。

永続ライセンス予約の前提条件

- Cisco Smart Software Manager でマスター アカウントを作成します。

  https://software.cisco.com/#module/SmartLicensing

  まだアカウントをお持ちでない場合は、リンクをクリックして新しいアカウントを設定してください。Smart Software Manager では、組織のマスター アカウントを作成できます。永続ライセンス予約には ASA からスマートライセンスサーバーへのインターネット接続が必要ですが、永続ライセンスの管理には Smart Software Manager が使用されます。

- 永続ライセンス予約のサポートはライセンスチームから受けられます。永続ライセンス予約を使用する理由を示す必要があります。アカウントが承認されていない場合、永続ライセンスを購入して適用することはできません。
- 専用の永続ライセンスを購入します（モデルごとのライセンス PID （188 ページ）を参照）。アカウントに正しいライセンスがない場合、ASA でライセンスを予約しようとすると、「The licenses cannot be reserved because the Virtual Account does not contain a sufficient surplus of the following perpetual licenses: 1 - Firepower 4100 ASA PERM UNIV(perpetual)」のようなエラーメッセージが表示されます。
- 永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（「Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）」を参照）。
- ASA 仮想：永続ライセンスの予約は Azure ハイパーバイザではサポートされません。

スマート ソフトウェア ライセンスのガイドライン

- スマート ソフトウェア ライセンスのみがサポートされます。ASA 仮想 の古いソフトウェアについては、PAK ライセンスが供与された既存の ASA 仮想 をアップグレードする場合、前にインストールしたアクティベーションキーは無視されますが、デバイスに保持されます。ASA 仮想をダウングレードする場合は、アクティベーションキーが復活します。
- 永続ライセンスの予約については、デバイスを廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しいデバイスに再使用できません。
- Cisco Transport Gateway は非準拠の国番号の証明書を使用するため、ASA をその製品と組み合わせて使用する場合は HTTPS を使用できません。Cisco Transport Gateway で HTTP を使用する必要があります。

スマート ソフトウェア ライセンスのデフォルト

スマート転送

デフォルトでは、すべてのデバイスモデルがスマート ソフトウェア ライセンス通信に Smart Transport を使用し、次の URL を使用します。

```
https://smartreceiver.cisco.com/licservice/license
```

Firepower 4100/9300 では、シャーシレベルでスマート ソフトウェア ライセンスの通信を有効にする必要があります。

ASA 仮想

- ASA 仮想 を展開するときに、機能層とスループットレベルを設定します。現時点では、標準レベルのみを使用できます。Essentials永続ライセンス予約の場合、これらのパラメータを設定する必要はありません。永続ライセンス予約を有効にすると、これらのコマンドはコンフィギュレーションから削除されます。

（注） Essentials ライセンスは以前は標準ライセンスと呼ばれていました。CLI では引き続き「標準」という用語が使用されています。

```
license smart
  feature tier standard
  throughput level {100M | 1G | 2G | 10G | 20G | unlimited}
```

（注） VMware または KVM で 32 または 64 コア展開を使用している場合は、 **throughput level** コマンドで使用できるのは **unlimited** オプションのみです。

ASA 仮想：スマート ソフトウェア ライセンスの設定

このセクションでは、ASA 仮想 にスマート ソフトウェア ライセンスを設定する方法を説明します。

ASA 仮想：定期スマート ソフトウェア ライセンシングの設定

ASA 仮想 を展開する場合は、デバイスを事前に設定し、Smart Software Manager に登録するために登録トークンを適用して、スマート ソフトウェア ライセンシングを有効にできます。HTTP プロキシサーバー、ライセンス権限付与を変更する必要がある場合、または ASA 仮想 を登録する必要がある場合（Day0 設定に ID トークンを含めなかった場合など）は、このタスクを実行します。

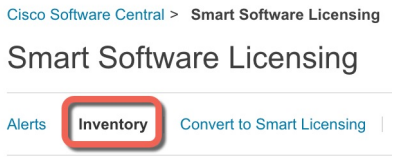
（注） ASA 仮想 を展開したときに、HTTP プロキシとライセンス権限付与が事前に設定されている可能性があります。また、ASA 仮想 を展開したときに Day0 設定で登録トークンが含まれている可能性があります。その場合は、この手順を使用して再登録する必要はありません。

手順

ステップ 1 （Cisco Smart Software Manager）で、このデバイスを追加するバーチャルアカウントの登録トークンを要求してコピーします。

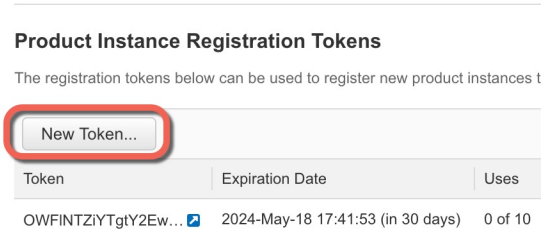
a) [Inventory] をクリックします。

図 *8*：インベントリ



b) [General] タブで、[New Token] をクリックします。

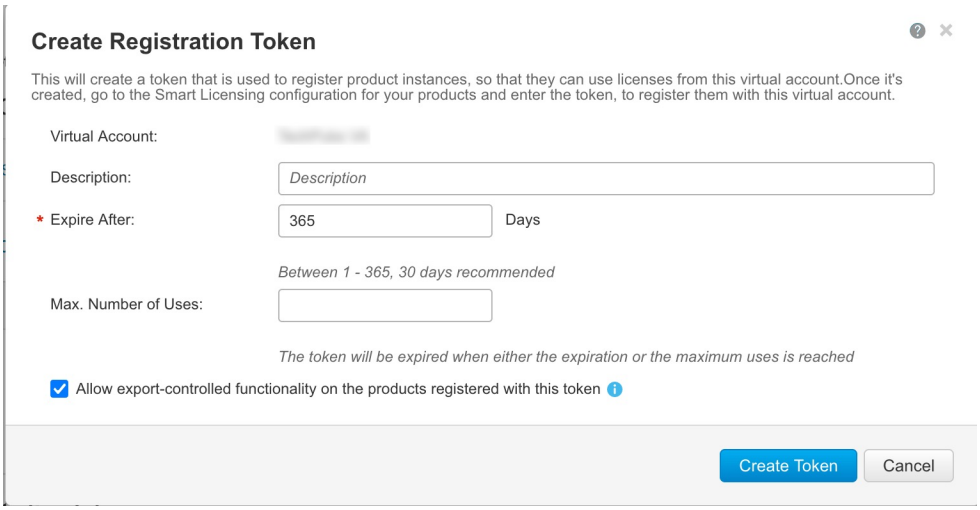
図 *9*：新しいトークン



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

- **説明**
- [有効期限（Expire After）]：推奨値は 30 日です。
- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

図 *10* : 登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *11* : トークンの表示

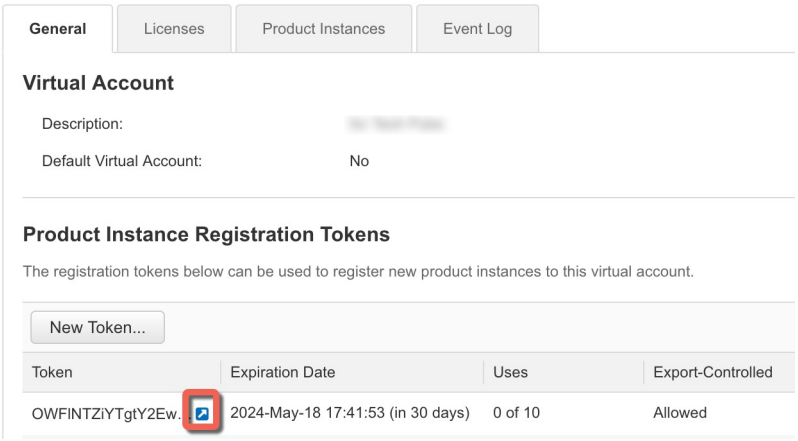
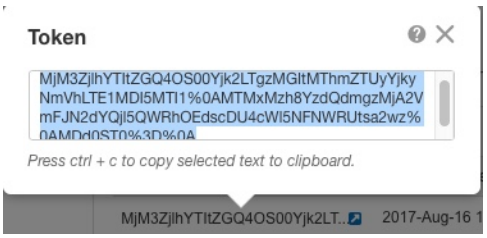


図 *12* : トークンのコピー



ステップ 2 （任意） ASA 仮想で、スマートトランスポートの HTTP プロキシ URL を指定します。

license smart

transport proxy *proxy_server_ip* **port** *port*

スマートトランスポートの代わりに Smart Call Home を使用するには、ステップ 4 （130 ページ）を参照してください。

（注）
- 認証を使用する HTTP プロキシはサポートされません。
- プロキシサーバーの URL を設定する場合は、プロトコルを指定しないでください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

ステップ 3 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。

c) Smart Software Manager から要求されるライセンスを決定するスループットレベルを設定します。

throughput level {**100M** | **1G** | **2G** | **10G** | **20G** | **unlimited**}

（注）
32 コアまたは 64 コアの展開を使用している場合は、**無制限の** オプションのみを使用できます。

次のスループットとライセンスの関係を参照してください。

- 100M：ASAv5

- 1G：ASAv10
- 2G：ASAv30
- 10G：ASAv50
- 20G：ASAv100
- [無制限（unlimited）]：ASAvU

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

a) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する（**exit** または **end**）か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 4 （任意） スマート ライセンス サーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトのスマートトランスポートを使用する必要があります。

a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する**ライセンス**と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （任意） HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

（注）
認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 5 Smart Software Manager で ASA 仮想 を登録します。

license smart register idtoken *id_token* [**force**]

ASA 仮想 が、Smart Software Manager への登録と設定されたライセンス権限付与の承認要求を試行します。

ASA 仮想 を登録すると、Smart Software Manager は ASA 仮想 と Smart Software Manager 間の通信用の ID 証明書を発行します。また、ASA 仮想 が該当する仮想アカウントに割り当てられます。通常、この手順は 1 回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、ASA 仮想 の再登録が必要になります。

force キーワードを使用して、Smart Software Manager と同期されていない可能性がある登録済みの ASA 仮想 を登録します。たとえば、Smart Software Manager から誤って ASA 仮想 を削除した場合に **force** を使用します。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ステップ 6 ライセンスのステータスを確認します。

show license status または **show running-config license**

Smart Software Manager との通信に失敗した場合は、DNS サーバーが設定されていることと、サーバーに到達するための正しいルーティングがあることを確認します。

例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Supported
  VRF:
    Not Supported

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 27 2024 06:34:02 UTC
    Failure reason: {"token":["The token 'sgdgdsdg' is not valid."]}

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>

Device Telemetry Report Summary:
================================
Data Channel: NOT AVAILABLE
Reports on disk: 0
```

例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

ASA 仮想：Smart Software Manager オンプレミスライセンシングの設定

この手順は、Smart Software Manager オンプレミスを使用する ASA 仮想 に適用されます。

始める前に

- Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、『*Cisco Smart Software Manager On-Prem Data Sheet*』を参照してください。
- バージョン 7.0 では、スマート トランスポートが Smart Software Manager オンプレミスに追加されました。これより古いバージョンを使用する場合、この手順に従って、 ASA 仮想 で Smart Call Home を有効にします。
- デバイスをエアギャップ ネットワークに配置する前に、クリプト CA トラストプールをダウンロードする。このトラストプールは通常、自動的にダウンロードされますが、エアギャップ ネットワークでは失効している可能性があります。

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

手順

ステップ 1 Smart Software Manager オンプレミスで登録トークンを要求します。

ステップ 2 （任意） ASA 仮想 で、スマートトランスポートの HTTP プロキシ URL を指定します。

license smart

transport proxy *proxy_server_ip* **port** *port*

スマート トランスポートの代わりに Smart Call Home を使用するには、 ステップ 5 （135 ページ）を参照してください。

（注）
認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

ステップ 3 ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

license smart

transport url https://*on-prem_ip_address***/SmartTransport**

スマートトランスポートの代わりに Smart Call Home を使用するには、 ステップ 5 （135 ページ）を参照してください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

ステップ 4 ライセンス権限付与を設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) 機能層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。**標準**は引き続き CLI で使用されています。

c) Smart Software Manager から要求されるライセンスを決定するスループットレベルを設定します。

throughput level {**100M** | **1G** | **2G** | **10G** | **20G** | **unlimited**}

（注）
32 コアまたは 64 コアの展開を使用している場合は、**無制限の** オプションのみを使用できます。

次のスループットとライセンスの関係を参照してください。

- 100M：ASAv5
- 1G：ASAv10
- 2G：ASAv30
- 10G：ASAv50
- 20G：ASAv100
- [無制限（unlimited）]：ASAvU

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

d) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

a) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する（**exit** または **end**）か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 5 （任意） スマート ライセンス サーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトのスマート トランスポートを使用する必要があります。

a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する**ライセンス**と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （任意） HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

（注）
認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

c) ライセンス サーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

call-home

profile License

destination address http
https://*on-prem_ip_address***/Transportgateway/services/DeviceRequestHandler**

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

ステップ 6 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

ASA が Smart Software Manager オンプレミスに登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager オンプレミスは、お使いのアカウントで許可すれば高度暗号化（3DES/AES）ライセンスも適用します。

ASA 仮想 を登録すると、Smart Software Manager オンプレミスは ASA 仮想 と Smart Software Manager 間の通信用の ID 証明書を発行します。また、ASA 仮想 が該当する仮想アカウントに割り当てられます。通常、この手順は1回限りのインスタンスです。ただし、通信の問題などが原因で ID 証明書の期限が切れた場合は、ASA 仮想 の再登録が必要になります。

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ステップ 7 ライセンスのステータスを確認します。

show license status

Smart Software Manager との通信に失敗した場合は、DNS サーバーが設定されていることと、サーバーに到達するための正しいルーティングがあることを確認します。

例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://10.1.5.5/SmartTransport
  Proxy:
    Not Supported
  VRF:
    Not Supported

Registration:
  Status: UNREGISTERED - REGISTRATION FAILED
  Export-Controlled Functionality: NOT ALLOWED
  Initial Registration: FAILED on Feb 27 2024 06:34:02 UTC
    Failure reason: {"token":["The token 'sgdgdsdg' is not valid."]}

License Authorization:
  Status: No Licenses in Use

Export Authorization Key:
  Features Authorized:
    <none>

Miscellaneous:
  Custom Id: <empty>

Device Telemetry Report Summary:
================================
Data Channel: NOT AVAILABLE
Reports on disk: 0
```

ASA 仮想：ユーティリティ（MSLA）スマート ソフトウェア ライセンシングの設定

マネージド サービス ライセンス契約（MSLA）のユーティリティ ライセンシングでは、ライセンス サブスクリプションまたは永久的ライセンスの 1 回かぎりの料金を支払うのではなく、ライセンスの使用時間に応じて支払うことができます。ユーティリティ ライセンシング モードでは、ASA 仮想 がライセンスの使用状況を時間単位（15 分間隔）で追跡します。ASA 仮想 は、Smart Software Manager に 4 時間ごとにライセンス使用状況レポート（「RUM レポート」と呼ばれます）を送信します。その後、使用状況レポートは、課金サーバーに転送されます。ユーティリティ ライセンシングでは、Smart Call Home は、ライセンシングメッセージのトランスポートとして使用されません。代わりに、メッセージが、スマートトランスポートを使用して HTTP/HTTPS 経由で直接送信されます。

始める前に

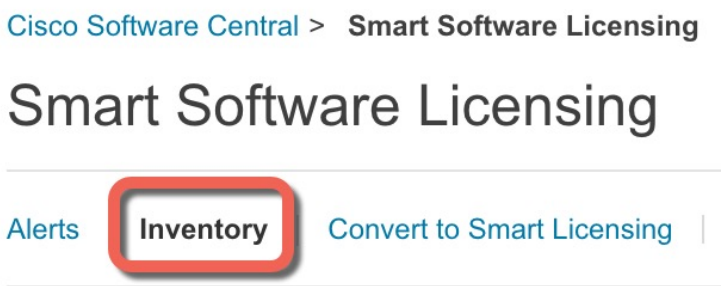
Smart Software Manager オンプレミスを使用している場合は、Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、『*Cisco Smart Software Manager On-Prem Data Sheet*』を参照してください。

手順

ステップ 1 Smart Software Manager（Cisco Smart Software Manager）で、このデバイスを追加するバーチャル アカウントの登録トークンを要求してコピーします。

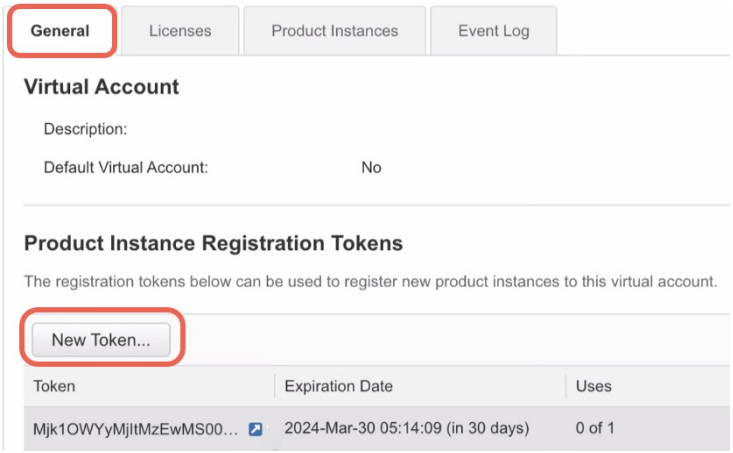
a) [Inventory] をクリックします。

図 *13*：インベントリ



b) [General] タブで、[New Token] をクリックします。

図 *14*：新しいトークン



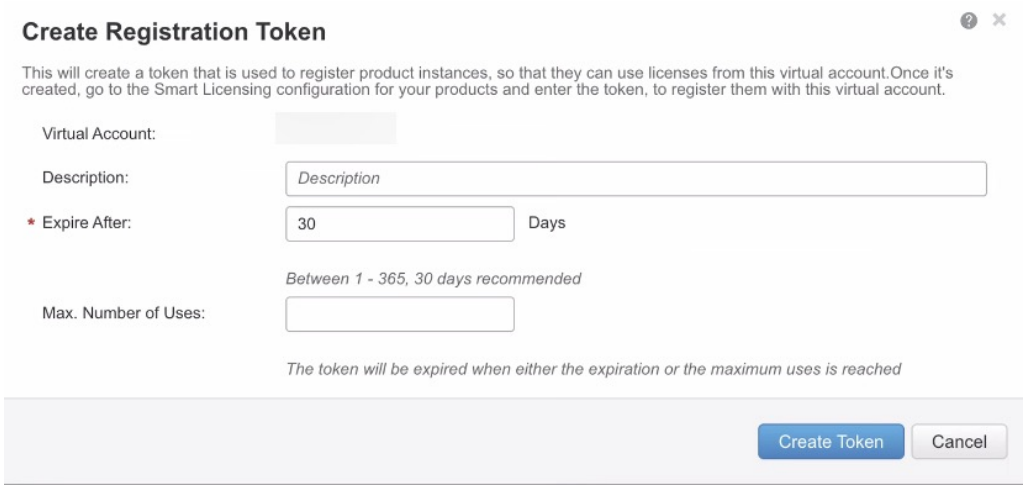
c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。

- 説明

- [有効期限（Expire After）]：推奨値は 30 日です。
- **[最大使用数]**：トークンの最大使用数。

  トークンは、有効期限または最大使用回数で期限切れになります。

図 *15*：登録トークンの作成



トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *16*：トークンの表示

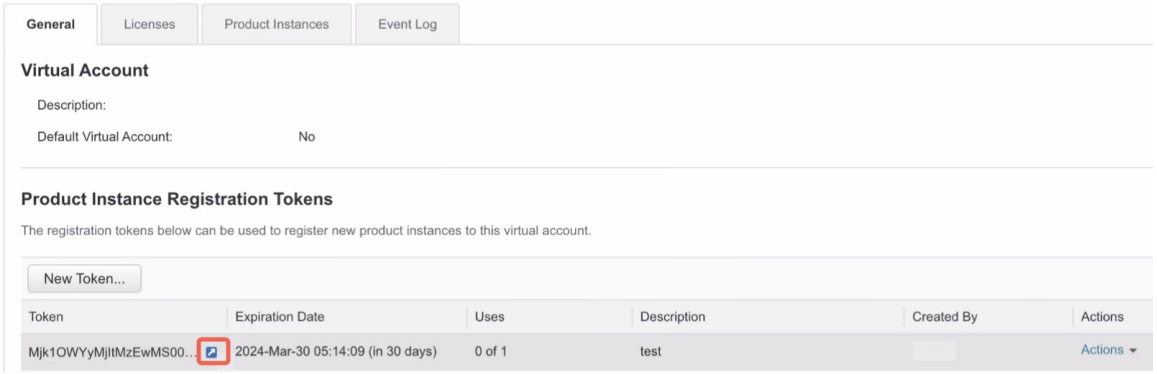
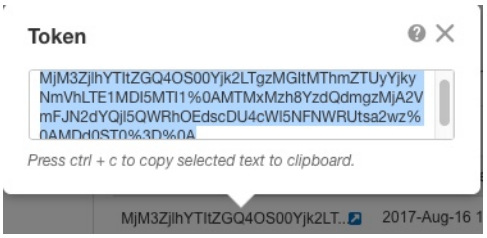


図 *17:* トークンのコピー



ステップ 2 ASA 仮想 で、スマート ライセンシングのパラメータを設定します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) スマートトランスポートを有効にします。

transport type smart

ユーティリティ ライセンシングには、Smart Call Home ではなくスマートトランスポートが必要です。

例：

```
ciscoasa(config-smart-lic)# transport type smart
```

c) （任意） Smart Software Manager 定期またはオンプレミスの URL を指定します。必要に応じて、ライセンス使用状況レポートの代替宛先を指定できます。

transport url {*transport_url* | **utility** *utility_url* | **default** }

URL を設定しない場合、スマートトランスポートとライセンス使用状況レポートの両方に **default** が使用されます。これは、**https://smartreceiver.cisco.com/licservice/license** です。

例：

```
ciscoasa(config-smart-lic)# transport url http://server99.cisco.com/SmartTransport
ciscoasa(config-smart-lic)# transport url utility
http://server-utility.cisco.com/SmartTransport
```

d) （任意） ネットワークでインターネットアクセスに HTTP プロキシを使用する場合は、プロキシアドレスを設定します。

transport proxy *proxy-url* **port** *proxy-port-number*

（注）
認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 443
```

e) ライセンスメッセージでライセンスデバイスのホスト名または Smart Agent バージョン番号を抑制します。

privacy {**all** | **hostname** | **version**}

例：

```
ciscoasa(config-smart-lic)# privacy all
```

f) 機能層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。Essentials ライセンスは、以前は**標準**ライセンスと呼ばれていました。

g) Smart Software Manager から要求されるライセンスを決定するスループットレベルを設定します。

throughput level {**100M** | **1G** | **2G** | **10G** | **20G** | **unlimited**}

（注）
32 コアまたは 64 コアの展開を使用している場合は、 **無制限の** オプションのみを使用できます。

次のスループットとライセンスの関係を参照してください。

- 100M：ASAv5
- 1G：ASAv10
- 2G：ASAv30
- 10G：ASAv50
- 20G：ASAv100
- [無制限（unlimited）]：ASAvU

例：

```
ciscoasa(config-smart-lic)# throughput level 2G
```

h) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウ

ントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

i) ライセンス スマート モードを終了して、変更を適用します。

exit

明示的にモードを終了する（**exit** または **end**）か、別のモードに移行するコマンドを入力することによってライセンス スマート コンフィギュレーション モードを終了するまで、変更が有効になりません。

例：

```
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

ステップ 3 ユーティリティ ライセンシングを設定します。

a) ユーティリティ コンフィギュレーション モードを開始します。

utility

例：

```
ciscoasa(config-smart-lic)# utility
ciscoasa(config-smart-lic-util)#
```

b) 一意の顧客 ID を作成します。この ID は、Utility Licensing 使用状況レポートメッセージに含まれます。

custom-id *custom-identifier*

例：

```
ciscoasa(config-smart-lic-util)# custom-id MyCustomID
```

c) 一意の顧客プロファイルを作成します。この情報は、Utility Licensing 使用状況レポートに含まれます。

customer-info {**city** | **country** | **id** | **name** | **postalcode** | **state** |**street**} *value*

例：

```
ciscoasa(config-smart-lic-util)# customer-info city MyCity
ciscoasa(config-smart-lic-util)# customer-info country MyCountry
ciscoasa(config-smart-lic-util)# customer-info id MyID
ciscoasa(config-smart-lic-util)# customer-info name MyName
ciscoasa(config-smart-lic-util)# customer-info postalcode MyPostalCode
ciscoasa(config-smart-lic-util)# customer-info state MyState
```

```
ciscoasa(config-smart-lic-util)# customer-info street MyStreet
```

d) ユーティリティ ライセンシングを有効にします。

mode standard

例：

```
ciscoasa(config-smart-lic-util)# mode standard
```

ステップ 4 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ステップ 5 ライセンスのステータスを確認します。

show license status

Smart Software Manager との通信に失敗した場合は、DNS サーバーが設定されていることと、サーバーに到達するための正しいルーティングがあることを確認します。

例：

```
asav1# show license status

Smart Licensing is ENABLED

Utility:
  Status: ENABLED
  Utility report:
    Last success: May 14 2018 21:37:25 UTC
    Last attempt: SUCCEEDED on May 14 2018 21:37:24 UTC
    Next attempt: May 15 2018 01:37:24 UTC

  Customer Information:
    Id: MyID
    Name: MyName
    Street: MyStreet
    City: MyCity
    State: MyState
    Country: MyCountry
    Postal Code: MyPostalCode

Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Smart
  Registration URL: http://server99.cisco.com/SmartTransport
  Utility URL: http://server-utility.cisco.com/SmartTransport
```

```
Registration:
  Status: REGISTERED
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on May 14 2018 21:37:20 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Sep 13 2018 13:34:40 UTC
  Registration Expires: May 14 2019 21:29:20 UTC

License Authorization:
  Status: AUTHORIZED on May 14 2018 21:37:22 UTC
  Last Communication Attempt: NOT STARTED
    Failure reason: Device in Thirdparty Utility Mode
  Next Communication Attempt: None
  Communication Deadline: Aug 12 2018 21:37:24 UTC
```

ASA 仮想：永続ライセンス予約の設定

ASA 仮想 に永続ライセンスを割り当てることができます。このセクションでは、ASA 仮想 の廃止やモデル層の変更などによって新しいライセンスが必要となった場合に、ライセンスを返却する方法についても説明します。

手順

ステップ 1 ASA 仮想 永続ライセンスのインストール （144 ページ）

ステップ 2 （オプション）ASA 仮想 の永続ライセンスの返却 （149 ページ）

ASA 仮想 永続ライセンスのインストール

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。ASA 仮想ASA 仮想 永続ライセンス予約の詳細については、 ASA Virtual 永久ライセンス予約 （95 ページ）を参照してください。

（注）

- 永続ライセンスの予約については、ASA 仮想 を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しいASA仮想に再使用できません。（オプション）ASA 仮想 の永続ライセンスの返却 （149 ページ）を参照してください。
- 永久ライセンスをインストールした後に設定をクリアした場合（**write erase** コマンドを使用するなど）、、引数を指定せずに **license smart reservation** コマンドを使用して永久ライセンスの予約を再度有効にする必要があります。この場合、この手順の残りの部分を完了する必要はありません。

始める前に

- 永続ライセンスを購入すると、Smart Software Manager でそれらのライセンスを使用できます。すべてのアカウントが永続ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。
- ASA 仮想の起動後に永続ライセンスを要求します。Day 0 設定の一部として永続ライセンスをインストールすることはできません。

手順

ステップ 1 （ASAv5 のみ、柔軟ではないライセンシング）DRAM が 2 GB（9.13 以降で必要な最小容量）の場合に ASAv5 永久ライセンスの使用を許可します。

license smart set_plr5

ステップ 2 （オプション）次のコマンドを実行して、RAM および vCPU に関係なく、永続ライセンスの予約を手動で設定します（フレキシブル永続ライセンス予約モード）。

license smart flex-model {**asav5_plr** | **asav10_plr** | **asav30_plr** | **asav50_plr** | **asav100_plr** | **asavu_plr**}

（注）
ASA 仮想 に 16 を超える vCPU がある場合は、ASAvU（無制限）ライセンスのみを設定できます。

柔軟な永続ライセンスの予約を無効にするには、[**no license smart reservation** コマンドを使用して永続ライセンスの予約モードを無効にした後、このコマンドの **no** 形式を使用します。

柔軟な永続ライセンス予約モードでは、ライセンス予約を有効にする前に任意の数で権限を変更できます。ライセンス予約を有効にした後に権限を変更するには、永続ライセンスの予約を無効にし、新しい権限で有効にしてから、ライセンス予約を有効にする必要があります。

たとえば、 ASA 仮想 に ASAv30 の権限があり、永続ライセンスの予約が有効になっているとします。

```
asav1# license smart flex-model asav30_plr
asav1# license smart reservation
```

ここで、権限付与を ASAv50 に変更すると、エラーが発生します。

```
asav1# license smart flex-model asav50_plr
ERROR: Flexible PLR CLI is disabled when license reservation is enabled
```

権限付与を ASAv50 に変更するには、次のコマンドを実行する必要があります。

```
asav1# no license smart reservation
asav1# license smart flex-model asav50_plr
asav1# license smart reservation
```

ステップ 3 ASA 仮想 CLI で、永続ライセンスの予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

通常のスマート ライセンスを使用するには、このコマンド を再入力する必要はありません。

ステップ 4 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa#
```

フレキシブル ライセンスの場合：モデルライセンスを変更せずに、ASA Virtual に割り当てられたメモリと vCPU を変更できます。

非柔軟なライセンスの場合：メモリまたはvCPUを変更する場合は、現在のライセンスを返却し、新しいモデルレベルで新しいライセンスを要求する必要があります。要求されたライセンスは、インストールされているメモリと vCPU と一致する必要があります。ASA 仮想 永続ライセンス予約の vCPU およびメモリとライセンス間のマトリックスの詳細については、ASA Virtual 永久ライセンス予約 （95 ページ）「[] 」を参照してください。

展開済みの ASA 仮想 のモデルを変更するには、新しいモデルの要件に合わせるために、ハイパーバイザから vCPU と DRAM の設定を変更します。各値については、ASA 仮想 のクイックスタートガイドを参照してください。現在のモデルを表示するには、**show vm** コマンドを使用します。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネントライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA 仮想 にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。（オプション）ASA 仮想 の永続ライセンスの返却 （149 ページ）を参照してください。

ステップ 5 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 6 **[ライセンス予約（License Reservation）]**をクリックし、**[予約要求コード（Reservation Request Code）]** フィールドに ASA 仮想 コードを入力します。

ステップ 7 **[次へ（Next）]** をクリックします。

[予約するライセンス（Licenses to Reserve）]の下に表示される永続ライセンスの予約資格を確認します。これは、ステップ 2で設定した権限付与である必要があります。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 情報を確認し、[承認コードの生成（Generate Authorization Code）] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

ステップ 10 [閉じる（Close）] をクリックします。

ステップ 11 ASA 仮想 CLI から、次のコマンドを実行し、承認コードを入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
INFO: ASAv platform license state is Licensed.
ciscoasa#
```

これで、ASA 仮想 ライセンスが完全に適用されました。

ステップ 12 コマンドを実行して実行設定をスタートアップ設定に保存して、再起動中の設定の損失を避けます。

write memory

ステップ 13 ライセンスのステータスと権限付与の制限を確認します。

- **show license all**

```
asav1# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: ALLOWED
  Initial Registration: SUCCEEDED on Nov 12 2024 06:40:36 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Nov 12 2024 06:27:23 UTC

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
```

```
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Smart
  URL: https://smartreceiver.cisco.com/licservice/license
  Proxy:
    Not Supported
  VRF:
    Not Supported

Miscellaneous:
  Custom Id: <empty>

License Usage
=============

No licenses in use

Product Information
===================
UDI: PID:ASAv,SN:9A9PJLLB849

Agent Version
=============
Smart Agent for Licensing: 5.7.25_asav/5

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:ASAv,SN:9A9PJLLB849
      Reservation status: UNIVERSAL INSTALLED on Nov 12 2024 06:27:23 UTC
```

- **show license features**

```
asav1# show license features
Serial Number:  9AEJMLUP4D4
Export Compliant: YES

License mode: Smart Licensing
License reservation: Enabled
ASAv Platform License State: Licensed
Active entitlement: ASAv50_PLR, enforce mode: Authorized
Firewall throughput limited to 10 Gbps
Licensed features for this platform:
Maximum VLANs                     : 50
Inside Hosts                      : Unlimited
Failover                          : Active/Standby
Encryption-DES                    : Enabled
Encryption-3DES-AES               : Enabled
Security Contexts                 : 0
Carrier                           : Enabled
AnyConnect Premium Peers          : 250
AnyConnect Essentials             : Disabled
Other VPN Peers                   : 250
Total VPN Peers                   : 250
AnyConnect for Mobile             : Enabled
AnyConnect for Cisco VPN Phone    : Enabled
Advanced Endpoint Assessment      : Enabled
Shared License                    : Disabled
Total TLS Proxy Sessions          : 500
```

```
Botnet Traffic Filter              : Enabled
Cluster                            : Enabled
```

（オプション）ASA 仮想 の永続ライセンスの返却

ASA 仮想 を廃棄する場合やモデルレベルの変更によって（新しいライセンスが必要になった場合など）永続ライセンスが不要になった場合、以下の手順に従ってライセンスを正式にSmart Software Manager に戻す必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために解除できなくなります。

手順

ステップ 1 ASA 仮想 CLI から、戻りコードを生成します。

license smart reservation return

例：

```
ciscoasa(config)# license smart reservation return
   WARNING: ASAv platform license state is Limited functionality.

   Enter this return code in Cisco Smart Software Manager portal:
   UDI: PID:ASAv,SN:9A6ST9AXQ24
       Return code: DrT1pZ-8cRT2N-xxxxx-64ABCD-xXYZeM-qD1
```

ステップ 2 ユニバーサル デバイス識別子（UDI）をコピーして、Smart Software Manager でこの ASA 仮想 インスタンスを見つることができます。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASA 仮想 を確認し、**[アクション（Actions）]** > **[削除（Remove）]** の順に選択して、ASA 仮想 の戻りコードを **[予約戻りコード（Reservation Return Code）]** フィールドに入力します。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

ステップ 5 をクリックします。

ステップ 6 永久ライセンス予約を無効にするには、次の手順を行います。

a) 永久ライセンス予約を無効にするには、 次のコマンドを実行します。

no license smart reservation

b) 次のコマンドを実行して、柔軟な永続ライセンスの予約を無効にします。

no license smart flex-model {**asav5_plr** | **asav10_plr** | **asav30_plr** | **asav_50_plr** | **asav100_plr** | **asavu_plr**}

c) 次のコマンドを実行して、ライセンスの登録が解除されたことを確認します。

show license features

コマンド出力には 、 `No active entitlement`と表示されます。

ステップ 7 コマンドを実行して実行設定をスタートアップ設定に保存して、再起動中の設定の損失を避けます。

write memory

非フレキシブル PLR モードからフレキシブル PLR モードへの切り替え

手順

ステップ 1 スマート アカウントから非柔軟な永続ライセンスの予約ライセンスの登録を解除します。

a) ASA 仮想 CLI から、戻りコードを生成します。

license smart reservation return

例：

```
ciscoasa(config)# license smart reservation return
   WARNING: ASAv platform license state is Limited functionality.

   Enter this return code in Cisco Smart Software Manager portal:
   UDI: PID:ASAv,SN:9A6ST9AXQ24
       Return code: DrT1pZ-8cRT2N-xxxxx-64ABCD-xXYZeM-qD1
```

b) ユニバーサル デバイス識別子（UDI）をコピーして、Smart Software Manager でこの ASA 仮想 インスタンスを見つることができます。

c) Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

d) ライセンスを解除する ASA 仮想 をUDI を使用して検索します。

e) **[アクション（Actions）]** > **[削除（Remove）]**を選択し、ASA 仮想 戻りコードを **[予約戻りコード（Reservation Return Code）]** フィールドに入力します。

f) [Remove Reservation] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

ステップ 2 永久ライセンス予約ライセンスを ASA 仮想 から無効にします。

a) 永久ライセンス予約を無効にするには、 次のコマンドを実行します。

no license smart reservation

ステップ 3 ASA 仮想 を柔軟な永続ライセンス予約ライセンスに登録します。詳細については、「ASA 仮想 永続ライセンスのインストール （144 ページ）」を参照してください。

回数変更可能な PLR モードから非 Flexible PLR モードへの切り替え

手順

ステップ 1 スマート アカウントからフレキシブルな永続ライセンスの予約ライセンスの登録を解除します。

a) ASA 仮想 CLI から、戻りコードを生成します。

license smart reservation return

例：

```
ciscoasa(config)# license smart reservation return
   WARNING: ASAv platform license state is Limited functionality.

   Enter this return code in Cisco Smart Software Manager portal:
   UDI: PID:ASAv,SN:9A6ST9AXQ24
       Return code: DrT1pZ-8cRT2N-xxxxx-64ABCD-xXYZeM-qD1
```

b) ユニバーサル デバイス識別子（UDI）をコピーして、Smart Software Manager でこの ASA 仮想 インスタンスを見つることができます。

c) Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

d) ライセンスを解除する ASA 仮想 をUDI を使用して検索します。

e) **[アクション（Actions）]** > **[削除（Remove）]**を選択し、ASA 仮想 戻りコードを **[予約戻りコード（Reservation Return Code）]** フィールドに入力します。

f) [Remove Reservation] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

ステップ 2 永久ライセンス予約ライセンスを ASA 仮想 から無効にします。

a) 永久ライセンス予約を無効にするには、 次のコマンドを実行します：

no license smart reservation

b) 次のコマンドを実行して、回数変更可能な永続ライセンスの予約を無効にします：

no license smart flex-model {**asav5_plr** | **asav10_plr** | **asav30_plr** | **asav_50_plr** | **asav100_plr** | **asavu_plr**}

ステップ 3 ASA 仮想 を非 Flexible の永続ライセンス予約ライセンスに登録します。詳細については、「ASA 仮想 永続ライセンスのインストール （144 ページ）」を参照してください。

（オプション）ASA 仮想 の登録解除（定期およびオンプレミス）

ASA 仮想 の登録を解除すると、アカウントから ASA 仮想 が削除され、ASA 仮想 のすべてのライセンス資格と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA 仮想 に利用することもできます。あるいは、Smart Software Manager から ASA 仮想 を削除できます。

（注） ASA 仮想 を登録解除した場合、ASA 仮想 をリロードすると重大なレート制限状態に戻ります。

手順

ASA 仮想 の登録を解除します。

license smart deregister

その後、ASA 仮想 がリロードされます。

（オプション）ASA 仮想 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス）

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

1000/1200/3100/4200：スマート ソフトウェア ライセンシングの設定

この項では、1000/1200/3100/4200 にスマート ソフトウェア ライセンシングを設定する方法を説明します。次の方法の中から 1 つを選択してください。

- 1000/1200/3100/4200：定期スマート ソフトウェア ライセンシングの設定 （153 ページ）

  （オプション） 1000/1200/3100/4200 の登録解除（定期およびオンプレミス） （168 ページ） または （オプション）1000/1200/3100/4200 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス） （169 ページ） も可能です。

- 1000/1200/3100/4200：Smart Software Manager オンプレミス ライセンシングの設定 （159 ページ）

  （オプション） 1000/1200/3100/4200 の登録解除（定期およびオンプレミス） （168 ページ） または （オプション）1000/1200/3100/4200 ID 証明書またはライセンス権限付与の更新（定期およびオンプレミス） （169 ページ） も可能です。

- 1000/1200/3100/4200：永久ライセンス予約の構成 （164 ページ）

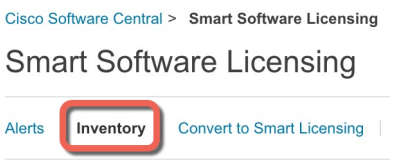
1000/1200/3100/4200：定期スマートソフトウェアライセンシングの設定

この手順は、Smart Software Manager を使用する ASA に適用されます。

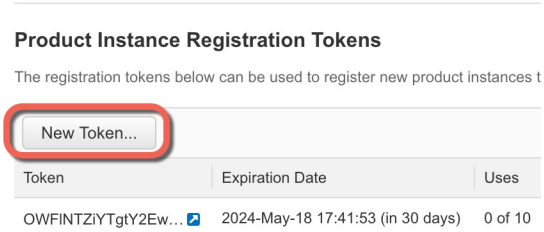
手順

ステップ 1 Smart Software Manager で、このデバイスを追加する仮想アカウントの登録トークンを要求してコピーします。

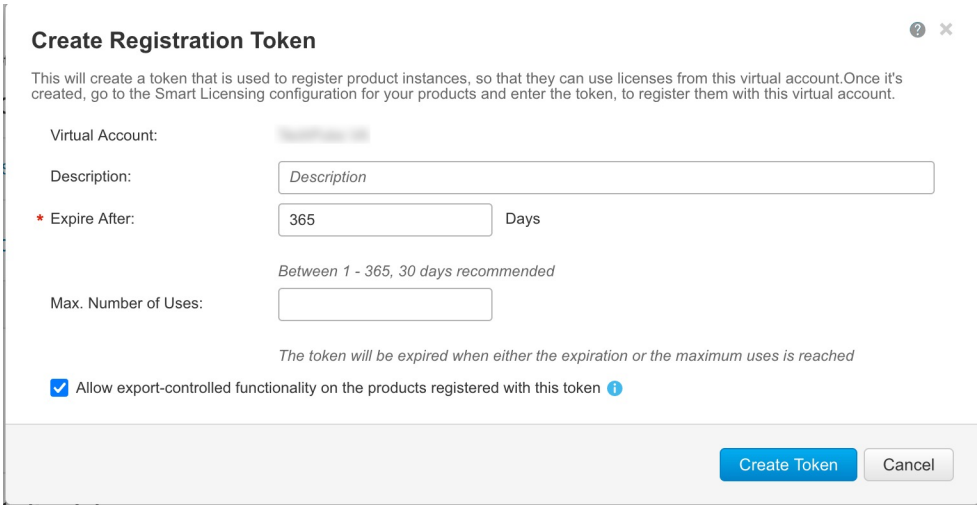
a) [Inventory] をクリックします。



b) [General] タブで、[New Token] をクリックします。



c) [登録トークンを作成（Create Registration Token）] ダイアログボックスで、以下の設定値を入力してから [トークンを作成（Create Token）] をクリックします。



- **説明**
- [有効期限（Expire After）]：推奨値は 30 日です。
- 最大使用回数（Max. Number of Uses）
- [このトークンに登録された製品で輸出管理機能を許可する（Allow export-controlled functionality on the products registered with this token）]：輸出コンプライアンス フラグを有効にします。

トークンはインベントリに追加されます。

d) トークンの右側にある矢印アイコンをクリックして [トークン（Token）] ダイアログボックスを開き、トークン ID をクリップボードにコピーできるようにします。ASA の登録が必要なときに後の手順で使用するために、このトークンを準備しておきます。

図 *18*：トークンの表示

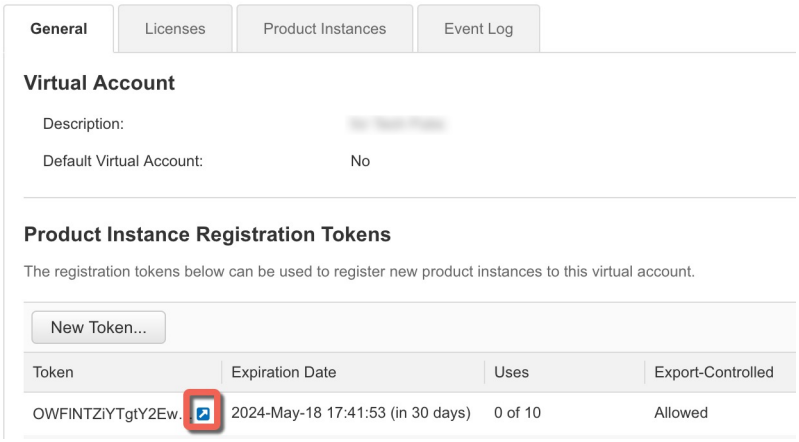
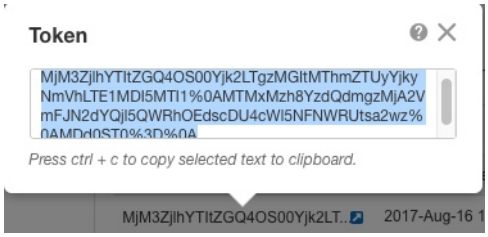


図 *19*：トークンのコピー



ステップ 2 （任意）

ステップ 3 （任意） ASA で、スマート トランスポートの HTTP プロキシ URL を指定します。

license smart

transport proxy *proxy_server_ip* **port** *port*

スマートトランスポートの代わりに Smart Call Home を使用するには、ステップ ステップ 5（157 ページ）を参照してください。

（注）
- 認証を使用する HTTP プロキシはサポートされません。
- プロキシサーバーの URL を設定する場合は、プロトコルを指定しないでください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy proxy.esl.cisco.com port 80
```

ステップ 4 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）機能階層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。階層ライセンスは、他の機能ライセンスを追加するための前提条件になります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。Secure Firewall モデルの場合、Essentialsライセンスは常に有効であり、無効にすることはできません。

c) セキュリティコンテキストのライセンスを要求します。

feature context *number*

（注）
このライセンスは、Firepower 1010ではサポートされません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：25 コンテキスト
- Cisco Secure Firewall 1210：5 コンテキスト
- Cisco Secure Firewall 1220：10 コンテキスト
- Cisco Secure Firewall 1230：25 コンテキスト
- Cisco Secure Firewall 1240：25 コンテキスト
- Cisco Secure Firewall 1250：25 コンテキスト
- Secure Firewall 3100：100 コンテキスト
- Cisco Secure Firewall 4200：100 コンテキスト

たとえば、Firepower 1150 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （任意） (Firepower 1010）Active/Standby Failover を有効にするために Security Plus License を要求します。

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意）（Cisco Secure Firewall 3100/4200）Diameter、GTP/GPRS、SCTP インスペクションのキャリアライセンスを要求します。

feature carrier

例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

ステップ 5 （任意） スマート ライセンス サーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトのスマート トランスポートを使用する必要があります。

a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する**ライセンス**と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
```

```
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （任意） HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

（注）
認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

ステップ 6 手順 1 でコピーしたトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager に登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager は、ご使用のアカウントが許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** または **show running-config license** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC
```

```
License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                     1 AUTHORIZED
```

例：

```
ciscoasa(config)# show running-config license
license smart
feature tier standard
throughput level 1G
transport proxy proxy.esl.cisco.com port 80
```

1000/1200/3100/4200：Smart Software Manager オンプレミス ライセンシングの設定

この手順は、Smart Software Manager オンプレミスを使用する ASA に適用されます。

始める前に

- Smart Software Manager オンプレミス OVA ファイルを Cisco.com からダウンロードし、VMware ESXi サーバーにインストールして設定します。詳細については、『*Cisco Smart Software Manager On-Prem Data Sheet*』を参照してください。
- バージョン 7.0 では、スマート トランスポートが Smart Software Manager On-Prem に追加されました。それよりも古いバージョンを使用している場合、次の手順に従って、ASA で Smart Call Home をイネーブルにします。
- デバイスをエアギャップ ネットワークに配置する前に、クリプト CA トラストプールをダウンロードする。このトラストプールは通常、自動的にダウンロードされますが、エアギャップ ネットワークでは失効している可能性があります。

  crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b

手順

ステップ 1 Smart Software Manager オンプレミスサーバーで登録トークンを要求します。

ステップ 2 （任意） ASA で、スマート トランスポートの HTTP プロキシ URL を指定します。

license smart

transport proxy *proxy_server_ip* **port** *port*

スマートトランスポートの代わりに Smart Call Home を使用するには、ステップ ステップ 5（162 ページ）を参照してください。

（注）

認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport proxy 10.1.1.1 port 10101
```

ステップ 3 ライセンスサーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

license smart

transport url https://*on-prem_ip_address***/SmartTransport**

スマートトランスポートの代わりに Smart Call Home を使用するには、ステップ ステップ 5（162 ページ）を参照してください。

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)# transport url https://10.1.5.5/SmartTransport
```

ステップ 4 ASA でライセンス権限付与を要求します。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）機能階層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。階層ライセンスは、他の機能ライセンスを追加するための前提条件になります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。Secure Firewall モデルの場合、Essentialsライセンスは常に有効であり、無効にすることはできません。

c) （任意） セキュリティコンテキストのライセンスを要求します。

feature context *number*

（注）
このライセンスは、Firepower 1010 および Cisco Secure Firewall 1210/1220ではサポートされません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルト コンテキストを差し引いたものを要求する必要があります。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：25 コンテキスト
- Cisco Secure Firewall 1210：5 コンテキスト
- Cisco Secure Firewall 1220：10 コンテキスト
- Cisco Secure Firewall 1230：25 コンテキスト
- Cisco Secure Firewall 1240：25 コンテキスト
- Cisco Secure Firewall 1250：25 コンテキスト
- Secure Firewall 3100：100 コンテキスト
- Cisco Secure Firewall 4200：100 コンテキスト

たとえば、Firepower 1150 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （任意）(Firepower 1010）Active/Standby Failover を有効にするために Security Plus License を要求します。

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意）（Cisco Secure Firewall 3100/4200）Diameter、GTP/GPRS、SCTP インスペクションのキャリアライセンスを要求します。

feature carrier

例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウ

ントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

ステップ 5 （任意） スマート ライセンス サーバーとの通信には、デフォルトの Smart Transport の代わりに Smart Call Home を使用します。

Smart Transport の代わりに Smart Call Home を使用する必要があることがわかっている場合は、次の手順を実行します。それ以外の場合は、デフォルトのスマートトランスポートを使用する必要があります。

a) 転送タイプを [Smart Call Home] に設定します。

license smart

transport type callhome

構成には、Smart Software Manager の URL を指定する**ライセンス**と呼ばれる Smart Call Home のプロファイルが含まれます。

```
call-home
  profile License
    destination address http
https://tools.cisco.com/its/service/oddce/services/DDCEService
```

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#transport type callhome
```

b) （任意） HTTP プロキシ URL を指定します。

call-home

http-proxy *ip_address* **port** *port*

（注）
認証を使用する HTTP プロキシはサポートされません。

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# http-proxy 10.1.1.1 port 443
```

c) ライセンス サーバーの URL を変更して、Smart Software Manager オンプレミスに移動します。

call-home

profile License

destination address http
https://*on-prem_ip_address*/**Transportgateway/services/DeviceRequestHandler**

例：

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile License
ciscoasa(cfg-call-home-profile)#destination address http
https://10.1.5.5/Transportgateway/services/DeviceRequestHandler
```

ステップ 6 手順 1 で要求したトークンを使用して ASA を登録します。

license smart register idtoken *id_token*

例：

```
ciscoasa# license smart register idtoken YjE3Njc5MzYtMGQzMi00OTA4
LWJhODItNzBhMGQ5NGRlYjUxLTE0MTQ5NDAy%0AODQzNzl8NXk2bzV3SDE0ZkgwQk
dYRmZ1NTNCNGlvRnBHUFpjcm02WTB4TU4w%0Ac2NnMD0%3D%0A
```

ASA が Smart Software Manager オンプレミスサーバーに登録され、設定されたライセンス権限付与の承認を要求します。Smart Software Manager オンプレミスサーバーは、お使いのアカウントで許可すれば高度暗号化（3DES/AES）ライセンスも適用します。ライセンスのステータスと使用状況をチェックするには、**show license summary** コマンドを使用します。

例：

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: Biz1
  Virtual Account: IT
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2018 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2017 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (FP1010-ASA-Std)                    1 AUTHORIZED
```

1000/1200/3100/4200：永久ライセンス予約の構成

1000、 Cisco Secure Firewall 1200/3100/4200 に永久ライセンスを割り当てることができます。この項では、ASA を廃止する場合にライセンスを返す方法についても説明します。

手順

ステップ 1 1000/1200/3100/4200 永続ライセンスの インストール （164 ページ）。

ステップ 2 （オプション）1000/1200/3100/4200 永続ライセンスの返却 （167 ページ）。

1000/1200/3100/4200 永続ライセンスの インストール

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。永続ライセンスでは、すべての機能が有効になります（セキュリティコンテキストが最大のEssentialsライセンス）。

（注） 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。（オプション）1000/1200/3100/4200 永続ライセンスの返却 （167 ページ）を参照してください。

始める前に

永続ライセンスを購入すると、Smart Software Manager でそれらのライセンスを使用できます。すべてのアカウントが永続ライセンスの予約について承認されているわけではありません。設定を開始する前にこの機能についてシスコの承認があることを確認します。

手順

ステップ 1 ASA CLI で、永続ライセンスの予約を次のように有効にします。

license smart reservation

例：

```
ciscoasa (config)# license smart reservation
ciscoasa (config)#
```

ステップ 2 Smart Software Manager に入力するライセンス コードを次のように要求します。

license smart reservation request universal

例：

```
ciscoasa# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
BB-ZFPR-2140:JAD200802RR-AzKmHcc71-2A
ciscoasa#
```

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、以下を入力します。

license smart reservation cancel

パーマネントライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。（オプション）1000/1200/3100/4200 永続ライセンスの返却 （167 ページ）を参照してください。

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Licenses] タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。

ステップ 4 [License Reservation] をクリックして、ASA のコードをボックスに入力します。[Reserve License] をクリックします。

Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[License Reservation] ボタンが表示されない場合、お使いのアカウントはパーマネント ライセンスの予約について承認されていません。この場合、パーマネントライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

ステップ 5 ASA で、承認コードを次のように入力します。

license smart reservation install *code*

例：

```
ciscoasa# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
ciscoasa#
```

ステップ 6 ASA でライセンス権限付与を要求します。

（注）
永続ライセンスにより、すべてのライセンスを完全に使用できますが、ASA がライセンスを使用できることを ASA が認識できるように、ASA 設定で権限をオンにする必要があります。

a) ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

b) （Firepower 1000）機能階層を設定します。

feature tier standard

使用できるのは標準（Essentials）層のみですが、設定で有効にする必要があります。階層ライセンスは、他の機能ライセンスを追加するための前提条件になります。Essentials ライセンスは、以前は標準ライセンスと呼ばれていました。「標準」は引き続き CLI で使用されています。Secure Firewall モデルの場合、Essentialsライセンスは常に有効であり、無効にすることはできません。

c) （任意） セキュリティコンテキストのライセンスを有効にします。

feature context *number*

（注）
このライセンスは、Firepower 1010ではサポートされません。

デフォルトでは、ASA は 2 つのコンテキストをサポートしているため、必要なコンテキストの数から 2 つのデフォルトコンテキストを差し引いたものを有効にする必要があります。永続ライセンスでは最大数が許可されるため、モデルの最大数を有効にすることができます。コンテキストの最大数は、モデルによって異なります。

- Firepower 1120：5 コンテキスト
- Firepower 1140：10 コンテキスト
- Firepower 1150：25 コンテキスト
- Cisco Secure Firewall 1210：5 コンテキスト
- Cisco Secure Firewall 1220：10 コンテキスト
- Cisco Secure Firewall 1230：25 コンテキスト
- Cisco Secure Firewall 1240：25 コンテキスト
- Cisco Secure Firewall 1250：25 コンテキスト
- Secure Firewall 3100：100 コンテキスト
- Cisco Secure Firewall 4200：100 コンテキスト

たとえば、Firepower 1150 で最大 25 のコンテキストを使用するには、コンテキストの数として 23 を入力します。この値は、デフォルトの 2 に追加されます。

例：

```
ciscoasa(config-smart-lic)# feature context 18
```

d) （任意）（Firepower 1010）Security Plus ライセンスを有効にして、フェールオーバーを有効にします。

feature security-plus

例：

```
ciscoasa(config-smart-lic)# feature security-plus
```

e) （任意）（Cisco Secure Firewall 3100/4200）Diameter、GTP/GPRS、SCTP インスペクションのキャリアライセンスを有効にします。

feature carrier

例：

```
ciscoasa(config-smart-lic)# feature carrier
```

f) （任意） 高度暗号化を有効にします。

feature strong-encryption

Smart Software Managerから高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature strong-encryption
```

（オプション）1000/1200/3100/4200 永続ライセンスの返却

永続ライセンスが不要になった場合（ASA を廃止する場合など）は、この手順を使用して正式に Smart Software Manager にライセンスを返却する必要があります。すべての手順を実行しないと、ライセンスが使用中のままになり、他の場所で使用するために容易に解除できなくなります。

手順

ステップ 1 ASA で返却コードを次のように生成します。

license smart reservation return

例：

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
```

ただちに ASA のライセンスがなくなり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンス（**license smart reservation request universal**）を要求すると、このコードを再表示できなくなることに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。評価期間が終了すると、ASA は期限切れ状態に移行します。コンプライアンス違反状態の詳細については、コンプライアンス逸脱状態 （198 ページ）を参照してください。

ステップ 2 ASA ユニバーサル デバイス識別子（UDI）が表示されるので、Smart Software Manager で ASA インスタンスを見つることができます。

show license udi

例：

```
ciscoasa# show license udi
UDI: PID:FPR-2140,SN:JAD200802RR
ciscoasa#
```

ステップ 3 Smart Software Manager インベントリ画面に移動して、[Product Instances] タブをクリックします。

https://software.cisco.com/#SmartLicensing-Inventory

[Product Instances] タブに、ライセンスが付与されているすべての製品が UDI によって表示されます。

ステップ 4 ライセンスを解除する ASA を確認し、**[Actions]** > **[Remove]** を選択して、ASA の返却コードをボックスに入力します。[Remove Product Instance] をクリックします。

パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

（オプション）1000/1200/3100/4200の登録解除（定期およびオンプレミス）

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。あるいは、Smart Software Manager（SSM）から ASA を削除できます。

手順

ASA の登録解除：

license smart deregister

（オプション）1000/1200/3100/4200ID証明書またはライセンス権限付与の更新（定期およびオンプレミス）

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

手順

ステップ 1 アイデンティティ証明書を更新します。

license smart renew id

ステップ 2 Renew the license entitlement:

license smart renew auth

Firepower 4100/9300：スマート ソフトウェア ライセンスの設定

この手順は、Smart Software Manager、Smart Software Manager オンプレミスを使用するシャーシ、または永続ライセンスの予約に適用されます。方法を前提条件として設定するには、FXOS 構成ガイドを参照してください。

永続ライセンス予約の場合、ライセンスはすべての機能、すなわちセキュリティ コンテキストが最大の標準ティアおよびキャリア ライセンスを有効にします。ただし、ASA がこれらの機能を使用することを「認識する」ためには、ASA でそれらを有効にする必要があります。

始める前に

ASA クラスタの場合は、設定作業のために制御ユニットにアクセスする必要があります。Firewall Chassis マネージャ でどのユニットが制御ノードなのかを確認してください。この手順に示すように、ASA CLI からも確認できます。

手順

ステップ 1 Firepower 4100/9300 シャーシ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module *slot* **console connect asa**

例：

```
Firepower> connect module 1 console
Firepower-module1> connect asa

asa>
```

次回 ASA コンソールに接続するときは、ASA に直接移動します。**connect asa** を再入力する必要はありません。

ASA クラスタの場合、ライセンス設定などの設定を行う場合にのみ、制御ユニットにアクセスする必要があります。通常、制御ユニットがスロット 1 にあるため、このモジュールにまず接続する必要があります。

ステップ 2 ASA CLI で、グローバル コンフィギュレーション モードを入力します。論理デバイスの展開時に設定しない限り、デフォルトではイネーブルパスワードは空白ですが、**enable** コマンドを最初に入力したときに変更するように求められます。

enable configure terminal

例：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
asa# configure terminal
asa(config)#
```

ステップ 3 ASA クラスタの場合は、必要に応じて、このユニットが制御ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster stbu: On
```

```
  This is "unit-1-1" in state SLAVE
    ID : 0
    Version : 9.5(2)
    Serial No.: P3000000025
    CCL IP : 127.2.1.1
    CCL MAC : 000b.fcf8.c192
    Last join : 17:08:59 UTC Sep 26 2015
    Last leave: N/A
Other members in the cluster:
  Unit "unit-1-2" in state SLAVE
    ID : 1
    Version : 9.5(2)
    Serial No.: P3000000001
    CCL IP : 127.2.1.2
    CCL MAC : 000b.fcf8.c162
    Last join : 19:13:11 UTC Sep 23 2015
    Last leave: N/A
  Unit "unit-1-3" in state MASTER
    ID : 2
    Version : 9.5(2)
    Serial No.: JAB0815R0JY
    CCL IP : 127.2.1.3
    CCL MAC : 000f.f775.541e
    Last join : 19:13:20 UTC Sep 23 2015
    Last leave: N/A
```

別のユニットが制御ユニットの場合は、接続を終了し、正しいユニットに接続します。接続の終了については、以下を参照してください。

ステップ 4 ライセンス スマート コンフィギュレーション モードを開始します。

license smart

例：

```
ciscoasa(config)# license smart
ciscoasa(config-smart-lic)#
```

ステップ 5 機能層を設定します。

feature tier standard

使用できるのは標準層だけです。ティア ライセンスは、他の機能ライセンスを追加するための前提条件です。アカウントに十分なティアライセンスが必要です。そうでないと、他の機能ライセンスまたはライセンスを必要とする機能を設定できません。

ステップ 6 次の機能の 1 つ以上をリクエストします。

- キャリア（GTP/GPRS、Diameter、および SCTP インスペクション）

  feature carrier

- セキュリティ コンテキスト

  feature context *<1-248>*

  永続ライセンスの予約では、最大コンテキスト（248）を指定できます。

- 強力な暗号化（3DES/AES）

feature strong-encryption

Smart Software Manager から高度暗号化トークンを受け取った場合、このライセンスは必要ありません。ただし、スマートアカウントで高度暗号化が許可されていないものの、高度暗号化の使用が許可されているとシスコが判断した場合、高度暗号化ライセンスをアカウントに手動で追加できます。アクティブユニットのみがこのライセンスを要求し、ライセンスの集約により両方のユニットがこれを使用できます。

例：

```
ciscoasa(config-smart-lic)# feature carrier
ciscoasa(config-smart-lic)# feature context 50
```

ステップ 7 ASA コンソールを終了して Telnet アプリケーションに戻るには、プロンプトで「~」と入力します。スーパバイザ CLI に戻るには、「**quit**」と入力します。

モデルごとのライセンス

このセクションでは、ASAv および Firepower 4100/9300 シャーシASA セキュリティ モジュールに使用可能なライセンス資格を示します。

ASA 仮想

ASAの構成設定で **throughput level** コマンドを使用してスループットレベルを設定するとき、または柔軟な永続ライセンス予約のために**license smart plr set** コマンドでモデルを指定する場合は、Smart Software Managerから要求されるライセンスの種類が決定されます。次のスループットレベルとライセンスの関係を参照してください。

- 100M：ASAv5
- 1G：ASAv10
- 2G：ASAv30
- 10G：ASAv50
- 20G：ASAv100
- 無制限：ASAvU

このスループットレベルにより、最大 セキュアクライアント および TLS プロキシセッションも決定されます。ただし、ASA 仮想 メモリプロファイルを小さくすると、実際のセッション数が制限されるため、セッションを決定するには、スループットレベルと搭載されているメモリの両方を確認する必要があります。

使用中の ASA 仮想 のメモリにより、最大同時ファイアウォール接続数と VLAN が決定されます（スループットレベルによっては決定されません）。

次の表に、ASA 仮想 シリーズのライセンス機能を示します。

ライセンス	説明
権限付与ライセンス	
スループット レベル	ASA 設定でスループットレベルを指定するには、**throughput level** コマンドを使用するか、柔軟な永続ライセンス予約の場合は、**license smart plr set** コマンドでモデルを指定します。このレベルにより、必要なライセンスが決定されます。 100M：ASAv5 1G：ASAv10 2G：ASAv30 10G：ASAv50 20G：ASAv100 無制限：ASAvU
ファイアウォール ライセンス	
Botnet Traffic Filter	イネーブル
ファイアウォールの接続、同時	ファイアウォール接続数は、ASA 仮想のメモリによって決定されます。 2 GB ～ 7.9 GB：100,000 8 GB ～ 15.9 GB：500,000 16 GB ～ 31.9 GB：2,000,000 32 GB ～ 64 GB：4,000,000 ASAvU：64 GB の最小メモリを使用する ASAvU を使用している場合、ファイアウォール接続の最大数は 8,000,000 です。
通信事業者	イネーブル

ライセンス	説明
Total TLS Proxy Sessions	TLS プロキシセッション数は、スループットレベルと ASA 仮想 のメモリによって決定されます。 100M スループット + 任意のメモリ：500 1G スループット + 任意のメモリ：500 2G スループット： • 2 GB ～ 7.9 GB のメモリ：500 • 8 GB 以上のメモリ：1000 10G スループット： • 2 GB ～ 7.9 GB のメモリ：500 • 8 GB ～ 15.9 GB のメモリ：1000 • 16 GB 以上のメモリ：10,000 20G スループット： • 2 GB ～ 7.9 GB のメモリ：500 • 8 GB ～ 15.9 GB のメモリ：1000 • 16 GB ～ 31.9 GB のメモリ：10,000 • 32 GB 以上のメモリ：20,000 無制限のスループット：64 GB の最小メモリを使用する ASAvU を使用している場合、TLS プロキシセッションの最大数は 40,000 です。
VPN ライセンス	

ライセンス	説明	
セキュアクライアントピア	Unlicensed	セキュアクライアント ピア数は、スループットレベルと ASA 仮想 のメモリによって決定されます。 オプション*Secure Client Advantage*または*Secure Client Premier*ライセンス、最大： *100M* スループット + 任意のメモリ：*50* *1G* スループット + 任意のメモリ：*250* *2G* スループット： • *2 GB* ～ *7.9 GB* のメモリ：*250* • *8 GB* 以上のメモリ：*750* *10G* スループット： • *2 GB* ～ *7.9 GB* のメモリ：*250* • *8 GB* ～ *15.9 GB* のメモリ：*750* • *16 GB* 以上のメモリ：*10,000* *20G* スループット： • *2 GB* ～ *7.9 GB* のメモリ：*250* • *8 GB* ～ *15.9 GB* のメモリ：*750* • *16 GB* ～ *31.9 GB*：*10,000* • *32 GB* 以上のメモリ：*20,000* 無制限のスループット：64 GB の最小メモリを使用する ASAvU を使用している場合、セキュアクライアント ピアの最大数は 40,000 です。

ライセンス	説明
その他の VPN ピア	（注） その他の VPN ピアの数は、スループットレベルと ASA 仮想のメモリによって決定されます。 100M スループット + 任意のメモリ：50 1G スループット + 任意のメモリ：250 2G スループット： • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB 以上のメモリ：750 10G スループット： • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB ～ 15.9 GB のメモリ：750 • 16 GB 以上のメモリ：10,000 20G スループット： • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB ～ 15.9 GB のメモリ：750 • 16 GB ～ 31.9 GB：10,000 • 32 GB 以上のメモリ：20,000 無制限のスループット：64 GB の最小メモリを使用する ASAvU を使用している場合、他の VPN ピアの最大数は 40,000 です。

ライセンス	説明
合計 VPN ピア。全タイプの合計	（注） VPN ピアの合計数は、スループットレベルと ASA 仮想 のメモリによって決定されます。 100M スループット + 任意のメモリ：50 1G スループット + 任意のメモリ：250 2G スループット： • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB 以上のメモリ：750 10G スループット： • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB ～ 15.9 GB のメモリ：750 • 16 GB 以上のメモリ：10,000 20G スループット： • 2 GB ～ 7.9 GB のメモリ：250 • 8 GB ～ 15.9 GB のメモリ：750 • 16 GB ～ 31.9 GB：10,000 • 32 GB 以上のメモリ：20,000 無制限のスループット：64 GB の最小メモリを使用する ASAvU を使用している場合、VPN ピアの最大数は 40,000 です。
一般ライセンス	
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）
フェールオーバー	アクティブ/スタンバイ
セキュリティ コンテキスト	サポートなし
クラスタ	有効

ライセンス	説明
VLAN、最大	VLAN 数は、ASA 仮想 のメモリによって決定されます。 2 GB ～ 7.9 GB：50 8 GB ～ 15.9 GB：200 16 GB ～ 31.9 GB：1,024 32 GB ～ 64 GB：1,024

Firepower 1010

次の表に、Firepower 1010 のライセンス機能を示します。

ライセンス	**Essentials ライセンス**	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	100,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシセッション	4,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*または*Secure Client VPN* のみライセンス、最大：*75*
その他の VPN ピア	75	
合計VPN ピア。全タイプの合計	75	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
Security Plus（フェールオーバー、VPN ロードバランシング）	無効	オプション

ライセンス	Essentials ライセンス
セキュリティ コンテキスト	サポートしない
クラスタ	サポートしない
VLAN、最大	60

Firepower 1100 シリーズ

次の表に、Firepower 1100 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 1120：200,000 Firepower 1140：400,000 Firepower 1150：600,000	
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシ セッション	Firepower 1120：4,000 Firepower 1140：8,000 Firepower 1150：8,000	
VPN ライセンス		
セキュア クライアント ピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス、最大： *Firepower 1120：150* *Firepower 1140：400* *Firepower 1150：800*
その他の VPN ピア	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	

ライセンス	Essentials ライセンス	
合計 VPN ピア。全タイプの合計	Firepower 1120：150 Firepower 1140：400 Firepower 1150：800	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大： *Firepower 1120：5* *Firepower 1140：10* *Firepower 1150：25*
クラスタ	サポートしない	
VLAN、最大	1024	

Cisco Secure Firewall 1210、1220

次の表に、Cisco Secure Firewall 1210 および 1220 のライセンス機能を示します。

ライセンス	Essentials ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。
ファイアウォールの接続、同時	Cisco Secure Firewall 1210：200000 Cisco Secure Firewall 1220：300000
通信事業者	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。
合計 TLS プロキシ セッション	Cisco Secure Firewall 1210：320 Cisco Secure Firewall 1220：320
VPN ライセンス	

ライセンス	Essentials ライセンス	
セキュアクライアントピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス、最大： *Cisco Secure Firewall 1210*：*200* *Cisco Secure Firewall 1220*：*300*
その他の VPN ピア	Cisco Secure Firewall 1210：200 Cisco Secure Firewall 1220：300	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 1210：200 Cisco Secure Firewall 1220：300	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大： *Cisco Secure Firewall 1210*：*5* *Cisco Secure Firewall 1220*：*10*
クラスタ	サポートしない	
VLAN、最大	1024	

Secure Firewall 1230、1240、1250

次の表に、Secure Firewall 1230、1240、1250、のライセンス機能を示します。

ライセンス	Essentials ライセンス
ファイアウォール ライセンス	
Botnet Traffic Filter	サポートなし。
ファイアウォールの接続、同時	Cisco Secure Firewall 1230：400000 Cisco Secure Firewall 1240：400000 Cisco Secure Firewall 1250：1000000

ライセンス	Essentials ライセンス	
サポートしないSCTPインスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	サポートしないSCTP インスペクション マップはサポートされていませんが、ACL を使用した SCTP ステートフル インスペクションがサポートされています。	
合計 TLS プロキシ セッション	Cisco Secure Firewall 1230：1000 Cisco Secure Firewall 1240：1000 Cisco Secure Firewall 1250：1000	
VPN ライセンス		
セキュア クライアント ピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス、最大： *Cisco Secure Firewall 1230：500* *Cisco Secure Firewall 1240：1000* *Cisco Secure Firewall 1250：1500*
その他の VPN ピア	Cisco Secure Firewall 1230：500 Cisco Secure Firewall 1240：1000 Cisco Secure Firewall 1250：1500	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 1230：500 Cisco Secure Firewall 1240：1000 Cisco Secure Firewall 1250：1500	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	

ライセンス	Essentials ライセンス	
セキュリティ コンテキスト	2	オプションライセンス、最大： *Cisco Secure Firewall 1230：25* *Cisco Secure Firewall 1240：25* *Cisco Secure Firewall 1250：25*
クラスタ	イネーブル	
VLAN、最大	1024	

Secure Firewall 3100 シリーズ

次の表に、Secure Firewall 3100 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Cisco Secure Firewall 3105：2,000,000 Cisco Secure Firewall 3110：2,000,000 Cisco Secure Firewall 3120：4,000,000 Cisco Secure Firewall 3130：6,000,000 Cisco Secure Firewall 3140：10,000,000	
通信事業者	ディセーブル	オプション ライセンス：通信事業者
合計 TLS プロキシセッション	Cisco Secure Firewall 3105：10,000 Cisco Secure Firewall 3110：10,000 Cisco Secure Firewall 3120：15,000 Cisco Secure Firewall 3130：15,000 Cisco Secure Firewall 3140：15,000	
VPN ライセンス		

ライセンス	Essentials ライセンス	
セキュアクライアントピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス、最大： *Cisco Secure Firewall 3105*：*3,000* *Cisco Secure Firewall 3110*：*3,000* *Cisco Secure Firewall 3120*：*7,000* *Cisco Secure Firewall 3130*：*15,000* *Cisco Secure Firewall 3140*：*20,000*
その他の VPN ピア	Cisco Secure Firewall 3105：3,000 Cisco Secure Firewall 3110：3,000 Cisco Secure Firewall 3120：7,000 Cisco Secure Firewall 3130：15,000 Cisco Secure Firewall 3140：20,000	
合計VPNピア。全タイプの合計	Cisco Secure Firewall 3105：3,000 Cisco Secure Firewall 3110：3,000 Cisco Secure Firewall 3120：7,000 Cisco Secure Firewall 3130：15,000 Cisco Secure Firewall 3140：20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	2	オプションライセンス、最大：*100*
クラスタ	イネーブル	
VLAN、最大	1024	

Firepower 4100

次の表に、Firepower 4100 のライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 4112：10,000,000 Firepower 4115：15,000,000 Firepower 4125：25,000,000 Firepower 4145：40,000,000	
通信事業者	ディセーブル	オプション ライセンス：通信事業者
合計 TLS プロキシセッション	15,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス： *Firepower 4112：10,000* *Firepower 4115：15,000* *Firepower 4125：20,000* *Firepower 4145：20,000*
その他の VPN ピア	Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4125：20,000 Firepower 4145：20,000	
合計 VPN ピア。全タイプの合計	Firepower 4112：10,000 Firepower 4115：15,000 Firepower 4125：20,000 Firepower 4145：20,000	
一般ライセンス		

ライセンス	Essentials ライセンス	
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプションライセンス：最大 *250*
クラスタ	イネーブル	
VLAN、最大	1024	

Cisco Secure Firewall 4200 シリーズ

次の表に、Secure Firewall 4200 シリーズのライセンス機能を示します。

ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Cisco Secure Firewall 4215：40,000,000 Secure Firewall 4225：90,000,000 Secure Firewall 4245：180,000,000	
通信事業者	ディセーブル	オプション ライセンス：通信事業者
合計 TLS プロキシセッション	15,000	
VPN ライセンス		
セキュアクライアントピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、または*Secure Client VPN* のみライセンス、最大： *Cisco Secure Firewall 4215*：*20,000* *Cisco Secure Firewall 4225*：*25,000* *Cisco Secure Firewall 4245*：*30,000*

ライセンス	Essentials ライセンス	
その他の VPN ピア	Cisco Secure Firewall 4215：20,000 Cisco Secure Firewall 4225：25,000 Cisco Secure Firewall 4245：30,000	
合計 VPN ピア。全タイプの合計	Cisco Secure Firewall 4215：20,000 Cisco Secure Firewall 4225：25,000 Cisco Secure Firewall 4245：30,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプションライセンス、最大：*250*
クラスタ	イネーブル	
VLAN、最大	1024	

Firepower 9300

次の表に、Firepower 9300 のライセンス機能を示します。

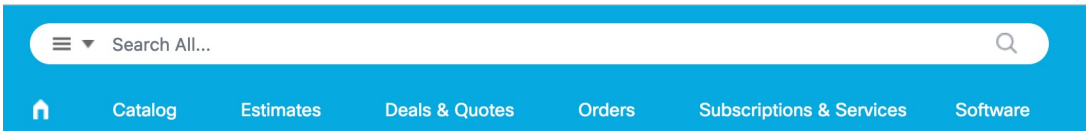
ライセンス	Essentials ライセンス	
ファイアウォール ライセンス		
Botnet Traffic Filter	サポートなし。	
ファイアウォールの接続、同時	Firepower 9300 SM-56：60,000,000 Firepower 9300 SM-48：60,000,000 Firepower 9300 SM-40：55,000,000	
キャリア	無効	オプション ライセンス：通信事業者
合計 TLS プロキシセッション	15,000	
VPN ライセンス		

ライセンス	Essentials ライセンス	
セキュアクライアントピア	Unlicensed	オプション*Secure Client Advantage*、*Secure Client Premier*、*Secure Client VPN* のみライセンス：最大 *20,000*
その他の VPN ピア	20,000	
合計 VPN ピア。全タイプの合計	20,000	
一般ライセンス		
暗号化	アカウントのエクスポート コンプライアンス設定によって、Base（DES）または Strong（3DES/AES）	
セキュリティ コンテキスト	10	オプションライセンス：最大 *250*
クラスタ	イネーブル	
VLAN、最大	1024	

モデルごとのライセンス PID

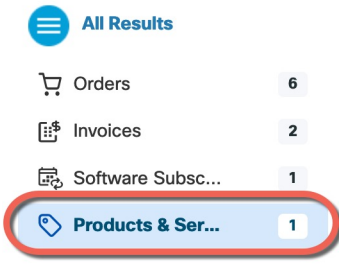
ライセンスは、シスコまたは販売代理店からデバイスを購入した際に、スマート ソフトウェア ライセンシング アカウントにリンクされています。ただし、自身でライセンスを追加する必要がある場合は、Cisco Commerce Workspace で [すべて検索（Search All）] フィールドを使用します。

図 *20*：ライセンス検索



結果から、[製品とサービス（Products and Services）] を選択します。

図 *21* : 結果



ASA 仮想 PID

ASA 仮想 Smart Software Manager 定期およびオンプレミスPID：

- ASAv5 license—L-ASAV5S-K9=
- ASAv10 license—L-ASAV10S-K9=
- ASAv30 license—L-ASAV30S-K9=
- ASAv50 license—L-ASAV50S-K9=
- ASAv100 license—L-ASAV100S-1Y=
- ASAv100 license—L-ASAV100S-3Y=
- ASAv100 license—L-ASAV100S-5Y=
- ASAvU license—L-ASA-V-U-K9=

（注） ASAv100 はサブスクリプションベースのライセンスで、期間は 1 年、3 年、または 5 年です。

ASA 仮想 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- ASAv5 license—L-ASAV5SR-K9=
- ASAv10 license—L-ASAV10SR-K9=
- ASAv30 license—L-ASAV30SR-K9=
- ASAv50 license—L-ASAV50SR-K9=
- ASAv100 license—L-ASAV100SR-K9=
- ASAvU license—ASA-V-U-ULR-K9=

Firepower 1010 PID

Firepower 1010 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：L-FPR1000-ASA=。必須。
- Security Plus：L-FPR1010-SEC-PL=。Security Plus ライセンスによってフェールオーバーが有効になります。
- 高度暗号化（3DES/AES）：L-FPR1K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1010 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-FPR1K-ASA-BPU=

Firepower 1100 PID

Firepower 1100 Smart Software Manager 定期およびオンプレミス PID：

- Essentials ：L-FPR1000-ASA=。必須。
- 5 コンテキスト：L-FPR1K-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：L-FPR1K-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 高度暗号化（3DES/AES）：L-FPR1K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 1100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-FPR1K-ASA-BPU=

Secure Firewall 1210/1220 PID

Secure Firewall 1210/1220 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：自動的に含められます。

- 5 コンテキスト：CSF1200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 高度暗号化（3DES/AES）：L-CSF1200-ENCK9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Secure Firewall 1210/1220 永続ライセンスの予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-CSF1200-ASA-BPU=

Cisco Secure Firewall 1230/1240/1250 PID

Secure Firewall 1230/1240/1250 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：自動的に含められます。
- 5 コンテキスト：CSF1200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：CSF1200-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 高度暗号化（3DES/AES）：L-CSF1200-ENCK9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Secure Firewall 1230/1240/1250 永続ライセンスの予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-CSF1200-ASA-BPU=

Secure Firewall 3100 PID

Secure Firewall 3100 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：自動的に含められます。
- 5 コンテキスト：L-FPR3K-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：L-FPR3K-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。

- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR3K-ASA-CAR=
- 高度暗号化（3DES/AES）：L-FPR3K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 3100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-FPR3K-ASA-BPU=

Firepower 4100 PID

Firepower 4100 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：L-FPR4100-ASA=。必須。
- 10 コンテキスト：L-FPR4K-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 230 コンテキスト：L-FPR4K-ASASC-230=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 250 コンテキスト：L-FPR4K-ASASC-250=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR4K-ASA-CAR=
- 高度暗号化（3DES/AES）：L-FPR4K-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 4100 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-FPR4K-ASA-BPU=

Secure Firewall 4200 PID

Secure Firewall 4200 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：自動的に含められます。

- 5 コンテキスト：L-FPR4200-ASASC-5=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- 10 コンテキスト：L-FPR4200-ASASC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-FPR4200-ASA-CAR=
- 高度暗号化（3DES/AES）：L-FPR4200-ENC-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 4200 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-FPR4200-ASA-BPU=

Firepower 9300 PID

Firepower 9300 Smart Software Manager 定期およびオンプレミス PID：

- Essentials：L-F9K-ASA=。必須。
- 10 コンテキスト：L-F9K-ASA-SC-10=。コンテキストライセンスは追加的です。複数のライセンスを購入します。
- キャリア（Diameter、GTP/GPRS、M3UA、SCTP）：L-F9K-ASA-CAR=
- 高度暗号化（3DES/AES）：L-F9K-ASA-ENCR-K9=。アカウントに強力な暗号が承認されていない場合にのみ必要です。

Firepower 9300 永続ライセンス予約 PID：

永続ライセンスには、高度暗号化（3DES/AES）ライセンス（アカウントに資格がある場合）を含むすべての機能が含まれます。セキュアクライアント の使用権を有効にする セキュアクライアント ライセンスを購入すれば、セキュアクライアント の機能もプラットフォームの上限まで有効になります（Secure Client Advantage、Secure Client Premier、およびSecure Client VPN のみライセンス （103 ページ）を参照）。

- L-FPR9K-ASA-BPU=

スマート ソフトウェア ライセンシングのモニタリング

デバッグ メッセージをイネーブルにするだけでなく、ライセンスの機能、ステータス、および証明書をモニターすることもできます。

現在のライセンスの表示

ライセンスを表示するには、次の コマンドを参照してください。

- **show license features**

  次に、Essentialsライセンスのみ（現在のソフトウェア利用資格なし）の ASA 仮想 の例を示します。

```
Serial Number:  9AAHGX8514R

ASAv Platform License State: Unlicensed
No active entitlement: no feature tier configured

Licensed features for this platform:
Maximum Physical Interfaces       : 10             perpetual
Maximum VLANs                     : 50             perpetual
Inside Hosts                      : Unlimited      perpetual
Failover                          : Active/Standby perpetual
Encryption-DES                    : Enabled        perpetual
Encryption-3DES-AES               : Enabled        perpetual
Security Contexts                 : 0              perpetual
GTP/GPRS                          : Disabled       perpetual
AnyConnect Premium Peers          : 2              perpetual
AnyConnect Essentials             : Disabled       perpetual
Other VPN Peers                   : 250            perpetual
Total VPN Peers                   : 250            perpetual
Shared License                    : Disabled       perpetual
AnyConnect for Mobile             : Disabled       perpetual
AnyConnect for Cisco VPN Phone    : Disabled       perpetual
Advanced Endpoint Assessment      : Disabled       perpetual
UC Phone Proxy Sessions           : 2              perpetual
Total UC Proxy Sessions           : 2              perpetual
Botnet Traffic Filter             : Enabled        perpetual
Intercompany Media Engine         : Disabled       perpetual
Cluster                           : Disabled       perpetual
```

スマート ライセンス ステータスの表示

ライセンス ステータスを表示するには、次のコマンドを参照してください。

- **すべてのライセンスの表示**

  スマート ソフトウェア ライセンシング、スマート エージェントのバージョン、UDI 情報、スマートエージェントの状態、グローバル コンプライアンス ステータス、資格ステータス、使用許可証明書情報および予定のスマート エージェント タスクを表示します。

  次の例は、ASA 仮想 ライセンスを示しています。

```
ciscoasa# show license all
Smart Licensing Status
======================

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
```

```
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 21 21:17:35 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 21 21:17:35 2015 UTC
  Next Communication Attempt: Sep 24 00:44:10 2015 UTC
  Communication Deadline: Dec 20 21:14:33 2015 UTC

License Usage
==============

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:ASAv,SN:9AHV3KJBEKE

Agent Version
=============
Smart Agent for Licensing: 1.6_reservation/36
```

- **show license status**

  スマート ライセンスのステータスを表示します。

  次に、通常のスマート ソフトウェア ライセンシングを使用する ASA 仮想 のステータスの例を示します。

```
ciscoasa# show license status

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Initial Registration: SUCCEEDED on Sep 21 20:26:29 2015 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:28 2016 UTC
  Registration Expires: Sep 20 20:23:25 2016 UTC

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC
  Last Communication Attempt: SUCCEEDED on Sep 23 01:41:26 2015 UTC
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC
  Communication Deadline: Dec 22 01:38:25 2015 UTC
```

  次に、永続ライセンス予約を使用する ASA 仮想 のステータスの例を示します。

```
ciscoasa# show license status

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jan 28 16:42:45 2016 UTC

License Authorization:
  Status: AUTHORIZED - RESERVED on Jan 28 16:42:45 2016 UTC

Licensing HA configuration error:
    No Reservation Ha config error
```

- **show license summary**

  スマート ライセンスのステータスと使用量のサマリーを表示します。

  次に、通常のスマート ソフトウェア ライセンシングを使用する ASA 仮想 のサマリーの例を示します。

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: ASA
  Virtual Account: ASAv Internal Users
  Export-Controlled Functionality: Not Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Mar 19 20:26:29 2016 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Oct 23 01:41:26 2015 UTC

License Usage:
  License                 Entitlement tag               Count Status
  -----------------------------------------------------------------------------
  regid.2014-08.com.ci... (ASAv-STD-1G)                     1 AUTHORIZED
```

  次に、永続ライセンス予約を使用する ASA 仮想 のサマリーの例を示します。

```
ciscoasa# show license summary

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed

License Authorization:
  Status: AUTHORIZED - RESERVED
```

- **show license usage**

  スマート ライセンスの使用量を表示します。

  次に、ASA 仮想 の使用状況の例を示します。

```
ciscoasa# show license usage

License Authorization:
  Status: AUTHORIZED on Sep 23 01:41:26 2015 UTC

regid.2014-08.com.cisco.ASAv-STD-1G,1.0_4fd3bdbd-29ae-4cce-ad82-45ad3db1070c
(ASAv-STD-1G):
  Description: This entitlement tag was created via Alpha Extension application
  Count: 1
  Version: 1.0
  Status: AUTHORIZED
```

UDI の表示

ユニバーサル製品識別子（UDI）を表示するには、次のコマンドを参照してください。

show license udi

次に、ASAv の UDI の例を示します。

```
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
ciscoasa#
```

スマート ソフトウェア ライセンスのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug license agent** {**error** | **trace** | **debug** | **all**}

  スマート エージェントからのデバッグをオンにします。

- **debug license** *level*

  Smart Software Licensing Manager のデバッグの各種レベルをオンにします。

Smart Software Manager 通信

このセクションでは、デバイスが Smart Software Manager と通信する方法について説明します。

デバイスの登録とトークン

各仮想アカウントに登録トークンを作成できます。このトークンは、デフォルトで 30 日間有効です。各デバイスを導入するとき、または既存のデバイスを登録するときにこのトークン ID と権限付与レベルを入力します。既存のトークンの有効期限が切れている場合は、新しいトークンを作成できます。

（注） Firepower 4100/9300 シャーシ：デバイス登録は、ASA 論理デバイス上ではなく、シャーシで設定されます。

展開後の起動時、または既存のデバイスでこれらのパラメータを手動で設定した後、デバイスは Smart Software Manager に登録されます。トークンを使用してデバイスを登録すると、Smart Software Manager はデバイスと Smart Software Manager 間の通信用の ID 証明書を発行します。この証明書の有効期間は 1 年ですが、6 か月ごとに更新されます。

Smart Software Manager との定期的な通信

デバイスは、30 日ごとに Smart Software Manager と通信します。Smart Software Manager に変更を加えた場合は、デバイス上で許可を更新し、すぐに変更されるようにすることができます。または、スケジュールどおりにデバイスが通信するのを待ちます。

必要に応じて、HTTP プロキシを設定できます。

ASA 仮想

ASA 仮想では、少なくとも 90 日おきに、直接接続または HTTP プロキシを介したインターネットアクセスが必要です。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間遵守が維持されます。猶予期間終了後は、Smart Software Manager に連絡する必要があり、そうしないと ASA 仮想 がコンプライアンス違反の状態になります。その他の操作には影響ありません。

他のすべてのモデル

ASA は直接または HTTP プロキシ経由で少なくとも 90 日ごとにインターネット アクセスを行う必要があります。通常のライセンス通信が 30 日ごとに行われますが、猶予期間によって、デバイスは Call Home なしで最大 90 日間動作します。猶予期間後、Smart Software Manager に連絡しない限り、特別なライセンスを必要とする機能の設定変更を行えませんが、動作には影響ありません。

コンプライアンス逸脱状態

次の状況では、デバイスがコンプライアンスから逸脱している可能性があります。

- 使用超過：デバイスが利用できないライセンスを使用している場合。

- ライセンスの期限切れ：時間ベースのライセンスの期限が切れている場合。
- 通信の欠落：デバイスが再許可を得るために Licensing Authority に到達できない場合。

アカウントのステータスがコンプライアンス違反状態なのか、違反状態に近づいているのかを確認するには、デバイスで現在使用中の権限付与とスマートアカウントのものを比較する必要があります。

コンプライアンス違反状態では、モデルによってはデバイスが制限されている可能性があります。

- ASA 仮想：ASA 仮想 は影響を受けません。
- すべての他のモデル：特別なライセンスが必要な機能への設定変更はできなくなりますが、動作には影響ありません。たとえば、Essentialsのライセンス制限を超える既存のコンテキストは実行を継続でき、その構成を変更することもできますが、新しいコンテキストを追加することはできません。最初の登録時に十分なEssentialsライセンスがない場合、高度な暗号化機能を含むライセンス機能を設定できません。

Smart Call Home インフラストラクチャ

デフォルトでは、Smart Call Home のプロファイルは、Smart Software Manager の URL を指定する設定内にあります。このプロファイルは削除できません。ライセンスプロファイルの設定可能なオプションは、Smart Software Manager の宛先アドレス URL のみであることに注意してください。Cisco TAC に指示されない限り、Smart Software Manager の URL は変更しないでください。

（注） Firepower 4100/9300 シャーシ の場合、ライセンスの Smart Call Home は ASA ではなく Firepower 4100/9300 シャーシ スーパバイザで設定されます。

スマート ソフトウェア ライセンスの Smart Call Home をディセーブルにすることはできません。たとえば、**no service call-home** コマンドを使用して Smart Call Home を無効化しても、スマート ソフトウェア ライセンシングは無効化されません。

他の Smart Call Home の機能は、特に設定しない限り、有効になりません。

スマート ライセンス証明書の管理

ASA はスマート転送または、Smart Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。サーバー証明書を発行する階層が変更される場合、サービスの中断を防ぐため、定期的な trustpool バンドルの自動更新が有効になるように、**auto-update** コマンドを構成します。

スマート ライセンス サーバーから受信したサーバー証明書は、[Extended Key Usage] フィールドに「ServAuth」が含まれていなければなりません。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

Smart Software Licensing の履歴

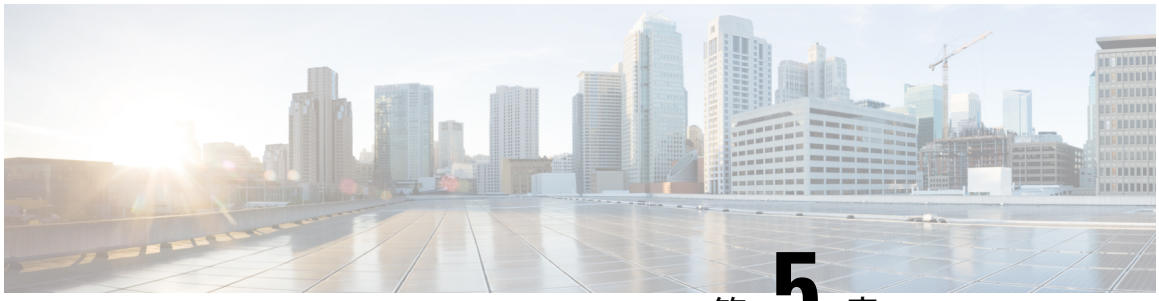
機能名	プラットフォーム リリース	説明
Secure Firewall 4200 の最大接続数の引き上げ	9.23(1)	最大接続数が引き上げられました。 • 4225：3,000 万 → **9,000 万** • 4245：6,000 万 → **18,000 万**
ASA 仮想 柔軟な永続ライセンスの予約	9.23(1)	柔軟な永続ライセンスの予約では、 ASA 仮想に割り当てられた RAM および vCPU に関係なく、モデル固有のライセンスを設定できます。 モデルライセンスは ASA 仮想 のスループットレベルを設定し、ASA 仮想 のメモリは最大 セキュアクライアント セッション、TLS プロキシセッション、最大同時ファイアウォール接続、および VLAN を決定します。ただし、ASA 仮想 メモリプロファイルを小さくすると、セッションと機能の実際の数が制限されます。 新規/変更されたコマンド：**license smart flex-model**、**show license features**
すべての Cisco Secure Firewall 1200 モデルでマルチ コンテキストをサポート	9.23(1)	マルチ コンテキスト モードのサポートが追加されました。Cisco Secure Firewall 1210/1220 • Cisco Secure Firewall 1210CE-5 コンテキスト。 • Cisco Secure Firewall 1210CP：5 コンテキスト。 • Cisco Secure Firewall 1220CX：10 コンテキスト。 スイッチポートはマルチ コンテキスト モードではサポートされていません。マルチ コンテキスト モードに変換する前に、すべてのインターフェイスをルータ インターフェイスに変換する必要があります。 Cisco Secure Firewall 1230/1240/1250 も最初のリリースでマルチ コンテキスト モードをサポートしています。 • Cisco Secure Firewall 1230：25 コンテキスト。 • Cisco Secure Firewall 1240：25 コンテキスト。 • Cisco Secure Firewall 1250：25 コンテキスト。

機能名	プラットフォーム リリース	説明
スマート トランスポートは、CSSM サーバーと通信するためのデフォルトのトランスポート メカニズムです。	9.22(1)	スマートライセンスでは現在、デフォルトの転送として Smart Transport を使用しています。必要に応じて、旧タイプの Smart Call Home を任意で有効にできます。 新規/変更されたコマンド：**transport proxy**、**transport type**、**transport url**
ASAvU ライセンス	9.22(1)	ASAvU ライセンスは、32 コアおよび 64 コアの展開で最大のスループットを実現します。このライセンスは、VMware および KVM でのみサポートされています。 新規/変更されたコマンド： **throughput level unlimited**
Secure Firewall 4200 の最大接続数の引き上げ	9.20(2)	最大接続数が引き上げられました。 • 4215：15M → **40M** • 4225：30M → **80M** • 4245：60M → **80M**
キャリアライセンスの Secure Firewall 3100 サポート	9.18(1)	キャリアライセンスは、Diameter、GTP/GPRS、SCTP 検査を有効にします。 新規/変更されたコマンド： **feature carrier**
ASAv100 永続ライセンス予約	9.14(1.30)	ASAv100 で製品 ID L-ASAV100SR-K9= を使用した永続ライセンス予約がサポートされるようになりました。**注**：すべてのアカウントが永続ライセンス予約について承認されているわけではありません。
ASA 仮想 MSLA サポート	9.13(1)	ASA 仮想 は、シスコのマネージド サービス ライセンス契約（MSLA）プログラムをサポートしています。このプログラムは、マネージド ソフトウェア サービスをサード パーティに提供するシスコのお客様およびパートナー向けに設計された、ソフトウェアのライセンスおよび消費のフレームワークです。 MSLAはスマートライセンスの新しい形式で、ライセンス スマート エージェントは時間単位でライセンス権限付与の使用状況を追跡します。 新規/変更されたコマンド：**license smart**、**mode**、**utility**、**custom-id**、**custom-info**、**privacy**、**transport type**、**transport url**、**transport proxy**

機能名	プラットフォーム リリース	説明
ASA 仮想 柔軟なライセンス	9.13(1)	すべての ASA 仮想 ライセンスは、サポートされているすべての ASA 仮想 vCPU/メモリ構成で使用できるようになりました。セキュアクライアント および TLS プロキシのセッション制限は、モデルタイプに関連付けられたプラットフォーム制限ではなく、インストールされた ASA 仮想 プラットフォームの権限付与によって決まります。 新規/変更されたコマンド： **show version**、**show vm**、**show cpu**、**show license features**
Firepower 4100/9300 シャーシのフェールオーバー ペアのライセンスの変更	9.7(1)	アクティブなユニットのみがライセンス権限を要求します。以前は、両方のユニットがライセンスの権限付与を要求していました。FXOS 2.1.1 でサポートされます。
ASA 仮想 の短かい文字列の拡張機能向けの永続ライセンス予約	9.6(2)	スマート エージェント（1.6.4 への）の更新により、要求と認証コードには短い文字列が使用されます。 変更されたコマンドはありません。
ASA 仮想 のサテライトサーバーのサポート	9.6(2)	デバイスがセキュリティ上の理由でインターネットにアクセスができない場合、オプションで、仮想マシン（VM）としてローカル Smart Software Manager サテライト サーバーをインストールできます。 変更されたコマンドはありません。
Firepower 4100/9300 シャーシ 上の ASA の永続ライセンス予約	9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、FirePOWER 9300 および FirePOWER 4100 の ASA 用に永続ライセンスを要求できます。永続ライセンスには、標準層、高度暗号化（該当する場合）、セキュリティ コンテキスト、キャリア ライセンスをはじめ、使用可能なすべてのライセンス権限が含まれます。FXOS 2.0.1 が必要です。 すべての設定はFirepower 4100/9300 シャーシで実行され、ASA の設定は不要です。
ASA 仮想 の永続ライセンス予約	9.5(2.200) 9.6(2)	Cisco Smart Software Manager との通信が許可されていない非常にセキュアな環境では、ASA 仮想 用に永続ライセンスを要求できます。 9.6(2) では、Amazon Web Services の ASA 仮想 向けに、この機能のサポートが追加されました。この機能は Microsoft Azure ではサポートされません。 次のコマンドが導入されました。**license smart reservation**、**license smart reservation cancel**、**license smart reservation install**、**license smart reservation request universal**、**license smart reservation return**

機能名	プラットフォーム リリース	説明
スマート エージェントの v1.6 へのアップグレード	9.5(2.200) 9.6(2)	スマート エージェントはバージョン 1.1 からバージョン 1.6 へアップグレードされました。このアップグレードは永続ライセンス予約をサポートするほか、ライセンス アカウントに設定された権限に従って、高度暗号化（3DES/AES）ライセンス権限の設定もサポートします。 （注） バージョン 9.5 （2.200）からダウングレードした場合、ASA 仮想 はライセンス登録状態を保持しません。**license smart register idtoken** *id_token* **force** コマンドを使用し、再登録する必要があります。Smart Software Manager から ID トークンを取得します。 次のコマンドが導入されました。**show license status**、**show license summary**、**show license udi**、**show license usage** 次のコマンドが変更されました。**show license all**、**show tech-support license** 次のコマンドが非推奨になりました。 **show license cert**、**show license entitlement**、**show license pool**、**show license registration**
FirePOWER 9300 の ASA に高度暗号化（3DES）ライセンスを自動的に適用	9.5(2.1)	通常の Cisco Smart Software Manager（SSM）ユーザーの場合、FirePOWER 9300 で登録トークンを適用すると、対象となるお客様には強力な暗号化ライセンスが自動的に有効になります。 （注） スマート ソフトウェア マネージャ サテライトが導入されている場合、ASDM や他の高度暗号機能を使用するには、ASA の展開後に ASA CLI を使用して、高度暗号化ライセンスを有効にする必要があります。 この機能には、FXOS 1.1.3 が必要です。 サテライト以外の構成では、次のコマンドが除去されました。**feature strong-encryption**
サーバー証明書の発行階層が変更された場合の Smart Call Home/スマート ライセンス証明書の検証	9.5(2)	スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを最初に設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA はサーバー証明書の発行階層が変更された場合の証明書の検証をサポートします。トラストプール バンドルの定期的な自動更新を有効にできます。 次のコマンドが導入されました。**auto-import**

機能名	プラットフォーム リリース	説明
新しいキャリア ライセンス	9.5(2)	新しいキャリア ライセンスは既存の GTP/GPRS ライセンスを置き換え、SCTP と Diameter インスペクションもサポートします。Firepower 9300 上の ASA の場合、**feature mobile-sp** コマンドは **feature carrier** コマンドに自動的に移行します。 次のコマンドが導入または変更されました。**feature carrier**、**show activation-key**、**show license**、**show tech-support**、**show version**
FirePOWER 9300 の ASA のシスコ スマート ソフトウェア ライセンシング	9.4(1.150)	FirePOWER 9300 に ASA のシスコ スマート ソフトウェア ライセンシングが導入されました。 次のコマンドが導入されました。**feature strong-encryption**、**feature mobile-sp**、**feature context**
ASA 仮想 のシスコ スマート ソフトウェア ライセンス	9.3(2)	Smart Software Licensing では、ライセンスのプールを購入して管理することができます。PAK ライセンスとは異なり、スマート ライセンスは特定のシリアル番号に関連付けられません。各ユニットのライセンスキーを管理しなくても、簡単に ASA 仮想 を展開したり使用を終了したりできます。スマート ソフトウェア ライセンスを利用すれば、ライセンスの使用状況と要件をひと目で確認することもできます。 **clear configure license**、**debug license agent**、**feature tier**、**http-proxy**、**license smart**、**license smart deregister**、**license smart register**、**license smart renew**、**show license**、**show running-config license**、**throughput level** 各コマンドが導入されました。



第 5 章

論理デバイス Firepower 4100/9300

Firepower 4100/9300は柔軟なセキュリティ プラットフォームが 1 つまたは複数の論理デバイスをインストールすることができます。この章では、基本的なインターフェイスの設定、および Firewall Chassis マネージャ を使用したスタンドアロンまたはハイ アベイラビリティ論理デバイスの追加方法について説明します。クラスタ化された論理デバイスを追加する場合は、Firepower 4100/9300 の ASA クラスタ （525 ページ）を参照してください。FXOS CLI を使用するには、FXOS CLI コンフィギュレーション ガイドを参照してください。高度な FXOS の手順とトラブルシューティングについては、FXOS コンフィギュレーション ガイドを参照してください。

- インターフェイスについて （205 ページ）
- 論理デバイスについて （210 ページ）
- のハードウェアとソフトウェアの要件と前提条件 （210 ページ）
- 論理デバイスに関する注意事項と制約事項 （212 ページ）
- インターフェイスの設定 （213 ページ）
- 論理デバイスの設定 （219 ページ）
- 論理デバイスの履歴 （229 ページ）

インターフェイスについて

Firepower 4100/9300 シャーシ は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスをサポートします。EtherChannel のインターフェイスには、同じタイプのメンバ インターフェイスを最大で 16 個含めることができます。

シャーシ管理インターフェイス

シャーシ管理インターフェイスは、SSH または Firewall Chassis マネージャ によって、FXOS シャーシの管理に使用されます。このインターフェイスは、アプリケーション管理の論理デバイスに割り当てる管理タイプのインターフェイスから分離されています。

このインターフェイスのパラメータを設定するには、CLI から設定にする必要があります。このインターフェイスについての情報を FXOS CLI で表示するには、ローカル管理に接続し、管理ポートを表示します。

FirePOWER **connect local-mgmt**

firepower(local-mgmt) # **show mgmt-port**

物理ケーブルまたはSFPモジュールが取り外されている場合や、**mgmt-port shut** コマンドが実行されている場合や、論理デバイスがオフラインになっている場合でも、シャーシ管理インターフェイスは稼働状態のままである点に注意してください。

（注） シャーシ管理インターフェイスはジャンボフレームをサポートしていません。

インターフェイス タイプ

物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスは、次のいずれかのタイプになります。

- Data：通常のデータに使用します。データインターフェイスを論理デバイス間で共有することはできません。また、論理デバイスからバックプレーンを介して他の論理デバイスに通信することはできません。データインターフェイスのトラフィックの場合、すべてのトラフィックは別の論理デバイスに到達するために、あるインターフェイスでシャーシを抜け出し、別のインターフェイスで戻る必要があります。
- Data-sharing：通常のデータに使用します。コンテナインスタンスでのみサポートされ、これらのデータインターフェイスは 1 つまたは複数の論理デバイス/コンテナインスタンス（Firewall Threat DefenseFirewall Management Center 専用）で共有できます。
- Mgmt：アプリケーション インスタンスの管理に使用します。これらのインターフェイスは、外部ホストにアクセスするために1つまたは複数の論理デバイスで共有できます。論理デバイスが、このインターフェイスを介して、インターフェイスを共有する他の論理デバイスと通信することはできません。各論理デバイスには、管理インターフェイスを1つだけ割り当てることができます。アプリケーションと管理によっては、後でデータインターフェイスから管理を有効にできます。ただし、データ管理を有効にした後で使用する予定がない場合でも、管理インターフェイスを論理デバイスに割り当てる必要があります。個別のシャーシ管理インターフェイスについては、シャーシ管理インターフェイス（205 ページ）を参照してください。

（注） 管理インターフェイスを変更すると、論理デバイスが再起動します。たとえば、e1/1 から e1/2 に1回変更すると、論理デバイスが再起動して新しい管理が適用されます。

- Eventing： Firewall Management Center デバイスを使用した Firewall Threat Defense のセカンダリ管理インターフェイスとして使用します。

（注） 各アプリケーションインスタンスのインストール時に、仮想イーサネットインターフェイスが割り当てられます。アプリケーションがイベントインターフェイスを使用しない場合、仮想インターフェイスは管理上ダウンの状態になります。

```
Firepower # show interface Vethernet775
Firepower # Vethernet775 is down (Administratively down)
Bound Interface is Ethernet1/10
Port description is server 1/1, VNIC ext-mgmt-nic5
```

- Cluster：クラスタ化された論理デバイスのクラスタ制御リンクとして使用します。デフォルトでは、クラスタ制御リンクは 48 番のポートチャネル上に自動的に作成されます。クラスタタイプは、EtherChannel インターフェイスのみでサポートされます。

スタンドアロン展開とクラスタ展開での Firewall Threat Defense および ASA アプリケーションのインターフェイスタイプのサポートについては、次の表を参照してください。

表 *3:* インターフェイスタイプのサポート

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
Firewall Threat Defense	スタンドアロン ネイティブ インスタンス	対応	—	—	—	○	○	—	—
	スタンドアロン コンテナ インスタンス	○	○	○	○	○	○	—	—
	クラスタ ネイティブ インスタンス	[はい（Yes）] に設定（シャーシ間クラスタリング専用の EtherChannel）	—	—	—	○	○	○	—
	クラスタ コンテナ インスタンス	[はい（Yes）] に設定（シャーシ間クラスタリング専用の EtherChannel）	—	—	—	○	○	○	○

アプリケーション		データ	データ：サブインターフェイス	データ共有	データ共有：サブインターフェイス	管理	イベント（Eventing）	クラスタ（EtherChannel のみ）	クラスタ：サブインターフェイス
ASA	スタンドアロン ネイティブ インスタンス	対応	—	—	—	対応	—	対応	—
	クラスタ ネイティブ インスタンス	[はい（Yes）] に設定 （シャーシ間クラスタリング専用の EtherChannel）	—	—	—	対応	—	対応	—

FXOS インターフェイスとアプリケーション インターフェイス

Firepower 4100/9300 は、物理インターフェイスおよび EtherChannel（ポートチャネル）インターフェイスの基本的なイーサネット設定を管理します。アプリケーション内で、より高いレベルの設定を行います。たとえば、FXOS では Etherchannel のみを作成できます。ただし、アプリケーション内の EtherChannel に IP アドレスを割り当てることができます。

続くセクションでは、インターフェイスの FXOS とアプリケーションの連携について説明します。

VLAN サブインターフェイス

すべての論理デバイスで、アプリケーション内に VLAN サブインターフェイスを作成できます。

シャーシとアプリケーションの独立したインターフェイスの状態

管理上、シャーシとアプリケーションの両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティングシステムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるため、シャーシとアプリケーションの間で不一致が発生することがあります。

論理デバイスについて

論理デバイスでは、1 つのアプリケーション インスタンス（ASA または Firewall Threat Defense のいずれか）および 1 つのオプション デコレータ アプリケーション（Radware DefensePro）を実行し、サービスチェーンを形成できます。

論理デバイスを追加する場合は、アプリケーション インスタンス タイプとバージョンを定義し、インターフェイスを割り当て、アプリケーション設定に送信されるブートストラップ設定を構成することもできます。

（注） Firepower 9300 の場合、異なるアプリケーションタイプ（ASA および Firewall Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

スタンドアロン論理デバイスとクラスタ化論理デバイス

次の論理デバイス タイプを追加できます。

- スタンドアロン：スタンドアロン論理デバイスは、スタンドアロン ユニットまたはハイアベイラビリティ ペアのユニットとして動作します。
- クラスタ：クラスタ化論理デバイスを使用すると複数の装置をグループ化することで、単一デバイスのすべての利便性（管理、ネットワークへの統合）を提供し、同時に複数デバイスによる高いスループットと冗長性を実現できます。Firepower 9300 などの複数のモジュール デバイスが、シャーシ内クラスタリングをサポートします。Firepower 9300 の場合、3 つすべてのモジュールがネイティブインスタンスとコンテナインスタンスの両方のクラスタに参加する必要があります。

のハードウェアとソフトウェアの要件と前提条件

Firepower 4100/9300では、複数のモデル、セキュリティモジュール、アプリケーションタイプ、および高可用性と拡張性の機能がサポートされています。可能な組み合わせについては、次の要件を参照してください。

Firepower 9300の要件

Firepower 9300 には、3 つのセキュリティモジュール スロットと複数タイプのセキュリティモジュールが実装されています。次の要件を確認します。

- セキュリティモジュール タイプ：Firepower 9300 には、さまざまなタイプのモジュールをインストールできます。たとえば、SM-48 をモジュール 1、SM-40 をモジュール 2 、SM-56 をモジュール 3 としてインストールできます。

- ネイティブインスタンスとコンテナインスタンス：セキュリティモジュールにコンテナインスタンスをインストールする場合、そのモジュールは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはモジュールのすべてのリソースを使用するため、モジュールにはネイティブインスタンスを1つのみインストールできます。一部のモジュールでネイティブインスタンスを使用し、その他のモジュールでコンテナインスタンスを使用することができます。たとえば、モジュール1とモジュール2にネイティブインスタンスをインストールできますが、モジュール3にはコンテナインスタンスをインストールできます。
- クラスタリング：クラスタ内またはシャーシ間であるかどうかにかかわらず、クラスタ内のすべてのセキュリティモジュールは同じタイプである必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシにインストールされているセキュリティモジュールの数はさまざまでかまいません。たとえば、シャーシ1に2つのSM-40を、シャーシ2に3つのSM-40をインストールできます。 同じシャーシに1つのSM-48および2つのSM-40をインストールする場合、クラスタリングは使用できません。
- 高可用性：高可用性はFirepower 9300の同じタイプのモジュール間でのみサポートされています。 ただし、2つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシにはSM-40、SM-48、およびSM-56があります。SM-40モジュール間、SM-48モジュール間、およびSM-56モジュール間にハイアベイラビリティペアを作成できます。
- ASAおよびFirewall Threat Defenseのアプリケーションタイプ：異なるアプリケーションタイプをシャーシ内の別個のモジュールにインストールすることができます。たとえば、モジュール1とモジュール2にASAをインストールし、モジュール3にFirewall Threat Defenseをインストールすることができます。
- ASAまたはFirewall Threat Defenseのバージョン：個別のモジュールで異なるバージョンのアプリケーション インスタンス タイプを実行することも、同じモジュール上の個別のコンテナインスタンスとして実行することもできます。たとえば、モジュール1にFirewall Threat Defense 6.3を、モジュール2にFirewall Threat Defense 6.4を、モジュール3にFirewall Threat Defense 6.5をインストールできます。

Firepower 4100の要件

Firepower 4100には複数のモデルがあります。次の要件を確認します。

- ネイティブインスタンスとコンテナインスタンス：Firepower 4100にコンテナインスタンスをインストールする場合、そのデバイスは他のコンテナインスタンスのみをサポートできます。ネイティブインスタンスはデバイスのすべてのリソースを使用するため、デバイスにはネイティブ インスタンスを1つのみインストールできます。
- クラスタリング ：クラスタ内のすべてのシャーシが同じモデルである必要があります。
- 高可用性：高可用性は同じタイプのモデル間でのみサポートされています。
- ASAおよびFirewall Threat Defenseのアプリケーションタイプ：Firepower 4100は、1つのアプリケーションタイプのみを実行できます。

論理デバイスに関する注意事項と制約事項

ガイドラインと制限事項については、以下のセクションを参照してください。

インターフェイスに関する注意事項と制限事項

デフォルトの MAC アドレス

デフォルトのMACアドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスでは、Burned-In MAC Address を使用します。
- EtherChannel: EtherChannelの場合は、そのチャネルグループに含まれるすべてのインターフェイスが同じMACアドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは1つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャネル インターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。

一般的なガイドラインと制限事項

ファイアウォール モード

Firewall Threat Defenseと ASA のブートストラップ設定でファイアウォール モードをルーテッドまたはトランスペアレントに設定できます。

ハイ アベイラビリティ

- アプリケーション設定内で高可用性を設定します。
- 任意のデータ インターフェイスをフェールオーバー リンクおよびステート リンクとして使用できます。 データ共有インターフェイスはサポートされていません。

コンテキストモード

- 展開後に、ASA のマルチ コンテキスト モードを有効にします。

ハイアベイラビリティの要件と前提条件

- ハイ アベイラビリティ フェールオーバーを設定される 2 つのユニットは、次の条件を満たしている必要があります。

- 個別のシャーシ上にあること。Firepower 9300 のシャーシ内ハイアベイラビリティはサポートされません。
- 同じモデルであること。
- 高可用性論理デバイスに同じインターフェイスを割り当てること。
- インターフェイスの数とタイプが同じであること。ハイアベイラビリティを有効にする前に、すべてのインターフェイスを FXOS で事前に同じ設定にすること。

- ハイアベイラビリティは Firepower 9300 の同じタイプのモジュール間でのみサポートされますが、2 つのシャーシに混在モジュールを含めることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。
- その他のハイ アベイラビリティ システム要件については、フェールオーバー のシステム要件 （316 ページ）を参照してください。

インターフェイスの設定

デフォルトでは、物理インターフェイスは無効になっています。インターフェイスの有効化、Etherchannel の追加、VLAN サブインターフェイスの、インターフェイスプロパティの編集、を実行できます。

（注） FXOS でインターフェイスを削除した場合（たとえば、ネットワークモジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 構成では元のコマンドが保持されます。構成からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

物理インターフェイスの設定

インターフェイスを物理的に有効および無効にすること、およびインターフェイスの速度とデュプレックスを設定することができます。インターフェイスを使用するには、インターフェイスをFXOS で物理的に有効にし、アプリケーションで論理的に有効にする必要があります。

（注）
- QSFPH40G-CUxM の場合、自動ネゴシエーションはデフォルトで常に有効になっており、無効にすることはできません。
- ポートの SFP を別の SFP モジュールに交換しても、インターフェイスの速度、デュプレックス、および自動ネゴシエーションは自動的に更新されません。インターフェイスを再構成する必要があります。

始める前に

- すでに EtherChannel のメンバーであるインターフェイスは個別に変更できません。EtherChannel に追加する前に、設定を行ってください。

手順

ステップ 1 インターフェイスモードに入ります。

scope eth-uplink

scope fabric a

ステップ 2 インターフェイスを有効にします。

enter interface *interface_id*

enable

例：

```
Firepower /eth-uplink/fabric # enter interface Ethernet1/8
Firepower /eth-uplink/fabric/interface # enable
```

（注）
すでにポートチャネルのメンバであるインターフェイスは個別に変更できません。ポートチャネルのメンバであるインターフェイスで **enter interface** コマンドまたは **scope interface** コマンドを使用すると、オブジェクトが存在しないことを示すエラーを受け取ります。ポートチャネルに追加する前に、**enter interface** コマンドを使用してインターフェイスを編集する必要があります。

ステップ 3 （任意）デバウンス時間を設定します。

set debounce-time 5000 {Enter a value between 0-15000 milli-seconds}

例：

```
Firepower /eth-uplink/fabric/interface # set debounce-time 5000
```

例：

（注）
デバウンス時間の設定は、1G インターフェイスではサポートされていません。

ステップ 4 （オプション）インターフェイスタイプを設定します。

set port-type {**data** | **mgmt** | **cluster**}

例：

```
Firepower /eth-uplink/fabric/interface # set port-type mgmt
```

data キーワードがデフォルトのタイプです。**cluster** キーワードは選択しないでください。デフォルトでは、クラスタ制御リンクはポートチャネル 48 に自動的に作成されます。

ステップ 5 インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

set auto-negotiation {**on** | **off**}

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 6 インターフェイスの速度を設定します。

set admin-speed {**1gbps** | **10gbps** | **40gbps** | **100gbps**}

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-speed 1gbps
```

ステップ 7 インターフェイスのデュプレックスモードを設定します。

set admin-duplex {**fullduplex** | **halfduplex**}

例：

```
Firepower /eth-uplink/fabric/interface* # set admin-duplex halfduplex
```

ステップ 8 デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。

set flow-control-policy *name*

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

ステップ 9 設定を保存します。

commit-buffer

例：

```
Firepower /eth-uplink/fabric/interface* # commit-buffer
Firepower /eth-uplink/fabric/interface #
```

EtherChannel（ポート チャネル）の追加

EtherChannel（ポートチャネルとも呼ばれる）は、同じメディアタイプと容量の最大16個のメンバーインターフェイスを含むことができ、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45またはSFPのいずれかです。異なるタイプ（銅と光ファイバ）のSFPを混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1GBインターフェイスと10GBインターフェイスなど）を混在させることはできません。リンク集約制御プロトコル（LACP）では、2つのネットワークデバイス間でリンク集約制御プロトコルデータユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理データインターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- オン：EtherChannelは常にオンであり、LACPは使用されません。「オン」のEtherChannelは、別の「オン」の EtherChannel のみと接続を確立できます。

（注） モードを [On] から [Active] に変更するか、[Active] から [On] に変更すると、EtherChannel が動作状態になるまで最大 3 分かかることがあります。

非データ インターフェイスのみがアクティブ モードをサポートしています。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

Firepower 4100/9300 シャーシが EtherChannel を作成すると、EtherChannel は [一時停止（Suspended）] 状態（Active LACP モードの場合）または [ダウン（Down）] 状態（On LACP モードの場合）になり、物理リンクがアップしても論理デバイスに割り当てるまでそのままになります。EtherChannel は次のような状況でこの [一時停止（Suspended）] 状態になります。

- EtherChannel がスタンドアロン論理デバイスのデータまたは管理インターフェイスとして追加された
- EtherChannel がクラスタの一部である論理デバイスの管理インターフェイスまたは Cluster Control Link として追加された
- EtherChannelがクラスタの一部である論理デバイスのデータインターフェイスとして追加され、少なくとも 1 つのユニットがクラスタに参加している

EtherChannelは論理デバイスに割り当てるまで動作しないことに注意してください。EtherChannelが論理デバイスから削除された場合や論理デバイスが削除された場合は、EtherChannel が [一時停止（Suspended）] または [ダウン（Down）] 状態に戻ります。

手順

ステップ 1 インターフェイス モードを開始します。

scope eth-uplink

scope fabric a

ステップ 2 ポートチャネルを作成します。

create port-channel *ID*

enable

ステップ 3 メンバ インターフェイスを割り当てます。

create member-port *interface_id*

同じメディアタイプとキャパシティで最大 16 のインターフェイスを追加できます。メンバーインターフェイスは、同じ速度とデュプレックスに設定する必要があり、このポートチャネルに設定した速度とデュプレックスと一致させる必要があります。メディアタイプはRJ-45 またはSFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。容量の大きいインターフェイスで速度を低く設定することによってインターフェイスの容量（1GBインターフェイスと10GBインターフェイスなど）を混在させることはできません。

例：

```
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/1
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/2
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/3
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
Firepower /eth-uplink/fabric/port-channel* # create member-port Ethernet1/4
Firepower /eth-uplink/fabric/port-channel/member-port* # exit
```

ステップ 4 （任意） インターフェイス タイプを設定します。

set port-type {**data** | **mgmt** | **cluster**}

例：

```
Firepower /eth-uplink/fabric/port-channel # set port-type data
```

data キーワードがデフォルトのタイプです。デフォルトの代わりにこのポートチャネルをクラスタ制御リンクとして使用する場合以外は、**cluster** キーワードを選択しないでください。

ステップ 5 ポートチャネルのメンバーに適したインターフェイス速度を設定します。

set speed {**10mbps** | **100mbps** | **1gbps** | **10gbps** | **40gbps** | **100gbps**}

指定した速度ではないメンバーインターフェイスを追加すると、ポートチャネルに正常に参加できません。デフォルトは **10gbps** です。

例：

```
Firepower /eth-uplink/fabric/port-channel* # set speed 1gbps
```

ステップ 6 （任意） ポートチャネルのメンバーに適したデュプレックスを設定します。

set duplex {**fullduplex** | **halfduplex**}

指定したデュプックスのメンバーインターフェイスを追加すると、ポートチャネルに正常に参加されます。デフォルトは **fullduplex** です。

例：

```
Firepower /eth-uplink/fabric/port-channel* # set duplex fullduplex
```

ステップ 7 インターフェイスでサポートされている場合、自動ネゴシエーションを有効化または無効化します。

set auto-negotiation {**on** | **off**}

例：

```
Firepower /eth-uplink/fabric/interface* # set auto-negotiation off
```

ステップ 8 データインターフェイスの LACP ポート チャネル モードを設定します。

非データインターフェイスの場合、モードは常にアクティブです。

set port-channel-mode {**active** | **on**}

例：

```
Firepower /eth-uplink/fabric/port-channel* # set port-channel-mode on
```

ステップ 9 デフォルトのフロー制御ポリシーを編集した場合は、インターフェイスにすでに適用されています。新しいポリシーを作成した場合は、そのポリシーをインターフェイスに適用します。

set flow-control-policy *name*

例：

```
Firepower /eth-uplink/fabric/interface* # set flow-control-policy flow1
```

ステップ 10 設定をコミットします。

commit-buffer

論理デバイスの設定

Firepower 4100/9300 シャーシに、スタンドアロン論理デバイスまたはハイ アベイラビリティ ペアを追加します。

クラスタ リングについては、#unique_225を参照してください。

スタンドアロン ASA の追加

スタンドアロンの論理デバイスは、単独またはハイ アベイラビリティ ペアで動作します。複数のセキュリティモジュールを搭載する Firepower 9300 では、クラスタまたはスタンドアロンデバイスのいずれかを展開できます。クラスタはすべてのモジュールを使用する必要があるため、たとえば、2モジュール クラスタと単一のスタンドアロンデバイスをうまく組み合わせることはできません。

Firepower 4100/9300 シャーシからルーテッドまたはトランスペアレント ファイアウォール モード ASA を展開できます。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

始める前に

- 論理デバイスに使用するアプリケーション イメージを Cisco.com からダウンロードし、そのイメージを Firepower 4100/9300 シャーシ。

（注） Firepower 9300 の場合、異なるアプリケーション タイプ（ASA および Firewall Threat Defense）をシャーシ内の個々のモジュールにインストールできます。別個のモジュールでは、異なるバージョンのアプリケーション インスタンス タイプも実行できます。

- 論理デバイスで使用する管理インターフェイスを設定します。管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理ポートと同じではありません（FXOS では、MGMT、management0 のような名前で表示されます）。
- 次の情報を用意します。
  - このデバイスのインターフェイス Id
  - 管理インターフェイス IP アドレスとネットワークマスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 2 アプリケーション インスタンスのイメージ バージョンを設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号を書き留めます。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
```

b) セキュリティ モジュール/エンジン スロットに範囲を設定します。

scope slot *slot_ID*

slot_id は、Firepower 4100 の場合は常に 1、Firepower 9300 の場合は 1、2、または 3 です。

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot #
```

c) アプリケーション インスタンスを作成します。

enter app-instance asa *devicename*

*Device_name*は、1 ～ 64 文字の範囲で指定できます。このインスタンスの論理デバイスを作成するときに、このデバイス名を使用します。

例：

```
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* #
```

d) ASA イメージバージョンを選択します。

set startup-version *version*

例：

```
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
```

e) スロット モードを終了します。

exit

例：

```
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* #
```

f) 終了して ssa モードにします。

exit

例：

```
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa ASA1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* #
```

ステップ 3 論理デバイスを作成します。

enter logical-device *device_name* **asa** *slot_id* **standalone**

以前に追加したアプリケーション インスタンスと同じ*device_name*を使用します。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1 standalone
Firepower /ssa/logical-device* #
```

ステップ 4 管理インターフェイスとデータインターフェイスを論理デバイスに割り当てます。各インターフェイスに対して、手順を繰り返します。

create external-port-link *name interface_id* **asa**

set description *description*

exit

- *name*：この名前は Firepower 4100/9300 シャーシ スーパーバイザによって使用されます。これは ASA の設定で使用するインターフェイス名ではありません。
- *description*：フレーズを引用符（"）で囲み、スペースを追加します。

管理インターフェイスは、シャーシ管理ポートと同じではありません。ASA のデータ インターフェイスを後で有効にして設定します。これには、IP アドレスの設定も含まれます。

例：

```
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
```

ステップ 5 管理ブートストラップ情報を設定します。

a) ブートストラップ オブジェクトを作成します。

create mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) ファイアウォール モード（「ルーテッド」または「トランスペアレント」）を指定します。

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

ルーテッドモードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォール モードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) admin とイネーブル パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) IPv4 管理インターフェイス設定を設定します。

create ipv4 *slot_id* **default**

set ip *ip_address* **mask** *network_mask*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.10.10.34 mask
255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.10.10.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

e) IPv6 管理インターフェイスを設定します。

create ipv6 *slot_id* **default**

set ip *ip_address* **prefix-length** *prefix*

set gateway *gateway_address*

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv6 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set ip 2001:0DB8:BA98::3210
prefix-length 64
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # set gateway 2001:0DB8:BA98::3211
Firepower /ssa/logical-device/mgmt-bootstrap/ipv6* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

f) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 6 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State（管理状態）] が [Enabled（有効）] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- --------------- ---------------
--------------- ------------ ---------- ------------ --------------- ------------
asa        asa1       2          Disabled    Not Installed                   9.12.1
       Native                    Not Applicable  None
ftd        ftd1       1          Enabled     Online          6.4.0.49        6.4.0.49
       Container   Default-Small Not Applicable  None
```

ステップ 7 セキュリティ ポリシーの設定を開始するには、『ASA 設定ガイド』を参照してください。

例

```
Firepower# scope ssa
Firepower /ssa # scope slot 1
Firepower /ssa/slot # enter app-instance asa MyDevice1
Firepower /ssa/slot/app-instance* # set startup-version 9.10.1
Firepower /ssa/slot/app-instance* # exit
Firepower /ssa/slot* # exit
Firepower /ssa* # create logical-device MyDevice1 asa 1 standalone
Firepower /ssa/logical-device* # create external-port-link inside Ethernet1/1 asa
Firepower /ssa/logical-device/external-port-link* # set description "inside link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link management Ethernet1/7 asa
Firepower /ssa/logical-device/external-port-link* # set description "management link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create external-port-link outside Ethernet1/2 asa
Firepower /ssa/logical-device/external-port-link* # set description "external link"
Firepower /ssa/logical-device/external-port-link* # exit
Firepower /ssa/logical-device* # create mgmt-bootstrap asa
```

```
Firepower /ssa/logical-device/mgmt-bootstrap* # enter bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value transparent
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: secretglassine
Confirm the value: secretglassine
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* # create ipv4 1 default
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set gateway 10.0.0.1
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # set ip 10.0.0.31 mask 255.255.255.0
Firepower /ssa/logical-device/mgmt-bootstrap/ipv4* # exit
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # commit-buffer
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key #
```

ハイ アベイラビリティ ペアの追加

Firewall Threat DefenseASA ハイ アベイラビリティ（フェールオーバーとも呼ばれます）は、FXOS ではなくアプリケーション内で設定されます。ただし、ハイ アベイラビリティのシャーシを準備するには、次の手順を参照してください。

始める前に

フェールオーバー のシステム要件 （316 ページ）を参照してください。

手順

ステップ 1 各論理デバイスに同一のインターフェイスを割り当てます。

ステップ 2 フェールオーバーリンクとステートリンクに 1 つまたは 2 つのデータインターフェイスを割り当てます。

これらのインターフェイスは、2つのシャーシ間で高可用性トラフィックを交換します。フェールオーバーリンクとステートリンクの組み合わせには、10 GB のデータインターフェイスを使用することを推奨します。使用可能なインターフェイスがある場合は、別のフェールオーバーリンクとステートリンクを使用できます。ステートリンクには、最も多くの帯域幅が必要です。フェールオーバーリンクまたはステートリンクに管理タイプのインターフェイスを使用することはできません。シャーシ間でスイッチを使用することをお勧めします。この場合、フェールオーバーインターフェイスと同じネットワークセグメント上に他のデバイスを配置できません。

ステップ 3 論理デバイスで高可用性を有効にします。ハイ アベイラビリティのためのフェールオーバー（315 ページ）を参照してください。

ステップ 4 高可用性を有効にした後にインターフェイスを変更する必要がある場合は、最初にスタンバイユニットで変更を実行してから、アクティブユニットで変更を実行します。

（注）
ASA の場合、FXOS でインターフェイスを削除すると（たとえば、ネットワークモジュールや EtherChannel を削除したり、インターフェイスを EtherChannel に再割り当てしたりすると）、

必要な調整を行うために、ASA設定に元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響を与える可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

ASA 論理デバイスのインターフェイスの変更

ASA論理デバイスでは、管理インターフェイスの割り当て、割り当て解除、または置き換えを行うことができます。ASDM は、新しいインターフェイスを自動的に検出します。

新しいインターフェイスを追加したり、未使用のインターフェイスを削除したりしても、ASA の設定に与える影響は最小限です。ただし、FXOS で割り当てられたインターフェイスを削除する場合（ネットワーク モジュールの削除、EtherChannel の削除、割り当てられたインターフェイスの EtherChannel への再割り当てなど）、そのインターフェイスがセキュリティポリシーで使用されると、削除は ASA の設定に影響を与えます。この場合、ASA 設定では元のコマンドが保持されるため、必要な調整を行うことができます。ASA OS の古いインターフェイス設定は手動で削除できます。

（注） 論理デバイスに影響を与えずに、割り当てられたEtherChannelのメンバーシップを編集できます。

始める前に

- 物理インターフェイスの設定 （213 ページ）およびEtherChannel（ポート チャネル）の追加 （216 ページ）に従って、インターフェイスを設定し、EtherChannel を追加します。
- すでに割り当てられているインターフェイスをEtherChannelに追加する場合(たとえば、すべてのインターフェイスがデフォルトでクラスタに割り当てられる場合)、最初にそのインターフェイスを論理デバイスから割り当て解除してから、EtherChannelに追加する必要があります。新しいEtherChannelの場合、EtherChannelをデバイスに割り当てることができます。
- クラスタ リングまたはフェールオーバーを追加するか、すべてのユニット上のインターフェイスの削除を確認します。最初にデータ/スタンバイユニットでインターフェイスを変更してから、制御/アクティブユニットで変更することをお勧めします。新しいインターフェイスは管理上ダウンした状態で追加されるため、インターフェイスモニタリングに影響を及ぼしません。

手順

ステップ 1 セキュリティ サービス モードを開始します。

Firepower# **scope ssa**

ステップ 2 論理デバイスを編集します。

Firepower /ssa # **scope logical-device** *device_name*

ステップ 3 論理デバイスからインターフェイスの割り当てを解除します。

Firepower /ssa/logical-device # **delete external-port-link** *name*

インターフェイス名を表示するには、**show external-port-link**コマンドを入力します。

管理インターフェイスの場合、新しい管理インターフェイスを追加する前に、現在のインターフェイスを削除し、**commit-buffer** コマンドを使用して変更をコミットします。

ステップ 4 論理デバイスに新しいインターフェイスを割り当てます。

Firepower /ssa/logical-device* # **create external-port-link** *name interface_id* **asa**

ステップ 5 設定を確定します。

commit-buffer

トランザクションをシステムの設定にコミットします。

アプリケーションのコンソールへの接続

アプリケーションのコンソールに接続するには、次の手順を使用します。

手順

ステップ 1 コンソール接続または Telnet 接続を使用して、モジュール CLI に接続します。

connect module *slot_number* {**console** | **telnet**}

複数のセキュリティ モジュールをサポートしないデバイスのセキュリティ エンジンに接続するには、*slot_number* として **1** を使用します。

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

例：

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit
```

```
Firepower-module1>
```

ステップ 2 アプリケーションのコンソールに接続します。

connect asa *name*

インスタンス名を表示するには、名前を付けずにコマンドを入力します。

例：

```
Firepower-module1> connect asa asa1
Connecting to asa(asa1) console... hit Ctrl + A + D  to return to bootCLI
[...]
asa>
```

ステップ 3 アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

- ASA：**Ctrl-a, d** と入力します。

ステップ 4 FXOS CLI のスーパバイザ レベルに戻ります。

コンソールを終了します。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

telnet>**quit**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

例

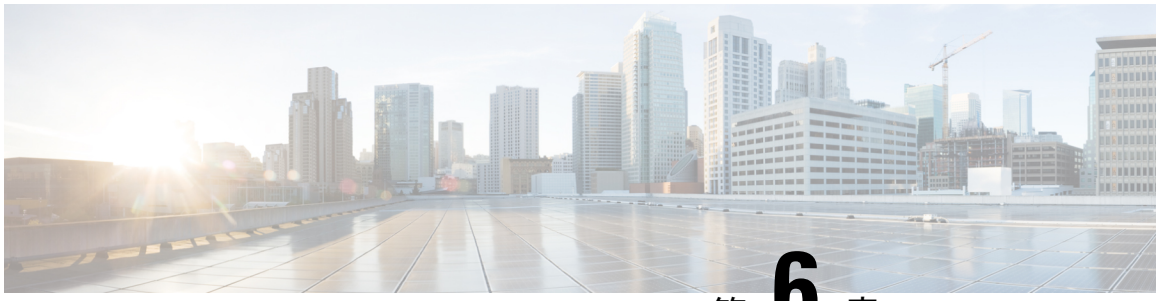
次に、セキュリティ モジュール 1 の ASA に接続してから、FXOS CLI のスーパバイザ レベルに戻る例を示します。

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>connect asa asa1
asa> ~
telnet> quit
Connection closed.
Firepower#
```

論理デバイスの履歴

機能	バージョン	詳細
Firepower 4112 用の ASA	9.14(1)	Firepower 4112 を導入しました。 （注） FXOS 2.8.1 が必要です。
Firepower 9300 SM-56 のサポート	9.12.2	SM-56 セキュリティ モジュールが導入されました。 （注） FXOS 2.6.1.157 が必要です。
Firepower 4115、4125、および 4145 向け ASA	9.12(1)	Firepower 4115、4125、および 4145 が導入されました。 （注） FXOS 2.6.1 が必要です。
Firepower 9300 SM-40 および SM-48 のサポート	9.12.1	セキュリティ モジュールの SM-40 と SM-48 が導入されました。 （注） FXOS 2.6.1 が必要です。
ASA および Firewall Threat Defense を同じ Firepower 9300 の別のモジュールでサポート	9.12.1	ASA および Firewall Threat Defense 論理デバイスを同じ Firepower 9300 上で展開できるようになりました。 （注） FXOS 2.6.1 が必要です。
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	9.10.1	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 （注） FXOS 2.4.1 が必要です。 新規/変更された FXOS コマンド： **set cluster-control-link network**

機能	バージョン	詳細
オン モードでのデータ EtherChannel のサポート	9.10.1	データおよびデータ共有 EtherChannel をアクティブ LACP モードまたはオン モードに設定できるようになりました。Etherchannel の他のタイプはアクティブ モードのみをサポートします。 （注） FXOS 2.4.1 が必要です。 新規/変更された FXOS コマンド：**set port-channel-mode**
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次のコマンドが変更されました。**site-id**
Firepower 4100 シリーズのサポート	9.6(1)	FXOS 1.1.4 では、ASA クラスタリングは、Firepower 4100 シリーズ のシャーシ間クラスタリングをサポートします。 変更されたコマンドはありません。
6 つのモジュールのシャーシ間クラスタリング、および FirePOWER 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 6 つのシャーシに最大 6 つのモジュールを含めることができます。 変更されたコマンドはありません。
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4（1.150）	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**



第 6 章

トランスペアレントファイアウォールモードまたはルーテッドファイアウォールモード

この章では、ファイアウォール モードをルーテッドまたはトランスペアレントに設定する方法と、各ファイアウォール モードでファイアウォールがどのように機能するかについて説明します。

マルチコンテキスト モードでは、コンテキストごとに別個にファイアウォール モードを設定できます。

- ファイアウォール モードについて （231 ページ）
- デフォルト設定 （241 ページ）
- ファイアウォール モードのガイドライン （242 ページ）
- ファイアウォール モードの設定 （243 ページ）
- ファイアウォール モードの例 （244 ページ）
- ファイアウォール モードの履歴 （255 ページ）

ファイアウォール モードについて

ASA は、でルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードの 2 つのファイアウォール モードをサポートします。

ルーテッド ファイアウォール モードについて

ルーテッド モードでは、ASAはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。 コンテキスト間でレイヤ3インターフェイスを共有することもできます。

統合ルーティングおよびブリッジングにより、ネットワーク上の複数のインターフェイスをまとめた「ブリッジグループ」を使用できます。そして、ASAはブリッジング技術を使用してインターフェイス間のトラフィックを通すことができます。各ブリッジグループには、ネット

ワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。ASA は BVI と通常のルーテッドインターフェイス間でルーティングを行います。マルチコンテキストモード、クラスタリング、EtherChannel、または Visual Networking Index（VNI）メンバーインターフェイスが必要ない場合は、トランスペアレントモードではなくルーテッドモードの使用を検討してください。ルーテッド モードでは、トランスペアレント モードと同様に 1 つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

トランスペアレント ファイアウォール モードについて

従来、ファイアウォールはルーテッドホップであり、保護されたサブネットのいずれかに接続するホストのデフォルト ゲートウェイとして機能します。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。ただし、他のファイアウォールのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のすべてのチェックが実施されます。

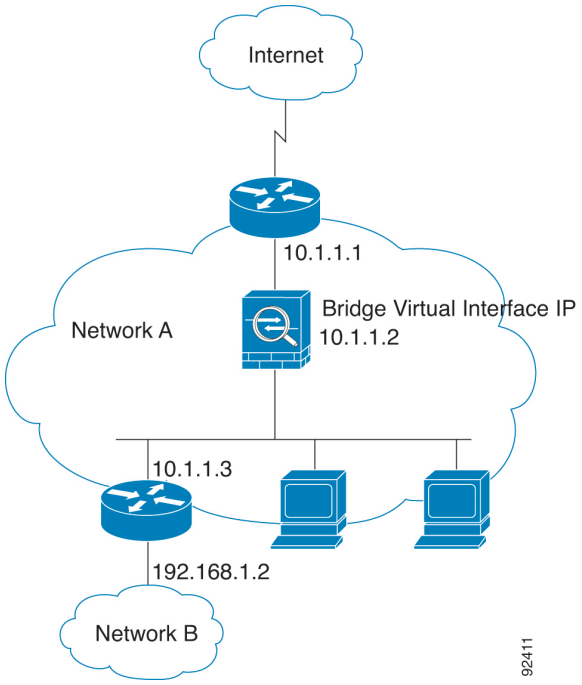
レイヤ 2 の接続は、ネットワーク上の内部と外部のインターフェイスをまとめた「ブリッジ グループ」を使用して確立されます。また、ASA はブリッジング技術を使用してインターフェイス間のトラフィックを通します。各ブリッジグループには、ネットワーク上で IP アドレスが割り当てられるブリッジ仮想インターフェイス（BVI）が含まれます。複数のネットワークに複数のブリッジグループを設定できます。トランスペアレントモードでは、これらのブリッジグループは相互通信できません。

ネットワークでのトランスペアレント ファイアウォールの使用

ASA は、自身のインターフェイス間を同じネットワークで接続します。トランスペアレント ファイアウォールはルーティングされたホップではないため、既存のネットワークに簡単に導入できます。

次の図に、外部デバイスが内部デバイスと同じサブネット上にある一般的なトランスペアレント ファイアウォール ネットワークを示します。内部ルータと各ホストは、外部ルータに直接接続されているように見えます。

図 *22*: トランスペアレント ファイアウォール ネットワーク



管理 インターフェイス

各ブリッジ仮想インターフェイス（BVI）IP アドレスのほかに、別の管理 スロット/ポート インターフェイスを追加できます。このインターフェイスはどのブリッジグループにも属さず、ASA への管理トラフィックのみを許可します。詳細については、管理インターフェイス（826 ページ）を参照してください。

ルーテッド モード機能のためのトラフィックの通過

トランスペアレント ファイアウォールで直接サポートされていない機能の場合は、アップストリーム ルータとダウンストリーム ルータが機能をサポートできるようにトラフィックの通過を許可することができます。たとえば、アクセス ルールを使用することによって、（サポートされていない DHCP リレー機能の代わりに）DHCP トラフィックを許可したり、IP/TV で作成されるようなマルチキャスト トラフィックを許可したりできます。また、トランスペアレント ファイアウォールを通過するルーティング プロトコル隣接関係を確立することもできます。つまり、OSPF、RIP、EIGRP、または BGP トラフィックをアクセス ルールに基づいて許可できます。同様に、HSRP や VRRP などのプロトコルは ASA を通過できます。

ブリッジグループについて

ブリッジ グループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。 ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。他のファイアウォール インターフェイ

スのように、インターフェイス間のアクセス制御は管理され、ファイアウォールによる通常のチェックがすべて実施されます。

ブリッジ仮想インターフェイス（BVI）

各ブリッジグループには、ブリッジ仮想インターフェイス（BVI）が含まれます。ASAは、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの BVI IP アドレスを使用します。BVI IP アドレスはブリッジグループ メンバー インターフェイスと同じサブネット上になければなりません。BVIでは、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IPアドレスと同じネットワーク上のトラフィックだけがサポートされています。

トランスペアレントモード：インターフェイスベースの各機能はブリッジグループのメンバーインターフェイスだけを指定でき、これらについてのみ使用できます。

ルーテッド モード：BVI はブリッジグループと他のルーテッド インターフェイス間のゲートウェイとして機能します。ブリッジグループ/ルーテッド インターフェイス間でルーティングするには、BVI を指定する必要があります。一部のインターフェイスベース機能に代わり、BVI 自体が利用できます。

- アクセス ルール：ブリッジグループのメンバー インターフェイスと BVI 両方のアクセスルールを設定できます。インバウンドのルールでは、メンバーインターフェイスが先にチェックされます。アウトバウンドのルールでは BVI が最初にチェックされます。
- DHCPv4 サーバ：BVI のみが DHCPv4 サーバの構成をサポートします。
- スタティック ルート：BVIのスタティック ルートを設定できます。メンバーインターフェイスのスタティック ルートは設定できません。
- Syslog サーバーと ASA 由来の他のトラフィック：syslog サーバー（または SNMP サーバー、ASAからトラフィックが送信される他のサービス）を指定する際、BVIまたはメンバー インターフェイスのいずれかも指定できます。

ルーテッド モードで BVI を指定しない場合、ASA はブリッジ グループのトラフィックをルーティングしません。この設定は、ブリッジグループのトランスペアレント ファイアウォール モードを複製します。マルチコンテキストモード、クラスタリング、またはEtherChannelまたは VNI メンバーインターフェイスが不要であれば、ルーテッドモードの使用を検討すべきです。ルーテッドモードでは、トランスペアレントモードと同様に1つ以上の分離されたブリッジ グループを含めることができます。また、モードが混在する導入に関しては、通常のルーテッド インターフェイスも含めることができます。

トランスペアレント ファイアウォール モードのブリッジグループ

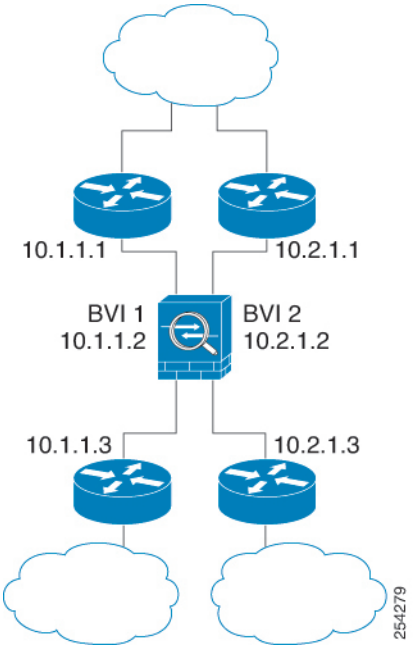
ブリッジグループのトラフィックは他のブリッジグループから隔離され、トラフィックはASA内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジグループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバまたは AAA サーバの設定は、すべてのブリッジ グループで共有されます。セキュリティ ポリシーを完全に分離する

には、各コンテキスト内に1つのブリッジグループにして、セキュリティ コンテキストを使用します。

1 つのブリッジグループにつき複数のインターフェイスを入れることができます。サポートされるブリッジグループとインターフェイスの正確な数については、ファイアウォール モードのガイドライン（242ページ）を参照してください。ブリッジグループごとに2つ以上のインターフェイスを使用する場合は、内部、外部への通信だけでなく、同一ネットワーク上の複数のセグメント間の通信を制御できます。たとえば、相互通信を希望しない内部セグメントが3つある場合、インターフェイスを別々のセグメントに置き、外部インターフェイスとのみ通信させることができます。または、インターフェイス間のアクセスルールをカスタマイズし、希望通りのアクセスを設定できます。

次の図に、2つのブリッジ グループを持つ、ASA に接続されている2つのネットワークを示します。

図 *23*：*2* つのブリッジ グループを持つトランスペアレント ファイアウォール ネットワーク



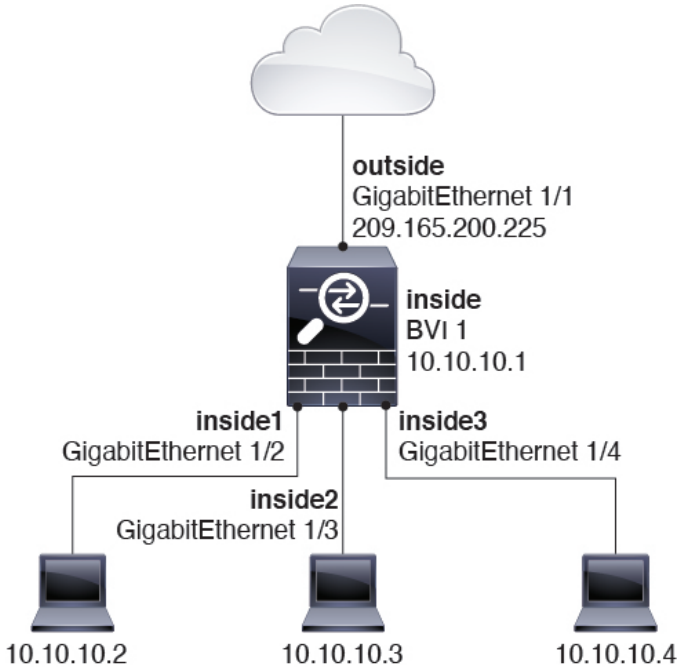
ルーテッド ファイアウォール モードのブリッジグループ

ブリッジグループ トラフィックは他のブリッジ グループまたはルーテッド インターフェイスにルーティングできます。ブリッジグループのBVIインターフェイスに名前を割り当てないことで、ブリッジグループのトラフィックを分離することもできます。BVIに名前を付けると、その BVI はその他の通常のインターフェイスと同様にルーティングに参加します。

ルーテッド モードでブリッジ グループを使用する方法として、外部スイッチの代わりに ASA 追加のインターフェイスを使用する方法があります。たとえば、デバイスの中には、通常のインターフェイスとして外部インターフェイスを持ち、その他すべてのインターフェイスが内部ブリッジグループに割り当てられているというデフォルト設定のものがあります。このブリッジグループは外部スイッチを置き換えることを目的としているので、すべてのブリッジグルー

プインターフェイスが自由に通信できるようにアクセス ポリシーを設定する必要があります。たとえば、デフォルト設定と同様に、すべてのインターフェイスを同じセキュリティ レベルに設定し、同じセキュリティ レベルのインターフェイス間の通信を有効にします。この通信ではアクセス ルールは不要です。

図 *24*:内部ブリッジグループと外部ルーテッド インターフェイスからなるルーテッド ファイアウオール ネットワーク



ルーテッド モードで許可されないトラフィックの通過

ルーテッド モードでは、アクセス ルールで許可しても、いくつかのタイプのトラフィックは ASA を通過できません。ただし、ブリッジグループは、アクセス ルール（IP トラフィックの場合）または EtherType ルール（非 IP トラフィックの場合）を使用してほとんどすべてのトラフィックを許可できます。

- IP トラフィック：ルーテッド ファイアウォール モードでは、ブロードキャストとマルチキャスト トラフィックは、アクセスルールで許可されている場合でもブロックされます。これには、サポートされていないダイナミック ルーティング プロトコルおよび DHCP（DHCP リレーを設定している場合を除く）が含まれます。ブリッジグループ内では、このトラフィックをアクセス ルール（拡張 ACL を使用）で許可できます。
- 非 IP トラフィック：AppleTalk、IPX、BPDU や MPLS などは、EtherType ルールを使用することで、通過するように設定できます。

（注） ブリッジ グループは、CDP パケットおよび 0x600 以上の有効な EtherType を持たないパケットの通過を拒否します。サポートされる例外は、BPDU および IS-IS です。

レイヤ 3 トラフィックの許可

- ユニキャストの IPv4 および IPv6 トラフィックは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスに移動する場合、アクセス ルールなしで自動的にブリッジグループを通過できます。
- セキュリティの低いインターフェイスからセキュリティの高いインターフェイスに移動するレイヤ 3 トラフィックの場合、セキュリティの低いインターフェイスでアクセル ルールが必要です。
- ARP は、アクセス ルールなしで両方向にブリッジグループを通過できます。ARP トラフィックは、ARP インスペクションによって制御できます。
- IPv6 ネイバー探索およびルータ送信要求パケットは、アクセス ルールを使用して通過させることができます。
- ブロードキャストおよびマルチキャスト トラフィックは、アクセス ルールを使用して通過させることができます。

許可される MAC アドレス

アクセス ポリシーで許可されている場合、以下の宛先 MAC アドレスをブリッジグループで使用できます（レイヤ 3 トラフィックの許可 （237 ページ）を参照）。このリストにない MAC アドレスはドロップされます。

- FFFF.FFFF.FFFF の TRUE ブロードキャスト宛先 MAC アドレス
- 0100.5E00.0000 ～ 0100.5EFE.FFFF の IPv4 マルチキャスト MAC アドレス
- 3333.0000.0000 ～ 3333.FFFF.FFFF の IPv6 マルチキャスト MAC アドレス
- 0100.0CCC.CCCD に等しい BPDU マルチキャスト アドレス
- 0900.0700.0000 ～ 0900.07FF.FFFF までの AppleTalk マルチキャスト MAC アドレス

BPDU 処理

スパニングツリープロトコルを使用するときのループを防止するために、デフォルトで BPDU が渡されます。BPDU をブロックするには、BPDU を拒否するように EtherType ルールを設定する必要があります。外部スイッチで BPDU をブロックすることもできます。たとえば、同じブリッジグループのメンバーが異なる VLAN のスイッチポートに接続されている場合、スイッチで BPDU をブロックできます。この場合、一方の VLAN からの BPDU がもう一方の VLAN で認識されるため、スパニング ツリー ルート ブリッジの選定プロセスで問題が発生する可能性があります。

フェールオーバーを使用している場合、BPDU をブロックして、トポロジが変更されたときにスイッチ ポートがブロッキング ステートに移行することを回避できます。詳細については、フェールオーバーのブリッジ グループ要件 （328 ページ）を参照してください。

MAC アドレスとルート ルックアップ

ブリッジ グループ内のトラフィックでは、パケットの発信インターフェイスは、ルート ルックアップではなく宛先 MAC アドレス ルックアップを実行することによって決定されます。

ただし、次の場合にはルート ルックアップが必要です。

- トラフィックの発信元が ASA：syslog サーバーなどがあるリモート ネットワーク宛てのトラフィック用に、ASA にデフォルト/スタティック ルートを追加します。
- インスペクションが有効になっている Voice over IP（VoIP）および TFTP トラフィック、エンドポイントが 1 ホップ以上離れている：セカンダリ接続が成功するように、リモート エンドポイント宛てのトラフィック用に、ASA にスタティック ルートを追加します。ASA は、セカンダリ接続を許可するためにアクセス コントロール ポリシーに一時的な「ピンホール」を作成します。セカンダリ接続ではプライマリ接続とは異なる IP アドレスのセットが使用される可能性があるため、ASA は正しいインターフェイスにピンホールをインストールするために、ルート ルックアップを実行する必要があります。

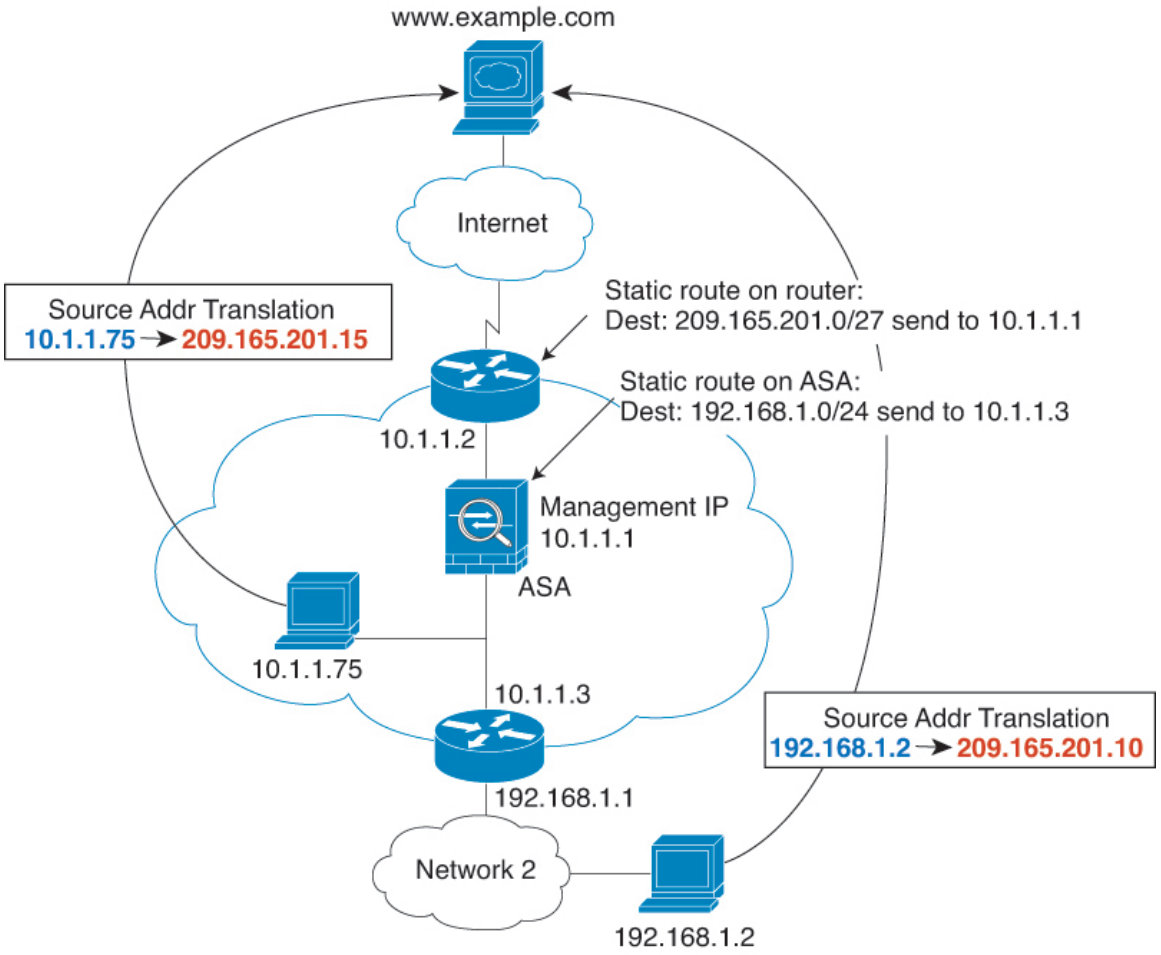
  影響を受けるアプリケーションは次のとおりです。

  - CTIQBE
  - GTP
  - H.323
  - MGCP
  - RTSP
  - SIP
  - Skinny（SCCP）
  - SQL*Net
  - SunRPC
  - TFTP

- ASA が NAT を実行する 1 ホップ以上離れたトラフィック：リモート ネットワーク宛てのトラフィック用に、ASA にスタティック ルートを設定します。また、ASA に送信されるマッピング アドレス宛てのトラフィック用に、上流に位置するルータにもスタティック ルートが必要です。

  このルーティング要件は、インスペクションと NAT が有効になっている VoIP と DNS の、1 ホップ以上離れている組み込み IP アドレスにも適用されます。ASA は、変換を実行できるように正しい出力インターフェイスを識別する必要があります。

図 *25 : NAT* の例：ブリッジ グループ内の *NAT*



トランスペアレント モードのブリッジ グループのサポートされていない機能

次の表に、トランスペアレント モードのブリッジ グループでサポートされない機能を示します。

表 *4 :* トランスペアレント モードでサポートされない機能

特長	説明
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	ブリッジグループ メンバー インターフェイスでは、DHCPv4 サーバのみがサポートされます。

特長	説明
DHCP リレー	トランスペアレント ファイアウォールは DHCPv4 サーバーとして機能することができますが、DHCP リレーはサポートしません。2 つのアクセス ルール（1 つは内部インターフェイスから外部インターフェイスへの DHCP 要求を許可し、もう 1 つはサーバーからの応答を逆方向に許可します。）を使用して DHCP トラフィックを通過させることができるので、DHCP リレーは必要ありません。
ダイナミック ルーティング プロトコル	ただし、ブリッジグループ メンバー インターフェイスの場合、ASA で発信されたトラフィックにスタティック ルートを追加できます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが ASA を通過できるようにすることもできます。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが ASA を通過できるようにすることができます。
QoS	-
通過トラフィック用の VPN 終端	トランスペアレント ファイアウォールは、ブリッジ グループ メンバー インターフェイスでのみ、管理接続用のサイト間 VPN トンネルをサポートします。これは、ASAを通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックに ASA を通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。
Unified Communications	—

ルーテッド モードのブリッジ グループのサポートされていない機能

次の表に、ルーテッド モードのブリッジ グループでサポートされない機能を示します。

表 *5:* ルーテッド モードでサポートされない機能

特長	説明
EtherChannel または VNI メンバー インターフェイス	物理インターフェイスおよびサブインターフェイスのみがブリッジグループ メンバーインターフェイスとしてサポートされます。 管理 インターフェイスもサポートされていません。
クラスタリング	ブリッジ グループはクラスタリングでサポートされません。
ダイナミック DNS	-
DHCPv6 ステートレス サーバ	DHCPv4 サーバーのみが BVI でサポートされます。

特長	説明
DHCP リレー	ルーテッド ファイアウォールは DHCPv4 サーバーとして機能することができますが、DHCP リレーを BVI またはブリッジ グループ メンバー インターフェイスでサポートしません。
ダイナミック ルーティング プロトコル	ただし、BVI のスタティック ルートを追加することはできます。アクセス ルールを使用して、ダイナミック ルーティング プロトコルが ASA を通過できるようにすることもできます。非ブリッジ グループ インターフェイスはダイナミック ルーティングをサポートします。
マルチキャスト IP ルーティング	アクセス ルールで許可することによって、マルチキャスト トラフィックが ASA を通過できるようにすることができます。非ブリッジ グループ インターフェイスはマルチキャスト ルーティングをサポートします。
マルチ コンテキスト モード	ブリッジ グループは、マルチ コンテキスト モードではサポートされません。
QoS	非ブリッジ グループ インターフェイスは、QoS をサポートします。
通過トラフィック用の VPN 終端	VPN 接続を BVI で終端することはできません。非ブリッジ グループ インターフェイスは、VPN をサポートします。 ブリッジ グループ メンバー インターフェイスは、管理接続専用のサイト間 VPN トンネルをサポートします。これは、ASA を通過するトラフィックに対して VPN 接続を終端しません。アクセス ルールを使用して VPN トラフィックにブリッジ グループを通過させることはできますが、非管理接続は終端されません。クライアントレス SSL VPN もサポートされていません。
Unified Communications	非ブリッジ グループ インターフェイスは、Unified Communications をサポートします。

デフォルト設定

デフォルト モード（Default Mode）

デフォルト モードはルーテッド モードです。

ブリッジ グループのデフォルト

デフォルトでは、すべての ARP パケットはブリッジ グループ内で渡されます。

ファイアウォール モードのガイドライン

コンテキスト モードのガイドライン

コンテキストごとにファイアウォール モードを設定します。

ブリッジグループのガイドライン（トランスペアレントおよびルーテッドモード）

- 64 のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および ASA を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の ASAv50 の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- Firepower 1010 および Secure Firewall 1210/20 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォールインターフェイスを混在させることはできません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークからの管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は 管理 インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、ASA 定義の EtherChannel および VNI インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

その他のガイドラインと制限事項

- ファイアウォールモードを変更すると、多くのコマンドが両方のモードでサポートされていないため、ASA は実行コンフィギュレーションをクリアします。スタートアップ コンフィギュレーションは変更されません。保存しないでリロードすると、スタートアップ コンフィギュレーションがロードされて、モードは元の設定に戻ります。 コンフィギュレーション ファイルのバックアップについては、ファイアウォール モードの設定 （243 ページ）を参照してください。
- **firewall transparent** コマンドでモードを使用して変更するテキスト コンフィギュレーションを ASA にダウンロードする場合、コマンドをコンフィギュレーションの先頭に配置してください。このコマンドが読み込まれるとすぐに ASA がモードを変更し、その後ダウンロードされたコンフィギュレーションを引き続き読み込みます。コマンドがコンフィギュレーションの後ろの方にあると、ASA はそのコマンドよりも前の位置に記述されているすべての行をクリアします。テキストファイルのダウンロードの詳細については、ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定（1573 ページ）を参照してください。

ファイアウォール モードの設定

この項では、ファイアウォール モードを変更する方法を説明します。

（注） ファイアウォールモードを変更すると実行コンフィギュレーションがクリアされるので、他のコンフィギュレーションを行う前にファイアウォールモードを設定することをお勧めします。

始める前に

モードを変更すると、ASA は実行コンフィギュレーションをクリアします（詳細については、ファイアウォール モードのガイドライン （242 ページ）を参照してください）。

- 設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。このバックアップは、新しいコンフィギュレーション作成時の参照として使用できます。コンフィギュレーションまたはその他のファイルのバックアップと復元 （1577 ページ）を参照してください。
- モードを変更するには、コンソール ポートで CLI を使用します。ASDM コマンドラインインターフェイス ツールやSSHなどの他のタイプのセッションを使用する場合、コンフィギュレーションがクリアされるときにそれが切断されるので、いずれの場合もコンソールポートを使用して ASA に再接続する必要があります。
- コンテキスト内でモードを設定します。

（注） 設定が削除された後にファイアウォール モードをトランスペアレントに設定し、ASDM への管理アクセスを設定するには、ASDM アクセスの設定 （18 ページ）を参照してください。

手順

ファイアウォール モードをトランスペアレントに設定します。

firewall transparent

例：

```
ciscoasa(config)# firewall transparent
```

モードをルーテッドに変更するには、**no firewall transparent** コマンドを入力します。

（注）
ファイアウォール モードの変更では確認は求められず、ただちに変更が行われます。

ファイアウォール モードの例

このセクションには、ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードで、ASA を介してどのようにトラフィックが転送されるかを説明する例が含まれます。

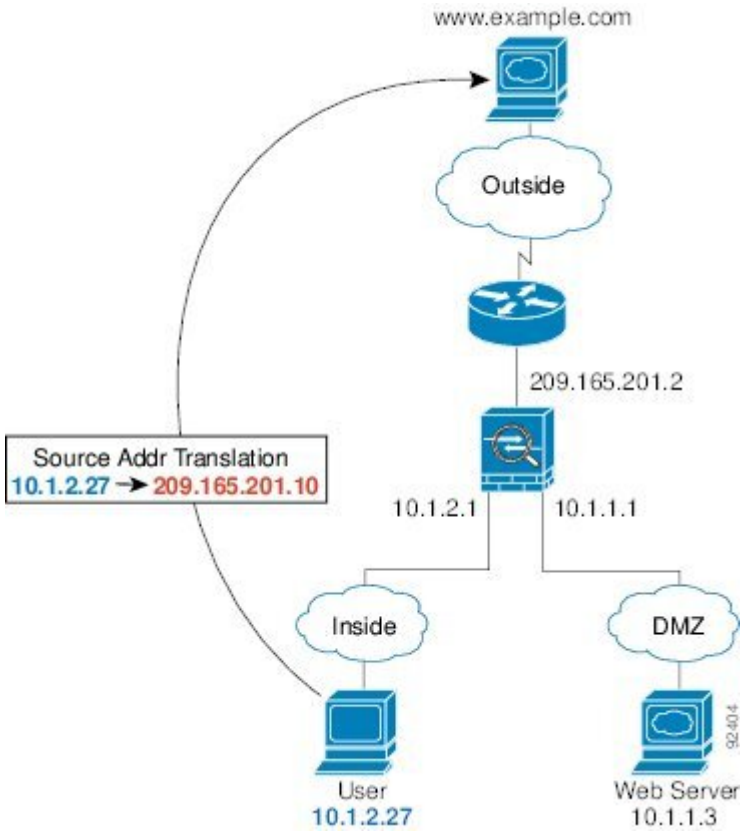
ルーテッド ファイアウォール モードで ASA を通過するデータ

次のセクションでは、複数のシナリオのルーテッドファイアウォールモードで、データがASAをどのように通過するかを示します。

内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバーにアクセスしていることを示しています。

図 *26 :* 内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザーは、www.example.com から Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティ ポリシーの条件に従って、パケットが許可されているか確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASA は、実アドレス（10.1.2.27）をマップ アドレス 209.165.201.10 に変換します。このマップ アドレスは外部インターフェイスのサブネット上にあります。

   マップ アドレスは任意のサブネット上に設定できますが、外部インターフェイスのサブネット上に設定すると、ルーティングが簡素化されます。
4. 次に、ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. www.example.com が要求に応答すると、パケットはASAを通過します。これはすでに確立されているセッションであるため、パケットは、新しい接続に関連する多くのルックアッ

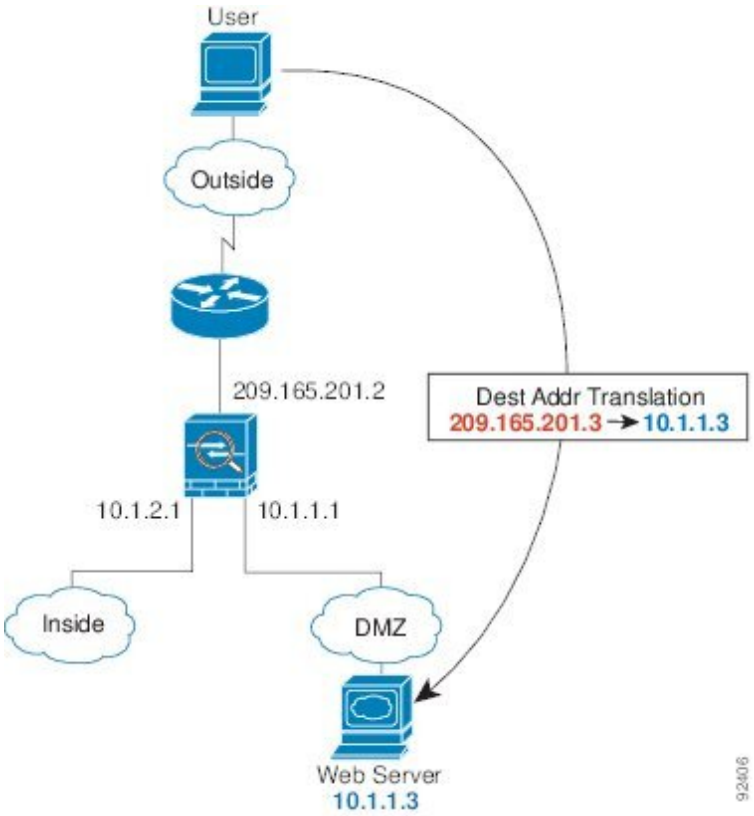
プをバイパスします。ASAは、グローバル宛先アドレスをローカルユーザアドレス10.1.2.27に変換せずに、NAT を実行します。

6. ASAは、パケットを内部ユーザに転送します。

外部ユーザーが DMZ 上の Web サーバーにアクセスする

次の図は、外部ユーザーが DMZ の Web サーバーにアクセスしていることを示しています。

図 *27 :* 外部から *DMZ* へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーがマップ アドレス 209.165.201.3 を使用して、DMZ 上の Web サーバーに Web ページを要求します。これは、外部インターフェイスのサブネット上のアドレスです。
2. ASA はパケットを受信し、マッピング アドレスは実アドレス 10.1.1.3 に変換しません。
3. ASA は新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

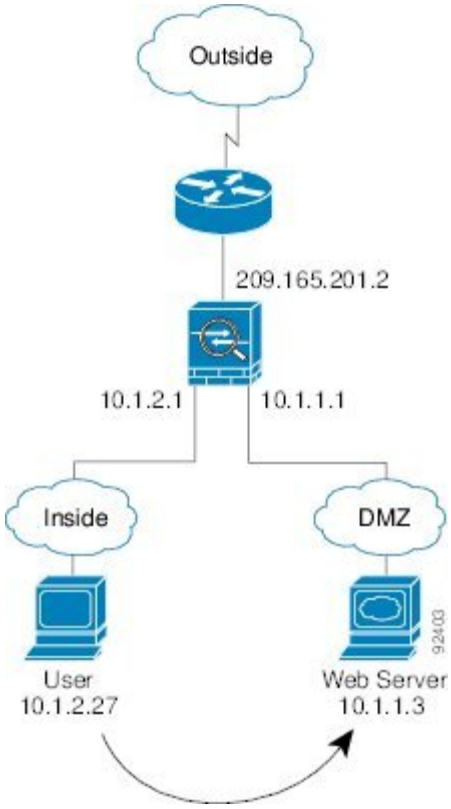
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
4. 次に、ASAはセッションエントリを高速パスに追加し、DMZインターフェイスからパケットを転送します。

5. DMZ Web サーバが要求に応答すると、パケットはASAを通過します。また、セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。ASA は、実アドレスを 209.165.201.3 に変換することで NAT を実行します。
6. ASAは、パケットを外部ユーザに転送します。

内部ユーザーが DMZ 上の Web サーバーにアクセスする

次の図は、内部ユーザーが DMZ の Web サーバーにアクセスしていることを示しています。

図 *28 :* 内部から *DMZ* へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワーク上のユーザーは、宛先アドレス 10.1.1.3 を使用して DMZ Web サーバーから Web ページを要求します。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーの条件に従ってパケットが許可されているか確認します。

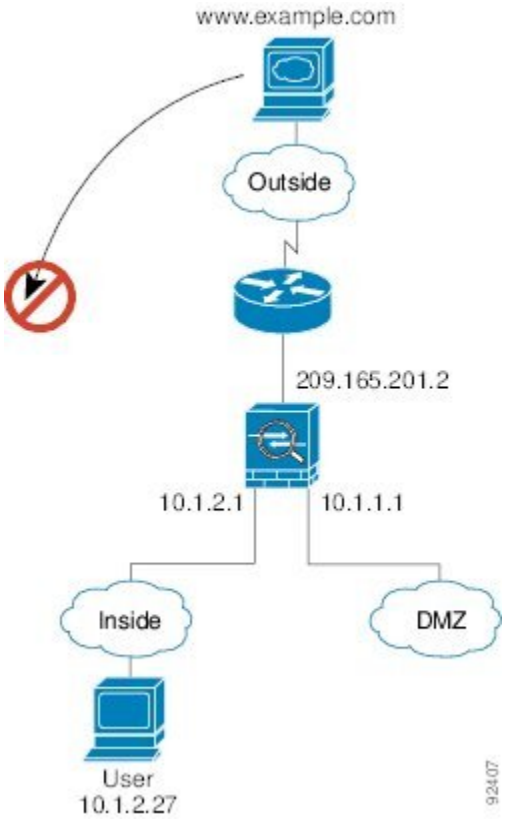
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. 次に、ASAはセッションが確立されたことを記録し、DMZ インターフェイスからパケットを転送します。

4. DMZ Web サーバーが要求に応答すると、パケットは高速パスを通過します。これのため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
5. ASAは、パケットを内部ユーザに転送します。

外部ユーザーが内部ホストにアクセスしようとする

次の図は、外部ユーザーが内部ネットワークにアクセスしようとしていることを示しています。

図 *29* : 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーが、内部ホストに到達しようとします（ホストにルーティング可能な IP アドレスがあると想定します）。

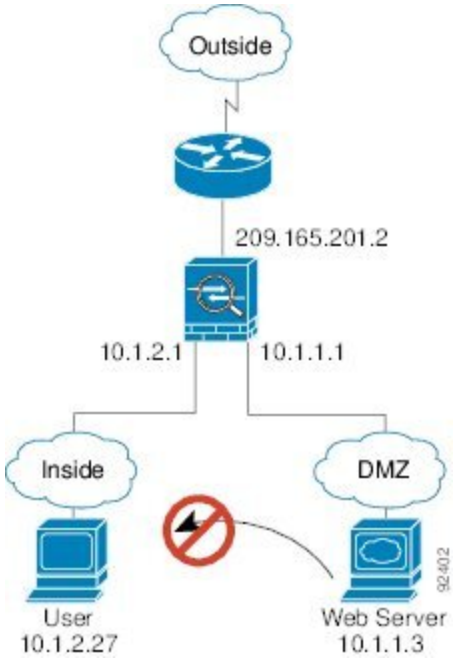
   内部ネットワークがプライベート アドレスを使用している場合、外部ユーザーが NAT なしで内部ネットワークに到達することはできません。外部ユーザーは既存の NAT セッションを使用して内部ユーザーに到達しようとすることが考えられます。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。
3. パケットが拒否され、ASAはパケットをドロップし、接続試行をログに記録します。

外部ユーザが内部ネットワークを攻撃しようとした場合、ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

DMZ ユーザーによる内部ホストへのアクセスの試み

次の図は、DMZ 内のユーザーが内部ネットワークにアクセスしようとしていることを示しています。

図 *30 : DMZ* から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

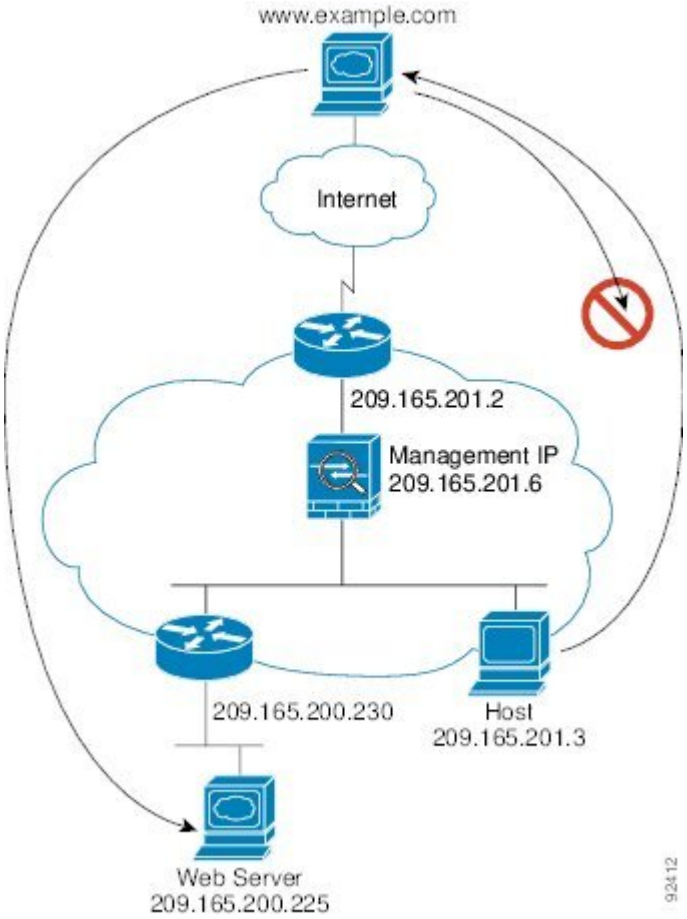
1. DMZ ネットワーク上のユーザーが、内部ホストに到達しようとします。DMZ はインターネット上のトラフィックをルーティングする必要がないので、プライベートアドレッシング方式はルーティングを回避しません。
2. ASA はパケットを受信します。これは新しいセッションであるため、ASA はセキュリティポリシーに従って、パケットが許可されているか確認します。

   パケットが拒否され、ASAはパケットをドロップし、接続試行をログに記録します。

トランスペアレント ファイアウォールを通過するデータの動き

次の図に、パブリック Web サーバを含む内部ネットワークを持つ一般的なトランスペアレント ファイアウォールの実装を示します。内部ユーザーがインターネット リソースにアクセスできるよう、ASA にはアクセス ルールがあります。別のアクセス ルールによって、外部ユーザーは内部ネットワーク上の Web サーバーだけにアクセスできます。

図 *31 :* 一般的なトランスペアレント ファイアウォールのデータ パス

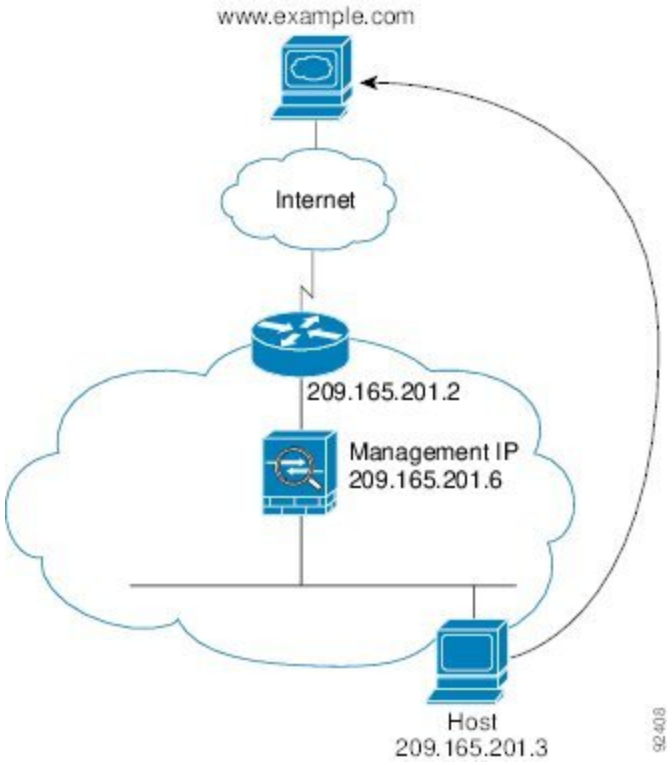


次のセクションでは、データが ASA をどのように通過するかを示します。

内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバーにアクセスしていることを示しています。

図 *32 :* 内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザーは、www.example.com から Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

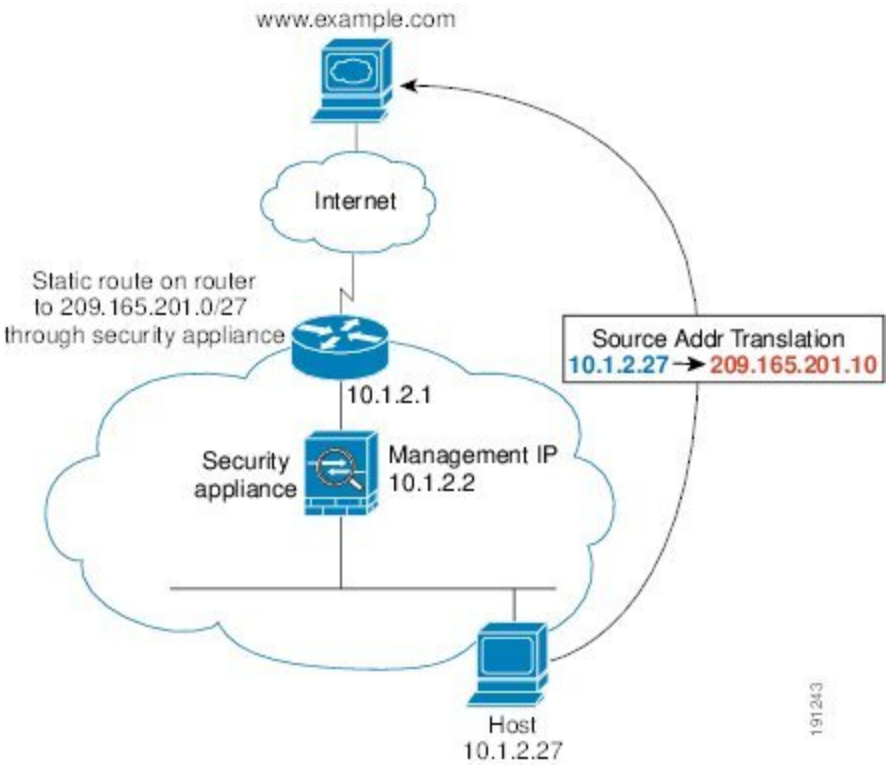
   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先 MAC アドレスは、アップストリーム ルータのアドレス 209.165.201.2 です。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求または ping を送信します。最初のパケットはドロップされます。
5. Web サーバーが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASAは、パケットを内部ユーザに転送します。

NAT を使用して内部ユーザーが Web サーバーにアクセスする

次の図は、内部ユーザーが外部 Web サーバーにアクセスしていることを示しています。

図 *33 : NAT* を使用して内部から外部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 内部ネットワークのユーザーは、www.example.com から Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASAは、固有なインターフェイスに従ってパケットを分類します。
3. ASAは実際のアドレス（10.1.2.27）をマッピング アドレス 209.165.201.10 に変換します。

   マッピング アドレスは外部インターフェイスと同じネットワーク上にないため、アップストリーム ルータにASAをポイントするマッピング ネットワークへのスタティック ルートがあることを確認します。
4. 次に、ASAはセッションが確立されたことを記録し、外部インターフェイスからパケットを転送します。
5. 宛先 MAC アドレスがテーブル内にある場合、ASAは外部インターフェイスからパケットを転送します。宛先MACアドレスは、アップストリームルータのアドレス 10.1.2.1 です。

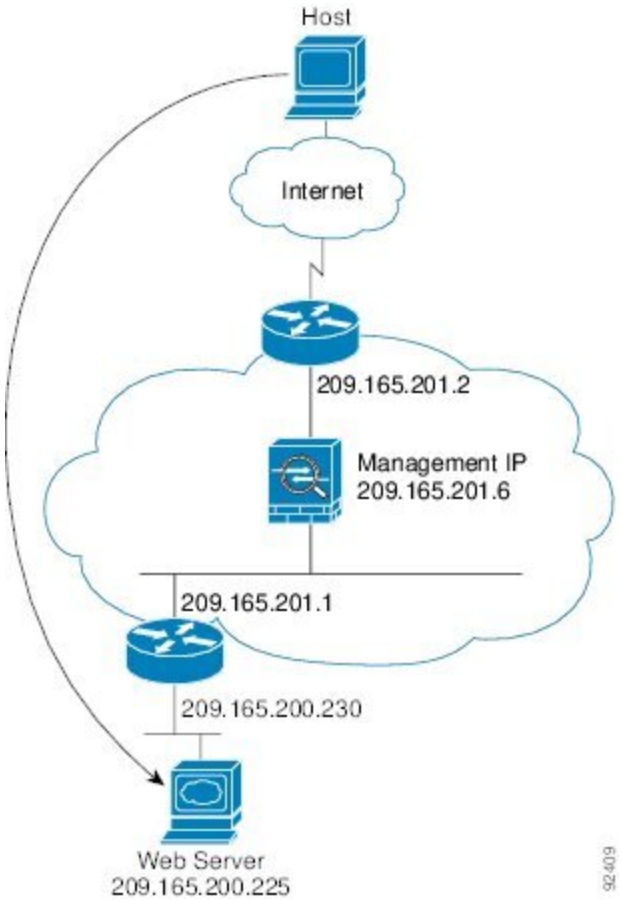
宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。

6. Web サーバーが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
7. ASA は、マッピング アドレスを実際のアドレス 10.1.2.27 にせずに、NAT を実行します。

外部ユーザーが内部ネットワーク上の Web サーバーにアクセスする

次の図は、外部ユーザーが内部の Web サーバーにアクセスしていることを示しています。

図 *34* : 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーは、内部 Web サーバーから Web ページを要求します。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されていることを確認します。

   マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

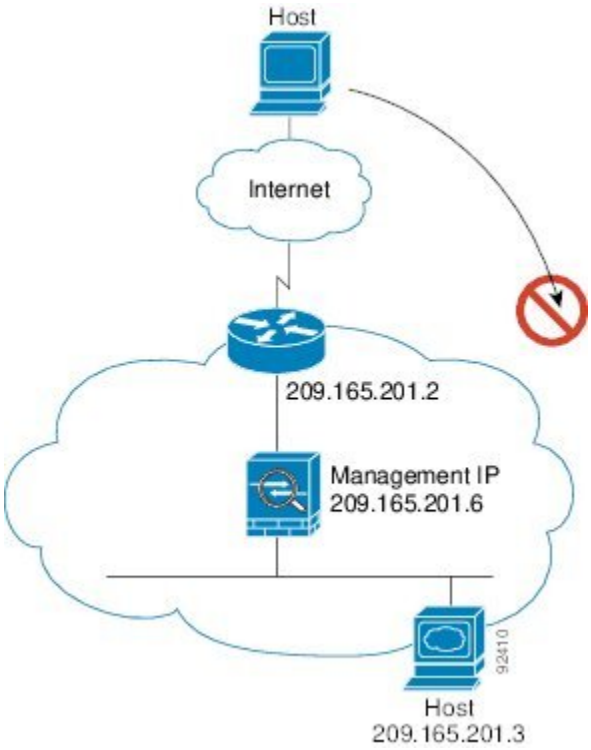
3. ASAは、セッションが確立されたことを記録します。
4. 宛先 MAC アドレスがテーブル内にある場合、ASAは内部インターフェイスからパケットを転送します。宛先 MAC アドレスは、ダウンストリーム ルータ 209.165.201.1 のアドレスです。

   宛先 MAC アドレスが ASA のテーブルにない場合、ASA は MAC アドレスを検出するために ARP 要求と ping を送信します。最初のパケットはドロップされます。
5. Web サーバーが要求に応答します。セッションがすでに確立されているため、パケットは、新しい接続に関連する多くのルックアップをバイパスします。
6. ASAは、パケットを外部ユーザに転送します。

外部ユーザーが内部ホストにアクセスしようとする

次の図は、外部ユーザーが内部ネットワーク上のホストにアクセスしようとしていることを示しています。

図 *35 :* 外部から内部へ



次の手順では、データが ASA をどのように通過するかを示します。

1. 外部ネットワーク上のユーザーが、内部ホストに到達しようとします。
2. ASAはパケットを受信し、必要な場合、送信元 MAC アドレスを MAC アドレス テーブルに追加します。これは新しいセッションであるため、セキュリティ ポリシーの条件に従って、パケットが許可されているか確認します。

マルチ コンテキスト モードの場合、ASA はパケットをまずコンテキストに分類します。

3. 外部ホストを許可するアクセス ルールは存在しないため、パケットは拒否され、ASA によってドロップされます。
4. 外部ユーザが内部ネットワークを攻撃しようとした場合、ASAは多数のテクノロジーを使用して、すでに確立されたセッションに対してパケットが有効かどうかを判別します。

ファイアウォール モードの履歴

表 *6:* ファイアウォール モードの各機能履歴

機能名	プラットフォーム リリース	機能情報
トランスペアレント ファイアウォール モード	7.0(1)	トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。 **firewall transparent**、および **show firewall** コマンドが導入されました。
トランスペアレント ファイアウォール ブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに 1 つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードでは最大 8 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 （注） ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。 **interface bvi**、**bridge-group**、**show bridge-group** の各コマンドが導入されました。

機能名	プラットフォーム リリース	機能情報
マルチ コンテキスト モードのファイアウォール モードの混合がサポートされます。	8.5(1)/9.0(1)	セキュリティ コンテキスごとに個別のファイアウォール モードを設定できます。したがってその一部をトランスペアレント モードで実行し、その他をルーテッド モードで実行することができます。 **firewall transparent** コマンドが変更されました。
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	9.3(1)	ブリッジ グループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 **interface bvi** コマンド、**bridge-group** コマンドが変更されました。
トランスペアレント モードで、ブリッジ グループごとのインターフェイス数が最大で 64 に増加	9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更されたコマンドはありません。

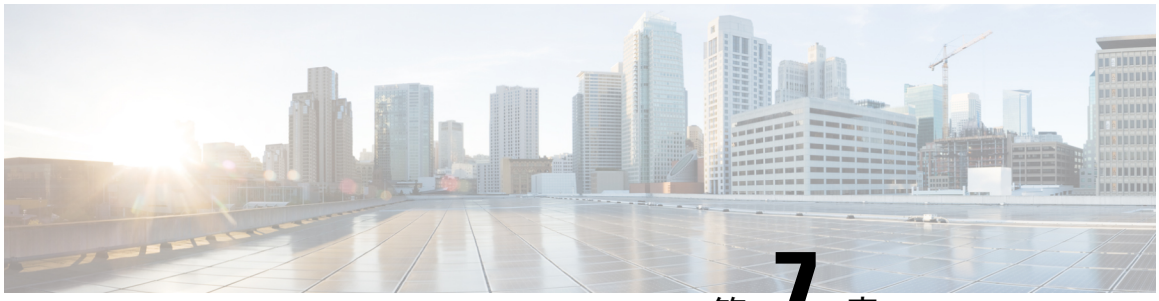
機能名	プラットフォーム リリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASA がルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバーなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッドモードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次のコマンドが変更されました。**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**

機能名	プラットフォーム リリース	機能情報
Firepower 4100/9300 ASA 論理デバイスのトランスペアレントモード展開のサポート	9.10(1)	Firepower 4100/9300 で ASA を展開するときに、トランスペアレントまたはルーテッドモードを指定できるようになりました。 新規/変更された FXOS コマンド：**enter bootstrap-key FIREWALL_MODE**、**set value routed**、**set value transparent**

第 II 部

ハイ アベイラビリティとスケーラビリティ

- マルチ コンテキスト モード （261 ページ）
- ハイ アベイラビリティのためのフェールオーバー （315 ページ）
- パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー （383 ページ）
- Cisco Secure Firewall 3100/4200 の ASA クラスタ （407 ページ）
- Firepower 4100/9300 の ASA クラスタ （525 ページ）
- ASA クラスタのクラスタを展開する （639 ページ）
- パブリッククラウドにおける ASA Virtual の ASA クラスタ （717 ページ）



第 7 章

マルチ コンテキスト モード

この章では、ASA でマルチ セキュリティ コンテキストを設定する方法について説明します。

- セキュリティ コンテキストについて （261 ページ）
- マルチ コンテキスト モードのライセンス （273 ページ）
- マルチ コンテキスト モードの前提条件 （275 ページ）
- マルチ コンテキスト モードのガイドライン （275 ページ）
- マルチ コンテキスト モードのデフォルト （277 ページ）
- マルチ コンテキストの設定 （277 ページ）
- コンテキストとシステム実行スペースの切り替え （290 ページ）
- セキュリティ コンテキストの管理 （291 ページ）
- セキュリティ コンテキストのモニタリング （295 ページ）
- マルチ コンテキスト モードの例 （307 ページ）
- マルチ コンテキスト モードの履歴 （309 ページ）

セキュリティ コンテキストについて

単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスとして機能します。マルチ コンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチ コンテキスト モードでサポートされない機能については、マルチ コンテキスト モードのガイドライン （275 ページ）を参照してください。

この項では、セキュリティ コンテキストの概要について説明します。

セキュリティ コンテキストの一般的な使用方法

マルチセキュリティ コンテキストを使用する状況には次のようなものがあります。

- サービス プロバイダーとして、多数のカスタマーにセキュリティ サービスを販売する。ASA 上でマルチ セキュリティ コンテキストを有効にすることによって、費用対効果の高

い、省スペース ソリューションを実装できます。このソリューションでは、カスタマーのトラフィックすべての分離とセキュリティが確保され、設定も容易です。

- 大企業または広大な大学の構内で、各部門の完全な独立を維持する必要がある。
- 企業で、部門ごとに個別のセキュリティ ポリシーの提供が求められている。
- 複数の ASA が必要なネットワークを使用する場合。

コンテキスト コンフィギュレーション ファイル

この項では、ASA がマルチ コンテキスト モードのコンフィギュレーションを実装する方法について説明します。

コンテキスト コンフィギュレーション

コンテキストごとに、ASA の中に 1 つのコンフィギュレーションがあり、この中ではセキュリティ ポリシーやインターフェイスに加えて、スタンドアロン デバイスで設定できるすべてのオプションが指定されています。コンテキスト コンフィギュレーションはフラッシュ メモリ内に保存することも、TFTP、FTP、または HTTP（S）サーバーからダウンロードすることもできます。

システム設定

システム管理者は、各コンテキスト コンフィギュレーションの場所、割り当てられたインターフェイス、およびその他のコンテキスト操作パラメータをシステム コンフィギュレーションに設定することで、コンテキストを追加および管理します。このコンフィギュレーションは、シングル モードのコンフィギュレーション同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。システム コンフィギュレーションに含まれているものに、フェールオーバー トラフィック専用の特殊なフェールオーバー インターフェイスがあります。

管理コンテキストの設定

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。管理コンテキストは、リモートではなくフラッシュ メモリに置く必要があります。

システムがすでにマルチ コンテキスト モードになっている場合、またはシングル モードから変換された場合、管理コンテキストが admin.cfg と呼ばれるファイルとして内部フラッシュ メ

モリに自動的に作成されます。このコンテキストの名前は "admin" です。admin.cfg を管理コンテキストとして使用しない場合は、管理コンテキストを変更できます。

ASA がパケットを分類する方法

ASA に入ってくるパケットはいずれも分類する必要があります。その結果、ASA は、どのコンテキストにパケットを送信するかを決定できます。

（注） 宛先 MAC アドレスがマルチキャストまたはブロードキャスト MAC アドレスの場合、パケットが複製され、各コンテキストに送信されます。

有効な分類子基準

この項では、分類子で使用される基準について説明します。

（注） インターフェイス宛の管理トラフィックでは、インターフェイス IP アドレスが分類に使用されます。

ルーティング テーブルはパケット分類には使用されません。

固有のインターフェイス

入力インターフェイスに関連付けられているコンテキストが 1 つだけの場合、ASA はパケットをそのコンテキストに分類します。トランスペアレント ファイアウォール モードでは、各コンテキストに固有のインターフェイスが必要なため、この方法は、常にパケット分類の目的で使用されます。

固有の MAC アドレス

複数のコンテキストが同じインターフェイスを共有している場合は、各コンテキストでそのインターフェイスに割り当てられた一意の MAC アドレスが分類子で使用されます。固有の MAC アドレスがないと、アップストリーム ルータはコンテキストに直接ルーティングできません。MAC アドレスの自動生成を有効にできます。各インターフェイスを設定するときに、手動で MAC アドレスを設定することもできます。

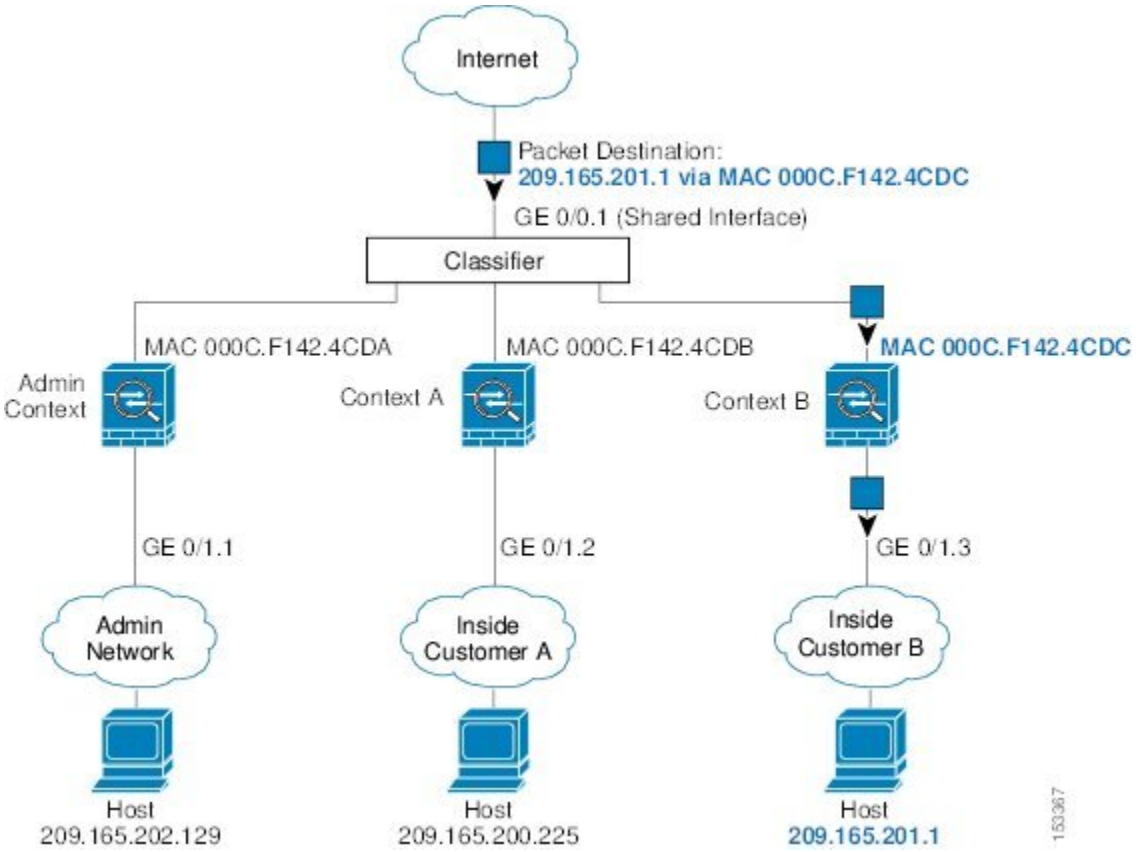
NAT の設定

固有の MAC アドレスの使用を有効にしなければ、ASA は、NAT コンフィギュレーション内のマッピングされたアドレスを使用してパケットを分類します。NAT コンフィギュレーションの完全性に関係なくトラフィック分類を行うことができるように、NAT ではなく MAC アドレスを使用することをお勧めします。

分類例

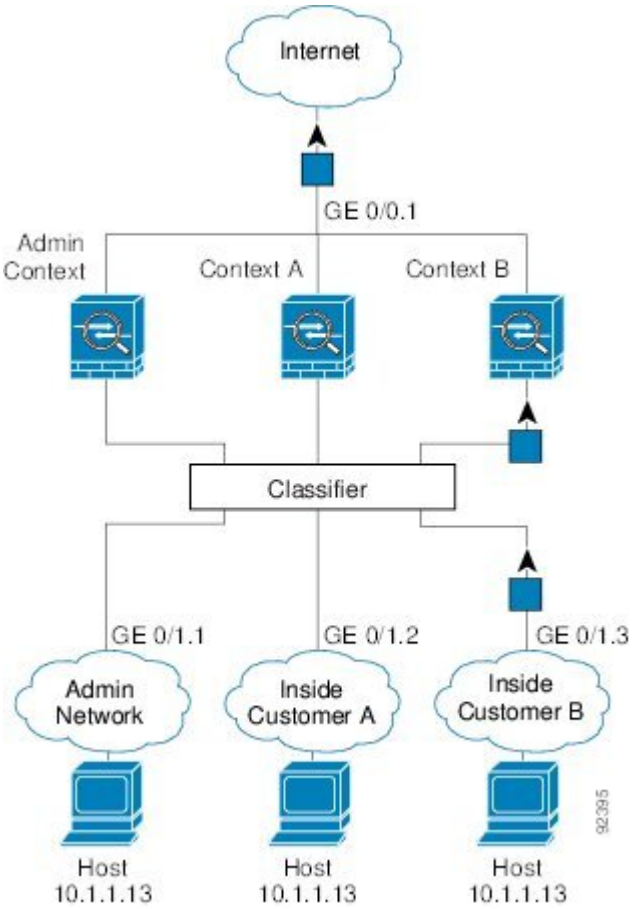
次の図に、外部インターフェイスを共有するマルチ コンテキストを示します。コンテキスト B にはルータがパケットを送信する MAC アドレスが含まれているため、分類子はパケットをコンテキスト B に割り当てます。

図 *36 : MAC* アドレスを使用した共有インターフェイスのパケット分類



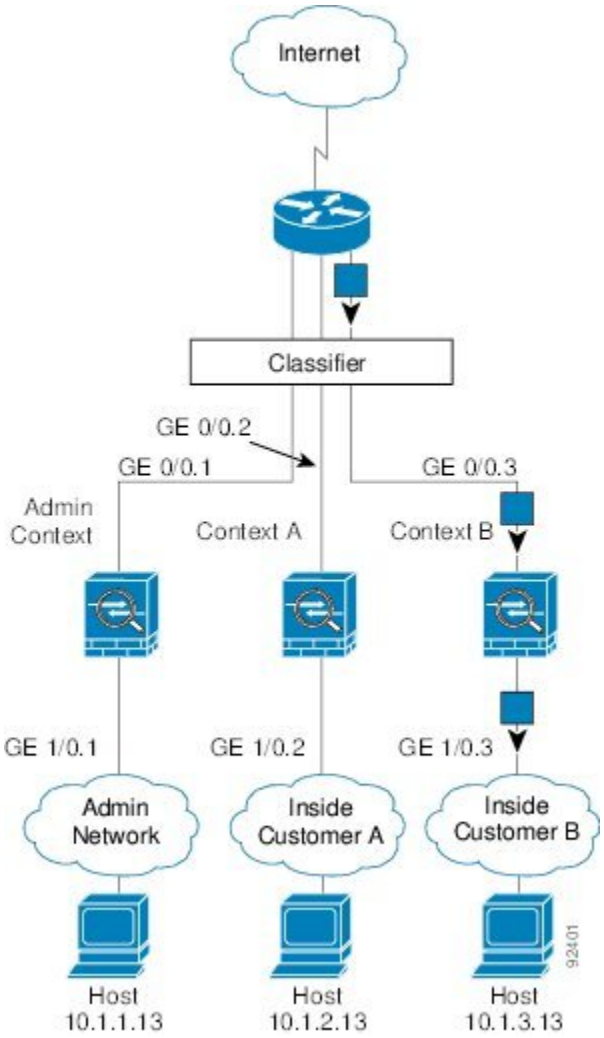
内部ネットワークからのものを含め、新たに着信するトラフィックすべてが分類される点に注意してください。次の図に、インターネットにアクセスするネットワーク内のコンテキストBのホストを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 0/1.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *37 :* 内部ネットワークからの着信トラフィック



トランスペアレントファイアウォールでは、固有のインターフェイスを使用する必要があります。次の図に、ネットワーク内のコンテキストBのホストに向けられたインターネットからのパケットを示します。分類子は、パケットをコンテキストBに割り当てます。これは、入力インターフェイスがギガビット イーサネット 1/0.3 で、このイーサネットがコンテキスト B に割り当てられているためです。

図 *38 :* トランスペアレント ファイアウォール コンテキスト



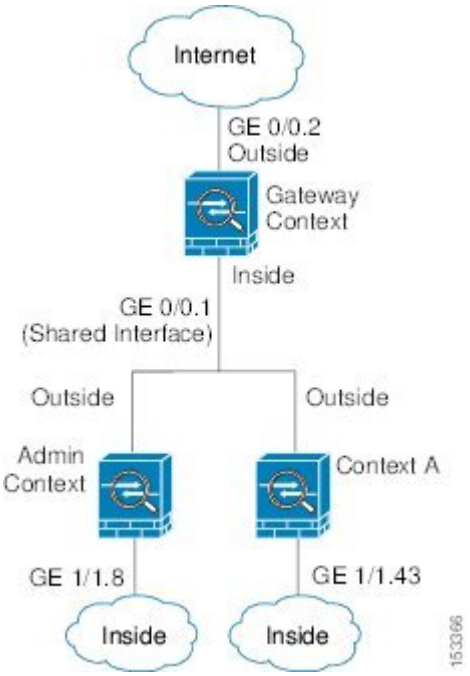
セキュリティ コンテキストのカスケード接続

コンテキストを別のコンテキストのすぐ前に置くことを、コンテキストをカスケード接続するといいます。一方のコンテキストの外部インターフェイスは、他方のコンテキストの内部インターフェイスと同じインターフェイスです。いくつかのコンテキストのコンフィギュレーションを単純化する場合、最上位のコンテキストの共有パラメータを設定することで、コンテキストをカスケード接続できます。

（注） コンテキストをカスケード接続するには、各コンテキスト インターフェイスに固有の MAC アドレスが必要です。MAC アドレスのない共有インターフェイスのパケットを分類するには限界があるため、固有の MAC アドレスを設定しないでコンテキストのカスケード接続を使用することはお勧めしません。

次の図に、ゲートウェイの背後に2つのコンテキストがあるゲートウェイ コンテキストを示します。

図 *39*：コンテキストのカスケード接続



セキュリティ コンテキストへの管理アクセス

ASA では、マルチ コンテキスト モードでのシステム管理アクセスと、各コンテキスト管理者のアクセスを提供します。

システム管理者のアクセス

2 つの方法で、システム管理者として ASA をアクセスできます。

- ASA コンソールにアクセスする。

  コンソールからシステム実行スペースにアクセスします。この場合、入力したコマンドは、システム コンフィギュレーションまたはシステムの実行（run-time コマンド）だけに影響します。

- Telnet、SSH、または ASDM を使用して管理コンテキストにアクセスする

システム管理者として、すべてのコンテキストにアクセスできます。

システム実行スペースでは AAA コマンドはサポートされていませんが、個別のログインのために、固有のイネーブル パスワードおよびユーザー名をローカル データベースに設定することができます。

コンテキスト管理者のアクセス

Telnet、SSH、または ASDM を使用して、コンテキストにアクセスできます。管理外コンテキストにログインすると、アクセスできるのはそのコンテキストのコンフィギュレーションだけになります。そのコンテキストに個別のログインを付与できます。

インターフェイス使用率の管理

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

ルーテッド ファイアウォール モードでは、管理インターフェイスをすべてのコンテキストで共有できます。

トランスペアレント ファイアウォール モードの管理インターフェイスは特殊です。許可される最大通過トラフィック インターフェイスに加えて、この管理インターフェイスを個別の管理専用インターフェイスとして使用できます。ただし、マルチコンテキストモードでは、どのインターフェイスもトランスペアレントコンテキスト間で共有させることはできません。代わりに、管理インターフェイスのサブインターフェイスを使用して、各コンテキストにインターフェイスを 1 つ割り当てることができます。ただし、サブインターフェイスを使用できるのは、Firepower デバイスモデル の管理インターフェイスに限られます。の ASA モデルの場合は、データインターフェイスまたはデータインターフェイスのサブインターフェイスを使用して、コンテキスト内のブリッジグループに追加する必要があります。

Firepower 4100/9300 シャーシトランスペアレントコンテキストでは、管理インターフェイスとサブインターフェイスのいずれも、特別なステータスを保持しません。この場合は、コンテキストをデータインターフェイスとして扱い、ブリッジグループに追加する必要があります(シングルコンテキストモードでは、管理インターフェイスで特別なステータスが保持されるので注意してください)。

トランスペアレントモードに関するもう 1 つの考慮事項：マルチコンテキストモードを有効にすると、設定されているすべてのインターフェイスが自動的に管理コンテキストに割り当てられます。たとえば、デフォルト設定に管理インターフェイスが含まれている場合、そのインターフェイスは管理コンテキストに割り当てられます。メインインターフェイスを管理コンテキストに割り当てたままで、ネイティブ VLAN を使用してメインインターフェイスを管理し、サブインターフェイスを使用して各コンテキストを管理するという選択肢もあります。管理コンテキストを透過的にすると、その IP アドレスは削除されることに注意してください。管理コンテキストをブリッジグループに割り当て、BVI に IP アドレスを割り当てる必要があります。

リソース管理の概要

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管

理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

リソース クラス

ASAは、リソースクラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。クラスの設定を使用するには、コンテキストを定義するときに、そのコンテキストをクラスに割り当てます。すべてのコンテキストは、別のクラスに割り当てられていなければ、デフォルトクラスに属します。したがって、コンテキストをデフォルト クラスに割り当てる必要は特にありません。コンテキストは1つのリソースクラスにだけ割り当てることができます。このルールの例外は、メンバ クラスで未定義の制限はデフォルト クラスから継承されることです。そのため実際には、コンテキストがデフォルト クラスおよび別のクラスのメンバになります。

リソース制限値

個々のリソースの制限値は、パーセンテージ（ハードシステム制限がある場合）または絶対値として設定できます。

ほとんどのリソースについては、ASAはクラスに割り当てられたコンテキストごとにリソースの一部を確保することはしません。代わりに、ASAはコンテキストごとに上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。例外は、VPN リソース タイプです。このリソースはオーバーサブスクライブできないため、各コンテキストに割り当てられたリソースは保証されます割り当てられた量を超える、VPNセッションの一時的なバーストに対応できるように、ASAは「burst」という VPN リソース タイプをサポートしています。このリソースは、残りの未割り当て VPN セッションに等しくなります。バーストセッションはオーバーサブスクライブでき、コンテキストが先着順で使用できます。

デフォルト クラス

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルトクラスから継承されます。これとは逆に、すべてのリソースに対する制限値を設定してクラスを作成すると、そのクラスではデフォルトクラスの設定を何も使用しません。

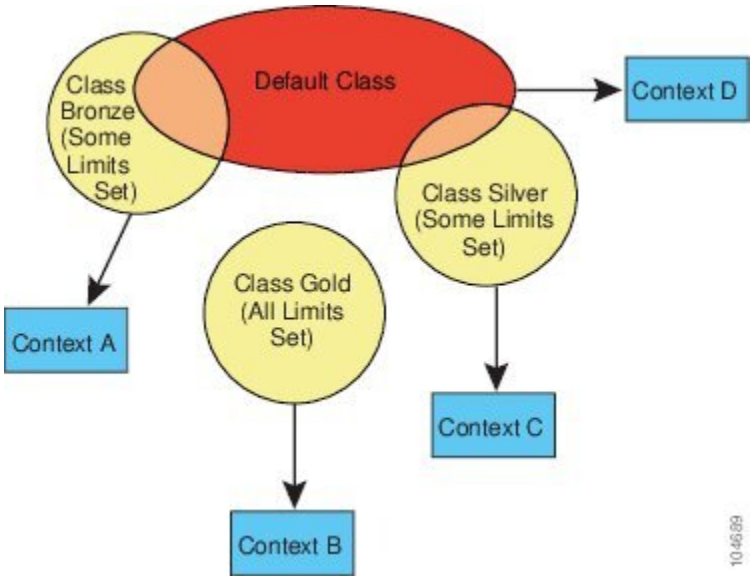
ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。

- ASDM セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：（モデルによって異なる）。（システムの最大値）。
- セキュアクライアント ピア — 0 セッション。（セキュアクライアント ピアを許可するようにクラスを手動で設定する必要があります）。
- VPN サイトツーサイト トンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。

次の図に、デフォルト クラスと他のクラスの関係を示します。コンテキスト A および C は、いくつかの制限が設定されたクラスに属しており、それ以外の制限はデフォルト クラスから継承します。コンテキスト B は、属している Gold クラスですべての制限が設定されているため、デフォルト クラスから制限値を継承しません。コンテキスト D はクラスに割り当てられなかったため、デフォルトでデフォルト クラスのメンバになります。

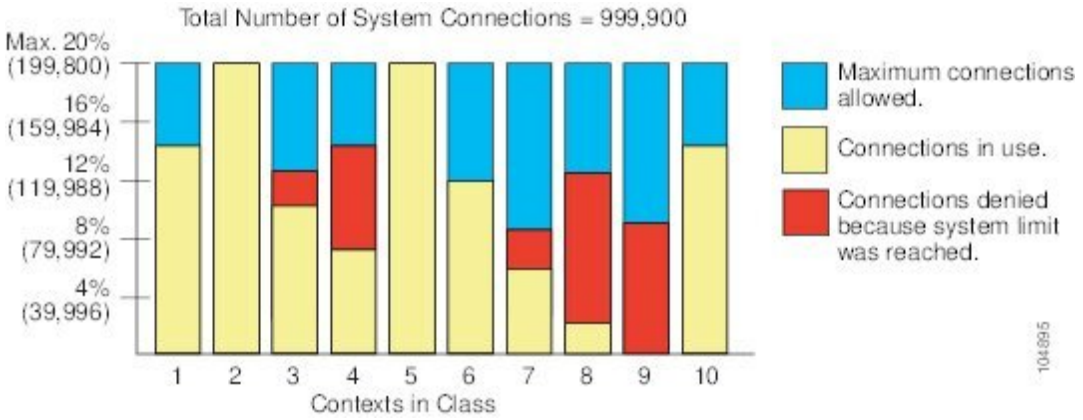
図 *40 :* リソース クラス



オーバーサブスクライブ リソースの使用

ASA をオーバーサブスクライブするには、割り当て率の合計が 100% を超えるようにあるリソースをすべてのコンテキストに割り当てます（非バーストの VPN リソースを除く）。たとえば、接続がコンテキストあたり 20% までに制限されるように Bronze クラスを設定し、それから 10 個のコンテキストをそのクラスに割り当てれば、リソースの合計を 200% にできます。コンテキストがシステム制限を超えて同時に使用する場合、各コンテキストは意図した 20% を下回ります。

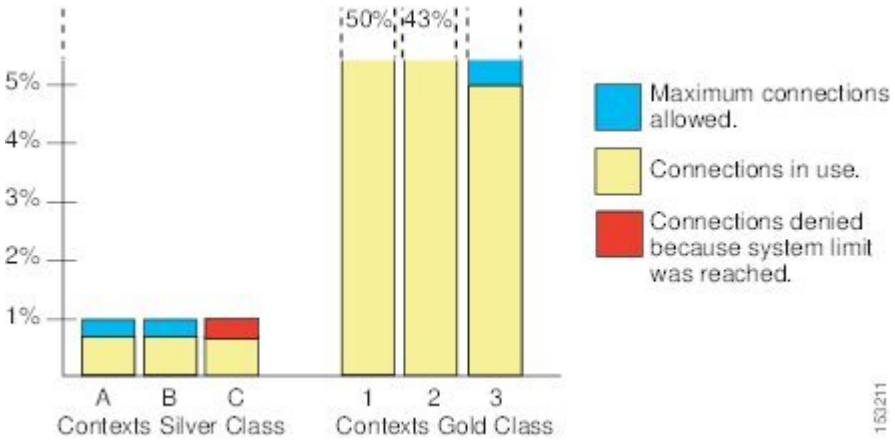
図 *41* : リソース オーバーサブスクリプション



無限リソースの使用

ASA は、パーセンテージや絶対値ではなく、クラス内の 1 つ以上のリソースに無制限アクセスを割り当てることができます。リソースが無制限の場合、コンテキストはシステムで使用可能な量までリソースを使用できます。たとえば、コンテキスト A、B、C が Silver クラスに属しており、クラスの各メンバの使用量が接続の 1% に制限されていて、合計 3% が割り当てられているが、3 つのコンテキストが現在使用しているのは合計 2% だけだとします。Gold クラスは、接続に無制限にアクセスできます。Gold クラスのコンテキストは、「未割り当て」接続のうち 97% を超える分も使用できます。つまり、現在コンテキスト A、B、C で使用されていない、接続の 1% も使用できます。その場合は、コンテキスト A、B、C の使用量が、これらの制限の合計である 3% に達することは不可能になります無制限アクセスの設定は、ASA のオーバーサブスクライブと同様ですが、システムをどの程度オーバーサブスクライブできるかを詳細には制御できません。

図 *42* : 無限リソース



MAC アドレスについて

手動でMACアドレスを割り当てて、デフォルトを上書きすることができます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。.

（注） 親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

マルチコンテキスト モードでの MAC アドレス

MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。あるインターフェイスを共有させる場合に、コンテキストごとにそのインターフェイスの固有 MAC アドレスを設定していなかった場合は、他の分類方法が試行されますが、その方法では十分にカバーされないことがあります。

コンテキスト間でのインターフェイス共有を許可するには、共有されるコンテキストインターフェイスそれぞれで仮想 MAC アドレスの自動生成を有効にしてください。

自動 MAC アドレス

マルチコンテキストモードでは、自動生成によって、コンテキストに割り当てられたすべてのインターフェイスに一意のMACアドレスが割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASAは、次の形式を使用して MACアドレスを生成します。

A2*xx.yyzz.zzzz*

*xx.yy*はユーザ定義プレフィックスまたはインターフェイスMACアドレスの最後の2バイトに基づいて自動生成されたプレフィックスであり、*zz.zzzz* はASAによって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例としてたとえば、プレフィックス77を設定すると、ASAは77を16進数値004D (*yyxx*)に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆転されます（*xxyy*）。

A24**D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのないMACアドレス形式は、従来のバージョンです。従来の形式に関する詳細については、コマンドリファレンスの**mac-address auto**コマンドを参照してください。

VPN サポート

VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

マルチ コンテキスト モードでサイト間 VPN を使用できます。

リモート アクセス VPN の場合は、SSL VPN および IKEv2 プロトコルに AnyConnect 3.x 以降を使用する必要があります。 セキュアクライアント のイメージとカスタマイズ、およびすべてのコンテキストで共有フラッシュメモリを使用するために、コンテキストごとにフラッシュストレージをカスタマイズできます。サポートされていない機能については、マルチ コンテキスト モードのガイドライン （275 ページ） を参照してください。ASA リリースごとにサポートされる VPN 機能の詳細なリストについては、マルチ コンテキスト モードの履歴 （309 ページ） を参照してください。

（注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードのライセンス

モデル	ライセンス要件
Firepower 1010	サポートしない

モデル	ライセンス要件
Firepower 1100	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Firepower 1120*：*5* *Firepower 1140*：*10* *Firepower 1150*：*25*
Cisco Secure Firewall 1210/1220	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Cisco Secure Firewall 1210*：*5* *Cisco Secure Firewall 1220*：*10*
Secure Firewall 1230/1240/1250	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Cisco Secure Firewall 1230*：*25* *Cisco Secure Firewall 1240*：*25* *Cisco Secure Firewall 1250*：*25*
Cisco Secure Firewall 3100	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Secure Firewall 3105*：*100* *Cisco Secure Firewall 3110*：*100* *Cisco Secure Firewall 3120*：*100* *Cisco Secure Firewall 3130*：*100* *Cisco Secure Firewall 3140*：*100*
Firepower 4100	Essentialsライセンス：10 コンテキスト オプションライセンス：最大 *250* コンテキスト
Cisco Secure Firewall 4200	Essentialsライセンス：2 コンテキスト オプションライセンス、最大： *Secure Firewall 4215*：*250* *Secure Firewall 4225*：*250* *Secure Firewall 4245*：*250*

モデル	ライセンス要件
Firepower 9300	Essentialsライセンス：10 コンテキスト オプションライセンス：最大 *250* コンテキスト
ISA 3000	サポートしない
ASA 仮想	サポートしない

（注） 管理コンテキストに管理専用インターフェイスのみが含まれていて、通過トラフィックのデータインターフェイスが含まれていない場合は、制限に対してカウントされません。

（注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。

マルチ コンテキスト モードの前提条件

マルチ コンテキスト モードに切り替えた後で、システム コンフィギュレーションにアクセスするためにシステムまたは管理コンテキストに接続します。管理以外のコンテキストからシステムを設定することはできません。デフォルトでは、マルチ コンテキスト モードをイネーブルにした後はデフォルトの管理 IP アドレスを使用して管理コンテキストに接続できます。

マルチ コンテキスト モードのガイドライン

フェールオーバー

アクティブ/アクティブ モードフェールオーバーは、マルチ コンテキスト モードでのみサポートされます。

IPv6

クロス コンテキスト IPv6 ルーティングはサポートされません。

サポートされない機能

マルチコンテキスト モードでは、次の機能をサポートしません。

- RIP
- OSPFv3 （OSPFv2 がサポートされます）。

- マルチキャスト ルーティング
- 脅威の検出
- ユニファイド コミュニケーション
- QoS
- 仮想トンネルインターフェイス（VTI）
- スタティック ルート トラッキング
- Cisco Secure Firewall 1210/1220 のスイッチポート。

マルチ コンテキスト モードでは、次のリモート アクセス VPN の機能を現在サポートしません。

- AnyConnect 2.x 以前
- IKEv1
- SAML
- WebLaunch
- VLAN Mapping
- HostScan
- VPN ロード バランシング
- カスタマイゼーション
- L2TP

その他のガイドライン

- コンテキストモード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。コンフィギュレーションを別のデバイスにコピーする必要がある場合は、新規デバイスのモードを match に設定します。
- デフォルトで、Cisco Secure Firewall 1210/1220デバイスは、シングル コンテキスト モードになります。スイッチポートはマルチ コンテキスト モードではサポートされていないため、マルチ コンテキスト モードに変換する前に、すべてのインターフェイスをルータ インターフェイスに変換する必要があります。を参照してください。
- フラッシュ メモリのルート ディレクトリにコンテキスト コンフィギュレーションを保存する場合、一部のモデルでは、メモリに空き容量があっても、そのディレクトリに保存する余地がなくなることがあります。この場合は、コンフィギュレーション ファイルのサブディレクトリを作成します。Background: some models use the FAT 16 file system for internal flash memory, and if you do not use 8.3-compliant short names, or use uppercase characters, then fewer than 512 files and folders can be stored because the file system uses up slots to store long file names（see http://support.microsoft.com/kb/120138/en-us).

- ACI では、すべてのリーフで同じ MAC アドレスを使用してポリシーベースリダイレクト（PBR）ヘルスチェックが実行されます（L2 ping）。これにより、MAC フラップが発生します。MAC フラップを解決するには、インラインセットでタップモードオプションを設定します。ただし、Firewall Threat Defense ハイアベイラビリティが設定されている場合は、フェールオーバー中の接続処理のために MAC 学習を有効にする必要があります。したがって、インラインセット インターフェイスを使用する HA ペアの Firewall Threat Defense を含む ACI 環境では、パケット損失を回避するために、スタンドアロンかクラスタで Firewall Threat Defense を展開します。

マルチ コンテキスト モードのデフォルト

- デフォルトで、ASA はシングル コンテキスト モードになります。
- 「デフォルト クラス （269 ページ）」を参照してください。

マルチ コンテキストの設定

手順

ステップ 1 マルチ コンテキスト モードの有効化または無効化 （278 ページ）.

ステップ 2 （任意）リソース管理用のクラスの設定 （280 ページ）。

（注）
VPN のサポートのために、リソース クラスの VPN リソースを設定する必要があります。デフォルト クラスは VPN を許可しません。

ステップ 3 システム実行スペースでインターフェイスを設定します。

- Firepower 1100、Secure Firewall 3100/4200：基本的なインターフェイス設定 （825 ページ）。
- Cisco Secure Firewall 1200 ー 基本的なインターフェイス設定 （825 ページ） および Firepower 1010 と Cisco Secure Firewall 1210/1220 スイッチポートの基本インターフェイス設定 （845 ページ）。
- Firepower 4100/9300：論理デバイス Firepower 4100/9300 （205 ページ）

ステップ 4 セキュリティ コンテキストの設定 （285 ページ）.

ステップ 5 （任意）コンテキスト インターフェイスへの MAC アドレスの自動割り当て （289 ページ）。

ステップ 6 コンテキストのインターフェイス コンフィギュレーションを完成させます。「ルーテッドモードおよびトランスペアレント モードのインターフェイス （927 ページ）」を参照してください。

マルチ コンテキスト モードの有効化または無効化

シスコへの発注方法によっては、ASA がすでにマルチセキュリティ コンテキスト用に設定されている場合があります。シングル モードからマルチ モードに変換する必要がある場合は、この項の手順に従ってください。

マルチ コンテキスト モードの有効化

シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。これらはシステム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーションと、（内部フラッシュ メモリのルート ディレクトリの）管理コンテキストで構成される admin.cfg です。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュ メモリのルート ディレクトリに）保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

始める前に

スタートアップ コンフィギュレーションが実行コンフィギュレーションと異なっている場合はバックアップします。シングル モードからマルチ モードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイルに変換します。元のスタートアップ コンフィギュレーションは保存されません。コンフィギュレーションまたはその他のファイルのバックアップと復元（1577 ページ）を参照してください。

手順

マルチコンテキストモードに変更します。

mode multiple

例：

モードを変更して設定を変換し、システムをリロードするように求められます。

（注）
SSH接続を再確立する前に、管理コンテキストでRSAキーペアを再生成する必要があります。コンソールから、**crypto key generate rsa modulus** コマンドを入力します。詳細については、SSH アクセスの設定 （1495 ページ）を参照してください。

例：

```
ciscoasa(config)# mode multiple
```

```
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm]
Convert the system configuration? [confirm]
!
The old running configuration file will be written to flash

Converting the configuration - this may take several minutes for a large configuration

The admin context configuration will be written to flash

The new running configuration file was written to flash
Security context mode: multiple
ciscoasa(config)#


***
*** --- START GRACEFUL SHUTDOWN ---
***
*** Message to all terminals:
***
***   change mode
Shutting down isakmp
Shutting down webvpn
Shutting down License Controller
Shutting down File system



***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
```

シングルコンテキスト モードの復元

以前の実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてモードをシングル モードに変更するには、次の手順を実行します。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 元の実行コンフィギュレーションのバックアップ バージョンを現在のスタートアップ コンフィギュレーションにコピーします。

copy disk0:old_running.cfg startup-config

例：

```
ciscoasa(config)# copy disk0:old_running.cfg startup-config
```

ステップ 2 モードをシングル モードに設定します。

mode single

例：

```
ciscoasa(config)# mode single
```

ASA をリブートするよう求められます。

リソース管理用のクラスの設定

システム コンフィギュレーションでクラスを設定するには、次の手順を実行します。新しい値を指定してコマンドを再入力すると、特定のリソース制限値を変更できます。

始める前に

- この手順はシステム実行スペースで実行します。
- 以下の表に、リソース タイプおよび制限を記載します。**show resource types** コマンドも参照してください。

（注） 「システム制限」に「該当なし」と記述されている場合、そのリソースにはハードシステム制限がないため、リソースのパーセンテージを設定できません。

表 *7:* リソース名および制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
asdm	同時接続数	最小 1 最大 5	200	ASDM 管理セッション。 ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 200 の場合、HTTPS セッション数は 400 に制限されます。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
conns	同時またはレート	該当なし	同時接続数：モデルごとの接続制限については、モデルごとのライセンス（172ページ）を参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。 （注） syslog メッセージは、xlates または conns のいずれか制限が低い方に対して生成されます。たとえば、xlates の制限を 7、conns の制限を 9 に設定した場合、ASA は syslog メッセージ 321001（「Resource 'xlates' limit of 7 reached for context 'ctx1'」）のみ生成し、321002（「Resource 'conn rate' limit of 5 reached for context 'ctx1'」）は生成しません。
hosts	同時接続数	N/A	なし	ASA 経由で接続可能なホスト。
inspects	利率	N/A	なし	アプリケーション インスペクション数/秒。
mac-addresses	同時接続数	該当なし	（モデルによって異なる）	トランスペアレントファイアウォールモードでは、MAC アドレス テーブルで許可される MAC アドレス数。
ルート	同時接続数	N/A	なし	ダイナミック ルート。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
vpn burst anyconnect	同時接続数	該当なし	モデルに応じた セキュアクライアント ピア数から、**vpn anyconnect** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn anyconnect** でコンテキストに割り当てられた数を超えて許可されるセキュアクライアント セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、**vpn anyconnect** で割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが **vpn burst anyconnect** に使用可能です。**vpn anyconnect** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst anyconnect** ではオーバーサブスクライブが可能です。バーストプールをすべてのコンテキストが、先着順に使用できます。
vpn anyconnect	同時接続数	該当なし	ご使用のモデルに使用できる セキュアクライアント Premium ピアについては、モデルごとのライセンス（172 ページ）を参照してください。	セキュアクライアントピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。
vpn burst other	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえばモデルが 5000 セッションをサポートしており、**vpn other** のすべてのコンテキスト全体で 4000 セッションを割り当てると、残りの 1000 セッションは **vpn burst other** に使用できます。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能です。すべてのコンテキストでバースト プールを先着順に使用できます。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限	説明
vpn other	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、モデルごとにサポートされている機能のライセンス （72 ページ）を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。
ikev1 in-negotiation	同時（パーセンテージのみ）	該当なし	このコンテキストに割り当てられている Other VPN セッションのパーセンテージ。セッションをコンテキストに割り当てるには、**vpn other** リソースを参照してください。	コンテキストでの Other VPN パーセンテージ制限として表される、着信 IKEv1 SA ネゴシエーション。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション。
ストレージ	MB	最大値は、指定するフラッシュ メモリのドライブによって異なります。	最大値は、指定するフラッシュ メモリのドライブによって異なります。	コンテキストでのディレクトリのストレージ制限（MB 単位）。ドライブを指定するには、**storage-url** コマンドを使用します。
syslogs	利率	N/A	なし	Syslog メッセージ数/秒。
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
xlates	同時接続数	N/A	なし	ネットワーク アドレス変換。

手順

ステップ 1 クラス名を指定して、クラス コンフィギュレーション モードを開始します。

class *name*

例：

```
ciscoasa(config)# class gold
```

name は、最大 20 文字の文字列です。デフォルト クラスの制限値を設定するには、名前として **default** と入力します。

ステップ 2 リソース タイプのリソース制限を設定します。

limit-resource [**rate**] *resource_name number*[**%**]

例：

```
ciscoasa(config-class)# limit-resource rate inspects 10
```

- リソース タイプのリストについては、上記の表を参照してください。**all** を指定すると、すべてのリソースが同じ値に設定されます。特定のリソースの値も指定した場合は、その制限は **all** に対して設定された制限よりも優先されます。
- **rate** 引数を入力して、特定のリソースの毎秒レートを設定します。
- ほとんどのリソースについては、**0** を *number* に対して設定すると、そのリソースは無制限となるか、システム制限を上限とする（システム制限がある場合）ことになります。VPN のリソースについては、**0** を指定すると制限なしと設定されます。
- システム制限がないリソースの場合は、パーセンテージ（**%**）を設定できません。絶対値のみを設定できます。
- また、コンテキスト内で **quota management-session** コマンドを設定して最大管理セッション（SSH など）を設定した場合は、小さい方の値が使用されます。

例

たとえば、conns のデフォルト クラス制限を無制限ではなく 10% に設定し、サイト ツーサイト VPN トンネル 5 本と VPN バースト用のトンネル 2 本を許可するには、次のコマンドを入力します。

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 5
ciscoasa(config-class)# limit-resource vpn burst other 2
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
```

```
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 5000
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5
```

コンテキストにリソース クラスが設定されている場合、チェックが行われます。VPN リモート アクセスの接続試行の前に適切なライセンスがインストールされていなければ、警告メッセージが生成されます。その場合、管理者が Secure Client Premier ライセンスを取得する必要があります。たとえば、次のような警告が表示されます。

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn anyconnect 10.0%
ciscoasa(config-class)# context test
Creating context 'text'...Done. (3)
ciscoasa(config-ctx)# member vpn
WARNING: Multi-mode remote access VPN support requires an AnyConnect Apex license.
Warning: An Access Context license is required for remote-access VPN support in multi-mode.
ciscoasa(config-ctx)#
```

セキュリティ コンテキストの設定

システム コンフィギュレーションのセキュリティ コンテキスト定義では、コンテキスト名、コンフィギュレーション ファイルの URL、コンテキストが使用できるインターフェイス、およびその他の設定値を指定します。

始める前に

- この手順はシステム実行スペースで実行します。
- インターフェイスを設定します。トランスペアレントモードのコンテキストでは、コンテキスト間でインターフェイスを共有できないため、サブインターフェイスの使用が必要になる場合があります。管理インターフェイスの使用計画については、「インターフェイス使用率の管理 （268 ページ）」を参照してください。
  - Firepower 1100、Secure Firewall 3100/4200：基本的なインターフェイス設定 （825 ページ）。
  - Firepower 4100/9300：論理デバイス Firepower 4100/9300 （205 ページ）
- 管理コンテキストがない場合（コンフィギュレーションをクリアした場合など）は、最初に次のコマンドを入力して管理コンテキスト名を指定する必要があります。

  ```
  ciscoasa(config)# admin-context name
  ```

  このコンテキストはコンフィギュレーション内にまだ存在しませんが、続いて **context** *name* コマンドを入力して管理コンテキスト コンフィギュレーションに進むことができます。

手順

ステップ 1 コンテキストを追加または変更します。

context *name*

例：

```
ciscoasa(config)# context admin
```

name は最大 32 文字の文字列です。この名前では大文字と小文字が区別されるため、たとえば、「customerA」および「CustomerA」という 2 つのコンテキストを保持できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンは使用できません。

（注）
「System」および「Null」（大文字と小文字の両方）は予約されている名前であり、使用できません。

ステップ 2 （任意） このコンテキストの説明を追加します。

description *text*

例：

```
ciscoasa(config-ctx)# description Admin Context
```

ステップ 3 コンテキストで使用できるインターフェイスを指定します。

インターフェイスを割り当てるには：

allocate-interface *interface_id* [*mapped_name*] [**visible** | **invisible**]

1 つまたは複数のサブインターフェイスを割り当てるには：

allocate-interface *interface_id***.***subinterface* [**-***interface_id***.***subinterface*] [*mapped_name*[**-***mapped_name*]] [**visible** | **invisible**]

例：

```
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

（注）
インターフェイス タイプとポート番号の間にスペースを含めないでください。

- これらのコマンドを複数回入力して複数の範囲を指定します。このコマンドの **no** 形式を使用して割り当てを削除すると、このインターフェイスを含むコンテキスト コマンドはいずれも実行コンフィギュレーションから削除されます。

- ルーテッドモードでは、必要に応じて同じインターフェイスを複数のコンテキストに割り当てることができます。トランスペアレントモードでは、インターフェイスを共有できません。
- *mapped_name* は、インターフェイス ID の代わりにコンテキスト内で使用できるインターフェイスの英数字のエイリアスです。マッピング名を指定しない場合、インターフェイス IDがコンテキスト内で使用されます。セキュリティ目的で、コンテキストがどのインターフェイスを使用しているかをコンテキスト管理者には知らせないようにすることができます。マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線のみを使用できます。たとえば、次の名前を使用できます。**int0**、**inta**、**int_0**。
- サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。
  - マッピング名は、アルファベット部分と、それに続く数値部分で構成する必要があります。マッピング名のアルファベット部分は、範囲の両端で一致している必要があります。たとえば、次のような範囲を入力します。**int0-int10**。たとえば、gig0/1.1-gig0/1.5 **happy**1-**sad**5 と入力した場合、このコマンドは失敗します。
  - マッピング名の数値部分には、サブインターフェイスの範囲と同じ個数の数値を含める必要があります。たとえば、次のように、両方の範囲に 100 個のインターフェイスが含まれている場合：**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100**。たとえば、gig0/0.**100**-gig0/0.**199** int**1**-int**15** と入力した場合、コマンドは失敗します。
- マッピング名を設定している場合に **show interface** コマンドで実際のインターフェイス ID を参照するには、**visible** を指定します。デフォルトの **invisible** キーワードでは、マッピング名だけが表示されます。

ステップ 4 システムがコンテキスト コンフィギュレーションをダウンロードする URL を識別します。

config-url *url*

フラッシュ メモリまたはリモート サーバのファイルを指定できます。

例：

```
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
```

ステップ 5 （任意） 各コンテキストでフラッシュメモリを使用して セキュアクライアント などの VPN パッケージを保存できるだけでなく、セキュアクライアントポータルのカスタマイズ用のストレージも提供できます。たとえば、マルチコンテキストモードを使用してダイナミック アクセス ポリシーに セキュアクライアント プロファイルを設定する場合、コンテキスト固有のプライベートストレージを計画する必要があります。読み取り専用の共有記憶域だけでなく、コンテキストごとに専用の記憶域も使用できます。**注**：**mkdir** コマンドを使用して、指定したディスク上にターゲット ディレクトリがすでに存在することを確認してください。

storage-url {**private** | **shared**} [**disk***n***:/**]*path* [*context_label*]

例：

```
ciscoasa(config)# mkdir disk1:/private-storage
ciscoasa(config)# mkdir disk1:/shared-storage
ciscoasa(config)# context admin
ciscoasa(config-ctx)# storage-url private disk1:/private-storage context
ciscoasa(config-ctx)# storage-url shared disk1:/shared-storage shared
```

private 記憶域は、コンテキストごとに 1 つ指定できます。コンテキスト内から（およびシステム実行スペースから）、このディレクトリの読み取り/書き込み/削除操作を実行できます。ディスク番号を指定しない場合、デフォルトで disk0 に設定されます。ASA は指定された *path* にサブディレクトリを作成し、コンテキストに基づく名前を付けます。たとえば、contextA の場合、**disk1:/private-storage** をパスとして指定すると、ASA はこのコンテキストのサブディレクトリを **disk1:/private-storage/contextA/** に作成します。オプションで、ファイル システムがコンテキスト管理者に公開されないよう、このパスにコンテキスト内での名前を指定することもできます。それには、*context_label* を使用します。たとえば、*context_label* を **context** として指定すると、コンテキスト内からは、このディレクトリは **context:** と呼ばれます。コンテキストごとに許容するディスク容量を制御する方法については、リソース管理用のクラスの設定（280 ページ）を参照してください。

指定できる読み取り専用の **shared** 記憶域はコンテキストごとに 1 つですが、共有ディレクトリは複数作成できます。セキュアクライアントパッケージなど、すべてのコンテキストで共有できる共通の大きなファイルの重複を減らすために、共有のストレージスペースを使用できます。この記憶域は複数のコンテキストで共有されるため、ASA は記憶域にはコンテキストのサブディレクトリを作成しません。共有ディレクトリの書き込みおよび削除操作は、システム実行スペースでのみ実行できます。

ステップ 6 （任意） コンテキストをリソース クラスに割り当てます。

member *class_name*

例：

```
ciscoasa(config-ctx)# member gold
```

クラスを指定しない場合、コンテキストはデフォルト クラスに属します。コンテキストは 1 つのリソース クラスにだけ割り当てることができます。

ステップ 7 （任意）アクティブ/アクティブ フェールオーバーのフェールオーバー グループにコンテキストを割り当てます。

join-failover-group {**1** | **2**}

例：

```
ciscoasa(config-ctx)# join-failover-group 2
```

デフォルトでは、コンテキストはグループ 1 にあります。管理コンテキストは常にグループ 1 に置く必要があります。

ステップ 8 （任意） このコンテキストに対してクラウド Web セキュリティを有効にします。

scansafe [**license** *key*]

例：

```
ciscoasa(config-ctx)# scansafe
```

license を指定しない場合は、システム コンフィギュレーションで設定されているライセンスがこのコンテキストで使用されます。ASAは、要求がどの組織からのものかを示すために、認証キーをクラウド Web セキュリティ プロキシ サーバーに送信します。認証キーは 16 バイトの 16 進数です。

ScanSafeの詳細については、ファイアウォールのコンフィギュレーション ガイドを参照してください。

例

次の例では、管理コンテキストを「administrator」と設定し、「administrator」というコンテキストを内部フラッシュ メモリに作成してから、2 つのコンテキストを FTP サーバから追加します。

```
ciscoasa(config)# admin-context admin
ciscoasa(config)# context admin
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold


ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member silver
```

コンテキスト インターフェイスへの MAC アドレスの自動割り当て

この項では、MACアドレスの自動生成の設定方法について説明します。MACアドレスは、コンテキスト内でパケットを分類するために使用されます。

始める前に

- コンテキストでインターフェイスの **nameif** コマンドを設定すると、ただちに新規MACアドレスが生成されます。コンテキストインターフェイスを設定した後でこの機能をイネー

ブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。

手順

プライベート MAC アドレスを各コンテキスト インターフェイスに自動的に割り当てます。

mac-address auto [**prefix** *prefix*]

例：

```
ciscoasa(config)# mac-address auto prefix 19
```

プレフィックスを入力しない場合は、ASA によって、インターフェイスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

コンテキストとシステム実行スペースの切り替え

システム実行スペース（または管理コンテキスト）にログインした場合は、コンテキストを切り替えながら、各コンテキスト内でコンフィギュレーションやタスクのモニタリングを実行することができます。コンフィギュレーション モードで編集される実行コンフィギュレーション、つまり **copy** コマンドや **write** コマンドで使用される実行コンフィギュレーションは、ユーザーのログイン先によって決まります。システム実行スペースにログインした場合、実行コンフィギュレーションはシステム コンフィギュレーションのみで構成され、コンテキストにログインした場合は、実行コンフィギュレーションはそのコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムおよびすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

手順

ステップ 1 コンテキストに変更します。

changeto context *name*

プロンプトが ciscoasa/*name*# に変化します。

ステップ 2 システム実行スペースに変更します。

changeto system

プロンプトが ciscoasa# に変化します。

セキュリティ コンテキストの管理

この項では、セキュリティ コンテキストを管理する方法について説明します。

セキュリティ コンテキストの削除

現在の管理コンテキストは削除できません。ただし、**clear context** コマンドを使用してすべてのコンテキストを削除すれば、管理コンテキストも削除できます。

（注） フェールオーバーを使用すると、アクティブ装置でコンテキストを削除した時刻と、スタンバイ装置でコンテキストが削除された時刻との間で遅延が生じます。アクティブ装置とスタンバイ装置の間でインターフェイス数が一致していないことを示すエラー メッセージが表示される場合があります。このエラーは一時的に表示されるもので、無視できます。

始める前に

この手順はシステム実行スペースで実行します。

手順

ステップ 1 単一のコンテキストを削除します。

no context *name*

すべてのコンテキスト コマンドを削除することもできます。コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

ステップ 2 すべてのコンテキスト（管理コンテキストを含む）を削除します。

clear context

コンテキスト コンフィギュレーション ファイルがコンフィギュレーション URL の場所から削除されることはありません。

管理コンテキストの変更

システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

管理コンテキストは、他のコンテキストとまったく同じです。ただ、ユーザーが管理コンテキストにログインすると、システム管理者権限を持つので、システム コンテキストおよび他のすべてのコンテキストにアクセス可能になる点が異なります。管理コンテキストは制限されていないため、通常のコンテキストとして使用できます。ただし、管理コンテキストにログインすると、すべてのコンテキストへの管理者特権が付与されるため、場合によっては、管理コンテキストへのアクセスを適切なユーザーに制限する必要があります。

始める前に

- コンフィギュレーション ファイルが内部フラッシュ メモリに保存されている限り、任意のコンテキストを管理コンテキストとして設定できます。
- この手順はシステム実行スペースで実行します。

手順

管理コンテキストを設定します。

admin-context *context_name*

例：

```
ciscoasa(config)# admin-context administrator
```

Telnet、SSH、HTTPS など、管理コンテキストに接続しているリモート管理セッションはすべて終了します。新しい管理コンテキストに再接続する必要があります。

いくつかのシステム コンフィギュレーション コマンド、たとえば **ntp server** では、管理コンテキストに所属するインターフェイス名が指定されます。管理コンテキストを変更した場合に、そのインターフェイス名が新しい管理コンテキストに存在しないときは、そのインターフェイスを参照するシステム コマンドはすべて、アップデートしてください。

セキュリティ コンテキスト URL の変更

この項では、コンテキスト URL を変更する方法について説明します。

始める前に

- セキュリティ コンテキスト URL は、新しい URL からコンフィギュレーションをリロードしないと変更できません。ASA は、新しいコンフィギュレーションを現在の実行コンフィギュレーションにマージします。
- 同じ URL を再入力した場合でも、保存されたコンフィギュレーションが実行コンフィギュレーションにマージされます。
- マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。
  - コンフィギュレーションが同じ場合、変更は発生しません。
  - コマンドが衝突する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。実行コンフィギュレーションが空白の場合（たとえば、サーバが使用不可でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。
- コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションをクリアしてから、新しい URL からコンフィギュレーションをリロードすることができます。
- この手順はシステム実行スペースで実行します。

手順

ステップ 1 （オプション、マージを実行しない場合）コンテキストに変更して、コンフィギュレーションをクリアします。

changeto context *name*

clear configure all

例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(config)# clear configure all
```

マージを実行する場合は、ステップ 2 にスキップします。

ステップ 2 システム実行スペースに変更します。

changeto system

例：

```
ciscoasa/ctx1(config)# changeto system
ciscoasa(config)#
```

ステップ 3 変更するコンテキストのコンテキスト コンフィギュレーション モードを開始します。

context *name*

例：

```
ciscoasa(config)# context ctx1
```

ステップ 4 新しい URL を入力します。システムは、動作中になるように、ただちにコンテキストをロードします。

config-url *new_url*

例：

```
ciscoasa(config)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/ctx1.cfg
```

セキュリティ コンテキストのリロード

セキュリティ コンテキストは、次の 2 つの方法でリロードできます。

- 実行コンフィギュレーションをクリアし、スタートアップ コンフィギュレーションをインポートします。

  この操作により、接続や NAT テーブルなど、コンテキストと関連付けられている大部分の属性がクリアされます。

- セキュリティ コンテキストをシステム コンフィギュレーションから削除する。

  このアクションでは、トラブルシューティングに役立つ可能性のあるメモリ割り当てなど補足的な属性がクリアされます。しかし、コンテキストをシステムに戻して追加するには、URL とインターフェイスを再指定する必要があります。

コンフィギュレーションのクリアによるリロード

手順

ステップ 1 リロードするコンテキストに変更します。

changeto context *name*

例：

```
ciscoasa(config)# changeto context ctx1
ciscoasa/ctx1(comfig)#
```

ステップ 2 実行コンフィギュレーションをクリアします。

clear configure all

このコマンドを実行するとすべての接続がクリアされます。

ステップ 3 コンフィギュレーションをリロードします。

copy startup-config running-config

例：

```
ciscoasa/ctx1(config)# copy startup-config running-config
```

ASA は、システム コンフィギュレーションに指定された URL からコンフィギュレーションをコピーします。コンテキスト内で URL を変更することはできません。

コンテキストの削除および再追加によるリロード

コンテキストを削除し、その後再追加することによってコンテキストをリロードするには、次の手順を実行してください。

手順

ステップ 1 セキュリティ コンテキストの削除 （291 ページ）。

ステップ 2 セキュリティ コンテキストの設定 （285 ページ）

セキュリティ コンテキストのモニタリング

この項では、コンテキスト情報を表示およびモニタリングする方法について説明します。

コンテキスト情報の表示

システム実行スペースから、名前、割り当てられているインターフェイス、コンフィギュレーション ファイル URL を含むコンテキストのリストを表示できます。

手順

すべてのコンテキストの表示：

show context [*name* | **detail**| **count**]

特定のコンテキストの情報を表示する場合は、*name* にコンテキスト名を指定します。

detail オプションを指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

count オプションを指定すると、コンテキストの合計数が表示されます。

例

次に、**show context** コマンドの出力例を示します。この出力例は、3 個のコンテキストを示しています。

```
ciscoasa# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      disk0:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      disk0:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      disk0:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

次の表は、各フィールドの説明を示しています。

表 *8 : show context* のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
インターフェイス	このコンテキストに割り当てられたインターフェイス。
URL	ASA がコンテキストのコンフィギュレーションをロードする URL。

次に、**show context detail** コマンドの出力例を示します。

```
ciscoasa# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: disk0:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
```

```
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

detail の出力の詳細については、コマンド リファレンスを参照してください。

次に、**show context count** コマンドの出力例を示します。

```
ciscoasa# show context count
Total active contexts: 2
```

リソースの割り当ての表示

システム実行スペースから、すべてのクラスおよびクラス メンバーに渡るリソースごとの割り当て状況を表示できます。

手順

リソース割り当てを表示します。

show resource allocation [**detail**]

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況の詳細については、リソースの使用状況の表示（300ページ）を参照してください。

detail 引数を指定すると、追加情報が表示されます。詳細については、次の出力例を参照してください。

例

次の出力例には、各リソースの合計割り当て量が絶対値および使用可能なシステム リソースの割合として示されています。

```
ciscoasa# show resource allocation
Resource                    Total       % of Avail
 Conns [rate]               35000           N/A
 Inspects [rate]            35000           N/A
```

```
Syslogs [rate]             10500           N/A
Conns                     305000           30.50%
Hosts                      78842           N/A
SSH                           35           35.00%
Routes                      5000           N/A
Telnet                        35           35.00%
Xlates                     91749           N/A
AnyConnect                  1000           10%
AnyConnectBurst              200           2%
Other VPN Sessions            20           2.66%
Other VPN Burst               20           2.66%
All                    unlimited
```

次の表は、各フィールドの説明を示しています。

表 *9 : show resource allocation* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは1秒あたりのインスタンスの絶対量です。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	リソースにハードウェア システム制限がある場合に、コンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースにシステム制限がない場合、このカラムには N/A と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
ciscoasa# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
```

```
                  gold                1       C     200000     200000     20.00%
                  silver              1      CA     100000     100000     10.00%
                  bronze              0      CA      50000
                  All Contexts:       3                        300000     30.00%

Hosts             default           all      CA  unlimited
                  gold                1      DA  unlimited
                  silver              1      CA      26214      26214      N/A
                  bronze              0      CA      13107
                  All Contexts:       3                         26214      N/A

SSH               default           all       C          5
                  gold                1       D          5          5      5.00%
                  silver              1      CA         10         10     10.00%
                  bronze              0      CA          5
                  All Contexts:       3                           20     20.00%

Telnet            default           all       C          5
                  gold                1       D          5          5      5.00%
                  silver              1      CA         10         10     10.00%
                  bronze              0      CA          5
                  All Contexts:       3                           20     20.00%

Routes            default           all       C  unlimited                 N/A
                  gold                1       D  unlimited          5      N/A
                  silver              1      CA         10         10      N/A
                  bronze              0      CA          5                 N/A
                  All Contexts:       3                           20      N/A

Xlates            default           all      CA  unlimited
                  gold                1      DA  unlimited
                  silver              1      CA      23040      23040     N/A
                  bronze              0      CA      11520
                  All Contexts:       3                         23040     N/A

mac-addresses     default           all       C      65535
                  gold                1       D      65535      65535    100.00%
                  silver              1      CA       6553       6553      9.99%
                  bronze              0      CA       3276
                  All Contexts:       3                        137623    209.99%
```

次の表は、各フィールドの説明を示しています。

表 *10 : show resource allocation detail* のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
クラス	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラス全体での合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。

フィールド	説明
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限を個々のリソースとしてではなく、**all** オプションを使用して設定します。 • C：この制限はメンバー クラスから生成されます。 • D：この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 ASA では、「C」または「D」を「A」に組み合わせることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、ASA はこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは1秒あたりのインスタンスの絶対量です。リソースが無制限の場合、この表示は空白です。
% of Avail	クラス内のコンテキスト全体に渡って割り当てられている合計システム リソースの割合。リソースが無制限の場合、この表示は空白です。リソースにシステム制限がない場合、このカラムの表示は N/A になります。

リソースの使用状況の表示

システム実行スペースで、コンテキストごとのリソースの使用状況やシステム リソースの使用状況を表示できます。

手順

コンテキストごとのリソース使用状況を表示します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system**] [**resource** {*resource_name* | **all**} | **detail**] [**counter** *counter_name* [*count_threshold*]]

- デフォルトでは、**all**（すべての）コンテキストの使用状況が表示されます。各コンテキストは個別にリスト表示されます。
- 指定したリソースの上位 **n** 人のユーザーとなっているコンテキストを表示するには、*top n* キーワードを入力します。このオプションでは、**resource all** ではなく、リソース タイプを 1 つのみ指定する必要があります。

- **summary** オプションを指定すると、すべてのコンテキストの使用状況が組み合されて表示されます。
- **system** オプションでは、すべてのコンテキストの使用状況が組み合されて表示されますが、組み合されたコンテキスト制限ではなく、リソースに対するシステムの制限が表示されます。
- **resource** *resource_name* で使用可能なリソース名については、リソース管理用のクラスの設定 （280 ページ） を参照してください。**show resource type** コマンドも参照してください。すべてのタイプを表示するには **all**（デフォルト）を指定します。
- **detail** オプションを指定すると、管理できないリソースを含むすべてのリソースの使用状況が表示されます。たとえば、TCP 代行受信の数を表示できます。
- **counter** *counter_name* には、次のいずれかのキーワードを指定します。
  - **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。
  - **denied**：Limit カラムに示されるリソース制限を超えたため拒否されたインスタンスの数を表示します。
  - **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後にクリアされた時点から計測されます。
  - **all**：（デフォルト）すべての統計情報を表示します。
- *count_threshold* は、表示するリソースの下限を設定します。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*count_threshold* は現在の使用状況に適用されます。
- すべてのリソースを表示するには、*count_threshold* を **0** に設定します。

例

次に、**show resource usage context** コマンドの出力例を示します。ここでは、admin コンテキストのリソース使用状況を表示する例を示しています。

```
ciscoasa# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。ここでは、すべてのコンテキストとすべてのリソースのリソース使用状況を表示する例を示しています。ここでは、6 コンテキスト分の制限値が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      N/A            0 Summary
Conns                     584          763      280000(S)      0 Summary
Xlates                   8526         8966      N/A            0 Summary
Hosts                     254          254      N/A            0 Summary
Conns [rate]              270          535      N/A         1704 Summary
Inspects [rate]           270          535      N/A            0 Summary
AnyConnect                  2           25      1000           0 Summary
AnyConnectBurst             0            0      200            0 Summary
Other VPN Sessions          0           10      10           740 Summary
Other VPN Burst             0           10      10           730 Summary

S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage summary** コマンドの出力例を示します。このコマンドでは、25 コンテキストの制限が示されます。Telnet 接続および SSH 接続のコンテキストの限界がコンテキストごとに 5 であるため、合計の限界は 125 です。システムの限界が単に 100 であるため、システムの限界が表示されています。

```
ciscoasa# show resource usage summary

Resource              Current         Peak      Limit    Denied   Context
Telnet                      1            1        100[S]      0   Summary
SSH                         2            2        100[S]      0   Summary
Conns                      56           90        130000(S)   0   Summary
Hosts                      89          102        N/A         0   Summary
S = System: Combined context limits exceed the system limit; the system limit is shown.
```

次に、**show resource usage system** コマンドの出力例を示します。このコマンドは、すべてのコンテキストのリソース使用状況を表示しますが、組み合わせたコンテキストの限界ではなく、システムの限界を表示しています。現在使用中でないリソースを表示するには、**counter all 0** オプションを指定します。Denied の統計情報は、システム制限がある場合に、その制限によってリソースが拒否された回数を示します。

```
ciscoasa# show resource usage system counter all 0

Resource              Current         Peak      Limit          Denied    Context
Telnet                      0            0        100                0    System
SSH                         0            0        100                0    System
ASDM                        0            0         32                0    System
Routes                      0            0        N/A                0    System
IPSec                       0            0          5                0    System
Syslogs [rate]              1           18        N/A                0    System
Conns                       0            1     280000                0    System
Xlates                      0            0        N/A                0    System
Hosts                       0            2        N/A                0    System
Conns [rate]                1            1        N/A                0    System
Inspects [rate]             0            0        N/A                0    System
AnyConnect                  2           25      10000                0    System
AnyConnectBurst             0            0        200                0    System
```

```
Other VPN Sessions          0           10        750           740    System
Other VPN Burst             0           10        750           730    System
```

コンテキストでの SYN 攻撃のモニタリング

ASA は TCP 代行受信を使用して SYN 攻撃を阻止します。TCP 代行受信では、SYN クッキーアルゴリズムを使用して TCP SYN フラッディング攻撃を防ぎます。SYN フラッディング攻撃は、通常はスプーフィングされた IP アドレスから送信されてくる一連の SYN パケットで構成されています。SYN パケットのフラッディングが定常的に生じると、SYN キューが一杯になる状況が続き、接続要求に対してサービスを提供できなくなります。接続の初期接続しきい値を超えると、ASA はサーバーのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。ASA がクライアントから ACK を受信すると、クライアントを認証し、サーバーへの接続を許可できます。

手順

ステップ 1 各コンテキストについて、攻撃の割合をモニタリングします。

show perfmon

ステップ 2 個々のコンテキストの TCP 代行受信で使用されるリソースの量をモニターします。

show resource usage detail

ステップ 3 システム全体の TCP 代行受信で使用されるリソースをモニターします。

show resource usage summary detail

例

次に、**show perfmon** コマンドの出力例を示します。このコマンドは、admin というコンテキストの TCP 代行受信レートを表示します。

```
ciscoasa/admin# show perfmon

Context:admin
PERFMON STATS:   Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
```

```
AAA Author            0/s           0/s
AAA Account           0/s           0/s
TCP Intercept    322779/s      322779/s
```

次に、**show resource usage detail** コマンドの出力例を示します。このコマンドは、個々のコンテキストの TCP 代行受信で使用されるリソース量を表示します。（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage detail
Resource              Current         Peak      Limit         Denied Context
memory                 843732       847288  unlimited             0 admin
chunk:channels             14           15  unlimited             0 admin
chunk:fixup                15           15  unlimited             0 admin
chunk:hole                  1            1  unlimited             0 admin
chunk:ip-users             10           10  unlimited             0 admin
chunk:list-elem            21           21  unlimited             0 admin
chunk:list-hdr              3            4  unlimited             0 admin
chunk:route                 2            2  unlimited             0 admin
chunk:static                1            1  unlimited             0 admin
tcp-intercepts         328787       803610  unlimited             0 admin
np-statics                  3            3  unlimited             0 admin
statics                     1            1  unlimited             0 admin
ace-rules                   1            1  unlimited             0 admin
console-access-rul          2            2  unlimited             0 admin
fixup-rules                14           15  unlimited             0 admin
memory                 959872       960000  unlimited             0 c1
chunk:channels             15           16  unlimited             0 c1
chunk:dbgtrace              1            1  unlimited             0 c1
chunk:fixup                15           15  unlimited             0 c1
chunk:global                1            1  unlimited             0 c1
chunk:hole                  2            2  unlimited             0 c1
chunk:ip-users             10           10  unlimited             0 c1
chunk:udp-ctrl-blk          1            1  unlimited             0 c1
chunk:list-elem            24           24  unlimited             0 c1
chunk:list-hdr              5            6  unlimited             0 c1
chunk:nat                   1            1  unlimited             0 c1
chunk:route                 2            2  unlimited             0 c1
chunk:static                1            1  unlimited             0 c1
tcp-intercept-rate      16056        16254  unlimited             0 c1
globals                     1            1  unlimited             0 c1
np-statics                  3            3  unlimited             0 c1
statics                     1            1  unlimited             0 c1
nats                        1            1  unlimited             0 c1
ace-rules                   2            2  unlimited             0 c1
console-access-rul          2            2  unlimited             0 c1
fixup-rules                14           15  unlimited             0 c1
memory              232695716    232020648  unlimited             0 system
chunk:channels             17           20  unlimited             0 system
chunk:dbgtrace              3            3  unlimited             0 system
chunk:fixup                15           15  unlimited             0 system
chunk:ip-users              4            4  unlimited             0 system
chunk:list-elem          1014         1014  unlimited             0 system
chunk:list-hdr              1            1  unlimited             0 system
chunk:route                 1            1  unlimited             0 system
block:16384               510          885  unlimited             0 system
block:2048                 32           34  unlimited             0 system
```

次の出力例は、システム全体の TCP 代行受信で使用されるリソースを示します（**太字**のサンプル テキストは、TCP 代行受信情報を示します）。

```
ciscoasa(config)# show resource usage summary detail
Resource              Current         Peak      Limit        Denied Context
memory              238421312    238434336  unlimited             0 Summary
chunk:channels              46           48  unlimited             0 Summary
chunk:dbgtrace               4            4  unlimited             0 Summary
chunk:fixup                 45           45  unlimited             0 Summary
chunk:global                 1            1  unlimited             0 Summary
chunk:hole                   3            3  unlimited             0 Summary
chunk:ip-users              24           24  unlimited             0 Summary
chunk:udp-ctrl-blk           1            1  unlimited             0 Summary
chunk:list-elem           1059         1059  unlimited             0 Summary
chunk:list-hdr              10           11  unlimited             0 Summary
chunk:nat                    1            1  unlimited             0 Summary
chunk:route                  5            5  unlimited             0 Summary
chunk:static                 2            2  unlimited             0 Summary
block:16384                510          885  unlimited             0 Summary
block:2048                  32           35  unlimited             0 Summary
tcp-intercept-rate      341306       811579  unlimited             0 Summary
globals                      1            1  unlimited             0 Summary
np-statics                   6            6  unlimited             0 Summary
statics                      2            2        N/A             0 Summary
nats                         1            1        N/A             0 Summary
ace-rules                    3            3        N/A             0 Summary
console-access-rul           4            4        N/A             0 Summary
fixup-rules                 43           44        N/A             0 Summary
```

割り当てられた MAC アドレスの表示

システム コンフィギュレーション内またはコンテキスト内の自動生成された MAC アドレスを表示できます。

システム設定での MAC アドレスの表示

この項では、システム コンフィギュレーション内の MAC アドレスを表示する方法について説明します。

始める前に

MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

手順

システム実行スペースから割り当てられた MAC アドレスを表示します。

show running-config all context [*name*]

割り当てられた MAC アドレスを表示するには、**all** オプションが必要です。**mac-address auto** コマンドは、グローバル コンフィギュレーション モードに限りユーザー設定可能ですが、コ

ンテキスト コンフィギュレーション モードでは、このコマンドは読み取り専用エントリとして、割り当てられたMACアドレスとともに表示されます。コンテキスト内で**nameif**コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

例

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
ciscoasa# show running-config all context admin

context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキストインターフェイスのすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メイン インターフェイスはコンテキスト内部に **nameif** コマンドで設定されないため、それらのインターフェイスの MAC アドレスは生成されていないことに注意してください。

```
ciscoasa# show running-config all context

admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!

context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!

context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
```

```
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

コンテキスト内の MAC アドレスの表示

この項では、コンテキスト内で MAC アドレスを表示する方法について説明します。

手順

コンテキスト内で各インターフェイスに使用されている MAC アドレスを表示します。

/context# show interface | include (Interface)|(MAC)

例

次に例を示します。

```
ciscoasa/context# show interface | include (Interface)|(MAC)

Interface GigabitEthernet1/1.1 "g1/1.1", is down, line protocol is down
        MAC address a201.0101.0600, MTU 1500
Interface GigabitEthernet1/1.2 "g1/1.2", is down, line protocol is down
        MAC address a201.0102.0600, MTU 1500
Interface GigabitEthernet1/1.3 "g1/1.3", is down, line protocol is down
        MAC address a201.0103.0600, MTU 1500
...
```

（注） **show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当てた場合に、自動生成がイネーブルになっていたときは、システム コンフィギュレーション内の未使用の自動生成アドレスのみを表示できます。

マルチ コンテキスト モードの例

次に例を示します。

- 各コンテキストの MAC アドレスを、カスタム プレフィックスを使用して自動的に設定します。

- conns のデフォルト クラス制限を、無制限ではなく 10% に設定し、VPN other セッション数を 10、バーストを 5 に設定します。
- gold リソース クラスを作成します。
- 管理コンテキストを「administrator」と設定します。
- 「administrator」というコンテキストを、デフォルトのリソース クラスの一部になるように、内部フラッシュ メモリ上に作成します。
- gold リソース クラスの一部として FTP サーバーから 2 個のコンテキストを追加します。

```
ciscoasa(config)# mac-address auto prefix 19

ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
ciscoasa(config-class)# limit-resource vpn other 10
ciscoasa(config-class)# limit-resource vpn burst other 5

ciscoasa(config)# class gold
ciscoasa(config-class)# limit-resource mac-addresses 10000
ciscoasa(config-class)# limit-resource conns 15%
ciscoasa(config-class)# limit-resource rate conns 1000
ciscoasa(config-class)# limit-resource rate inspects 500
ciscoasa(config-class)# limit-resource hosts 9000
ciscoasa(config-class)# limit-resource asdm 5
ciscoasa(config-class)# limit-resource ssh 5
ciscoasa(config-class)# limit-resource rate syslogs 5000
ciscoasa(config-class)# limit-resource telnet 5
ciscoasa(config-class)# limit-resource xlates 36000
ciscoasa(config-class)# limit-resource routes 700
ciscoasa(config-class)# limit-resource vpn other 100
ciscoasa(config-class)# limit-resource vpn burst other 50

ciscoasa(config)# admin-context administrator
ciscoasa(config)# context administrator
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
ciscoasa(config-ctx)# config-url disk0:/admin.cfg

ciscoasa(config-ctx)# context test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold

ciscoasa(config-ctx)# context sample
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
ciscoasa(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
ciscoasa(config-ctx)# member gold
```

マルチ コンテキスト モードの履歴

表 *11*：マルチ コンテキスト モードの履歴

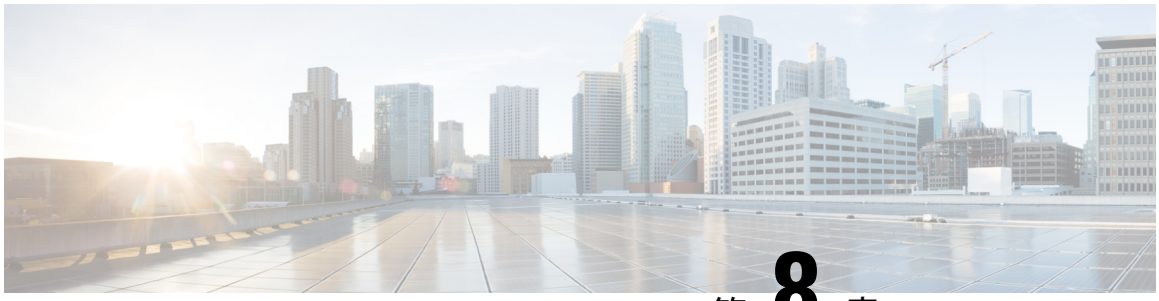
機能名	プラットフォーム リリース	機能情報
マルチセキュリティ コンテキスト	7.0(1)	マルチ コンテキスト モードが導入されました。 **context**、**mode**、**class** の各コマンドが導入されました。
MAC アドレス自動割り当て	7.2(1)	コンテキスト インターフェイスへの MAC アドレス自動割り当てが導入されました。 **mac-address auto** コマンドが導入されました。
リソース管理	7.2(1)	リソース管理が導入されました。 **class**、**limit-resource**、**member** の各コマンドが導入されました。
IPS 仮想センサー	8.0(2)	IPS ソフトウェアのバージョン 6.0 以降を実行している AIP SSM では、複数の仮想センサーを実行できます。つまり、AIP SSM に複数のセキュリティ ポリシーを設定することができます。各コンテキストまたはシングル モード ASA を 1 つまたは複数の仮想センサーに割り当てたり、複数のセキュリティ コンテキストを同じ仮想センサーに割り当てることができます。 **allocate-ips** コマンドが導入されました。
MAC アドレス自動割り当ての機能強化	8.0(5) 8.2(2)	MACアドレス形式が変更されました。プレフィックスが使用され、固定開始値（A2）が使用されます。また、フェールオーバー ペアのプライマリ装置とセカンダリ装置のMACアドレスそれぞれに異なるスキームが使用されます。MACアドレスはリロード後も維持されるようになりました。コマンド パーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MACアドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。 **mac-address auto prefix** コマンドが変更されました。
ASA 5550 および 5580 の最大コンテキスト数の増加	8.4(1)	ASA 5550 の最大セキュリティ コンテキスト数が 50 から 100 に増加しました。ASA 5580 での最大数が 50 から 250 に増加しました。
MAC アドレスの自動割り当てのデフォルトでの有効化	8.5(1)	MACアドレスの自動割り当てが、デフォルトでイネーブルになりました。 **mac-address auto** コマンドが変更されました。

機能名	プラットフォーム リリース	機能情報
MAC アドレス プレフィックスの自動生成	8.6(1)	マルチ コンテキスト モードで、ASA が MAC アドレス自動生成のコンフィギュレーションを変換し、デフォルトのプレフィックスを使用できるようになりました。ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）の MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。生成のプレフィックス方式は、セグメント上で一意の MAC アドレスがより適切に保証されるなど、多くの利点をもたらします。**show running-config mac-address** コマンドを入力して、自動生成されたプレフィックスを表示できます。プレフィックスを変更する場合、カスタム プレフィックスによって機能を再設定できます。MAC アドレス生成の従来の方法は使用できなくなります。 （注） フェールオーバー ペアのヒットレス アップグレードを維持するため、ASA は、フェールオーバーが有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。ただし、フェールオーバーを使用するときは、生成メソッドをプレフィックスに手動で変更することを強く推奨します（特に ASASM の場合）。プレフィックス メソッドを使用しない場合、異なるスロット番号にインストールされた ASASM では、フェールオーバーが発生した場合に MAC アドレスの変更が行われ、トラフィックの中断が発生することがあります。アップグレード後に、MAC アドレス生成のプレフィックス方式を使用するには、デフォルトのプレフィックスを使用する MAC アドレス生成を再びイネーブルにします。 **mac-address auto** コマンドが変更されました。
ASASM 以外のすべてのモデル上での MAC アドレスの自動割り当てはデフォルトでディセーブル	9.0(1)	自動 MAC アドレスの割り当ては ASASM を除いて、デフォルトでディセーブルになりました。 **mac-address auto** コマンドが変更されました。
セキュリティ コンテキストでのダイナミック ルーティング	9.0(1)	EIGRP と OSPFv2 ダイナミック ルーティング プロトコルが、マルチ コンテキスト モードでサポートされるようになりました。OSPFv3、RIP、およびマルチキャスト ルーティングはサポートされません。
ルーティング テーブル エントリのための新しいリソース タイプ	9.0(1)	新規リソース タイプ routes が作成されました。これは、各コンテキストでのルーティング テーブル エントリの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。

機能名	プラットフォーム リリース	機能情報
マルチ コンテキスト モードのサイトツーサイト VPN	9.0(1)	サイトツーサイト VPN トンネルが、マルチ コンテキスト モードでサポートされるようになりました。
サイトツーサイト VPN トンネルのための新しいリソース タイプ	9.0(1)	新しいリソース タイプ vpn other と vpn burst other が作成されました。これは、各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するためです。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
IKEv1 SA ネゴシエーションの新しいリソース タイプ	9.1(2)	CPU と暗号化エンジンの過負荷を防ぐため、コンテキストごとに IKEv1 SA ネゴシエーションの最大パーセンテージを設定するための新しいリソース タイプ ikev1 in-negotiation が作成されました。特定の条件（大容量の証明書、CRL、チェックなど）によっては、このリソースを制限する必要がある場合があります。 **limit-resource**、**show resource types**、**show resource usage**、**show resource allocation** の各コマンドが変更されました。
マルチ コンテキスト モードでのリモート アクセス VPN サポート	9.5(2)	次のリモート アクセス機能をマルチ コンテキスト モードで使用できるようになりました。 • AnyConnect 3.x 以降（SSL VPN のみ、IKEv2 はサポートしません） • 中央集中型 セキュアクライアント のイメージの設定 • セキュアクライアント のイメージのアップグレード • セキュアクライアント 接続のコンテキストリソース管理 （注） マルチコンテキストモードでは Secure Client Premier ライセンスが必要です。デフォルトやレガシーのライセンスは使用できません。 次のコマンドが導入されました。**limit-resource vpn anyconnect**、**limit-resource vpn burst anyconnect**
マルチ コンテキスト モードの場合の証明書の事前入力/ユーザー名	9.6(2)	セキュアクライアント SSL サポートが拡張され、これまでシングルモードでのみ使用可能だった証明書の事前入力とユーザー名取得機能の CLI がマルチコンテキストモードでも有効にできるようになりました。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	機能情報
リモート アクセス VPN のフラッシュ仮想化	9.6(2)	マルチ コンテキスト モードのリモート アクセス VPN はフラッシュ仮想化をサポートします。使用可能な合計フラッシュに基づき、コンテキストごとにプライベート記憶域と共有ストレージの場所が設定できます。 • プライベート記憶域：該当ユーザーのみに関連付けられ、該当ユーザー対象コンテンツ固有のファイルを保存します。 • 共有ストレージ：有効になると、この領域にファイルがアップロードされ、あらゆるユーザー コンテキストが読み取り/書き込みできるようこの領域へのアクセスが許可されます。 次のコマンドが導入されました。**limit-resource storage、storage-url**
マルチコンテキストデバイスでのセキュアクライアントプロファイルのサポート	9.6(2)	セキュアクライアント プロファイルは、マルチコンテキストデバイスでサポートされます。ASDM を使用して新しいプロファイルを追加するには、セキュアクライアントリリース 4.2.00748 または 4.3.03013 以降が必要です。
マルチコンテキストモードの セキュアクライアント接続のステートフル フェールオーバー	9.6(2)	マルチコンテキストモードで セキュアクライアント 接続のステートフル フェールオーバーがサポートされるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードでリモート アクセス VPN ダイナミック アクセス ポリシー（DAP）がサポートされました。	9.6(2)	マルチ コンテキスト モードで、コンテキストごとに DAP を設定できるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードでリモート アクセス VPN CoA（認可変更）がサポートされました。	9.6(2)	マルチ コンテキストモードで、コンテキストごとに CoA を設定できるようになりました。 変更されたコマンドはありません。
マルチ コンテキスト モードで、リモート アクセス VPN のローカライズがサポートされました。	9.6(2)	ローカリゼーションがグローバルでサポートされました。複数のコンテキストで共有されるローカリゼーション ファイル セットは 1 つだけです。 変更されたコマンドはありません。
IKEv2 のリモート アクセス VPN は、マルチ コンテキスト モードでサポートされています。	9.9(2)	リモート アクセス VPN は、IKEv2 のマルチ コンテキスト モードで構成できます。

機能名	プラットフォーム リリース	機能情報
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または 16 以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更されたコマンド：**quota management-session**、**show quota management-session**
Firepower 1140 の最大コンテキスト数が 5 から 10 に増加	9.16(1)	Firepower 1140 は、最大 10 のコンテキストをサポートするようになりました。
すべての Cisco Secure Firewall 1200 モデルでマルチ コンテキストをサポート	9.23(1)	マルチ コンテキスト モードのサポートが追加されました。Cisco Secure Firewall 1210/1220 • Cisco Secure Firewall 1210CE-5 コンテキスト。 • Cisco Secure Firewall 1210CP：5 コンテキスト。 • Cisco Secure Firewall 1220CX：10 コンテキスト。 スイッチポートはマルチ コンテキスト モードではサポートされていません。マルチ コンテキスト モードに変換する前に、すべてのインターフェイスをルータ インターフェイスに変換する必要があります。 Cisco Secure Firewall 1230/1240/1250 も最初のリリースでマルチ コンテキスト モードをサポートしています。 • Cisco Secure Firewall 1230：25 コンテキスト。 • Cisco Secure Firewall 1240：25 コンテキスト。 • Cisco Secure Firewall 1250：25 コンテキスト。



第 8 章

ハイ アベイラビリティのためのフェールオーバー

この章では、ASA のハイアベイラビリティを達成するために、アクティブ/スタンバイまたはアクティブ/アクティブフェールオーバーを設定する方法について説明します。

- フェールオーバーについて （315 ページ）
- フェールオーバーのライセンス （342 ページ）
- フェールオーバー のガイドライン （343 ページ）
- フェールオーバーのデフォルト （347 ページ）
- アクティブ/スタンバイ フェールオーバーの設定 （347 ページ）
- アクティブ/アクティブ フェールオーバーの設定 （353 ページ）
- オプションのフェールオーバー パラメータの設定 （359 ページ）
- フェールオーバー の管理 （369 ページ）
- フェールオーバーのモニタリング （376 ページ）
- フェールオーバーの履歴 （378 ページ）

フェールオーバーについて

フェールオーバーの設定では、専用フェールオーバー リンク（および任意でステート リンク）を介して相互に接続された 2 つの同じ ASA が必要です。アクティブユニットおよびインターフェイスのヘルスがモニターされて、所定のフェールオーバー条件に一致しているかどうかが判断されます。所定の条件に一致すると、フェールオーバーが行われます。

フェールオーバー モード

ASAは、アクティブ/アクティブ フェールオーバーとアクティブ/スタンバイ フェールオーバーの2つのフェールオーバー モードをサポートします。各フェールオーバー モードには、フェールオーバーを判定および実行する独自の方式があります。

- アクティブ/スタンバイフェールオーバーでは、一方のデバイスがアクティブユニットとしてトラフィックを通過させます。もう一方のデバイスはスタンバイユニットとなり、ア

クティブにトラフィックを通過させません。フェールオーバーが発生すると、アクティブユニットからスタンバイユニットにフェールオーバーし、そのスタンバイユニットがアクティブになります。シングルまたはマルチ コンテキスト モードでは、ASA のアクティブ/スタンバイ フェールオーバーを使用できます。

- アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つのフェールオーバー グループ に分割します。フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。一方のグループは、プライマリ ASA でアクティブになるよう割り当てられます。他方のグループは、セカンダリ ASA でアクティブになるよう割り当てられます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。

両方のフェールオーバー モードとも、ステートフルまたはステートレス フェールオーバーをサポートします。

フェールオーバー のシステム要件

この項では、フェールオーバー コンフィギュレーションにある ASAのハードウェア要件、ソフトウェア要件、およびライセンス要件について説明します。

ハードウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- 同じモデルであること。

  Firepower 9300 の場合、高可用性は同じタイプのモジュール間でのみサポートされていますが、2 台のシャーシにモジュールを混在させることができます。たとえば、各シャーシには SM-56、SM-48、および SM-40 があります。SM-56 モジュール間、SM-48 モジュール間、および SM-40 モジュール間にハイアベイラビリティペアを作成できます。

- インターフェイスの数とタイプが同じであること。

  プラットフォーム モードと Firepower 4100/9300 シャーシFirepower 2100 では、フェールオーバー を有効にする前に、すべてのインターフェイスが FXOS で同一に事前構成されている必要があります。フェールオーバーを有効にした後でインターフェイスを変更する場合は、スタンバイユニットの FXOS でそのインターフェイスを変更してから、アクティブユニットで同じ変更を行います。 FXOS でインターフェイスを削除した場合（たとえば、ネットワーク モジュールの削除、EtherChannel の削除、または EtherChannel へのインターフェイスの再割り当てなど）、必要な調整を行うことができるように、ASA 設定では元のコマンドが保持されます。設定からインターフェイスを削除すると、幅広い影響が出る可能性があります。ASA OS の古いインターフェイス設定は手動で削除できます。

- 同じモジュール（存在する場合）がインストールされていること。

- 同じ RAM がインストールされていること。

フェールオーバー コンフィギュレーションで装置に異なるサイズのフラッシュ メモリを使用している場合、小さい方のフラッシュ メモリを取り付けた装置に、ソフトウェア イメージ ファイルおよびコンフィギュレーション ファイルを格納できる十分な容量があることを確認してください。十分な容量がない場合、フラッシュ メモリの大きい装置からフラッシュ メモリの小さい装置にコンフィギュレーションの同期が行われると、失敗します。

ソフトウェア要件

フェールオーバー コンフィギュレーションの 2 台の装置は、次の条件を満たしている必要があります。

- コンテキスト モードが同じであること（シングルまたはマルチ）。
- 単一モードの場合：同じファイアウォール モードにあること（ルーテッドまたはトランスペアレント）。

  マルチコンテキスト モードでは、ファイアウォール モードはコンテキスト レベルで設定され、混合モードを使用できます。
- ソフトウェア バージョンが、メジャー（最初の番号）およびマイナー（2 番目の番号）ともに同じであること。ただし、アップグレード プロセス中は、異なるバージョンのソフトウェアを一時的に使用できます。たとえば、ある装置をバージョン 8.3(1) からバージョン 8.3(2) にアップグレードし、フェールオーバーをアクティブ状態のままにできます。長期的に互換性を維持するために、両方の装置を同じバージョンにアップグレードすることをお勧めします。
- 同じ セキュア クライアント イメージがあること。中断のないアップグレードを実行するときにフェールオーバー ペアのイメージが一致しないと、アップグレード プロセスの最後のリブート手順でクライアントレス SSL VPN 接続が切断され、データベースには孤立したセッションが残り、IP プールではクライアントに割り当てられた IP アドレスが「使用中」として示されます。
- 同じ FIPS モードであること。
- （Firepower 4100/9300）同じフロー オフロード モードを使用し、両方とも有効または無効になっている。

ライセンス要件

フェールオーバー コンフィギュレーションの 2 台の装置は、ライセンスが同じである必要はありません。これらのライセンスは結合され、1 つのフェールオーバー クラスタ ライセンスが構成されます。

フェールオーバー リンクとステートフル フェールオーバー リンク

フェールオーバー リンクとオプションのステートフル フェールオーバー リンクは、2 つの装置間の専用接続です。シスコでは、フェールオーバーリンクまたはステートフルフェールオーバーリンク内の2つのデバイス間で同じインターフェイスを使用することを推奨しています。たとえば、フェールオーバー リンクで、デバイス 1 で eth0 を使用していた場合は、デバイス 2 でも同じインターフェイス（eth0）を使用します。

⚠

注意 フェールオーバー リンクおよびステート リンク経由で送信される情報は、IPsec トンネルまたはフェールオーバー キーを使用して通信を保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端に ASA を使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザー名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。ASA を使用して VPN トンネルを終端する場合は、フェールオーバー通信を IPsec トンネルまたはフェールオーバー キーによってセキュリティ保護することをお勧めします。

フェールオーバー リンク

フェールオーバー ペアの 2 台の装置は、フェールオーバー リンク経由で常に通信して、各装置の動作ステータスを確認しています。

フェールオーバー リンク データ

次の情報がフェールオーバー リンク経由で伝達されています。

- 装置の状態（アクティブまたはスタンバイ）
- hello メッセージ（キープアライブ）
- ネットワーク リンクの状態
- MAC アドレス交換
- コンフィギュレーションの複製および同期

フェールオーバー リンクのインターフェイス

使用されていないデータインターフェイス（物理、サブインターフェイス、またはEtherChannel）はいずれもフェールオーバーリンクとして使用できます。ただし、現在名前が設定されているインターフェイスは指定できません。フェールオーバー リンク インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信のためにだけ存在します。このインターフェイスは、フェールオーバー リンク用にのみ使用できます（ステート リンク用としても使用できます）。ほとんどのモデルでは、以下で明示的に説明されていない限り、フェールオーバー用の管理インターフェイスを使用できません。

ASA は、ユーザー データとフェールオーバー リンク間でのインターフェイスの共有をサポートしていません。同じ親の別のサブインターフェイスをフェールオーバーリンクやデータのために使用することもできません。

フェールオーバー リンクについては、次のガイドラインを参照してください。

- 5506-X ～ 5555-X：管理インターフェイスをフェールオーバー リンクとして使用できません。データ インターフェイスを使用する必要があります。5506H-X は唯一の例外で、フェールオーバー リンクとして管理インターフェイスを使用できます。
- 5506H-X：フェールオーバー リンクとして管理 1/1 インターフェイスを使用できます。フェールオーバー用に設定した場合は、デバイスをリロードして変更を反映させる必要があります。この場合、管理プロセスに管理インターフェイスが必要であるため、ASA Firepower モジュールも使用できません。
- Firepower 4100/9300：フェールオーバー リンクに管理タイプのインターフェイスを使用することはできません。
- リンクのサイジングについては、次のガイドラインを参照してください。

表 *12*：フェールオーバー リンクのサイズ

モデル	結合フェールオーバー リンクとステート リンクのインターフェイス サイズ
Firepower 1010	1 Gbps
Firepower 1100	1 Gbps
Cisco Secure Firewall 1200	1 Gbps
Cisco Secure Firewall 3100	Cisco Secure Firewall 3105：1 Gbps Cisco Secure Firewall 3110：1 Gbps Cisco Secure Firewall 3120：1 Gbps Cisco Secure Firewall 3130：10 Gbps Cisco Secure Firewall 3140：10 Gbps
Firepower 4100	10 Gbps
Cisco Secure Firewall 4200	10 Gbps
Firepower 9300	10 Gbps

交替頻度は、ユニットのホールド時間と同じです（**failover polltime unit** コマンド）。

（注） 設定が大きく、ユニットのホールド時間が短い場合、メンバーインターフェイスを交互に切り替えると、セカンダリユニットの参加/再参加を防止できます。この場合、セカンダリユニットが参加するまで、メンバーインターフェイスの 1 つを無効にします。

フェールオーバー リンクとして使用される EtherChannel の場合は、順序が不正なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバー リンクとして使用中の EtherChannel の設定は変更できません。

フェールオーバー リンクの接続

フェールオーバー リンクを次の 2 つの方法のいずれかで接続します。

- ASA のフェールオーバーインターフェイスと同じネットワークセグメント（ブロードキャストドメインまたは VLAN）に他のデバイスのないスイッチを使用する。
- イーサネット ケーブルを使用してユニットを直接接続する。外部スイッチは必要ありません。

ユニット間でスイッチを使用しない場合、インターフェイスに障害が発生すると、リンクは両方のピアでダウンします。このような状況では、障害が発生してリンクがダウンする原因になったインターフェイスがどちらのユニットのものかを簡単に特定できないため、トラブルシューティング作業が困難になる場合があります。

ASAは、銅線イーサネット ポートで Auto-MDI/MDIX をサポートしているため、クロスオーバー ケーブルまたはストレート ケーブルのいずれかを使用できます。ストレート ケーブルを使用した場合は、インターフェイスが自動的にケーブルを検出して、送信/受信ペアの 1 つを MDIX にスワップします。

ステートフル フェールオーバー リンク

ステートフル フェールオーバーを使用するには、接続ステート情報を渡すためのステートフル フェールオーバー リンク（ステート リンクとも呼ばれる）を設定する必要があります。

フェールオーバー リンクの共有

インターフェイスを節約するための最適な方法はフェールオーバー リンクを共有することです。ただし、大規模な構成とトラフィックの多いネットワークを使用する場合は、ステート リンクとフェールオーバー リンクに専用のインターフェイスを使用することを検討する必要があります。

専用のインターフェイス

ステートリンク専用のデータインターフェイス（物理、または EtherChannel）を使用できます。専用のステートリンクの要件についてはフェールオーバー リンクのインターフェイス （318 ページ）、ステートリンクの接続についてはフェールオーバー リンクの接続 （320 ページ）を参照してください。

長距離のフェールオーバーを使用する場合のステート リンクの遅延は、パフォーマンスを最善にするには 10 ミリ秒未満でなければならず、250 ミリ秒を超えないようにする必要があります。遅延が 10 ミリ秒を上回る場合、フェールオーバー メッセージの再送信によって、パフォーマンスが低下する可能性があります。

フェールオーバーの中断の回避とデータ リンク

すべてのインターフェイスで同時に障害が発生する可能性を減らすために、フェールオーバー リンクとデータ インターフェイスは異なるパスを通すことを推奨します。フェールオーバー リンクがダウンした場合、フェールオーバーが必要かどうかの決定に、ASA はデータ インターフェイスを使用できます。その後、フェールオーバー動作は、フェールオーバー リンクのヘルスが復元されるまで停止されます。

耐障害性のあるフェールオーバー ネットワークの設計については、次の接続シナリオを参照してください。

シナリオ 1：非推奨

単一のスイッチまたはスイッチ セットが 2 つの ASA 間のフェールオーバー インターフェイスとデータ インターフェイスの両方の接続に使用される場合、スイッチまたはスイッチ間リンクがダウンすると、両方の ASA がアクティブになります。したがって、次の図で示されている次の 2 つの接続方式は推奨しません。

図 *43*：単一のスイッチを使用した接続：非推奨

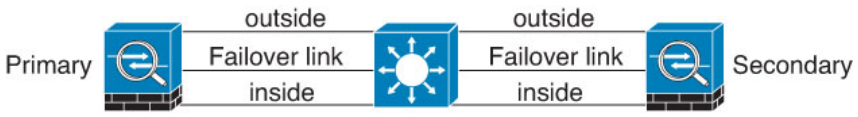
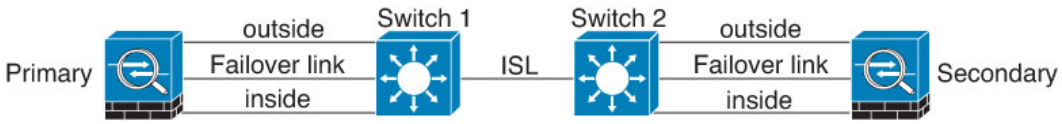


図 *44*：*2* つのスイッチを使用した接続：非推奨



シナリオ 2：推奨

フェールオーバー リンクには、データ インターフェイスと同じスイッチを使用しないことを推奨します。代わりに、次の図に示すように、別のスイッチを使用するか直接ケーブルを使用して、フェールオーバー リンクを接続します。

図 *45 :* 異なるスイッチを使用した接続

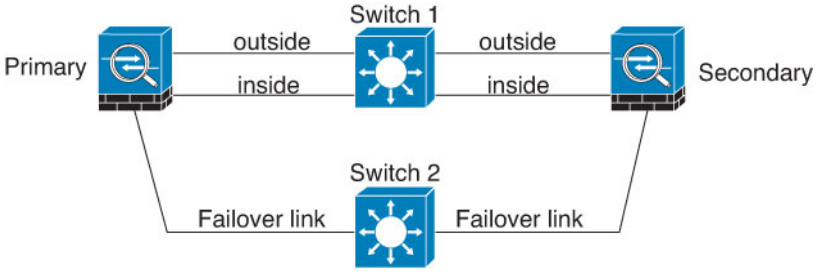
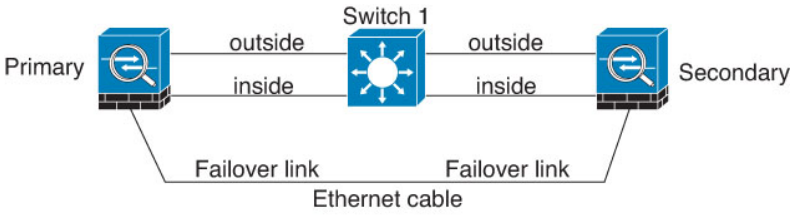


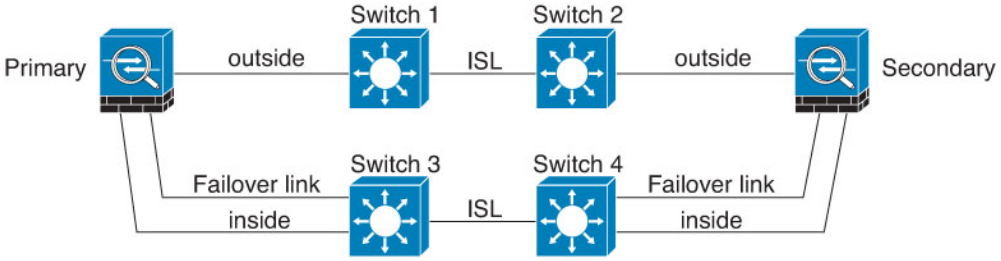
図 *46 :* ケーブルを使用した接続



シナリオ 3：推奨

ASA データ インターフェイスが複数セットのスイッチに接続されている場合、フェールオーバー リンクはいずれかのスイッチに接続できます。できれば、次の図に示すように、ネットワークのセキュアな側（内側）のスイッチに接続します。

図 *47 :* セキュア スイッチを使用した接続



フェールオーバー の MAC アドレスと IP アドレス

インターフェイスを設定する場合、同じネットワーク上にアクティブ IP アドレスとスタンバイ IP アドレスを指定できます。通常、フェールオーバーが発生すると、新しいアクティブ装置がアクティブな IP アドレスと MAC アドレスを引き継ぎます。ネットワークデバイスは、MAC と IP アドレスのペアリングの変更を認識しないため、ネットワーク上のどのような場所でも ARP エントリが変更されたり、タイムアウトが生じたりすることはありません。

（注） 推奨されてはいますが、スタンバイアドレスは必須ではありません。スタンバイ IP アドレスがなければ、アクティブ装置はネットワーク テストを実行してスタンバイ インターフェイスの状態を確認することはできません。できることはリンク ステートの追跡のみです。また、管理目的でそのインターフェイス上のスタンバイ装置に接続することもできません。

ステートリンクのIPアドレスおよびMACアドレスは、フェールオーバー時に変更されません。

アクティブ/スタンバイ IP アドレスと MAC アドレス

アクティブ/スタンバイ フェールオーバー の場合、フェールオーバーイベント中の IP アドレスと MAC アドレスの使用方法については、次を参照してください。

1. アクティブ装置は常に、プライマリ装置のIPアドレスとMACアドレスを使用します。
2. アクティブ装置がフェールオーバーすると、スタンバイ装置は障害が発生した装置の IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
3. 障害が発生した装置がオンライン状態に戻ると、スタンバイ状態になり、スタンバイの IP アドレスと MAC アドレスを引き継ぎます。

ただし、セカンダリ装置がプライマリ装置を検出せずに起動した場合、プライマリ装置の MAC アドレスを認識していないため、セカンダリ装置がアクティブ装置になり、自分の MAC アドレスを使用します。プライマリ装置が使用可能になると、セカンダリ（アクティブ）装置は MAC アドレスをプライマリ装置の MAC アドレスに変更します。このため、ネットワーク トラフィックが中断することがあります。同様に、新しいハードウェアでプライマリ装置をスワップ アウトすると新しい MAC アドレスが使用されます。

フェールオーバーを無効にし、フェールオーバー設定を無効状態に設定した場合は、フェールオーバーを手動で再開するか、デバイスを再起動する必要があります。デバイスを再起動するのではなく、コマンド **failover reset** を使用してフェールオーバーを再開することをお勧めします。フェールオーバー設定が無効なスタンバイ装置をリロードすると、スタンバイ装置はアクティブ装置として起動し、プライマリ装置の IP アドレスと MAC アドレスを使用します。これにより、IP アドレスが重複し、ネットワークトラフィックが中断されます。**failover reset** コマンドを使用してフェールオーバーを有効にし、トラフィックフローを復元します。

（注） スタンドアロンデバイスでフェールオーバーを有効にすると、データインターフェイスがフェールオーバーのネゴシエーション状態でダウンし、トラフィックが中断されます。

仮想 MAC アドレスがこの中断を防ぎます。なぜなら、アクティブ MAC アドレスは起動時にセカンダリ装置によって認識され、プライマリ装置のハードウェアが新しくなっても変わらないからです。セカンダリ装置がプライマリ装置より先にオンラインになった場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスを使用するように、プライマリ装置とセカンダリ装置の両方で仮想MACアドレスを設定することをお勧めします。仮想MACアドレスを設定しなかった場合、トラフィック フローを復元するために、接続されたルータの

ARP テーブルをクリアする必要がある場合があります。MACアドレスが変わった場合、ASAはスタティックNATアドレスに対してGratuitous ARPを送信しません。そのため、接続されたルータはこれらのアドレスのMACアドレス変更を認識できません。

アクティブ/アクティブ IP アドレスと MAC アドレス

アクティブ/アクティブフェールオーバーの場合、フェールオーバーイベント中の IP アドレスと MAC アドレスの使用方法については、次を参照してください。

1. プライマリ装置は、フェールオーバーグループ 1 および 2 のコンテキストにあるすべてのインターフェイスに対してアクティブおよびスタンバイ MACアドレスを自動生成します。また、MACアドレスが競合している場合などには、必要に応じて手動でMACアドレスを設定できます。
2. 各装置は、アクティブ フェールオーバー グループのアクティブな IP アドレスと MAC アドレス、およびスタンバイ フェールオーバー グループのスタンバイアドレスを使用します。たとえば、プライマリ装置はフェールオーバーグループ 1 に対してアクティブであるため、フェールオーバーグループ 1 のコンテキストに対してアクティブなアドレスを使用します。また、スタンバイアドレスを使用するフェールオーバーグループ 2 のコンテキストに対してはスタンバイです。
3. ある装置がフェールオーバーすると、別の装置が障害が発生したフェールオーバーグループのアクティブな IP アドレスと MAC アドレスを引き継ぎ、トラフィックを通過させます。
4. 障害が発生した装置がオンライン状態に戻り、プリエンプトオプションを有効にすると、フェールオーバーグループが再開されます。

仮想 MAC アドレス

ASA には仮想 MAC アドレスを設定する複数の方法があります。1 つの方法だけ使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合、使用される MAC アドレスは多くの変数によって決まるため、予測できないことがあります。手動の方法には、次で説明されている自動生成方法に加えて、インターフェイスモード **mac-address** コマンド、**failover mac address** コマンドが含まれ、アクティブ/アクティブフェールオーバーの場合は、フェールオーバー グループ モード **mac address** コマンドが含まれます。

マルチコンテキストモードでは、共有インターフェイスに対して仮想アクティブおよびスタンバイ MAC アドレスを自動的に生成するように ASA を設定できます。また、これらの割り当てはセカンダリ装置に同期されます（**mac-address auto** コマンドを参照）。非共有インターフェイスの場合、アクティブ/スタンバイモードのMACアドレスを手動で設定できます（アクティブ/アクティブモードでは、すべてのインターフェイスのMACアドレスが自動生成されます）。

アクティブ/アクティブ フェールオーバーでは、仮想 MAC アドレスはデフォルト値またはインターフェイスごとに設定できる値のいずれかとともに常に使用されます。

フェールオーバーでの MAC アドレス テーブルの更新

フェールオーバー時、新しいアクティブ デバイスとして指定されたデバイスは、MAC テーブル内の各 MAC アドレス エントリに対してマルチキャスト パケットを生成し、それをすべてのブリッジ グループ インターフェイスに送信します。このアクションにより、ブリッジグループ内の上流スイッチは、新しいアクティブデバイスのインターフェイスでルーティングテーブルを更新し、正確なトラフィック転送を保証します。

マルチキャストパケットの生成および上流スイッチのルーティングテーブルを更新するのにかかる時間は、MACアドレステーブルのエントリ数とブリッジ グループ インターフェイスの数によって異なります。フェールオーバーイベント中に発生した遅延に関連する統計を表示するには、コマンド **show failover statistics state-switch-delay** を使用します。

ステートレス フェールオーバーとステートフル フェールオーバー

ASA は、アクティブ/スタンバイ モードとアクティブ/アクティブ モードの両方に対して、ステートレスとステートフルの 2 種類のフェールオーバーをサポートします。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフルフェールオーバーを使用する必要があります。ステートレスフェールオーバーは、クライアントレス SSL VPN には推奨されません。

ステートレス フェールオーバー

フェールオーバーが行われると、アクティブ接続はすべてドロップされます。新しいアクティブ装置が引き継ぐ場合、クライアントは接続を再確立する必要があります。

（注） クライアントレス SSL VPN の一部のコンフィギュレーション要素（ブックマークやカスタマイゼーションなど）はVPNフェールオーバーサブシステムを使用していますが、これはステートフル フェールオーバーの一部です。フェールオーバー ペアのメンバ間でこれらの要素を同期するには、ステートフル フェールオーバーを使用する必要があります。ステートレス（標準）フェールオーバーは、クライアントレス SSL VPN には推奨できません。

ステートフル フェールオーバー

ステートフルフェールオーバーが有効な場合、アクティブ装置は接続ごとのステート情報をスタンバイ装置に継続的に渡しますアクティブ/アクティブ フェールオーバーの場合は、アクティブとスタンバイのフェールオーバー グループ間でこれが行われます。フェールオーバーの発生後も、新しいアクティブ装置で同じ接続情報が利用できます。サポートされているエンドユーザのアプリケーションでは、同じ通信セッションを保持するために再接続する必要はありません。

サポートされる機能

ステートフル フェールオーバーでは、次のステート情報がスタンバイ ASA に渡されます。

- NAT 変換テーブル
- TCP 接続状態と UDP 接続状態（）。その他の IP プロトコル タイプと ICMP は、新しいパケットが到着すると新しいアクティブデバイスで確立されるため、アクティブ装置によって解析されません。
- HTTP 接続テーブル（HTTP 複製が有効でない場合）。
- HTTP 接続状態（HTTP 複製が有効の場合）：デフォルトでは、ステートフル フェールオーバーが有効のときには、ASA は HTTP セッション情報を複製しません。HTTP レプリケーションを有効にすることをお勧めします。
- SCTP 接続状態ただし、SCTP インスペクションのステートフル フェールオーバーはベストエフォートです。フェールオーバー中、SACK パケットが失われると、失われたパケットが受信されるまで、新しいアクティブユニットはキューにある他のすべての順序が不正なパケットを破棄します。
- ARP テーブル
- レイヤ 2 ブリッジ テーブル（ブリッジ グループ用）
- ISAKMP および IPSec SA テーブル
- GTP PDP 接続データベース
- SIP シグナリング セッションおよびピン ホール。
- ICMP 接続状態：ICMP 接続の複製は、個々のインターフェイスが非対称ルーティング グループに割り当てられている場合にだけ有効になります。
- スタティック/ダイナミック ルーティング テーブル：ステートフル フェールオーバーは OSPF や EIGRP などのダイナミック ルーティング プロトコルに参加します。そのため、アクティブ装置上のダイナミック ルーティング プロトコルを介して学習されたルートは、スタンバイ装置のルーティング情報ベース（RIB）テーブルに保持されます。フェールオーバーイベントが発生した場合、最初はアクティブなセカンダリ装置にプライマリ装置をミラーリングするルールがあるため、パケットは通常は最小限の切断でトラフィックに移動します。フェールオーバーの直後に、新しくアクティブになった装置で再コンバージェンス タイマーが開始されます。次に、RIB テーブルのエポック番号が増加します。再コンバージェンス中に、OSPF および EIGRP ルートは新しいエポック番号で更新されます。タイマーが期限切れになると、失効したルート エントリ（エポック番号によって決定される）はテーブルから削除されます。これで、RIB には新しくアクティブになった装置での最新のルーティング プロトコル転送情報が含まれます。

（注） ルートは、アクティブ装置上のリンクアップまたはリンクダウンイベントの場合のみ同期されます。スタンバイ装置上でリンクがアップまたはダウンすると、アクティブ装置から送信されたダイナミック ルートが失われることがあります。これは正常な予期された動作です。

- DHCP サーバ：DHCP アドレス リースは複製されません。ただし、インターフェイス上に構成された DHCP サーバは DHCP クライアントにアドレスを付与する前に ping を送信してアドレスが使用されていないことを確認するため、サービスに影響はありません。ステート情報は、DHCP リレーまたは DDNS には関係ありません。
- Cisco IP SoftPhone セッション：コール セッション ステート情報がスタンバイ装置に複製されるため、Cisco IP SoftPhone セッションの実行中にフェールオーバーが起こっても、コールは実行されたままです。コールが終了すると、IP SoftPhone クライアントでは Cisco Call Manager との接続が解除されます。これは、CTIQBE ハングアップ メッセージのセッション情報がスタンバイ装置に存在しないために発生します。IP SoftPhone クライアントでは、一定の時間内に CallManager からの応答が受信されない場合、CallManager に到達できないものと判断されて登録が解除されます。
- RA VPN：リモート アクセス VPN のエンド ユーザは、フェールオーバー後に VPN セッションを再認証または再接続する必要はありません。ただし、VPN 接続上で動作するアプリケーションは、フェールオーバー プロセス中にパケットを失って、パケット損失から回復できない可能性があります。
- すべての接続から、確立された接続だけがスタンバイ デバイスに複製されます。

サポートされない機能

ステートフル フェールオーバーでは、次のステート情報はスタンバイ ASA に渡されません。

- ユーザ認証（uauth）テーブル
- TCP ステート バイパス接続。
- マルチキャスト ルーティング。
- 一部のクライアントレス SSL VPN 機能。
  - スマート トンネル
  - ポートフォワーディング
  - プラグイン
  - Java アプレット
  - IPv6 クライアントレスまたは セキュアクライアント セッション
  - Citrix 認証（Citrix ユーザはフェールオーバー後に再認証が必要です）

フェールオーバーのブリッジ グループ要件

ブリッジグループを使用する場合は、フェールオーバーに関して特別な考慮事項があります。

アプライアンス、ASAv のブリッジグループ必須要件

アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニングツリープロトコル（STP）を実行している接続済みスイッチ ポートは、トポロジ変更を検出すると 30 ～ 50 秒間ブロッキング ステートに移行できます。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチ ポート モードに応じて次の回避策のいずれかを設定できます。

- アクセス モード：スイッチで STP PortFast 機能をイネーブルにします。

```
interface interface_id
  spanning-tree portfast
```

  PortFast機能を設定すると、リンクアップと同時にポートがSTPフォワーディング モードに遷移します。ポートはSTPに参加し続けます。したがって、ポートがループの一部になる場合、最終的にはSTP ブロッキング モードに遷移します。

- トランク モード：EtherTypeアクセス ルールを使用して、ブリッジグループのメンバー インターフェイス上の ASA の BPDU をブロックします。

```
access-list id ethertype deny bpdu
access-group id in interface name1
access-group id in interface name2
```

  BPDU をブロックすると、スイッチの STP はディセーブルになります。ネットワーク レイアウトで ASA を含むループを設定しないでください。

上記のオプションのどちらも使用できない場合は、フェールオーバー機能またはSTPの安定性に影響する、推奨度の低い次の回避策のいずれかを使用できます。

- インターフェイス モニタリングをディセーブルにします。
- ASA がフェールオーバーする前に、インターフェイスのホールド時間を STP が収束可能になる大きい値に増やします。
- STPがインターフェイスのホールド時間よりも速く収束するように、STPタイマーを減らします。

フェールオーバーのヘルス モニタリング

ASAは、各装置について全体的なヘルスおよびインターフェイス ヘルスをモニターします。この項では、各装置の状態を判断するために、ASAがテストを実行する方法について説明します。

装置のヘルス モニターリング

ASAは、helloメッセージでフェールオーバー リンクをモニタして相手装置のヘルスを判断します。フェールオーバー リンクで3回連続してhelloメッセージを受信しなかったときは、フェールオーバー リンクを含む各データ インターフェイスでLANTESTメッセージを送信し、ピアが応答するかどうかを確認します。 FirePOWER 9300および4100シリーズでは、helloメッセージよりも信頼性の高いBidirectional Forwarding Detection（BFD）を有効にできます。ASAが行うアクションは、相手装置からの応答によって決まります。次の可能なアクションを参照してください。

- ASAがフェールオーバー リンクで応答を受信した場合、フェールオーバーは行われません。
- ASAがフェールオーバー リンクで応答を受信せず、データ インターフェイスで応答を受信した場合、装置のフェールオーバーは行われません。フェールオーバー リンクは故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイにフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
- ASAがどのインターフェイスでも応答を受信しなかった場合、スタンバイ装置がアクティブ モードに切り替わり、相手装置を故障に分類します。

ハートビートモジュールの冗長性

HAの各ユニットは、クラスタ制御リンクを介してブロードキャスト キープアライブ ハートビートパケットを定期的に送信します。コントロールプレーンがトラフィックの処理でビジー状態になっていると、ハートビートパケットがピアに届かなかったり、CPUの過負荷が原因でピアがハートビートパケットを処理しないことがあります。設定可能なタイムアウト期間内にピアがキープアライブステータスを伝えられない場合、誤ったフェールオーバーまたはスプリットブレインシナリオが発生します。

データプレーンのハートビートモジュールは、コントロールプレーンでのトラフィックの輻輳による誤ったフェールオーバーまたはスプリットブレインの発生を回避するために役立ちます。

- 追加のハートビートモジュールは、コントロール プレーン モジュールと同様に機能しますが、データ プレーン トランスポート インフラストラクチャを使用してハートビートメッセージを送受信します。
- ピアがデータプレーンでハートビートパケットを受信すると、カウンタが増加します。
- コントロールプレーンでのハートビート転送が失敗した場合、ノードはデータプレーンのハートビートカウンタをチェックします。カウンタが増加している場合、ピアは稼働しており、この状況ではクラスタはフェールオーバーを実行しません。

（注）
- HA が有効な場合、追加のハートビートモジュールは常にデフォルトで有効になっています。データプレーンの追加のハートビートモジュールのポーリング間隔を設定する必要はありません。このモジュールは、コントロールプレーンに設定したものと同じハートビート間隔を使用します。
- この機能は、バージョン 7.3 では使用できません。

インターフェイス モニタリング

最大 1025 のインターフェイスを監視できます（マルチコンテキスト モードでは、すべてのコンテキスト間で分割）。重要なインターフェイスをモニターする必要があります。たとえば、マルチコンテキストモードでは、共有インターフェイスを監視するように1つのコンテキストを設定する場合があります（インターフェイスが共有されているため、すべてのコンテキストがそのモニタリングによる利点を得ることができます）。

ユニットは、モニター対象のインターフェイス上で 15 秒間 hello メッセージを受信しなかった場合に（デフォルト）、インターフェイステストを実行します。（この時間を変更するには、**failover polltime interface** コマンド、アクティブ/アクティブ フェールオーバーの場合は **polltime interface** コマンドを参照してください）1 つのインターフェイスに対するインターフェイステストのいずれかが失敗したものの、他のユニット上のこの同じインターフェイスが正常にトラフィックを渡し続けている場合は、そのインターフェイスに障害があるものと見なされ、ASA はテストの実行を停止します。

障害が発生したインターフェイスの数に対して定義したしきい値が満たされ（**failover interface-policy** コマンド、またはアクティブ/アクティブ フェールオーバーの場合は **interface-policy** コマンドを参照）、さらに、アクティブユニットでスタンバイ装置よりも多くの障害が発生した場合は、フェールオーバーが発生します。両方のユニット上のインターフェイスに障害が発生した場合は、両方のインターフェイスが「未知」状態になり、フェールオーバー インターフェイス ポリシーで定義されているフェールオーバー限界値に向けてのカウントは行われません。

インターフェイスは、何らかのトラフィックを受信すると、再度動作状態になります。故障した ASA は、インターフェイス障害しきい値が満たされなくなった場合、スタンバイ モードに戻ります。

インターフェイスに IPv4 および IPv6 アドレスが設定されている場合、ASA は IPv4 を使用してヘルス モニタリングを実行します。インターフェイスに IPv6 アドレスだけが設定されている場合、ASAは ARP ではなく IPv6 ネイバー探索を使用してヘルス モニタリング テストを実行します。ブロードキャスト ping テストの場合、ASA は IPv6 全ノード アドレス（FE02::1）を使用します。

（注）
障害が発生した装置が回復せず、実際には障害は発生していないと考えられる場合は、**failover reset** コマンドを使用して状態をリセットできます。ただし、フェールオーバー条件が継続している場合、装置は再び障害状態になります。

インターフェイス テスト

ASAでは、次のインターフェイステストが使用されます。各テストの時間は約1.5秒（デフォルト）、またはフェールオーバー インターフェイスの保留時間の 1/16 です（**failover polltime interface** コマンドを参照するか、アクティブ/アクティブフェールオーバーの場合は **interface-policy** コマンドを参照）。

1. リンク アップ/ダウンテスト：インターフェイス ステータスのテストです。リンク アップ/ダウン テストでインターフェイスがダウンしていることが示された場合、ASA は障害が発生し、テストが停止したと見なします。ステータスがアップの場合、ASAはネットワーク アクティビティを実行します。

2. ネットワーク アクティビティ テスト：ネットワークの受信アクティビティのテストです。テストの開始時に、各装置はインターフェイスの受信パケット カウントをリセットします。テスト中にユニットが適切なパケットを受信すると、すぐにインターフェイスは正常に動作していると見なされます。両方の装置がトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はARP テストを開始します。

3. ARP テスト：ARP が正しく応答するかどうかをテストします。各ユニットは、ARP テーブル内の最新のエントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。ユニットが ARP 応答を受信しない場合、ASAは、ARP テーブル内の「次の」エントリの IP アドレスに対して単一の ARP 要求を送信します。ユニットがテスト中に ARP 応答またはその他のネットワーク トラフィックを受信する場合、インターフェイスは動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信していない場合は、ASA はブートストラップ ping テストを開始します。

4. ブロードキャスト Ping テスト：ping 応答が正しいかどうかをテストします。各ユニットがブロードキャスト ping を送信し、受信したすべてのパケットをカウントします。パケットはテスト中にパケットを受信すると、インターフェイスは正常に動作していると見なされます。両方のユニットがトラフィックを受信した場合、テストは停止します。どちらか一方のユニットだけがトラフィックを受信している場合は、トラフィックを受信していないユニットのインターフェイスで障害が発生していると見なされ、テストは停止します。どちらのユニットもトラフィックを受信しない場合、ARP テストを使用してテストが再開されます。両方の装置が ARP およびブロードキャスト ping テストからトラフィックを受信し続けない場合、これらのテストは永久に実行し続けます。

インターフェイス ステータス

モニタ対象のインターフェイスには、次のステータスがあります。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理のためにダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

フェールオーバー 時間

Firepower ハイアベイラビリティペアでは、次のイベントでフェールオーバーがトリガーされます。

- アクティブユニットの 50% を超える Snort インスタンスがダウンした場合
- アクティブユニットのディスク容量使用率が 90% を超えた場合
- アクティブユニットで **no failover active** コマンドが実行された場合、またはスタンバイユニットで **failover active** コマンドが実行された場合
- アクティブユニットで障害が発生したインターフェイスの数がスタンバイユニットよりも多くなった場合
- アクティブデバイスのインターフェイス障害が設定されたしきい値を超えた場合

  デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。デフォルト値を変更するには、フェールオーバーが発生するしきい値として、障害が発生したインターフェイスの数またはモニター対象インターフェイスの割合を設定します。アクティブデバイスでしきい値を超えると、フェールオーバーが発生します。スタンバイデバイスでしきい値を超えると、ユニットが **Fail** 状態に移行します。

  デフォルトのフェールオーバー条件を変更するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

表 *13 :*

コマンド	目的
failover interface-policy num [%] `hostname (config)# failover interface-policy 20%`	デフォルトのフェールオーバー基準を変更します。 インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 250 を設定できます。 インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

（注） CLI または ASDM を使用して手動でフェールオーバーした場合、もしくは ASA をリロードした場合、フェールオーバーはすぐに開始され、次に示すタイマーの影響は受けません。

表 *14 : ASA*

フェールオーバー条件	最小	デフォルト	最大数
アクティブユニットの電源の喪失、ハードウェアのダウン、ソフトウェアのリロードまたはクラッシュにより、モニター対象インターフェイスまたはフェールオーバーリンクでhelloメッセージを受信しなくなる。	800 ミリ秒	15 秒	45 秒
アクティブ ユニット メインボード インターフェイスリンクがダウンする。	500 ミリ秒	5 秒	15 秒
アクティブ ユニットの 4GE モジュール インターフェイス リンクがダウンする。	2 秒	5 秒	15 秒
アクティブ ユニットのインターフェイスは実行されているが、接続の問題によりインターフェイステストを行っている。	5 秒	25 秒	75 秒

設定の同期

フェールオーバーには、さまざまなタイプのコンフィギュレーション同期があります。

コンフィギュレーションの複製の実行

コンフィギュレーションの複製は、フェールオーバーペアの一方または両方のデバイスのブート時に実行されます。

アクティブ/スタンバイ フェールオーバーでは、コンフィギュレーションは常に、アクティブ装置からスタンバイ装置に同期化されます。

アクティブ/アクティブ フェールオーバーでは、起動ユニットのプライマリまたはセカンダリ指定に関係なく、2番目に起動したユニットは、最初に起動したユニットから実行コンフィギュレーションを取得します。両方のユニットの起動後、システム実行スペースに入力されたコマンドは、フェールオーバー グループ 1 がアクティブ状態であるユニットから複製されます。

スタンバイ/セカンドユニットが初期スタートアップを完了すると、実行コンフィギュレーションを削除し（アクティブ ユニットとの通信に必要な **failover** コマンドを除く）、アクティブ ユニットはコンフィギュレーション全体をスタンバイ/セカンド ユニットに送信します。複製が開始されると、アクティブ ユニットの ASA コンソールに「Beginning configuration replication: Sending to mate,」というメッセージが表示され、完了すると ASA に「End Configuration Replication to mate.」というメッセージが表示されます。コンフィギュレーションのサイズによって、複製には数秒から数分かかります。

コンフィギュレーションを受信する装置の場合、コンフィギュレーションは実行メモリにだけ存在します。コンフィギュレーションの変更の保存 （40 ページ）に従ってコンフィギュレーションをフラッシュ メモリに保存する必要があります。たとえば、アクティブ/アクティブ フェールオーバーでは、フェールオーバー グループ 1 がアクティブ状態であるユニット上のシステム実行スペースに **write memory all** コマンドを入力します。コマンドはピア装置に複製され、コンフィギュレーションがフラッシュ メモリに書き込まれます。

（注） 複製中、コンフィギュレーションを送信しているユニット上に入力されたコマンドは、ピア ユニットに正常に複製されず、コンフィギュレーションを受信するユニット上に入力されたコマンドは、受信したコンフィギュレーションによって上書きできます。コンフィギュレーションの複製処理中には、フェールオーバー ペアのどちらの装置にもコマンドを入力しないでください。

ファイルの複製

コンフィギュレーションの同期は次のファイルと構成コンポーネントを複製しません。したがって、これらのファイルが一致するように手動でコピーする必要があります。

- セキュア クライアント イメージ
- CSD イメージ
- セキュア クライアント プロファイル

  ASA では、フラッシュ ファイル システムに保存されたファイルではなく、cache:/stc/profiles に保存された セキュア クライアント プロファイルのキャッシュ済みファイルが使用されます。セキュア クライアント プロファイルをスタンバイ装置に複製するには、次のいずれかを実行します。

  - アクティブ装置で **write standby** コマンドを入力します。
  - アクティブ装置でプロファイルを再適用します。

- スタンバイ装置をリロードします。

- ローカル認証局（CA）
- ASA イメージ
- ASDM イメージ

コマンドの複製

起動した後、アクティブユニットで入力したコマンドはただちにスタンバイユニットに複製されます。 コマンドを複製する場合、アクティブ コンフィギュレーションをフラッシュ メモリに保存する必要はありません。

アクティブ/アクティブ フェールオーバーでは、システム実行スペースに入力したコマンドは、フェールオーバー グループ 1 がアクティブ状態である装置から複製されます。

コマンドの複製を行うのに適切な装置上でコマンドを入力しなかった場合は、コンフィギュレーションは同期されません。この変更内容は、次回に初期コンフィギュレーション同期が行われると失われることがあります。

スタンバイ ASA に複製されるコマンドは、次のとおりです。

- すべてのコンフィギュレーション コマンド（**mode**、**firewall**、および **failover lan unit** を除く）
- **copy running-config startup-config**
- **delete**
- **mkdir**
- **rename**
- **rmdir**
- **write memory**

スタンバイ ASA に複製されないコマンドは、次のとおりです。

- すべての形式の **copy** コマンド（**copy running-config startup-config** を除く）
- すべての形式の **write** コマンド（**write memory** を除く）
- **debug**
- **failover lan unit**
- **firewall**
- **show**
- **terminal pager** および **pager**

設定同期の最適化

デバイスが一時停止後に再起動するか、フェールーバーを再開する場合、参加するデバイスは実行中の設定をクリアします。次に、アクティブデバイスが、設定全体を参加デバイスに送信して完全に同期します。アクティブデバイスの設定が大規模な場合、このプロセスには数分かかることがあります。

設定同期最適化機能により、設定ハッシュ値を交換して、参加ユニットとアクティブユニットの設定を比較できます。アクティブデバイスと参加デバイスの両方で計算されたハッシュが一致する場合、参加デバイスは完全な設定同期をスキップし、フェールオーバー設定に再参加します。 この機能により、さらに迅速なピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。

設定同期の最適化のガイドラインと制限事項

- 設定同期最適化機能は、デフォルトで有効になっています。
- ASA のマルチコンテキストモードは、完全な設定同期中にコンテキストの順序を共有することによって設定同期最適化をサポートし、後続のノード再参加中にコンテキストの順序を比較できるようにします。
- パスフレーズとフェールオーバー IPsec キーを設定すると、アクティブユニットとスタンバイユニットで計算されたハッシュ値が異なるため、設定同期の最適化で効果を得られません。
- ダイナミック ACL または SNMPv3 を使用してデバイスを設定すると、設定同期最適化は効果を発揮しません。
- アクティブデバイスは、デフォルトの動作として、LAN リンクのフラッピングによって完全な設定を同期します。アクティブデバイスとスタンバイデバイス間のフェールオーバーフラッピングの間、設定同期最適化はトリガーされず、デバイスによって完全な設定同期が実行されます。
- フェールオーバー設定が中断やアクティブデバイスとスタンバイデバイス間のネットワーク通信の切断から復旧する際に、設定同期最適化がトリガーされます。

設定同期の監視

設定同期最適化機能が有効になっている場合、syslog メッセージが生成され、アクティブユニットと参加ユニットで計算されたハッシュ値が一致するか、一致しないか、または操作がタイムアウトになったかどうかが表示されます。また、ハッシュ要求を送信してからハッシュ応答を取得して比較するまでの経過時間も表示されます。

設定同期の最適化をモニタリングするには、次のコマンドを使用します。

- **show failover config-sync checksum**

  デバイスのステータスとチェックサムに関する情報を表示します。

- **show failover config-sync configuration**

  デバイスの設定とチェックサムに関する情報を表示します。

- **show failover config-sync status**

  設定同期最適化機能のステータスを表示します。

アクティブ/スタンバイ フェールオーバーについて

アクティブ/スタンバイ フェールオーバーでは、障害が発生した装置の機能を、スタンバイ ASA に引き継ぐことができます。アクティブ装置に障害が発生した場合、スタンバイ装置がアクティブ装置になります。ただし、セカンダリ装置の設定を保持するために、障害が発生した装置を交換する前に、スタンバイ装置をプライマリに設定する必要があります。

（注） マルチ コンテキスト モードでは、ASA は装置全体（すべてのコンテキストを含む）のフェールオーバーを行いますが、各コンテキストを個別にフェールオーバーすることはできません。

プライマリ/セカンダリ ロールとアクティブ/スタンバイ ステータス

フェールオーバーペアの2つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がスタンバイであるか、つまりどちらの IP アドレスを使用し、どちらの装置でアクティブにトラフィックを渡すかということに関連します。

しかし、プライマリである装置（コンフィギュレーションで指定）とセカンダリである装置との間で、いくつかの相違点があります。

- 両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。
- プライマリ装置の MAC アドレスは常にアクティブ IP アドレスと組み合わされます。このルールの例外は、セカンダリ装置がアクティブになり、フェールオーバー リンク経由でプライマリ装置の MAC アドレスを取得できない場合に発生します。この場合、セカンダリ装置の MAC アドレスが使用されます。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はスタンバイ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時にブートされた場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がスタンバイ装置になります。

フェールオーバー イベント

アクティブ/スタンバイフェールオーバーでは、フェールオーバーは装置ごとに行われます。マルチコンテキストモードで動作中のシステムでも、個々のコンテキストまたはコンテキストのグループをフェールオーバーすることはできません。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、スタンバイ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *15*：フェールオーバー イベント

障害イベント	ポリシー	アクティブユニットのアクション	スタンバイユニットのアクション	注記
アクティブユニットが故障(電源またはハードウェア)	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする	モニタ対象インターフェイスまたはフェールオーバーリンクでhelloメッセージが受信されることはありません。
以前にアクティブだったユニットが復旧	フェールオーバーなし	スタンバイになる	なし	なし。
スタンバイユニットが故障(電源またはハードウェア)	フェールオーバーなし	スタンバイに故障とマークする	該当なし	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。
動作中にフェールオーバーリンクに障害が発生した	フェールオーバーなし	フェールオーバーリンクに故障とマークする	フェールオーバーリンクに故障とマークする	フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる フェールオーバーリンクに故障とマークする	アクティブになる フェールオーバーリンクに故障とマークする	スタートアップ時にフェールオーバーリンクがダウンしていると、両方の装置がアクティブになります。
ステート リンクの障害	フェールオーバーなし	なし	なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。

障害イベント	ポリシー	アクティブユニットのアクション	スタンバイユニットのアクション	注記
しきい値を超えたアクティブユニットでインターフェイスに障害が発生	フェールオーバー	アクティブを障害としてマークする	アクティブになる	なし。
しきい値を超えたスタンバイユニットでインターフェイスに障害が発生	フェールオーバーなし	なし	スタンバイに故障とマークする	スタンバイ装置が故障とマークされている場合、インターフェイス障害しきい値を超えても、アクティブ装置はフェールオーバーを行いません。

アクティブ/アクティブ フェールオーバーの概要

この項では、アクティブ/アクティブ フェールオーバーについて説明します。

アクティブ/アクティブ フェールオーバーの概要

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、両方の ASA がネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーは、マルチ コンテキスト モードの ASA でのみ使用できます。アクティブ/アクティブ フェールオーバーでは、ASA のセキュリティ コンテキストを 2 つまでのフェールオーバー グループに分割します。

フェールオーバー グループは、1 つまたは複数のセキュリティ コンテキストの論理グループにすぎません。フェールオーバー グループをプライマリ ASA でアクティブに割り当て、フェールオーバー グループ 2 をセカンデリ ASA でアクティブに割り当てることができます。フェールオーバーが行われる場合は、フェールオーバー グループ レベルで行われます。たとえば、インターフェイス障害パターンに応じて、フェールオーバー グループ 1 をセカンデリ ASA にフェールオーバーし、続いてフェールオーバー グループ 2 をプライマリ ASA にフェールオーバーすることができます。このイベントは、プライマリ ASA でフェールオーバー グループ 1 のインターフェイスがダウンしたがセカンデリではアップしており、セカンデリ ASA でフェールオーバー グループ 2 のインターフェイスがダウンしたがプライマリ ASA ではアップしている場合に発生する可能性があります。

管理コンテキストは、常にフェールオーバー グループ 1 のメンバです。未割り当てセキュリティ コンテキストもまた、デフォルトでフェールオーバー グループ 1 のメンバです。アクティブ/アクティブ フェールオーバーが必要であるが複数コンテキストは必要ない場合、最もシンプルな設定は他のコンテキストを 1 つ追加し、それをフェールオーバー グループ 2 に割り当てることです。

（注） アクティブ/アクティブ フェールオーバーを構成する場合は、両方の装置の合計トラフィックが各装置の容量以内になるようにしてください。

（注） 必要に応じて両方のフェールオーバー グループを1つのASAに割り当てることもできますが、この場合、アクティブな ASA を 2 つ持つというメリットはありません。

フェールオーバー グループのプライマリ/セカンデリ ロールとアクティブ/スタンバイ ステータス

アクティブ/スタンバイ フェールオーバーと同様、アクティブ/アクティブ フェールオーバー ペアの 1 つの装置がプライマリ ユニットに指定され、もう 1 つの装置がセカンダリ ユニットに指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方の装置が同時に起動された場合、この指定ではどちらの装置がアクティブになるか指示しません。代わりに、プライマリまたはセカンダリの指定時に、次の 2 つの点を判定します。

- ペアが同時に起動したときに、プライマリ装置が実行コンフィギュレーションを提供します。
- コンフィギュレーションの各フェールオーバー グループは、プライマリまたはセカンダリ装置プリファレンスが設定されます。プリエンプションで使用すると、このプレファレンスはフェールオーバー グループが起動後に正しいユニットで実行されるようにします。プリエンプションがない場合、両方のグループは最初に起動したユニットで動作します。

起動時のフェールオーバー グループのアクティブ装置の決定

フェールオーバー グループがアクティブになる装置は、次のように決定されます。

- ピア装置が使用できないときに装置がブートされると、両方のフェールオーバー グループがピア装置でアクティブになります。
- ピア装置がアクティブ（両方のフェールオーバー グループがアクティブ状態）の場合に装置がブートされると、フェールオーバー グループは、アクティブ装置でアクティブ状態のままになります。これは、次のいずれかの状態になるまで、フェールオーバー グループのプライマリ プリファレンスまたはセカンダリ プリファレンスには関係ありません。
  - フェールオーバーが発生した。
  - 手動でフェールオーバーを強制実行した。
  - フェールオーバーグループのプリエンプションを設定した。この設定により、優先する装置が使用可能になると、フェールオーバーグループはその装置上で自動的にアクティブになります。

フェールオーバー イベント

アクティブ/アクティブ フェールオーバー コンフィギュレーションでは、フェールオーバーは、システムごとに行うのではなく、フェールオーバー グループごとに行われます。たとえば、プライマリユニットで両方のフェールオーバーグループをアクティブと指定し、フェール

オーバーグループ 1 が故障すると、フェールオーバーグループ 2 はプライマリユニットでアクティブのままですが、フェールオーバーグループ 1 はセカンダリユニットでアクティブになります。

フェールオーバー グループには複数のコンテキストを含めることができ、また各コンテキストには複数のインターフェイスを含めることができるので、1 つのコンテキストのインターフェイスがすべて故障しても、そのコンテキストに関連するフェールオーバー グループが故障と判断されない可能性があります。

次の表に、各障害イベントに対するフェールオーバーアクションを示します。各障害イベントに対して、ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ フェールオーバー グループのアクション、およびスタンバイ フェールオーバー グループのアクションを示します。

表 *16 :* フェールオーバー イベント

障害イベント	ポリシー	アクティブ グループのアクション	スタンバイ グループのアクション	注記
装置で電源断またはソフトウェア障害が発生した	フェールオーバー	スタンバイになる 故障とマークする	アクティブになる アクティブを障害としてマークする	フェールオーバーペアの装置が故障すると、その装置のアクティブ フェールオーバー グループはすべて故障とマークされ、ピア装置のフェールオーバー グループがアクティブになります。
アクティブ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバー	アクティブ グループに故障とマークする	アクティブになる	なし。
スタンバイ フェールオーバー グループにおけるしきい値を超えたインターフェイス障害	フェールオーバーなし	なし	スタンバイ グループに故障とマークする	スタンバイ フェールオーバー グループが故障とマークされている場合、インターフェイス フェールオーバー障害しきい値を超えても、アクティブ フェールオーバー グループはフェールオーバーを行いません。
以前にアクティブであったフェールオーバー グループの復旧	フェールオーバーなし	なし	なし	フェールオーバー グループのプリエンプションが設定されている場合を除き、フェールオーバー グループは現在の装置でアクティブのままです。

障害イベント	ポリシー	アクティブ グループのアクション	スタンバイ グループのアクション	注記
スタートアップ時にフェールオーバー リンクに障害が発生した	フェールオーバーなし	アクティブになる	アクティブになる	スタートアップ時にフェールオーバー リンクがダウンしていると、両方の装置の両方のフェールオーバー グループがアクティブになります。
ステート リンクの障害	フェールオーバーなし	なし	なし	ステート情報が古くなり、フェールオーバーが発生するとセッションが終了します。
動作中にフェールオーバー リンクに障害が発生した	フェールオーバーなし	適用対象外	適用対象外	各装置で、フェールオーバー リンクが故障とマークされます。フェールオーバー リンクがダウンしている間、装置はスタンバイ装置にフェールオーバーできないため、できるだけ早くフェールオーバー リンクを復元する必要があります。

フェールオーバーのライセンス

ほとんどのモデルでは、フェールオーバーユニットは、各ユニット上で同一のライセンスを必要としません。両方のユニット上にライセンスがある場合、これらのライセンスは単一の実行フェールオーバー クラスタ ライセンスに結合されます。このルールには、いくつかの例外があります。フェールオーバーの正確なライセンス要件については、次の表を参照してください。

モデル	ライセンス要件
ASA 仮想	ASAv のフェールオーバー ライセンス （108 ページ）を参照してください。
Firepower 1010	両方のユニットの Security Plus ライセンス。Firepower 1010 のフェールオーバー ライセンス （108 ページ）を参照してください。
Firepower 1100	Firepower 1100 のフェールオーバー ライセンス （108 ページ）を参照してください。
Cisco Secure Firewall 1210/1220	「Secure Firewall 1210/1220 のフェールオーバー ライセンス （110 ページ）」を参照してください。
Secure Firewall 1230/1240/1250	Secure Firewall 1230/1240/1250 のフェールオーバー ライセンス （112 ページ）を参照してください。

モデル	ライセンス要件
Cisco Secure Firewall 3100/4200	Secure Firewall 3100 のフェールオーバーライセンス （114 ページ）を参照してください。
Firepower 4100/9300	「Firepower 4100/9300のフェールオーバーライセンス （117 ページ）」を参照してください。
ISA 3000	両方のユニットの Security Plus ライセンス。 （注） 各ユニットに同じ暗号化ライセンスが必要です。

（注） 有効な永続キーが必要です。まれに、ISA 3000 で、PAK 認証キーを削除できることもあります。キーがすべて 0 の場合は、フェールオーバーを有効化するには有効な認証キーを再インストールする必要があります。

フェールオーバー のガイドライン

コンテキスト モード

- アクティブ/アクティブ モードは、マルチ コンテキスト モードでのみサポートされます。
- マルチ コンテキスト モードでは、特に注記がない限り、手順はすべてシステム実行スペースで実行します。

モデルのサポート

- Firepower 1010 および Cisco Secure Firewall 1210/1220：
  - フェールオーバーを使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェールオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニタできますが、スイッチ ポートはモニタできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、フェールオーバー を正常に使用することができますが、代わりに物理ファイアウォール インターフェイスを使用する設定の方が簡単です。
  - ファイアウォール インターフェイスはフェールオーバー リンクとしてのみ使用できます。

- FirePOWER 9300：シャーシ間フェールオーバーを使用して最良の冗長性を確保することを推奨します。
- Microsoft Azure や Amazon Web Services などのパブリック クラウド ネットワーク上の ASA 仮想 では、レイヤ 2 接続が必要なため、通常の フェールオーバーはサポートされません。代わりに、パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー（383 ページ）を参照してください。

ハイアベイラビリティを実現するための ASA 仮想 のフェールオーバー

ASA 仮想 を使用してフェールオーバーペアを作成する場合は、データインターフェイスを各 ASA 仮想 に同じ順序で追加する必要があります。完全に同じインターフェイスが異なる順序で各 ASA 仮想 に追加されると、ASA 仮想 コンソールにエラーが表示されることがあります。また、フェールオーバー機能にも影響が出ることがあります。

その他のガイドライン

- アクティブ装置がスタンバイ装置にフェールオーバーするときに、スパニング ツリー プロトコル（STP）を実行している接続済みスイッチ ポートが、トポロジの変化を検出すると 30 ～ 50 秒間ブロッキング状態になる可能性があります。ポートがブロッキング ステートである間のトラフィックの損失を回避するために、スイッチで STP PortFast 機能を有効にすることができます。

  interface *interface_id* **spanning-tree portfast**

  この回避策は、ルーテッド モード インターフェイスとブリッジ グループ インターフェイスの両方に接続されたスイッチに適用されます。PortFast 機能を設定すると、リンクアップと同時にポートが STP フォワーディング モードに遷移します。ポートは STP に参加し続けます。したがって、ポートがループの一部になる場合、最終的には STP ブロッキング モードに遷移します。

- ASA フェールオーバーペアに接続されたスイッチ上でポートセキュリティを設定すると、フェールオーバーイベントが発生したときに通信の問題が起きることがあります。この問題は、あるセキュア ポートで設定または学習されたセキュア MAC アドレスが別のセキュア ポートに移動し、スイッチのポート セキュリティ機能によって違反フラグが付けられた場合に発生します。
- すべてのコンテキストにわたり、1 台の装置の最大 1025 のインターフェイスをモニタできます。
- アクティブ/スタンバイ フェールオーバー と VPN IPsec トンネルの場合、SNMP を使用して VPN トンネル上でアクティブ ユニットとスタンバイ ユニットの両方をモニターすることはできません。スタンバイ ユニットにはアクティブ VPN トンネルがないため、NMS に向けられたトラフィックはドロップされます。代わりに暗号化付き SNMPv3 を使用すれば、IPsec トンネルが不要になります。
- アクティブ/アクティブ フェールオーバーでは、同じコンテキスト内の 2 つのインターフェイスを同じ ASR グループ内で設定することはできません。

- アクティブ/アクティブ フェールオーバーでは、最大 2 つのフェールオーバー グループを定義できます。
- アクティブ/アクティブ フェールオーバーでフェールオーバー グループを削除する場合は、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には常に管理コンテキストが含まれます。フェールオーバー グループに割り当てられていないコンテキストはすべて、デフォルトでフェールオーバー グループ 1 になります。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。
- フェールオーバーの直後に、syslog メッセージの送信元アドレスが数秒間フェールオーバー インターフェイス アドレスになります。
- （フェールオーバー中に）コンバージェンスを向上させるには、どの設定やインスタンスにも関連付けられていない HA ペアのインターフェイスをシャットダウンする必要があります。
- 評価モードでフェールオーバー暗号化を設定すると、システムは暗号化に DES を使用します。エクスポート準拠アカウントを使用してデバイスを登録すると、デバイスはリブート後に AES を使用します。したがって、アップグレードのインストール後など、何らかの理由でシステムがリブートすると、ピアは通信できなくなり、両方のユニットがアクティブユニットになります。デバイスを登録するまで、暗号化を設定しないことを推奨します。評価モードで暗号化を設定する場合は、デバイスを登録する前に暗号化を削除することを推奨します。
- フェールオーバーで SNMPv3 を使用する場合、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットにレプリケートされません。ユーザを新しいユニットに強制的にレプリケートするには、SNMPv3 ユーザをアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます。アクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してスタンバイユニットに直接入力することにより、各ユーザを再設定します。
- デバイスは、SNMP クライアントのエンジンデータをピアと共有しません。
- 非常に多数のアクセスコントロールルールと NAT ルールがある場合、設定のサイズによって効率的な設定のレプリケーションが妨げられる可能性があり、その結果、スタンバイユニットがスタンバイ準備完了状態に達するまでの時間が長くなります。これは、コンソールまたは SSH セッションを介したレプリケーション中にスタンバイユニットに接続する機能にも影響を与える可能性があります。設定のレプリケーションのパフォーマンスを向上させるには、**asp rule-engine transactional-commit access-group** および **asp rule-engine transactional-commit nat** コマンドを使用して、アクセスルールと NAT の両方でトランザクションコミットを有効にします。
- スタンバイロールに移行する フェールオーバー ペアのユニットは、アクティブユニットとクロックを同期します。

  例：

```
firepower#show clock
01:00:52 UTC Mar 1 2022

...
01:01:18 UTC Mar 1 2022 <======= Incorrect (previous) clock
Cold Standby               Sync Config               Detected an Active mate

19:38:21 UTC Apr 9 2022 <======= Updated clock
Sync Config                Sync File System          Detected an Active mate
...
firepower/sec/stby#show clock
19:38:40 UTC Apr 9 2022
```

- フェールオーバーのユニットは、クロックを動的に同期しません。同期が行われるときのイベントの例を次に示します。
  - 新しい フェールオーバー ペアが作成される。
  - フェールオーバー が中断されて再作成される。
  - フェールオーバーリンクを介した通信が中断され、再確立される。
  - 、フェールオーバーステータスが CLI で手動で変更された。
- フェールオーバー を有効にすると、すべてのルートが強制的に削除され、フェールオーバーの進行がアクティブ状態に変わった後に再度追加されます。このフェーズ中に接続が失われる可能性があります。
- スタンドアロンデバイスでフェールオーバーを有効にすると、データインターフェイスがフェールオーバーのネゴシエーション状態でダウンし、トラフィックが中断されます。
- フェールオーバー設定では、一般にポート53を使用する短時間の接続はすぐに閉じられ、それらの接続がアクティブからスタンバイに転送または同期されることはありません。そのため、両方の フェールオーバー デバイスの接続数に違いが生じる可能性があります。これは、短時間の接続の予期される動作です。長時間（たとえば、30 ～ 60 秒を超える）の接続の比較を試みることができます。
- フェールオーバー 設定では、初期接続（3 ウェイ ハンドシェイク プロセスがまだ完了していない接続要求）はすぐに閉じられ、アクティブデバイスとスタンバイデバイス間で同期されません。この設計により、HA システムの効率とセキュリティが確保されます。このため、両方のフェールオーバーデバイスで接続数に違いが生じる可能性がありますが、これは予想されることです。
- フェールオーバー LAN リンクがバックツーバックで接続されておらず、代わりに 1 つ以上のスイッチを介して接続されている場合、中間経路内の障害によってアクティブユニットとスタンバイユニットの接続が失われ、アクティブ/スタンバイ状態の一貫性が失われる可能性があります。これは フェールオーバー 機能には影響しませんが、アクティブユニットとスタンバイユニット間のフェールオーバーリンク経路を確認して回復することをお勧めします。

  フェールオーバー LAN リンクがダウンしている場合、設定はピアユニットに複製されない可能性があるため、設定を展開することは推奨されません。

- Cisco ASA の OSPF では、近くのスイッチがダウンし、Cisco ASA インターフェイスが同じスイッチに接続されている場合、ファイアウォール内のインターフェイスもダウンしてスイッチの障害が発生します。これは予期された動作です。これにより、設計どおりに高可用性フェールオーバーがトリガーされます。
- スタンバイの Cisco ASA が別のスイッチに接続されている場合は、インターフェイスが起動すると、ルーティングテーブルは、アクティブの Cisco ASA のルーティングテーブルとは異なります。これにより、ルートと隣接関係（アジャセンシー）が更新されるまでの短期間（約 15 ー 17 秒）の障害が発生します。
- トランスペアレントモードでは、アクティブユニットでホットスタンバイルータ（HSRP）の MAC アドレスが失われるという問題が発生した場合は、MAC アドレスのスタティック マッピングを作成します。

フェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートフル フェールオーバーでの HTTP 複製は行われません。
- 単一のインターフェイス障害でフェールオーバーが行われます。
- インターフェイスのポーリング時間は 5 秒です。
- インターフェイスのホールド時間は 25 秒です。
- 装置のポーリング時間は 1 秒です。
- 装置のホールド時間は 15 秒です。
- 仮想 MAC アドレスはマルチコンテキストモードで無効化されていますが。
- すべての物理インターフェイスをモニタリングします。

アクティブ/スタンバイ フェールオーバーの設定

アクティブ/スタンバイ フェールオーバーを設定するには、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。その他すべての設定をプライマリ装置でのみ行った後、セカンデリ装置に設定を同期させます。

アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/スタンバイ フェールオーバー構成のプライマリを設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

始める前に

- フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。 ポイントツーポイント接続に 31 ビット サブネット マスクを使用する場合、スタンバイ IP アドレスを設定しないでください。いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 この装置をプライマリ装置に指定します。

failover lan unit primary

ステップ 2 フェールオーバー リンクとして使用するインターフェイスを指定します。

failover lan interface *if_name interface_id*

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、データ物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。Firepower 1010 および Secure Firewall 1210/1220 では、インターフェイスはファイアウォール インターフェイス ID です。スイッチ ポート ID または VLAN ID を指定することはできません。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。

ステップ 3 アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

failover interface ip *failover_if_name* {*ip_address mask* | *ipv6_address* / *prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

または：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

このアドレスは未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステップ 4 フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5 （オプション）ステートリンクに別のインターフェイスを使用する場合は、そのインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link folink gigabitethernet0/4
```

別のインターフェイスを指定しない場合、フェールオーバーリンクがステートリンクに使用されます。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。Firepower 1010 および Secure Firewall 1210/1220 では、インターフェイスはファイアウォール インターフェイス ID です。スイッチ ポート ID または VLAN ID を指定することはできません。

ステップ 6 別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

failover interface ip *state_if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
```

```
2001:a0a:b00:a::a0a:b71
```

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバー リンクやステート リンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 7 別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 8 （オプション）フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のいずれかを実行します。

- （優先）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsec pre-shared-key [**0** | **8**] *key*

  例：

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

  マスターパスフレーズ（マスターパスフレーズの設定（1015ページ）を参照）を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば**more system:running-config** の出力からのコピー）、キーワード **8** を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  show running-config の出力では、**failover ipsec pre-shared-key** は ***** のように表示されます。このマスクされたキーはコピーできません。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  例：

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **16 進数**キーを使用します。*shared_secret* には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または 16 進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスターパスフレーズ（マスターパスフレーズの設定（1015ページ）を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば **more system:running-config** の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  failover key の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

ステップ 9 フェールオーバーをイネーブルにします。

failover

ステップ 10 システム コンフィギュレーションをフラッシュ メモリに保存します。

write memory

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
```

```
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link folink gigabitethernet0/3
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/スタンバイ フェールオーバーのセカンダリ装置の設定

セカンデリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

始める前に

- いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。アクティブ/スタンバイ フェールオーバーのプライマリ装置の設定 （347 ページ）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-ifc)# no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2 フェールオーバー コンフィギュレーションが同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

```
ciscoasa(config)# write memory
```

アクティブ/アクティブ フェールオーバーの設定

ここでは、アクティブ/アクティブ フェールオーバーの設定方法について説明します。

アクティブ/アクティブ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/アクティブ フェールオーバー コンフィギュレーションでプライマリ装置を設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

始める前に

- マルチ コンテキスト モードの有効化または無効化 （278 ページ）に従って、マルチ コンテキスト モードをイネーブルにします。
- ルーテッドモードおよびトランスペアレントモードのインターフェイス （927ページ）に従って、フェールオーバー リンクとステート リンクを除くすべてのインターフェイスのスタンバイ IP アドレスを設定することを推奨します。 ポイントツーポイント接続に 31 ビット サブネット マスクを使用する場合、スタンバイ IP アドレスを設定しないでください。いずれかのインターフェイスがDHCP用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 この装置をプライマリ装置に指定します。

failover lan unit primary

ステップ 2 フェールオーバー リンクとして使用するインターフェイスを指定します。

failover lan interface *if_name interface_id*

例：

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
```

このインターフェイスは、他の目的には使用できません（オプションのステート リンクは除く）。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、またはEtherChannelインターフェイス ID を指定できます。Firepower 4100/9300 では、任意のデータタイプ インターフェイスを使用できます。

ステップ 3 アクティブ IP アドレスとスタンバイ IP アドレスをフェールオーバー リンクに割り当てます。

standby failover interface ip *if_name* {*ip_address mask* | *ipv6_address*/*prefix* } **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

または：

```
ciscoasa(config)# failover interface ip folink 2001:a0a:b00::a0a:b70/64 standby
2001:a0a:b00::a0a:b71
```

このアドレスは未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステップ 4 フェールオーバー リンクをイネーブルにします。

interface *failover_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# no shutdown
```

ステップ 5 （オプション）ステートリンクに別のインターフェイスを使用する場合は、そのインターフェイスを指定します。

failover link *if_name interface_id*

例：

```
ciscoasa(config)# failover link statelink gigabitethernet0/4
```

フェールオーバーリンクとは別のステートリンクを使用することをお勧めします。別のインターフェイスを指定しない場合、フェールオーバーリンクがステートリンクに使用されます。

if_name 引数は、インターフェイスに名前を割り当てます。

interface_id 引数には、物理インターフェイス、サブインターフェイス、または EtherChannel インターフェイス ID を指定できます。

ステップ 6 別のステート リンクを指定した場合、ステート リンクにアクティブ IP アドレスとスタンバイ IP アドレスを割り当てます。

このアドレスは、フェールオーバー リンクとは異なる未使用のサブネット上になければなりません。 このサブネットは IP アドレスが 2 つだけの 31 ビット（255.255.255.254）にすることができます。169.254.1.0/24 and fd00:0:0:*::/64 は内部的に使用されるサブネットであり、フェールオーバーリンクやステートリンクに使用することはできません。

スタンバイ IP アドレスは、アクティブ IP アドレスと同じサブネットである必要があります。

ステート リンクを共有する場合は、この手順をとばしてください。

failover interface ip state *if_name* {*ip_address mask* | *ipv6_address*/*prefix*} **standby** *ip_address*

例：

```
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
```

または：

```
ciscoasa(config)# failover interface ip statelink 2001:a0a:b00:a::a0a:b70/64 standby
2001:a0a:b00:a::a0a:b71
```

ステップ 7 別のステート リンクを指定した場合、ステート リンクをイネーブルにします。

interface *state_interface_id*

no shutdown

例：

```
ciscoasa(config)# interface gigabitethernet 0/4
ciscoasa(config-if)# no shutdown
```

ステート リンクを共有する場合は、この手順をとばしてください。

ステップ 8 （オプション）フェールオーバー リンクおよびステート リンクの通信を暗号化するには、次のいずれかを実行します。

- （優先）すべてのフェールオーバー通信を暗号化するには、装置間のフェールオーバー リンクおよびステート リンクの IPsec LAN-to-LAN トンネルを確立します。

  failover ipsec pre-shared-key [**0** | **8**] *key*

  ```
  ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
  ```

  key は最大 128 文字です。両方の装置に同じキーを指定します。キーは IKEv2 によってトンネルを確立するために使用されます。

マスターパスフレーズ（マスターパスフレーズの設定（1015ページ）を参照）を使用している場合、キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば**more system:running-config**の出力からのコピー）、キーワード**8**を使用してキーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

show running-config の出力では、**failover ipsec pre-shared-key** は ***** のように表示されます。このマスクされたキーはコピーできません。

フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

IPsec 暗号化とレガシーの **failover key** 暗号化の両方を使用することはできません。両方の方法を設定した場合は、IPsec が使用されます。ただし、マスター パスフレーズを使用する場合、IPsec 暗号化を設定する前に **no failover key** コマンドを使用してフェールオーバー キーを削除する必要があります。

フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。

- （オプション）フェールオーバー リンクおよびステート リンクのフェールオーバー通信を暗号化します。

  failover key [**0** | **8**] {**hex** *key* | *shared_secret*}

  ```
  ciscoasa(config)# failover key johncr1cht0n
  ```

  1 ～ 63 文字の *shared_secret* または 32 文字の **16 進数**キーを使用します。

  shared_secret には、数字、文字、または句読点の任意の組み合わせを使用できます。共有秘密または16進数キーは暗号キーを生成するために使用されます。両方の装置に同じキーを指定します。

  マスターパスフレーズ（マスターパスフレーズの設定（1015ページ）を参照）を使用している場合、共有秘密または 16 進数キーはコンフィギュレーション内で暗号化されています。コンフィギュレーションからコピーする場合は（たとえば**more system:running-config**の出力からのコピー）、キーワード **8** を使用して共有秘密または 16 進数キーが暗号化されていることを指定します。デフォルトでは、暗号化されていないパスワードを指定する **0** が使用されます。

  failover key の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。

  フェールオーバー リンクおよびステート リンクの暗号化を設定しない場合、フェールオーバー通信はクリア テキストになります。この通信にはコマンド複製中に送信されるコンフィギュレーション内のすべてのパスワードやキーも含まれます。

ステップ 9　フェールオーバー グループ 1 を作成します。

failover group 1

primary

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# failover group 1
ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 1200
```

通常、プライマリ装置にグループ 1 を割り当て、セカンデリ装置にグループ 2 を割り当てます。グループの primary または secondary の設定にかかわらず、両方のフェールオーバー グループが最初にブートしたユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。**preempt** コマンドは、指定された装置が使用可能になったときに、フェールオーバー グループがその装置で自動的にアクティブになるようにします。

オプションの *delay* 値に秒数を入力して、その時間フェールオーバー グループが現在の装置でアクティブ状態に維持され、その後に指定された装置で自動的にアクティブになるようにできます。有効な値は 1 ～ 1200 です。

ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバー グループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

手動でフェールオーバーすると、**preempt** コマンドは無視されます。

ステップ 10 フェールオーバー グループ 2 を作成して、セカンデリ装置に割り当てます。

failover group 2

secondary

preempt [*delay*]

例：

```
ciscoasa(config-fover-group)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 1200
```

ステップ 11 特定のコンテキストのコンテキスト コンフィギュレーション モードに入り、そのコンテキストをフェールオーバー グループに割り当てます。

context *name*

join-failover-group{**1** |**2**}

例：

```
ciscoasa(config)# context Eng
ciscoasa(config-ctx)# join-failover-group 2
```

コンテキストごとにこのコマンドを繰り返します。

未割り当てのコンテキストはすべて、自動的にフェールオーバー グループ 1 に割り当てられます。管理コンテキストは常にフェールオーバー グループ 1 のメンバーです。グループ 2 に割り当てることはできません。

ステップ 12 フェールオーバーをイネーブルにします。

failover

ステップ 13 システム コンフィギュレーションをフラッシュ メモリに保存します。

write memory

例

次に、プライマリ装置用のフェールオーバー パラメータの設定例を示します。

```
failover lan unit primary
failover lan interface folink gigabitethernet0/3

failover interface ip folink 172.27.48.0 255.255.255.254 standby 172.27.48.1
interface gigabitethernet 0/3
  no shutdown
failover link statelink gigabitethernet0/4

failover interface ip statelink 172.27.48.2 255.255.255.254 standby 172.27.48.3
interface gigabitethernet 0/4
  no shutdown
failover group 1
  primary
  preempt
failover group 2
  secondary
  preempt
context admin
  join-failover-group 1
failover ipsec pre-shared-key a3rynsun
failover
```

アクティブ/アクティブ フェールオーバーのセカンデリ装置の設定

セカンデリ装置に必要なコンフィギュレーションは、フェールオーバー リンクのコンフィギュレーションだけです。セカンダリ装置には、プライマリ装置と初期に通信するために、これらのコマンドが必要です。プライマリ装置がセカンダリ装置にコンフィギュレーションを送信した後、2 つのコンフィギュレーション間で唯一、不変の相違点は **failover lan unit** コマンドです。このコマンドで各装置がプライマリかセカンダリかを識別します。

始める前に

- マルチ コンテキスト モードの有効化または無効化 （278 ページ）に従って、マルチ コンテキスト モードをイネーブルにします。

- いずれかのインターフェイスが DHCP 用に設定されている場合、フェールオーバーをイネーブルにすることはできません。
- フェールオーバー リンクおよびステート リンクに **nameif** を設定しないでください。
- この手順はシステム実行スペースで実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 **failover lan unit primary** コマンドを除いて、プライマリ装置とまったく同じコマンドを再入力します。任意で **failover lan unit secondary** コマンドに置き換えることもできますが、**secondary** はデフォルト設定のため、必須ではありません。また、プライマリ装置から複製されるので、**failover group** コマンドおよび **join-failover-group** コマンドを入力する必要もありません。アクティブ/アクティブ フェールオーバーのプライマリ装置の設定（353 ページ）を参照してください。

次に例を示します。

```
ciscoasa(config)# failover lan interface folink gigabitethernet0/3
INFO: Non-failover interface config is cleared on GigabitEthernet0/3 and its sub-interfaces
ciscoasa(config)# failover interface ip folink 172.27.48.1 255.255.255.0 standby
172.27.48.2
ciscoasa(config)# interface gigabitethernet 0/3
no shutdown
ciscoasa(config)# failover link statelink gigabitethernet0/4
INFO: Non-failover interface config is cleared on GigabitEthernet0/4 and its sub-interfaces
ciscoasa(config)# failover interface ip statelink 172.27.49.1 255.255.255.0 standby
172.27.49.2
ciscoasa(config)# interface gigabitethernet 0/4
no shutdown
ciscoasa(config)# failover ipsec pre-shared-key a3rynsun
ciscoasa(config)# failover
```

ステップ 2 フェールオーバー コンフィギュレーションがプライマリ装置と同期された後で、コンフィギュレーションをフラッシュ メモリに保存します。

ciscoasa(config)# **write memory**

ステップ 3 必要に応じて、フェールオーバー グループ 2 がセカンデリ装置でアクティブになるように設定します。

failover active group 2

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、フェールオーバーのデフォルト（347ページ）を参照してください。アクティブ/アクティブモードでは、ほとんどの条件をフェールオーバー グループごとに設定します。

始める前に

- マルチ コンテキスト モードのシステム実行スペースで次の設定を行います。
- ユニットのヘルス モニタリングの Bidirectional Forwarding Detection（BFD）については次の制限を参照してください。
  - FirePOWER 9300 および 4100 のみ
  - アクティブ/スタンバイのみ
  - ルーテッド モードのみ

手順

ステップ 1 装置のポーリング時間およびホールド時間を変更します。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

例：

```
ciscoasa(config)# failover polltime unit msec 200 holdtime msec 800
```

polltime の範囲は 1 ～ 15 秒または 200 ～ 999 ミリ秒です。**holdtime** の範囲は 1 ～ 45 秒または 800 ～ 999 ミリ秒です。ユニットのポーリング時間の 3 倍未満のホールド時間の値を入力することはできません。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

1 回のポーリング期間中に、装置がフェールオーバー通信インターフェイスで hello パケットを検出しなかった場合、残りのインターフェイスで追加テストが実行されます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

アクティブ/アクティブモードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

ステップ 2 ユニットのヘルス モニタリングの BFD を設定します。

CPU の使用率が高い場合、通常のユニットのモニタリングにより誤ってアラームが発生する可能性があります。BFD メソッドは分散されていてるため、CPU の使用率が高い場合でも動作に影響はありません。

a) フェールオーバーのヘルス検出に使用する BFD テンプレートを定義します。

bfd-template single-hop *template_name*

bfd interval min-tx *milliseconds***min-rx** *milliseconds* **multiplier** *multiplier_value*

例：

```
ciscoasa(config)# bfd template single-hop failover-temp
ciscoasa(config-bfd)# bfd interval min-tx 50 min-rx 50 multiplier 3
```

min-tx で、BFD 制御パケットがフェールオーバー ピアに送信されるレートを指定します。有効値は 50 ～ 999 ミリ秒です。**min-rx** で、BFD 制御パケットをフェールオーバー ピアから受信するレートの期待値を指定します。有効値は 50 ～ 999 ミリ秒です。フェールオーバー ピアから紛失した連続した BFD 制御パケットの数が、**multiplier** で指定した数に達すると、BFD はそのピアが利用不可になっていることを宣言します。指定できる範囲は 3 ～ 50 です。

このテンプレートのエコーおよび認証も設定できます。BFDテンプレートの作成（1189ページ） を参照してください。

b) ヘルス モニタリングの BFD を有効化します。

failover health-check bfd *template_name*

例：

```
ciscoasa(config)# failover health-check bfd failover-temp
```

ステップ 3 インターフェイス リンク ステート ポーリング時間を変更します。

failover polltime link-state msec *poll_time*

例：

```
ciscoasa(config)# failover polltime link-state msec 300
```

範囲は 300 ～ 799 ミリ秒です。デフォルトでは、フェールオーバーのペアの ASA では、インターフェイスのリンク ステートが 500 ミリ秒ごとに確認されます。polltime はカスタマイズできます。たとえば、polltime を 300 ミリ秒に設定すると、ASA ではインターフェイスの障害やトリガーのフェールオーバーをより早く検出できるようになります。

アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

ステップ 4 セッションの複製レートを、1 秒間の接続数で設定します。

failover replication rate *conns*

例：

```
ciscoasa(config)# failover replication rate 20000
```

最小および最大レートはモデルによって異なります。デフォルトは最大レートです。アクティブ/アクティブ モードでは、システムに対してこのレートを設定します。フェールオーバー グループごとにこのレートを設定することはできません。

ステップ 5 スタンバイ装置またはコンテキストのコンフィギュレーションを直接変更できないようにします。

failover standby config-lock

デフォルトでは、スタンバイ ユニットまたはスタンバイ コンテキストに対するコンフィギュレーションは、警告メッセージ付きで許可されます。

ステップ 6 （アクティブ/アクティブ モードのみ）カスタマイズするフェールオーバー グループを指定します。

failover group {**1** | **2**}

例：

```
ciscoasa(config)# failover group 1
ciscoasa(config-fover-group)#
```

ステップ 7 HTTP ステート複製をイネーブルにします。

- アクティブ/スタンバイ モードの場合

  failover replication http

- アクティブ/アクティブ モードの場合

  replication http

HTTP 接続がステート情報複製に含まれるようにするには、HTTP 複製をイネーブルにする必要があります。HTTP ステート複製を有効にすることをお勧めします。

（注）
フェールオーバーを使用しているときに、スタンバイ装置からHTTPフローを削除すると遅延が生じます。このため **show conn count** 出力には、アクティブ装置とスタンバイ装置で異なる数が表示されることがあります。数秒待ってコマンドを再発行すると、両方の装置で同じカウントが表示されます。

ステップ 8 インターフェイスに障害が発生したときのフェールオーバーのしきい値を設定します。

- アクティブ/スタンバイ モードの場合

  failover interface-policy *num* [%]

  例：

  ```
  ciscoasa (config)# failover interface-policy 20%
  ```

- アクティブ/アクティブ モードの場合

  interface-policy *num* [%]

例：

```
ciscoasa(config-fover-group)# interface-policy 20%
```

デフォルトでは、1 つのインターフェイス障害でフェールオーバーが行われます。

インターフェイスの具体的な数を指定するときは、*num* 引数に 1 ～ 1025 を設定できます。

インターフェイスの割合を指定するときは、*num* 引数に 1 ～ 100 を設定できます。

ステップ 9 インターフェイスのポーリング時間とホールド時間を変更します。

- アクティブ/スタンバイ モードの場合

  failover polltime interface [**msec**] *polltime* [**holdtime** *time*]

  例：

  ```
  ciscoasa(config)# failover polltime interface msec 500 holdtime 5
  ```

- アクティブ/アクティブ モードの場合

  polltime interface [**msec**] *polltime* [**holdtime***time*]

  例：

  ```
  ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
  ```

- *polltime*：helloパケットをピアに送信するまで待機する時間を設定します。polltimeに有効な値は 1 ～ 15 秒で、オプションの **msec** キーワードを使用する場合は 500 ～ 999 ミリ秒です。デフォルトは 5 秒です。
- **holdtime***time*：ピア ユニットからの最後に受信した hello メッセージとインターフェイス テストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイス テストの期間を holdtime/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、polltime の5倍です。polltime の 5 倍よりも短い holdtime 値は入力できません。

  インターフェイステストを開始するまでの時間（y）を計算するには、次のようにします。

  1. x = (*holdtime*/*polltime*)/2、最も近い整数に丸められます。（.4 以下は切り下げ、.5 以上は切り上げ。）
  2. y = x**polltime*

  たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。

ステップ 10 インターフェイスの仮想 MAC アドレスを設定します。

- アクティブ/スタンバイ モードの場合

  failover mac address *phy_if active_mac standby_mac*

例：

```
ciscoasa(config)# failover mac address gigabitethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

- アクティブ/アクティブ モードの場合

  mac address *phy_if active_mac standby_mac*

  例：

```
ciscoasa(config-fover-group)# mac address gigabitethernet0/2 00a0.c969.87c8
00a0.c918.95d8
```

phy_if 引数は、インターフェイスの物理名（gigabitethernet0/1 など）です。

active_mac および *standby_mac* 引数は、H.H.H 形式（H は 16 ビットの 16 進数）の MAC アドレスです。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。

active_mac アドレスはインターフェイスのアクティブ *IP* アドレスに関連付けられ、standby_mac はインターフェイスのスタンバイ IP アドレスに関連付けられます。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

show interface コマンドを使用して、インターフェイスが使用している MAC アドレスを表示します。

ステップ 11 （アクティブ/アクティブ モードのみ）他のフェールオーバー グループについてこの手順を繰り返します。

インターフェイス モニタリングの設定

デフォルトでは、すべての物理インターフェイス、または Firepower 1010 の場合、および Secure Firewall 1210/1220 すべての VLAN インターフェイス インターフェイス モニタリングの場合、Firepower 1010 および Secure Firewall 1210/1220 スイッチポートが対象です。

重要度の低いネットワークに接続されているインターフェイスがフェールオーバー ポリシーに影響を与えないように除外できます。

装置ごとに最大 1025 のインターフェイスをモニターできます（マルチ コンテキスト モードのすべてのコンテキストにわたって）。

始める前に

マルチ コンテキスト モードで、各コンテキスト内のインターフェイスを設定します。

手順

インターフェイスのヘルス モニタリングをイネーブルまたはディゼーブルにします。

[**no**] **monitor-interface** {*if_name*}

例：

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)# no monitor-interface eng1
```

非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）

アクティブ/アクティブ フェールオーバーでの実行中に、ピア装置を経由して開始された接続に対する返送パケットを、装置が受信する場合があります。そのパケットを受信する ASA にはそのパケットの接続情報がないために、パケットはドロップされます。このドロップが多く発生するのは、アクティブ/アクティブ フェールオーバー ペアの 2 台の ASA が異なるサービス プロバイダーに接続されており、アウトバウンド接続に NAT アドレスが使用されていない場合です。

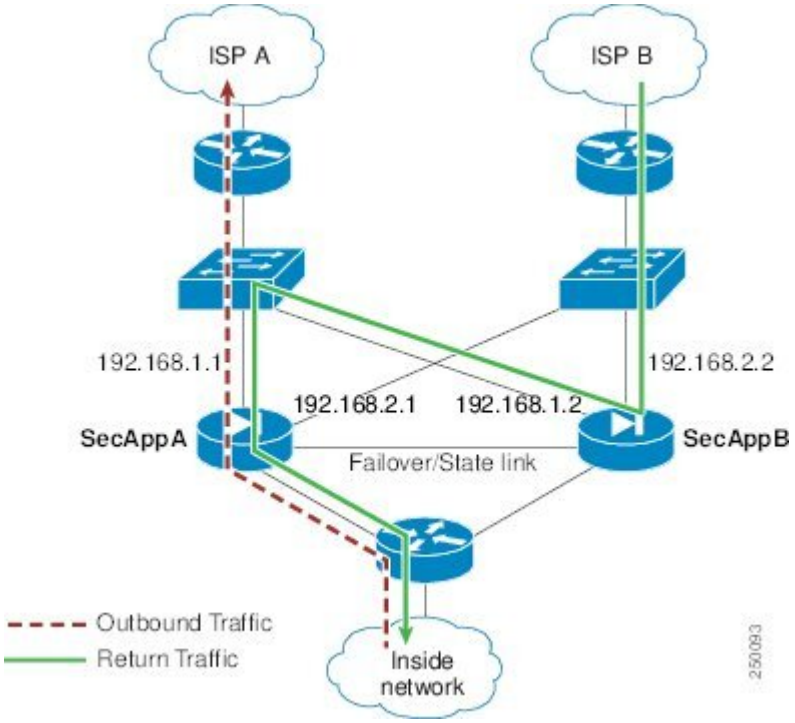
返送パケットのドロップは、非対称にルーティングされたパケットを許可することによって防ぐことができます。そのためには、それぞれの ASA の同様のインターフェイスを同じ ASR グループに割り当てます。たとえば、両方の ASA が、内部インターフェイスでは同じ内部ネットワークに接続している一方、外部インターフェイスでは別の ISP に接続しているとします。プライマリ装置で、アクティブ コンテキストの外部インターフェイスを ASR グループ 1 に割り当て、セカンダリ装置でも、アクティブ コンテキストの外部インターフェイスを同じ ASR グループ 1 に割り当てます。プライマリ装置の外部インターフェイスがセッション情報を持たないパケットを受信すると、同じグループ（この場合 ASR グループ 1）内のスタンバイ コンテキストの他のインターフェイスのセッション情報をチェックします。一致する情報が見つからない場合、パケットはドロップされます。一致する情報が見つかると、次の動作のうちいずれかが開始します。

- 着信トラフィックがピア装置に発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットは他の装置にリダイレクトされます。このリダイレクトは、セッションがアクティブである限り続行されます。
- 着信トラフィックが同じ装置の別のインターフェイスに発信されると、レイヤ 2 ヘッダーの一部またはすべてが書き直され、パケットはストリームに再注入されます。

（注） この機能は、非対称ルーティングを提供しません。非対称にルーティングされたパケットを正しいインターフェイスに戻します。

次の図に、非対称にルーティングされたパケットの例を示します。

図 *48 : ASR* の例



1. アウトバウンド セッションが、アクティブな SecAppA コンテキストを持つ ASA を通過します。このパケットは、インターフェイス外の ISP-A（192.168.1.1）から送信されます。
2. 非対称ルーティングがアップストリームのどこかで設定されているため、リターン トラフィックは、アクティブな SecAppB コンテキストを持つ ASA のインターフェイス外部の ISP-B（192.168.2.2）経由で戻ります。
3. 通常、リターン トラフィックは、そのインターフェイス 192.168.2.2 上にリターン トラフィックに関するセッション情報がないので、ドロップされます。しかし、このインターフェイスは、ASR グループ 1 の一部として設定されています。装置は、同じ ASR グループ ID で設定された他のインターフェイス上のセッションを探します。
4. このセッション情報は、SecAppB を持つ装置上のスタンバイ状態のインターフェイス outsideISP-A（192.168.1.2）にあります。ステートフル フェールオーバーは、SecAppA から SecAppB にセッション情報を複製します。
5. ドロップされる代わりに、レイヤ 2 ヘッダーはインターフェイス 192.168.1.1 の情報で書き直され、トラフィックはインターフェイス 192.168.1.2 からリダイレクトされます。そこか

ら、発信元の装置のインターフェイスを経由して戻ります（SecAppA の 192.168.1.1）。この転送は、必要に応じて、セッションが終了するまで続行されます。

始める前に

- ステートフル フェールオーバー：アクティブ フェールオーバー グループにあるインターフェイスのセッションのステート情報を、スタンバイ フェールオーバー グループに渡します。
- replication http：HTTP セッションのステート情報は、スタンバイ フェールオーバー グループに渡されないため、スタンバイ インターフェイスに存在しません。ASA が非対称にルーティングされた HTTP パケットを再ルーティングできるように、HTTP ステート情報を複製する必要があります。
- プライマリ装置およびセカンダリ装置の各アクティブ コンテキスト内でこの手順を実行します。
- コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキストインターフェイスも ASR グループに含めることはできません。

手順

ステップ 1 プライマリ装置で、非対称にルーティングされたパケットを許可するインターフェイスを指定します。

interface *phy_if*

例：

```
primary/admin(config)# interface gigabitethernet 0/0
```

ステップ 2 インターフェイスの ASR グループ番号を設定します。

asr-group *num*

例：

```
primary/admin(config-ifc)# asr-group 1
```

num 範囲に有効な値は、1 ～ 32 です。

ステップ 3 セカンダリ装置で、非対称にルーティングされたパケットを許可するインターフェイスを指定します。

interface *phy_if*

例：

```
secondary/ctx1(config)# interface gigabitethernet 0/1
```

ステップ 4 インターフェイスの ASR グループ番号をプライマリ装置のインターフェイスに一致するように設定します。

asr-group *num*

例：

```
secondary/ctx1(config-ifc)# asr-group 1
```

例

2 つの装置に次のコンフィギュレーションがあります（コンフィギュレーションは関連するコマンドだけを示します）。図の「SecAppA」というラベルの付いたデバイスは、フェールオーバー ペアのプライマリ装置です。

プライマリ装置のシステム コンフィギュレーション

```
interface GigabitEthernet0/1
  description LAN/STATE Failover Interface
interface GigabitEthernet0/2
  no shutdown
interface GigabitEthernet0/3
  no shutdown
interface GigabitEthernet0/4
  no shutdown
interface GigabitEthernet0/5
  no shutdown
failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/1
failover link folink
failover interface ip folink 10.0.4.1 255.255.255.0 standby 10.0.4.11
failover group 1
  primary
failover group 2
  secondary
admin-context SecAppA
context admin
  allocate-interface GigabitEthernet0/2
  allocate-interface GigabitEthernet0/3
  config-url flash:/admin.cfg
  join-failover-group 1
context SecAppB
  allocate-interface GigabitEthernet0/4
  allocate-interface GigabitEthernet0/5
  config-url flash:/ctx1.cfg
  join-failover-group 2
```

SecAppA コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/2
```

```
  nameif outsideISP-A
  security-level 0
  ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
  asr-group 1
interface GigabitEthernet0/3
  nameif inside
  security-level 100
  ip address 10.1.0.1 255.255.255.0 standby 10.1.0.11
monitor-interface outside
```

SecAppB コンテキスト コンフィギュレーション

```
interface GigabitEthernet0/4
  nameif outsideISP-B
  security-level 0
  ip address 192.168.2.2 255.255.255.0 standby 192.168.2.1
  asr-group 1
interface GigabitEthernet0/5
  nameif inside
  security-level 100
  ip address 10.2.20.1 255.255.255.0 standby 10.2.20.11
```

フェールオーバー の管理

この項では、フェールオーバーの設定を変更する方法、ある装置から別の装置にフェールオーバーを強制実行する方法など、フェールオーバー を有効化した後に フェールオーバー 装置を管理する方法について説明します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 スタンバイ装置で入力した場合、フェールオーバーが強制実行されます。スタンバイ装置はアクティブ装置になります。

group *group_id* を指定する場合は、指定するアクティブ/アクティブ フェールオーバー グループのスタンバイ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。スタンバイ装置はそのフェールオーバー グループのアクティブ装置になります。

- アクティブ/スタンバイ モードのスタンバイ装置の場合

  failover active

- アクティブ/アクティブ モードのスタンバイ装置の場合

  failover active [**group** *group_id*]

  例：

```
standby# failover active group 1
```

ステップ 2 アクティブ装置で入力した場合、フェールオーバーが強制実行されます。アクティブ装置はスタンバイ装置になります。

group *group_id* を指定する場合は、指定するフェールオーバー グループのアクティブ装置でこのコマンドを入力すると、フェールオーバーが強制実行されます。アクティブ装置はそのフェールオーバー グループのスタンバイ装置になります。

- アクティブ/スタンバイ モードのアクティブ装置の場合

  no failover active

- アクティブ/アクティブ モードのアクティブ装置の場合

  no failover active [**group** *group_id*]

  例：

```
active# no failover active group 1
```

フェールオーバーのディセーブル化

1 つまたは両方の装置でフェールオーバーをディセーブルにすると、リロードするまで各装置のアクティブおよびスタンバイ状態が維持されます。アクティブ/アクティブ フェールオーバー ペアの場合、どの装置を優先するように設定されていようと、フェールオーバー グループはアクティブであるすべての装置でアクティブ状態のまま維持されます。

フェールオーバーをディセーブルにする際、次の特性を参照してください。

- スタンバイ装置/コンテキストはスタンバイ モードのまま維持されるので、両方の装置はトラフィックの転送を開始しません（これは疑似スタンバイ状態と呼ばれます）。
- スタンバイ装置/コンテキストは、アクティブ装置/コンテキストに接続されていない場合でもそのスタンバイ IP アドレスを引き続き使用します。
- スタンバイ装置/コンテキストによる、フェールオーバー上における接続に対するリッスンは継続されます。フェールオーバーをアクティブ装置/コンテキストで再度イネーブルにすると、そのコンフィギュレーションの残りが再同期化された後に、スタンバイ装置/コンテキストが通常のスタンバイ状態に戻ります。

- スタンバイ装置で手動でフェールオーバーをイネーブルにしてアクティブ化しないでください。代わりに、フェールオーバーの強制実行（369 ページ）を参照してください。スタンバイ装置でフェールオーバーをイネーブルにすると、MAC アドレスの競合が発生し、IPv6 トラフィックが中断される可能性があります。
- 完全にフェールオーバーをディセーブルにするには、no failover コンフィギュレーションをスタートアップ コンフィギュレーションに保存してからリロードします。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 フェールオーバーをディセーブルにします。

no failover

ステップ 2 完全にフェールオーバーをディセーブルにするには、コンフィギュレーションを保存してをリロードします。

write memory

reload

障害が発生した装置の復元

障害が発生した装置を障害のない状態に復元するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースでこの手順を実行します。

手順

ステップ 1 障害が発生したユニットを障害が発生していない状態に復元します。

- アクティブ/スタンバイ モードの場合

  failover reset

- アクティブ/アクティブ モードの場合

  failover reset [**group** *group_id*]

  例：

```
ciscoasa(config)# failover reset group 1
```

障害が発生した装置を障害のない状態に復元しても、その装置が自動的にアクティブになるわけではありません。復元された装置は、（強制または自然な形での）フェールオーバーによってアクティブになるまではスタンバイ状態のままです。例外は、フェールオーバー グループ（アクティブ/アクティブ モードのみ）にフェールオーバー プリエンプションが設定されている場合です。以前アクティブであったフェールオーバー グループにプリエンプションが設定されており、障害が発生した装置が優先装置の場合、そのフェールオーバー グループはアクティブになります。

group *group_id* を指定した場合、このコマンドは障害が発生したアクティブ/アクティブ フェールオーバー グループを障害のない状態に復元します。

ステップ 2 （アクティブ/アクティブ モードのみ）フェールオーバーをフェールオーバー グループ レベルで復元するには次を行います。

a) システムで、[Monitoring] > [Failover] > [Failover Group #] を開きます。# は、制御するフェールオーバー グループの番号です。

b) [Reset Failover] をクリックします。

コンフィギュレーションの再同期

アクティブ装置に write standby コマンドを入力すると、スタンバイ装置で実行コンフィギュレーションが削除され（アクティブ装置との通信に使用するフェールオーバー コマンドを除く）、アクティブ装置のコンフィギュレーション全体がスタンバイ装置に送信されます。

マルチ コンテキスト モードの場合、システム実行スペースに **write standby** コマンドを入力すると、すべてのコンテキストが複製されます。あるコンテキスト内で **write standby** コマンドを入力すると、コマンドはそのコンテキスト コンフィギュレーションだけを複製します。

複製されたコマンドは、実行コンフィギュレーションに保存されます。

フェールオーバー機能のテスト

フェールオーバー機能をテストするには、次の手順を実行します。

手順

ステップ 1 FTP などを使用して、異なるインターフェイス上のホスト間でファイルを送信し、アクティブ装置が予期したとおりにトラフィックを渡しているかどうかをテストします。

ステップ 2 アクティブ装置で次のコマンドを入力し、フェールオーバーを強制実行します。

アクティブ/スタンバイ モード

ciscoasa(config)# **no failover active**

アクティブ/アクティブ モード

ciscoasa(config)# **no failover active group** *group_id*

ステップ 3 FTP を使用して、2 つの同じホスト間で別のファイルを送信します。

ステップ 4 テストが成功しなかった場合は、**show failover** コマンドを入力してフェールオーバー ステータスを確認します。

ステップ 5 テストが終了したら、新しくアクティブになった装置で次のコマンドを入力すると、装置をアクティブ ステータスに復元できます。

アクティブ/スタンバイ モード

ciscoasa(config)# **no failover active**

アクティブ/アクティブ モード

ciscoasa(config)# **failover active group** *group_id*

（注）
ASA インターフェイスの 1 つがダウンしたとき、フェールオーバーの観点からは、これも装置の問題と見なされます。インターフェイスの 1 つがダウンしていることを ASA が検出した場合は、インターフェイスのホールド時間を待たずに、フェールオーバーがただちに行われます。インターフェイスのホールド時間が有効であるのは、ASA が自身のステータスを OK と見なしているときだけです（ピアから hello パケットを受信していなくても）。インターフェイスのホールド時間をシミュレートするには、ピアが他のピアから hello パケットを受信するのを停止させるために、スイッチ上で VLAN をシャットダウンします。

リモート コマンドの実行

リモート コマンドを実行すると、コマンド ラインに入力されたコマンドを特定のフェールオーバー ピアに送信できます。

コマンドの送信

コンフィギュレーション コマンドはアクティブ装置またはコンテキストからスタンバイ装置またはコンテキストに複製されるため、いずれの装置にログインしているかにかかわらず、**failover exec** コマンドを使用して正しい装置にコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ装置にログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ装置に送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置やコンテキストへの設定コマンドの送信には、**failover exec** コマンドを使用しないでください。これらの設定の変更はアクティブ装置に複製されないため、2 つの設定が同期されなくなります。

configuration、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されるため、 **failover exec** コマンドを使用し、ピア装置で **show** コマンドを発行して、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

手順

ステップ 1 マルチ コンテキスト モードの場合は、**changeto context***name* コマンドを使用して、設定したいコンテキストに変更します。**failover exec** コマンドを使用して、フェールオーバー ピアでコンテキストを変更することはできません。

ステップ 2 次のコマンドを使用して、所定のフェールオーバー装置にコマンドを送信します。

ciscoasa(config)# **failover exec** {**active** | **mate** | **standby**}

active または **standby** キーワードを使用すると、その装置が現在の装置であっても、コマンドは指定された装置で実行されます。**mate** キーワードを使用すると、コマンドはフェールオーバー ピアで実行されます。

コマンドモードを変更するコマンドによって、現在のセッションのプロンプトが変更されることはありません。コマンドが実行されるコマンド モードを表示するには、 **show failover exec** コマンドを使用する必要があります。詳細については、コマンドモードの変更（7-53 ページ）を参照してください。

コマンド モードの変更

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトでは、**failover exec** コマンド モードは、指定されたデバイスのグローバル コンフィギュレーション モードで開始されます。このコマンド モードを変更するには、 **failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。**failover exec** を使用してモードを変更しても、セッション プロンプトは変更されません。

たとえば、フェールオーバーペアのアクティブユニットのグローバル コンフィギュレーション モードにログインし、**failover exec active** コマンドを使用してインターフェイス コンフィギュレーション モードを変更した場合、ターミナルプロンプトはグローバル コンフィギュレーション モードのままですが、**failover exec** を使用して入力されるコマンドは、インターフェイス コンフィギュレーション モードで入力されます。

次の例は、ターミナル セッション モードと **failover exec** コマンド モードの違いを示しています。この例で、管理者はアクティブ装置の **failover exec** モードを、インターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーション モードに変更します。その後、**failover exec active** を使用して入力されたすべてのコマンドがインターフェイス GigabitEthernet0/1 用のインターフェイス コンフィギュレーション モードに送信されます。次に、管理者は failover exec active を使用して、そのインターフェイスに IP アドレスを割り当てます。プロンプトはグローバル コンフィギュレーション モードを示していますが、**failover exec active** モードはインターフェイス コンフィギュレーション モードです。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# failover exec active ip address 192.168.1.1 255.255.255.0 standby
192.168.1.2
ciscoasa(config)# router rip
ciscoasa(config-router)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ装置のインターフェイス コンフィギュレーション モードで、**failover exec** コマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。その結果、デバイスとのセッションはインターフェイス コンフィギュレーション モードのままで、**failover exec active** を使用して入力されたコマンドは、指定されたルーティング プロセスを実行するためルータ コンフィギュレーション モードに送信されます。

```
ciscoasa(config-if)# failover exec active router ospf 100
ciscoasa(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。**show failover exec** コマンドでは、**failover exec** コマンドと同じキーワード、つまり **active**、**mate**、または **standby** が使用されます。各デバイスの **failover exec** モードは個別に追跡されます。

次に、スタンバイ装置に入力された **show failover exec** コマンドの出力例を示します。

```
ciscoasa(config)# failover exec active interface GigabitEthernet0/1
ciscoasa(config)# sh failover exec active
Active unit Failover EXEC is at interface sub-command mode

ciscoasa(config)# sh failover exec standby
Standby unit Failover EXEC is at config mode

ciscoasa(config)# sh failover exec mate
Active unit Failover EXEC is at interface sub-command mode
```

セキュリティに関する考慮事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防ぐためには、フェールオーバー リンクの暗号化をイネーブルにする必要があります。

リモート コマンドの実行に関する制限事項

リモートコマンドの使用には、次の制限事項があります。

- ゼロダウンタイム アップグレード手順を使用して1台の装置だけをアップグレードする場合は、 **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。

- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしている装置でそのコンテキストに変更する必要があります。
- 次のコマンドを **failover exec** コマンドと一緒に使用することはできません。
  - **changeto**
  - **debug (undebug)**
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。
- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** の出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア装置で **failover exec** を使用してコンフィギュレーション コマンドを入力した場合、現在の装置でグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** コマンドのような、再帰的な failover exec コマンドは入力できません。
- ユーザーの入力または確認が必要なコマンドでは、**noconfirm** オプションを使用する必要があります。たとえば、mate をリロードするには、次を入力します。

  failover exec mate reload noconfirm

フェールオーバーのモニタリング

このセクションの手順に従うことで、フェールオーバーのステータスをモニターできます。

フェールオーバー メッセージ

フェールオーバーが発生すると、両方の ASA がシステム メッセージを送信します。

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、syslog メッセージ ガイドを参照してください。フェールオーバーに関連付けられているメッセージ ID の範囲は次のとおりです：101xxx、102xxx、103xxx、104xxx、105xxx、210xxx、311xxx、709xxx、727xxx。たとえば、105032 および 105043 はフェールオーバー リンクとの問題を示しています。

（注） フェールオーバーの最中に、ASAは論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージ 411001 および 411002 を生成します。これは通常のアクティビティです。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステムパフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

フェールオーバー ステータスのモニタリング

フェールオーバー ステータスをモニターするには、次のいずれかのコマンドを入力します。

- **show failover**

  装置のフェールオーバー状態についての情報を表示します。

- **show failover group**

  装置のフェールオーバー状態に関する情報を表示します。表示される情報は、**show failover** コマンドの場合と似ていますが、指定されたグループに対象が限定されます。

- **show monitor-interface**

  モニター対象インターフェイスの情報を表示します。

- **show running-config failover**

  実行コンフィギュレーション内のフェールオーバー コマンドを表示します。

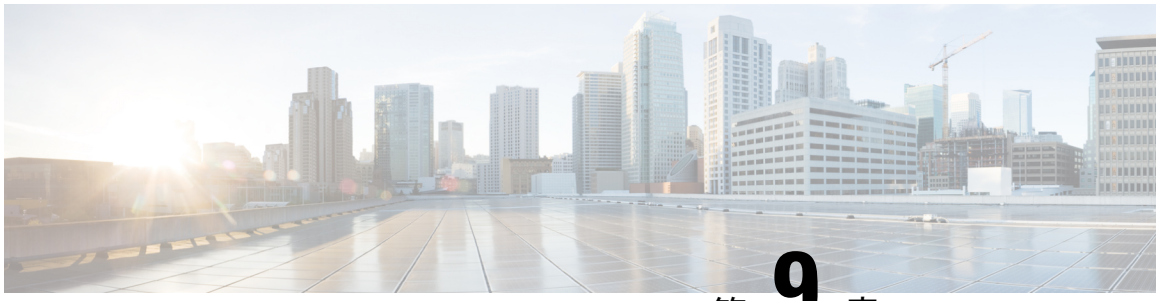
フェールオーバーの履歴

機能名	リリース	機能情報
アクティブ/スタンバイ フェールオーバー	7.0(1)	この機能が導入されました。
アクティブ/アクティブ フェールオーバー	7.0(1)	この機能が導入されました。
フェールオーバー キーの 16 進数値サポート	7.0(4)	フェールオーバー リンクの暗号化用に 16 進数値が指定できるようになりました。 **failover key hex** コマンドが変更されました。
フェールオーバー キーのマスターパスフレーズのサポート	8.3(1)	フェールオーバー キーが、実行コンフィギュレーションとスタートアップ コンフィギュレーションの共有キーを暗号化するマスターパスフレーズをサポートするようになりました。一方の ASA から他方に共有秘密をコピーする場合、たとえば、**more system:running-config** コマンドを使用して、正常に暗号化共有キーをコピーして貼り付けることができます。 （注） **failover key** の共有秘密は、**show running-config** の出力に ***** と表示されます。このマスクされたキーはコピーできません。 **failover key** [**0** | **8**] コマンドが変更されました。
フェールオーバーに IPv6 のサポートが追加	8.2(2)	次のコマンドが変更されました。**failover interface ip**、**show failover**、**ipv6 address**、**show monitor-interface**
「同時」ブートアップ中のフェールオーバー グループのユニットの設定の変更	9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。

機能名	リリース	機能情報
フェールオーバー リンクおよびステート リンクの通信を暗号化する IPsec LAN-to-LAN トンネルのサポート	9.1(2)	フェールオーバー キーに独自の暗号化を使用する代わりに（**failover key** コマンド）、フェールオーバー リンクおよびステート リンクの暗号化に IPsec LAN-to-LAN トンネルが使用できるようになりました。 （注） フェールオーバー LAN-to-LAN トンネルは、IPsec（その他の VPN）ライセンスには適用されません。 **failover ipsec pre-shared-key**、**show vpn-sessiondb** の各コマンドが導入または変更されました。
ハードウェア モジュールのヘルス モニタリングの無効化	9.3(1)	ASA はデフォルトで、インストール済みハードウェア モジュール（ASA FirePOWER モジュールなど）のヘルス モニタリングを行います。特定のハードウェア モジュールの障害によってフェールオーバーをトリガーすることが望ましくない場合は、モジュールのモニタリングをディセーブルにできます。 **monitor-interface service-module** コマンドが変更されました。
フェールオーバー ペアのスタンバイ装置またはスタンバイ コンテキストのコンフィギュレーション変更のロック	9.3(2)	通常のコンフィギュレーションの同期を除いてスタンバイ装置上で変更ができないように、スタンバイ装置（アクティブ/スタンバイ フェールオーバー）またはスタンバイ コンテキスト（アクティブ/アクティブ フェールオーバー）のコンフィギュレーション変更をロックできるようになりました。 **failover standby config-lock** コマンドが導入されました。
ASA 5506H のフェールオーバー リンクとして、管理 1/1 インターフェイスを使用可能	9.5(1)	管理 1/1 インターフェイスは、ASA 5506H に限りフェールオーバー リンクとして設定できるようになりました。この機能により、デバイスの他のインターフェイスをデータ インターフェイスとして使用できます。この機能を使用した場合、ASA FirePOWER モジュールは使用できません。このモジュールでは管理 1/1 インターフェイスを通常の管理インターフェイスとして維持することが必須です。 次のコマンドが変更されました。**failover lan interface**、**failover link**

機能名	リリース	機能情報
キャリアグレードNATの強化がフェールオーバーおよびASAクラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよびASAクラスタの導入でサポートされます。 次のコマンドが変更されました。**show local-host**
アクティブ/スタンバイフェールオーバーを使用するときの セキュアクライアント からのダイナミック ACL における同期時間の改善	9.6(2)	フェールオーバーペアで セキュアクライアント を使用するとき、関連付けられているダイナミック ACL（dACL）におけるスタンバイユニットへの同期時間が改善されました。以前は、大規模な dACL の場合、スタンバイユニットが可用性の高いバックアップを提供するのではなく同期作業で忙しい間は、同期時間が長時間に及ぶことがありました。 変更されたコマンドはありません。
マルチコンテキストモードのセキュアクライアント接続のステートフルフェールオーバー	9.6(2)	マルチコンテキストモードで セキュアクライアント 接続のステートフルフェールオーバーがサポートされるようになりました。 変更されたコマンドはありません。
より迅速に検出を行うためのインターフェイスのリンクステートモニタリングを設定可能	9.7(1)	デフォルトでは、フェールオーバーペアのASAは、500 ミリ秒ごとにインターフェイスのリンク ステートをチェックします。ポーリングの間隔を 300 ミリ秒から 799 ミリ秒の間で設定できるようになりました。たとえば、ポーリング時間を300ミリ秒に設定すると、ASAはインターフェイス障害やトリガーのフェールオーバーをより迅速に検出できます。 次のコマンドが導入されました。**failover polltime link-state**
FirePOWER 9300および4100でのアクティブ/スタンバイ フェールオーバー ヘルス モニタリングで、双方向フォワーディング検出（BFD）がサポートされました。	9.7(1)	FirePOWER 9300および4100上のアクティブ/スタンバイペアの 2 つのユニット間のフェールオーバー ヘルス チェックに対して、双方向フォワーディング検出（BFD）を有効にできるようになりました。ヘルス チェックにBFDを使用すると、デフォルトのヘルスチェックより信頼性が高まり、CPU の使用を抑えることができます。 次のコマンドが導入されました。**failover health-check bfd**

機能名	リリース	機能情報
フェールオーバー遅延の無効化	9.15(1)	ブリッジグループまたは IPv6 DAD を使用する場合、フェールオーバーが発生すると、新しいアクティブユニットは、スタンバイユニットがネットワーキングタスクを完了してスタンバイ状態に移行するまで、最大3000ミリ秒待機します。その後、アクティブユニットはトラフィックの受け渡しを開始できます。この遅延を回避するために、待機時間を無効にすると、スタンバイユニットが移行する前にアクティブユニットがトラフィックの受け渡しを開始します。 新規/変更されたコマンド： **failover wait-disable**
HA ピアリングを高速化する設定同期最適化機能	9.18(1)	設定同期最適化機能により、config-hash 値を交換して参加ユニットとアクティブユニットの設定を比較できます。アクティブユニットと参加ユニットの両方で計算されたハッシュが一致する場合、参加ユニットは完全な設定同期をスキップして HA に再参加します。この機能により、さらに迅速な HA ピアリングが可能になり、メンテナンスウィンドウとアップグレード時間が短縮されます。
ハートビートモジュールの冗長性	9.20(1)	ASA 高可用性のデータプレーンに追加のハートビートモジュールが導入されました。このハートビートモジュールは、コントロールプレーンのトラフィックの輻輳や CPU の過負荷が原因で発生する可能性のある、偽フェールオーバーやスプリットブレインシナリオを回避するのに役立ちます。



第 9 章

パブリック クラウドでのハイ アベイラビリティのためのフェールオーバー

この章では、Microsoft Azure などのパブリッククラウド環境で ASA 仮想 のハイアベイラビリティを実現できるようにアクティブ/バックアップ フェールオーバーを設定する方法について説明します。

- パブリック クラウドでのフェールオーバーについて （383 ページ）
- パブリック クラウドでのフェールオーバーのライセンス （389 ページ）
- パブリック クラウドでのフェールオーバーのデフォルト （389 ページ）
- Microsoft Azure での ASA 仮想 ハイアベイラビリティについて （390 ページ）
- アクティブ/バックアップ フェールオーバーの設定 （393 ページ）
- オプションのフェールオーバー パラメータの設定 （395 ページ）
- アクティブ/バックアップ フェールオーバーの有効化 （400 ページ）
- パブリック クラウドでのフェールオーバーの管理 （403 ページ）
- パブリック クラウドでのフェールオーバーのモニター （405 ページ）
- パブリック クラウドでのフェールオーバーの履歴 （406 ページ）

パブリック クラウドでのフェールオーバーについて

冗長性を確保するために、ASA 仮想 をアクティブ/バックアップ ハイ アベイラビリティ（HA）設定でパブリッククラウド環境に展開します。パブリッククラウドでの HA では、アクティブな ASA 仮想 の障害時に、バックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーできるステートレスなアクティブ/バックアップソリューションが実装されます。

次のリストは、HA パブリック クラウド ソリューションの主要コンポーネントを示しています。

- **アクティブ ASA 仮想**：HA ピアのファイアウォール トラフィックを処理するように設定された HA ペア内の ASA 仮想。
- **バックアップ ASA 仮想**：ファイアウォール トラフィックを処理せず、アクティブ ASA 仮想 に障害が発生した場合にアクティブ ASA 仮想 を引き継ぐ HA ペア内の ASA 仮想。こ

れは、フェールオーバーの際にピアの識別情報を引き継がないため、スタンバイではなくバックアップと呼ばれます。

- **HA エージェント**：ASA 仮想 上で実行され、ASA 仮想 の HA ロール（アクティブ/バックアップ）を判断し、その HA ピアの障害を検出し、その HA ロールに基づいてアクションを実行する軽量プロセス。

物理 ASA および非パブリック クラウドの仮想 ASA では、Gratuitous ARP 要求を使用してフェールオーバー条件を処理しますが、バックアップ ASA は、アクティブな IP アドレスと MAC アドレスに関連付けられていることを示す Gratuitous ARPP を送信します。ほとんどのパブリック クラウド環境では、このようなブロードキャスト トラフィックは許可されていません。このため、パブリック クラウドの HA 設定では、フェールオーバーが発生したときに通信中の接続を再起動する必要があります。

アクティブ装置の状態がバックアップ装置によってモニタされ、所定のフェールオーバー条件に一致しているかどうかが判別されます。所定の条件に一致すると、フェールオーバーが行われます。フェールオーバー時間は、パブリック クラウド インフラストラクチャの応答性に応じて、数秒～ 1 分を超える場合があります。

アクティブ/バックアップ フェールオーバーについて

アクティブ/バックアップ フェールオーバーでは、1 台の装置がアクティブ装置です。この装置がトラフィックを渡します。バックアップ装置は積極的にトラフィックを渡したり、アクティブ装置と設定情報を交換したりしません。アクティブ/バックアップ フェールオーバーでは、障害が発生した装置の機能をバックアップ ASA 仮想デバイスに引き継ぐことができます。アクティブ装置が故障すると、バックアップ状態に変わり、そしてバックアップ装置がアクティブ状態に変わります。

プライマリ/セカンダリの役割とアクティブ/バックアップ ステータス

アクティブ/バックアップ フェールオーバーを設定する場合、1 つの装置をプライマリとして設定し、もう 1 つの装置をセカンダリとして設定します。この時点で、2 つの装置は、デバイスとポリシーの設定、およびイベント、ダッシュボード、レポート、ヘルス モニタリングで、2 つの個別のデバイスとして機能します。

フェールオーバー ペアの 2 つの装置の主な相違点は、どちらの装置がアクティブでどちらの装置がバックアップであるか、つまりどちらの装置がアクティブにトラフィックを渡すかということに関連します。両方の装置がトラフィックを渡すことができますが、プライマリ装置だけがロード バランサ プローブに応答し、構成済みのルートをプログラミングしてルートの接続先として使用します。バックアップ装置の主な機能は、プライマリ装置の正常性を監視することです。両方の装置が同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、プライマリ装置が常にアクティブ装置になります。

フェールオーバー接続

バックアップ ASA 仮想 は、TCP を介して確立されたフェールオーバー接続を使用して、アクティブ ASA 仮想 の正常性を監視します。

- アクティブ ASA 仮想 は、リッスンポートを開くことで接続サーバーとして機能します。
- バックアップ ASA 仮想 は、接続ポートを使用してアクティブ ASA 仮想 に接続します。
- 通常、ASA 仮想 装置間で何らかのネットワークアドレス変換が必要な場合を除き、リッスンポートと接続ポートは同じです。

フェールオーバー接続の状態によって、アクティブASA仮想の障害を検出します。バックアップASA仮想は、フェールオーバー接続が切断されたことを確認すると、アクティブASA仮想で障害が発生したと判断します。同様に、バックアップ ASA 仮想 がアクティブ装置に送信されたキープアライブメッセージに対する応答を受信しない場合も、アクティブ ASA 仮想 で障害が発生したと判断します。

関連項目

ポーリングと Hello メッセージ

バックアップ ASA 仮想 はフェールオーバー接続を介してアクティブ ASA 仮想 に Hello メッセージを送信し、Hello 応答の返信を期待します。メッセージのタイミングには、ポーリング間隔、つまりバックアップ ASA 仮想 装置が Hello 応答を受信して次の Hello メッセージが送信されるまでの間の時間間隔が使用されます。応答の受信は、ホールド時間と呼ばれる受信タイムアウトによって強制されます。Hello 応答の受信がタイムアウトすると、アクティブ ASA 仮想 で障害が発生したとみなされます。

ポーリング間隔とホールド時間間隔は設定可能なパラメータです（フェールオーバー基準とその他の設定の構成 （395 ページ） を参照）。

起動時のアクティブ装置の判別

アクティブ装置は、次の条件で判別されます。

- 装置がブートされ、ピアがすでにアクティブとして動作中であることを検出すると、その装置はバックアップ装置になります。
- 装置がブートされてピアを検出できないと、その装置はアクティブ装置になります。
- 両方の装置が同時に起動された場合は、プライマリ装置がアクティブ装置になり、セカンダリ装置がバックアップ装置になります。

フェールオーバー イベント

アクティブ/バックアップ フェールオーバーでは、フェールオーバーがユニットごとに行われます。次の表に、各障害イベントに対するフェールオーバーアクションを示します。この表には、各フェールオーバー イベントに対して、フェールオーバー ポリシー（フェールオーバーまたはフェールオーバーなし）、アクティブ装置が行うアクション、バックアップ装置が行うアクション、およびフェールオーバー条件とアクションに関する特別な注意事項を示します。

表 *17*: フェールオーバー イベント

障害イベント	ポリシー	アクティブアクション	バックアップアクション	注
バックアップ装置がフェールオーバー接続のクローズを確認	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする	これは標準のフェールオーバーの使用例です。
アクティブ装置がフェールオーバー接続のクローズを確認	フェールオーバーなし	バックアップを障害としてマークする	n/a	非アクティブ装置へのフェールオーバーは発生しません。
アクティブ装置がフェールオーバーリンクで TCP タイムアウトを確認	フェールオーバーなし	バックアップを障害としてマークする	動作なし	アクティブ装置がバックアップ装置から応答を受信しない場合、フェールオーバーは発生しません。
バックアップ装置がフェールオーバー リンクで TCP タイムアウトを確認	フェールオーバー	該当なし	アクティブになる アクティブを障害としてマークする アクティブ装置にフェールオーバー コマンドの送信を試行する	バックアップ装置はアクティブ装置が動作を続行できないと見なし、引き継ぎます。 アクティブ装置がまだ起動しているが時間内に応答を送信できない場合、バックアップ装置はフェールオーバー コマンドをアクティブ装置に送信します。

障害イベント	ポリシー	アクティブアクション	バックアップアクション	注
アクティブ認証の失敗	フェールオーバーなし	なし	なし	バックアップ装置はルートテーブルを変更するため、バックアップ装置が Azure に認証する必要がある唯一の装置になります。 アクティブ装置が Azure に認証されているかどうかは関係ありません。
バックアップ認証の失敗	フェールオーバーなし	バックアップを未認証としてマークする	動作なし	バックアップ装置が Azure に認証されていない場合、フェールオーバーは発生しません。
アクティブ装置が意図的なフェールオーバーを開始	フェールオーバー	バックアップになる	アクティブになる	アクティブ装置は、フェールオーバー リンク接続を閉じることでフェールオーバーを開始します。 バックアップ装置は接続のクローズを確認し、アクティブ装置になります。
バックアップ装置が意図的なフェールオーバーを開始	フェールオーバー	バックアップになる	アクティブになる	バックアップ装置は、フェールオーバー メッセージをアクティブ装置に送信することによってフェールオーバーを開始します。 アクティブ装置はメッセージを確認すると、接続を閉じてバックアップ装置になります。 バックアップ装置は接続のクローズを確認し、アクティブ装置になります。
以前にアクティブだったユニットが復旧	フェールオーバーなし	バックアップになる	片方をバックアップとマークする	フェールオーバーは確実に必要でない限り発生しません。
アクティブ装置がバックアップ装置からのフェールオーバー メッセージを確認する	フェールオーバー	バックアップになる	アクティブになる	ユーザーが手動フェールオーバーを開始した場合に発生する可能性があります。または、バックアップ装置が TCP タイムアウトを確認したが、アクティブ装置がバックアップ装置からメッセージを受信できる場合に発生する可能性があります。

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

パブリッククラウドでハイアベイラビリティを実現するための ASA 仮想 のフェールオーバー

冗長性を確保するために、ASA 仮想をアクティブ/バックアップ ハイ アベイラビリティ（HA）設定でパブリッククラウド環境に展開します。

- Microsoft Azure パブリッククラウドでのみサポートされています。ASA 仮想 VM を設定する場合、サポートされる vCPU の最大数は 8、サポートされる最大メモリ容量は 64GB RAM です。サポートされるインスタンスの包括的なリストについては、『ASA 仮想 Getting Started Guide』を参照してください。
- アクティブ ASA 仮想 で障害が発生したときにバックアップ ASA 仮想 へのシステムの自動フェールオーバーをトリガーできる、ステートレスなアクティブ/バックアップ ソリューションを実装します。

制限事項

- フェールオーバーはミリ秒ではなく、秒単位で行われます。
- HA の役割の決定と HA 装置として参加できるかどうかは、HA ピア間、および HA 装置と Azure インフラストラクチャとの間の TCP 接続に依存します。ASA 仮想 が HA 装置として参加できない状況がいくつかあります。
  - HA ピアへのフェールオーバー接続を確立できない。
  - Azure から認証トークンを取得できない。
  - Azure で認証できない。
- アクティブ装置からバックアップ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。
- フェールオーバー ルートテーブルの制限

  パブリッククラウドの HA のルートテーブルには次の制限があります。
  - 設定できるルートテーブルの数は最大 16 個です。
  - ルートテーブルで設定できるルートの数は最大 64 個です。

  いずれの場合も、制限に達すると、ルートテーブルまたはルートを削除して再試行することを推奨するアラートが表示されます。
- ASDM サポートはありません。
- IPSec リモート アクセス VPN はサポートされていません。

（注） パブリック クラウドでサポートされる VPN トポロジについては、『Cisco Adaptive Security Virtual Appliance (ASAv) Quick Start Guide』を参照してください。

- ASA 仮想 の VM インスタンスは、同じ可用性セットにある必要があります。Azure の現在の ASA 仮想 ユーザーである場合、既存の展開から HA にアップグレードすることはできません。インスタンスを削除し、Azure マーケットプレイスから ASA 仮想 4 NIC HA オファリングを展開する必要があります。

パブリック クラウドでのフェールオーバーのライセンス

ASA 仮想 はシスコ スマート ソフトウェア ライセンシングを使用しています。スマート ライセンスは、通常の操作に必要です。各 ASA 仮想 は、ASA 仮想 プラットフォームライセンスを使用して個別にライセンスを取得する必要があります。ライセンスをインストールするまで、スループットは 100 Kbps に制限されるため、予備接続テストを実行できます。ASA 仮想 の正確なライセンス要件については、『Cisco ASA シリーズの機能ライセンス』ページを参照してください。

パブリック クラウドでのフェールオーバーのデフォルト

デフォルトでは、フェールオーバー ポリシーは次の事項が含まれます。

- ステートレスなフェールオーバーのみ。
- フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。
- フェールオーバーの TCP 制御ポート番号は 44442 です。
- Azure ロード バランサの健全性プローブ ポート番号は 44441 です。
- 装置のポーリング時間は 5 秒です。
- 装置のホールド時間は 15 秒です。
- ASA 仮想 はプライマリインターフェイス（管理 0/0）のヘルスプローブに応答します。
- Azure サービスプリンシパルによる ASA 仮想 の認証は、プライマリインターフェイス（管理 0/0）で実行されます。

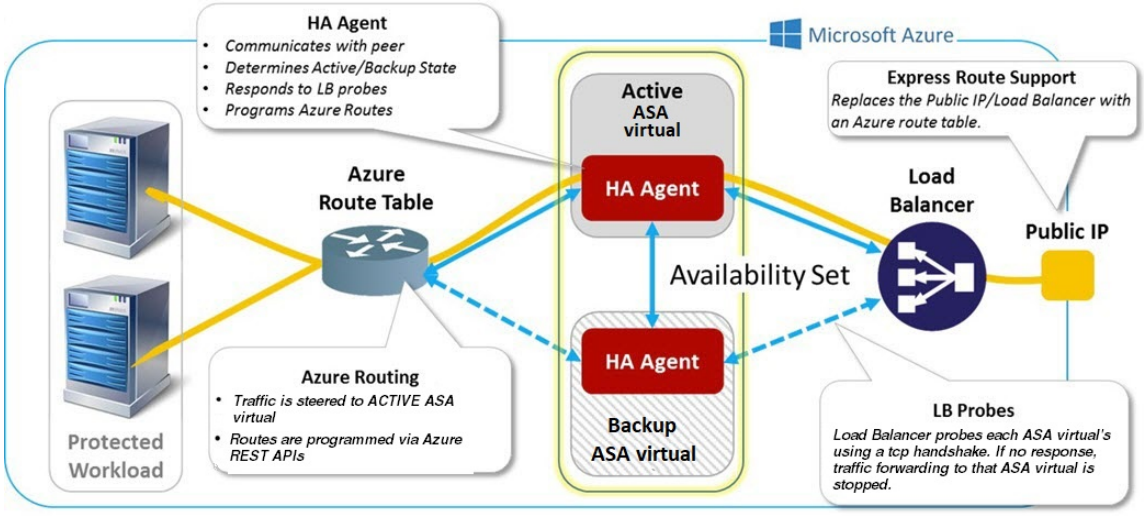
（注） フェールオーバーポート番号、ヘルスプローブポート番号、ポーリング時間、およびプライマリインターフェイスを変更するオプションについては、オプションのフェールオーバー パラメータの設定 （395 ページ）を参照してください。

Microsoft Azure での ASA 仮想 ハイアベイラビリティについて

次の図に、Azure での ASA 仮想 HA 展開の概要を示します。アクティブ/バックアップ フェールオーバー設定の 2 つの ASA 仮想 インスタンスの背後でワークロードが保護されます。Azure ロードバランサは、3 ウェイ TCP ハンドシェイクを使用して両方の ASA 仮想 ユニットをプローブします。アクティブ ASA 仮想 は、3 ウェイハンドシェイクを完了して正常であることを示しますが、バックアップ ASA 仮想 は意図的に応答しません。ロードバランサに応答しないことで、バックアップ ASA 仮想はロードバランサには正常ではないように見え、トラフィックが送信されません。

フェールオーバーでは、アクティブ ASA 仮想 がロードバランサプローブへの応答を停止し、バックアップ ASA 仮想 が応答を開始することで、すべての新しい接続がバックアップ ASA 仮想 に送信されます。バックアップ ASA 仮想 は、ルートテーブルを変更してトラフィックがアクティブユニットからバックアップユニットにリダイレクトされるように API 要求を Azure ファブリックに送信します。この時点で、バックアップ ASA 仮想 がアクティブユニットになり、アクティブユニットは、フェールオーバーの理由に応じてバックアップユニットになるかオフラインになります。

図 *49 : Azure* での *ASA* 仮想 *HA* 展開



自動的に API 呼び出しによって Azure ルートテーブルが変更されるようにするには、ASA 仮想 HA ユニットに Azure Active Directory のログイン情報が必要です。Azure は、簡単に言えば

サービス アカウントであるサービス プリンシパルの概念を採用しています。サービス プリンシパルを使用すると、あらかじめ定義されたAzureリソースセット内でタスクを実行するのに十分な権限と範囲のみを持つアカウントをプロビジョニングできます。

ASA 仮想 HA 展開でサービスプリンシパルを使用して Azure サブスクリプションを管理できるようにするには、次の 2 つの手順を実行します。

1. Azure Active Directory アプリケーションとサービス プリンシパルを作成します（Azure サービス プリンシパルについて （391 ページ） を参照）。
2. サービスプリンシパルを使用して Azure で認証するように ASA 仮想 インスタンスを設定します（「Azure サービス プリンシパル用の認証クレデンシャルの設定 （397 ページ）」を参照）。

関連項目

ロード バランサの詳細については、Azure のマニュアルを参照してください。

Azure サービス プリンシパルについて

Azure リソース（ルート テーブルなど）へのアクセスまたはリソースの変更が必要となるアプリケーションがある場合は、Azure Active Directory（AD）アプリケーションを設定し、必要な権限を割り当てる必要があります。この方法は、以下の理由から、自分のクレデンシャルでアプリケーションを実行するよりも推奨されます。

- 自分の権限とは異なる権限をアプリケーション ID に割り当てることができる。通常、割り当てる権限は、アプリケーションが実行する必要があるものだけに制限します。
- 職責が変わった場合でも、アプリケーションのクレデンシャルを変更する必要がない。
- 無人スクリプトの実行時に、証明書を使用して認証を自動化できる。

Azure ポータルに Azure AD アプリケーションを登録すると、アプリケーション オブジェクトとサービス プリンシパル オブジェクトの 2 つのオブジェクトが Azure AD テナントに作成されます。

- **アプリケーション オブジェクト**：Azure AD アプリケーションは、そのアプリケーションが登録されている Azure AD テナント（アプリケーションの「ホーム」テナント）にある唯一のアプリケーション オブジェクトによって定義されます。
- **サービス プリンシパル オブジェクト**：サービス プリンシパル オブジェクトは、特定のテナントでのアプリケーションの使用に関するポリシーと権限を定義し、アプリケーション実行時のセキュリティ プリンシパルの基礎を提供します。

Azure は、『*Azure Resource Manager Documentation*』で Azure AD アプリケーションとサービス プリンシパルを作成する方法について説明しています。詳しい手順については、次のトピックを参照してください。

- リソースにアクセスできる Azure AD アプリケーションとサービス プリンシパルをポータルで作成する

- Azure PowerShell を使用して資格情報でのサービス プリンシパルを作成する

（注） サービス プリンシパルを設定したら、**ディレクトリ ID**、**アプリケーション ID**、および**秘密鍵**を取得します。これらは、Azure 認証クレデンシャルを設定するために必要です（Azure サービス プリンシパル用の認証クレデンシャルの設定 （397 ページ） を参照）。

Azure での ASA 仮想 ハイアベイラビリティの設定要件

#unique_418 unique_418_Connect_42_fig_cgx_dlh_h1b で説明しているのと同じ設定を導入するには、以下が必要です。

- 次の Azure 認証情報（Azure サービス プリンシパルについて （391 ページ） を参照）
  - ディレクトリ ID
  - Application ID
  - 秘密鍵
- 次の Azure ルート情報（Azure ルート テーブルの設定 （399 ページ） を参照）。
  - Azure サブスクリプション ID
  - ルート テーブル リソース グループ
  - テーブル名
  - アドレス プレフィックス
  - ネクスト ホップ アドレス。
- 次の ASA 設定（アクティブ/バックアップ フェールオーバーの設定 （393 ページ）、パブリック クラウドでのフェールオーバーのデフォルト （389 ページ） を参照）
  - アクティブ/バックアップ IP アドレス
  - HA エージェント通信ポート
  - ロード バランサのプローブ ポート
  - ポーリング間隔

（注） プライマリ装置とセカンダリ装置の両方で基本のフェールオーバー設定を構成します。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

アクティブ/バックアップ フェールオーバーの設定

アクティブ/バックアップ フェールオーバーを設定するには、プライマリ装置とセカンデリ装置の両方で基本的なフェールオーバー設定を構成します。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバー トラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

始める前に

- Azure 可用性セットで ASA 仮想 HA ペアを展開します。
- Azure サブスクリプション ID とサービス プリンシパルの Azure 認証クレデンシャルを含む、Azure 環境情報を入手します。

アクティブ/バックアップ フェールオーバーのプライマリ装置の設定

この項の手順に従って、アクティブ/バックアップ フェールオーバー構成のプライマリを設定します。この手順では、プライマリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。

例

次の例に、プライマリ/アクティブ装置のフェールオーバー パラメータを設定する方法を示します。

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.5 port 4444
ciscoasa(config)#
```

ここで入力するピア IP アドレスは、ASA 仮想 HA ピア上の管理インターフェイスの IP アドレスである必要があります。

次のタスク

必要に応じて、追加のパラメータを設定します。

- バックアップ装置の設定（アクティブ/バックアップ フェールオーバーのセカンダリ装置の設定 （394 ページ） を参照）。
- Azure認証の設定（Azureサービス プリンシパル用の認証クレデンシャルの設定 （397ページ） を参照）。
- Azure ルート情報の設定（Azure ルート テーブルの設定 （399 ページ） を参照）。

- 追加パラメータの確認（フェールオーバー基準とその他の設定の構成（395ページ）を参照）。

アクティブ/バックアップ フェールオーバーのセカンダリ装置の設定

この項の手順に従って、アクティブ/バックアップ フェールオーバー構成でセカンダリ装置を設定します。この手順では、セカンダリ装置でフェールオーバーをイネーブルにするために必要な最小のコンフィギュレーションが用意されています。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。

手順

ステップ 1 この装置をバックアップ装置に指定します。

failover cloud unit secondary

ステップ 2 アクティブ IP アドレスをフェールオーバー リンクに割り当てます。

failover cloud peer ip *ip-address* [**port** *port-number*]

この IP アドレスは、HA ピアへの TCP フェールオーバー制御接続を確立するために使用されます。このポートは、すでにアクティブ装置である可能性がある HA ピアへのフェールオーバー接続を開こうとするときに使用されます。NAT が HA ピア間に配置されている場合は、ここでポートを設定する必要がある場合があります。ほとんどの場合は、ポートを設定する必要はありません。

ここで入力するピア IP アドレスは、ASA 仮想 HA ピア上の管理インターフェイスの IP アドレスである必要があります。

例

次の例に、セカンダリ/バックアップ装置のフェールオーバー パラメータを設定する方法を示します。

```
failover cloud unit secondary
failover cloud peer ip 10.4.3.4 port 4444
```

次のタスク

必要に応じて、追加のパラメータを設定します。

- Azure認証の設定（Azureサービス プリンシパル用の認証クレデンシャルの設定 （397ページ） を参照）。
- Azure ルート情報の設定（Azure ルート テーブルの設定 （399 ページ） を参照）。
- 追加パラメータの確認（フェールオーバー基準とその他の設定の構成 （395ページ） を参照）。

オプションのフェールオーバー パラメータの設定

必要に応じてフェールオーバー設定をカスタマイズできます。

フェールオーバー基準とその他の設定の構成

この項で変更可能な多くのパラメータのデフォルト設定については、パブリック クラウドでのフェールオーバーのデフォルト （389 ページ）を参照してください。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。
- プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

手順

ステップ 1 HA ピアとの通信に使用する TCP ポートを指定します。

failover cloud port control *port-number*

例：

```
ciscoasa(config)# failover cloud port control 4444
```

port-number 引数は、ピアツーピア通信に使用される TCP ポートの番号を割り当てます。

これにより、アクティブ装置のロール状態にあるときに接続を受け入れるフェールオーバー接続 TCP ポートが設定されます。これは、バックアップ ASA 仮想 が接続するアクティブ ASA 仮想 で開かれたポートです。

（注）
両方の HA ピアのデフォルト値である 44442 を維持することをお勧めします。一方の HA ピアのデフォルト値を変更する場合は、もう一方の HA 装置にも同じ変更を加えることをお勧めします。

ステップ 2 装置のポーリング時間およびホールド時間を変更します。

failover polltime *poll_time* [**holdtime** *time*]

例：

```
ciscoasa(config)# failover polltime 10 holdtime 30
```

polltime の範囲は 1 ～ 15 秒です。hello パケットを受信できなかったときから装置が失敗としてマークされるまでの時間が、保持時間によって決まります。**holdtime** の範囲は 3 ～ 60 秒です。装置のポーリング時間の 3 倍に満たない保持時間は入力できません。ポーリング間隔を短くすると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。

ステップ 3 Azure ロード バランサの健全性プローブに使用される TCP ポートを指定します。

failover cloud port probe *port-number*

例：

```
ciscoasa(config)# failover cloud port probe 4443
```

展開で Azure ロードバランサが使用されている場合、着信接続がアクティブ装置に送信されるように、アクティブ ASA 仮想 はロードバランサからの TCP プローブに応答する必要があります。

ステップ 4 Azure Load Balancer 正常性プローブのセカンダリインターフェイスを指定します。

failover cloud port probe *port-number* **interface** *if-name*

例：

```
ciscoasa(config)# failover cloud port probe 4443 interface inside
```

クラウド HA で使用される TCP プローブの送信元 IP アドレス 168.63.129.16 です。このアドレスは、Azure の仮想パブリック IP アドレスです。このアドレスは、Azure DHCP パケットの送信元アドレスであり、Azure の DNS ネームサーバのアドレスです。

デフォルトでは、ASA 仮想 は、ASA ルートテーブルに従って、168.63.129.16 に到達可能なプローブに応答します。デフォルトルートが存在するため、最終的にプライマリインターフェイス（Management0/0）になります。

Management0/0 以外のインターフェイスでロードバランサをサポートするには、ポートプローブに別のインターフェイスを設定します。また、2 つのスタティックルートを設定する必要があります。1 つはプライマリインターフェイス用で、もう 1 つはロードバランサプローブ用に設定されたインターフェイス用です。

ステップ 5 プライマリインターフェイスとロードバランサプローブ用に設定されたインターフェイスのスタティックルートを追加します。

route *if-name dest_ip mask gateway_ip* **[distance]**

例：

```
ciscoasa(config)# route outside 168.63.129.16 255.255.255.255 10.22.0.1 1
ciscoasa(config)# route inside 168.63.129.16 255.255.255.255 10.22.1.1 2
```

distance 引数は、ルートのアドミニストレーティブ ディスタンスです。値を指定しない場合、デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。宛先が同じルートが複数存在する場合（168.63.129.16）、ルートのアドミニストレーティブ ディスタンスによってプライオリティが決まります。

アドミニストレーティブディスタンスが1のプライマリインターフェイス（外部）のスタティックルートは、168.63.129.16宛てのパケットの優先インターフェイスとしてプライマリインターフェイスを確立しますが、ロードバランサプローブ用に設定されたインターフェイスが168.63.129.16 にパケットを送信できるようにします。

（注）
プローブに応答するメカニズムは、インターフェイス上にTCPソケットを作成することです。クラウドHAは168.63.129.16のルートルックアップを使用して、ソケットを作成するインターフェイスを決定します。デフォルトルートが存在するため、これが最終的にプライマリインターフェイスになります。プローブ用に設定されたインターフェイスのスタティックルートがないと、ASA はロードバランサから送信された TCP パケットに応答しません。

Azure サービス プリンシパル用の認証クレデンシャルの設定

ASA 仮想 HA ピアが、Azure サービスプリンシパルを使用してルートテーブルなどの Azure リソースにアクセスしたり、それらのリソースを変更したりできるようにすることが可能です。Azure Active Directory（AD）アプリケーションを設定し、必要な権限を割り当てる必要があります。次のコマンドを使用すると、ASA 仮想 はサービスプリンシパルを使用して Azure で認証されます。Azureサービスプリンシパルの詳細については、ASA仮想クイックスタートガイドの「Azure」の章を参照してください。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。
- プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。

手順

ステップ 1 Azure サービス プリンシパルの Azure サブスクリプション ID を設定します。

failover cloud subscription-id *subscription-id*

例：

```
(config)# failover cloud subscription-id ab2fe6b2-c2bd-44
```

Azure サブスクリプション ID は、クラウド HA ユーザーが内部ルートをアクティブ装置に向ける場合など、Azure ルート テーブルを変更するために必要です。

ステップ 2 Azure サービス プリンシパルのクレデンシャル情報を設定します。

failover cloud authentication {**application-id** | **directory-id** | **key**}

フェールオーバー中に Azure ルート テーブルを変更するには、Azure インフラストラクチャからアクセス キーを入手してからルート テーブルにアクセスする必要があります。アクセス キーは、HA ペアを制御する Azure サービス プリンシパルのアプリケーション ID、ディレクトリ ID、および秘密鍵を使用して取得します。

ステップ 3 Azure サービス プリンシパルのアプリケーション ID を設定します。

failover cloud authentication application-id *appl-id*

例：

```
(config)# failover cloud authentication application-id dfa92ce2-fea4-67b3-ad2a-6931704e4201
```

Azure インフラストラクチャからアクセス キーを要求するときは、このアプリケーション ID が必要です。

ステップ 4 Azure サービス プリンシパルのディレクトリ ID を設定します。

failover cloud authentication directory-id *dir-id*

例：

```
(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138b77ae9
```

Azure インフラストラクチャからアクセス キーを要求するときは、このディレクトリ ID が必要です。

ステップ 5 Azure サービス プリンシパルの秘密鍵 ID を設定します。

failover cloud authentication key *secret-key* [**encrypt**]

例：

```
(config)# failover cloud authentication key 5yOhH593dtD/O8gzAlWgulrkWz5dH02d2STk3LDbI4c=
```

Azure インフラストラクチャからアクセス キーを要求するときは、この秘密鍵が必要です。**encrypt** キーワードが存在する場合、秘密鍵は **running-config** で暗号化されます。

Azure ルート テーブルの設定

ルートテーブル設定は、ASA 仮想 がアクティブなロールを引き継ぐときに更新する必要のある Azure ユーザー定義ルートに関する情報で構成されています。フェールオーバーでは、内部ルートをアクティブ装置に向ける必要があります。アクティブ装置は、設定されたルートテーブル情報を使用して自動的にルートを自身に向けます。

（注） アクティブ装置とバックアップ装置の両方で Azure ルートテーブル情報を設定する必要があります。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。
- プライマリ装置とセカンダリ装置の両方でこれらの設定を構成します。プライマリ装置からセカンダリ装置への設定の同期はありません。
- Azure サブスクリプション ID とサービス プリンシパルの Azure 認証クレデンシャルを含む、Azure 環境情報を入手します。

手順

ステップ 1 フェールオーバー時に更新が必要な Azure ルート テーブルを設定します。

failover cloud route-table *table-name* [**subscription-id** *sub-id*]

例：

```
ciscoasa(config)# failover cloud route-table inside-rt
```

（オプション）2 つ以上の Azure サブスクリプションでユーザー定義のルートを更新するには、**subscription-id** パラメータを含めます。

例：

```
ciscoasa(config)# failover cloud route-table inside-rt subscription-id cd5fe6b4-d2ed-45
```

route-table コマンド レベルの **subscription-id** パラメータは、グローバル レベルで指定された Azure サブスクリプション ID をオーバーライドします。Azure サブスクリプション ID を指定せずに **route-table** コマンドを入力すると、グローバル **subscription-id** パラメータが使用されます。Azure サブスクリプション ID の詳細については、Azure サービス プリンシパル用の認証クレデンシャルの設定 （397 ページ）を参照してください。

（注）
route-table コマンドを入力すると、ASA 仮想 は **cfg-fover-cloud-rt** モードに切り替わります。

ステップ 2 ルート テーブルに Azure リソース グループを構成します。

rg *resource-group*

例：

```
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
```

Azure でのルート テーブルの更新要求にはリソース グループが必要です。

ステップ 3 フェールオーバー時に更新が必要なルートを設定します。

route name *route-name* **prefix** *address-prefix* **nexthop** *ip-address*

例：

```
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4
```

アドレスプレフィックスは、IPアドレスプレフィックス、スラッシュ（'/'）および数字のネットマスクとして設定されます。たとえば *192.120.0.0/16* などです。

例

全構成の例を次に示します。

```
ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4
```

アクティブ/バックアップ フェールオーバーの有効化

アクティブ/バックアップ フェールオーバーを有効にするには、プライマリ装置とセカンダリ装置の両方で設定を行う必要があります。プライマリ装置からセカンダリ装置に設定が同期されることはありません。フェールオーバートラフィックの処理に関して、各装置で同様の設定を個々に構成する必要があります。

アクティブ/バックアップ フェールオーバーのプライマリ装置の有効化

この項の手順に従って、アクティブ/バックアップ フェールオーバー構成のプライマリを有効にします。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。

手順

ステップ 1 フェールオーバーをイネーブルにします。

ciscoasa(config)# failover

ステップ 2 システム コンフィギュレーションをフラッシュ メモリに保存します。

ciscoasa(config)# write memory

例

次に、プライマリ装置の完全な設定の例を示します。

```
ciscoasa(config)# failover cloud unit primary
ciscoasa(config)# failover cloud peer ip 10.4.3.4

ciscoasa(config)# failover cloud authentication application-id
dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

次のタスク

セカンダリ装置を有効にします。

アクティブ/バックアップ フェールオーバーのセカンダリ装置の有効化

この項の手順に従って、アクティブ/バックアップ フェールオーバー構成のセカンダリを有効にします。

始める前に

- シングル コンテキスト モードのシステム実行スペースで次の設定を行います。

手順

ステップ 1 フェールオーバーをイネーブルにします。

ciscoasa(config)# **failover**

ステップ 2 システム コンフィギュレーションをフラッシュ メモリに保存します。

ciscoasa(config)# **write memory**

例

次に、セカンダリ装置の完全な設定の例を示します。

```
ciscoasa(config)# failover cloud unit secondary
ciscoasa(config)# failover cloud peer ip 10.4.3.5

ciscoasa(config)# failover cloud authentication application-id
dfa92ce2-fea4-67b3-ad2a-693170
ciscoasa(config)# failover cloud authentication directory-id 227b0f8f-684d-48fa-9803-c08138
ciscoasa(config)# failover cloud authentication key 5yOhH593dtD/O8gzAWguH02d2STk3LDbI4c=
ciscoasa(config)# failover cloud authentication subscription-id ab2fe6b2-c2bd-44

ciscoasa(config)# failover cloud route-table inside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-outside prefix 10.4.2.0/24 nexthop 10.4.1.4

ciscoasa(config)# failover cloud route-table outside-rt
ciscoasa(cfg-fover-cloud-rt)# rg east-rg
ciscoasa(cfg-fover-cloud-rt)# route route-to-inside prefix 10.4.1.0/24 nexthop 10.4.2.4

ciscoasa(config)# failover
ciscoasa(config)# write memory
```

パブリック クラウドでのフェールオーバーの管理

この項では、フェールオーバーを有効にした後でクラウド内の フェールオーバー 装置を管理する方法について説明します。ある装置から別の装置にフェールオーバーを強制的に変更する方法についても説明します。

フェールオーバーの強制実行

スタンバイ装置を強制的にアクティブにするには、次のコマンドを実行します。

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ステップ 1 スタンバイ装置で入力した場合、フェールオーバーが強制実行されます。

failover active

例：

```
ciscoasa# failover active
```

スタンバイ装置はアクティブ装置になります。

ステップ 2 アクティブ装置で入力した場合、フェールオーバーが強制実行されます。

no failover active

例：

```
ciscoasa# no failover active
```

アクティブ装置はスタンバイ装置になります。

ルートの更新

Azure のルートの状態がアクティブロールの ASA 仮想 と矛盾している場合は、次の EXEC コマンドを使用して ASA 仮想 でルート更新を強制できます。

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

アクティブ装置のルートを更新します。

failover cloud update routes

例：

```
ciscoasa# failover cloud update routes
Beginning route-table updates
Routes changed
```

このコマンドは、アクティブロールの ASA 仮想 でのみ有効です。認証に失敗すると、コマンド出力は `Route changes failed` となります。

Azure 認証の検証

Azure で ASA 仮想 HA の展開を成功させるには、サービスプリンシパルの設定が完全かつ正確である必要があります。適切な Azure 認証がないと、ASA 仮想 ユニットはリソースにアクセスして、フェールオーバーを処理したりルート更新を実行したりできません。フェールオーバー設定をテストして、Azure サービス プリンシパルの次の要素に関連するエラーを検出できます。

- ディレクトリ ID
- Application ID
- Authentication Key

始める前に

シングル コンテキスト モードのシステム実行スペースで次のコマンドを使用します。

手順

ASA 仮想 HA 設定の Azure 認証要素をテストします。

test failover cloud authentication

例：

```
ciscoasa(config)# test failover cloud authentication
Checking authentication to cloud provider
Authentication Succeeded
```

認証に失敗すると、コマンド出力は `Authentication Failed` となります。

ディレクトリ ID またはアプリケーション ID が正しく設定されていない場合、Azure は認証トークンを取得するための REST 要求で指定されたリソースを認識しません。この条件エントリのイベント履歴は次のようになります。

```
Error Connection - Unexpected status in response to access token request: Bad Request
```

ディレクトリ ID またはアプリケーション ID は正しいが、認証キーが正しく設定されていない場合、Azure は認証トークンを生成する権限を許可しません。この条件エントリのイベント履歴は次のようになります。

```
Error Connection - Unexpected status in response to access token request: Unauthorized
```

パブリック クラウドでのフェールオーバーのモニター

この項では、フェールオーバー ステータスをモニターする方法について説明します。

フェールオーバー ステータス

フェールオーバー ステータスをモニターするには、次のいずれかのコマンドを入力します。

- **show failover**

  装置のフェールオーバー状態についての情報を表示します。未設定の設定要素の値は *not configured* と表示されます。

  ルート更新情報は、アクティブ装置に対してのみ表示されます。

- **show failover history**

  タイムスタンプ、重大度レベル、イベントタイプ、およびイベントテキストを含むフェールオーバー イベントの履歴を表示します。

フェールオーバー メッセージ

フェールオーバーの syslog メッセージ

ASA は、深刻な状況を表すプライオリティ レベル 2 のフェールオーバーについて、複数の syslog メッセージを発行します。これらのメッセージを表示するには、syslog メッセージ ガイドを参照してください。Syslog メッセージの範囲は 1045xx と 1055xx です。

（注） フェールオーバーの最中に、ASA は論理的にシャットダウンした後、インターフェイスを起動し、syslog メッセージを生成します。これは通常のアクティビティです。

スイッチオーバー中に生成される syslog の例を次に示します。

```
%ASA-3-105509: (Primary) Error sending Hello message to peer unit 10.22.3.5, error:
Unknown error
%ASA-1-104500: (Primary) Switching to ACTIVE - switch reason: Unable to send message to
 Active unit
%ASA-5-105522: (Primary) Updating route-table wc-rt-inside
%ASA-5-105523: (Primary) Updated route-table wc-rt-inside
%ASA-5-105522: (Primary) Updating route-table wc-rt-outside
%ASA-5-105523: (Primary) Updated route-table wc-rt-outside
%ASA-5-105542: (Primary) Enabling load balancer probe responses
%ASA-5-105503: (Primary) Internal state changed from Backup to Active no peer
%ASA-5-105520: (Primary) Responding to Azure Load Balancer probes
```

パブリック クラウドの導入に関連する各 syslog には、装置の役割が最初に追加されます（(Primary) または (Secondary)）。

フェールオーバー デバッグ メッセージ

デバッグ メッセージを表示するには、**debug fover** コマンドを入力します。詳細については、コマンド リファレンスを参照してください。

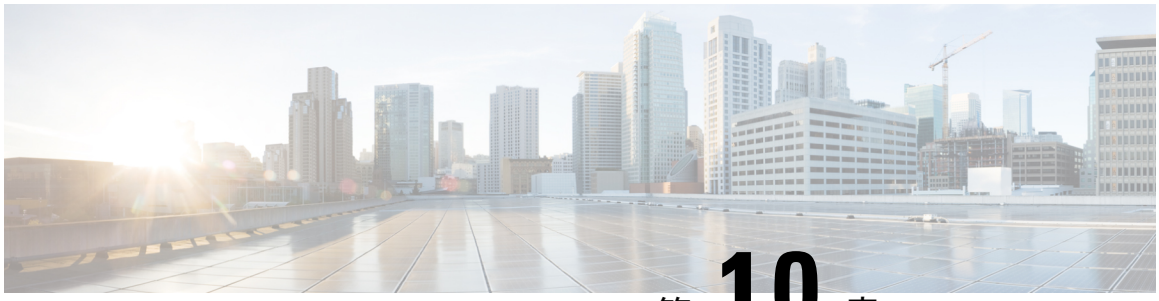
（注） CPUプロセスではデバッグ出力に高プライオリティが割り当てられているため、デバッグ出力を行うとシステムパフォーマンスに大きく影響することがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug fover** コマンドを使用してください。

SNMP のフェールオーバー トラップ

フェールオーバーに対する SNMP syslog トラップを受信するには、SNMP トラップを SNMP 管理ステーションに送信するように SNMP エージェントを設定し、syslog ホストを定義し、お使いの SNMP 管理ステーションに Cisco syslog MIB をコンパイルします。

パブリック クラウドでのフェールオーバーの履歴

機能名	リリース	機能情報
Microsoft Azure でのアクティブ/バックアップ フェールオーバー	9.8(200)	この機能が導入されました。



第 10 章

Cisco Secure Firewall 3100/4200 の ASA クラスタ

クラスタリングを利用すると、複数の ASA をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「クラスタリングでサポートされない機能 （503 ページ）」を参照してください。

- ASA クラスタリングの概要 （407 ページ）
- ASA クラスタリングのライセンス （412 ページ）
- ASA クラスタリングの要件と前提条件 （414 ページ）
- クラスタリングに関するガイドライン （416 ページ）
- ASA クラスタリングの設定 （422 ページ）
- クラスタノードの管理 （468 ページ）
- ASA クラスタのモニタリング （474 ページ）
- 分散型サイト間 VPN のトラブルシューティング （486 ページ）
- ASA クラスタリングの例 （488 ページ）
- クラスタリングの参考資料 （503 ページ）
- Cisco Secure Firewall 3100/4200 の ASA クラスタリングの履歴 （522 ページ）

ASA クラスタリングの概要

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのユニットとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離された高速バックプレーン ネットワーク。クラスタ制御リンクと呼ばれます。
- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。

クラスタをネットワーク内に配置するときは、クラスタが送受信するデータのロードバランシングを、アップストリームおよびダウンストリームのルータが次のいずれかの方法でできることが必要です：

- スパンド EtherChannel（推奨）：クラスタ内の複数のメンバのインターフェイスをグループ化して 1 つの EtherChannel とします。この EtherChannel がユニット間のロードバランシングを実行します。
- ポリシーベース ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してユニット間のロード バランシングを実行します。
- 等コスト マルチパス ルーティング（ルーテッド ファイアウォール モードのみ）：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミック ルートを使用してユニット間のロード バランシングを実行します。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。ここでは、各メンバーのロールの特長について説明します。

ブートストラップ設定

各デバイスで、最小限のブートストラップ コンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。通常、クラスタリングを有効にする最初のノードが制御ノードになります。以降のノードに対してクラスタリングをイネーブルにすると、そのノードはデータノードとしてクラスタに参加します。

制御ノードとデータノードの役割

クラスタ内のメンバーの 1 つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。一般的には、クラスタを作成

した後で最初に追加したノードが制御ノードとなります。これは単に、その時点でクラスタに存在する唯一のノードであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ノード上のみで実行する必要があります。コンフィギュレーションは、データノードに複製されます。物理的アセット（たとえばインターフェイス）の場合は、制御ノードのコンフィギュレーションがすべてのデータノード上でミラーリングされます。たとえば、内部インターフェイスとしてイーサネット1/2を設定し、外部インターフェイスとしてイーサネット1/1を設定した場合、これらのインターフェイスは内部および外部インターフェイスとしてデータノードでも使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

クラスタ インターフェイス

データインターフェイスは、スパンドEtherChannelとして設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータインターフェイスのタイプが同一であるか。詳細については、クラスタインターフェイスについて（423ページ）を参照してください。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。詳細については、クラスタ制御リンク（423ページ）を参照してください。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

ASA クラスタ管理

ASAクラスタリングを使用することの利点の1つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理インターフェイスについては、専用管理インターフェイスの1つを使用することを推奨します。管理インターフェイスは、個別インターフェイスとして設定することも（ルーテッドモードとトランスペアレントモードの両方）、スパンドEtherChannelインターフェイスとして設定することもできます。

、管理用には、個別インターフェイスを使用することを推奨します。個別インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンドEtherChannelインターフェイスでは、現在の制御ユニットへのリモート接続しかできません。

（注） スパンドEtherChannelインターフェイスモードを使用して、管理インターフェイスを個別インターフェイスとして構成する場合は、管理インターフェイスに対してダイナミックルーティングをイネーブルにすることはできません。スタティック ルートを使用する必要があります。

個別インターフェイスの場合は、メインクラスタ IP アドレスはそのクラスタの固定アドレスであり、常に現在の制御ユニットに属します。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ユニット（現在の制御ユニットも含まれます）がその範囲内のローカルアドレスを使用できるようになります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタの管理をシームレスに続行できます。ローカル IP アドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の制御ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

（注） to-the-box トラフィックをノードの管理IPアドレスに転送する必要があります。to-the-box トラフィックは、クラスタ制御リンクを介して他のノードに転送されません。

TFTP や syslog などの発信管理トラフィックの場合、制御ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバーに接続します。

スパンド EtherChannel インターフェイスの場合は、IP アドレスは 1 つだけ設定でき、その IP アドレスは常に制御ユニットに関連付けられます。EtherChannel インターフェイスを使用してデータユニットに直接接続することはできません。管理インターフェイスは個別インターフェイスとして設定することを推奨します。各ユニットに接続できるようにするためです。デバイス ローカル EtherChannel を管理に使用できます。

制御ユニット管理とデータユニット管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。ま

た、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。
- ノードごとのSyslogモニタリング（コンソールレプリケーションが有効な場合にコンソールに送信される Syslog を除く）。
- SNMP
- NetFlow

暗号キー複製

制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有のMACアドレスおよびIPアドレスを使用するのに対し、クラスタで受信したパケットは、グローバルMACアドレスおよびIPアドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイ

トの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト ID は、LISP インスペクションを使用したフロー モビリティの有効化、データセンターのサイト間クラスタリングのパフォーマンス向上とラウンドトリップ時間の遅延短縮のためのディレクタ ローカリゼーションの有効化、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトに存在する接続に対するサイト冗長性の有効化のためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：ASA クラスタリングの要件と前提条件 （414 ページ）
- サイト間のガイドライン：クラスタリングに関するガイドライン （416 ページ）
- クラスタ フロー モビリティの設定：クラスタ フロー モビリティの設定 （456 ページ）
- ディレクタ ローカリゼーションの有効化：ディレクタ ローカリゼーションの有効化 （454 ページ）
- サイト冗長性の有効化：ディレクタ ローカリゼーションの有効化 （454 ページ）
- サイト間での例：サイト間クラスタリングの例 （498 ページ）

ASA クラスタリングのライセンス

Smart Software Manager Regular およびオンプレミス

各ユニットには、Essentialsライセンス（デフォルトで有効）と同じ暗号化ライセンスが必要です。ライセンス不一致の問題を回避するために、クラスタリングを有効にする前に、ライセンスサーバで各ユニットのライセンスを取得することをお勧めします。また、高度暗号化ライセンスを使用する場合は、クラスタ制御リンクの暗号化に関する問題も発生します。

クラスタリング機能自体にライセンスは必要ありません。データユニットのコンテキストライセンスに追加料金はかかりません。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、Essentialsライセンスはすべてのユニットで常にデフォルトで有効になっています。制御ユニットにのみスマートライセンスを設定できます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Essentials：各ユニットには、サーバーからのEssentialsのライセンスが必要です。

- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは2のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。

  - クラスタ内に 6 つの Secure Firewall 3100 があります。Essentialsライセンスは 2 のコンテキストを含みます。6ユニットの場合、合計で12のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは32のコンテキストを含みます。シャーシごとのプラットフォームの制限が 100 であるため、結合されたライセンスでは最大 100 のコンテキストが許容されます。32 コンテキストは制限の範囲内です。したがって、制御ユニット上で最大32コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して 32 コンテキストを持つことになります。

  - クラスタ内に 3 つの Secure Firewall 3100 があります。Essentialsライセンスは 2 のコンテキストを含みます。3 ユニットの場合、合計で 6 のコンテキストが加算されます。制御ユニット上で追加の 100 コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 106 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 100 であるため、統合されたライセンスでは最大 100 のコンテキストが許容されます。106 コンテキストは制限を超えています。したがって、制御ユニット上で最大100のコンテキストのみを設定できます。各データユニットも、設定の複製を介して100のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして 94 のコンテキストのみを設定する必要があります。

- 高度な暗号化（3DES）：スマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されているとシスコが判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。制御ユニットのみがこのライセンスを要求し、ライセンスの集約により、すべてのユニットがそれを使用できます。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブ装置は、ライセンスのコンプライアンスが確保されるまで 35 秒ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

ASA クラスタリングの要件と前提条件

モデルの要件

- Secure Firewall 3100：最大 16 ユニット
- Secure Firewall 4200：最大 16 ユニット

ASA のハードウェアおよびソフトウェア要件

クラスタ内のすべてのユニット：

- 同じ DRAM を使用する同じモデルである必要があります。フラッシュ メモリの容量は同一である必要はありません。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレスアップグレードがサポートされます。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- セキュリティ コンテキスト モードが一致している必要があります（シングルまたはマルチ）。
- （シングル コンテキスト モード）ファイアウォール モードが一致している必要があります（ルーテッドまたはトランスペアレント）。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタメンバーは、制御ユニットと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。

スイッチ要件

- ASA でクラスタリングを設定する前に、スイッチのコンフィギュレーションを完了する必要があります。
- サポートされているスイッチのリストについては、『Cisco ASA Compatibility』[英語] を参照してください。

ASA の要件

- ユニットを管理ネットワークに追加する前に、一意の IP アドレスを各ユニットに提供します。
  - ASA への接続および管理 IP アドレスの設定に関する詳細については、「使用する前に」の章を参照してください。

- 制御ユニット（通常は最初にクラスタに追加されたユニット）で使用される IP アドレスを除き、これらの管理 IP アドレスは一時的に使用されるだけです。
- データユニットがクラスタに参加すると、管理インターフェイス設定はマスターユニットからの複製に置き換えられます。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用に Data Center Interconnect（DCI）に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCI の最小帯域幅は、1 つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバの場合。
  - 合計 4 クラスタ メンバ
  - 各サイト 2 メンバ
  - メンバあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。
- 3 サイトの 6 メンバの場合、サイズは増加します。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。
- 2 サイトの 2 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

その他の要件

ターミナル サーバーを使用して、すべてのクラスタ メンバ ユニットのコンソール ポートにアクセスすることをお勧めします。初期設定および継続的な管理（ユニットがダウンしたときなど）では、ターミナル サーバーがリモート管理に役立ちます。

クラスタリングに関するガイドライン

コンテキスト モード

モードは、各メンバー ユニット上で一致している必要があります。

ファイアウォール モード

シングル モードの場合、ファイアウォール モードがすべてのユニットで一致している必要があります。

フェールオーバー

フェールオーバーは、クラスタリングではサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

スイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンク インターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンク インターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。さらに、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS XR インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS XR *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。

- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。
- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **src-dst-mixed-ip-port** を使用することをお勧めします（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシング アルゴリズムは変更しないでください。
- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリー プロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。
- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。
- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。
- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS 設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

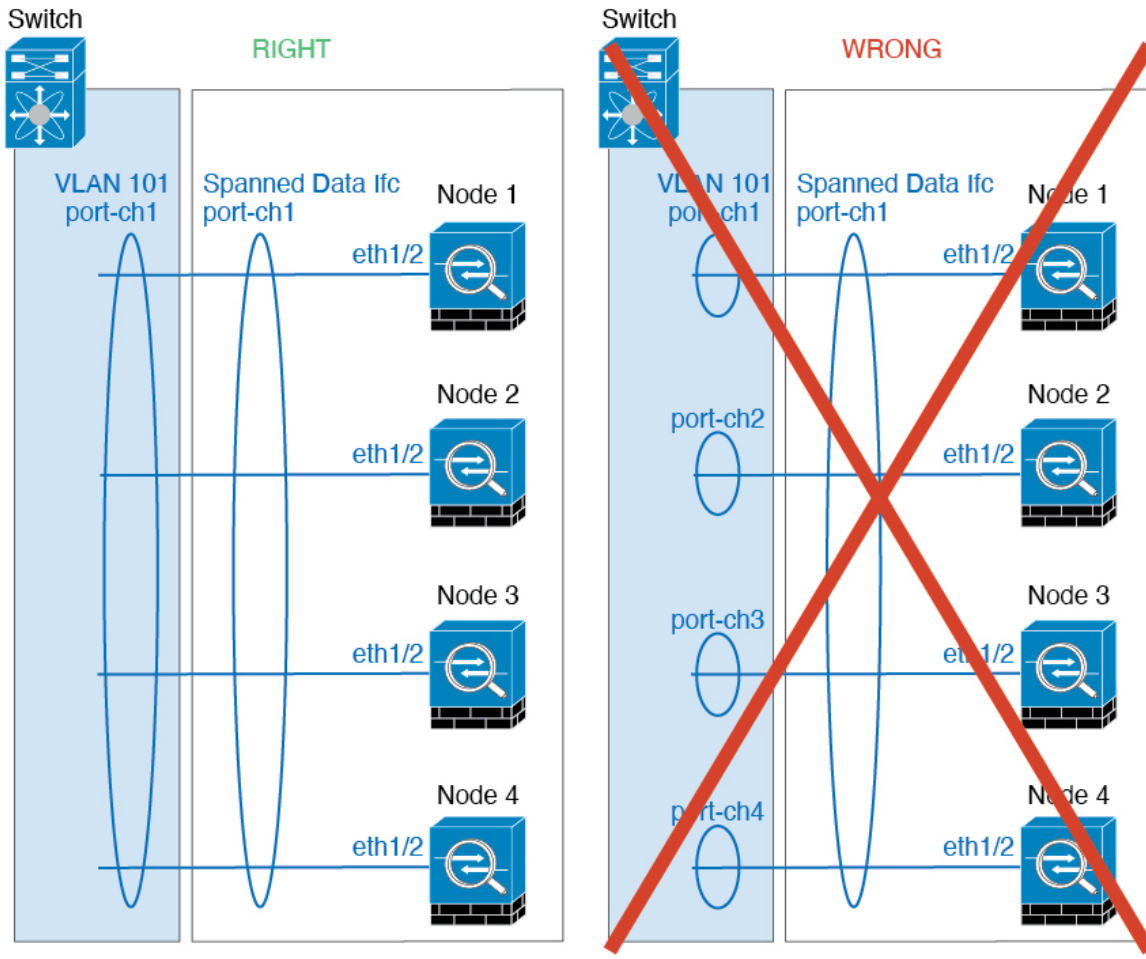
  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

- Cisco Nexus スイッチのクラスタに接続されたすべての EtherChannel インターフェイスで、LACP グレースフル コンバージェンス機能を無効化する必要があります。

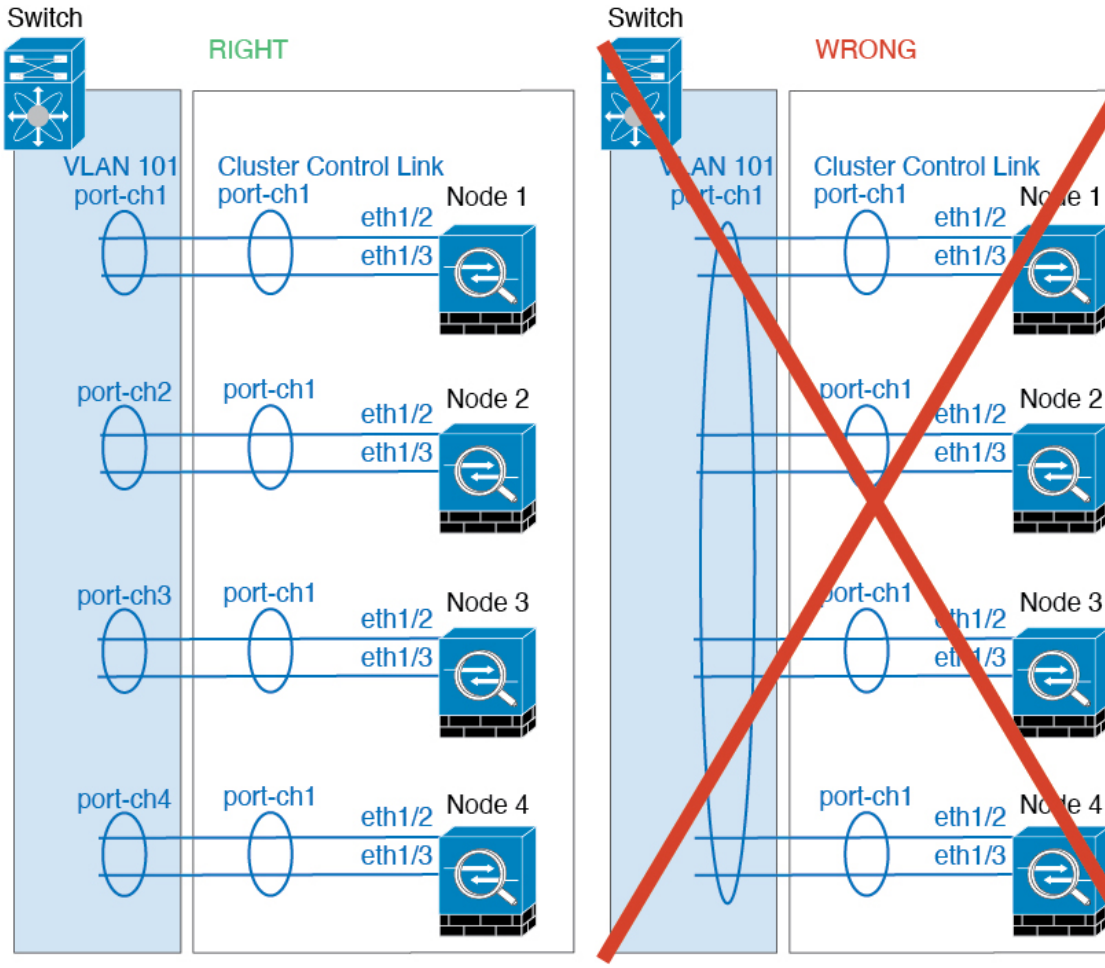
EtherChannel

- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。
  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



  - デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間のガイドライン

サイト間クラスタリングについては、次のガイドラインを参照してください。

- 次のインターフェイスおよびファイアウォール モードで Inter-Site クラスタリングをサポートします。

インターフェイス モード	ファイアウォール モード	
	ルーテッド	Transparent
個別インターフェイス	対応	N/A
スパンド EtherChannel	○	○

- 個別インターフェイス モードでは、マルチキャスト ランデブー ポイント（RP）に向けて ECMP を使用する場合、ネクストホップとしてメイン クラスタ IP アドレスを使用する RP IP アドレスのスタティック ルートを使用することをお勧めします。このスタティック ルートは、データユニットにユニキャスト PIM 登録パケットが送信されるのを防ぎます。デー

タユニットがPIM登録パケットを受け取った場合、パケットはドロップされ、マルチキャストストリームは登録できません。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- ASAは専用リンクであるため、データセンター相互接続（DCI）で使用されている場合でも、クラスタ制御リンクで転送されるデータトラフィックを暗号化しません。オーバーレイトランスポート仮想化（OTV）を使用する場合、またはローカル管理ドメインの外部でクラスタ制御リンクを拡張する場合は、OTE を介した 802.1AE MacSec などの境界ルータで暗号化を設定できます。
- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタのローカリゼーションを有効にすると、ローカルディレクタのロールは常に（サイト ID に従って）接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。
- ディレクタ ローカリゼーションでは、次のトラフィック タイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション クエリ。
- ノースサウス展開での UDP の長期的フローでは、元のフローの所有者サイトのノードに障害が発生してから復帰し、その後フローが元のサイトに戻されると、ルーティング ループが発生する可能性があります。他のサイトの新しい所有者に宛先へのルートがない場合、フローがインターネットに戻され、ループが発生します。この場合、新しい所有者に対して **clear conn** コマンドを使用して、強制的にフローを再確立します。
- トランスペアレントモードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じMACアドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレントモードの場合、内部ネットワーク間のファイル用に各サイトのデータネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ

VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。

- トランスペアレントモードでは、クラスタが HSRP ルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして ASA に追加する必要があります（ブリッジ グループのスタティック MAC アドレスの追加（1114 ページ）を参照）。隣接ルータで HSRP が使用される場合、HSRP IP アドレス宛てのトラフィックは HSRP MAC アドレスに送信されますが、リターントラフィックは特定のルータのインターフェイスの MAC アドレスから HSRP ペアで送信されます。したがって、ASA MAC アドレステーブルは通常、HSRP IP アドレスの ASA ARP テーブルエントリが期限切れになり、ASA が ARP 要求を送信して応答を受信した場合にのみ更新されます。ASA の ARP テーブルエントリはデフォルトで 14400 秒後に期限切れになりますが、MAC アドレステーブルエントリはデフォルトで 300 秒後に期限切れになるため、MAC アドレステーブルの期限切れトラフィックのドロップを回避するために静的 MAC アドレスエントリが必要です。

- スパンド EtherChannel を使用したルーテッド モードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが 1 つのサイトで到達不能になった場合、トラフィックが他のサイトのクラスタ ノードに正常に到達できるようにフィルタを削除する必要があります。ダイナミック ルーティングは、サイト間クラスタが拡張セグメントのファースト ホップ ルータとして機能する場合はサポートされません。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、ファイアウォール上でのインターフェイスまたはスイッチの有効化または無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するための追加スイッチの追加など）、ヘルス チェック機能や無効なインターフェイスのインターフェイス モニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。

- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。

- スパンド EtherChannel に接続された Windows 2003 Server を使用している場合、syslog サーバー ポートがダウンし、サーバーが ICMP エラー メッセージを調整しないと、多数の ICMP メッセージがクラスタに送信されます。このようなメッセージにより、クラスタの

一部のユニットでCPU使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。

- 個別インターフェイス モードのVXLANはサポートされていません。スパンドEtherChannelモードでのみ VXLAN をサポートしています。
- シスコは、スパンド EtherChannel モードの IS-IS をサポートしません。個別インターフェイス モードのみが IS-IS をサポートします。
- クラスタ内のすべてのユニットに変更が複製されるまでには時間がかかります。たとえば、オブジェクトグループを使用するアクセスコントロールルール（展開時に複数のルールに分割される）を追加するなどの大きな変更を行うと、変更の完了に必要な時間がクラスタユニットが成功メッセージで応答できるタイムアウトを超える可能性があります。この場合、「failed to replicate command」というメッセージが表示されることがあります。このメッセージは無視できます。

クラスタリングのデフォルト

- スパンド EtherChannel を使用するときは、cLACP システム ID は自動生成され、システム プライオリティはデフォルトで 1 です。
- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が5分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

ASA クラスタリングの設定

クラスタリングを設定するには、次のタスクを実行します。

（注） クラスタリングを有効または無効にするには、コンソール接続（CLIの場合）またはASDM接続を使用します。

ユニットのケーブル接続およびインターフェイスの設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。次に、インターフェイスを設定します。

クラスタ インターフェイスについて

データインターフェイスは、スパンドEtherChannelとして設定することも、個別インターフェイスとして設定することもできます。1つのクラスタ内のすべてのデータインターフェイスのタイプが同一であることが必要です。イーサネット1/1をスパンドEtherChannelとして設定し、イーサネット1/2を同じクラスタ内の個別インターフェイス（など）として設定することはできません。

また、各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。

クラスタ制御リンク

各ユニットの、少なくとも1つのハードウェアインターフェイスをクラスタ制御リンク専用とする必要があります。可能な場合は、クラスタ制御リンクにEtherChannelを使用することを推奨します。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンク インターフェイスとネットワーク

次の例外を除き、クラスタ制御リンクには任意のデータ インターフェイスを使用できます。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。
- 管理 *x*/*x* インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。

EtherChannel インターフェイスを使用できます。

各クラスタ制御リンクは、同じサブネット上の IP アドレスを持ちます。このサブネットは、他のすべてのトラフィックからは隔離し、ASA クラスタ制御リンク インターフェイスだけが含まれるようにしてください。

2 メンバー クラスタの場合、ASA と ASA の間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンクのサイジング

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- ネットワークアクセスに対する AAA は一元的な機能であるため、すべてのトラフィックが制御ユニットに転送されます。
- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

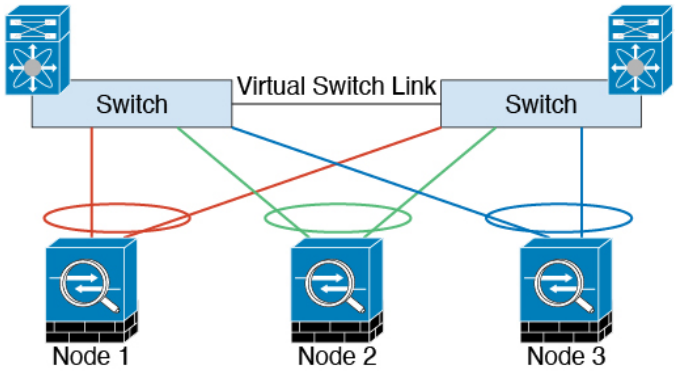
（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンクの冗長性

クラスタ制御リンクにはEtherChannelを使用することを推奨します。冗長性を実現しながら、EtherChannel 内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチングシステム（VSS）、仮想ポートチャネル（vPC）、StackWise、または StackWise Virtual 環境でクラスタ制御リンクとして EtherChannel を使用する方法を示します。EtherChannel のすべてのリンクがアクティブです。スイッチが冗長システムの一部である場合は、同じ EtherChannel 内のファイアウォールインターフェイスをそれぞれ、冗長システム内の異なるスイッチに接続できます。スイッチ インターフェイスは同じ EtherChannel ポートチャネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動

作するからです。このEtherChannelは、スパンドEtherChannelではなく、デバイスローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が20 ms未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタメンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクでpingを実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンクの障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データインターフェイスはシャットダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。

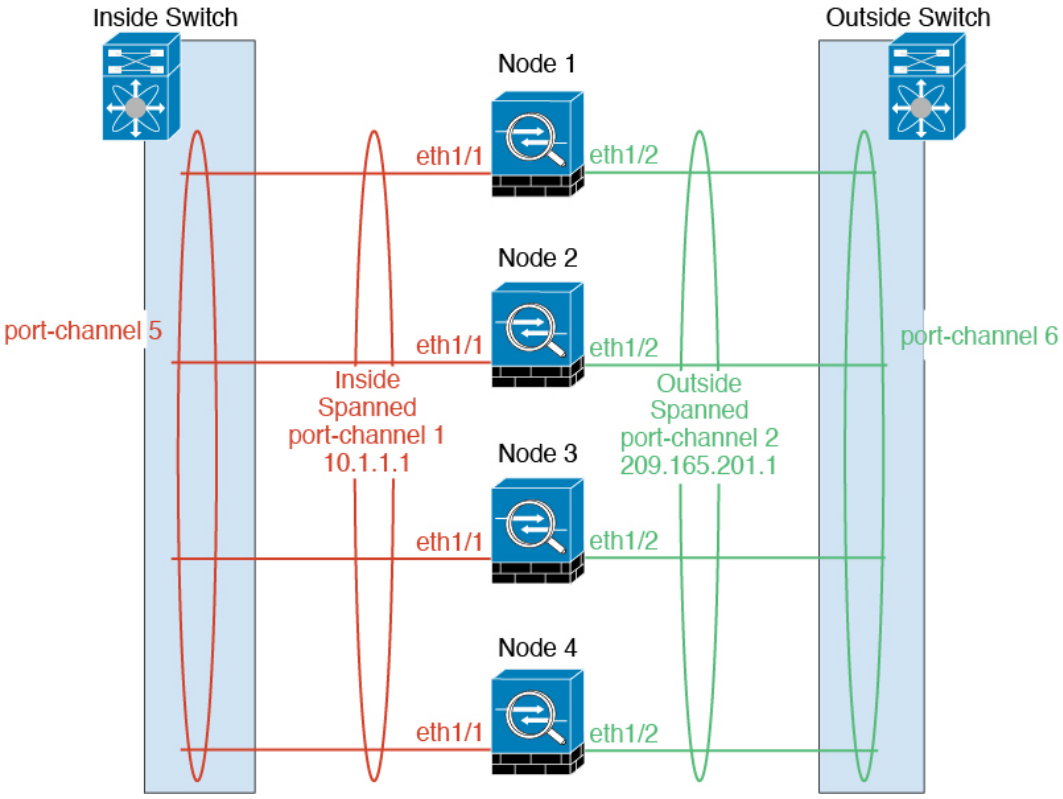
（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットがクラスタIPプールから受け取ったIPアドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（制御ユニットと同じメインIPアドレスを使用するため）。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

スパンドEtherChannel（推奨）

シャーシあたり1つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がるEtherChannelとすることができます。EtherChannelによって、チャネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。

スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。

EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



スパンド *EtherChannel* の利点

EtherChannel 方式のロードバランシングは、次のような利点から、他の方式よりも推奨されます。

- 障害検出までの時間が短い。
- コンバージェンス時間が短い。個別インターフェイスはルーティング プロトコルに基づきトラフィックをロード バランシングしますが、ルーティング プロトコルはリンク障害時にコンバージェンスが遅くなることがよくあります。
- コンフィギュレーションが容易である。

最大スループットのガイドライン

最大スループットを実現するには、次のことを推奨します。

- 使用するロード バランシング ハッシュ アルゴリズムは「対称」であるようにします。つまり、どちらの方向からのパケットも同じハッシュを持たせて、スパンド EtherChannel 内

の同じ ASA に送信します。送信元と宛先の IP アドレス（デフォルト）または送信元と宛先のポートをハッシュ アルゴリズムとして使用することを推奨します。

- ASA をスイッチに接続するときは、同じタイプのラインカードを使用します。すべてのパケットに同じハッシュ アルゴリズムが適用されるようにするためです。

ロード バランシング

EtherChannel リンクは、送信元または宛先 IP アドレス、TCP ポートおよび UDP ポート番号に基づいて、専用のハッシュ アルゴリズムを使用して選択されます。

（注） スイッチでは、アルゴリズム **source-dest-ip** または **source-dest-ip-port**（Cisco Nexus OS または Cisco IOS の **port-channel load-balance** コマンドを参照）を使用することをお勧めします。クラスタのノードにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。

EtherChannel 内のリンク数はロード バランシングに影響を及ぼします。

対称ロード バランシングは常に可能とは限りません。NAT を設定する場合は、フォワード パケットとリターン パケットとで IP アドレスやポートが異なります。リターン トラフィックはハッシュに基づいて別のユニットに送信されるため、クラスタはほとんどのリターン トラフィックを正しいユニットにリダイレクトする必要があります。

EtherChannel の冗長性

EtherChannel には、冗長性機能が組み込まれています。これは、すべてのリンクの回線プロトコル ステータスをモニターします。リンクの 1 つで障害が発生すると、トラフィックは残りのリンク間で再分散されます。EtherChannel のすべてのリンクが特定のユニット上で停止したが、他方のユニットがまだアクティブである場合は、そのユニットはクラスタから削除されます。

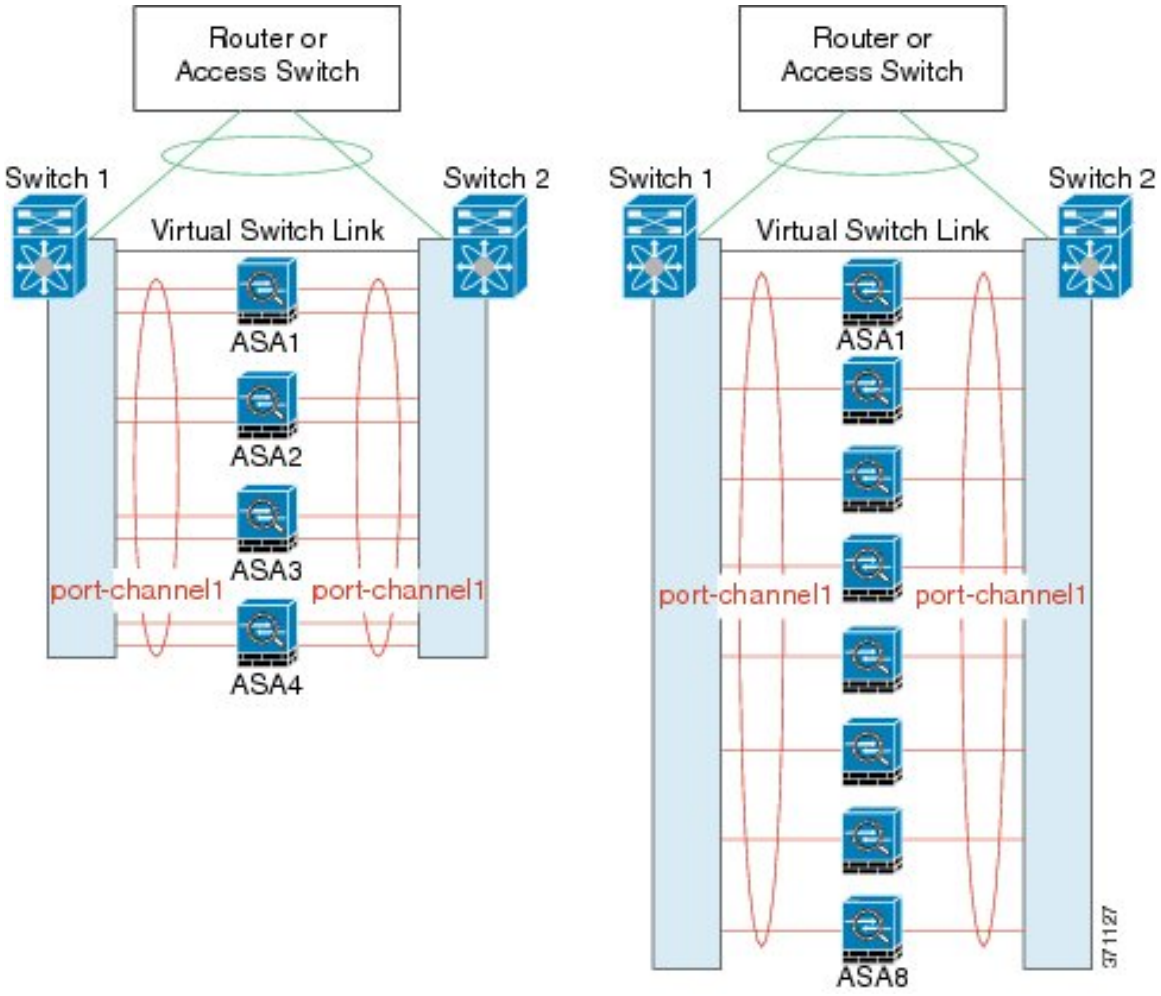
冗長スイッチシステムへの接続

1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS、vPC、StackWise、または StackWise Virtual の両方のスイッチに接続するときです。

スイッチによっては、スパンド EtherChannel に最大 32 個のアクティブ リンクを設定できます。この機能では、vPC 内の両方のスイッチが、それぞれ 16 個のアクティブ リンクの EtherChannel をサポートする必要があります（例：Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。

EtherChannel で 8 個のアクティブリンクをサポートするスイッチの場合、冗長システムで 2 台のスイッチに接続すると、スパンド EtherChannel に最大 16 個のアクティブリンクを設定できます。

次の図では、4 ノードクラスタおよび 8 ノードクラスタでの 16 アクティブリンクのスパンド EtherChannel を示します。

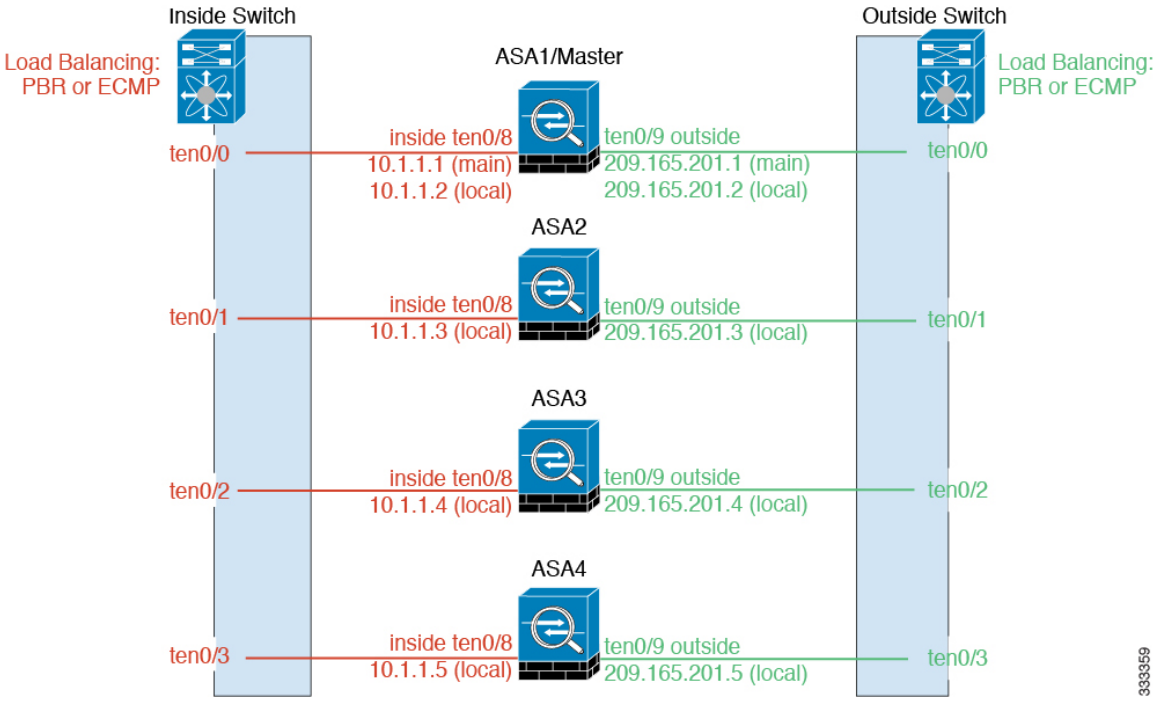


個別インターフェイス（ルーテッド ファイアウォール モードのみ）

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル *IP* アドレスを持ちます。各インターフェイスのメインクラスタ *IP* アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。

インターフェイス コンフィギュレーションは制御ノード上だけで行う必要があるため、IP アドレスプールを設定して、このプールのアドレスがクラスタノード（制御ノード用を含む）の特定のインターフェイスに使用されるようにします。

アップストリームスイッチ上でロードバランシングを別途する必要があります。



ポリシーベース ルーティング

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロードバランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA に分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 ASA をモニタします。これで、PBR は、特定の ASA の到達可能性に基づいてルート マップを有効化または無効化できます。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

等コスト マルチパス ルーティング

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MACアドレスを維持します。ロードバランシング方法の1つが、等コストマルチパス（ECMP）ルーティングです。

この方法が推奨されるのは、すでにECMPを使用しており、既存のインフラストラクチャを活用したい場合です。

ECMPルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannelのように、送信元および宛先のIPアドレスや送信元および宛先のポートのハッシュを使用してネクストホップの1つにパケットを送信できます。ECMPルーティングにスタティックルートを使用する場合は、ASAの障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生したASAへのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA を設定する必要があります。

Cisco Intelligent Traffic Director（ルーテッド ファイアウォール モードのみ）

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。Intelligent Traffic Director（ITD）とは、Nexus 5000、6000、7000 および9000スイッチシリーズの高速ハードウェア ロードバランシング ソリューションです。従来の PBR の機能を完全に網羅していることに加え、簡略化された構成ワークフローを提供し、粒度の細かい負荷分散を実現するための複数の追加機能を備えています。

ITD は、IP スティッキ性、双方向フロー対称性のためのコンシステント ハッシュ法、仮想 IP アドレッシング、ヘルス モニタリング、高度な障害処理ポリシー（N+M 冗長性）、加重ロードバランシング、およびアプリケーション IP SLA プローブ（DNS を含む）をサポートします。ロードバランシングの動的な性質により、PBRに比べて、すべてのクラスタノードでより均一なトラフィック分散を実現します。双方向フロー対称性を実現するために、接続のフォワードおよびリターンパケットが同じ ASA に送信されるように ITD を設定することを推奨します。詳細については、次の URL を参照してください。

https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/itd_deployment/ITD_ASA_Deployment_Guide.pdf

クラスタユニットのケーブル接続とアップストリームおよびダウンストリーム機器の設定

クラスタリングを設定する前に、クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

手順

ステップ 1 クラスタ制御リンク ネットワーク、管理ネットワーク、およびデータ ネットワークをケーブルで接続します。

（注）
クラスタに参加するようにノードを設定する前に、少なくとも、アクティブなクラスタ制御リンクネットワークが必要です。

ステップ 2 アップストリームとダウンストリームの機器も設定する必要があります。たとえば、EtherChannel を使用する場合は、EtherChannel のアップストリーム/ダウンストリーム機器を設定する必要があります。

各ユニットでのクラスタ インターフェイス モードの設定

クラスタリング用に設定できるインターフェイスのタイプは、スパンド EtherChannel と個別インターフェイスのいずれか一方のみです。1 つのクラスタ内でインターフェイス タイプを混在させることはできません。

始める前に

- モードの設定は、クラスタに追加する各 ASA で個別に行う必要があります。
- 管理専用インターフェイスはいつでも、スパンド EtherChannel モードのときでも個別インターフェイス（推奨）として設定できます（スパンド EtherChannel モードのときでも管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。
- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。
- マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのインターフェイス タイプを選択する必要があります。たとえば、トランスペアレント モードとルーテッド モードのコンテキストが混在している場合は、すべてのコンテキストにスパンド EtherChannel モードを使用する必要があります。これが、トランスペアレント モードで許可される唯一のインターフェイス タイプであるからです。

手順

ステップ 1 互換性のないコンフィギュレーションを表示し、強制的にインターフェイス モードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

cluster interface-mode {**individual** | **spanned**} **check-details**

例：

```
ciscoasa(config)# cluster interface-mode spanned check-details
```

ステップ 2 クラスタリング用にインターフェイス モードを設定します。

cluster interface-mode {**individual** | **spanned**} **force**

例：

```
ciscoasa(config)# cluster interface-mode spanned force
```

デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

force オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソールポートに接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

制御ノードでのインターフェイスの設定

クラスタリングを有効にする前に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。他のインターフェイスについては、クラスタリングの有効化の前後で設定できます。すべての設定が新しいクラスタメンバーと同期するように、すべてのインターフェイスを事前に設定することを推奨します。

ここでは、クラスタリング互換となるようにインターフェイスを設定する方法について説明します。データ インターフェイスは、スパンド EtherChannel として設定することも、個別インターフェイスとして設定することもできます。各方式では異なるロードバランシング メカニズムが使用されます。同じコンフィギュレーションで両方のタイプを設定することはできません。ただし、管理インターフェイスは例外で、スパンドEtherChannelモードであっても個別インターフェイスにできます。

個々のインターフェイスを設定する（管理用インターフェイスの場合推奨）

個別インターフェイスは通常のルーテッド インターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に制御ノードに属します。

スパンドEtherChannelモード個別管理インターフェイスならば、必要に応じて各ユニットに直接接続できますが、スパンドEtherChannelインターフェイスでは、制御ノードへの接続しかできません。

始める前に

- 管理専用インターフェイスの場合を除き、個別インターフェイスモードであることが必要です。
- マルチ コンテキスト モードの場合は、この手順を各コンテキストで実行します。まだコンテキスト コンフィギュレーション モードに入っていない場合は、**changeto context** *name* コマンドを入力します。
- 個別インターフェイスの場合は、ネイバー デバイスでのロード バランシングを設定する必要があります。管理インターフェイスには、外部のロードバランシングは必要ありません。
- （オプション）インターフェイスをデバイスローカル EtherChannel インターフェイスとして設定する、およびサブインターフェイスを設定する作業を必要に応じて行います。
  - EtherChannel の場合、この EtherChannel はユニットに対してローカルであり、スパンド EtherChannel ではありません。

手順

ステップ 1 ローカル IP アドレス（IPv4 と IPv6 の一方または両方）のプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタ ユニットに割り当てられます。

（IPv4）

ip local pool *poolname first-address — last-address* [**mask** *mask*]

（IPv6）

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8:45:1002/64 8
```

最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。クラスタを拡張する予定の場合は、アドレスを増やします。現在のプライマリ ユニットに属するメイン クラスタ IP アドレスは、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメイン クラスタ IP アドレス用に確保してください。

各ユニットに割り当てられるローカルアドレスを、事前に正確に特定することはできません。各ユニットで使用されているアドレスを表示するには、**show ip**[**v6**] **local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。

ステップ 2 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface management 1/1
```

ステップ 3 （管理インターフェイスのみ）インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。

management-only

デフォルトでは、管理タイプのインターフェイスは管理専用として設定されます。トランスペアレントモードでは、このコマンドは管理タイプのインターフェイスに対して常にイネーブルになります。

この設定は、クラスタ インターフェイス モードがスパンドの場合に必要です。

ステップ 4 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif management
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 5 メイン クラスタの IP アドレスを設定し、クラスタ プールを指定します。

（IPv4）

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

（IPv6）

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8:45:1002::99/64 cluster-pool insipv6
```

この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。IPv4 アドレスと IPv6 アドレスの一方または両方を設定できます。

DHCP、PPPoE、および IPv6 自動設定はサポートされません。IP アドレスを手動で設定する必要があります。リンクローカルアドレスの手動設定もサポートされていません。

ステップ 6 セキュリティ レベルを設定します。*number* には、0（最低）～ 100（最高）の整数を指定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

ステップ 7 インターフェイスをイネーブルにします。

no shutdown

例

次の例では、イーサネット 1/3 およびイーサネット 1/4 インターフェイスをデバイス ローカル EtherChannel として設定してから、この EtherChannel を個別インターフェイスとして設定します。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface ethernet 1/3
channel-group 1 mode active
no shutdown

interface ethernet 1/4
channel-group 1 mode active
no shutdown

interface port-channel 1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8:45:1002::99/64 cluster-pool mgmtipv6
security-level 100
management-only
```

スパンド EtherChannel の設定

スパンド EtherChannel は、クラスタ内のすべての ASA に広がるものであり、EtherChannel の動作の一部としてロード バランシングを行うことができます。

始める前に

- スパンド EtherChannel インターフェイス モードにする必要があります。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。ブリッジ仮想インターフェイス（BVI）の設定 （937 ページ）を参照してください。
- スパンド EtherChannel を使用している場合、クラスタリングが完全にイネーブルになるまで、ポートチャネル インターフェイスは起動しません。この要件により、クラスタのアクティブではないユニットにトラフィックが転送されるのが防がれます。

手順

ステップ 1 チャネル グループに追加するインターフェイスを指定します。

interface *physical_interface*

例：

```
ciscoasa(config)# interface ethernet 1/1
```

physical_interface ID には、タイプ、スロット、およびポート番号（type slot/port）が含まれます。チャネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。

ステップ 2 EtherChannel にこのインターフェイスを割り当てます。

channel-group *channel_id* **mode active**

例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id は 1 ～ 48 です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合は、自動的に追加されます。

interface port-channel *channel_id*

active モードだけがスパンド EtherChannel に対してサポートされます。

ステップ 3 インターフェイスをイネーブルにします。

no shutdown

ステップ 4 （オプション）EtherChannel にさらにインターフェイスを追加するには、上記のプロセスを繰り返します。

例：

```
ciscoasa(config)# interface ethernet 1/2
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# no shutdown
```

ユニットごとに複数のインターフェイスが EtherChannel に含まれていると、VSS、vPC、StackWise、または StackWise Virtual のスイッチに接続する場合に役立ちます。

ステップ 5 ポートチャネル インターフェイスを指定します。

interface port-channel *channel_id*

例：

```
ciscoasa(config)# interface port-channel 1
```

このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。

ステップ 6 （オプション）このEtherChannel上にVLANサブインターフェイスを作成する予定の場合は、この時点で作成します。

例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 7 （マルチ コンテキスト モード）コンテキストにインターフェイスを割り当てます。その後で、次のとおりに入力します。

changeto context *name*
interface port-channel *channel_id*

例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

マルチ コンテキスト モードの場合は、インターフェイス コンフィギュレーションの残りの部分は各コンテキスト内で行われます。

ステップ 8 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 9 ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード：IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

  （IPv4）

  ip address *ip_address* [*mask*]

  （IPv6）

  ipv6 address *ipv6-prefix*/*prefix-length*

例：

```
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
```

DHCP、PPPoE、および IPv6 自動設定はサポートされません。ポイントツーポイント接続の場合、31 ビットのサブネット マスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。リンクローカルアドレスの手動設定もサポートされていません。

- トランスペアレント モード：インターフェイスをブリッジ グループに割り当てます。

  bridge-group *number*

  例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number は、1 ～ 100 の整数です。ブリッジ グループには最大 64 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジグループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 10 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 11 潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel の固有で、手動のグローバル MAC アドレスを構成します：

mac-address *mac_address*

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

ネットワーク上で現在使用されていない一意の MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在の制御ユニットに留まります。MAC アドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。

非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。

自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ステップ 12 （ルーテッドモード）サイト間クラスタリングの場合、サイトごとにサイト固有の MAC アドレスおよび IP アドレスを設定します。

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

例：

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

サイト固有の IP アドレスは、グローバル IP アドレスと同じサブネット上にある必要があります。ユニットで使用するサイト固有の MAC アドレスおよび IP アドレスは、各ユニットのブートストラップ コンフィギュレーションに指定したサイト ID によって異なります。

ブートストラップ コンフィギュレーションの作成

クラスタ内の各ノードがクラスタに参加するには、ブートストラップ設定が必要です。

制御ノードのブートストラップの設定

クラスタ内の各ノードがクラスタに参加するには、ブートストラップ設定が必要です。一般的には、クラスタに参加するように最初に設定したノードが制御ノードとなります。クラスタリングをイネーブルにした後で、選定期間が経過すると、クラスタの制御ノードが選定されます。最初はクラスタ内に 1 つのノードしかないため、そのノードが制御ノードになります。クラスタに追加する後続のノードはデータノードになります。

始める前に

- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。
- マルチ コンテキスト モードの場合、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- クラスタリングをイネーブルまたはディセーブルにするには、コンソール ポートを使用する必要があります。Telnet または SSH を使用することはできません。

- クラスタ制御リンクを除いて、コンフィギュレーション内のインターフェイスはすべて、クラスタ IP プールを指定して設定されているか、スパンド EtherChannel として設定されている必要があります。この設定は、クラスタリングをイネーブルにする前に、インターフェイス モードに応じて行います。既存のインターフェイス コンフィギュレーションがある場合は、そのインターフェイス コンフィギュレーションをクリアすることも（**clear configure interface**）、インターフェイスをクラスタ インターフェイスに変換することもできます。これは、クラスタリングをイネーブルにする前に行います。
- 稼働中のクラスタにノードを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがありますが、これは想定内の動作です。
- クラスタ制御リンクのサイズをあらかじめ決定しておきます。クラスタ制御リンクのサイジング （424 ページ）を参照してください。

手順

ステップ 1 クラスタに参加する前に、クラスタ制御リンク インターフェイスをイネーブルにします。

後でクラスタリングをイネーブルにするときに、このインターフェイスをクラスタ制御リンクとして識別します。

十分な数のインターフェイスがある場合は、複数のクラスタ制御リンク インターフェイスを結合して 1 つの EtherChannel とすることを推奨します。この EtherChannel は ASA に対してローカルであり、スパンド EtherChannel ではありません。

クラスタ制御リンク インターフェイス コンフィギュレーションは、制御ノードからデータノードには複製されませんが、同じコンフィギュレーションを各ノードで使用する必要があります。このコンフィギュレーションは複製されないため、クラスタ制御リンクインターフェイスの設定は各ノードで個別に行う必要があります。

- VLAN サブインターフェイスをクラスタ制御リンクとして使用することはできません。
- 管理 *x*/*x* インターフェイスをクラスタ制御リンクとして使用することはできません（単独か EtherChannel かにかかわらず）。

a) インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface ethernet 1/6
```

b) （任意、EtherChannel の場合）EtherChannel にこの物理インターフェイスを割り当てます。

channel-group *channel_id* **mode on**

例：

```
ciscoasa(config-if)# channel-group 1 mode on
```

channel_id は 1 ～ 48 です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合は、自動的に追加されます。

interface port-channel *channel_id*

クラスタ制御リンクでの不要なトラフィックを削減できるように、クラスタ制御リンクのメンバー インターフェイスに対しては On モードを使用することを推奨します。クラスタ制御リンクは LACP トラフィックのオーバーヘッドを必要としません。これは隔離された、安定したネットワークであるからです。**注**：データ EtherChannel を Active モードに設定することをお勧めします。

c) インターフェイスをイネーブルにします。

no shutdown

必要があるのはインターフェイスのイネーブル化だけです。インターフェイスの名前などのパラメータを設定しないでください。

d) （EtherChannel の場合）EtherChannel に追加するインターフェイスごとに繰り返します。

例：

```
ciscoasa(config)# interface ethernet 1/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

ステップ 2 クラスタ制御リンクインターフェイスの最大伝送ノードを指定します。データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。

mtu cluster *bytes*

例：

```
ciscoasa(config)# mtu cluster 9198
```

MTU は 1400 ～ 9198 バイトの間で設定しますが、その範囲内でも 2561 ～ 8362 の間には設定しないでください。ブロック プールの処理により、この MTU サイズはシステム動作に最適ではありません。デフォルトの MTU は 1500 バイトです。クラスタ制御リンクの MTU を最大値。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。

たとえば、最大 MTU は 9198 バイトであるため、データインターフェイスの最大 MTU は 9098 になり、クラスタ制御リンクは 9198 に設定できます。

このコマンドはグローバル コンフィギュレーション コマンドですが、ノード間で複製されないブートストラップ コンフィギュレーションの一部でもあります。

クラスタに参加したノードは、クラスタ制御リンクMTUと一致するパケットサイズで制御ノードにpingを送信することでMTUの互換性をチェックします。pingが失敗すると、通知が生成されるため、接続スイッチのMTU不一致を修正して再試行することができます。

ステップ3 クラスタに名前を付け、クラスタ コンフィギュレーション モードにします。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

名前は1～38文字のASCII文字列であることが必要です。ノードごとに設定できるクラスタグループは1つだけです。クラスタのすべてのメンバが同じ名前を使用する必要があります。

ステップ4 クラスタのこのメンバの名前を指定します。

local-unit *unit_name*

1～38文字の一意のASCII文字列を使用します。各ノードには一意の名前が必要です。クラスタ内の他のノードと同じ名前を付けることはできません。

例：

```
ciscoasa(cfg-cluster)# local-unit node1
```

ステップ5 クラスタ制御リンク インターフェイス（EtherChannelを推奨）を指定します。

cluster-interface *interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

サブインターフェイスと管理インターフェイスは許可されません。

IPアドレスにはIPv4アドレスを指定します。IPv6は、このインターフェイスではサポートされません。このインターフェイスには、**nameif** を設定することはできません。

ノードごとに、同じネットワーク上の異なるIPアドレスを指定します。

ステップ6 （ルーテッドモード、スパンドEtherChannelモード）サイト間クラスタリングを使用している場合、次のようにこのノードのサイトIDを設定し、サイト固有のMACアドレスが使用されるようにします。

site-id *number*

例：

```
ciscoasa(cfg-cluster)# site-id 1
```

number には、1～8の範囲内の値を入力します。

ステップ 7 制御ノードの選択に対するこのノードのプライオリティを設定します。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 1
```

プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。

ステップ 8 （オプション）クラスタ制御リンクの制御トラフィックの認証キーを設定します。

key *shared_secret*

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このコマンドは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

ステップ 9 （オプション）cLACP システム ID およびシステムのプライオリティを手動で指定します。

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

例：

```
ciscoasa(cfg-cluster)# clacp system-mac 000a.0000.aaaa
```

スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。cLACP ネゴシエーションの際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの（仮想）デバイスであるかのように見えます。cLACP ネゴシエーションのパラメータの 1 つであるシステム ID は、MAC アドレスの形式をとります。クラスタ内のすべての ASA が同じシステム ID を使用します。これは制御ノードによって自動生成され（デフォルト）、すべてのセカンダリノードに複製されます。あるいは、このコマンドに *H.H.H* の形式で手動で指定することもできます。H は 16 ビットの 16 進数です。（たとえば、MAC アドレス 00-0A-00-00-AA-AA は、000A.0000.AAAA と入力します）。トラブルシューティングの目的で、たとえば、識別が容易な MAC アドレスを使用できるように、手動で MAC アドレスを設定することがあります。一般的には、自動生成された MAC アドレスを使用します。

システムプライオリティ（1 ～ 65535）は、どのノードがバンドルの決定を行うかを決めるために使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。

このコマンドは、ブートストラップ設定の一部ではなく、制御ノードからデータノードに複製されます。ただし、クラスタリングをイネーブルにした後は、この値は変更できません。

ステップ 10 クラスタリングをイネーブルにします。

enable [**noconfirm**]

例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

enable コマンドが入力されると、ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルト コンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するように求められます。応答として **No** を入力した場合は、クラスタリングはイネーブルになりません。確認を省略し、互換性のないコマンドを自動的に削除するには、**noconfirm** キーワードを使用します。

最初にイネーブルにしたノードについては、制御ノード選定が発生します。これまでは最初のノードがクラスタの唯一のメンバーである必要があるため、これが制御ノードになります。この期間中にコンフィギュレーション変更を実行しないでください。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注）
クラスタリングをディセーブルにした場合は、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスだけがアクティブになります。

例

次の例では、管理インターフェイスを設定し、クラスタ制御リンク用のデバイスローカル EtherChannel を設定し、その後で、「node1」という名前の ASA のクラスタリングをイネーブルにします。これは最初にクラスタに追加されるノードであるため、制御ノードになります。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/32 8
interface management 1/1
   nameif management
   ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
   ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
   security-level 100
   management-only
   no shutdown
```

```
interface ethernet 1/6
   channel-group 1 mode on
   no shutdown

interface ethernet 1/7
   channel-group 1 mode on
   no shutdown

cluster group pod1
   local-unit node1
   cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
   priority 1
   key chuntheunavoidable
   enable noconfirm
```

データノードのブートストラップの設定

データノードを設定するには、次の手順に従います。

始める前に

- クラスタリングをイネーブルまたはディセーブルにするには、コンソールポートを使用する必要があります。Telnet または SSH を使用することはできません。
- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- コンフィギュレーション内に、クラスタリング用として設定されていないインターフェイスがある場合は（たとえば、デフォルト コンフィギュレーションの管理 1/1 インターフェイス）、データノードとしてクラスタに参加させることができます（現在の選定で制御ノードになる可能性はありません）。
- 稼働中のクラスタにノードを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがありますが、これは想定内の動作です。

手順

ステップ 1 制御ノードに設定したものと同じクラスタ制御リンクインターフェイスを設定します。

例：

```
ciscoasa(config)# interface ethernet 1/6
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
ciscoasa(config)# interface ethernet 1/7
ciscoasa(config-if)# channel-group 1 mode on
ciscoasa(config-if)# no shutdown
```

ステップ 2 制御ノードに設定したものと同じ MTU を指定します。

例：

```
ciscoasa(config)# mtu cluster 9198
```

クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。

ステップ 3 制御ノードに設定したものと同じクラスタ名を指定します。

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 4 クラスタのこのメンバに一意の文字列で名前を指定します。

local-unit *unit_name*

例：

```
ciscoasa(cfg-cluster)# local-unit node2
```

1 ～ 38 文字の ASCII 文字列を指定します。

各ノードには一意の名前が必要です。クラスタ内の他のノードと同じ名前を付けることはできません。

ステップ 5 制御ノードに設定したものと同じクラスタ制御リンクインターフェイスを指定しますが、ノードごとに同じネットワーク上の異なる IP アドレスを指定します。

cluster-interface *interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface port-channel2 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on Port-Channel2
```

IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。このインターフェイスには、**nameif** を設定することはできません。

ステップ 6 （ルーテッドモード、スパンド EtherChannel モード）サイト間クラスタリングを使用している場合、次のようにこのノードのサイト ID を設定し、サイト固有の MAC アドレスが使用されるようにします。

site-id *number*

例：

```
ciscoasa(cfg-cluster)# site-id 1
```

number は 1 ～ 8 です。

ステップ 7 制御ノードの選定に対するこのノードのプライオリティを設定します。通常は、制御ノードより高い値にします。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 2
```

プライオリティを 1 ～ 100 に設定します。1 が最高のプライオリティです。

ステップ 8 制御ノードに設定したものと同じ認証キーを設定します。

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

ステップ 9 クラスタリングをイネーブルにします。

enable as-data-node

enable as-data-node コマンドを使用することによって、設定に関するすべての非互換性（主にまだクラスタリング用に設定されていないインターフェイスの存在）を回避できます。このコマンドを実行すると、クラスタに参加させるデータノードが現在の選定において制御ノードとなる可能性をなくすことができます。データノードのコンフィギュレーションは、制御ノードから同期されたコンフィギュレーションによって上書きされます。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注）
クラスタリングをディセーブルにした場合は、すべてのデータインターフェイスがシャットダウンされ、管理インターフェイスだけがアクティブになります。

例

次の例には、データノード node2 の設定が含まれています。

```
interface ethernet 1/6

channel-group 1 mode on
no shutdown

interface ethernet 1/7

channel-group 1 mode on
no shutdown

cluster group pod1

local-unit node2
```

```
cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

クラスタリング動作のカスタマイズ

クラスタリング ヘルス モニタリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

制御ノードで次の手順を実行します。

ASA クラスタの基本パラメータの設定

制御ノード上のクラスタ設定をカスタマイズできます。

始める前に

- マルチコンテキストモードでは、制御ノード上のシステム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （任意） データノードから制御ノードへのコンソール複製を有効にします。

console-replicate

この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート 1 つだけです。

ステップ 3 クラスタリング イベントの最小トレース レベルを設定します。

trace-level *level*

必要に応じて最小レベルを設定します。

- **critical**：クリティカル イベント（重大度 = 1）
- **warning**：警告（重大度 = 2）
- **informational**：情報イベント（重大度 = 3）
- **debug**：デバッグ イベント（重大度 = 4）

ステップ 4 フローオーナーからディレクタおよびバックアップオーナーへのフロー状態更新メッセージ（clu_keepalive および clu_update メッセージ）のキープアライブ間隔を設定します。

clu-keepalive-interval *seconds*

- *seconds*：15 ～ 55。デフォルトは 15 です。

クラスタ制御リンクのトラフィック量を減らすために、デフォルトよりも長い間隔を設定することもできます。

のヘルス モニタリングおよび自動再結合の設定

この手順では、ノードとインターフェイスのヘルスモニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。任意のポート チャネル ID、冗長 ID、単一の物理インターフェイス ID、をモニターできます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

ステップ 2 クラスタノードのヘルスチェック機能をカスタマイズします。

health-check [**holdtime** *timeout*] [**vss-enabled**]

ノードのヘルスを確認するため、ASA のクラスタノードはクラスタ制御リンクで他のノードにハートビート メッセージを送信します。ノードが保留時間内にピアノードからハートビート メッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。

- **holdtime** *timeout*：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は .3 ～ 45 秒で、デフォルトは 3 秒です。
- **vss-enabled**：クラスタ制御リンクのすべての EtherChannel インターフェイスでハートビート メッセージをフラッディングして、少なくとも 1 台のスイッチがそれを受信できるようにします。EtherChannel としてクラスタ制御リンクを設定し（推奨）、VSS、vPC、StackWise、または vPC StackWise Virtual ペアに接続している場合、**vss-enabled** オプションをイネーブルにする必要がある場合があります。一部のスイッチでは、冗長システムの 1 つのノードがシャットダウンまたは起動すると、そのスイッチに接続された EtherChannel

メンバーインターフェイスが ASA に対してアップ状態であるように見えますが、これらのインターフェイスはスイッチ側のトラフィックを通していません。ASA holdtime timeout を低い値（0.8 秒など）に設定した場合、ASA が誤ってクラスタから削除される可能性があり、ASA はキープアライブ メッセージをこれらのいずれかの EtherChannel インターフェイスに送信します。

何らかのトポロジ変更（たとえばデータインターフェイスの追加/削除、ASA、またはスイッチ上のインターフェイスの有効化/無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイス ヘルス チェックを無効化します。

no health-check monitor-interface *interface_id*

インターフェイスのヘルスチェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のノード上では障害が発生したが、別のノード上の同じ論理インターフェイスでアクティブポートがある場合、そのノードはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブル（無効）にすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。

- *interface_id*：ポートチャネル ID と冗長 ID、または単一の物理インターフェイス ID のモニタリングを無効にします。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、またはスイッチ上のインターフェイスの有効化/無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし（**no health-check**）、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

ステップ 4 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**：内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
- **unlimited**：（**cluster-interface** のデフォルト）再結合の試行回数を制限しません。
- *auto-rejoin-max*：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。**data-interface** と **system** のデフォルトは 3 です。
- *auto_rejoin_interval*：再結合試行の間隔を 2 ～ 60 の範囲の分単位で定義します。デフォルト値は 5 分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- *auto_rejoin_interval_variation*：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の 2 倍、**3**：直前の間隔の 3 倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタ インターフェイスの場合は **1**、データ インターフェイスおよびシステムの場合は **2** です。

例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

ステップ 5 ASA がインターフェイスを障害が発生していると見なし、クラスタからノードが削除されるまでのデバウンス時間を設定します。

health-check monitor-interface debounce-time *ms*

例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

デバウンス時間は 300 ～ 9000 ms の範囲の値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからノードを削除するまで指定されたミリ秒数待機します。EtherChannel がダウン状態からアップ状態に移行する場合（スイッチがリロードされた、スイッチで EtherChannel が有効になったなど）、デバウンス時間がより長くなり、ポートのバンドルにおいて別のクラスタノードの方が高速なため、クラスタノードでインターフェイスの障害が表示されることを妨げることがあります。

ステップ 6 （任意）トラフィック負荷のモニタリングを設定します。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds*：モニタリングメッセージ間の時間を、10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。

- **intervals** *intervals*： ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

クラスタメンバのトラフィック負荷をモニターできます。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのノードが負荷を処理できる場合は、ノードのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティモジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティモジュールがクラスタを離れると、そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ノードでクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 25 interval:
   0           0            0            12             28
   1           0            0            13             27
```

例

次の例では、ヘルスチェック保留時間を .3 秒に設定し、VSS を有効にし、管理に使用されるイーサネット 1/2 インターフェイスのモニタリングを無効にし、データインターフェイスの自動再結合の試行回数を 2 分から開始して前回の間隔の 3 倍増加させる計 4 回に設定し、クラスタ制御リンクの自動再結合の試行回数を 2 分おきの計 6 回に設定しています。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3 vss-enabled
ciscoasa(cfg-cluster)# no health-check monitor-interface ethernet1/2
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

接続の再分散およびクラスタ TCP 複製の遅延の設定

接続の再分散を設定できます。詳細については、新しい TCP 接続のクラスタ全体での再分散（522 ページ）を参照してください。

TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップフローが作成される前にノードが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のノードに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 TCP 接続のクラスタ複製の遅延を有効化します。

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

1 ～ 15 の範囲で秒数を設定します。**http** 遅延はデフォルトで 5 秒間有効になります。

マルチ コンテキスト モードで、コンテキスト内でこの設定を行います。

ステップ 2 クラスタの設定モードを開始します。

cluster group *name*

ステップ 3 （オプション）TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合、ASA は、1 秒あたりの接続数に関する情報を定期的に交換し、新しい接続を、1 秒あたりの接続数が多いデバイスから低負荷のデバイスにオフロードします。既存の接続は移動されません。さらに、このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。

サイト間機能の設定

サイト間クラスタリングの場合、冗長性と安定性を高めるために、設定をカスタマイズできます。

ディレクタ ローカリゼーションの有効化

データセンターのサイト間クラスタリングのパフォーマンスを向上させ、ラウンドトリップ時間を短縮するために、ディレクターローカリゼーションをイネーブルにすることができます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASAは任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバルディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。
- 次のトラフィック タイプは、ローカリゼーションをサポートしていません：NAT および PAT トラフィック、SCTP 検査されたトラフィック、フラグメンテーション所有クエリ。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 ディレクタ ローカリゼーションをイネーブルにします。

director-localization

サイト冗長性の有効化

サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 サイトの冗長性を有効にします。

site-redundancy

サイトごとの Gratuitous ARP の設定

ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。

クラスタから送信されたサイトごとのMACおよびIPアドレスとパケットがサイト固有のMACアドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。GARP 間隔をカスタマイズするか、または GARP を無効にすることができます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。

- 制御ユニット設定では、スパンド EtherChannel のサイトごとの MAC アドレスを設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 GARP 間隔をカスタマイズします。

site-periodic-garp interval *seconds*

- *seconds*：GARP 生成の間隔を 1 ～ 1000000 秒間の秒単位で設定します。デフォルトは 290 秒です。

GARP を無効にするには、**no site-periodic-garp interval** を入力します。

クラスタ フロー モビリティの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

LISP インスペクションについて

LISP トラフィックを検査することで、サイト間のフローのモビリティを有効にできます。

LISP について

VMware VMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンター サーバ モビリティをサポートするには、サーバの移動時にサーバへの入力ルートをルータが更新できる必要があります。Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID、つまりエンドポイント ID（EID）をその場所、つまりルーティング ロケータ（RLOC）から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

LISP では、LISP の出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、ファースト ホップ ルータ、マップ リゾルバ（MR）、およびマップ サーバ（MS）などのある一定のロールにおいてルータとサーバが必要です。サーバが別のルータに接続されていることをサーバのファースト ホップ ルータが感知すると、そのルータは他のすべてのルータとデータベースを

更新し、クライアントに接続されているITRがトラフィックを代行受信してカプセル化し、新しいサーバの場所に送信できるようにします。

ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISPの統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフローオーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーニング」または「ヘアピニング」と呼ばれます。

LISP 統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR 間でやり取りされる LISP トラフィックを検査し、フローの所有者を新しいサイトに変更できます。

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。
- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々のノードに属しているフローは新しいオーナーには移動されません。半分散されたフローにはSIPなどのアプリケーションが含まれており、親フローとそのすべての子フローが同じ ASA によって所有されます。
- クラスタはレイヤ 3 および 4 のフロー状態を移動させるだけです。一部のアプリケーション データが失われる可能性があります。
- 短時間のフローまたはビジネスに不可欠でないフローの場合、オーナーの移動は有用でない可能性があります。インスペクション ポリシーを設定するときに、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

ASA LISP の実装

この機能には、複数の相互に関係する設定が含まれています（それらについてはすべてこの章で説明します）。

1. （任意）ホストまたはサーバ IP アドレスに基づく検査対象 EID の制限：ファースト ホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。
2. LISP トラフィック インスペクション：ASA は、ファーストホップルータと ITR または ETR の間で送信される EID 通知メッセージにおいて、UDP ポート 4342 上の LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持しま

す。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。LISP トラフィックにはディレクタが割り当てられておらず、LISP トラフィック自体はクラスタ状態の共有に参加しないことに注意してください。

3. 指定されたトラフィック上のフロー モビリティを有効にするサービス ポリシー：フロー モビリティはビジネスクリティカルなトラフィックに対して有効にする必要があります。たとえば、フロー モビリティを HTTPS トラフィックおよび/または特定のサーバへのトラフィックのみに制限できます。

4. サイト ID：ASA は、各クラスタノードのサイト ID を使用して新しいオーナーを特定します。

5. フローモビリティをイネーブルにするためのクラスタレベル設定：フローモビリティは、クラスタ レベルでも有効にする必要があります。このオン/オフ トグルを使用すると、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP インスペクションの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

始める前に

- 制御ノードのブートストラップの設定 （439 ページ） および データノードのブートストラップの設定 （445ページ） に従って、各クラスタユニットをサイト ID に割り当てます。
- LISP のトラフィックはデフォルト インスペクション トラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

手順

ステップ 1 （任意） LISP インスペクション マップを設定して、IP アドレスに基づいて検査済みの EID を制限し、LISP の事前共有キーを設定します。

a) 拡張 ACL を作成します。宛先 IP アドレスのみが EID 組み込みアドレスと照合されます。

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) LISP インスペクション マップを作成し、パラメータ モードに移行します。

policy-map type inspect lisp *inspect_map_name*

parameters

c) 作成した ACL を識別して、許可された EID を定義します。

allowed-eid access-list *eid_acl_name*

ファースト ホップ ルータまたは ITR/ETR は、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信することがあります。このため、クラスタに関連するサーバーまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

d) 必要に応じて、事前共有キーを入力します。

validate-key *key*

例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

ステップ 2 ファースト ホップ ルータとポート 4342 の ITR または ETR の間の UDP トラフィック の LISP インスペクションの設定。

a) 拡張 ACL を設定して LISP のトラフィックを特定します。

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

UDP ポート 4342 を指定する必要があります。IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) ACL のクラス マップを作成します。

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) ポリシー マップ、クラス マップを指定し、オプションの LISP インスペクション マップを使用してインスペクションを有効化し、サービス ポリシーをインターフェイスに適用します（新規であれば）。

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

既存のサービス ポリシーある場合は、既存のポリシー マップ名を指定します。デフォルトで、ASA には **global_policy** と呼ばれるグローバル ポリシーが含まれているため、グローバル ポリシーの名前を指定します。ポリシーをグローバルに適用しない場合は、インターフェイスごとに 1 つのサービス ポリシーを作成することもできます。LISP インスペクショ

ンは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービス ポリシーを適用する必要はありません。トラフィックが両方向のクラス マップに一致する場合、ポリシーマップを適用するインターフェイスに入るまたは存在するトラフィックのすべてが影響を受けます。

例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASAは、ファースト ホップ ルータと ITR または ETR の間で送信される EID 通知メッセージの LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。

ステップ 3 トラフィック クラスのフロー モビリティを有効化します。

a) 拡張 ACL を設定して、サーバーがサイトを変更するときに、最適なサイトに再割り当てするビジネス クリティカルなトラフィックを特定します。

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。フロー モビリティは、ビジネスクリティカルなトラフィックに対してイネーブルにする必要があります。たとえば、フロー モビリティを HTTPS トラフィックのみ、または特定のサーバへのトラフィックのみに制限できます。

b) ACL のクラス マップを作成します。

class-map *flow_map_name*

match access-list *flow_acl_name*

c) LISP インスペクションを有効化した同じポリシー マップ、フロー クラス マップを指定して、フロー モビリティを有効にします。

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0
255.255.255.0 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
```

```
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

ステップ 4 クラスタ グループ コンフィギュレーション モードに移行し、クラスタのフローのモビリティを有効化します。

cluster group *name*

flow-mobility lisp

このオン/オフの切り替えにより、フロー モビリティの有効化や無効化を簡単に行えます。

例

次に例を示します。

- EID を 10.10.10.0/24 ネットワーク上の EID に制限します。
- 192.168.50.89（内部）にある LISP ルータと 192.168.10.8（別の ASA インターフェイス上）にある ITR または ETR ルータの間の LISP トラフィック（UDP 4342）を検査します。
- HTTPS を使用して 10.10.10.0/24 のサーバーに送信されるすべての内部トラフィックに対してフロー モビリティを有効化します。
- クラスタに対してフロー モビリティをイネーブルにします。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

分散型サイト間 VPN の設定

デフォルトでは、クラスタは集中型のサイト間 VPN モードを使用します。クラスタリングの拡張性を活用するために、分散型サイト間 VPN モードを有効にできます。

分散型サイト間 VPN について

この分散モードでは、サイト間 IPsec IKEv2 VPN 接続がクラスタのノード全体に分散されます。VPN接続をクラスタのノード間に分散させると、クラスタのキャパシティとスループットの両方を最大限に活用できるため、集中型 VPN 機能を超えて VPN サポートを大幅に拡張できます。

分散型 *VPN* 接続の役割

分散型 VPN モードで実行すると、次の役割がクラスタ ノードに割り当てられます。

- アクティブセッション オーナー：最初に接続を受信したノード、またはバックアップセッションをアクティブ セッションに移行したノード。オーナーは、IKE と IPsec トンネル、およびそれらに関連付けられたすべてのトラフィックを含む、完全なセッションの状態を維持し、パケットを処理します。
- バックアップ セッション オーナー：既存のアクティブ セッションのバックアップ セッションを処理しているノード。アクティブセッション オーナーに障害が発生すると、バックアップ セッション オーナーがアクティブ セッション オーナーになり、新しいバックアップ セッションが別のノードで確立されます。
- フォワーダ：VPN セッションに関連付けられたトラフィックが VPN セッションを所有していないノードに送信された場合、そのノードは VPN セッションを所有しているノードにトラフィックを転送するために っクラスター制御リンクを使用します。
- オーケストレータ：オーケストレータ（常にクラスタ制御ノード）は、アクティブセッションの再配布（ASR）を実行する際に、移動するセッションとその移動先を計算する役割があります。オーケストレータは、オーナー ノード X に N セッションをメンバー Y に移動する要求を送信します。ノード X は、完了時に移動できたセッション数を指定して、オーケストレータに応答を返します。

分散型 *VPN* セッションの特性

分散型サイト間 VPN セッションには、次の特性があります。それ以外の場合、VPN 接続は、クラスタ上にない場合に通常動作するように動作します。

- VPN セッションは、セッション レベルでクラスタ全体に分散されます。つまり、1 つの VPN 接続に対し、同じクラスタ ノードが IKE および IPsec トンネルと、そのすべてのトラフィックを処理します。VPN セッション トラフィックが、その VPN セッションを所有していないクラスタ ノードに送信された場合、トラフィックは VPN セッションを所有しているクラスタ ノードに転送されます。
- VPN セッションには、クラスタ全体で一意のセッション ID があります。セッション ID を使用して、トラフィックが検証され、転送の決定が行われ、IKE ネゴシエーションが完了します。

- サイト間 VPN ハブ アンド スポーク構成では、クライアントがクラスタを介して接続する場合（ヘアピニングと呼ばれる）、流入するセッション トラフィックと流出するセッション トラフィックは、異なるクラスタ ノード上にある可能性があります。

クラスタ イベントの分散型 *VPN* の処理

イベント	分散型 VPN
ノード障害	この障害が発生したノード上のすべてのアクティブ セッションに対し、（別のノード上の）バックアップセッションがアクティブになり、バックアップ セッションは別のノードに再割り当てされます。
クラスタ ノードの非アクティブ化	非アクティブになっているクラスタ ノード上のすべてのアクティブ セッションに対し、（別のノード上の）バックアップセッションがアクティブになり、バックアップ戦略に従って別のノードにバックアップセッションを再割り当てします。
クラスタ ノードの参加	新しいノードの VPN クラスタモードが分散型に設定されていない場合、制御ノードはモード変更を要求します。 VPN モードに互換性があった後で、クラスタ ノードには、通常の操作の流れでアクティブ セッションとバックアップ セッションが割り当てられます。

IPsec IKEv2 の変更

IKEv2 は、分散型サイト間 VPN モードでは次のように変更されます。

- IP/ポート タプルの代わりに ID が使用されます。これにより、パケットの適切な転送の決定、および他のクラスタ メンバー上にある可能性がある以前の接続のクリーンアップが可能になります。
- 単一の IKEv2 セッションを識別する（SPI）識別子は、ローカルで生成されたランダムな 8 バイトの値で、クラスタ全体で一意です。SPI には、タイム スタンプとクラスタ ノード ID が埋め込まれています。IKE ネゴシエーション パケットの受信時に、タイム スタンプまたはクラスタ ノード ID のチェックに失敗すると、パケットがドロップされ、理由を示すメッセージが記録されます。
- NAT-T ネゴシエーションがクラスタ メンバー間で分割されることによって失敗しないように IKEv2 処理が変更されました。新しい ASP 分類ドメインである *cluster_isakmp_redirect*、およびルールは、IKEv2 がインターフェイスで有効になっている場合に追加されます。**show asp table classify domain cluster_isakmp_redirect** コマンドを使用して、ルールを参照します。

CMPv2

CMPv2 ID 証明書とキーペアはクラスター ノード間で同期されます。ただし、クラスター内の制御ノードのみが CMPv2 証明書を自動的に更新してキーの再生成を行います。制御ノードは更新時に、これらの新しい ID 証明書とキーをすべてのクラスター ノードに同期させます。こ

のようにして、クラスター内のすべてのノード メンバーは CMPv2 証明書を利用して認証を行い、また、すべてのノードが制御ノードを継承することができます。

分散型サイト間 VPN のライセンシング

キャリア ライセンスは、クラスターの各メンバーで、分散型サイト間 VPN に必要です。

各 VPN 接続には、2 つの *Other VPN* ライセンス済みセッションが必要です（*Other VPN* ライセンスは*Essentials*ライセンスの一部です）。1 つはアクティブセッション用、もう 1 つはバックアップ セッション用です。クラスタの最大 VPN セッション容量は、セッションごとに 2 つのライセンスを使用するため、ライセンス済み容量の半分以下にすることができます。

分散型サイト間 VPN の前提条件

モデルのサポート

- Cisco Secure Firewall 4200

クラスタの要件

- スパンド EtherChannel モード。
- ルーテッド ファイアウォール モード。

分散型サイト間 VPN のガイドライン

ファイアウォールモード

分散型サイト間 VPN は、ルーテッド モードでのみサポートされています。

コンテキスト モード

分散型サイト間 VPN は、シングル コンテキスト モードおよびマルチ コンテキスト モードの両方で動作します。ただし、マルチ コンテキスト モードでは、アクティブ セッションの再配布はコンテキスト レベルではなくシステム レベルで行われます。これにより、コンテキストに関連付けられたアクティブセッションが、異なるコンテキストに関連付けられたアクティブセッションを含むクラスタ メンバーに移動し、予期せずに持続不可能な負荷が発生するのを防ぎます。

サポートされていないインスペクション

次のタイプの検査は、分散型サイト間 VPN モードではサポートされていないか、または無効になっています。

- CTIQBE
- DCERPC
- H323、H225、および RAS
- IPSec パススルー

- MGCP
- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP（Skinny）
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

その他のガイドライン

- 分散型サイト間VPNモードではIKEv2 IPsecサイト間VPNのみがサポートされています。IKEv1 はサポートされていません。IKEv1 サイト間は、集中型 VPN モードでサポートされています。
- サイト間クラスタリングはサポートされていません。
- ダイナミック PAT は、分散型サイト間 VPN モードでは使用できません。

分散型サイト間 VPN を有効にします

分散型サイト間VPNを有効にして、VPNセッションのクラスタリングの拡張性を活用します。

（注） 集中型または分散型の間でVPNモードを変更するには、クラスタ内のすべてのノードをリロードする必要があります。

始める前に

『VPN Configuration Guide』に従って、サイト間 VPN を設定します。

手順

制御ノードの分散型サイト間 VPN を有効にします。

vpn-mode distributed

リロードするよう求められます。このコマンドは、リロード前にすべてのデータノードに複製されます。クラスタ内のすべてのノードがリロードされます。

分散型サイト間 VPN を無効にするには、 **vpn-mode centralized** コマンドを使用します。

例：

```
ciscoasa(cfg-cluster)# vpn-mode distributed
WARNING: Do you want to proceed with changing the vpn-mode, save the device configuration,
and initiate a reboot? [confirm]
```

分散型 S2S VPN セッションの再配布

アクティブ セッションの再配布（ASR）では、アクティブな VPN セッションの負荷がクラスタ メンバー全体に再配布されます。セッションの開始と終了の動的な性質のため、ASR は、すべてのクラスタ メンバー間でセッションのバランスを取るためのベスト エフォートです。繰り返される再配布アクションによってバランスが最適化されます。

再配布はいつでも実行でき、クラスタ内のトポロジ変更後に実行する必要があります。また、新しいメンバーがクラスタに参加した後に実行することを推奨します。再配布の目的は、安定した VPN クラスタを作成することです。安定した VPN クラスタには、ノード間でほぼ同数のアクティブ セッションとバックアップ セッションがあります。

セッションを移動するには、バックアップ セッションがアクティブ セッションになり、別のノードが新しいバックアップ セッションをホストするように選択されます。移動セッションは、アクティブ セッションのバックアップの場所と、その特定のバックアップ ノード上にすでに存在するアクティブセッションの数に依存します。何らかの理由でバックアップセッション ノードがアクティブセッションをホストできない場合、元のノードはセッションのオーナーのままです。

マルチコンテキスト モードでは、アクティブ セッションの再配布は、個々のコンテキスト レベルではなくシステム レベルで行われます。コンテキスト レベルで実行されない理由は、あるコンテキスト内のアクティブセッションが別のコンテキスト内のより多くのアクティブセッションを含むメンバーに移動され、そのクラスタ メンバーに多くの負荷がかかるためです。

始める前に

- 再配布アクティビティをモニターする場合は、システム ログを有効にします。
- この手順は、クラスタの制御ユニットで実行する必要があります。

手順

ステップ 1 制御ノード上でアクティブ セッションとバックアップ セッションがクラスタ全体でどのように配布されているかを表示します。

show cluster vpn-sessiondb distribution

例：

配布情報は次のように表示されます。

```
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

各行には、メンバー ID、メンバー名、アクティブ セッション数、およびバックアップ セッションが存在するメンバーが含まれています。上記の例では、次のように情報が読み取れます。

- メンバー 0 には 209 のアクティブ セッションがあり、111 のセッションはメンバー 1 にバックアップされ、98 のセッションはメンバー 2 にバックアップされます。
- メンバー 1 には 204 のアクティブ セッションがあり、108 のセッションはメンバー 0 にバックアップされ、96 のセッションはメンバー 2 にバックアップされます。
- メンバー 2 にはアクティブ セッションがないため、クラスタ メンバーはこのノードのセッションをバックアップしていません。このメンバーは最近クラスタに参加しました。

ステップ 2 セッションを再配布します。

cluster redistribute vpn-sessiondb

このコマンドは、バックグラウンドで実行中に即座に戻ります（メッセージなしで）。

再配布するセッションの数とクラスタの負荷に応じて、これには時間がかかることがあります。再配布アクティビティが発生すると、次のフレーズ（およびここには表示されていない他のシステムの詳細）を含む Syslog が提供されます。

Syslog フレーズ	注
VPN session redistribution started	制御ノードのみ
Sent request to move *number* sessions from *orig-member-name* to *dest-member-name*	制御ノードのみ
Failed to send session redistribution message to *member-name*	制御ノードのみ
Received request to move *number* sessions from *orig-member-name* to *dest-member-name*	データ ノードのみ
Moved *number* sessions to *member-name*	名前付きクラスタに移動したアクティブ セッションの数。
Failed to receive session move response from *dest-member-name*	制御ノードのみ
VPN session completed	制御ノードのみ
Cluster topology change detected. VPN session redistribution aborted.	

ステップ 3 **show cluster vpn-sessiondb distribution** コマンドを再入力して結果を表示します。

クラスタノードの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタノードを管理できます。

非アクティブノードになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのノード上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのノードをクラスタから完全に削除します。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

no enable

このノードが制御ノードであった場合は、新しい制御ノードの選定が実行され、別のメンバーが制御ノードになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

ノードの非アクティブ化

ログインしているノード以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASA が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

クラスタからノードを削除します。

cluster remove unit *node_name*

ブートストラップ コンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ノードがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各ノードの現在のコンフィギュレーションは（アクティブユニットから同期されて）同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IPアドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

始める前に

コンソールポートを使用する必要があります。クラスタのコンフィギュレーションを削除すると、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスがシャットダウンされます。さらに、クラスタリングのイネーブルまたはディセーブルを、リモートCLI接続から行うことはできません。

手順

ステップ1 データノードの場合、クラスタリングを次のように無効化します。

cluster group *cluster_name* **no enable**

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがデータノード上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ2 クラスタ コンフィギュレーションをクリアします。

clear configure cluster

ASAは、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ3 クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ4 バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy *backup_cfg* **running-config**

例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config
```

```
Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

ステップ 5 コンフィギュレーションをスタートアップに保存します。

write memory

ステップ 6 バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

制御ノードの変更

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

新しいノードを制御ノードとして設定します。

cluster control-node unit*node_name*

例：

```
ciscoasa(config)# cluster control-node unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバー名を表示するには、**cluster control-node unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのノードに、または特定のノードに送信するには、次の手順を実行します。**show** コマンドをすべてのノードに送信すると、すべての出力が収集されて現在のノードのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

手順

すべてのノードにコマンドを送信します。ノード名を指定した場合は、特定のノードに送信します。

cluster exec [**unit** *node_name*] コマンド

例：

```
ciscoasa# cluster exec show xlate
```

ノード名を表示するには、**cluster exec unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャファイルをクラスタ内のすべてのノードから同時に TFTP サーバにコピーするには、制御ノードで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ノードから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にノード名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 と asa2 はクラスタノード名です。

次の例では、**cluster exec show port-channel summary** コマンドの出力に、クラスタの各ノードの EtherChannel 情報が表示されています。

```
ciscoasa# cluster exec show port-channel summary
control node(LOCAL):**************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster  Ports
------+-------------+----------+-----------------------------------------------
1         Po1             LACP       Yes  Gi0/0(P)
2         Po2             LACP       Yes  Gi0/1(P)
 slave:********************************************************************
 Number of channel-groups in use: 2
Group  Port-channel  Protocol  Span-cluster   Ports
------+-------------+----------+-----------------------------------------------
```

```
1         Po1             LACP       Yes   Gi0/0(P)
2         Po2             LACP       Yes   Gi0/1(P)
```

ASA クラスタのモニタリング

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info** [**health** [**details**]]

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ノードおよびクラスタ全体の現在の状態を表示します。**details** キーワードは、ハートビート メッセージの失敗数を表示します。

  show cluster info コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID   : 2
```

```
      Version   : 9.4(1)
Serial No.: P3000000191
CCL IP    : 10.0.0.2
CCL MAC   : 000b.fcf8.c61e
Last join : 19:13:50 UTC Sep 23 2011
Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  時間遅延後にクラスタノードがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルスチェック障害など）がクリアされたかどうかを示します。ノードが永続的に無効になっている場合、またはノードがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。

  show cluster info auto-join コマンドについては次の出力を参照してください。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check
failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp**[**detail**]}

  次のトランスポート関連の統計情報を表示します。

  - **asp**：データ プレーンのトランスポート統計情報。
  - **cp**：コントロール プレーンのトランスポート統計情報。

    detail キーワードを入力すると、クラスタで信頼性の高いトランスポート プロトコルの使用状況が表示され、バッファがコントロールプレーンでいっぱいになったときにパケット ドロップの問題を特定できます。**show cluster info transport cp detail** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
```

```
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
--------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0
```

```
    total:                  0
    current:                0
    high watermark:         0

    delivered:              0
    deliver failures:       0

    buffer full drops:      0
    message truncate drops: 0

    gate close ref count:   0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ------------------------------------------------------------------
```

```
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  クラスタの履歴、およびクラスタノードが参加できなかった理由や、ノードがクラスタを離れた理由に関するエラーメッセージが表示されます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用して制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

クラスタリソースのモニタリング

クラスタリソースのモニタリングについては、次のコマンドを参照してください。

show cluster {**cpu** | **memory** | **resource**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタトラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail]、cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダのどのフローであるかを示します。**cluster exec show conn** コマンドを任意のノードで使用すると、すべての接続が表示されます。このコマンドの表示からは、1 つのフローのトラフィック

がクラスタ内のさまざまなASAにどのように到達するかがわかります。クラスタのスループットは、ロードバランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

また、**show conn detail** コマンドはフローモビリティの影響を受けるフローを表示します。

次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
 uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
 received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
 NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
 Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic
received at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface
NP Identity
Ifc Locally received: 716 (8 byte/s)
```

接続フローのトラブルシューティングを行うには、最初にすべてのノードの接続を一覧表示します。それには、任意のノードで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3 つのすべての ASA での 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が表示されています。ASA1 には z フラグがあり、この接続のフォワーダであることを表しています。ASA3 には Y フラグがあり、この接続のディレクタであることを表しています。ASA2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットはASA2の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパ

ケットはASA1およびASA3の外部インターフェイスに入り、クラスタ制御リンクを介してASA2に転送され、次にASA2の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:************************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:************************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes
0, flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution コマンドと **show cluster info packet-distribution** コマンドは、すべてのクラスタノードへのトラフィック分散を表示します。これらのコマンドは、外部ロードバランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

  show cluster info flow-mobility counters コマンドは、EIDおよびフローの所有者の動作情報を表示します。**show cluster info flow-mobility counters** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  この**show cluster info load-monitor**コマンドは、最後の間隔のクラスタメンバのトラフィック負荷と、設定された間隔の合計数（デフォルトでは30）を表示します。各間隔の各測定値を表示するには、**details** キーワードを使用します。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 30 interval:
   0           0            0            12             28
```

```
   1           0           0           13              27

ciscoasa(cfg-cluster)# show cluster info load-monitor details

ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

show cluster access-list コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのノードでの合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*****************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:************************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

  クラスタのルーティング情報を表示します。

- **show lisp eid**

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

  cluster exec show lisp eid コマンドからの、次の出力を参照してください。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**************************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  このコマンドは、トラブルシューティングに役立ちます。

分散型サイト間 VPN のモニタリング

次のコマンドを使用して、VPN セッションのステータスと分布を監視します。

- セッションの全体的な分布は、**show cluster vpn-sessiondb distribution** を使用して示されます。マルチコンテキスト環境で実行している場合は、このコマンドをシステム実行スペースで実行する必要があります。

  この show コマンドを使用すると、各ノードで **show vpn-sessiondb summary** を実行する必要なく、セッションのクイックビューが提供されます。

- **show cluster vpn-sessiondb summary** コマンドを使用して、クラスタ上の VPN 接続の統一されたビューも使用できます。

- **show vpn-sessiondb** コマンドを使用した個々のデバイス モニタリングでは、通常の VPN 情報に加えて、デバイス上のアクティブ セッションとバックアップ セッションの数が表示されます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ノードは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

クラスタのインターフェイスのモニタリング

クラスタのインターフェイスのモニタリングについては、次のコマンドを参照してください。

- **show cluster interface-mode**

  クラスタ インターフェイスのモードを表示します。

- **show port-channel**

  ポートチャネルがスパンドかどうかに関する情報が含まれます。

- **show lacp cluster {system-mac | system-id}**

  cLACP システム ID およびプライオリティを表示します。

- **debug lacp cluster [all | ccp | misc | protocol]**

  cLACP のデバッグ メッセージを表示します。

- **show interface**

  MAC アドレスを使用している場合、その使用状況を表示します。

```
ciscoasa# show interface port-channel1.3151
Interface Port-channel1.3151 "inside", is up, line protocol is up
Hardware is EtherChannel/LACP, BW 1000 Mbps, DLY 10 usec
VLAN identifier 3151
MAC address aaaa.1111.1234, MTU 1500
Site Specific MAC address aaaa.1111.aaaa
IP address 10.3.1.1, subnet mask 255.255.255.0
Traffic Statistics for "inside":
132269 packets input, 6483425 bytes
1062 packets output, 110448 bytes
98530 packets dropped
```

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **debug cluster flow-mobility**

クラスタリング フロー モビリティ関連のイベントを表示します。

- **debug lisp eid-notify-intercept**

  EID 通知メッセージ代行受信時のイベントを表示します。

- **show cluster info trace**

  show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

  show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

たとえば、同じ**ローカルユニット**名を持つ2つのノードが制御ノードとして機能していることを示す次のメッセージが表示された場合は、2 つのノードの**ローカルユニット**名が同じである（設定を確認してください）か、1つのノードが自身のブロードキャストメッセージを受信している（ネットワークを確認してください）可能性があります。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node

 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
 Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
 CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

分散型サイト間 VPN のトラブルシューティング

分散型 VPN の通知

分散型 VPN を実行しているクラスタで、次のエラー状況が発生した場合、識別されたフレーズを含むメッセージが通知されます。

状況	通知
クラスタに参加しようとしているときに、既存のまたは参加しているクラスター データ ノードが分散型 VPN モードにない場合は、次のメッセージが通知されます。	`New cluster member (member-name) rejected due to vpn mode mismatch.` および 制御ノード（*control-name*）は、VPN モード機能に制御ノードの設定との互換性がないという理由でユニット（unit-name）からの登録要求を拒否します。
分散型VPNのクラスタ メンバーでライセンスが正しく設定されていない場合は、次のメッセージが通知されます。	`ERROR: Control node requested cluster vpn-mode change to distributed. Unable to change mode due to missing Carrier License.`

受信した IKEv2 パケットの SPI でタイム スタンプまたはメンバー ID が無効な場合は、次のメッセージが通知されます。	`Expired SPI received`
	または
	`Corrupted SPI detected`

クラスタがバックアップ セッションを作成できない場合は、次のメッセージが通知されます。	`Failed to create the backup for an IKEv2 session.`
IKEv2 初期接点（IC）処理エラーの場合は、次のメッセージが通知されます。	`IKEv2 Negotiation aborted due to ERROR: Stale backup session found on backup`
再配布の問題の場合は、次のメッセージが通知されます。	`Failed to send session redistribution message to` *`member-name`* `Failed to receive session move response from` *`member-name`* `(control node only)`
セッションの再配布中にトポロジが変更された場合は、次のメッセージが通知されます。	`Cluster topology change detected. VPN session redistribution aborted.`

次のいずれかの状況が発生している可能性があります。

- サイト間 VPN セッションは**port-channel load-balance src-dst l4port** コマンドを使用して N7K スイッチにロード バランシング アルゴリズムとしてレイヤ 4 ポート が設定されている場合、クラスターのシャーシの 1 つにのみ配布されます。クラスタ セッションの割り当ての例を次に示します。

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
 5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
 5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
 5(2501)
```

```
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

サイト間 IKEv2 VPN は送信元ポートと宛先ポートの両方にポート 500 を使用するため、IKE パケットは Nexus 7K とシャーシ間に接続されたポート チャネル内のリンクの 1 つにのみ送信されます。

port-channel load-balance src-dst ip-l4port を使用して、N7K ロード バランシング アルゴリズムを IP およびレイヤ 4 ポートに変更します。その後、IKE パケットはすべてのリンクに、そしてすべてのノード送信されます。

より即座に調整するには、クラスターの制御ノードで **cluster redistribute vpn-sessiondb** を実行することで、アクティブな VPN セッションを他のシャーシのクラスター ノードに再配布できます。

ASA クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

ASA およびスイッチのコンフィギュレーションの例

次のコンフィギュレーション例は、ASA とスイッチ間の次のインターフェイスを接続します。

ASA インターフェイス	スイッチインターフェイス
イーサネット1/2	GigabitEthernet 1/0/15
イーサネット 1/3	GigabitEthernet 1/0/16
イーサネット 1/4	GigabitEthernet 1/0/17
イーサネット 1/5	GigabitEthernet 1/0/18

ASA の設定

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ASA1 制御ユニットのブートストラップ設定

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
```

```
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit A
 cluster-interface Port-channel1 ip 10.0.0.1 255.255.255.0
 priority 10
 key emphyri0
 enable noconfirm
```

ASA2 データユニットのブートストラップ設定

```
interface Ethernet1/6
 channel-group 1 mode on
 no shutdown
!
interface Ethernet1/7
 channel-group 1 mode on
 no shutdown
!
interface Port-channel1
 description Clustering Interface
!
cluster group Moya
 local-unit B
 cluster-interface Port-channel1 ip 10.0.0.2 255.255.255.0
 priority 11
 key emphyri0
 enable as-data-node
```

制御ユニットのインターフェイス設定

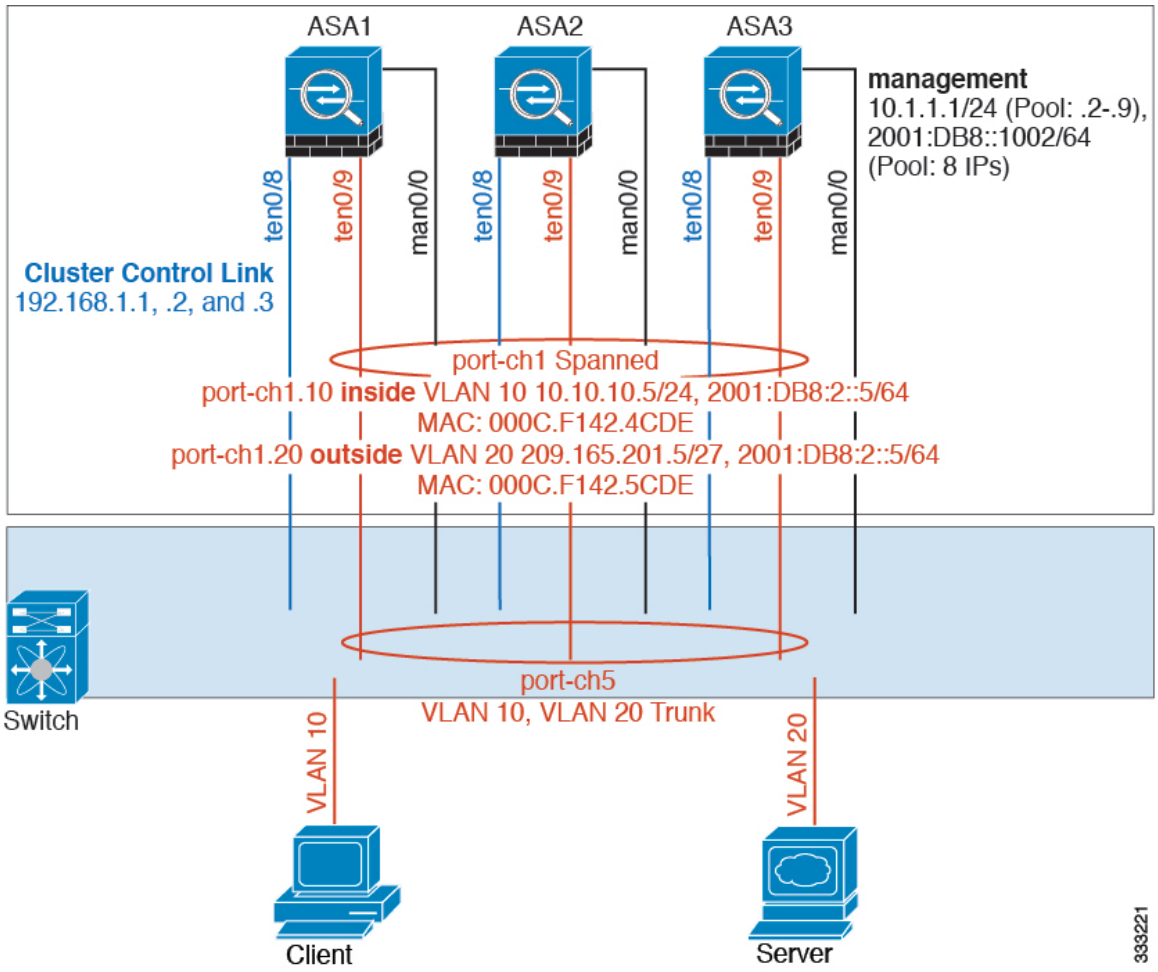
```
ip local pool mgmt-pool 10.53.195.231-10.53.195.232

interface Ethernet1/2
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/3
 channel-group 10 mode active
 no shutdown
!
interface Ethernet1/4
 channel-group 11 mode active
 no shutdown
!
interface Ethernet1/5
 channel-group 11 mode active
 no shutdown
!
interface Management1/1
 management-only
 nameif management
 ip address 10.53.195.230 cluster-pool mgmt-pool
 security-level 100
```

```
 no shutdown
!
interface Port-channel10
 mac-address aaaa.bbbb.cccc
 nameif inside
 security-level 100
 ip address 209.165.200.225 255.255.255.224
!
interface Port-channel11
 mac-address aaaa.dddd.cccc
 nameif outside
 security-level 0
 ip address 209.165.201.1 255.255.255.224
```

Cisco IOS スイッチのコンフィギュレーション

```
interface GigabitEthernet1/0/15
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/16
 switchport access vlan 201
 switchport mode access
 spanning-tree portfast
 channel-group 10 mode active
!
interface GigabitEthernet1/0/17
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active
!
interface GigabitEthernet1/0/18
 switchport access vlan 401
 switchport mode access
 spanning-tree portfast
 channel-group 11 mode active

interface Port-channel10
 switchport access vlan 201
 switchport mode access

interface Port-channel11
 switchport access vlan 401
 switchport mode access
```

スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。ASA が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ユニット 1 制御ユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa1
cluster-interface ethernet1/8 ip 192.168.1.1 255.255.255.0
priority 1
key chuntheunavoidable
enable noconfirm
```

ユニット 2 データユニットのブートストラップ設定

```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa2
cluster-interface ethernet1/8 ip 192.168.1.2 255.255.255.0
priority 2
key chuntheunavoidable
enable as-data-node
```

ユニット 3 データユニットのブートストラップ設定

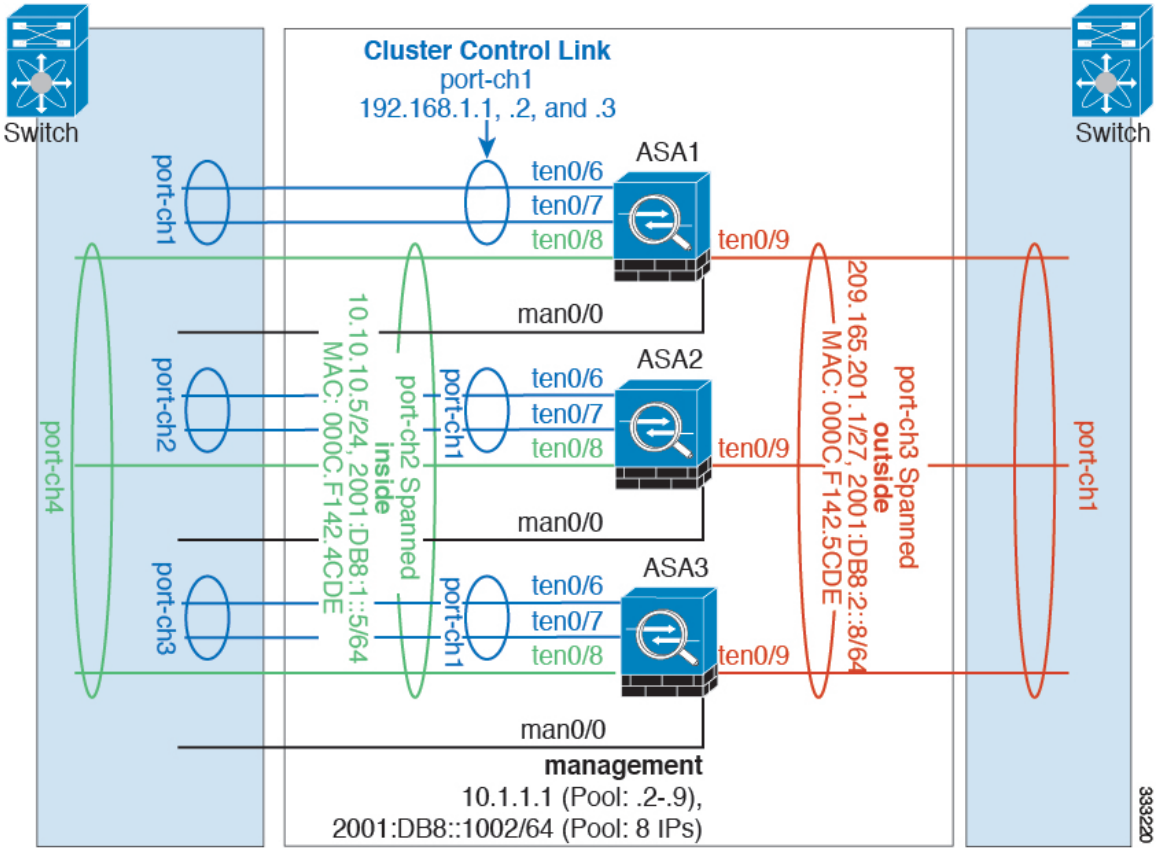
```
interface ethernet1/8
no shutdown
description CCL

cluster group cluster1
local-unit asa3
cluster-interface ethernet1/8 ip 192.168.1.3 255.255.255.0
priority 3
key chuntheunavoidable
enable as-data-node
```

制御ユニットのインターフェイス設定

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
security-level 100
management-only
no shutdown

interface ethernet1/1
channel-group 1 mode active
no shutdown
```

```
interface port-channel 1

interface port-channel 1.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE

interface port-channel 1.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

各ユニットのインターフェイス モード

```
cluster interface-mode spanned force
```

ユニット 1 制御ユニットのブートストラップ設定

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa1
 cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
 priority 1
 key chuntheunavoidable
 enable noconfirm
```

ユニット 2 データユニットのブートストラップ設定

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL

cluster group cluster1
 local-unit asa2
 cluster-interface port-channel1 ip 192.168.1.2 255.255.255.0
 priority 2
 key chuntheunavoidable
 enable as-data-node
```

ユニット 3 データユニットのブートストラップ設定

```
interface ethernet 1/6
 channel-group 1 mode on
 no shutdown

interface ethernet 1/7
 channel-group 1 mode on
 no shutdown

interface port-channel 1
 description CCL
```

```
cluster group cluster1
 local-unit asa3
 cluster-interface port-channel1 ip 192.168.1.3 255.255.255.0
 priority 3
 key chuntheunavoidable
 enable as-data-node
```

制御ユニットのインターフェイス設定

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8::1002/64 8

interface management 1/1
 nameif management
 ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
 ipv6 address 2001:DB8::1001/32 cluster-pool mgmtipv6
 security-level 100
 management-only
 no shutdown

interface ethernet 1/8
 channel-group 2 mode active
 no shutdown

interface port-channel 2
 nameif inside
 ip address 10.10.10.5 255.255.255.0
 ipv6 address 2001:DB8:1::5/64
 mac-address 000C.F142.4CDE

interface ethernet 2/1
 channel-group 3 mode active
 no shutdown

interface port-channel 3
 nameif outside
 ip address 209.165.201.1 255.255.255.224
 ipv6 address 2001:DB8:2::8/64
 mac-address 000C.F142.5CDE
```

ルーテッド モード サイト間クラスタリングの OTV 設定

スパンド EtherChannel を使用したルーテッド モードに対するサイト間クラスタリングの成功は、OTV の適切な設定とモニタリングによって異なります。OTV は、DCI 全体にパケットを転送することで、重要な役割を果たします。OTV は、転送テーブルに MAC アドレスを学習するときにのみ、DCI 全体にユニキャスト パケットを転送します。MAC アドレスが OTV 転送テーブルに学習されていない場合、ユニキャスト パケットはドロップされます。

OTV 設定の例

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC
```

```
feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown
```

```
otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

サイト障害のために必要な OTV フィルタの変更

サイトがダウンした場合は、グローバル MAC アドレスをそれ以上ブロックしなくて済むように、フィルタを OTV から削除する必要があります。必要ないくつかの追加設定があります。

機能しているサイトで OTV スイッチ上の ASA グローバル MAC アドレスに対するスタティック エントリを追加する必要があります。このエントリによって、反対側の OTV はオーバーレイ インターフェイスにこれらのエントリを追加できます。サーバとクライアントに ASA 用の ARP エントリがすでにある場合（これは既存の接続の場合です）、ARP は再送信されないので、この手順が必要になります。したがって、OTV は転送テーブルに ASA グローバル MAC アドレスを学習する機会はありません。OTV には転送テーブル内にグローバル MAC アドレスがなく、OTV の設計ごとに OTV はオーバーレイ インターフェイスを介してユニキャスト パケットをフラッディングしないので、ユニキャスト パケットはサーバからのグローバル MAC アドレスにドロップされ、既存の接続は切断されます。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

他のサイトが復元した場合は、フィルタを再度追加して、OTV でこのスタティック エントリを削除する必要があります。グローバル MAC アドレスのオーバーレイ エントリをクリアするには、両方の OTV でダイナミック MAC アドレス テーブルをクリアすることが非常に重要です。

MAC アドレス テーブルのクリア

サイトがダウンし、グローバル MAC アドレスへのスタティック エントリが OTV に追加される場合は、他の OTV がオーバーレイ インターフェイスのグローバル MAC アドレスを学習できるようにする必要があります。他のサイトが起動したら、これらのエントリをクリアする必

要があります。OTV の転送テーブルにこれらのエントリがないことを確認するために、MAC アドレス テーブルを必ず消去してください。

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP キャッシュのモニタリング

OTV は、OTV インターフェイス全体で学習した IP アドレスに対するプロキシ ARP への ARP キャッシュを維持します。

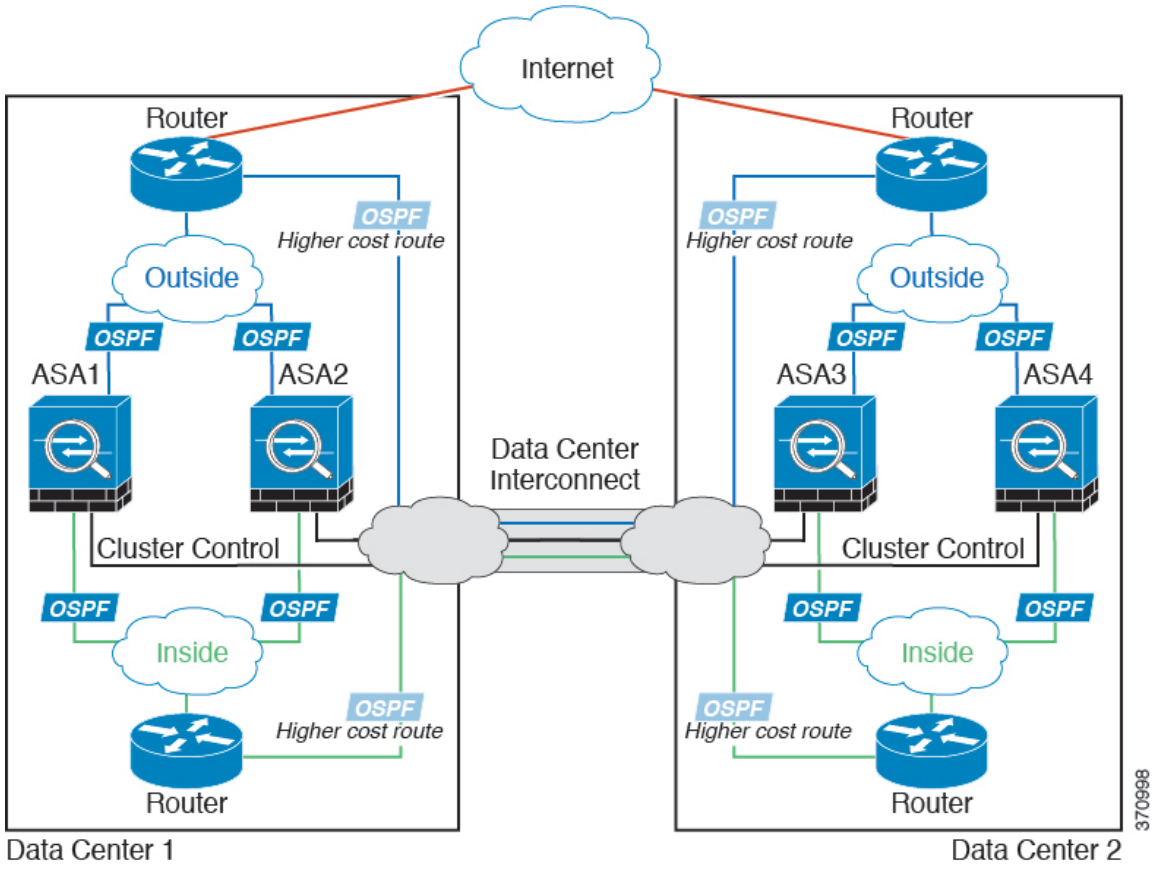
```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

個別インターフェイス ルーテッド モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つの ASA クラスタノードがある場合を示します。クラスタノードは、DCI 経由のクラスタ制御リンクによって接続されています。各データセンターの内部ルータと外部ルータは、OSPF と PBR または ECMP を使用してクラスタ メンバ間でトラフィックをロードバランスします。DCI に高コストルートを割り当てることにより、特定のサイトのすべての ASA クラスタノードがダウンしない限り、トラフィックは各データセンター内に維持されます。1 つのサイトのすべてのクラスタノードに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトの ASA クラスタノードに送られます。



サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド EtherChannel ルーテッド モードの例

次の例では、各サイトのゲートウェイ ルータと内部ネットワーク間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部両方のネットワークに対しスパンド EtherChannel を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

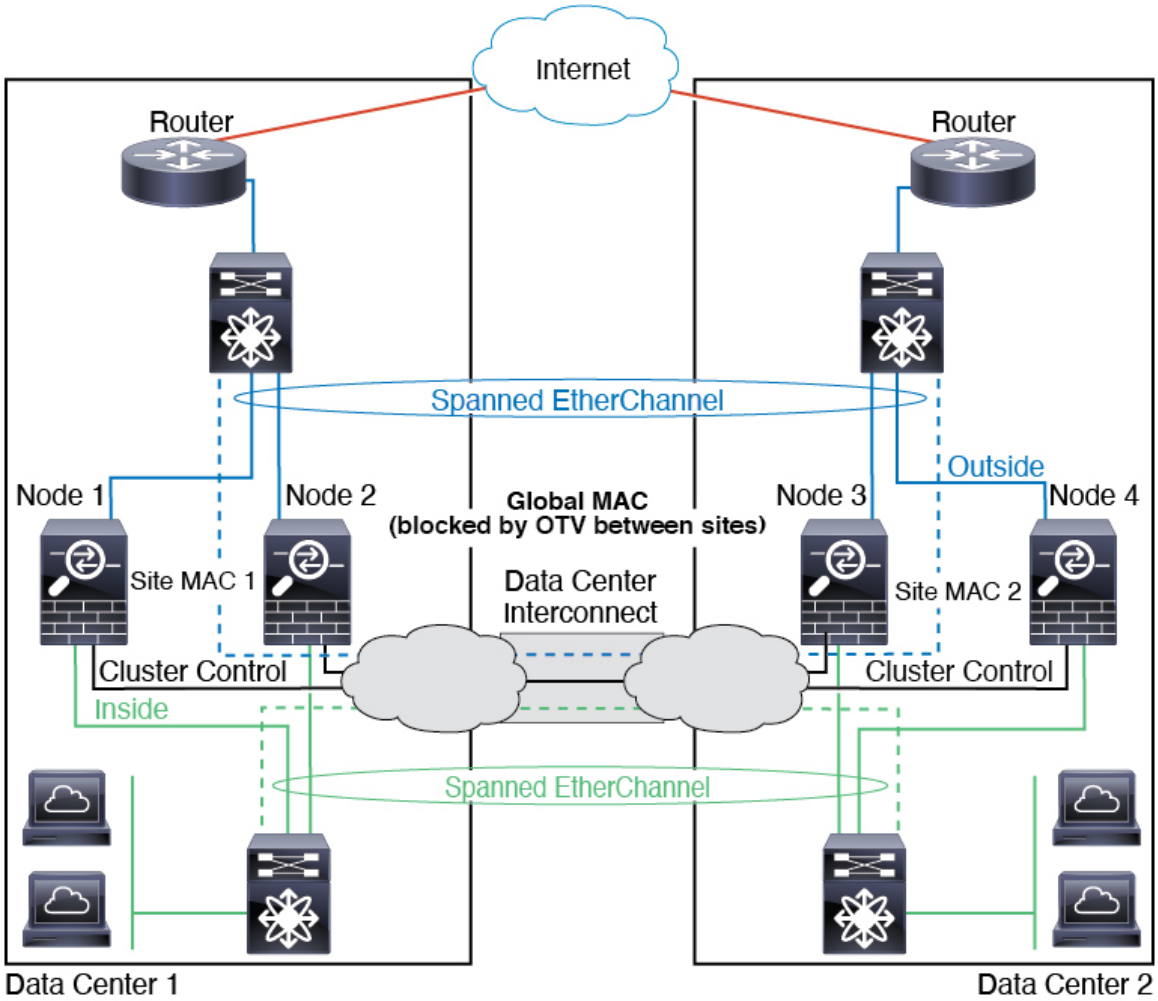
データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロックするフィルタを追加する必要があります。1 つのサイトのクラスタ ノードが到達不能になった場合、トラフィックが他のサイトのクラスタ ノードに送信されるようにフィルタを削除する必要があります。Vacl を使用して、グローバルの MAC アドレスのフィルタ リングする必要があります。F3 シリーズライン カードを使用した Nexus などの一部のスイッチでは、グローバル MAC アドレスからの ARP パケットをブロックするために ARP インスペクションも使用する必要があります。ARP インスペクションでは、ASA でサイトの MAC アドレスとサイトの IP

アドレスの両方を設定する必要があります。サイトの MAC アドレスのみを設定する場合は必ず ARP インスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタノード間で共有されるグローバルな仮想 MAC は、パケットを受信するためだけに使用されます。発信パケットは、各 DC クラスタからのサイト固有の MAC アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。

このシナリオでは、次のようになります。

- クラスタから送信されるすべての出力パケットは、サイトの MAC アドレスを使用し、データセンターでローカライズされます。
- クラスタへのすべての入力パケットは、グローバル MAC アドレスを使用して送信されるため、両方のサイトにある任意のノードで受信できます。OTV のフィルタによって、データセンター内のトラフィックがローカライズされます。



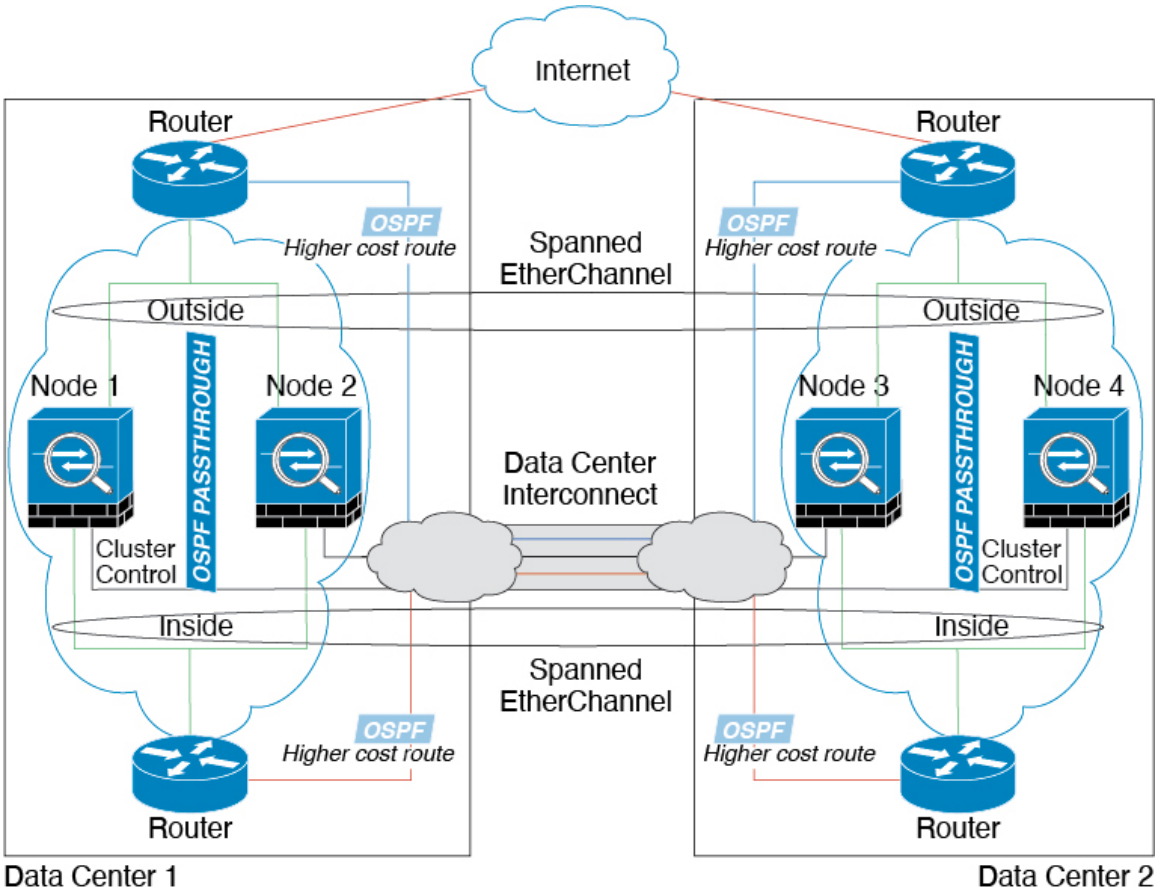
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コストルートを割り当てることにより、特定のサイトですべてのクラスタ メンバがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1 つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタ メンバに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

- サイト間 VSS、vPC、StackWise、StackWise Virtual：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、冗長スイッチトラフィックは DCI を経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCI が余分なトラフィックを処理できる場合、必要に応じて、各ノードを DCI 経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCI を非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS、vPC、StackWise、StackWise Virtual：スイッチの冗長性を高めるには、各サイトに 2 つの異なる冗長スイッチペアをインストールできます。この場合、クラスタノードは、両方のローカルスイッチだけに接続されたデータセンター 1 のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター 2 のシャーシではスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル冗長スイッチは、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。

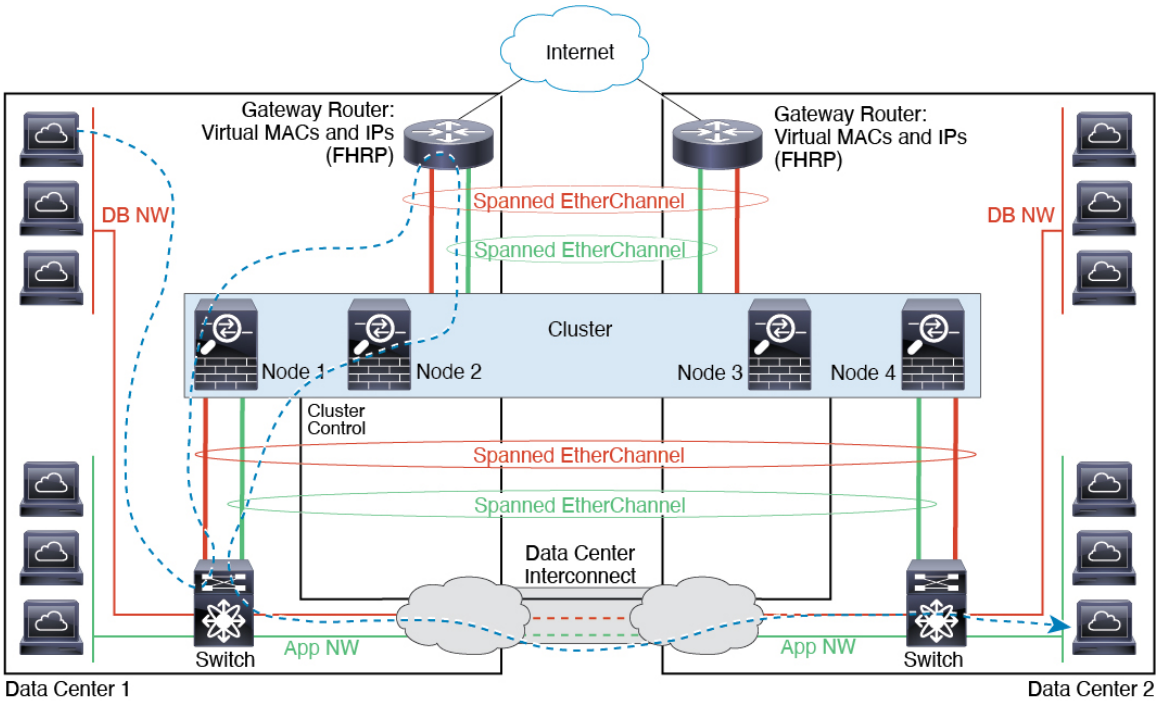


スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイ ルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレス と IP アドレスを提供します。MAC アドレスの予期せぬフラッピングを避けるため、**mac-address-table static** *outside_interface mac_address* コマンドを使用して、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト 1 のゲートウェイがサイト 2 のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト 2 に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイ ルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1 つのサイトのゲート

ウェイ ルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- 次のアプリケーション インスペクション：
  - CTIQBE

- H323、H225、および RAS
- IPsec パススルー
- MGCP
- MMP
- RTSP
- SCCP（Skinny）
- WAAS
- WCCP

- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- VPN ロード バランシング
- Azure でのフェールオーバー
- 統合ルーティングおよびブリッジング
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - IM

- NetBIOS
- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- スタティック ルート モニタリング
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス
- サイト間 VPN
- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ダイナミック ルーティング（スパンド EtherChannel モードのみ）

個々のノードに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。
- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有され

る EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証と許可は、クラスタリング制御ノード上で中央集中型機能として実装されており、データ構造がクラスタデータノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるため、フローに対するアカウンティングが設定されている場合、そのフローを所有するクラスタノードがアカウンティング開始と停止のメッセージを AAA サーバに送信します。

接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます（**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、および **set connection per-client-max** コマンドを参照）。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用する場合、制御チャネルのフローは制御ノードに集中されます。

ICMP インスペクションとクラスタリング

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインスペクションが有効かどうかによって異なります。ICMP インスペクションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インスペクションを使用する場合、ICMP フローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットの

ディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

マルチキャスト ルーティングとクラスタリング

マルチキャスト ルーティングは、インターフェイス モードによって動作が異なります。

スパンド EtherChannel モードでのマルチキャストルーティング

スパンドEtherChannelモードでは、ファストパス転送が確立されるまで、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを処理します。接続が確立された後は、各データユニットがマルチキャスト データ パケットを転送できます。

個別インターフェイス モードでのマルチキャスト ルーティング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべて制御ユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NATが使用されるときは、インバウンドとアウトバウンドとで、パケットのIPアドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。これは、スパンドEtherChannelの問題ではありません。クラスタ インターフェイスには関連付けられた IP アドレスが 1 つしかないためです。
- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラ

スタでは、ホストからのトラフィックが3つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。

- バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
- PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
- クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは512ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。
- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。

- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。たとえば、TCP/443 の HTTPS TLS と比較してずっと優れたパフォーマンスを発揮する代替手段として、UDP/443 を用いる Quick プロトコルの使用が増加している場合、UDP/443 に対し per-session PAT を有効にする必要があります。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

ダイナミック ルーティングおよびクラスタリング

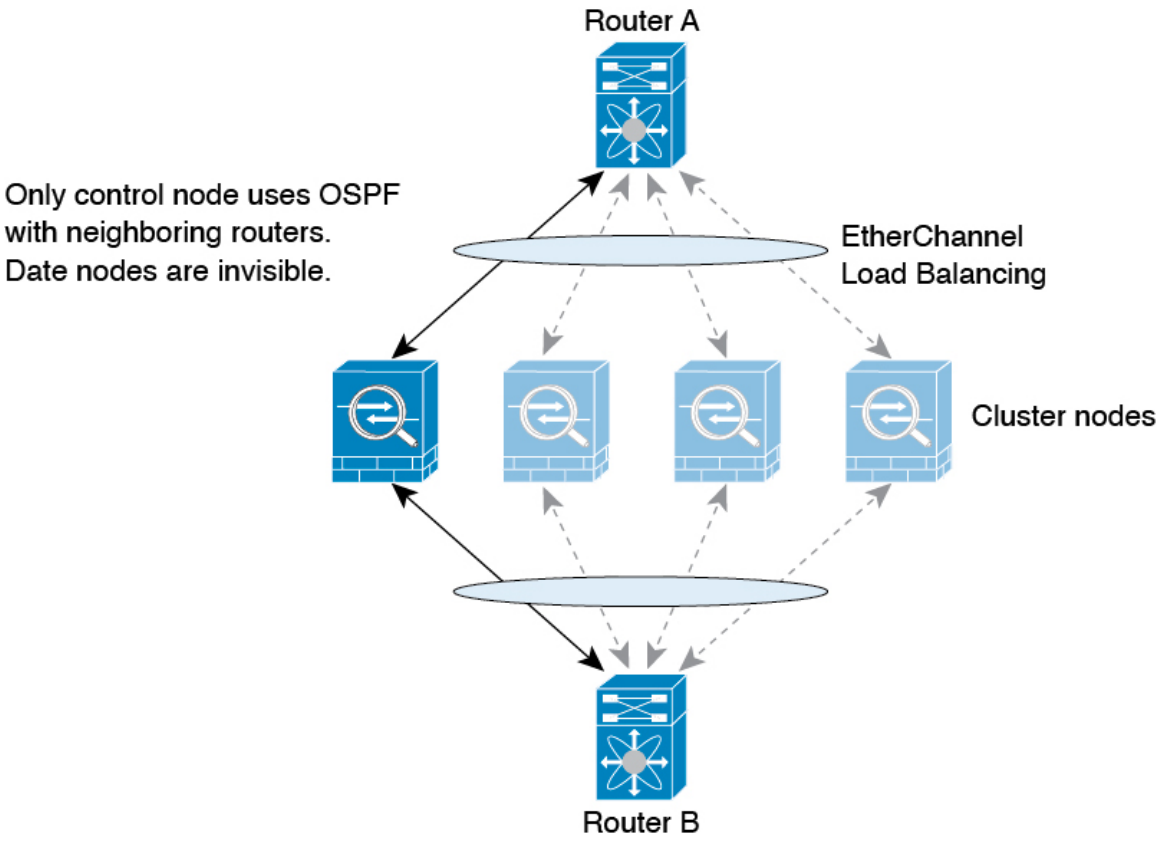
ここでは、クラスタリングでダイナミック ルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

（注） IS-IS は、スパンド EtherChannel モードではサポートされていません。

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *50 :* スパンド *EtherChannel* モードでのダイナミック ルーティング



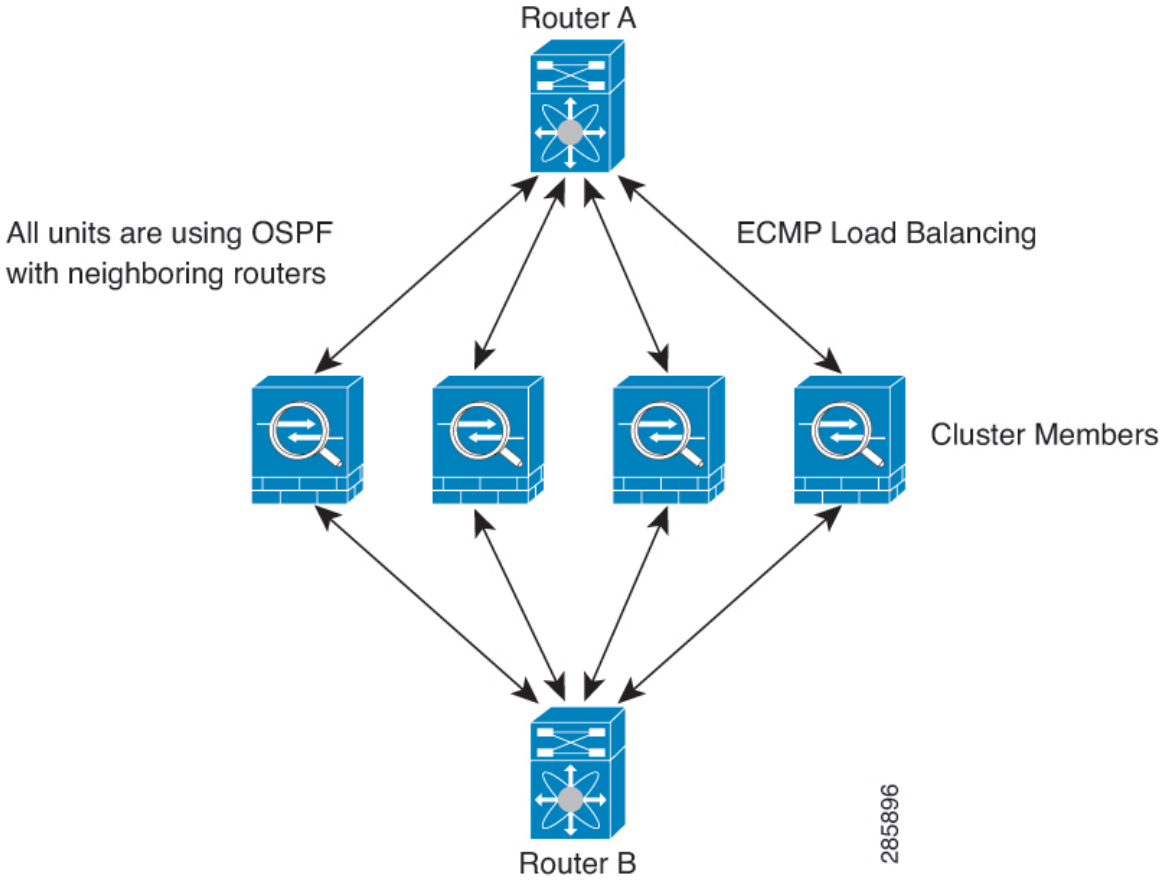
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ IDがクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *51* : 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィック ゾーンにこれらすべてのノード インターフェイスをまとめます。トラフィック ゾーンの設定 （995 ページ）を参照してください。

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、その 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、STUNインスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN要求の受信後にノードに障害が発生し、別のノードがSTUN応答を受信した場合、STUN応答はドロップされます。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカル ノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。
- NetFlow：クラスタの各ノードは自身のNetFlowストリームを生成します。NetFlowコレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN接続を再確立する必要があります。

VPN トンネルをスパンド EtherChannel アドレスに接続すると、接続が自動的に制御ノードに転送されます。 PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80%になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps（8 ユニット x 10 Gbps）の約 80% で 64 Gbps になります。

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

（注） 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。
5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注） ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、ノードとインターフェイスの正常性をモニターし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション 2 のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

詳細については、制御ノードの選定 （513 ページ）を参照してください。

インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェア インターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

- スパンド EtherChannel：クラスタ Link Aggregation Control Protocol（cLACP）を使用します。各ノードは、リンクステータスおよび cLACP プロトコルメッセージをモニタして、ポートがまだ EtherChannel でアクティブであるかどうかを判断します。ステータスが制御ノードに報告されます。
- 個別インターフェイス（ルーテッドモードのみ）：各ノードが自身のインターフェイスを自己モニタし、インターフェイスのステータスを制御ノードに報告します。

ヘルスモニタリングを有効にすると、すべての物理インターフェイス（主要な EtherChannel インターフェイスを含む）がデフォルトでモニタされるため、オプションでインターフェイスごとのモニタリングを無効化することができます。指名されたインターフェイスのみモニターできます。たとえば、指名された EtherChannel に障害が発生したと判断される必要がある場合、つまり、EtherChannel のすべてのメンバー ポートはクラスタ削除をトリガーすることに失敗する必要があります（最小ポート バンドリング設定に応じて）。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ASA がメンバーをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのノードが確立済みメンバーであるかクラスタに参加しようとしているかによって異なります。EtherChannel の場合（スパニングかどうかを問わない）：確立済みメンバーのインターフェイスがダウン状態の場合、ASA はそのメンバーを 9 秒後に削除します。ASA は、ノードがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。EtherChannel 以外の場合は、メンバー状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASAが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでノードがまだ非アクティブになっていると、管理インターフェイスは無効になります。さらに設定を行う場合は、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタノードがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：（最初の参加時）クラスタ制御リンクの問題を解決した後、コンソールポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASA は、無限に 5 分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動でイネーブルにする必要があります。この動作は設定可能です。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングが **enable** コマンドでまだイネーブルになっているなら、ノードは再起動するとクラスタに再参加することを意味します。ASA は 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。ノードは、5 分、10 分、20 分の間隔で自動的にクラスタに再参加しようとします。この動作は設定可能です。

制御ノードのブートストラップの設定 （439 ページ）を参照してください。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *18 :* クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	あり	—

Traffic	状態のサポート	注意
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—
Firepower 4100/9300 の分散型 VPN（サイト間）	Yes	バックアップセッションがアクティブセッションになると、新しいバックアップセッションが作成されます。

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

  サイト間クラスタリングのディレクタローカリゼーションを有効にすると、ローカルバックアップとグローバルバックアップの2つのバックアップ オーナー権限があります。オーナーは、常に同じサイトのローカルバックアップをオーナー自身として選択します（サイ

トIDに基づいて）。グローバルバックアップはどのサイトにあってもよく、ローカルバックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

サイトの冗長性を有効にし、バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。シャーシバックアップとサイトバックアップは独立しているため、フローにはシャーシ バックアップとサイト バックアップの両方が含まれている場合があります。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルディレクタとグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（Site Id に基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにあってもよく、ローカルディレクタと同一ノードとすることもできます。元のオーナーに障害が発生すると、ローカルディレクタはこのサイトで新しい接続オーナーを選択します。

  ICMP/ICMPv6 ハッシュの詳細：

  - エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
  - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
  - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタのローカリゼーションを有効にすると、フォワーダは常にローカルディレクタに問い合わせます。フォワーダがグローバルディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタ メンバーが受信する場合などです。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえ

ばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

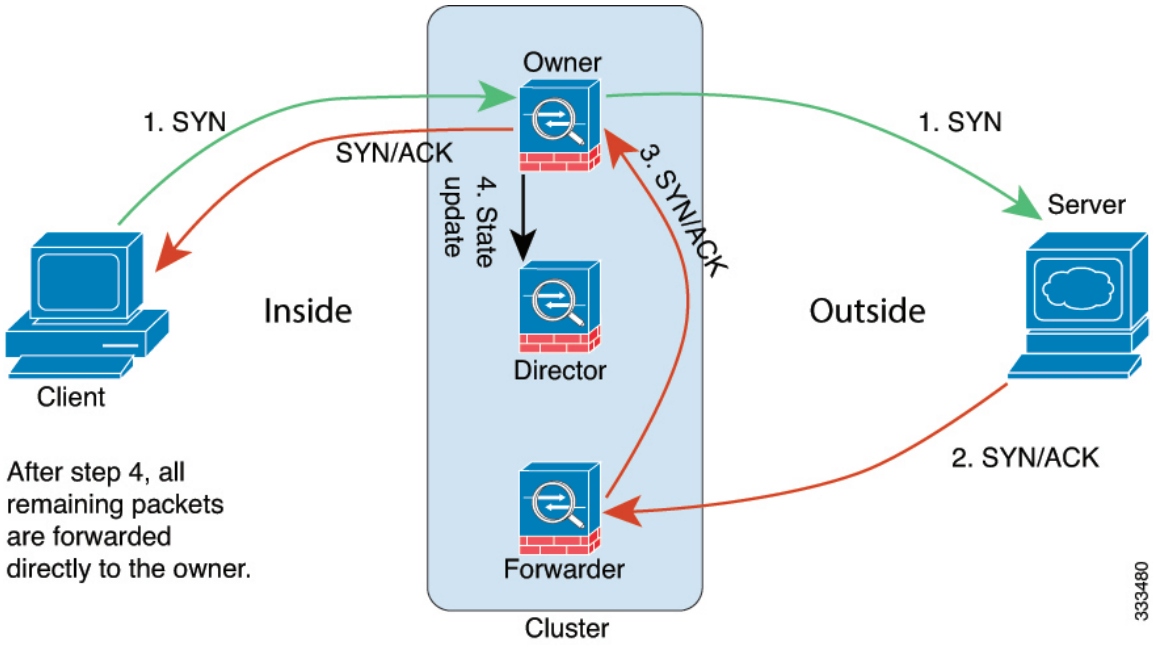
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1つのフローの両方向が同じノードに到着するとともに、フローがノード間に均等に分散されるようにするためです。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。



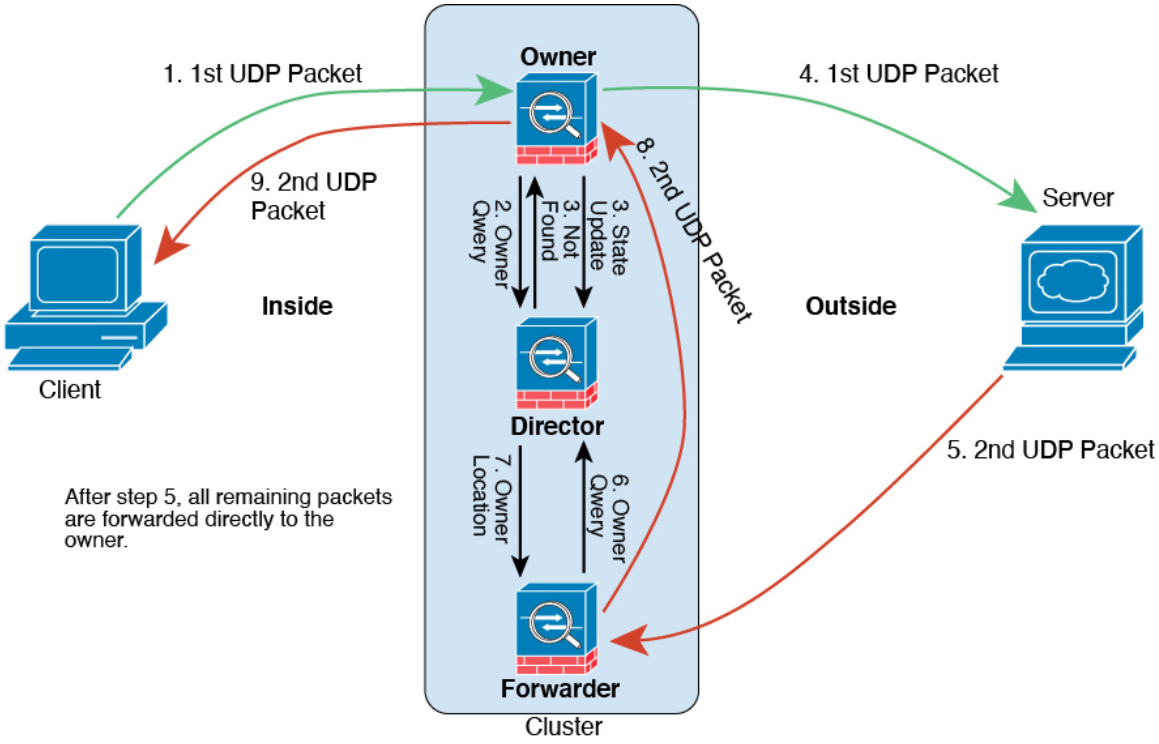
1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。

6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

1. 図 *52 : ICMP* および *UDP* データフロー



UDP パケットがクライアントから発信され、1 つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。

5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

新しい TCP 接続のクラスタ全体での再分散

アップストリームルータまたはダウンストリームルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しい接続再分散を設定して、1 秒あたりの新しい接続数が多いノードから他のノードに新しい TCP フローをリダイレクトすることができます。既存のフローは他のノードには移動されません。

このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。

接続が別のノードにオフロードされると、非対称接続になります。

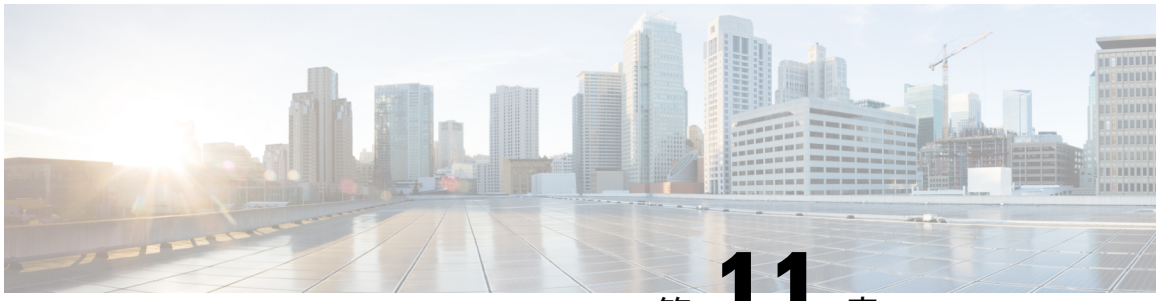
サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタメンバには新しい接続を再分散できません。

Cisco Secure Firewall 3100/4200 の ASA クラスタリングの履歴

機能名	バージョン	機能情報
Secure Firewall 4200 のクラスタリングを使用した分散型サイト間 VPN	9.23(1)	Firepower 4200 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ノードだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。 新規または変更されたコマンド：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn-mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show conn detail**、**show crypto ikev2 stats**

機能名	バージョン	機能情報
クラスタ リダイレクト： Cisco Secure Firewall 4200 非対称クラスタ トラフィックのフローオフロードのサポート	9.23(1)	非対称フローの場合、クラスタリダイレクトにより、転送ノードはハードウェアにフローをオフロードできます。この機能はデフォルトで有効になっています。 既存のフローのトラフィックが別のノードに送信されると、そのトラフィックはクラスタ制御リンクを介してオーナー ノードにリダイレクトされます。非対称フローは、クラスタ制御リンクに大量のトラフィックを作成する可能性があるため、フォワーダにこれらのフローをオフロードさせると、パフォーマンスが向上します。 追加/変更されたコマンド： **flow-offload cluster-redirect**、**show conn**、**show flow-offload flow**、**show flow-offload info**。
分散型サイト間 VPN モードの Cisco Secure Firewall 4200 のクラスタ制御リンクのトラフィックの IPsec フローのオフロード	9.23(1)	分散型サイト間 VPN モードの非対称フローの場合、IPsec フロー オフロードにより、フロー オーナーは、クラスタ制御リンクを介して転送されたハードウェア内の IPsec トラフィックを復号できます。この機能は構成可能ではありません。IPsec フローのオフロードを有効にすると常に使用できます。 追加/変更されたコマンド： **flow-offload-ipsec**、**show crypto ipsec sa detail**
ノード参加時の MTU ping テスト	9.23(1)	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
クラスタノードの最大数を 16 に増加	9.22(1)	最大ノード数が 8 から 16 に増加しました。
個別インターフェイス モード	9.22(1)	個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル *IP* アドレスを持ちます。各インターフェイスのメインクラスタ *IP* アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。 アップストリームスイッチ上でロードバランシングを別途する必要があります。 新規/変更されたコマンド： **cluster interface-mode individual**
フローステータスの設定可能なクラスタキープアライブ間隔	9.20(1)	フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。 新規/変更されたコマンド： **clu-keepalive-interval**

機能名	バージョン	機能情報
Secure Firewall 4200 でのクラスタリングのサポートが導入されました	9.20(1)	Spanned EtherChannel モードでは、最大 8 つの Cisco Secure Firewall 4200 ノードをクラスタ化できます。
バイアス言語の除去	9.19(1)	「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。 新規/変更されたコマンド：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**
Secure Firewall 3100 でのクラスタリングのサポートが導入されました	9.17(1)	Spanned EtherChannel モードでは、最大 8 つの Cisco Secure Firewall 3100 ノードをクラスタ化できます。



第 11 章

Firepower 4100/9300 の ASA クラスタ

クラスタリングを利用すると、複数のFirepower 4100/9300 シャーシ ASA をグループ化して、1 つの論理デバイスにすることができます。Firepower 4100/9300 シャーシ シリーズには、Firepower 9300 および Firepower 4100 シリーズ が含まれます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「クラスタリングでサポートされない機能 （611 ページ）」を参照してください。

- Firepower 4100/9300 シャーシのクラスタリングについて （525 ページ）
- Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 （533 ページ）
- でのクラスタリングのライセンス Firepower 4100/9300 シャーシ （535 ページ）
- クラスタリング ガイドラインと制限事項 （537 ページ）
- でのクラスタリングの設定 Firepower 4100/9300 シャーシ （543 ページ）
- FXOS：クラスタノードの削除 （582 ページ）
- ASA：クラスタ メンバの管理 （584 ページ）
- ASA：での ASA クラスタのモニタリング Firepower 4100/9300 シャーシ （589 ページ）
- 分散型 S2S VPN のトラブルシューティング （600 ページ）
- ASA クラスタリングの例 （602 ページ）
- クラスタリングの参考資料 （611 ページ）
- Firepower 4100/9300 上の ASA クラスタリングの履歴 （629 ページ）

Firepower 4100/9300 シャーシのクラスタリングについて

Firepower 4100/9300 シャーシ にクラスタを展開すると、以下の処理が実行されます。

- ノード間通信用のクラスタ制御リンク（デフォルトのポートチャネル48）を作成します。

  1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタの場合、このリンクはクラスタ通信に Firepower 9300 バックプレーンを使用します。

複数のシャーシによるクラスタリングでは、シャーシ間通信用にこのEtherChannelに物理インターフェイスを手動で割り当てる必要があります。

- アプリケーション内のクラスタブートストラップコンフィギュレーションを作成します。

  クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがシャーシスーパバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部は、アプリケーション内でユーザが設定できます。

- スパンドインターフェイスとして、クラスタにデータインターフェイスを割り当てます。

  1つのFirepower 9300シャーシ内のセキュリティモジュールに隔離されたクラスタの場合、スパンドインターフェイスは、複数のシャーシによるクラスタリングの場合のようにEtherChannelに制限されません。Firepower 9300スーパーバイザは共有インターフェイスの複数のモジュールにトラフィックをロードバランシングするために内部でEtherChannelテクノロジーを使用するため、スパンドモードではあらゆるタイプのデータインターフェイスが機能します。複数のシャーシによるクラスタリングでは、すべてのデータインターフェイスでスパンドEtherChannelを使用します。

（注） 管理インターフェイス以外の個々のインターフェイスはサポートされていません。

- 管理インターフェイスをクラスタ内のすべてのユニットに指定します。

クラスタリングの詳細については、以下の項を参照してください。

ブートストラップ設定

クラスタを展開すると、クラスタ名、クラスタ制御リンクインターフェイス、およびその他のクラスタ設定を含む最小限のブートストラップ コンフィギュレーションがFirepower 4100/9300シャーシスーパバイザから各ユニットに対してプッシュされます。クラスタリング環境をカスタマイズする場合、ブートストラップコンフィギュレーションの一部はユーザーが設定できます。

クラスタ メンバー

クラスタ メンバーは連携して動作し、セキュリティ ポリシーおよびトラフィック フローの共有を達成します。

クラスタ内のメンバーの1つが**制御**ユニットになります。制御ユニットは自動的に決定されます。他のすべてのメンバーは**データ**ユニットになります。

すべてのコンフィギュレーション作業は制御ユニット上でのみ実行する必要があります。コンフィギュレーションはその後、データユニットに複製されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ユニットがすべてのトラフィックを処理します。クラスタリングの中央集中型機能 （612 ページ）を参照してください。

クラスタ制御リンク

クラスタ制御リンクはユニット間通信用の EtherChannel（ポート チャネル 48）です。シャーシ内クラスタリングでは、このリンクは、クラスタ通信に Firepower 9300 バックプレーンを使用します。シャーシ間クラスタリングでは、シャーシ間通信のために、Firepower 4100/9300 シャーシ のこの EtherChannel に物理インターフェイスを手動で割り当てる必要があります。

2 シャーシのシャーシ間クラスタの場合、シャーシと他のシャーシの間をクラスタ制御リンクで直接接続しないでください。インターフェイスを直接接続した場合、一方のユニットで障害が発生すると、クラスタ制御リンクが機能せず、他の正常なユニットも動作しなくなります。スイッチを介してクラスタ制御リンクを接続した場合は、正常なユニットについてはクラスタ制御リンクは動作を維持します。

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンクの詳細については、以下の項を参照してください。

クラスタ制御リンクのサイジング

可能であれば、各シャーシの予想されるスループットに合わせてクラスタ制御リンクをサイジングする必要があります。そうすれば、クラスタ制御リンクが最悪のシナリオを処理できます。

クラスタ制御リンク トラフィックの内容は主に、状態アップデートや転送されたパケットです。クラスタ制御リンクでのトラフィックの量は常に変化します。転送されるトラフィックの量は、ロードバランシングの有効性、または中央集中型機能のための十分なトラフィックがあるかどうかによって決まります。次に例を示します。

- NAT では接続のロード バランシングが低下するので、すべてのリターン トラフィックを正しいユニットに再分散する必要があります。
- ネットワークアクセスに対する AAA は一元的な機能であるため、すべてのトラフィックが制御ユニットに転送されます。

- メンバーシップが変更されると、クラスタは大量の接続の再分散を必要とするため、一時的にクラスタ制御リンクの帯域幅を大量に使用します。

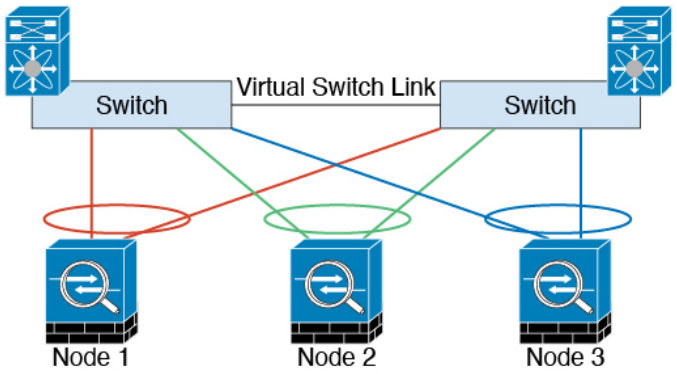
クラスタ制御リンクの帯域幅を大きくすると、メンバーシップが変更されたときの収束が高速になり、スループットのボトルネックを回避できます。

（注） クラスタに大量の非対称（再分散された）トラフィックがある場合は、クラスタ制御リンクのサイズを大きくする必要があります。

クラスタ制御リンクの冗長性

クラスタ制御リンクにはEtherChannelを使用することを推奨します。冗長性を実現しながら、EtherChannel内の複数のリンクにトラフィックを渡すことができます。

次の図は、仮想スイッチングシステム（VSS）、仮想ポートチャネル（vPC）、StackWise、またはStackWise Virtual環境でクラスタ制御リンクとしてEtherChannelを使用する方法を示します。EtherChannelのすべてのリンクがアクティブです。スイッチが冗長システムの一部である場合は、同じEtherChannel内のファイアウォールインターフェイスをそれぞれ、冗長システム内の異なるスイッチに接続できます。スイッチ インターフェイスは同じEtherChannelポートチャネルインターフェイスのメンバです。複数の個別のスイッチが単一のスイッチのように動作するからです。このEtherChannelは、スパンドEtherChannelではなく、デバイスローカルであることに注意してください。



クラスタ制御リンクの信頼性

クラスタ制御リンクの機能を保証するには、ユニット間のラウンドトリップ時間（RTT）が20 ms未満になるようにします。この最大遅延により、異なる地理的サイトにインストールされたクラスタメンバとの互換性が向上します。遅延を調べるには、ユニット間のクラスタ制御リンクでpingを実行します。

クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、サイト間の導入の場合、専用リンクを使用する必要があります。

クラスタ制御リンク ネットワーク

Firepower 4100/9300 シャーシは、シャーシ ID とスロット ID（127.2.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。クラスタを展開するときに、この IP アドレスをカスタマイズできます。クラスタ制御リンク ネットワークでは、ユニット間にルータを含めることはできません。レイヤ 2 スイッチングだけが許可されています。 サイト間トラフィックには、オーバーレイ トランスポート仮想化（OTV）を使用することをお勧めします。

クラスタ インターフェイス

1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタでは、物理インターフェイスと EtherChannel（「ポートチャネル」とも呼ばれる）の両方を割り当てることができます。クラスタに割り当てられたインターフェイスはクラスタ内のすべてのメンバーのトラフィックのロード バランシングを行うスパンド インターフェイスです。

複数のシャーシによるクラスタリングでは、データ EtherChannel のみをクラスタに割り当てできます。これらのスパンド EtherChannel は、各シャーシの同じメンバー インターフェイスを含みます。上流に位置するスイッチでは、これらのインターフェイスはすべて単一の EtherChannel に含まれ、スイッチは複数のデバイスに接続されていることを察知しません。

管理インターフェイス以外の個々のインターフェイスはサポートされていません。

冗長スイッチシステムへの接続

インターフェイスに冗長性を持たせるために、EtherChannel を VSS、vPC、StackWise、または StackWise Virtual システムなどの冗長スイッチシステムに接続することをお勧めします。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

Secure Firewall ASA クラスタの管理

ASA クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのユニットを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理タイプのインターフェイスをクラスタに割り当てる必要があります。このインターフェイスはスパンド インターフェイスではなく、特別な個別インターフェイスです。管理インターフェイスによって各ユニットに直接接続できます。

メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ユニットに属します。アドレス範囲も設定して、現在の制御ユニットを含む各ユニットがその範囲内のローカルアドレスを使用できるようにします。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ユニットが変更されると、メインクラスタ IP アドレスは新しい制御ユニットに移動するので、クラスタの管理をシームレスに続行できます。

たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の制御ユニットに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。

（注） to-the-box トラフィックをノードの管理 IP アドレスに転送する必要があります。to-the-box トラフィックは、クラスタ制御リンクを介して他のノードに転送されません。

TFTP や syslog などの発信管理トラフィックの場合、制御ユニットを含む各ユニットは、ローカル IP アドレスを使用してサーバーに接続します。

制御ユニット管理とデータユニット管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。また、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。
- ノードごとの Syslog モニタリング（コンソールレプリケーションが有効な場合にコンソールに送信される Syslog を除く）。
- SNMP
- NetFlow

暗号キー複製

制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH 接続に対して同じキーが使用されるため、新

しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

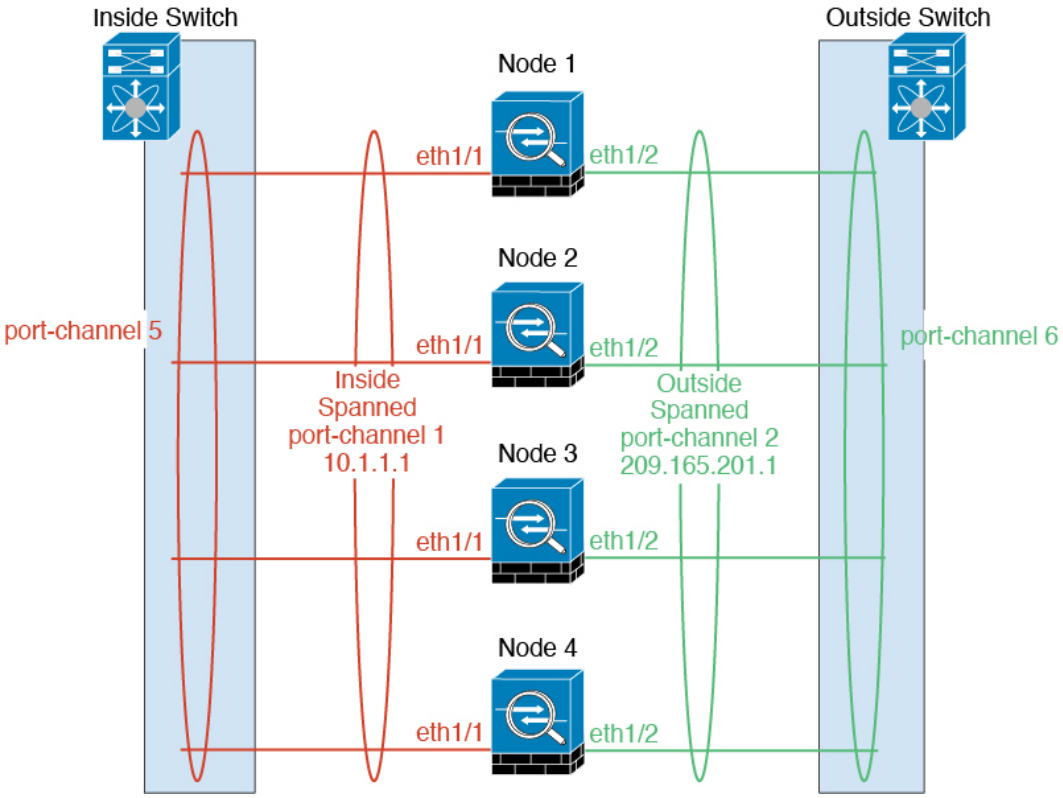
デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

スパンド EtherChannel（推奨）

シャーシあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのシャーシに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。

スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレント モードでは、IP アドレスはブリッジグループ メンバーではなく BVI に割り当てられます。

EtherChannel は初めから、ロードバランシング機能を基本的動作の一部として備えています。



サイト間クラスタリング

サイト間インストールの場合、推奨されるガイドラインに従っていれば、ASA クラスタリングを活用できます。

各クラスタ シャーシを個別のサイト ID に属するように設定できます。

サイト ID は、サイト固有の MAC アドレスおよび IP アドレスと連動します。クラスタから送信されたパケットは、サイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。サイト固有の MAC アドレスおよび IP アドレスは、スパンド EtherChannel のみを使用したルーテッド モードでサポートされます。

サイト ID は、LISP インスペクションを使用したフロー モビリティの有効化、データセンターのサイト間クラスタリングのパフォーマンス向上とラウンドトリップ時間の遅延短縮のためのディレクタ ローカリゼーションの有効化、およびトラフィック フローのバックアップ オーナーが常にオーナーとは異なるサイトに存在する接続に対するサイト冗長性の有効化のためにも使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件 （533 ページ）
- サイト間のガイドライン：クラスタリング ガイドラインと制限事項 （537 ページ）
- クラスタ フロー モビリティの設定：クラスタ フロー モビリティの設定 （569 ページ）
- ディレクタ ローカリゼーションの有効化：ディレクタ ローカリゼーションの有効化 （566 ページ）
- サイト冗長性の有効化：ディレクタ ローカリゼーションの有効化 （566 ページ）

Firepower 4100/9300 シャーシでのクラスタリングの要件と前提条件

モデルあたりの最大クラスタリング ユニット

- Firepower 4100：16 シャーシ
- Firepower 9300：16 モジュール。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。

インター シャーシ クラスタ化に関するハードウェアおよびソフトウェアの要件

クラスタ内のすべてのシャーシ：

- Firepower 4100：すべてのシャーシが同じモデルである必要があります。Firepower 9300：すべてのセキュリティ モジュールは同じタイプである必要があります。たとえば、クラスタリングを使用する場合は、Firepower 9300 のすべてのモジュールは SM-40 である必要があります。空のスロットを含め、シャーシ内にあるすべてのモジュールはクラスタに属している必要がありますが、各シャーシに設置されているセキュリティ モジュールの数はさまざまでかまいません。
- イメージアップグレード時を除き、同じ FXOS およびアプリケーション ソフトウェアを実行する必要があります。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- クラスタに割り当てるインターフェイスは、管理インターフェイス、EtherChannel、アクティブインターフェイス、スピード、デュプレックスなど、同じインターフェイス構成を含める必要があります。同じインターフェイス ID の容量が一致し、インターフェイスが同じスパンド EtherChannel に内に問題なくバンドルできる限り、シャーシに異なるタイプのネットワーク モジュールを使用できます。複数のシャーシによるクラスタでは、すべてのデータインターフェイスを EtherChannel にする必要があることに注意してください。（インターフェイスモジュールの追加や削除、または EtherChannel の設定などにより）ク

ラスタリングを有効にした後にFXOSでインターフェイスを変更した場合は、各シャーシで同じ変更を行います（データノードから始めて、制御ノードで終わります）。FXOSでインターフェイスを削除すると、必要な調整を行うことができるように、ASAの設定では関連するコマンドが保持されることに注意してください。設定からインターフェイスを削除すると、幅広い影響が生じる可能性があります。古いインターフェイス設定は手動で削除することができます。

- 同じ NTP サーバを使用する必要があります。時間を手動で設定しないでください。
- ASA：各 FXOS シャーシは、License Authority またはサテライト サーバに登録されている必要があります。データノードは追加料金なしで使用できます。永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入する必要があります。Firewall Threat Defense では、すべてのライセンスは、Firewall Management Center によって処理されます。

スイッチ要件

- Firepower 4100/9300 シャーシのクラスタリングを設定する前に、スイッチの設定を完了し、シャーシからスイッチまですべての EtherChannel を良好に接続してください。
- サポートされているスイッチの特性については、『Cisco FXOS Compatibility』を参照してください。

サイト間クラスタリング用の Data Center Interconnect のサイジング

次の計算と同等の帯域幅をクラスタ制御リンク トラフィック用にData Center Interconnect（DCI）に確保する必要があります。

$$\frac{\text{\# of cluster members per site}}{2} \times \text{cluster control link size per member}$$

メンバの数が各サイトで異なる場合、計算には大きい方の値を使用します。DCIの最小帯域幅は、1 つのメンバに対するクラスタ制御リンクのサイズ未満にすることはできません。

次に例を示します。

- 4 サイトの 2 メンバの場合。
  - 合計 4 クラスタ メンバ
  - 各サイト 2 メンバ
  - メンバあたり 5 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 5 Gbps（2/2 x 5 Gbps）。
- 3 サイトの 6 メンバの場合、サイズは増加します。
  - 合計 6 クラスタ メンバ
  - サイト 1 は 3 メンバ、サイト 2 は 2 メンバ、サイト 3 は 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

予約する DCI 帯域幅 = 15 Gbps（3/2 x 10 Gbps）。

- 2 サイトの 2 メンバの場合。
  - 合計 2 クラスタ メンバ
  - 各サイト 1 メンバ
  - メンバあたり 10 Gbps クラスタ制御リンク

  予約する DCI 帯域幅 = 10 Gbps（1/2 x 10 Gbps = 5 Gbps、ただし最小帯域幅がクラスタ制御リンク（10 Gbps）のサイズ未満になってはなりません）。

でのクラスタリングのライセンス Firepower 4100/9300 シャーシ

Smart Software Manager Regular およびオンプレミス

クラスタリング機能自体にライセンスは必要ありません。強力な暗号化およびその他のオプションのライセンスを使用するには、それぞれの Firepower 4100/9300 シャーシ がライセンス機関または Smart Software Manager の通常およびオンプレミスサーバーに登録されている必要があります。データユニットは追加料金なしで使用できます。

高度暗号化ライセンスは、登録トークンを適用すると、対象となるお客様の場合自動的に有効化されます。トークンを使用している場合、各シャーシに同じ暗号化ライセンスが必要です。ASA 設定で有効化される高度暗号化（3DES/AES）機能ライセンスについては、以下を参照してください。

ASA ライセンス設定では、制御ユニットに対するスマートライセンスの設定のみを行えます。設定はデータユニットに複製されますが、一部のライセンスに対しては、データユニットはこの設定を使用しません。この設定はキャッシュ状態のままになり、制御ユニットのみがこのライセンスを要求します。ライセンスは単一のクラスタライセンスにまとめられ、クラスタの各ユニットで共有されます。この集約ライセンスはデータユニットにもキャッシュされ、その中の 1 つが将来制御ユニットとなったときに使用されます。各ライセンス タイプは次のように処理されます:

- Essentials：制御ユニットのみがサーバーからEssentialsライセンスを要求し、ライセンスの集約により、両方のユニットがそれを使用できます。
- コンテキスト：制御ユニットのみがサーバーからコンテキストライセンスを要求します。デフォルトでEssentialsライセンスは 10 のコンテキストを含み、すべてのクラスタメンバー上に存在します。各ユニットのEssentialsライセンスの値と、制御ユニットのコンテキストライセンスの値は、集約されたクラスタライセンスでのプラットフォーム制限まで統合されます。次に例を示します。
  - クラスタに 6 台の Firepower9300 モジュールがある場合を考えます。Essentialsライセンスは 10 のコンテキストを含みます。6 つユニットの場合、合計で 60 のコンテキストが加算されます。制御ユニット上で追加の 20 コンテキストライセンスを設定しま

す。したがって、集約されたクラスタライセンスは 80 のコンテキストを含みます。モジュールごとのプラットフォーム制限は250であるため、統合されたライセンスに最大250のコンテキストが許容されます。80のコンテキストは制限範囲内です。したがって、制御ユニット上で最大 80 コンテキストを設定できます。各データユニットも、コンフィギュレーションの複製を介して80コンテキストを持つことになります。

- クラスタに Firepower 4112 が 3 台あるとします。Essentialsライセンスは 10 のコンテキストを含みます。3つユニットの場合、合計で30のコンテキストが加算されます。制御ユニット上で追加の250コンテキストライセンスを設定します。したがって、集約されたクラスタライセンスは 280 のコンテキストを含みます。ユニットごとのプラットフォームの制限が 250 であるため、統合されたライセンスでは最大250のコンテキストが許容されます。280 コンテキストは制限を超えています。したがって、制御ユニット上で最大250のコンテキストのみを設定できます。各データユニットも、コンフィギュレーションの複製を介して250のコンテキストを持つことになります。この場合では、制御ユニットのコンテキストライセンスとして220のコンテキストのみを設定する必要があります。

- キャリア：分散型 S2S VPN に必要。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。
- 高度な暗号化（3DES）：2.3.0 以前の Cisco Smart Software Manager オンプレミス展開の場合。またはスマートアカウントで高度な暗号化が許可されていないが、高度な暗号化の使用が許可されていると Cisco が判断した場合、高度な暗号化ライセンスをアカウントに手動で追加できます。このライセンスはユニットごとの権限付与であり、各ユニットはサーバーから各自のライセンスを要求します。

新しい制御ユニットが選定されると、このユニットが集約ライセンスを引き続き使用します。また、制御ユニットのライセンスを再要求するために、キャッシュされたライセンス設定も使用します。古い制御ユニットがデータユニットとしてクラスタに再度参加すると、制御ユニットのライセンス権限付与が解放されます。アカウントに利用可能なライセンスがない場合、データユニットがライセンスを解放する前に、制御ユニットのライセンスがコンプライアンス違反状態になることがあります。保持されたライセンスは 30 日間有効ですが、この猶予期間以降もコンプライアンス違反となる場合、特別なライセンスを必要とする機能の設定変更を行なえません。ただし、動作には影響ありません。新しいアクティブユニットは、ライセンスのコンプライアンスが確保されるまで 12 時間ごとに権限承認更新要求を送信します。ライセンス要求が完全に処理されるまで、設定の変更を控えてください。ユニットがクラスタから離れた場合、キャッシュされた制御ユニットの設定は削除されます。一方で、ユニットごとの権限は保持されます。この場合、クラスタ外のユニットのコンテキストライセンスを再要求する必要があります。

永続ライセンスの予約

永続ライセンスを予約するには、シャーシごとに個別のライセンスを購入し、クラスタリングを設定する前にライセンスを有効にする必要があります。

クラスタリング ガイドラインと制限事項

クラスタリングのスイッチ

- 接続されているスイッチが、クラスタ データ インターフェイスとクラスタ制御リンクインターフェイスの両方の MTU と一致していることを確認します。クラスタ制御リンクインターフェイスの MTU は、データインターフェイスの MTU より 100 バイト以上大きく設定する必要があります。そのため、スイッチを接続するクラスタ制御リンクを適切に設定してください。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。さらに、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。

- Cisco IOS XR システムでデフォルト以外の MTU を設定する場合は、クラスタデバイスの MTU よりも 14 バイト大きい IOS XR インターフェイスの MTU を設定します。そうしないと、**mtu-ignore** オプションを使用しない限り、OSPF 隣接関係ピアリングの試行が失敗する可能性があります。クラスタデバイス MTU は、IOS XR *IPv4* MTU と一致させる必要があります。この調整は、Cisco Catalyst および Cisco Nexus スイッチでは必要ありません。

- クラスタ制御リンク インターフェイスのスイッチでは、クラスタ ユニットに接続されるスイッチ ポートに対してスパニングツリー PortFast をイネーブルにすることもできます。このようにすると、新規ユニットの参加プロセスを高速化できます。

- スイッチでは、EtherChannel ロードバランシング アルゴリズム **source-dest-ip** または **src-dst-mixed-ip-port** を使用することをお勧めします（Cisco Nexus OS および Cisco IOS-XE の **port-channel load-balance** コマンドを参照）。クラスタのデバイスにトラフィックを不均一に配分する場合があるので、ロード バランス アルゴリズムでは **vlan** キーワードを使用しないでください。クラスタデバイスのデフォルトのロードバランシング アルゴリズムは変更しないでください。

- スイッチの EtherChannel ロードバランシング アルゴリズムを変更すると、スイッチの EtherChannel インターフェイスは一時的にトラフィックの転送を停止し、スパニングツリープロトコルが再始動します。トラフィックが再び流れ出すまでに、少し時間がかかります。

- クラスタ制御リンク パスのスイッチでは、L4 チェックサムを検証しないようにする必要があります。クラスタ制御リンク経由でリダイレクトされたトラフィックには、正しい L4 チェックサムが設定されていません。L4 チェックサムを検証するスイッチにより、トラフィックがドロップされる可能性があります。

- ポートチャネル バンドルのダウンタイムは、設定されているキープアライブ インターバルを超えてはなりません。

- Supervisor 2T EtherChannel では、デフォルトのハッシュ配信アルゴリズムは適応型です。VSS設計での非対称トラフィックを避けるには、クラスタ デバイスに接続されているポートチャネルでのハッシュ アルゴリズムを固定に変更します。

  router(config)# **port-channel** *id* **hash-distribution fixed**

  アルゴリズムをグローバルに変更しないでください。VSS ピア リンクに対しては適応型アルゴリズムを使用できます。

- ASA ハードウェアクラスタとは異なり、Firepower 4100/9300 クラスタは LACP グレースフル コンバージェンスをサポートしています。したがって、プラットフォームでは、接続されている Cisco Nexus スイッチで LACP グレースフル コンバージェンスを有効のままにしておくことができます。

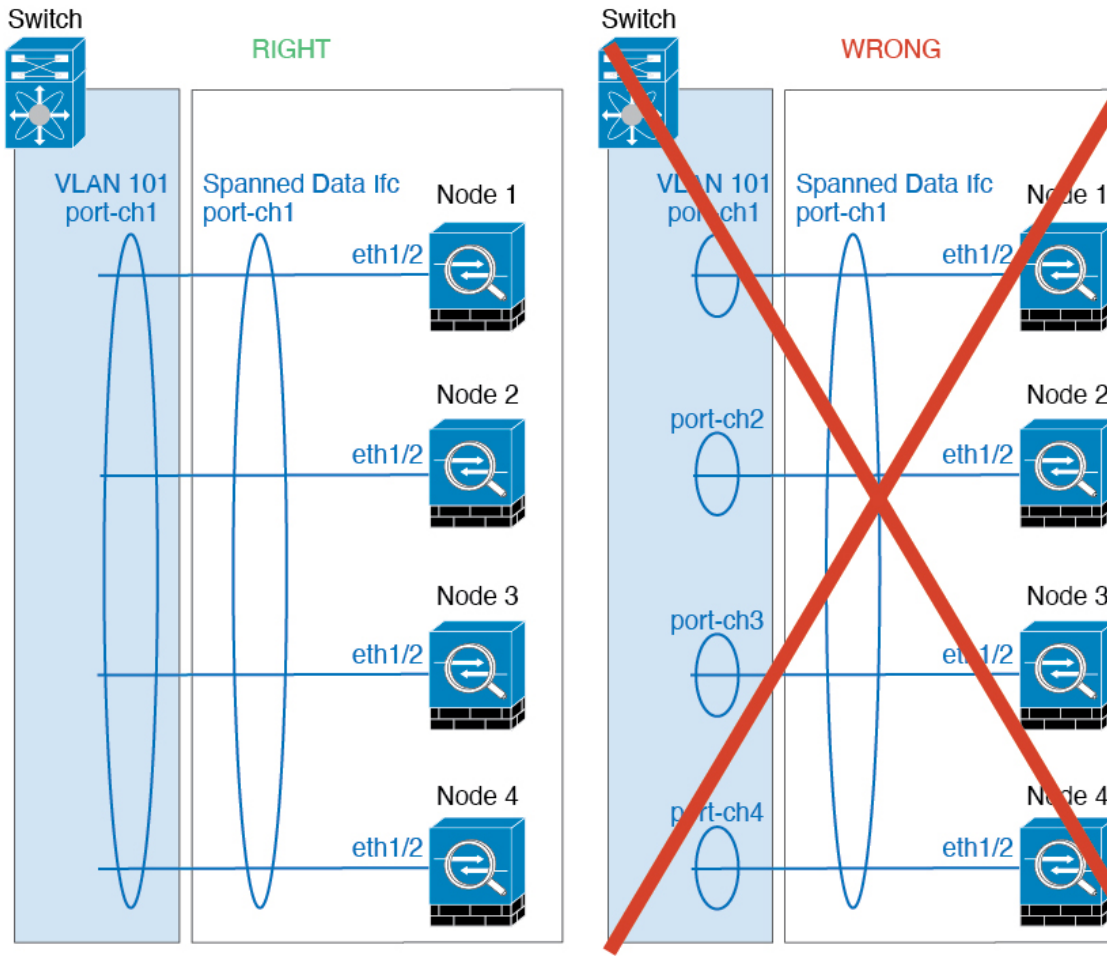
- スイッチ上のスパンド EtherChannel のバンドリングが遅いときは、スイッチの個別インターフェイスに対して LACP 高速レートをイネーブルにできます。FXOS EtherChannel にはデフォルトで [高速（fast）] に設定されている LACP レートがあります。Nexus シリーズなど一部のスイッチでは、インサービス ソフトウェア アップグレード（ISSU）を実行する際にLACP高速レートがサポートされないことに注意してください。そのため、クラスタリングで ISSU を使用することは推奨されません。

クラスタリングの EtherChannel

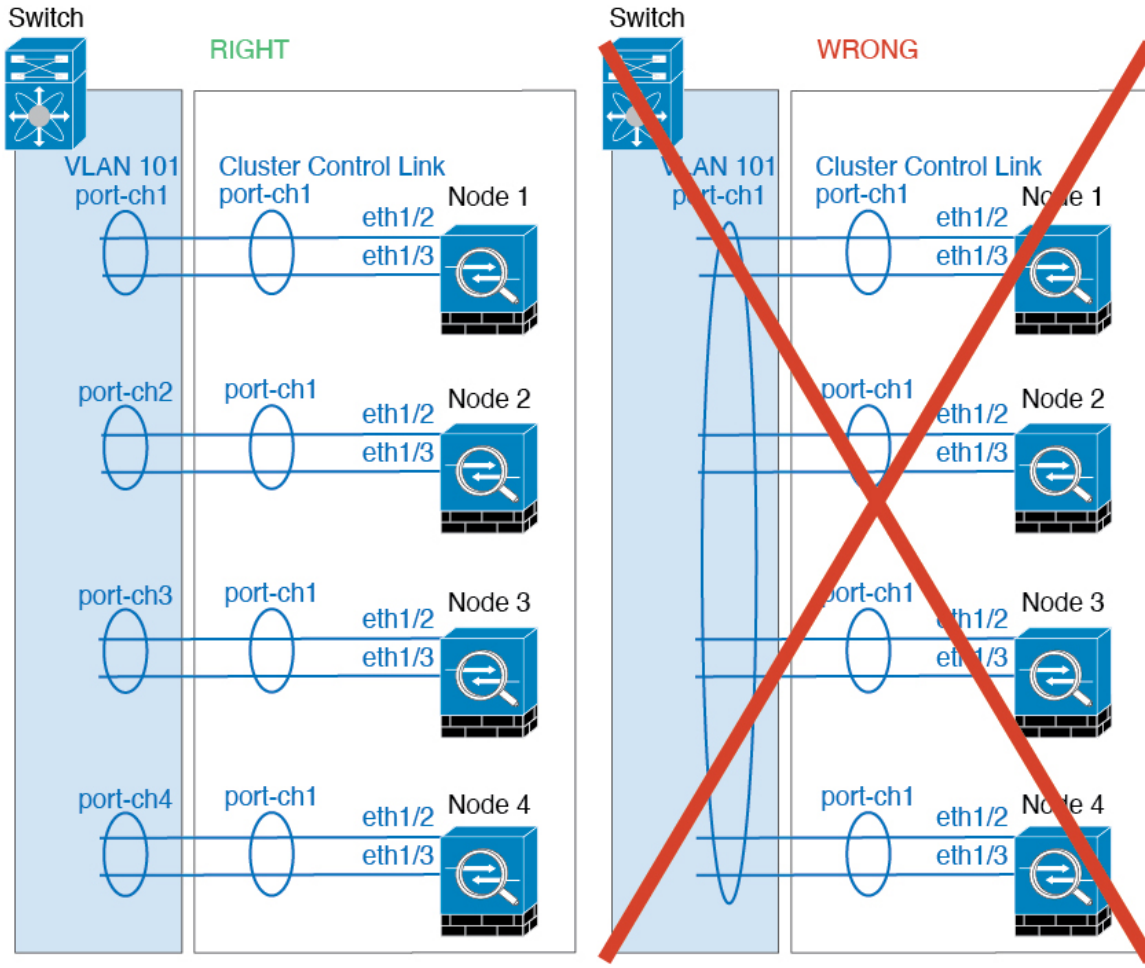
- 15.1(1)S2 より前の Catalyst 3750-X Cisco IOS ソフトウェア バージョンでは、クラスタ ユニットはスイッチ スタックに EtherChannel を接続することをサポートしていませんでした。デフォルトのスイッチ設定では、クラスタユニット EtherChannel がクロススタックに接続されている場合、制御ユニットのスイッチの電源がオフになると、残りのスイッチに接続されている EtherChannel は起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば 8 分、0 （無制限）などを設定します。または、15.1(1)S2 など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。

- スパンド EtherChannel とデバイス ローカル EtherChannel のコンフィギュレーション：スパンド EtherChannel と デバイス ローカル EtherChannel に対してスイッチを適切に設定します。

  - スパンド EtherChannel：クラスタ ユニット スパンド EtherChannel（クラスタのすべてのメンバに広がる）の場合は、複数のインターフェイスが結合されてスイッチ上の単一の EtherChannel となります。各インターフェイスがスイッチ上の同じチャネル グループ内にあることを確認してください。



- デバイス ローカル EtherChannel：クラスタ ユニット デバイス ローカル EtherChannel（クラスタ制御リンク用に設定された EtherChannel もこれに含まれます）は、それぞれ独立した EtherChannel としてスイッチ上で設定してください。スイッチ上で複数のクラスタ ユニット EtherChannel を結合して 1 つの EtherChannel としないでください。



サイト間クラスタリング

サイト間クラスタリングについては、次のガイドラインを参照してください。

- クラスタ制御リンクの遅延が、ラウンドトリップ時間（RTT）20 ms 未満である必要があります。
- クラスタ制御リンクは、順序の異常やパケットのドロップがない信頼性の高いものである必要があります。たとえば、専用リンクを使用する必要があります。
- 接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには接続を再分散できません。
- ASA は専用リンクであるため、データセンター相互接続（DCI）で使用されている場合でも、クラスタ制御リンクで転送されるデータトラフィックを暗号化しません。オーバーレイトランスポート仮想化（OTV）を使用する場合、またはローカル管理ドメインの外部でクラスタ制御リンクを拡張する場合は、OTE を介した 802.1AE MacSec などの境界ルータで暗号化を設定できます。

- クラスタの実装では、着信接続用の複数のサイトでメンバが区別されません。したがって、特定の接続に対する接続のロールが複数のサイトにまたがる場合があります。これは想定されている動作です。ただし、ディレクタのローカリゼーションを有効にすると、ローカルディレクタのロールは常に（サイト ID に従って）接続オーナーと同じサイトから選択されます。また、元のオーナーに障害が発生すると、ローカルディレクタが同じサイトで新しいオーナーを選択します（注：サイト間でトラフィックが非対称で、元のオーナーに障害が発生した後もリモートサイトから継続的にトラフィックが発生する場合、リモートサイトのノードが再ホスティングウィンドウ内でデータパケットを受信する場合にはこのリモートサイトのノードが新しいオーナーとなることがあります）。
- ディレクタ ローカリゼーションでは、次のトラフィック タイプのローカリゼーションをサポートしていません。NAT または PAT のトラフィック、SCTP がインスペクションを行うトラフィック、オーナーのフラグメンテーション クエリ。
- ノースサウス展開での UDP の長期的フローでは、元のフローの所有者サイトのノードに障害が発生してから復帰し、その後フローが元のサイトに戻されると、ルーティング ループが発生する可能性があります。他のサイトの新しい所有者に宛先へのルートがない場合、フローがインターネットに戻され、ループが発生します。この場合、新しい所有者に対して **clear conn** コマンドを使用して、強制的にフローを再確立します。
- トランスペアレント モードの場合、内部ルータと外部ルータのペア間にクラスタを配置すると（AKA ノースサウス挿入）、両方の内部ルータが同じ MAC アドレスを共有し、両方の外部ルータが同じ MAC アドレスを共有する必要があります。サイト 1 のクラスタ メンバがサイト 2 のメンバに接続を転送するとき、宛先 MAC アドレスは維持されます。MAC アドレスがサイト 1 のルータと同じである場合にのみ、パケットはサイト 2 のルータに到達します。
- トランスペアレント モードの場合、内部ネットワーク間のファイル用に各サイトのデータ ネットワークとゲートウェイ ルータ間にクラスタを配置すると（AKA イーストウェスト挿入）、各ゲートウェイ ルータは、HSRP などの First Hop Redundancy Protocol（FHRP）を使用して、各サイトで同じ仮想 IP および MAC アドレスの宛先を提供します。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）または同様のものを使用してサイト全体にわたって拡張されます。ローカル ゲートウェイ ルータ宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。ゲートウェイ ルータが 1 つのサイトで到達不能になった場合、トラフィックが正常に他のサイトのゲートウェイに到達できるようにフィルタを削除する必要があります。
- トランスペアレントモードでは、クラスタが HSRP ルータに接続されている場合、ルータの HSRP MAC アドレスを静的 MAC アドレステーブルエントリとして ASA に追加する必要があります（ブリッジ グループのスタティック MAC アドレスの追加 （1114 ページ）を参照）。隣接ルータで HSRP が使用される場合、HSRP IP アドレス宛てのトラフィックは HSRP MAC アドレスに送信されますが、リターントラフィックは特定のルータのインターフェイスの MAC アドレスから HSRP ペアで送信されます。したがって、ASA MAC アドレステーブルは通常、HSRP IP アドレスの ASA ARP テーブルエントリが期限切れになり、ASA が ARP 要求を送信して応答を受信した場合にのみ更新されます。ASA の ARP テーブルエントリはデフォルトで 14400 秒後に期限切れになりますが、MAC アドレステーブルエントリはデフォルトで 300 秒後に期限切れになるため、MAC アドレステーブルの期

限切れトラフィックのドロップを回避するために静的 MAC アドレスエントリが必要です。

- スパンド EtherChannel を使用したルーテッド モードでは、サイト固有の MAC アドレスを設定します。OTV または同様のものを使用してサイト全体にデータ VLAN を拡張します。グローバル MAC アドレス宛てのトラフィックが DCI 経由で他のサイトに送信されないようにするには、フィルタを作成する必要があります。クラスタが 1 つのサイトで到達不能になった場合、トラフィックが他のサイトのクラスタノードに正常に到達できるようにフィルタを削除する必要があります。ダイナミック ルーティングは、サイト間クラスタが拡張セグメントのファースト ホップ ルータとして機能する場合はサポートされません。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、Firepower 4100/9300 シャーシ上でのインターフェイスまたはスイッチの有効化または無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスのインターフェイス モニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。
- ユニットを既存のクラスタに追加したときや、ユニットをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは想定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- スパンド EtherChannel インターフェイスに接続された Windows 2003 Server を使用している場合、syslog サーバポートがダウンしたときにサーバが ICMP エラーメッセージを抑制しないと、多数の ICMP メッセージがクラスタに送信されることになります。このようなメッセージにより、クラスタの一部のユニットで CPU 使用率が高くなり、パフォーマンスに影響する可能性があります。ICMP エラー メッセージを調節することを推奨します。
- 冗長性を持たせるため、VSS、vPC、StackWise、または StackWise Virtual に EtherChannel を接続することを推奨します。
- シャーシ内では、スタンドアロン モードで一部のシャーシ セキュリティ モジュールをクラスタ化し、他のセキュリティ モジュールを実行することはできません。クラスタ内にすべてのセキュリティ モジュールを含める必要があります。

デフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は 3 秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。

- 失敗したクラスタ制御リンクのクラスタ自動再参加機能は、5 分間隔で無制限に試行されるように設定されます。
- 失敗したデータインターフェイスのクラスタ自動再参加機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

でのクラスタリングの設定 Firepower 4100/9300 シャーシ

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。このセクションでは、デフォルトのブートストラップ設定と ASA で実行できるオプションのカスタマイズについて説明します。また、ASA 内からクラスタ メンバーを管理する方法についても説明します。クラスタ メンバーシップは Firepower 4100/9300 シャーシからも管理できます。詳細については、Firepower 4100/9300 シャーシ のマニュアルを参照してください。

手順

ステップ 1 FXOS：ASA クラスタの追加 （543 ページ）
ステップ 2 ASA：ファイアウォール モードとコンテキスト モードの変更 （555 ページ）
ステップ 3 ASA：データ インターフェイスの設定 （555 ページ）
ステップ 4 ASA：クラスタ設定のカスタマイズ （558 ページ）
ステップ 5 ASA：クラスタ メンバの管理 （584 ページ）

FXOS：ASA クラスタの追加

単独の Firepower 9300 シャーシをシャーシ内クラスタとして追加することも、複数のシャーシをシャーシ間クラスタリングに追加することもできます。 シャーシ間クラスタリングでは、各シャーシを別々に設定します。1 つのシャーシにクラスタを追加したら、次のシャーシにほぼ同じ設定を入力します。

ASA クラスタの作成

範囲をイメージバージョンに設定します。

クラスタは、Firepower 4100/9300 シャーシ スーパバイザから簡単に展開できます。すべての初期設定が各ユニット用に自動生成されます。

複数のシャーシにわたるクラスタリングの場合は、各シャーシを個別に設定する必要があります。導入を容易にするために、1 つのシャーシにクラスタを導入し、その後、最初のシャーシから次のシャーシにブートストラップ コンフィギュレーションをコピーできます。

Firepower 9300 シャーシでは、モジュールがインストールされていない場合でも、3 つのすべてのモジュールでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

マルチ コンテキスト モードの場合、最初に論理デバイスを展開してから、ASA アプリケーションでマルチ コンテキスト モードを有効にする必要があります。

クラスタを導入すると、Firepower 4100/9300 シャーシ スーパバイザが次のブートストラップ コンフィギュレーションで各 ASA アプライアンスを設定します。ブートストラップ コンフィギュレーションの一部（**太字**のテキストで示されている部分）は、後から必要に応じて ASA から変更できます。

```
interface Port-channel48
   description Clustering Interface
cluster group <service_type_name>
   key <secret>
   local-unit unit-<chassis#-module#>
   site-id <number>
   cluster-interface port-channel48 ip 127.2.<chassis#>.<module#> 255.255.255.0
   priority <auto>
   health-check holdtime 3
   health-check data-interface auto-rejoin 3 5 2
   health-check cluster-interface auto-rejoin unlimited 5 1
   enable

ip local pool cluster_ipv4_pool <ip_address>-<ip_address> mask <mask>

interface <management_ifc>
   management-only individual
   nameif management
   security-level 0
   ip address <ip_address> <mask> cluster-pool cluster_ipv4_pool
   no shutdown

http server enable
http 0.0.0.0 0.0.0.0 management
route management <management_host_ip> <mask> <gateway_ip> 1
```

（注） **local-unit** 名は、クラスタリングを無効化した場合にのみ変更できます。

始める前に

- 論理デバイスに使用するアプリケーションイメージを Cisco.com からダウンロードして、そのイメージを Firepower 4100/9300 シャーシ にアップロードします。
- 次の情報を用意します。
  - 管理インターフェイス ID、IP アドレスおよびネットワークマスク
  - ゲートウェイ IP アドレス

手順

ステップ 1 インターフェイスを設定します。

a) クラスタを展開する前に、1 つ以上のデータ タイプのインターフェイスまたは EtherChannel（ポートチャネルとも呼ばれる）を追加します。EtherChannel（ポート チャネル）の追加（216 ページ）または物理インターフェイスの設定 （213 ページ）を参照してください。

複数のシャーシにわたるクラスタリングの場合は、すべてのデータインターフェイスが、少なくとも 1 つのメンバーインターフェイスを持つスパンド EtherChannel である必要があります。各シャーシに同じ EtherChannel を追加します。スイッチ上で、すべてのクラスタユニットからメンバーインターフェイスを 1 つの EtherChannel へと結合します。EtherChannel の詳細については、クラスタリング ガイドラインと制限事項 （537 ページ）を参照してください。

b) 管理タイプのインターフェイスまたは EtherChannel を追加します。EtherChannel（ポートチャネル）の追加 （216ページ）または物理インターフェイスの設定 （213ページ）を参照してください。

管理インターフェイスが必要です。この管理インターフェイスは、シャーシの管理のみに使用されるシャーシ管理インターフェイスと同じではありません（FXOS では、シャーシ管理インターフェイスは MGMT、management0 のような名前で表示されます）。

複数のシャーシにわたるクラスタリングの場合、各シャーシに同じ管理インターフェイスを追加します。

c) 複数のシャーシにわたるクラスタリングでは、メンバーインターフェイスをクラスタ制御リンクの EtherChannel（デフォルトではポートチャネル 48）に追加します。EtherChannel （ポート チャネル）の追加 （216 ページ） を参照してください。

1 つの Firepower 9300 シャーシ内のセキュリティモジュールに隔離されたクラスタのメンバーインターフェイスを追加しないでください。メンバーを追加すると、シャーシはこのクラスタが複数のシャーシを使用すると見なし、たとえば、スパンド EtherChannel の使用のみが許可されます。

各シャーシに同じメンバインターフェイスを追加します。クラスタ制御リンクは、各シャーシのデバイスローカル EtherChannel です。デバイスごとにスイッチで個別の EtherChannel を使用します。EtherChannel の詳細については、クラスタリング ガイドラインと制限事項 （537 ページ）を参照してください。

ステップ 2 セキュリティ サービス モードを開始します。

scope ssa

例：

```
Firepower# scope ssa
Firepower /ssa #
```

ステップ 3 アプリケーション インスタンス パラメータ（イメージ バージョンを含む）を設定します。

a) 使用可能なイメージを表示します。使用するバージョン番号を書き留めます。

show app

例：

```
Firepower /ssa # show app
    Name       Version         Author     Supported Deploy Types CSP Type    Is
Default App
    ---------- --------------- ---------- ---------------------- -----------
--------------
    asa        9.9.1           cisco      Native                 Application No
    asa        9.10.1          cisco      Native                 Application Yes
    ftd        6.2.3           cisco      Native                 Application Yes
    ftd        6.3.0           cisco      Native,Container       Application Yes
```

b) 範囲をイメージバージョンに設定します。

scope app asa *application_version*

例：

```
Firepower /ssa # scope app asa 9.10.1
Firepower /ssa/app #
```

c) このバージョンをデフォルトとして設定します。

set-default

例：

```
Firepower /ssa/app # set-default
Firepower /ssa/app* #
```

d) 終了して ssa モードを開始します。

exit

例：

```
Firepower /ssa/app* # exit
Firepower /ssa* #
```

例：

```
Firepower /ssa # scope app asa 9.12.1
Firepower /ssa/app # set-default
Firepower /ssa/app* # exit
Firepower /ssa* #
```

ステップ 4 クラスタを作成します。

enter logical-device *device_name* **asa** *slots* **clustered**

- *device_name*：Firepower 4100/9300 シャーシスーパバイザがクラスタリングを設定してインターフェイスを割り当てるために使用します。この名前は、セキュリティモジュール設定で使用されるクラスタ名ではありません。まだハードウェアをインストールしていない場合でも、3 つすべてのセキュリティ モジュールを指定する必要があります。
- スロット: シャーシ モジュールをクラスタに割り当てます。Firepower 4100 の場合は、**1** を指定します。Firepower 9300 の場合は、**1,2,3** を指定します。モジュールがインストールされていない場合でも、Firepower 9300 シャーシの 3 つすべてのモジュール スロットでクラスタリングを有効にする必要があります。3 つすべてのモジュールを設定していないと、クラスタは機能しません。

例：

```
Firepower /ssa # enter logical-device ASA1 asa 1,2,3 clustered
Firepower /ssa/logical-device* #
```

ステップ 5 クラスタブートストラップのパラメータを設定します。

これらの設定は、初期導入専用、またはディザスタ リカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

a) クラスタ ブートストラップ オブジェクトを作成します。

enter cluster-bootstrap

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* #
```

b) シャーシ ID を設定します。

set chassis-id *id*

クラスタの各シャーシは一意の ID が必要です。

c) サイト間クラスタリングの場合、サイト ID は 1 ～ 8 の範囲で設定します。

set site-id *number*.

サイト ID を削除するには、値を **0** に設定します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set site-id 1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

d) クラスタ制御リンクの制御トラフィック用の認証キーを設定します。

set key

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set key
```

```
Key: diamonddogs
```

共有秘密を入力するように求められます。

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このオプションは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

e) クラスタ インターフェイス モードを設定します。

set mode spanned-etherchannel

サポートされているモードは、スパンド EtherChannel モードのみです。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
Firepower /ssa/logical-device/cluster-bootstrap* #
```

f) セキュリティ モジュール設定でクラスタ グループ名を設定します。

set service-type *cluster_name*

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* #
```

g) （任意） Cluster Control Link IP ネットワークを設定します。

set cluster-control-link network*a*.*b*.**0.0**

クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。この場合、クラスタの固有ネットワークに任意の /16 ネットワーク アドレスを指定できます。

- ***a*.*b*.0.0**：任意の /16 ネットワークアドレスを指定します（ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）のアドレスを除く）。値を 0.0.0.0 に設定すると、デフォルトのネットワーク（127.2.0.0）が使用されます。

シャーシは、シャーシ ID とスロット ID（*a*.*b*.*chassis_id*.*slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイスの IP アドレスを自動生成します。

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set cluster-control-link network
 10.10.0.0
```

h) 管理 IP アドレス情報を設定します。

この情報は、セキュリティ モジュール設定で管理インターフェイスを設定するために使用されます。

1. ローカル IP アドレスのプールを設定します。このアドレスの 1 つが、インターフェイス用の各クラスタユニットに割り当てられます。

   set ipv4 pool *start_ip end_ip*

   set ipv6 pool *start_ip end_ip*

   最低でも、クラスタ内のユニット数と同じ数のアドレスが含まれるようにしてください。Firepower 9300 の場合、すべてのモジュール スロットが埋まっていないとしても、シャーシごとに 3 つのアドレスを含める必要があることに注意してください。クラスタを拡張する予定の場合は、アドレスを増やします。現在の制御ユニットに属する仮想 IP アドレス（メインクラスタ IP アドレスと呼ばれる）は、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。IPv4 アドレスと IPv6 アドレス（どちらか一方も可）を使用できます。

2. 管理インターフェイスのメインクラスタ IP アドレスを設定します。

   set virtual ipv4 *ip_address* **mask** *mask*

   set virtual ipv6 *ip_address* **prefix-length** *prefix*

   この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。

3. ネットワーク ゲートウェイ アドレスを入力します。

   set ipv4 gateway *ip_address*

   set ipv6 gateway *ip_address*

例：

```
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 gateway 10.1.1.254
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv4 pool 10.1.1.11 10.1.1.27
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 gateway 2001:DB8::AA
Firepower /ssa/logical-device/cluster-bootstrap* # set ipv6 pool 2001:DB8::11
2001:DB8::27
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv4 10.1.1.1 mask
255.255.255.0
Firepower /ssa/logical-device/cluster-bootstrap* # set virtual ipv6 2001:DB8::1
prefix-length 64
```

i) クラスタ ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device* # enter cluster-bootstrap
Firepower /ssa/logical-device/cluster-bootstrap* # set chassis-id 1
Firepower /ssa/logical-device/cluster-bootstrap* # set key
  Key: f@arscape
Firepower /ssa/logical-device/cluster-bootstrap* # set mode spanned-etherchannel
```

```
Firepower /ssa/logical-device/cluster-bootstrap* # set service-type cluster1
Firepower /ssa/logical-device/cluster-bootstrap* # exit
Firepower /ssa/logical-device/* #
```

ステップ 6 管理ブートストラップパラメータを設定します。

これらの設定は、初期導入専用、またはディザスタリカバリ用です。通常の運用では、後でアプリケーション CCLI 設定のほとんどの値を変更できます。

a) 管理ブートストラップ オブジェクトを作成します。

enter mgmt-bootstrap asa

例：

```
Firepower /ssa/logical-device* # enter mgmt-bootstrap asa
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

b) admin とイネーブル パスワードを指定します。

create bootstrap-key-secret PASSWORD

set value

値の入力：*password*

値の確認：*password*

exit

例：

事前設定されている ASA 管理者ユーザおよびイネーブル パスワードはパスワードの回復時に役立ちます。FXOS アクセスができる場合、管理者ユーザ パスワードを忘れたときにリセットできます。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key-secret PASSWORD
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # set value
Enter a value: floppylampshade
Confirm the value: floppylampshade
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key-secret* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

c) ファイアウォール モード（「ルーテッド」または「トランスペアレント」）を指定します。

create bootstrap-key FIREWALL_MODE

set value {**routed** | **transparent**}

exit

ルーテッドモードでは、デバイスはネットワーク内のルータ ホップと見なされます。ルーティングを行う各インターフェイスは異なるサブネット上にあります。一方、トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォー

ル」のように機能するレイヤ 2 ファイアウォールであり、接続されたデバイスへのルータ ホップとしては認識されません。

ファイアウォールモードは初期展開時にのみ設定します。ブートストラップの設定を再適用する場合、この設定は使用されません。

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # create bootstrap-key FIREWALL_MODE
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # set value routed
Firepower /ssa/logical-device/mgmt-bootstrap/bootstrap-key* # exit
Firepower /ssa/logical-device/mgmt-bootstrap* #
```

d) 管理ブートストラップ モードを終了します。

exit

例：

```
Firepower /ssa/logical-device/mgmt-bootstrap* # exit
Firepower /ssa/logical-device* #
```

ステップ 7 設定を保存します。

commit-buffer

シャーシは、指定したソフトウェアバージョンをダウンロードし、アプリケーションインスタンスにブートストラップ設定と管理インターフェイス設定をプッシュすることで、論理デバイスを導入します。**show app-instance** コマンドを使用して、展開のステータスを確認します。[Admin State（管理状態）] が [Enabled（有効）] で、[Oper State] が [Online] の場合、アプリケーション インスタンスは実行中であり、使用できる状態になっています。

例：

```
Firepower /ssa/logical-device* # commit-buffer
Firepower /ssa/logical-device # exit
Firepower /ssa # show app-instance
App Name   Identifier Slot ID    Admin State Oper State       Running Version Startup
Version Deploy Type Profile Name Cluster State   Cluster Role
---------- ---------- ---------- ----------- ---------------- ---------------
--------------- ----------- ------------ ---------------- -------------
ftd        cluster1   1          Enabled     Online           7.3.0.49        7.3.0.49
       Native                   In Cluster      Data Node
ftd        cluster1   2          Enabled     Online           7.3.0.49        7.3.0.49
       Native                   In Cluster      Control Node
ftd        cluster1   3          Disabled    Not Available                    7.3.0.49
       Native                   Not Applicable  None
```

ステップ 8 クラスタに別のシャーシを追加する場合は、この手順を繰り返しますが、固有の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、両方のシャーシで同じ設定を使用します。

インターフェイス コンフィギュレーションが新しいシャーシと同じであることを確認します。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。

ステップ 9 制御ユニット ASA に接続して、クラスタリング設定をカスタマイズします。

例

シャーシ 1：

```
scope eth-uplink
  scope fabric a
    enter port-channel 1
      set port-type data
      enable
      enter member-port Ethernet1/1
        exit
      enter member-port Ethernet1/2
        exit
      exit
    enter port-channel 2
      set port-type data
      enable
      enter member-port Ethernet1/3
        exit
      enter member-port Ethernet1/4
        exit
      exit
    enter port-channel 3
      set port-type data
      enable
      enter member-port Ethernet1/5
        exit
      enter member-port Ethernet1/6
        exit
      exit
    enter port-channel 4
      set port-type mgmt
      enable
      enter member-port Ethernet2/1
        exit
      enter member-port Ethernet2/2
        exit
      exit
    enter port-channel 48
      set port-type cluster
      enable
      enter member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer

scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 1
```

```
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.27
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::27
      set key
      Key: f@arscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

シャーシ 2：

```
scope eth-uplink
  scope fabric a
    create port-channel 1
      set port-type data
      enable
      create member-port Ethernet1/1
        exit
      create member-port Ethernet1/2
        exit
      exit
    create port-channel 2
      set port-type data
      enable
      create member-port Ethernet1/3
        exit
      create member-port Ethernet1/4
        exit
      exit
    create port-channel 3
      set port-type data
      enable
      create member-port Ethernet1/5
        exit
      create member-port Ethernet1/6
        exit
      exit
    create port-channel 4
      set port-type mgmt
      enable
      create member-port Ethernet2/1
        exit
      create member-port Ethernet2/2
        exit
      exit
    create port-channel 48
      set port-type cluster
      enable
      create member-port Ethernet2/3
        exit
      exit
    exit
  exit
commit-buffer
```

```
scope ssa
  enter logical-device ASA1 asa "1,2,3" clustered
    enter cluster-bootstrap
      set chassis-id 2
      set ipv4 gateway 10.1.1.254
      set ipv4 pool 10.1.1.11 10.1.1.15
      set ipv6 gateway 2001:DB8::AA
      set ipv6 pool 2001:DB8::11 2001:DB8::19
      set key
      Key: f@rscape
      set mode spanned-etherchannel
      set service-type cluster1
      set virtual ipv4 10.1.1.1 mask 255.255.255.0
      set virtual ipv6 2001:DB8::1 prefix-length 64
      exit
    exit
  scope app asa 9.5.2.1
    set-default
    exit
  commit-buffer
```

クラスタ メンバの追加

ASA クラスタメンバーを追加または置き換えます。

（注） この手順は、シャーシの追加または置換にのみ適用されます。クラスタリングがすでに有効になっている Firepower 9300 にモジュールを追加または置換する場合、モジュールは自動的に追加されます。

始める前に

- 既存のクラスタに、この新しいメンバ用の管理 IP アドレスプール内で十分な IP アドレスが割り当てられているようにしてください。それ以外の場合は、この新しいメンバを追加する前に、各シャーシ上の既存のクラスタ ブートストラップ設定を編集する必要があります。この変更により論理デバイスが再起動します。
- インターフェイスの設定は、新しいシャーシでの設定と同じである必要があります。FXOS シャーシ設定をエクスポートおよびインポートし、このプロセスを容易にすることができます。
- マルチ コンテキスト モードでは、最初のクラスタ メンバの ASA アプリケーションでマルチ コンテキスト モードを有効にします。追加のクラスタ メンバはマルチ コンテキスト モード設定を自動的に継承します。

手順

ステップ 1 [OK] をクリックします。

ステップ 2 クラスタに別のシャーシを追加する場合は、ASA クラスタの作成（543 ページ）の手順を繰り返しますが、一意の **chassis-id** と正しい **site-id** を設定する必要があります。それ以外の場合は、新しいシャーシに同じ設定を使用します。

ASA：ファイアウォール モードとコンテキスト モードの変更

デフォルトでは、FXOS シャーシはルーテッド ファイアウォール モード、およびシングル コンテキスト モードでクラスタを展開します。

- ファイアウォールモードの変更：展開後にモードを変更するには、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。を参照してください。ファイアウォールモードの設定（243 ページ）マルチコンテキストモードでは、コンテキストごとにファイアウォールモードを設定します。
- マルチコンテキストモードに変更：展開後にマルチコンテキストモードに変更するには、制御ユニットでモードを変更します。これにより、すべてのデータユニットのモードが一致するように自動的に変更されます。マルチコンテキストモードの有効化（278 ページ）を参照してください。

ASA：データ インターフェイスの設定

この手順では、FXOS にクラスタを展開したときにクラスタに割り当てられた各データ インターフェイスの基本的なパラメータを設定します。複数のシャーシにわたるクラスタリングの場合、データインターフェイスは常にスパンド EtherChannel インターフェイスです。

（注） 管理インターフェイスは、クラスタを展開したときに事前設定されました。ASA で管理インターフェイス パラメータを変更することもできますが、この手順はデータ インターフェイスに焦点を当てています。管理インターフェイスは、スパンドインターフェイスとは対照的に、個別のインターフェイスです。詳細については、「管理インターフェイス（530 ページ）」を参照してください。

始める前に

- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで開始します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- トランスペアレント モードの場合は、ブリッジ グループを設定します。 ブリッジ仮想インターフェイス（BVI）の設定（937 ページ）を参照してください。
- 複数のシャーシによるクラスタにスパンド EtherChannel を使用している場合、クラスタリングが完全に有効になるまで、ポートチャネルインターフェイスは起動しません。この要

件により、クラスタのアクティブではないノードにトラフィックが転送されるのが防がれます。

手順

ステップ 1 インターフェイス ID を指定します

interface *id*

このクラスタに割り当てられているインターフェイスのFXOSシャーシを参照してください。インターフェイス ID には、次のものがあります。

- **port-channel** *integer*
- **ethernet** *slot/port*

例：

```
ciscoasa(config)# interface port-channel 1
```

ステップ 2 インターフェイスをイネーブルにします。

no shutdown

ステップ 3 （オプション）このインターフェイス上に VLAN サブインターフェイスを作成する予定の場合は、この時点で作成します。

例：

```
ciscoasa(config)# interface port-channel 1.10
ciscoasa(config-if)# vlan 10
```

この手順の残りの部分は、サブインターフェイスに適用されます。

ステップ 4 （マルチ コンテキスト モード）インターフェイスをコンテキストに割り当ててから、コンテキストに変更し、インターフェイス モードを開始します。

例：

```
ciscoasa(config)# context admin
ciscoasa(config)# allocate-interface port-channel1
ciscoasa(config)# changeto context admin
ciscoasa(config-if)# interface port-channel 1
```

マルチ コンテキスト モードの場合は、インターフェイス コンフィギュレーションの残りの部分は各コンテキスト内で行われます。

ステップ 5 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 6 ファイアウォール モードに応じて、次のいずれかを実行します。

- ルーテッド モード：IPv4 アドレスと IPv6 アドレスの一方または両方を設定します。

  （IPv4）

  ip address *ip_address* [*mask*]

  （IPv6）

  ipv6 address *ipv6-prefix*/*prefix-length*

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
  ciscoasa(config-if)# ipv6 address 2001:DB8::1001/32
  ```

  DHCP、PPPoE、および IPv6 自動設定はサポートされません。ポイントツーポイント接続の場合、31 ビットのサブネット マスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。リンクローカルアドレスの手動設定もサポートされていません。

- トランスペアレント モード：インターフェイスをブリッジ グループに割り当てます。

  bridge-group *number*

  例：

  ```
  ciscoasa(config-if)# bridge-group 1
  ```

  number は、1 ～ 100 の整数です。ブリッジ グループには最大 64 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジグループに割り当てることはできません。BVI のコンフィギュレーションには IP アドレスが含まれていることに注意してください。

ステップ 7 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 8 （複数のシャーシにわたるクラスタリング）潜在的なネットワークの接続問題を回避するために、スパンド EtherChannel の固有で、手動のグローバル MAC アドレスを設定します。

mac-address *mac_address*

- *mac_address*：MAC アドレスは、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

ネットワーク上で現在使用されていない一意の MAC アドレスを設定する必要があります。MAC アドレスが手動設定されている場合、その MAC アドレスは現在の制御ユニットに留まります。MAC アドレスを設定していない場合に、制御ユニットが変更された場合、新しい制御ユニットはインターフェイスに新しい MAC アドレスを使用します。これにより、一時的なネットワークの停止が発生する可能性があります。

マルチコンテキストモードでは、コンテキスト間でインターフェイスを共有する場合は、MAC アドレスの自動生成を有効にして、手動で MAC アドレスを設定しなくてすむようにします。非共有インターフェイスの場合は、このコマンドを使用して MAC アドレスを手動で設定する必要があることに注意してください。

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

ステップ 9 （シャーシ間のクラスタリング）サイトごとにサイト固有の MAC アドレスを、ルーテッドモードの場合は IP アドレスを設定します。

mac-address *mac_address* **site-id** *number* **site-ip** *ip_address*

例：

```
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.9.9.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.9.9.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.9.9.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.9.9.4
```

サイト固有の IP アドレスは、グローバル IP アドレスと同じサブネット上にある必要があります。ユニットで使用するサイト固有の MAC アドレスおよび IP アドレスは、各ユニットのブートストラップ コンフィギュレーションに指定したサイト ID によって異なります。

ASA：クラスタ設定のカスタマイズ

クラスタを展開した後にブートストラップ設定を変更する場合や、クラスタリング ヘルス モニタリング、TCP 接続複製の遅延、フロー モビリティ、およびその他の最適化など、追加のオプションを設定する場合は、制御ユニットで行うことができます。

ASA クラスタの基本パラメータの設定

制御ノード上のクラスタ設定をカスタマイズできます。

始める前に

- マルチコンテキストモードでは、制御ユニット上のシステム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- local-unit name およびその他の複数のオプションは、FXOS シャーシでのみ設定することができます。また、それらのオプションは、クラスタリングを無効にしている場合にASAでのみ変更できます。そのため、次の手順には含まれていません。

手順

ステップ 1 このユニットが制御ユニットであることを確認します。

show cluster info

例：

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state CONTROL_NODE
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state DATA_NODE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state DATA_NODE
        ID        : 1
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state DATA_NODE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
```

```
CCL MAC   : 0015.c500.020f
Last join : 20:19:57 UTC Nov 4 2015
Last leave: 20:24:55 UTC Nov 4 2015
```

別のユニットが制御ユニットの場合は、接続を終了し、正しいユニットに接続します。

ステップ 2 クラスタ制御リンクインターフェイスの最大伝送ユニットを指定します。データインターフェイスの最大 MTU より少なくとも 100 バイト高い値を指定します。

mtu cluster *bytes*

例：

```
ciscoasa(config)# mtu cluster 9184
```

クラスタ制御リンクの MTU を最大値に設定することを推奨します。最小値は 1400 バイトです。さらに、クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッドにも対応する必要があります。たとえば、最大MTUは9184バイトであるため、データインターフェイスの最大 MTU は 9084 になり、クラスタ制御リンクは 9184 に設定できます。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。

ステップ 3 クラスタの設定モードを開始します。

cluster group *name*

ステップ 4 （任意）データユニットから制御ユニットへのコンソール複製を有効にします。

console-replicate

この機能はデフォルトで無効に設定されています。ASAは、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製をイネーブルにすると、データユニットから制御ユニットにコンソールメッセージが送信されるので、モニターが必要になるのはクラスタのコンソールポート 1 つだけとなります。

ステップ 5 クラスタリング イベントの最小トレース レベルを設定します。

trace-level *level*

必要に応じて最小レベルを設定します。

- **critical**：クリティカル イベント（重大度 = 1）
- **warning**：警告（重大度 = 2）
- **informational**：情報イベント（重大度 = 3）
- **debug**：デバッグ イベント（重大度 = 4）

ステップ 6 （任意）（Firepower 9300 のみ）シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されていることを確認します。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。

unit parallel-join*num_of_units* **max-bundle-delay** *max_delay_time*

- *num_of_units*：モジュールがクラスタに参加する前に準備する必要がある同じシャーシ内のモジュールの最小数（1 ～ 3）を指定します。デフォルトは 1 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。たとえば、値を 3 に設定した場合、各モジュールは *max_delay_time* の間、または 3 つすべてのモジュールの準備が完了するまで待機してからクラスタに参加します。3 のすべてのモジュールがほぼ同時にクラスタの参加を要求し、同時期にトラフィックの受信を開始します。
- *max_delay_time*：最大遅延時間を分単位（0 ～ 30 分）で指定します。この時間が経過すると、モジュールは他のモジュールの準備が完了するのを待つことをやめて、クラスタに参加します。デフォルトは 0 です。つまり、モジュールは他のモジュールの準備完了を待たずに、クラスタに参加することを意味します。*num_of_units* を 1 に設定した場合、この値は 0 にする必要があります。*num_of_units* を 2 または 3 に設定した場合、この値は 1 以上にする必要があります。このタイマーはモジュールごとのタイマーですが、最初のモジュールがクラスタに参加すると、その他すべてのモジュールのタイマーが終了し、残りのモジュールがクラスタに参加します。

たとえば、*num_of_units* を 3、*max_delay_time* を 5 分に設定します。モジュール 1 が起動すると、その 5 分間のタイマーが開始されます。モジュール 2 が 2 分後に起動すると、その 5 分間のタイマーが開始されます。モジュール 3 が 1 分後に起動し、すべてのモジュールが 4 分符号でクラスタに参加します。モジュールはタイマーが完了するまで待機しません。モジュール 3 が起動しない場合、モジュール 1 は 5 分間タイマーの終了時にクラスタに参加し、モジュール 2 も参加します。モジュール 2 はタイマーがまだ 2 分残っていますが、タイマーが完了するまで待機しません。

ステップ 7 クラスタメンバの最大数を設定します。

cluster-member-limit *number*

- *number*：2 ー 16。デフォルトは 16 です。

クラスタが最大の 16 ユニットよりも少ないことがわかっている場合は、実際の計画ユニット数を設定することを推奨します。最大ユニット数を設定すると、クラスタのリソース管理が向上します。たとえば、ポートアドレス変換（PAT）を使用する場合、制御ユニットは計画されたメンバー数にポートブロックを割り当てることができ、使用する予定のない追加のユニット用にポートを予約する必要がなくなります。

ステップ 8 フローオーナーからディレクタおよびバックアップオーナーへのフロー状態更新メッセージ（clu_keepalive および clu_update メッセージ）のキープアライブ間隔を設定します。

clu-keepalive-interval *seconds*

- *seconds*：15 ～ 55。デフォルトは 15 です。

クラスタ制御リンクのトラフィック量を減らすために、デフォルトよりも長い間隔を設定することもできます。

のヘルス モニタリングおよび自動再結合の設定

この手順では、ユニットとインターフェイスのヘルス モニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。ポートチャネル ID、または単一の物理インターフェイス ID をモニターできます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 クラスタ ユニットのヘルス チェック機能を次のようにカスタマイズします。

health-check [**holdtime** *timeout*]

holdime は、ユニットのハートビート ステータス メッセージの間隔を指定します。指定できる範囲は .3 ～ 45 秒で、デフォルトは 3 秒です。

ユニットのヘルスを確認するため、ASA のクラスタ ユニットはクラスタ制御リンクで他のユニットにハートビート メッセージを送信します。ユニットが保留時間内にピア ユニットからハートビート メッセージを受信しない場合は、そのピア ユニットは応答不能またはデッド状態と見なされます。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 4100/9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS、vPC、StackWise、または StackWise Virtual を形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし、無効化したインターフェイスのモニタリングも無効にしてください（**no health-check monitor-interface**）。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイス ヘルス チェックを次のように無効化します。

no health-check monitor-interface [*interface_id* | **service-application**]

インターフェイスのヘルス チェックはリンク障害をモニターします。特定の論理インターフェイスのすべての物理ポートが、特定のユニット上では障害が発生したが、別のユニット上の同

じ論理インターフェイスでアクティブポートがある場合、そのユニットはクラスタから削除されます。ASAがメンバをクラスタから削除するまでの時間は、インターフェイスのタイプと、そのユニットが確立済みメンバであるか、またはクラスタに参加しようとしているかによって異なります。

デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブルにすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ヘルス モニタリングは VLAN サブインターフェイス、または VNI や BVI などの仮想インターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニタされています。**service-application** を指定して、デコレータ アプリケーションのモニタリングをディセーブルにします。

何らかのトポロジ変更（たとえばデータ インターフェイスの追加/削除、ASA、Firepower 4100/9300 シャーシ、またはスイッチ上のインターフェイスの有効化/無効化、VSS、vPC、StackWise、またはStackWise Virtualを形成するスイッチの追加）を行うときには、ヘルスチェック機能を無効にし（**no health-check**）、無効化したインターフェイスのモニタリングも無効にしてください。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、ヘルス チェック機能を再度イネーブルにできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface port-channel1
```

ステップ 4 ヘルス チェック失敗後の自動再結合クラスタ設定を次のようにカスタマイズします。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**：内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
- **unlimited**：（**cluster-interface** のデフォルト）再結合の試行回数を制限しません。
- *auto-rejoin-max*：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。**data-interface** と **system** のデフォルトは 3 です。
- *auto_rejoin_interval*：再結合試行の間隔を 2 ～ 60 の範囲の分単位で定義します。デフォルト値は5分です。クラスタへの再結合をユニットが試行する最大合計時間は、最後の失敗から 14,400 分に限られています。
- *auto_rejoin_interval_variation*：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の2倍、**3**：直前の間隔の3倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタ インターフェイスの場合は **1**、データ インターフェイスおよびシステムの場合は **2** です。

例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

ステップ 5 シャーシハートビート障害の **health-check system auto-rejoin** コマンドと一致するようにシャーシ再参加を設定します。

health-check chassis-heartbeat-delay-rejoin

デフォルトでは、シャーシハートビート障害から回復すると、ノードはすぐにクラスタに再参加します。ただし、**health-check chassis-heartbeat-delay-rejoin** コマンドを設定すると、**health-check system auto-rejoin** コマンドの設定に従って再参加します。

ステップ 6 ASAがインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定します。

health-check monitor-interface debounce-time *ms*

デバウンス時間は 300 ～ 9000 ms の範囲の値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。 ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタユニットの方がポートのバンドルが速いという理由だけで、クラスタユニット上でインターフェイスがエラー表示されるのを防ぐことができます。

例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

ステップ 7 シャーシのヘルス チェック間隔を設定します。

app-agent heartbeat [**interval** *ms*] [**retry-count** *number*]

- **interval** *ms*：ハートビートの時間間隔を 100 ～ 6000 ms の範囲の 100 の倍数単位で設定します。デフォルトは 1000 ms です。
- **retry-count** *number*：再試行の回数を 1 ～ 30 の範囲の値に設定します。デフォルトの試行回数は 3 回です。

ASA はホストシャーシとのバックプレーンを介して通信できるかどうかをチェックします。

最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできません。たとえば、間隔を 100 に、再試行回数を 3 に設定した場合、合計結合時間は 300 ミリ秒になりますが、これはサポートされていません。たとえば、間隔を 100 に設定し、再試行回数を 6 に設定して最小時間（600 ms）を満たすことができます。

例：

```
ciscoasa(cfg-cluster)# app-agent heartbeat interval 1000 retry-count 10
```

ステップ 8 （任意）トラフィック負荷のモニタリングを設定します。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds*：モニタリングメッセージ間の時間を、10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。
- **intervals** *intervals*： ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

クラスタメンバのトラフィック負荷をモニターできます。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティモジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティモジュールがクラスタを離れると、そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ユニットでクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 25 interval:
   0           0            0            12             28
   1           0            0            13             27
```

接続の再分散およびクラスタ TCP 複製の遅延の設定

接続の再分散を設定できます。TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップ フローが作成される前にユニットが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のユニットに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （オプション）TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合、ASA は、1 秒あたりの接続数に関する情報を定期的に交換し、新しい接続を、1 秒あたりの接続数が多いデバイスから低負荷のデバイスにオフロードします。既存の接続は移動されません。さらに、このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタ メンバには新しい接続を再分散できません。

ステップ 3 TCP 接続のクラスタ複製の遅延を有効化します。

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

1 ～ 15 の範囲で秒数を設定します。**http** 遅延はデフォルトで 5 秒間有効になります。

サイト間機能の設定

サイト間クラスタリングの場合、冗長性と安定性を高めるために、設定をカスタマイズできます。

ディレクタ ローカリゼーションの有効化

データセンターのサイト間クラスタリングのパフォーマンスを向上させ、ラウンドトリップ時間を短縮するために、ディレクター ローカリゼーションをイネーブルにすることができます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有

されています。しかし、ASAは任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバルディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。

始める前に

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。
- 次のトラフィック タイプは、ローカリゼーションをサポートしていません：NAT および PAT トラフィック、SCTP 検査されたトラフィック、フラグメンテーション所有クエリ。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 次のようにディレクタ ローカリゼーションをイネーブルにします。

director-localization

サイト冗長性の有効化

サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。

始める前に

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 サイトの冗長性を有効にします。

site-redundancy

サイトごとの Gratuitous ARP の設定

ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保ちます。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。

クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチングインフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。

各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。GARP 間隔をカスタマイズするか、または GARP を無効にすることができます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。
- 制御ユニット設定では、スパンド EtherChannel のサイトごとの MAC アドレスを設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 GARP 間隔をカスタマイズします。

site-periodic-garp interval *seconds*

- *seconds*：GARP 生成の間隔を 1 ～ 1000000 秒間の秒単位で設定します。デフォルトは 290 秒です。

GARP を無効にするには、**no site-periodic-garp interval** を入力します。

例：

```
ciscoasa(cfg-cluster)# site-periodic-garp interval 500
```

クラスタ フロー モビリティの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

LISP インスペクションについて

LISP トラフィックを検査することで、サイト間のフローのモビリティを有効にできます。

LISP について

VMware VMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンター サーバ モビリティをサポートするには、サーバの移動時にサーバへの入力ルートをルータが更新できる必要があります。Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID、つまりエンドポイント ID（EID）をその場所、つまりルーティング ロケータ（RLOC）から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアントに対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

LISP では、LISP の出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、ファースト ホップ ルータ、マップ リゾルバ（MR）、およびマップ サーバ（MS）などのある一定のロールにおいてルータとサーバが必要です。サーバが別のルータに接続されていることをサーバのファースト ホップ ルータが感知すると、そのルータは他のすべてのルータとデータベースを更新し、クライアントに接続されている ITR がトラフィックを代行受信してカプセル化し、新しいサーバの場所に送信できるようにします。

Secure Firewall ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISP の統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフローオーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーニング」または「ヘアピニング」と呼ばれます。

LISP 統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR 間でやり取りされる LISP トラフィックを検査し、フローの所有者を新しいサイトに変更できます。

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。
- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々のノードに属しているフローは新しいオーナーには移動されません。半分散されたフローには SIP などのアプリケーションが含まれており、親フローとそのすべての子フローが同じ ASA によって所有されます。
- クラスタはレイヤ 3 および 4 のフロー状態を移動させるだけです。一部のアプリケーション データが失われる可能性があります。
- 短時間のフローまたはビジネスに不可欠でないフローの場合、オーナーの移動は有用でない可能性があります。インスペクション ポリシーを設定するときに、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

ASA LISP の実装

この機能には、複数の相互に関係する設定が含まれています（それらについてはすべてこの章で説明します）。

1. （任意）ホストまたはサーバ IP アドレスに基づく検査対象 EID の制限：ファースト ホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。
2. LISP トラフィック インスペクション：ASA は、ファーストホップルータと ITR または ETR の間で送信される EID 通知メッセージにおいて、UDP ポート 4342 上の LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。LISP トラフィックにはディレクタが割り当てられておらず、LISP トラフィック自体はクラスタ状態の共有に参加しないことに注意してください。
3. 指定されたトラフィック上のフロー モビリティを有効にするサービス ポリシー：フロー モビリティはビジネスクリティカルなトラフィックに対して有効にする必要があります。たとえば、フロー モビリティを HTTPS トラフィックおよび/または特定のサーバへのトラフィックのみに制限できます。
4. サイト ID：ASA は、各クラスタノードのサイト ID を使用して新しいオーナーを特定します。

5. フローモビリティをイネーブルにするためのクラスタレベル設定：フローモビリティは、クラスタ レベルでも有効にする必要があります。このオン/オフ トグルを使用すると、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP インスペクションの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

始める前に

- Firepower 4100/9300 シャーシ スーパバイザ上のシャーシのサイト ID を設定します。
- LISP のトラフィックはデフォルト インスペクション トラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

手順

ステップ 1 （任意） LISP インスペクション マップを設定して、IP アドレスに基づいて検査済みの EID を制限し、LISP の事前共有キーを設定します。

a) 拡張 ACL を作成します。宛先 IP アドレスのみが EID 組み込みアドレスと照合されます。

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) LISP インスペクション マップを作成し、パラメータ モードに移行します。

policy-map type inspect lisp *inspect_map_name*

parameters

c) 作成した ACL を識別して、許可された EID を定義します。

allowed-eid access-list *eid_acl_name*

ファースト ホップ ルータまたは ITR/ETR は、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信することがあります。このため、クラスタに関連するサーバーまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

d) 必要に応じて、事前共有キーを入力します。

validate-key *key*

例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

ステップ 2 ファースト ホップ ルータとポート 4342 の ITR または ETR の間の UDP トラフィック の LISP インスペクションの設定。

a) 拡張 ACL を設定して LISP のトラフィックを特定します。

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

UDP ポート 4342 を指定する必要があります。IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) ACL のクラス マップを作成します。

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) ポリシー マップ、クラス マップを指定し、オプションの LISP インスペクション マップを使用してインスペクションを有効化し、サービス ポリシーをインターフェイスに適用します（新規であれば）。

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

既存のサービス ポリシーある場合は、既存のポリシー マップ名を指定します。デフォルトで、ASA には **global_policy** と呼ばれるグローバル ポリシーが含まれているため、グローバル ポリシーの名前を指定します。ポリシーをグローバルに適用しない場合は、インターフェイスごとに 1 つのサービス ポリシーを作成することもできます。LISP インスペクションは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービス ポリシーを適用する必要はありません。トラフィックが両方向のクラス マップに一致する場合、ポリシー マップを適用するインターフェイスに入るまたは存在するトラフィックのすべてが影響を受けます。

例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
```

```
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASAは、ファーストホップルータとITRまたはETRの間で送信されるEID通知メッセージのLISPトラフィックを検査します。ASAは、EIDとサイトIDを関連付けるEIDテーブルを保持します。

ステップ3 トラフィック クラスのフロー モビリティを有効化します。

a) 拡張ACLを設定して、サーバーがサイトを変更するときに、最適なサイトに再割り当てするビジネス クリティカルなトラフィックを特定します。

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

IPv4 ACLおよびIPv6 ACLのどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。フロー モビリティは、ビジネス クリティカルなトラフィックに対してイネーブルにする必要があります。たとえば、フロー モビリティをHTTPSトラフィックのみ、または特定のサーバへのトラフィックのみに制限できます。

b) ACLのクラス マップを作成します。

class-map *flow_map_name*

match access-list *flow_acl_name*

c) LISPインスペクションを有効化した同じポリシー マップ、フロー クラス マップを指定して、フロー モビリティを有効にします。

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0
255.255.255.0 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

ステップ4 クラスタ グループ コンフィギュレーション モードに移行し、クラスタのフローのモビリティを有効化します。

cluster group *name*

flow-mobility lisp

このオン/オフの切り替えにより、フロー モビリティの有効化や無効化を簡単に行えます。

例

次に例を示します。

- EID を 10.10.10.0/24 ネットワーク上の EID に制限します。
- 192.168.50.89（内部）にある LISP ルータと 192.168.10.8（別の ASA インターフェイス上）にある ITR または ETR ルータの間の LISP トラフィック（UDP 4342）を検査します。
- HTTPS を使用して 10.10.10.0/24 のサーバーに送信されるすべての内部トラフィックに対してフロー モビリティを有効化します。
- クラスタに対してフロー モビリティをイネーブルにします。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
!
cluster group cluster1
   flow-mobility lisp
```

分散型サイト間 VPN の設定

デフォルトでは、クラスタは集中型のサイト間 VPN モードを使用します。クラスタリングの拡張性を活用するために、分散型サイト間 VPN モードを有効にできます。

分散型サイト間 VPN について

この分散モードでは、サイト間 IPsec IKEv2 VPN 接続がクラスタのノード全体に分散されます。VPN接続をクラスタのノード間に分散させると、クラスタのキャパシティとスループットの両方を最大限に活用できるため、集中型 VPN 機能を超えて VPN サポートを大幅に拡張できます。

分散型 *VPN* 接続の役割

分散型 VPN モードで実行すると、次の役割がクラスタ ノードに割り当てられます。

- アクティブセッションオーナー：最初に接続を受信したノード、またはバックアップセッションをアクティブ セッションに移行したノード。オーナーは、IKE と IPsec トンネル、およびそれらに関連付けられたすべてのトラフィックを含む、完全なセッションの状態を維持し、パケットを処理します。
- バックアップ セッション オーナー：既存のアクティブ セッションのバックアップ セッションを処理しているノード。アクティブセッションオーナーに障害が発生すると、バックアップ セッション オーナーがアクティブ セッション オーナーになり、新しいバックアップ セッションが別のノードで確立されます。
- フォワーダ：VPN セッションに関連付けられたトラフィックが VPN セッションを所有していないノードに送信された場合、そのノードは VPN セッションを所有しているノードにトラフィックを転送するために っクラスター制御リンクを使用します。
- オーケストレータ：オーケストレータ（常にクラスタ制御ノード）は、アクティブセッションの再配布（ASR）を実行する際に、移動するセッションとその移動先を計算する役割があります。オーケストレータは、オーナー ノード X に N セッションをメンバー Y に移動する要求を送信します。ノード X は、完了時に移動できたセッション数を指定して、オーケストレータに応答を返します。

分散型 *VPN* セッションの特性

分散型サイト間 VPN セッションには、次の特性があります。それ以外の場合、VPN 接続は、クラスタ上にない場合に通常動作するように動作します。

- VPN セッションは、セッション レベルでクラスタ全体に分散されます。つまり、1 つの VPN 接続に対し、同じクラスタ ノードが IKE および IPsec トンネルと、そのすべてのトラフィックを処理します。VPN セッション トラフィックが、その VPN セッションを所有していないクラスタ ノードに送信された場合、トラフィックは VPN セッションを所有しているクラスタ ノードに転送されます。
- VPN セッションには、クラスタ全体で一意のセッション ID があります。セッション ID を使用して、トラフィックが検証され、転送の決定が行われ、IKE ネゴシエーションが完了します。
- サイト間 VPN ハブ アンド スポーク構成では、クライアントがクラスタを介して接続する場合（ヘアピニングと呼ばれる）、流入するセッション トラフィックと流出するセッション トラフィックは、異なるクラスタ ノード上にある可能性があります。
- バックアップ セッションを別のシャーシのセキュリティ モジュールに割り当てるように要求することができます。これにより、シャーシの障害を防止します。または、クラスタ内の任意のノードにバックアップセッションを割り当てることもできます。これはノードの障害のみを防止します。クラスタにシャーシが 2 つある場合は、リモートシャーシバックアップを強く推奨します。

クラスタ イベントの分散型 *VPN* の処理

イベント	分散型 VPN
ノード障害	この障害が発生したノード上のすべてのアクティブ セッションに対し、（別のノード上の）バックアップセッションがアクティブになり、バックアップセッションはバックアップ戦略に従って別のノードに再割り当てされます。
シャーシ障害	リモートシャーシバックアップ戦略が使用されている場合、障害が発生したシャーシ上のすべてのアクティブセッションに対し、（他のシャーシのノード上の）バックアップセッションがアクティブになります。ノードが交換されると、これらの現在アクティブなセッションに対するバックアップ セッションが、交換されたシャーシのノードに再割り当てされます。 フラット バックアップ戦略が使用されている場合、アクティブ セッションとバックアップ セッションの両方が障害の発生したシャーシ上にあると、接続は切断されます。他のシャーシのノード上にバックアップ セッションがあるアクティブセッションはすべて、これらのセッションにフォールバックします。新しいバックアップセッションは、残存しているシャーシ内の別のノードに割り当てられます。
クラスタ ノードの非アクティブ化	非アクティブになっているクラスタ ノード上のすべてのアクティブ セッションに対し、（別のノード上の）バックアップセッションがアクティブになり、バックアップ戦略に従って別のノードにバックアップセッションを再割り当てします。
クラスタ ノードの参加	新しいノードの VPN クラスタモードが分散型に設定されていない場合、制御ノードはモード変更を要求します。 VPN モードに互換性があった後で、クラスタ ノードには、通常の操作の流れでアクティブ セッションとバックアップ セッションが割り当てられます。

IPsec IKEv2 の変更

IKEv2 は、分散型サイト間 VPN モードでは次のように変更されます。

- IP/ポート タプルの代わりに ID が使用されます。これにより、パケットの適切な転送の決定、および他のクラスタ メンバー上にある可能性がある以前の接続のクリーンアップが可能になります。
- 単一の IKEv2 セッションを識別する（SPI）識別子は、ローカルで生成されたランダムな 8 バイトの値で、クラスタ全体で一意です。SPI には、タイム スタンプとクラスタ ノード ID が埋め込まれています。IKE ネゴシエーション パケットの受信時に、タイム スタンプまたはクラスタ ノード ID のチェックに失敗すると、パケットがドロップされ、理由を示すメッセージが記録されます。

- NAT-T ネゴシエーションがクラスタ メンバー間で分割されることによって失敗しないようにIKEv2 処理が変更されました。新しいASP 分類ドメインである *cluster_isakmp_redirect*、およびルールは、IKEv2 がインターフェイスで有効になっている場合に追加されます。**show asp table classify domain cluster_isakmp_redirect** コマンドを使用して、ルールを参照します。

クラスタ内の分散型サイト間 *VPN* の高可用性

次の機能により、セキュリティ モジュールまたはシャーシの単一障害に対する復元力が提供されます。

- 任意のシャーシ上のクラスタ内にある別のセキュリティ モジュールにバックアップされた VPN セッションは、セキュリティ モジュールの障害に耐性があります。
- 別のシャーシにバックアップされた VPN セッションは、シャーシの障害に耐性があります。
- 制御ノードは、VPN サイト間セッションを失うことなく変更できます。

クラスタが安定する前に追加の障害が発生すると、アクティブ セッションとバックアップ セッションの両方が障害の発生したノードにある場合、接続が失われる可能性があります。

VPN クラスタ モードの無効化、クラスタ ノードのリロード、およびその他の予想されるシャーシの変更など、ノードが正常な状態でクラスタを離れるときにセッションが失われないように、すべての試行が行われます。これらのタイプの操作では、操作間でセッションのバックアップを再確立する時間がクラスタに与えられている限り、セッションは失われません。最後のクラスタ ノードで正常な終了がトリガーされた場合、既存のセッションが正常に切断されます。

CMPv2

CMPv2 ID 証明書とキーペアはクラスター ノード間で同期されます。ただし、クラスター内の制御ノードのみが CMPv2 証明書を自動的に更新してキーの再生成を行います。制御ノードは更新時に、これらの新しい ID 証明書とキーをすべてのクラスター ノードに同期させます。このようにして、クラスター内のすべてのノード メンバーは CMPv2 証明書を利用して認証を行い、また、すべてのノードが制御ノードを継承することができます。

分散型サイト間 VPN のライセンス

キャリア ライセンスは、クラスターの各メンバーで、分散型サイト間 VPN に必要です。

各 VPN 接続には、2 つの *Other VPN* ライセンス済みセッションが必要です（*Other VPN* ライセンスは*Essentials*ライセンスの一部です）。1 つはアクティブ セッション用、もう 1 つはバックアップ セッション用です。クラスタの最大 VPN セッション容量は、セッションごとに 2 つのライセンスを使用するため、ライセンス済み容量の半分以下にすることができます。

分散型サイト間 VPN の前提条件

モデルのサポート

- Firepower 9300
- 最大 2 つのシャーシで、最大 6 つのモジュール。各シャーシで異なる数のセキュリティ モジュールを設置することができますが、均等な分配を推奨しています。

最大 VPN セッション数

各セキュリティ モジュールは、6 つのノードにわたる最大約 36,000 のセッションに対し、最大 6,000 の VPN セッションをサポートします。

クラスタ ノードでサポートされる実際のセッション数は、プラットフォームの容量、割り当てられたライセンス、コンテキストごとのリソース割り当てによって決まります。使用率が制限値に近い場合、各クラスタ ノードで最大容量に達していなくても、セッションの作成が失敗することがあります。これは、アクティブ セッションの割り当てが外部スイッチングによって決定され、バックアップ セッションの割り当てが内部クラスタ アルゴリズムによって決定されるためです。顧客は、使用率を適宜調整し、不均一な配布に対するスペースを確保することが推奨されます。

分散型サイト間 VPN のガイドライン

ファイアウォール モード

分散型サイト間 VPN は、ルーテッド モードでのみサポートされています。

コンテキスト モード

分散型サイト間 VPN は、シングル コンテキスト モードおよびマルチ コンテキスト モードの両方で動作します。ただし、マルチ コンテキスト モードでは、アクティブ セッションの再配布はコンテキスト レベルではなくシステム レベルで行われます。これにより、コンテキストに関連付けられたアクティブ セッションが、異なるコンテキストに関連付けられたアクティブ セッションを含むクラスタ メンバーに移動し、予期せずに持続不可能な負荷が発生するのを防ぎます。

サポートされていないインスペクション

次のタイプの検査は、分散型サイト間 VPN モードではサポートされていないか、または無効になっています。

- CTIQBE
- DCERPC
- H323、H225、および RAS
- IPSec パススルー
- MGCP

- MMP
- NetBIOS
- PPTP
- RADIUS
- RSH
- RTSP
- SCCP（Skinny）
- SUNRPC
- TFTP
- WAAS
- WCCP
- XDMCP

その他のガイドライン

- 分散型サイト間VPNモードではIKEv2 IPsecサイト間VPNのみがサポートされています。IKEv1 はサポートされていません。IKEv1 サイト間は、集中型 VPN モードでサポートされています。
- サイト間クラスタリングはサポートされていません。
- ダイナミック PAT は、分散型サイト間 VPN モードでは使用できません。

分散型サイト間 VPN を有効にします

分散型サイト間VPNを有効にして、VPNセッションのクラスタリングの拡張性を活用します。

（注） 集中型と分散型間で VPN モードを変更するには、クラスターのすべてのノードがリロードする必要があります。バックアップ モードの変更は動的で、セッションは終了しません。

始める前に

『VPN Configuration Guide』に従って、サイト間 VPN を設定します。

手順

ステップ 1 クラスタの制御ノードで、クラスター構成モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 分散型サイト間 VPN を有効にします

vpn-mode distributed backup flat

または

vpn-mode distributed backup remote-chassis

フラット バックアップ モードでは、他のクラスタ ノードにスタンバイ セッションが確立されます。これにより、ユーザはモジュール障害から保護されますが、シャーシ障害の保護は保証されません。

リモートシャーシ バックアップ モードでは、クラスタ内の別のシャーシのノードにスタンバイ セッションが確立されます。これにより、ユーザはモジュール障害とシャーシ障害の両方から保護されます。

リモートシャーシが単一のシャーシ環境（意図的に構成されたものまたは障害の結果）で構成されている場合、別のシャーシが結合されるまでバックアップは作成されません。

例：

```
ciscoasa(cfg-cluster)# vpn-mode distributed backup remote-chassis
WARNING: Do you want to proceed with changing the vpn-mode, save the device configuration,
and initiate a reboot? [confirm]
```

分散型 S2S VPN セッションの再配布

アクティブ セッションの再配布（ASR）では、アクティブな VPN セッションの負荷がクラスタ メンバー全体に再配布されます。セッションの開始と終了の動的な性質のため、ASR は、すべてのクラスタ メンバー間でセッションのバランスを取るためのベスト エフォートです。繰り返される再配布アクションによってバランスが最適化されます。

再配布はいつでも実行でき、クラスタ内のトポロジ変更後に実行する必要があります。また、新しいメンバーがクラスタに参加した後に実行することを推奨します。再配布の目的は、安定した VPN クラスタを作成することです。安定した VPN クラスタには、ノード間でほぼ同数のアクティブ セッションとバックアップ セッションがあります。

セッションを移動するには、バックアップ セッションがアクティブ セッションになり、別のノードが新しいバックアップ セッションをホストするように選択されます。移動セッションは、アクティブ セッションのバックアップの場所と、その特定のバックアップ ノード上にすでに存在するアクティブセッションの数に依存します。何らかの理由でバックアップセッション ノードがアクティブセッションをホストできない場合、元のノードはセッションのオーナーのままです。

マルチコンテキスト モードでは、アクティブ セッションの再配布は、個々のコンテキスト レベルではなくシステム レベルで行われます。コンテキスト レベルで実行されない理由は、あるコンテキスト内のアクティブセッションが別のコンテキスト内のより多くのアクティブセッションを含むメンバーに移動され、そのクラスタ メンバーに多くの負荷がかかるためです。

始める前に

- 再配布アクティビティをモニターする場合は、システム ログを有効にします。
- この手順は、クラスタの制御ユニットで実行する必要があります。

手順

ステップ 1 制御ノード上でアクティブ セッションとバックアップ セッションがクラスタ全体でどのように配布されているかを表示します。

show cluster vpn-sessiondb distribution

例：

配布情報は次のように表示されます。

```
Member 0 (unit-1-1): active: 209; backups at: 1(111), 2(98)
Member 1 (unit-1-3): active: 204; backups at: 0(108), 2(96)
Member 2 (unit-1-2): active: 0
```

各行には、メンバー ID、メンバー名、アクティブ セッション数、およびバックアップ セッションが存在するメンバーが含まれています。上記の例では、次のように情報が読み取れます。

- メンバー 0 には 209 のアクティブ セッションがあり、111 のセッションはメンバー 1 にバックアップされ、98 のセッションはメンバー 2 にバックアップされます。
- メンバー 1 には 204 のアクティブ セッションがあり、108 のセッションはメンバー 0 にバックアップされ、96 のセッションはメンバー 2 にバックアップされます。
- メンバー2にはアクティブセッションがないため、クラスタ メンバーはこのノードのセッションをバックアップしていません。このメンバーは最近クラスタに参加しました。

ステップ 2 セッションを再配布します。

cluster redistribute vpn-sessiondb

このコマンドは、バックグラウンドで実行中に即座に戻ります（メッセージなしで）。

再配布するセッションの数とクラスタの負荷に応じて、これには時間がかかることがあります。再配布アクティビティが発生すると、次のフレーズ（およびここには表示されていない他のシステムの詳細）を含む Syslog が提供されます。

Syslog フレーズ	注
VPN session redistribution started	制御ノードのみ
Sent request to move *number* sessions from *orig-member-name* to *dest-member-name*	制御ノードのみ
Failed to send session redistribution message to *member-name*	制御ノードのみ
Received request to move *number* sessions from *orig-member-name* to *dest-member-name*	データ ノードのみ
Moved *number* sessions to *member-name*	名前付きクラスタに移動したアクティブ セッションの数。
Failed to receive session move response from *dest-member-name*	制御ノードのみ
VPN session completed	制御ノードのみ
Cluster topology change detected. VPN session redistribution aborted.	

ステップ 3 **show cluster vpn-sessiondb distribution** コマンドを再入力して結果を表示します。

FXOS：クラスタノードの削除

ここでは、ノードをクラスタから一時的に、または永続的に削除する方法について説明します。

一時的な削除

たとえば、ハードウェアまたはネットワークの障害が原因で、クラスタノードはクラスタから自動的に削除されます。この削除は、条件が修正されるまでの一時的なものであるため、クラスタに再参加できます。また、手動でクラスタリングを無効にすることもできます。

デバイスが現在クラスタ内に存在するか確認するには、Firewall Chassis マネージャ [論理デバイス（Logical Devices）] ページで、**show cluster info** コマンドを使用してアプリケーション内のクラスタステータスを確認します。

```
ciscoasa# show cluster info
Clustering is not enabled
```

- アプリケーションでのクラスタリングの無効化：アプリケーションCLIを使用してクラスタリングを無効にすることができます。**cluster remove unit** *name* コマンドを入力して、ログインしているノード以外のすべてのユニットを削除します。ブートストラップコンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

デバイスが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがブートストラップ設定から受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。

クラスタリングを再度有効にするには、ASA で **cluster group** *name* を入力してから **enable** を入力します。

- アプリケーション インスタンスの無効化：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # scope slot 1
Firepower-chassis /ssa/slot # scope app-instance asa asa1
Firepower-chassis /ssa/slot/app-instance # disable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

再度有効にするには、次の手順を実行します。

```
Firepower-chassis /ssa/slot/app-instance # enable
Firepower-chassis /ssa/slot/app-instance* # commit-buffer
Firepower-chassis /ssa/slot/app-instance #
```

- セキュリティ モジュール/エンジン のシャットダウン：Firewall Chassis マネージャ の [セキュリティモジュール/エンジン（Security Module/Engine）] ページで、[電源オフ（Power Off）] アイコンをクリックします。FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope service-profile server 1/1
Firepower-chassis /org/service-profile # power down soft-shut-down
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

電源を投入するには、次の手順を実行します。

```
Firepower-chassis /org/service-profile # power up
Firepower-chassis /org/service-profile* # commit-buffer
Firepower-chassis /org/service-profile #
```

- シャーシのシャットダウン：Firewall Chassis マネージャの [概要（Overview）] ページで、[シャットダウン（Shut Down）] アイコンをクリックします。FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope chassis 1
Firepower-chassis /chassis # shutdown no-prompt
```

完全な削除

次の方法を使用して、クラスタノードを完全に削除できます。

- 論理デバイスの削除：FXOS CLI で、次の例を参照してください。

```
Firepower-chassis# scope ssa
Firepower-chassis /ssa # delete logical-device cluster1
Firepower-chassis /ssa* # commit-buffer
Firepower-chassis /ssa #
```

- サービスからのシャーシまたはセキュリティモジュールの削除：サービスからデバイスを削除する場合は、交換用ハードウェアをクラスタの新しいノードとして追加できます。

ASA：クラスタ メンバの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタ メンバを管理できます。

非アクティブなメンバーになる

クラスタの非アクティブなメンバーになるには、クラスタリング コンフィギュレーションは変更せずに、そのノード上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのノードをクラスタから完全に削除します。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

始める前に

- コンソール ポートを使用する必要があります。クラスタリングのイネーブルまたはディセーブルを、リモート CLI 接続から行うことはできません。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

no enable

このノードが制御ノードであった場合は、新しい制御ノードの選定が実行され、別のメンバーが制御ノードになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

ユニットの非アクティブ化

ログインしているノード以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

クラスタからノードを削除します。

cluster remove unit *node_name*

ブートストラップコンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ノードがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

始める前に

- クラスタリングを再イネーブルにするには、コンソール ポートを使用する必要があります。他のインターフェイスはシャットダウンされます。
- マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。
- クラスタへの再参加を試行する前に、障害が解決されていることを確認します。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

制御ユニットの変更

⚠

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードの場合は、この手順をシステム実行スペースで実行します。まだシステム コンフィギュレーション モードに入っていない場合は、**changeto system** コマンドを入力します。

手順

新しいノードを制御ノードとして設定します。

cluster control-node unit*node_name*

例：

```
ciscoasa(config)# cluster control-node unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバー名を表示するには、**cluster control-node unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのメンバに、または特定のメンバに送信するには、次の手順を実行します。**show** コマンドをすべてのメンバーに送信すると、すべての出力が収集されて現在のユニットのコンソールに表示されます。（または、制御ユニットで show コマンドを入力するとクラスタ全体の統計情報を表示できます。）**capture** や **copy** などのその他のコマンドも、クラスタ全体での実行を活用できます。

手順

コマンドをすべてのメンバに送信します。ユニット名を指定した場合は、特定のメンバに送信されます。

cluster exec [unit *unit_name*] コマンド

例：

```
ciscoasa# cluster exec show xlate
```

メンバー名を表示するには、**cluster exec unit ?** コマンドを入力するか（現在のユニットを除くすべての名前を表示する場合）、**show cluster info** コマンドを入力します。

例

同じキャプチャファイルをクラスタ内のすべてのユニットから同時に TFTP サーバーにコピーするには、制御ユニットで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 および asa2 がクラスタ ユニット名です。

次の **cluster exec show memory** コマンドの出力例では、クラスタの各メンバーのメモリ情報が表示されています。

```
ciscoasa# cluster exec show memory
unit-1-1(LOCAL):*******************************************************
Free memory:      108724634538 bytes (92%)
Used memory:        9410087158 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-3:*******************************************************************
```

```
Free memory:      108749922170 bytes (92%)
Used memory:        9371097334 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)


unit-1-2:************************************************************
Free memory:      108426753537 bytes (92%)
Used memory:        9697869087 bytes ( 8%)
-------------     ------------------
Total memory:     118111600640 bytes (100%)
```

ASA：での ASA クラスタのモニタリング Firepower 4100/9300 シャーシ

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info [health], show cluster chassis info**

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバーのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ユニットおよびクラスタ全体の現在の状態を表示します。

  show cluster info コマンドの次の出力を参照してください。

```
asa(config)# show cluster info
Cluster cluster1: On
    Interface mode: spanned
    This is "unit-1-2" in state MASTER
        ID        : 2
        Version   : 9.5(2)
        Serial No.: FCH183770GD
        CCL IP    : 127.2.1.2
        CCL MAC   : 0015.c500.019f
        Last join : 01:18:34 UTC Nov 4 2015
        Last leave: N/A
Other members in the cluster:
    Unit "unit-1-3" in state SLAVE
        ID        : 4
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.3
        CCL MAC   : 0015.c500.018f
        Last join : 20:29:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
    Unit "unit-1-1" in state SLAVE
        ID        : 1
```

```
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.1.1
        CCL MAC   : 0015.c500.017f
        Last join : 20:20:53 UTC Nov 4 2015
        Last leave: 20:18:15 UTC Nov 4 2015
    Unit "unit-2-1" in state SLAVE
        ID        : 3
        Version   : 9.5(2)
        Serial No.: FCH19057ML0
        CCL IP    : 127.2.2.1
        CCL MAC   : 0015.c500.020f
        Last join : 20:19:57 UTC Nov 4 2015
        Last leave: 20:24:55 UTC Nov 4 2015
```

- **show cluster info auto-join**

  時間遅延後にクラスタユニットがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルス チェック障害など）がクリアされたかどうかを示します。ユニットが永続的に無効になっている場合、またはユニットがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。

  show cluster info auto-join コマンドについては次の出力を参照してください。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Master has application down that slave has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check
failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp**[**detail**]}

  次のトランスポート関連の統計情報を表示します。

  - **asp**：データ プレーンのトランスポート統計情報。
  - **cp**：コントロール プレーンのトランスポート統計情報。

detail キーワードを入力すると、クラスタで信頼性の高いトランスポート プロトコルの使用状況が表示され、バッファがコントロールプレーンでいっぱいになったときにパケット ドロップの問題を特定できます。**show cluster info transport cp detail** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
```

```
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ---------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ---------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ---------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
```

```
  Cluster Redirect Client                         3607          91%    0   0   0
  RRI Cluster Client                               317           8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                           Total messages  Percentage
  VPN Clustering HA Client                         578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                           Total messages  Percentage
  VPN Clustering HA Client                         572         99%
  Cluster VPN Unique ID Client                       1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  クラスタの履歴、およびクラスタユニットが参加できなかった理由や、ユニットがクラスタを離れた理由に関するエラーメッセージが表示されます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用して制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

クラスタリソースのモニタリング

クラスタリソースのモニタリングについては、次のコマンドを参照してください。

show cluster {cpu | memory | resource} [*options*]、**show cluster chassis [cpu | memory | resource usage]**

クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタ トラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail | count], cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダ フローのいずれであるかを示します。**cluster exec show conn** コマンドを任意のユニットで使用すると、すべての接続が表示されます。このコマンドの表示からは、1つのフローのトラフィックがクラスタ内のさまざまな ASA にどのように到達するかがわかります。クラスタのスループットは、ロード バランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

  次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/slave# show conn detail
15 in use, 21 most used
Cluster:
        fwd connections: 0 in use, 0 most used
        dir connections: 0 in use, 0 most used
        centralized connections: 0 in use, 44 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility
       M - SMTP data, m - SIP media, n - GUP
       N - inspected by Snort
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow

Cluster units to ID mappings:
  ID 0: unit-2-1
  ID 1: unit-1-1
  ID 2: unit-1-2
  ID 3: unit-2-2
  ID 4: unit-2-3
  ID 255: The default cluster member ID which indicates no ownership or affiliation

          with an existing cluster member
```

- **show cluster info [conn-distribution | packet-distribution | loadbalance]**

show cluster info conn-distribution および **show cluster info packet-distribution** コマンドは、すべてのクラスタユニット間のトラフィックの分布を表示します。これらのコマンドは、外部ロードバランサを評価し、調整するのに役立ちます。

show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

- **show cluster info load-monitor** [**details**]

  この**show cluster info load-monitor**コマンドは、最後の間隔のクラスタメンバのトラフィック負荷と、設定された間隔の合計数（デフォルトでは30）を表示します。各間隔の各測定値を表示するには、**details** キーワードを使用します。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
        0          0          0          0          0          0
        0          0          0          0          0          0

Buffer drops captured over 30 intervals:
Unit ID  0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
Unit ID  1
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
       25         25         30         30         30         35
       25         25         35         30         30         30
       25         25         30         25         25         35
       30         30         30         25         25         25
       25         20         30         30         30         30
Unit ID  1
       30         25         35         25         30         30
       25         25         35         25         30         35
       30         30         35         30         30         30
       25         20         30         25         25         30
       20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
```

```
Unit ID  0

        25          25          30          30          30          35

        25          25          35          30          30          30

        25          25          30          25          25          35

        30          30          30          25          25          25

        25          20          30          30          30          30

Unit ID  1

        30          25          35          25          30          30

        25          25          35          25          30          35

        30          30          35          30          30          30

        25          20          30          25          25          30

        20          30          35          30          30          35
```

- **show cluster {access-list | conn [count] | traffic | user-identity | xlate}** [*options*]、**show cluster chassis {access-list | conn | traffic | user-identity | xlate count}**

  クラスタ全体の集約データを表示します。使用可能なオプションはデータのタイプによって異なります。

  show cluster access-list コマンドの次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
```

```
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのユニットでの 合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:************************************************
124 in use, fwd connection 0 in use, dir connection 0 in use, centralized connection
0 in use (Cluster-wide aggregated)

unit-1-1(LOCAL):*****************************************************
40 in use, 48 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 46 most used

unit-2-2:************************************************************
18 in use, 40 most used, fwd connection 0 in use, 0 most used, dir connection 0 in
use,
0 most used, centralized connection 0 in use, 45 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

  クラスタのルーティング情報を表示します。

- **show lisp eid**

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

  cluster exec show lisp eid コマンドからの、次の出力を参照してください。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):***********************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:******************************************************************
     LISP EID       Site ID
    33.44.33.105        2
```

```
33.44.33.201        2
11.22.11.1   4
11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  このコマンドは、トラブルシューティングに役立ちます。

分散型 S2S VPN のモニタリング

次のコマンドを使用して、VPN セッションのステータスと分布を監視します。

- セッションの全体的な分布は、**show cluster vpn-sessiondb distribution** を使用して示されます。マルチコンテキスト環境で実行している場合は、このコマンドをシステム実行スペースで実行する必要があります。

  この show コマンドを使用すると、各ノードで **show vpn-sessiondb summary** を実行する必要なく、セッションのクイックビューが提供されます。

- **show cluster vpn-sessiondb summary** コマンドを使用して、クラスタ上の VPN 接続の統一されたビューも使用できます。

- **show vpn-sessiondb** コマンドを使用した個々のデバイス モニタリングでは、通常の VPN 情報に加えて、デバイス上のアクティブ セッションとバックアップ セッションの数が表示されます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ノードは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | service-module | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **debug service-module**

  スーパバイザとアプリケーション間のヘルス チェックの問題を含め、ブレード レベルの問題に関するデバッグ メッセージを表示します。

- **show cluster info trace**

show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
MASTER
```

たとえば、同じ**ローカルユニット**名を持つ2つのノードが制御ノードとして機能していることを示す次のメッセージが表示された場合は、2 つのノードの**ローカルユニット**名が同じである（設定を確認してください）か、1つのノードが自身のブロードキャストメッセージを受信している（ネットワークを確認してください）可能性があります。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node

 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
 Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
 CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

分散型 S2S VPN のトラブルシューティング

分散型 VPN の通知

分散型 VPN を実行しているクラスタで、次のエラー状況が発生した場合、識別されたフレーズを含むメッセージが通知されます。

状況	通知
クラスタに参加しようとしているときに、既存のまたは参加しているクラスター データ ノードが分散型 VPN モードにない場合は、次のメッセージが通知されます。	`New cluster member (member-name) rejected due to vpn mode mismatch.` および 制御ノード（*control-name*）は、VPN モード機能に制御ノードの設定との互換性がないという理由でユニット（unit-name）からの登録要求を拒否します。
分散型VPNのクラスタ メンバーでライセンスが正しく設定されていない場合は、次のメッセージが通知されます。	`ERROR: Control node requested cluster vpn-mode change to distributed. Unable to change mode due to missing Carrier License.`

状況	通知

受信した IKEv2 パケットの SPI でタイム スタンプまたはメンバー ID が無効な場合は、次のメッセージが通知されます。	`Expired SPI received`
	または
	`Corrupted SPI detected`

クラスタがバックアップ セッションを作成できない場合は、次のメッセージが通知されます。	`Failed to create the backup for an IKEv2 session.`
IKEv2 初期接点（IC）処理エラーの場合は、次のメッセージが通知されます。	`IKEv2 Negotiation aborted due to ERROR: Stale backup session found on backup`
再配布の問題の場合は、次のメッセージが通知されます。	`Failed to send session redistribution message to` *`member-name`* `Failed to receive session move response from` *`member-name`* `(control node only)`
セッションの再配布中にトポロジが変更された場合は、次のメッセージが通知されます。	`Cluster topology change detected. VPN session redistribution aborted.`

次のいずれかの状況が発生している可能性があります。

- サイト間 VPN セッションは**port-channel load-balance src-dst l4port** コマンドを使用して N7K スイッチにロード バランシング アルゴリズムとしてレイヤ 4 ポート が設定されている場合、クラスターのシャーシの 1 つにのみ配布されます。クラスタ セッションの割り当ての例を次に示します。

```
SSP-Cluster/data node(cfg-cluster)# show cluster vpn-sessiondb distribution
Member 0 (unit-1-3): active: 0
Member 1 (unit-2-2): active: 13295; backups at: 0(2536), 2(2769), 3(2495), 4(2835),
 5(2660)
Member 2 (unit-2-3): active: 12174; backups at: 0(2074), 1(2687), 3(2207), 4(3084),
 5(2122)
Member 3 (unit-2-1): active: 13416; backups at: 0(2419), 1(3013), 2(2712), 4(2771),
 5(2501)
Member 4 (unit-1-1): active: 0
Member 5 (unit-1-2): active: 0
```

サイト間 IKEv2 VPN は送信元ポートと宛先ポートの両方にポート 500 を使用するため、IKE パケットは Nexus 7K とシャーシ間に接続されたポート チャネル内のリンクの 1 つにのみ送信されます。

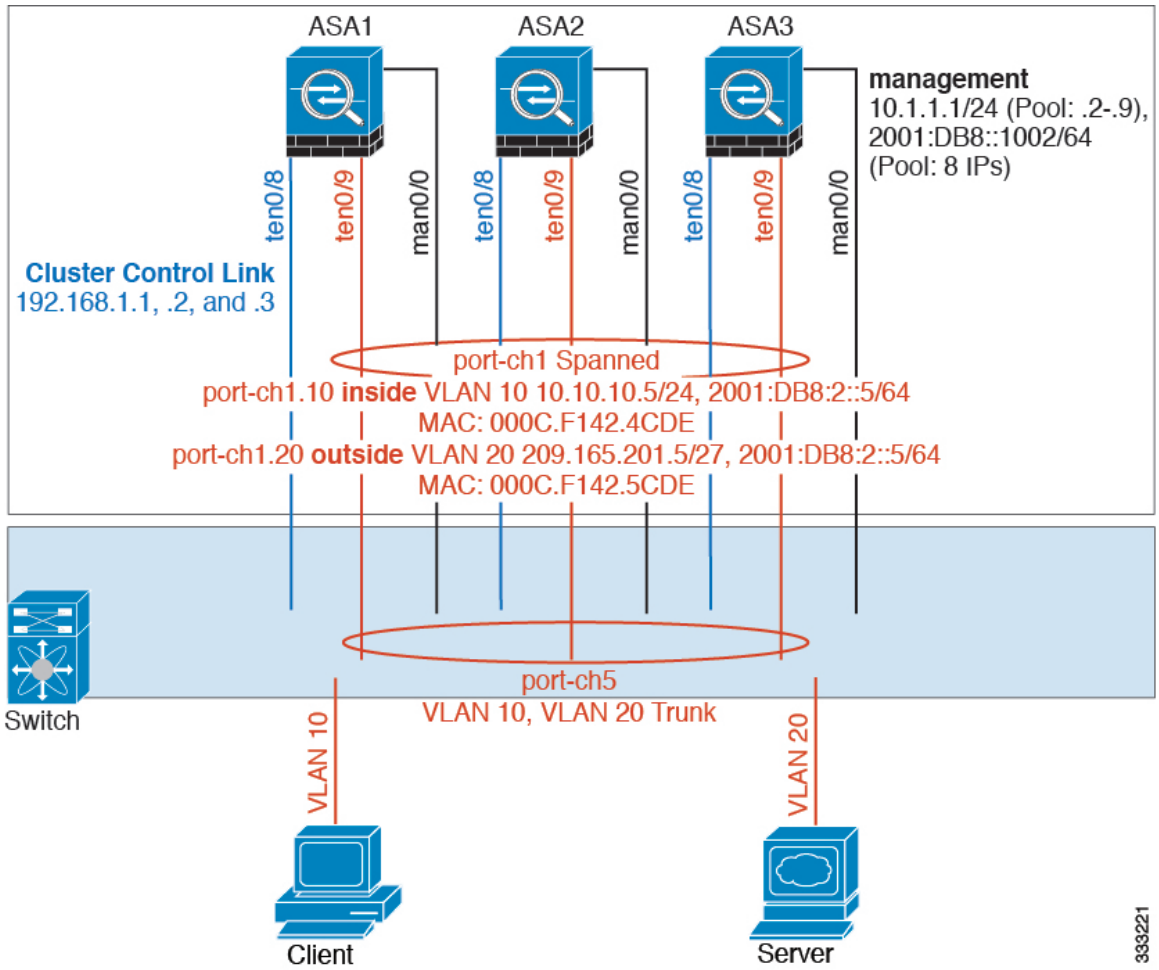
port-channel load-balance src-dst ip-l4port を使用して、N7K ロード バランシング アルゴリズムを IP およびレイヤ 4 ポートに変更します。その後、IKE パケットはすべてのリンクに、そしてすべてのノード送信されます。

より即座に調整するには、クラスターの制御ノードで **cluster redistribute vpn-sessiondb** を実行することで、アクティブな VPN セッションを他のシャーシのクラスター ノードに再配布できます。

ASA クラスタリングの例

これらの例には、一般的な導入が含まれます。

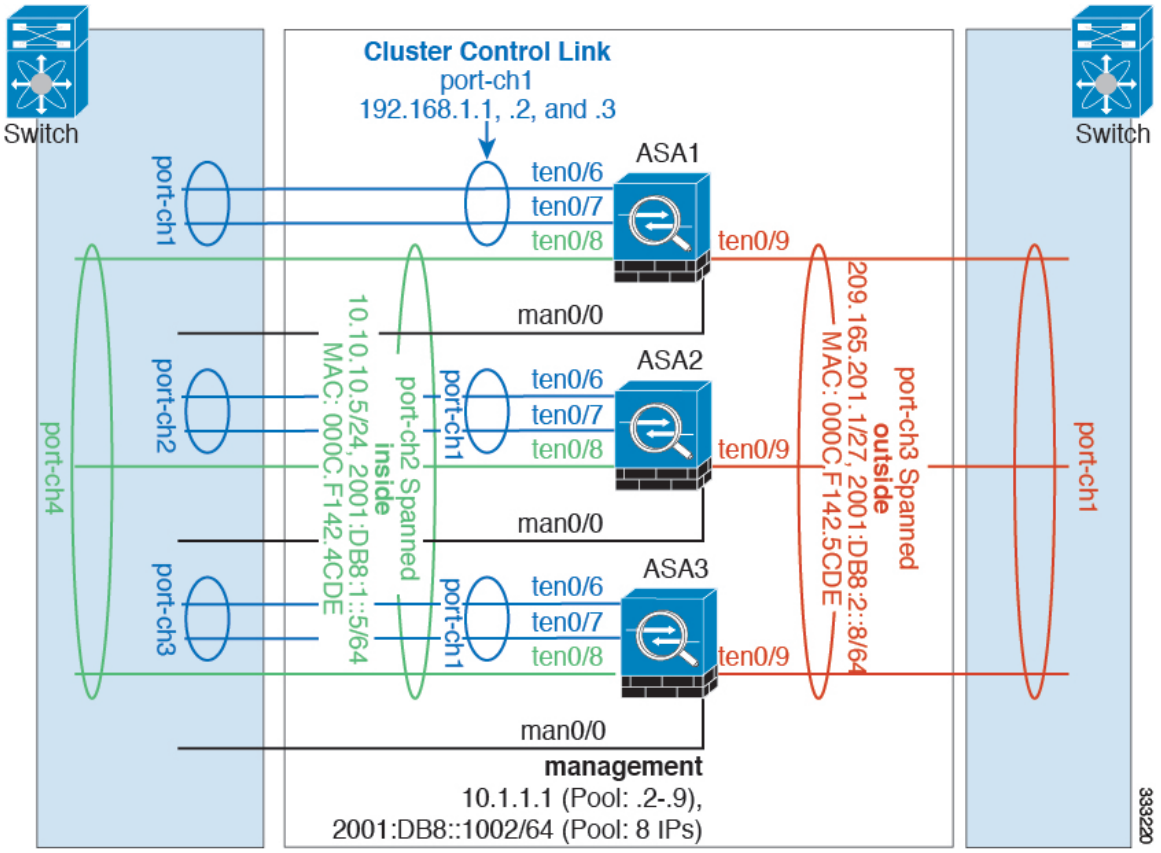
スティック上のファイアウォール



異なるセキュリティ ドメインからのデータ トラフィックには、異なる VLAN が関連付けられます。たとえば内部ネットワーク用には VLAN 10、外部ネットワークには VLAN 20 とします。各 ASA は単一の物理ポートがあり、外部スイッチまたはルータに接続されます。トランキングがイネーブルになっているので、物理リンク上のすべてのパケットが 802.1q カプセル化されます。ASA は、VLAN 10 と VLAN 20 の間のファイアウォールです。

スパンド EtherChannel を使用するときは、スイッチ側ですべてのデータ リンクがグループ化されて 1 つの EtherChannel となります。ASA が使用不可能になった場合は、スイッチは残りのユニット間でトラフィックを再分散します。

トラフィックの分離



内部ネットワークと外部ネットワークの間で、トラフィックを物理的に分離できます。

上の図に示すように、左側に一方のスパンドEtherChannelがあり、内部スイッチに接続されています。他方は右側にあり、外部スイッチに接続されています。必要であれば、各EtherChannel上にVLANサブインターフェイスを作成することもできます。

ルーテッド モード サイト間クラスタリングの OTV 設定

スパンド EtherChannel を使用したルーテッド モードに対するサイト間クラスタリングの成功は、OTV の適切な設定とモニタリングによって異なります。OTV は、DCI 全体にパケットを転送することで、重要な役割を果たします。OTVは、転送テーブルにMACアドレスを学習するときにのみ、DCI 全体にユニキャスト パケットを転送します。MAC アドレスが OTV 転送テーブルに学習されていない場合、ユニキャスト パケットはドロップされます。

OTV 設定の例

```
//Sample OTV config:
//3151 - Inside VLAN, 3152 - Outside VLAN, 202 - CCL VLAN
//aaaa.1111.1234 - ASA inside interface global vMAC
//0050.56A8.3D22 - Server MAC
```

```
feature ospf
feature otv

mac access-list ALL_MACs
  10 permit any any
mac access-list HSRP_VMAC
  10 permit aaaa.1111.1234 0000.0000.0000 any
  20 permit aaaa.2222.1234 0000.0000.0000 any
  30 permit any aaaa.1111.1234 0000.0000.0000
  40 permit any aaaa.2222.1234 0000.0000.0000
vlan access-map Local 10
  match mac address HSRP_VMAC
  action drop
vlan access-map Local 20
  match mac address ALL_MACs
  action forward
vlan filter Local vlan-list 3151-3152


//To block global MAC with ARP inspection:
arp access-list HSRP_VMAC_ARP
  10 deny aaaa.1111.1234 0000.0000.0000 any
  20 deny aaaa.2222.1234 0000.0000.0000 any
  30 deny any aaaa.1111.1234 0000.0000.0000
  40 deny any aaaa.2222.1234 0000.0000.0000
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP 3151-3152

no ip igmp snooping optimise-multicast-flood
vlan 1,202,1111,2222,3151-3152

otv site-vlan 2222
mac-list GMAC_DENY seq 10 deny aaaa.aaaa.aaaa ffff.ffff.ffff
mac-list GMAC_DENY seq 20 deny aaaa.bbbb.bbbb ffff.ffff.ffff
mac-list GMAC_DENY seq 30 permit 0000.0000.0000 0000.0000.0000
route-map stop-GMAC permit 10
  match mac-list GMAC_DENY

interface Overlay1
  otv join-interface Ethernet8/1
  otv control-group 239.1.1.1
  otv data-group 232.1.1.0/28
  otv extend-vlan 202, 3151
  otv arp-nd timeout 60
  no shutdown

interface Ethernet8/1
  description uplink_to_OTV_cloud
  mtu 9198
  ip address 10.4.0.18/24
  ip igmp version 3
  no shutdown

interface Ethernet8/2

interface Ethernet8/3
  description back_to_default_vdc_e6/39
  switchport
    switchport mode trunk
    switchport trunk allowed vlan 202,2222,3151-3152
  mac packet-classify
  no shutdown
```

```
otv-isis default
  vpn Overlay1
    redistribute filter route-map stop-GMAC
otv site-identifier 0x2
//OTV flood not required for ARP inspection:
otv flood mac 0050.56A8.3D22 vlan 3151
```

サイト障害のために必要な OTV フィルタの変更

サイトがダウンした場合は、グローバル MAC アドレスをそれ以上ブロックしなくて済むように、フィルタを OTV から削除する必要があります。必要ないくつかの追加設定があります。

機能しているサイトで OTV スイッチ上の ASA グローバル MAC アドレスに対するスタティック エントリを追加する必要があります。このエントリによって、反対側の OTV はオーバーレイ インターフェイスにこれらのエントリを追加できます。サーバとクライアントに ASA 用の ARP エントリがすでにある場合（これは既存の接続の場合です）、ARP は再送信されないので、この手順が必要になります。したがって、OTV は転送テーブルに ASA グローバル MAC アドレスを学習する機会はありません。OTV には転送テーブル内にグローバル MAC アドレスがなく、OTV の設計ごとに OTV はオーバーレイ インターフェイスを介してユニキャスト パケットをフラッディングしないので、ユニキャスト パケットはサーバからのグローバル MAC アドレスにドロップされ、既存の接続は切断されます。

```
//OTV filter configs when one of the sites is down

mac-list GMAC_A seq 10 permit 0000.0000.0000 0000.0000.0000
route-map a-GMAC permit 10
  match mac-list GMAC_A

otv-isis default
  vpn Overlay1
    redistribute filter route-map a-GMAC

no vlan filter Local vlan-list 3151

//For ARP inspection, allow global MAC:
arp access-list HSRP_VMAC_ARP_Allow
  50 permit ip any mac
ip arp inspection filter HSRP_VMAC_ARP_Allow 3151-3152

mac address-table static aaaa.1111.1234 vlan 3151 interface Ethernet8/3
//Static entry required only in the OTV in the functioning Site
```

他のサイトが復元した場合は、フィルタを再度追加して、OTV でこのスタティック エントリを削除する必要があります。グローバル MAC アドレスのオーバーレイ エントリをクリアするには、両方の OTV でダイナミック MAC アドレス テーブルをクリアすることが非常に重要です。

MAC アドレス テーブルのクリア

サイトがダウンし、グローバル MAC アドレスへのスタティック エントリが OTV に追加される場合は、他の OTV がオーバーレイ インターフェイスのグローバル MAC アドレスを学習できるようにする必要があります。他のサイトが起動したら、これらのエントリをクリアする必

要があります。OTV の転送テーブルにこれらのエントリがないことを確認するために、MAC アドレス テーブルを必ず消去してください。

```
cluster-N7k6-OTV# show mac address-table
Legend:
* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
age - seconds since last seen,+ - primary entry using vPC Peer-Link,
(T) - True, (F) - False
VLAN MAC Address Type age Secure NTFY Ports/SWID.SSID.LID
---------+-----------------+--------+---------+------+----+------------------
G -    d867.d900.2e42 static  -  F F sup-eth1(R)
O 202  885a.92f6.44a5 dynamic -  F F Overlay1
* 202  885a.92f6.4b8f dynamic 5  F F Eth8/3
O 3151 0050.5660.9412 dynamic -  F F Overlay1
* 3151 aaaa.1111.1234 dynamic 50 F F Eth8/3
```

OTV ARP キャッシュのモニタリング

OTV は、OTV インターフェイス全体で学習した IP アドレスに対するプロキシ ARP への ARP キャッシュを維持します。

```
cluster-N7k6-OTV# show otv arp-nd-cache
OTV ARP/ND L3->L2 Address Mapping Cache

Overlay Interface Overlay1
VLAN MAC Address Layer-3 Address Age Expires In
3151 0050.5660.9412 10.0.0.2 1w0d 00:00:31
cluster-N7k6-OTV#
```

サイト間クラスタリングの例

次の例では、サポートされるクラスタ導入を示します。

サイト固有の MAC アドレスおよび IP アドレスを使用したスパンド EtherChannel ルーテッド モードの例

次の例では、各サイトのゲートウェイ ルータと内部ネットワーク間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部両方のネットワークに対しスパンド EtherChannel を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

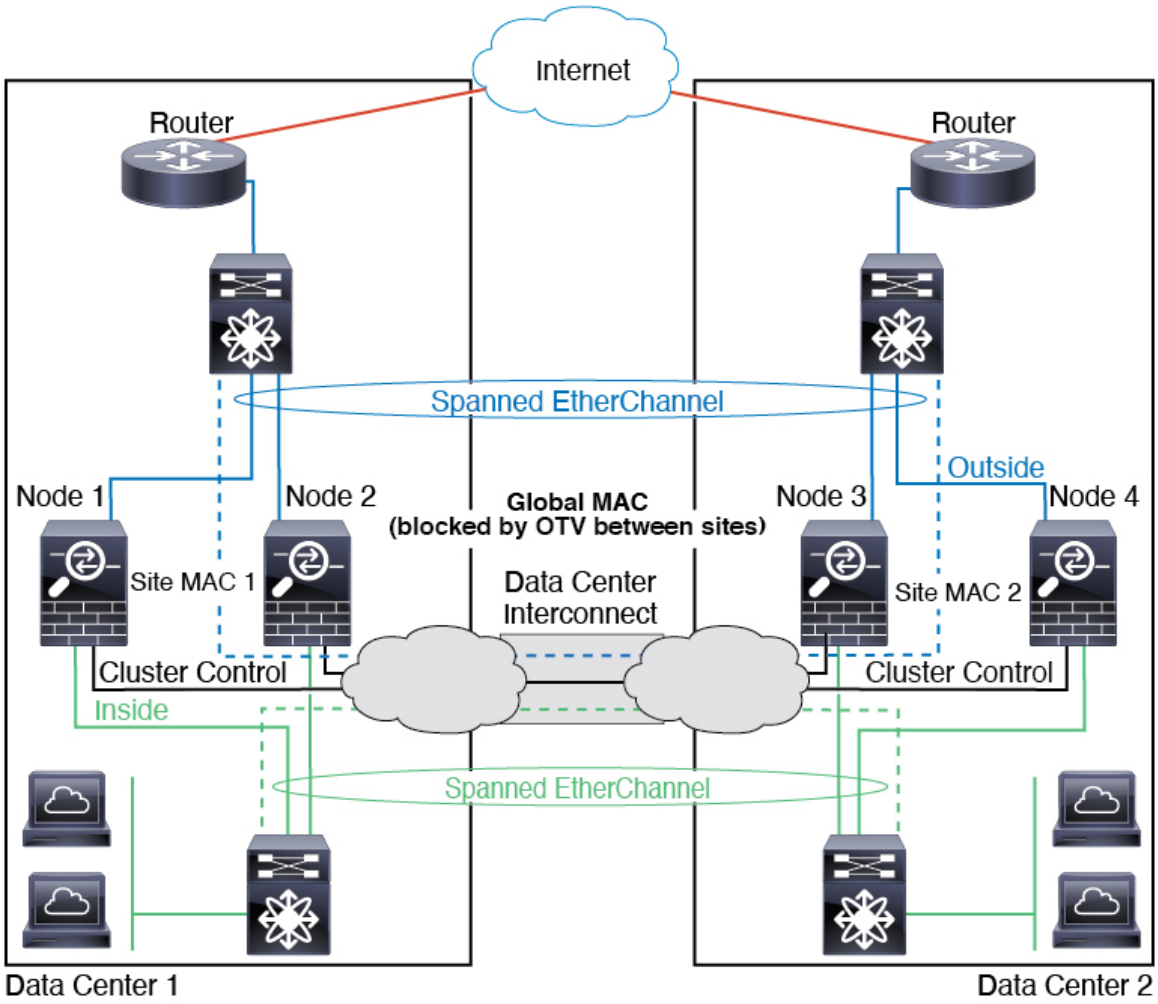
データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがクラスタ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、グローバル MAC アドレスをブロックするフィルタを追加する必要があります。1 つのサイトのクラスタノードが到達不能になった場合、トラフィックが他のサイトのクラスタノードに送信されるようにフィルタを削除する必要があります。Vacl を使用して、グローバルの MAC アドレスのフィルタ リングする必要があります。F3 シリーズラインカードを使用した Nexus などの一部のスイッチでは、グローバル

MAC アドレスからの ARP パケットをブロックするために ARP インスペクションも使用する必要があります。ARP インスペクションでは、ASA でサイトの MAC アドレスとサイトの IP アドレスの両方を設定する必要があります。サイトの MAC アドレスのみを設定する場合は必ず ARP インスペクションを無効にしてください。

クラスタは、内部ネットワークのゲートウェイとして機能します。すべてのクラスタノード間で共有されるグローバルな仮想 MAC は、パケットを受信するためだけに使用されます。発信パケットは、各 DC クラスタからのサイト固有の MAC アドレスを使用します。この機能により、MAC フラッピングの原因となる 2 つの異なるポートで両方のサイトから同じグローバル MAC アドレスをスイッチが学習するのを防止します。代わりに、スイッチはサイトの MAC アドレスのみを学習します。

このシナリオでは、次のようになります。

- クラスタから送信されるすべての出力パケットは、サイトの MAC アドレスを使用し、データセンターでローカライズされます。
- クラスタへのすべての入力パケットは、グローバル MAC アドレスを使用して送信されるため、両方のサイトにある任意のノードで受信できます。OTV のフィルタによって、データセンター内のトラフィックがローカライズされます。



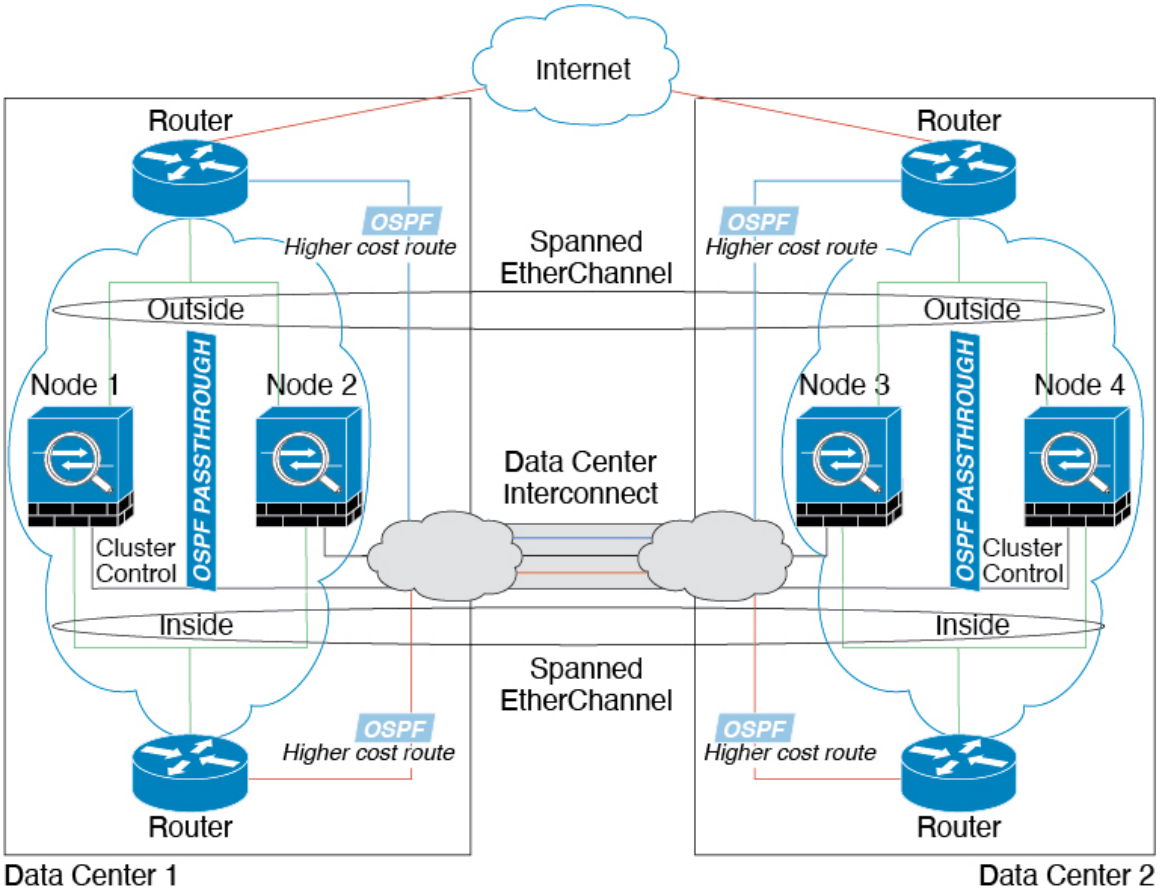
スパンド EtherChannel トランスペアレント モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各データセンターの内部ルータと外部ルータは OSPF を使用し、トランスペアレント ASA を通過します。MAC とは異なり、ルータの IP はすべてのルータで一意です。DCI に高コスト ルートを割り当てることにより、特定のサイトですべてのクラスタ メンバがダウンしない限り、トラフィックは各データセンター内に維持されます。クラスタが非対称型の接続を維持するため、ASA を通過する低コストのルートは、各サイトで同じブリッジ グループを横断する必要があります。1 つのサイトのすべてのクラスタ メンバに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトのクラスタ メンバに送られます。

各サイトのスイッチの実装には、次のものを含めることができます。

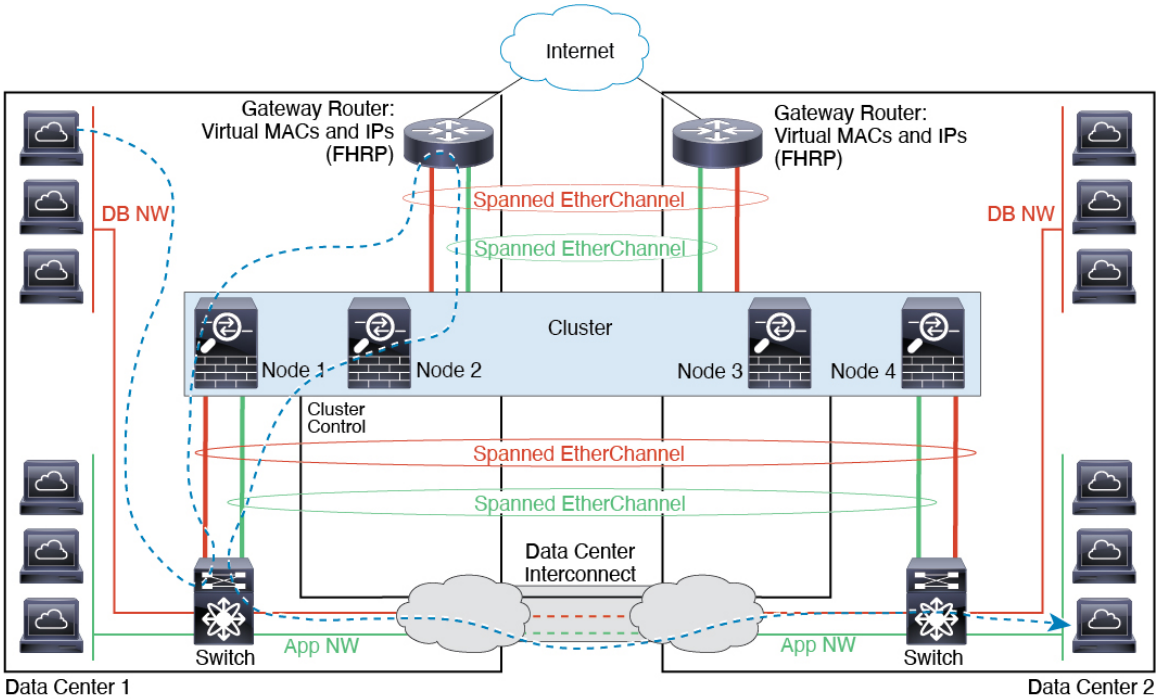
- サイト間 VSS、vPC、StackWise、StackWise Virtual：このシナリオでは、データセンター 1 に 1 台のスイッチをインストールし、データセンター 2 に別のスイッチをインストールします。1 つのオプションとして、各データセンターのクラスタノードはローカルスイッチだけに接続し、冗長スイッチトラフィックはDCIを経由します。この場合、接続のほとんどの部分は各データセンターに対してローカルに維持されます。DCIが余分なトラフィックを処理できる場合、必要に応じて、各ノードをDCI経由で両方のスイッチに接続できます。この場合、トラフィックは複数のデータセンターに分散されるため、DCIを非常に堅牢にするためには不可欠です。
- 各サイトのローカル VSS、vPC、StackWise、StackWise Virtual：スイッチの冗長性を高めるには、各サイトに2つの異なる冗長スイッチペアをインストールできます。この場合、クラスタノードは、両方のローカルスイッチだけに接続されたデータセンター1のシャーシ、およびそれらのローカルスイッチに接続されたデータセンター2のシャーシではスパンド EtherChannel を使用しますが、スパンド EtherChannel は基本的に「分離」しています。各ローカル冗長スイッチは、スパンド EtherChannel をサイトローカルの EtherChannel として認識します。



スパンド EtherChannel トランスペアレント モード イーストウェスト サイト間の例

次の例では、各サイトのゲートウェイ ルータと 2 つの内部ネットワーク（アプリケーション ネットワークと DB ネットワーク）間に配置された（イーストウェスト挿入）2 つのデータセンターのそれぞれに 2 つのクラスタ メンバがある場合を示します。クラスタ メンバは、DCI 経由のクラスタ制御リンクによって接続されています。各サイトのクラスタ メンバは、内部および外部のアプリケーション ネットワークと DB ネットワークの両方にスパンド EtherChannels を使用してローカル スイッチに接続します。各 EtherChannel は、クラスタ内のすべてのシャーシにスパンされます。

各サイトのゲートウェイ ルータは、HSRP などの FHRP を使用して、各サイトで同じ宛先の仮想 MAC アドレス と IP アドレスを提供します。MAC アドレスの予期せぬフラッピングを避けるため、**mac-address-table static** *outside_interface mac_address* コマンドを使用して、ゲートウェイルータの実際の MAC アドレスを ASA MAC アドレステーブルに静的に追加することをお勧めします。これらのエントリがないと、サイト 1 のゲートウェイがサイト 2 のゲートウェイと通信する場合に、そのトラフィックが ASA を通過して、内部インターフェイスからサイト 2 に到達しようとして、問題が発生する可能性があります。データ VLAN は、オーバーレイ トランスポート仮想化（OTV）（または同様のもの）を使用してサイト間に拡張されます。トラフィックがゲートウェイ ルータ宛てである場合にトラフィックが DCI を通過して他のサイトに送信されないようにするには、フィルタを追加する必要があります。1 つのサイトのゲートウェイ ルータが到達不能になった場合、トラフィックが他のサイトのゲートウェイに送信されるようにフィルタを削除する必要があります。



クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- IS-IS ルーティング
- 次のアプリケーション インスペクション：
  - CTIQBE
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- VPN ロード バランシング
- フェールオーバー

- 統合ルーティングおよびブリッジング
- デッド接続検出（DCD）
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス
- サイト間 VPN

集中モードでは、VPN 接続はクラスタの制御ノードとのみ確立されます。 これは VPN クラスタリングのデフォルト モードです。サイト間 VPN は、分散 VPN モードでも展開できます。この場合、S2S IKEv2 VPN 接続がノード間で分散されます。

- IGMP マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- PIM マルチキャスト コントロール プレーン プロトコル処理（データ プレーン転送はクラスタ全体に分散されます）
- ダイナミック ルーティング

個々のユニットに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。
- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証と許可は、クラスタリング制御ノード上で中央集中型機能として実装されており、データ構造がクラスタデータノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるため、フローに対するアカウンティングが設定されている場合、そのフローを所有するクラスタノードがアカウンティング開始と停止のメッセージを AAA サーバに送信します。

接続設定

接続制限は、クラスタ全体に適用されます（**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、および **set connection per-client-max** コマンドを参照）。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

FTP とクラスタリング

- FTPデータ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用する場合、制御チャネルのフローは制御ノードに集中されます。

ICMP インスペクション

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインスペクションが有効かどうかによって異なります。ICMPインスペクションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インスペクションを使用する場合、ICMPフローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットのディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

マルチキャスト ルーティングとクラスタリング

ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャストルーティングパケットとデータパケットを処理します。接続が確立された後は、各データユニットがマルチキャスト データ パケットを転送できます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NATが使用されるときは、インバウンドとアウトバウンドとで、パケットのIPアドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続

を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

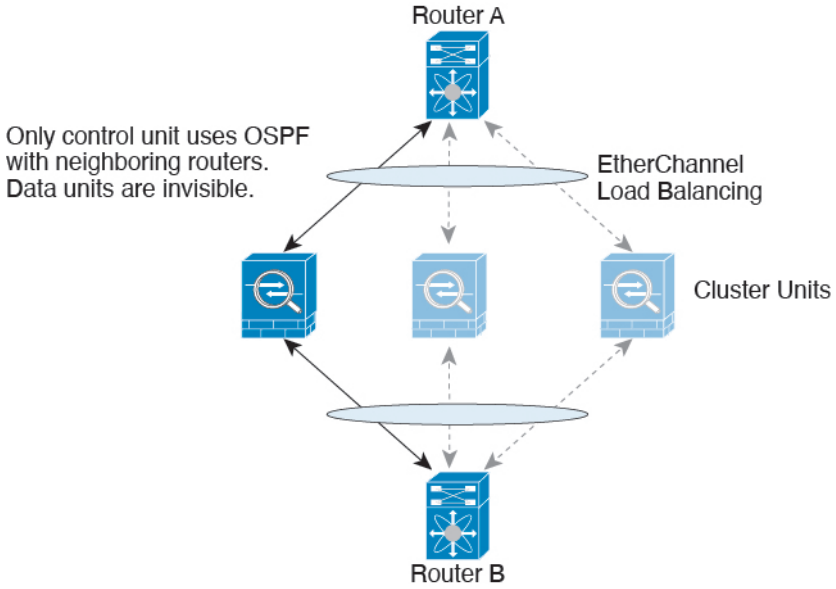
- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。
- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。
- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。

- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。たとえば、TCP/443 の HTTPS TLS と比較してずっと優れたパフォーマンスを発揮する代替手段として、UDP/443 を用いる Quick プロトコルの使用が増加している場合、UDP/443 に対し per-session PAT を有効にする必要があります。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

ダイナミック ルーティングおよびクラスタリング

ルーティングプロセスは制御ユニット上だけで実行されます。ルートは制御ユニットを介して学習され、セカンダリに複製されます。ルーティングパケットがデータユニットに到着した場合は、制御ユニットにリダイレクトされます。

図 *53*：ダイナミック ルーティング



データユニットが制御ユニットからルートを学習した後は、各ユニットが個別に転送に関する判断を行います。

OSPF LSA データベースは、制御ユニットからデータユニットに同期されません。制御ユニットのスイッチオーバーが発生した場合は、隣接ルータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ ID がクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、その 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、STUNインスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN要求の受信後にノードに障害が発生し、別のノードがSTUN応答を受信した場合、STUN応答はドロップされます。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。
- NetFlow：クラスタの各ノードは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

Secure Firewall eXtensible オペレーティングシステム（FXOS）シャーシ上の VPN とクラスタリング

ASA FXOS クラスタは、S2S VPN に対する相互排他的な 2 つのモード（集中型または分散型）のいずれかをサポートしています。

- 集中型 VPN モード。デフォルト モードです。集中モードでは、VPN 接続はクラスタの制御ユニットとのみ確立されます。

  VPN機能を使用できるのは制御ユニットだけであり、クラスタの高可用性機能は活用されません。制御ユニットで障害が発生した場合は、すべての既存のVPN接続が失われ、VPN接続されたユーザーにとってはサービスの中断となります。新しい制御ユニットが選定されたときに、VPN 接続を再確立する必要があります。

  VPN トンネルをスパンドインターフェイスのアドレスに接続すると、接続が自動的に制御ユニットに転送されます。VPN 関連のキーと証明書は、すべてのユニットに複製されます。

- 分散型 VPN モード。このモードでは、S2S IPsec IKEv2 VPN 接続が ASA クラスタのメンバー全体に分散され、拡張性が提供されます。クラスタのメンバー全体に VPN 接続を分散することで、クラスタの容量とスループットの両方を最大限に活用できるため、集中型 VPN の機能を超えて大幅に VPN サポートを拡張できます。

（注） 集中型 VPN クラスタリング モードは、S2S IKEv1 と S2S IKEv2 をサポートしています。

分散型 VPN クラスタリング モードは、S2S IKEv2 のみをサポートしています。

分散型 VPN クラスタリング モードは、Firepower 9300 でのみサポートされています。

リモート アクセス VPN は、集中型または分散型の VPN クラスタリング モードではサポートされていません。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80% になります。

たとえば、TCP スループットについては、3 つの SM-40 モジュールを備えた Firepower 9300 が処理できる実際のファイアウォール トラフィックは、単独動作時は約 135 Gbps となります。2 シャーシの場合、最大スループットの合計は 270 Gbps（2 シャーシ X 135 Gbps）の約 80 %、つまり 216 Gbps です。

制御ユニットの選定

クラスタのメンバーは、クラスタ制御リンクを介して通信して制御ユニットを選定します。方法は次のとおりです。

1. クラスタを展開すると、各ユニットは選定要求を 3 秒ごとにブロードキャストします。
2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティはクラスタの展開時に設定され、設定の変更はできません。

3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットが制御ユニットになります。

（注） 最高のプライオリティを持つユニットが複数ある場合は、クラスタユニット名、次にシリアル番号を使用して制御ユニットが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的に制御ユニットになることはありません。既存の制御ユニットは常に制御ユニットのままです。ただし、制御ユニットが応答を停止すると、その時点で新しい制御ユニットが選定されます。

5. 「スプリットブレイン」シナリオで一時的に複数の制御ユニットが存在する場合、優先順位が最も高いユニットが制御ユニットの役割を保持し、他のユニットはデータユニットの役割に戻ります。

（注） 特定のユニットを手動で強制的に制御ユニットにすることができます。中央集中型機能については、制御ユニット変更を強制するとすべての接続がドロップされるので、新しい制御ユニット上で接続を再確立する必要があります。

クラスタ内のハイ アベイラビリティ

クラスタリングは、シャーシ、ユニットとインターフェイスの正常性を監視し、ユニット間で接続状態を複製することにより、ハイ アベイラビリティを提供します。

シャーシ アプリケーションのモニターリング

シャーシ アプリケーションのヘルス モニターリングは常に有効になっています。Firepower 4100/9300 シャーシ スーパバイザは、ASA アプリケーションを定期的に確認します（毎秒）。ASA が作動中で、Firepower 4100/9300 シャーシ スーパバイザと 3 秒間通信できなければ、ASA は syslog メッセージを生成して、クラスタを離れます。

Firepower 4100/9300 シャーシ スーパバイザが 45 秒後にアプリケーションと通信できなければ、ASA をリロードします。ASA がスーパバイザと通信できなければ、自身をクラスタから削除します。

装置のヘルス モニターリング

各ユニットは、クラスタ制御リンクを介してブロードキャストキープアライブハートビートパケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからキープアライブハートビートパケット、またはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション 2 のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。詳細については、制御ユニットの選定 （619 ページ）を参照してください。

インターフェイス モニタリング

各ノードは、使用中のすべてのハードウェアインターフェイスのリンクステータスを監視し、ステータスの変更を制御ノードに報告します。複数のシャーシにわたるクラスタリングの場合、スパンド EtherChannel はクラスタ Link Aggregation Control Protocol（cLACP）を使用します。各シャーシはリンク ステータスと cLACP プロトコル メッセージをモニターして EtherChannel でポートがアクティブであるかどうかを判別し、インターフェイスがダウンしている場合には ASA アプリケーションに通知します。ヘルスモニターリングを有効にすると、デフォルトではすべての物理インターフェイスがモニターされます（EtherChannel インターフェイスのメイン EtherChannel を含む）。アップ状態の名前付きインターフェイスのみモニターできます。たとえば、名前付き EtherChannel がクラスタから削除されるまでは、EtherChannel のすべてのメンバー ポートは失敗しなければなりません（最小ポート バンドル設定により異なる）。ヘルスチェックは、インターフェイスごとに、モニターリングをオプションで無効にすることができます。

特定のノードで監視対象のインターフェースに障害が発生し、その他のノードでそのインターフェイスがアクティブになっている場合、そのノードはクラスタから削除されます。ASA によってノードがクラスタから削除されるまでの時間は、そのノードが確立済みのメンバーであるかクラスタに参加しようとしているかによって異なります。ASA は、ノードがクラスタに参加する最初の 90 秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。確立済みのメンバーの場合は、500 ミリ秒後にノードが削除されます。

複数のシャーシにわたるクラスタリングの場合、クラスタから EtherChannel を追加または削除すると、各シャーシに変更を加えられるように、インターフェイス ヘルス モニタリングは 95 秒間中断されます。

デコレータ アプリケーションのモニタリング

インターフェイスに Radware DefensePro アプリケーションなどのデコレータ アプリケーションをインストールした場合、ユニットがクラスタ内にとどまるには ASA、デコレータ アプリケーションの両方が動作している必要があります。両方のアプリケーションが動作状態になるまで、ユニットはクラスタに参加しません。いったんクラスタに参加すると、ユニットはデコレータ アプリケーションが正しく動作しているか 3 秒ごとにモニターします。デコレータ アプリケーションがダウンすると、ユニットはクラスタから削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASAが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでノードがまだ非アクティブになっていると、管理インターフェイスは無効になります。さらに設定を行う場合は、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタ メンバがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害（最初の参加時）：クラスタ制御リンクの問題を解決した後、ASA コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを再びイネーブルにすることによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASA は、無限に 5 分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データ インターフェイスの問題を解決した後、ASA コンソール ポートで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動でイネーブルにする必要があります。この動作は設定可能です。
- ユニットの障害：ユニットがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働している限り、ユニットは再起動するとクラスタに再参加します。ユニットは 5 秒ごとにクラスタへの再参加を試みます。
- シャーシアプリケーション通信の障害：ASA がシャーシアプリケーションの状態が回復したことを検出すると、ASA はすぐにクラスタの再参加を試みます。または、内部エラーの場合と同じ再参加設定を使用するように ASA を設定できます（以下を参照）。
- デコレータ アプリケーションの障害：ASA はデコレータ アプリケーションが復帰したことを確認すると、クラスタへ再参加します。

- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 ユニットは5分、10分、および20分の間隔でクラスタに自動的に再参加を試行します。この動作は設定可能です。

データ パス接続状態の複製

どの接続にも、1つのオーナーおよび少なくとも1つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *19*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システム アップ タイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—
Firepower 4100/9300 の分散型 VPN（サイト間）	Yes	バックアップ セッションがアクティブ セッションになると、新しいバックアップ セッションが作成されます。

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発

生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。

- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

  サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルバックアップとグローバルバックアップの2つのバックアップ オーナー権限があります。オーナーは、常に同じサイトのローカルバックアップをオーナー自身として選択します（サイトIDに基づいて）。グローバルバックアップはどのサイトにあってもよく、ローカルバックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

  サイトの冗長性を有効にし、バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。シャーシバックアップとサイトバックアップは独立しているため、フローにはシャーシ バックアップとサイト バックアップの両方が含まれている場合があります。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルディレクタとグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（Site Id に基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにあってもよく、ローカルディレクタと同一ノー

ドとすることもできます。元のオーナーに障害が発生すると、ローカルディレクタはこのサイトで新しい接続オーナーを選択します。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
- 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
- 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタのローカリゼーションを有効にすると、フォワーダは常にローカルディレクタに問い合わせます。フォワーダがグローバルディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタ メンバーが受信する場合などです。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定され

た接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

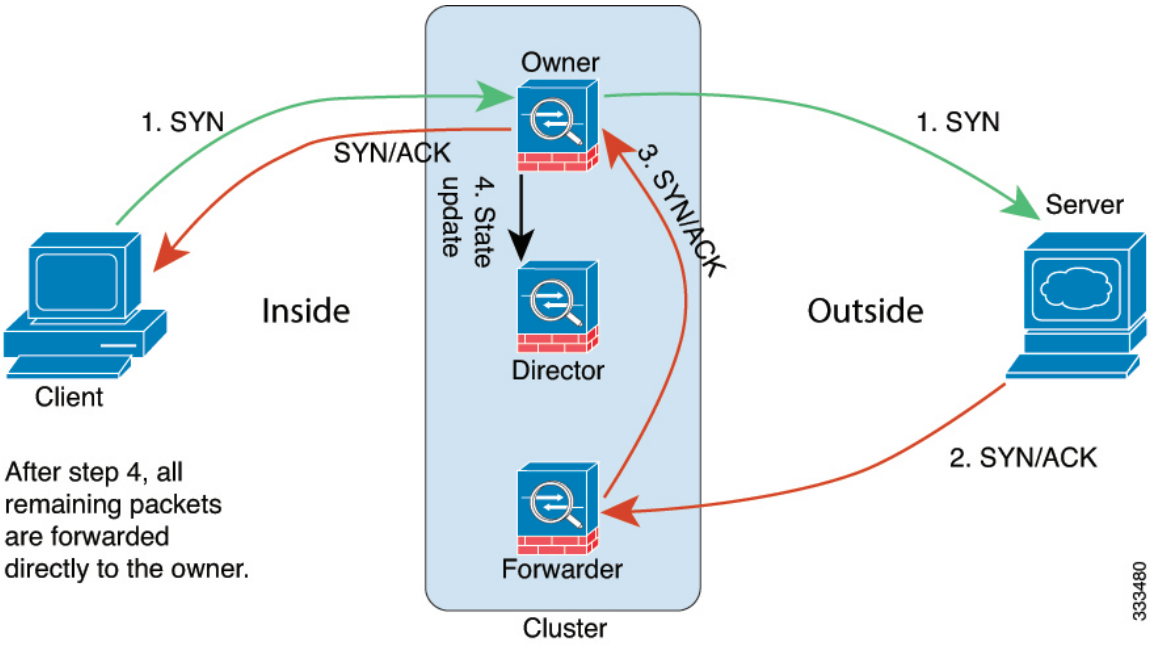
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

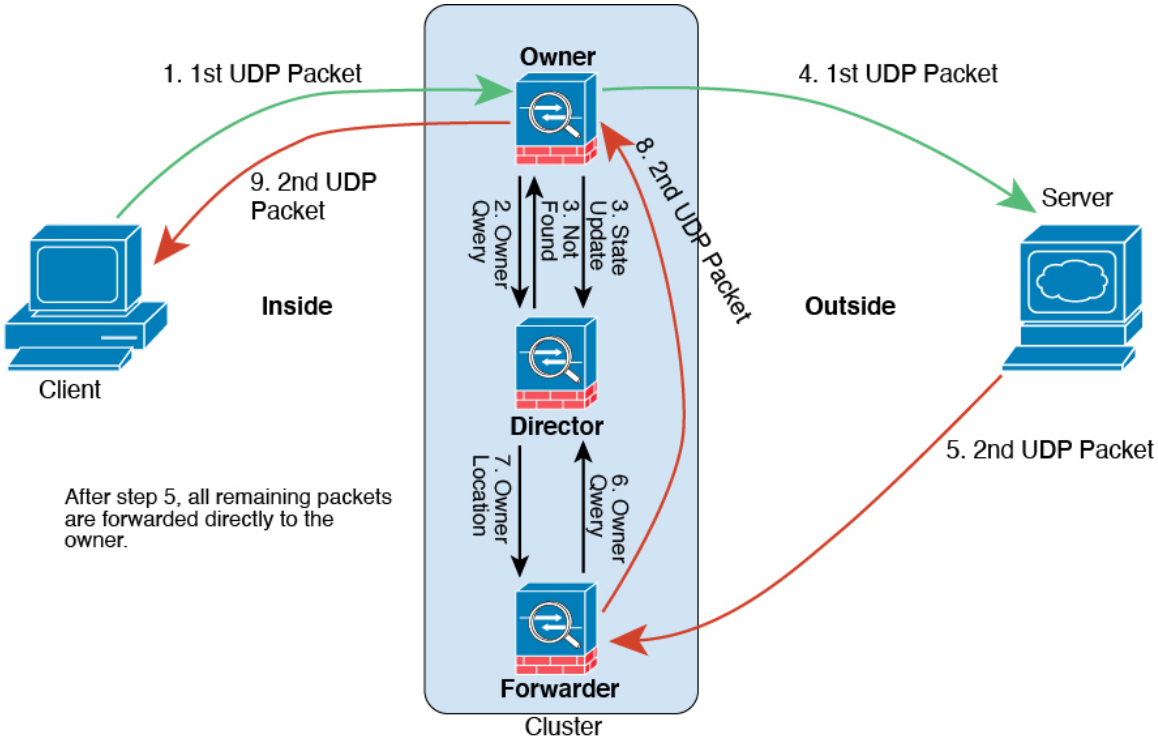


1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

1. 図 *54 : ICMP* および *UDP* データフロー



UDP パケットがクライアントから発信され、1 つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

新しい TCP 接続のクラスタ全体での再分散

アップストリームルータまたはダウンストリームルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しい接続再分散を設定して、1 秒あたりの新しい接続数が多いノードから他のノードに新しい TCP フローをリダイレクトすることができます。既存のフローは他のノードには移動されません。

このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。

接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタメンバには新しい接続を再分散できません。

Firepower 4100/9300 上の ASA クラスタリングの履歴

機能名	バージョン	機能情報
ノード参加時の MTU ping テスト	9.23(1)	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
シャーシハートビート障害後にクラスタに再参加するための設定可能な遅延（Firepower 4100/9300）	9.20(2)	デフォルトでは、シャーシハートビート障害から回復すると、ノードはすぐにクラスタに再参加します。ただし、**health-check chassis-heartbeat-delay-rejoin** コマンドを設定すると、**health-check system auto-rejoin** コマンドの設定に従って再参加します。 新規/変更されたコマンド： **health-check chassis-heartbeat-delay-rejoin**
フローステータスの設定可能なクラスタキープアライブ間隔	9.20(1)	フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。 新規/変更されたコマンド： **clu-keepalive-interval**
バイアス言語の除去	9.19(1)	「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。 新規/変更されたコマンド：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**

機能名	バージョン	機能情報
Firepower 4100/9300 でのクラスタリング用の PAT ポートブロック割り当ての改善	9.16(1)	PAT ポートブロック割り当ての改善により、制御ユニットはノードに参加するためにポートを確保し、未使用のポートを積極的に再利用できるようになります。割り当てを最適化するために、**cluster-member-limit** コマンドを使用して、クラスタ内に配置する予定の最大ノードを設定できます。これにより、制御ユニットは計画されたノード数にポートブロックを割り当てることができ、使用する予定のない追加のノード用にポートを予約する必要がなくなります。デフォルトは 16 ノードです。また、syslog 747046 を監視して、新しいノードに使用できるポートが十分にあることを確認することもできます。 新規/変更されたコマンド：**cluster-member-limit**、**show nat pool cluster** [**summary**]、**show nat pool ip detail**
show cluster history コマンドの改善	9.16(1)	**show cluster history** コマンドの出力が追加されました。 新規/変更されたコマンド： **show cluster history brief**、**show cluster history latest**、**show cluster history reverse**、**show cluster history time**
データユニットとの設定の並列同期	9.14(1)	制御ユニットでは、デフォルトで設定変更がデータユニットと同時に同期化されるようになりました。以前は、順番に同期が行われていました。 新規/変更されたコマンド： **config-replicate-parallel**
クラスタへの参加失敗や削除のメッセージが、以下に追加されました。 **show cluster history**	9.14(1)	クラスタユニットがクラスタへの参加に失敗した場合や、クラスタを離脱した場合の新しいメッセージが、 **show cluster history** コマンドに追加されました。 新規/変更されたコマンド： **show cluster history**
デッド接続検出（DCD）の発信側および応答側の情報、およびクラスタ内の DCD のサポート。	9.13(1)	デッド接続検出（DCD）を有効にした場合は、**show conn detail** コマンドを使用して発信側と応答側に関する情報を取得できます。デッド接続検出を使用すると、非アクティブな接続を維持できます。**show conn** の出力は、エンドポイントがプローブされた頻度が示されます。さらに、DCD がクラスタでサポートされるようになりました。 新しい/変更されたコマンド：**show conn**（出力のみ）
クラスタのトラフィック負荷のモニター	9.13(1)	クラスタ メンバのトラフィック負荷をモニターできるようになりました。これには、合計接続数、CPU とメモリの使用率、バッファ ドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。 新規/変更されたコマンド：**debug cluster load-monitor**、**load-monitor**、**show cluster info load-monitor**

機能名	バージョン	機能情報
クラスタ結合の高速化	9.13(1)	データユニットが制御ユニットと同じ設定の場合、設定の同期をスキップし、結合を高速化します。この機能は、デフォルトでイネーブルにされています。この機能はユニットごとに設定され、制御ユニットからデータユニットには複製されません。 （注） 一部の設定コマンドは、クラスタ結合の高速化と互換性がありません。これらのコマンドがユニットに存在する場合、クラスタ結合の高速化が有効になっていても、設定の同期は常に発生します。クラスタ結合の高速化を動作させるには、互換性のない設定を削除する必要があります。**show cluster info unit-join-acceleration incompatible-config** を使用して、互換性のない設定を表示します。 新規/変更されたコマンド：**unit join-acceleration**、**show cluster info unit-join-acceleration incompatible-config**
サイトごとのクラスタリング用 Gratuitous ARP	9.12(1)	ASA では、Gratuitous ARP（GARP）パケットを生成してスイッチング インフラストラクチャを常に最新の状態に保つようになりました。各サイトの優先順位値が最も高いメンバによって、グローバル MAC/IP アドレスの GARP トラフィックが定期的に生成されます。クラスタから送信されたサイトごとの MAC および IP アドレスとパケットがサイト固有の MAC アドレスおよび IP アドレスを使用するのに対し、クラスタで受信したパケットは、グローバル MAC アドレスおよび IP アドレスを使用します。トラフィックがグローバル MAC アドレスから定期的に生成されない場合、グローバル MAC アドレスのスイッチで MAC アドレスのタイムアウトが発生する可能性があります。タイムアウト後にグローバル MAC アドレスへのトラフィックがスイッチング インフラストラクチャ全体にわたりフラッディングされ、これによりパフォーマンスおよびセキュリティ上の問題が発生することがあります。各スパンド EtherChannel のユニットおよびサイト MAC アドレスごとにサイト ID を設定すると、GARP がデフォルトで有効になります。 新規/変更されたコマンド： **site-periodic-garp interval**
Firepower 9300 シャーシごとのユニットのパラレル クラスタ参加	9.10(1)	Firepower 9300 の場合、この機能により、シャーシ内のセキュリティ モジュールがクラスタに同時に参加し、トラフィックがモジュール間で均等に分散されるようになります。他のモジュールよりもかなり前に参加したモジュールは、他のモジュールがまだ負荷を共有できないため、必要以上のトラフィックを受信することがあります。 新規/変更されたコマンド： **unit parallel-join**

機能名	バージョン	機能情報
Firepower 4100/9300 のクラスタ制御リンクのカスタマイズ可能な IP アドレス	9.10(1)	クラスタ制御リンクのデフォルトでは 127.2.0.0/16 ネットワークが使用されます。これで FXOS でクラスタを展開するときにネットワークを設定できます。シャーシは、シャーシ ID およびスロット ID（127.2.*chassis_id.slot_id*）に基づいて、各ユニットのクラスタ制御リンク インターフェイス IP アドレスを自動生成します。ただし、一部のネットワーク展開では、127.2.0.0/16 トラフィックはパスできません。そのため、ループバック（127.0.0.0/8）およびマルチキャスト（224.0.0.0/4）アドレスを除き、FXOS にクラスタ制御リンクのカスタム /16 サブネットを作成できるようになりました。 新規/変更された FXOS コマンド： **set cluster-control-link network**
クラスタ インターフェイス デバウンス時間は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。	9.10(1)	インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで **health-check monitor-interface debounce-time** コマンドまたは ASDM **[Configuration]** > **[Device Management]** > **[High Availability and Scalability]** > **[ASA Cluster]** 画面で指定されたミリ秒数待機します。この機能は、ダウン状態から稼働状態に変更するインターフェイスに適用されるようになりました。たとえば、ダウン状態から稼働状態に移行している EtherChannel の場合（スイッチがリロードされた、またはスイッチが有効になっている EtherChannel など）、デバウンス時間を長くすることで、他のクラスタ ユニットの方がポートのバンドルが速いという理由だけで、クラスタ ユニット上でインターフェイスがエラー表示されるのを防ぐことができます。 変更されたコマンドはありません。
内部障害発生後に自動的にクラスタに再参加する	9.9(2)	以前は、多くのエラー状態によりクラスタ ユニットがクラスタから削除されていました。この問題を解決した後、手動でクラスタに再参加する必要がありました。現在は、ユニットはデフォルトで 5 分、10 分、および 20 分の間隔でクラスタに自動的に再参加を試行します。これらの値は設定できます。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。 新規または変更されたコマンド：**health-check system auto-rejoin**、**show cluster info auto-join**
クラスタの信頼性の高いトランスポート プロトコル メッセージのトランスポートに関連する統計情報の表示	9.9(2)	ユニットごとのクラスタの信頼性の高いトランスポート バッファ使用率を確認して、バッファがコントロール プレーンでいっぱいになったときにパケット ドロップの問題を特定できるようになりました。 新規または変更されたコマンド：**show cluster info transport cp detail**

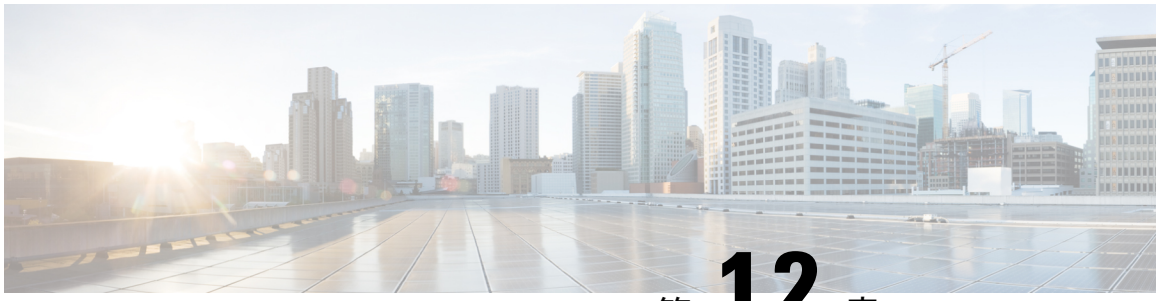
機能名	バージョン	機能情報
動作と一致する**cluster remove unit**コマンドの動作**no enable**	9.9(1)	**cluster remove unit** コマンドは、**no enable** コマンドと同様に、クラスタリングまたはリロードを手動で再度有効にするまで、クラスタからユニットを削除するようになりました。以前は、FXOS からブートストラップ設定を再展開すると、クラスタリングが再度有効になりました。無効化されたステータスは、ブートストラップ設定の再展開の場合でも維持されるようになりました。ただし、ASA をリロードすると、クラスタリングが再度有効になります。 新規または変更されたコマンド：cluster remove unit
シャーシのシャーシヘルスチェックの障害検出の向上	9.9(1)	シャーシヘルスチェックの保留時間をより低い値（100 ms）に設定できるようになりました。以前の最小値は 300 ms でした。最小の結合時間（*interval* x *retry-count*）は、600 ミリ秒未満にすることはできないことに注意してください。 新規または変更されたコマンド：**app-agent heartbeat interval**
クラスタリングのサイト間冗長性	9.9(1)	サイト間の冗長性により、トラフィック フローのバックアップ オーナーは常にオーナーとは別のサイトに置かれます。この機能によって、サイトの障害から保護されます。 新規または変更されたコマンド：**site-redundancy**、**show asp cluster counter change**、**show asp table cluster chash-table**、**show conn flag**
Firepower 9300 上のクラスタリングによる分散型サイト間 VPN	9.9(1)	Firepower 9300 上の ASA クラスタは、分散モードでサイト間 VPN をサポートします。分散モードでは、（集中モードなどの）制御ユニットだけでなく、ASA クラスタのメンバー間で多数のサイト間 IPsec IKEv2 VPN 接続を分散させることができます。これにより、集中型 VPN の機能を超えて VPN サポートが大幅に拡張され、高可用性が実現します。分散型 S2S VPN は、それぞれ最大 3 つのモジュールを含む最大 2 つのシャーシのクラスタ（合計 6 つのクラスタ メンバー）上で動作し、各モジュールは最大約 36,000 のアクティブ セッション（合計 72,000)に対し、最大 6,000 のアクティブ セッション（合計 12,000）をサポートします。 新規または変更されたコマンド：**cluster redistribute vpn-sessiondb**、**show cluster vpn-sessiondb**、**vpn mode**、**show cluster resource usage**、**show vpn-sessiondb**、**show connection detail**、**show crypto ikev2**

機能名	バージョン	機能情報
クラスタ ユニット ヘルスチェック障害検出の改善	9.8(1)	ユニット ヘルスチェックの保留時間をより低めの値に設定できます（最小値は .3 秒）以前の最小値は .8 秒でした。この機能は、ユニット ヘルス チェック メッセージング スキームを、コントロール プレーンのキープアライブからデータ プレーンのハートビートに変更します。ハートビートを使用すると、コントロールプレーン CPU のホッギングやスケジューリングの遅延の影響を受けないため、クラスタリングの信頼性と応答性が向上します。保留時間を短く設定すると、クラスタ制御リンクのメッセージング アクティビティが増加することに注意してください。保留時間を短く設定する前にネットワークを分析することをお勧めします。たとえば、ある保留時間間隔の間に 3 つのハートビート メッセージが存在するため、クラスタ制御リンクを介してあるユニットから別のユニットへの ping が保留時間/3 以内に戻ることを確認します。保留時間を 0.3 ～ 0.7 に設定した後に ASA ソフトウェアをダウングレードした場合、新しい設定がサポートされていないので、この設定はデフォルトの 3 秒に戻ります。 次のコマンドを変更しました。**health-check holdtime**、**show asp drop cluster counter**、**show cluster info health details**
に対してインターフェイスを障害としてマークするために設定可能なデバウンス時間 Firepower 4100/9300 シャーシ	9.8(1)	ASA がインターフェイスを障害が発生していると見なし、クラスタからユニットが削除されるまでのデバウンス時間を設定できるようになりました。この機能により、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからユニットを削除するまで指定されたミリ秒数待機します。デフォルトのデバウンス時間は 500 ms で、有効な値の範囲は 300 ms ～ 9 秒です。 新規または変更されたコマンド：**health-check monitor-interface debounce-time**
Firepower 4100/9300 シャーシ 上の ASA のサイト間クラスタリングの改良	9.7(1)	ASA クラスタを展開すると、それぞれの Firepower 4100/9300 シャーシのサイト ID を設定できます。以前は ASA アプリケーション内でサイト ID を設定する必要がありました。この新しい機能は、初期導入を簡単にします。ASA 構成内でサイト ID を設定できなくなったことに注意してください。また、サイト間クラスタリングとの互換性を高めるために、安定性とパフォーマンスに関する複数の改善が含まれる ASA 9.7(1) および FXOS 2.1.1 にアップグレードすることを推奨します。 次のコマンドが変更されました。**site-id**

機能名	バージョン	機能情報
ディレクタ ローカリゼーション：データセンターのサイト間クラスタリングの改善	9.7(1)	データ センターのパフォーマンスを向上し、サイト間クラスタリングのトラフィックを維持するために、ディレクタ ローカリゼーションを有効にできます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバル ディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。 次のコマンドが導入または変更されました。**director-localization**、**show asp table cluster chash**、**show conn**、**show conn detail**
の 16 個のシャーシのサポート Firepower 4100 シリーズ	9.6(2)	Firepower 4100 シリーズ では最大 16 個のシャーシをクラスタに追加できるようになりました。 変更されたコマンドはありません。
Firepower 4100 シリーズ のサポート	9.6(1)	FXOS 1.1.4 では、ASA は最大 6 個のシャーシの Firepower 4100 シリーズ でサイト間クラスタリングをサポートします。 変更されたコマンドはありません。
ルーテッドおよびスパンド EtherChannel モードのサイト固有の IP アドレスのポート	9.6(1)	スパンド EtherChannel のルーテッド モードでのサイト間クラスタリングの場合、サイト個別の MAC アドレスに加えて、サイト個別の IP アドレスを設定できるようになりました。サイト IP アドレスを追加することにより、グローバル MAC アドレスからの ARP 応答を防止するために、ルーティング問題の原因になりかねない Data Center Interconnect（DCI）経由の移動によるオーバーレイ トランスポート仮想化（OTV）デバイスの ARP 検査を使用することができます。MAC アドレスをフィルタ処理するために VACL を使用できないスイッチには、ARP 検査が必要です。 次のコマンドが変更されました。**mac-address**、**show interface**
16 のモジュールのシャーシ間クラスタリング、および Firepower 9300 ASA アプリケーションのサイト間クラスタリング	9.5(2.1)	FXOS 1.1.3 では、シャーシ間、さらにサイト間クラスタリングを有効にできます。最大 16 のモジュールを搭載することができます。たとえば、16 のシャーシで 1 つのモジュールを使用したり、8 つのシャーシで 2 つのモジュールを使用して、最大 16 のモジュールを組み合わせることができます。 変更されたコマンドはありません。

機能名	バージョン	機能情報
ルーテッド ファイアウォールモードのスパンド EtherChannel のサイト間クラスタリング サポートのサイト別 MAC アドレス	9.5(2)	ルーテッドモードでは、スパンド EtherChannel サイト間クラスタリングを使用することができます。MAC アドレスのフラッピングを防ぐには、各インターフェイスのサイト別の MAC アドレスがサイトのユニット上で共有できるように、各クラスタ メンバーのサイト ID を設定します。 次のコマンドを導入または変更しました。**site-id**、**mac-address site-id**、**show cluster info**、**show interface**
インターフェイスまたはクラスタ制御リンクが失敗した場合の auto-rejoin 動作の ASA クラスタのカスタマイズ	9.5(2)	インターフェイスまたはクラスタ制御リンクが失敗した場合、auto-rejoin 動作をカスタマイズできます。 次のコマンドを導入しました。 **health-check auto-rejoin**
ASA クラスタは、GTPv1 と GTPv2 をサポートします	9.5(2)	ASA クラスタは、GTPv1 および GTPv2 インスペクションをサポートします。 変更されたコマンドはありません。
TCP 接続のクラスタ複製遅延	9.5(2)	この機能で、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。 次のコマンドを導入しました。**cluster replication delay**
サイト間フローモビリティの LISP インスペクション	9.5(2)	Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID をその場所から 2 つの異なるナンバリング スペースに分離し、サーバーの移行をクライアントに対して透過的にします。ASA は、場所変更の LISP トラフィックを検査し、その情報をシームレスなクラスタリング運用に活用できます。ASA クラスタ メンバーは、最初のホップ ルータと出力トンネル ルータまたは入力トンネル ルータの間の LISP トラフィックを検査し、フロー オーナーの所在場所を新規サイトに変更します。 次のコマンドが導入または変更されました。**allowed-eid**、**clear cluster info flow-mobility counters**、**clear lisp eid**、**cluster flow-mobility lisp**、**debug cluster flow-mobility**、**debug lisp eid-notify-intercept**、**flow-mobility lisp**、**inspect lisp**、**policy-map type inspect lisp**、**site-id**、**show asp table classify domain inspect-lisp**、**show cluster info flow-mobility counters**、**show conn**、**show lisp eid**、**show service-policy**、**validate-key**
キャリア グレード NAT の強化がフェールオーバーおよび ASA クラスタリングでサポート	9.5(2)	キャリア グレードまたは大規模 PAT では、NAT に 1 度に 1 つのポート変換を割り当てさせるのではなく、各ホストにポートのブロックを割り当てることができます（RFC 6888 を参照してください）。この機能は、フェールオーバーおよび ASA クラスタの導入でサポートされます。 次のコマンドが変更されました。**show local-host**

機能名	バージョン	機能情報
クラスタリング トレース エントリの設定可能なレベル	9.5(2)	デフォルトで、すべてのレベル クラスタリング イベントは、多くの下位レベルのイベント以外に、トレース バッファに含まれます。より上位レベルのイベントへのトレースを制限するために、クラスタの最小トレース レベルを設定できます。 次のコマンドが導入されました。**trace-level**
Firepower 9300 用シャーシ内 ASA クラスタリング	9.4 (1.150)	FirePOWER 9300 シャーシ内では、最大 3 つのセキュリティ モジュールをクラスタ化できます。シャーシ内のすべてのモジュールは、クラスタに属している必要があります。 次のコマンドを導入しました。**cluster replication delay**、**debug service-module**、**management-only individual**、**show cluster chassis**



第 12 章

ASA クラスタのクラスタを展開する

クラスタリングを利用すると、複数の ASA 仮想 をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。以下を使用して ASA 仮想 クラスタを展開できます。

- KVM
- VMware

（注） ルーテッド ファイアウォール モードのみがサポートされます。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「クラスタリングでサポートされない機能 （697 ページ）」を参照してください。

- ASA 仮想クラスタリングについて （640 ページ）
- ASA 仮想クラスタリングのライセンス （647 ページ）
- ASA 仮想クラスタリングの要件と前提条件 （647 ページ）
- ASA 仮想クラスタリングに関するガイドライン （648 ページ）
- Day0 設定を使用した ASA 仮想 クラスタリングの設定 （649 ページ）
- 展開後のASA 仮想クラスタリングの設定 （652 ページ）
- クラスタリング動作のカスタマイズ （666 ページ）
- クラスタノードの管理 （679 ページ）
- ASA 仮想クラスタのモニタリング （684 ページ）
- ASA 仮想クラスタリングの例 （695 ページ）
- クラスタリングの参考資料 （696 ページ）
- ASA 仮想クラスタリングの履歴 （714 ページ）

ASA 仮想クラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのデバイスとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離されたネットワーク。VXLAN インターフェイスを使用したクラスタ制御リンクと呼ばれます。レイヤ 3 物理ネットワーク上でレイヤ 2 仮想ネットワークとして機能する VXLAN により、ASA Virtual はクラスタ制御リンクを介してブロードキャスト/マルチキャストメッセージを送信できます。
- 各ファイアウォールへの管理アクセス（コンフィギュレーションおよびモニタリングのため）。ASA Virtual 導入には、クラスタノードの管理に使用するManagement 0/0 インターフェイスが含まれています。

クラスタをネットワーク内に配置するときは、アップストリームおよびダウンストリームのルータは、レイヤ3の個別インターフェイスおよび次のいずれかの方法を使用して、クラスタとの間で送受信されるデータをロードバランシングできる必要があります。

- ポリシーベースルーティング：アップストリームとダウンストリームのルータが、ルートマップと ACL を使用してノード間のロードバランシングを実行します。
- 等コスト マルチパス ルーティング：アップストリームとダウンストリームのルータが、等コストのスタティックまたはダイナミック ルートを使用してノード間のロードバランシングを実行します。

（注） レイヤ 2 スパンド EtherChannels はサポートされません。

クラスタ ノード

クラスタノードは連携して動作し、セキュリティポリシーおよびトラフィックフローの共有を達成します。ここでは、各ノードのロールの特長について説明します。

ブートストラップ設定

各デバイスで、最小限のブートストラップ コンフィギュレーション（クラスタ名、クラスタ制御リンク インターフェイスなどのクラスタ設定）を設定します。通常、クラスタリングを有効にする最初のノードが制御ノードになります。以降のノードに対してクラスタリングをイネーブルにすると、そのノードはデータノードとしてクラスタに参加します。

制御ノードとデータノードの役割

クラスタ内のメンバーの1つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。一般的には、クラスタを作成した後で最初に追加したノードが制御ノードとなります。これは単に、その時点でクラスタに存在する唯一のノードであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ノード上のみで実行する必要があります。コンフィギュレーションは、データノードに複製されます。物理的アセット（たとえばインターフェイス）の場合は、制御ノードのコンフィギュレーションがすべてのデータノード上でミラーリングされます。たとえば、内部インターフェイスとしてイーサネット1/2を設定し、外部インターフェイスとしてイーサネット1/1を設定した場合、これらのインターフェイスは内部および外部インターフェイスとしてデータノードでも使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

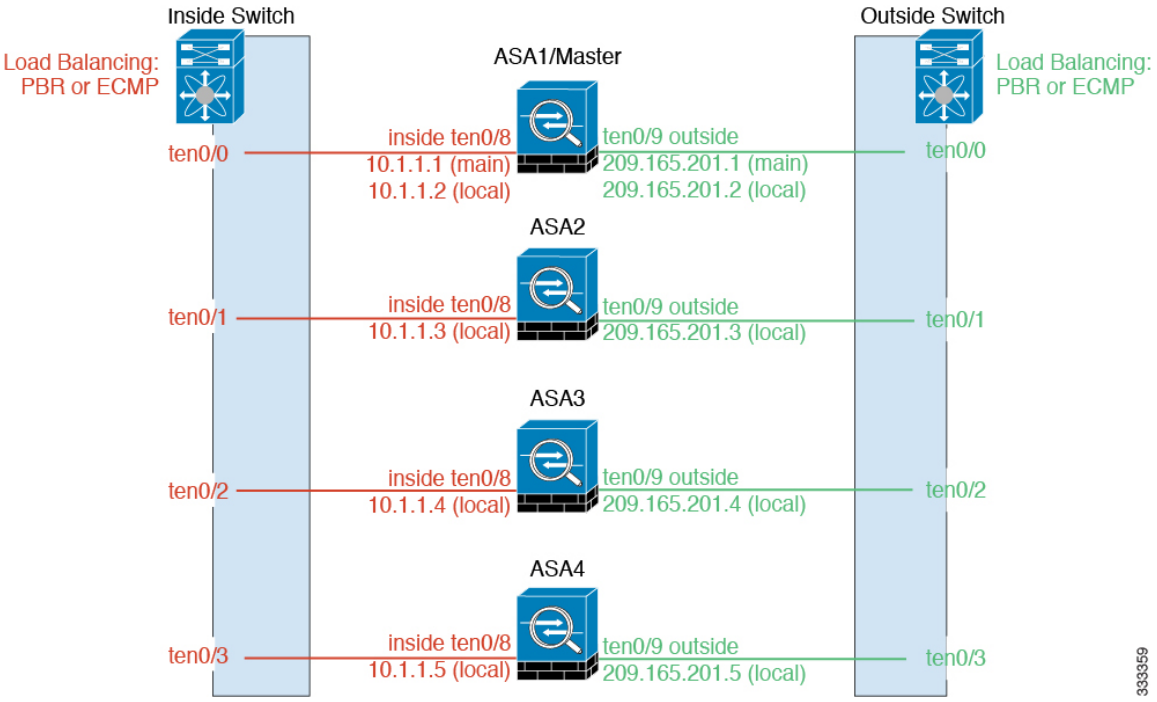
個々のインターフェイス

クラスターフェイスを個々のインターフェイスとして設定できます。

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のルーティング用ローカル *IP* アドレスを持ちます。各インターフェイスのメインクラスタ *IP* アドレスは、固定アドレスであり、常に制御ノードに属します。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。

インターフェイス コンフィギュレーションは制御ノード上だけで行う必要があるため、IP アドレスプールを設定して、このプールのアドレスがクラスタノード（制御ノード用を含む）の特定のインターフェイスに使用されるようにします。

アップストリームスイッチ上でロードバランシングを別途する必要があります。



（注） レイヤ 2 スパンド EtherChannels はサポートされません。

ポリシーベース ルーティング

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MAC アドレスを維持します。ロード バランシング方法の 1 つが、ポリシーベース ルーティング（PBR）です。

この方法が推奨されるのは、すでに PBR を使用しており、既存のインフラストラクチャを活用したい場合です。

PBR は、ルート マップおよび ACL に基づいて、ルーティングの決定を行います。管理者は、手動でトラフィックをクラスタ内のすべての ASA に分ける必要があります。PBR は静的であるため、常に最適なロードバランシング結果を実現できないこともあります。最高のパフォーマンスを達成するには、PBR ポリシーを設定するときに、同じ接続のフォワードとリターンのパケットが同じ ASA に送信されるように指定することを推奨します。たとえば、Cisco ルータがある場合は、冗長性を実現するには Cisco IOS PBR をオブジェクト トラッキングとともに使用します。Cisco IOS オブジェクト トラッキングは、ICMP ping を使用して各 ASA をモニタします。これで、PBR は、特定の ASA の到達可能性に基づいてルート マップを有効化または無効化できます。詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/data-center-virtualization/intelligent-traffic-director/index.html

http://www.cisco.com/en/US/products/ps6599/products_white_paper09186a00800a4409.shtml

等コスト マルチパス ルーティング

個別インターフェイスを使用するときは、各 ASA インターフェイスが専用の IP アドレスと MACアドレスを維持します。ロードバランシング方法の1つが、等コストマルチパス（ECMP）ルーティングです。

この方法が推奨されるのは、すでにECMPを使用しており、既存のインフラストラクチャを活用したい場合です。

ECMPルーティングでは、ルーティングメトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannelのように、送信元および宛先のIPアドレスや送信元および宛先のポートのハッシュを使用してネクストホップの1つにパケットを送信できます。ECMPルーティングにスタティックルートを使用する場合は、ASAの障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA を設定する必要があります。

クラスタ制御リンク

ノードごとに1つのインターフェイスをクラスタ制御リンク専用のVXLAN（VTEP）インターフェイスにする必要があります。VXLANの詳細については、VXLANインターフェイス（895ページ）を参照してください。

VXLAN トンネル エンドポイント

VXLANトンネルエンドポイント（VTEP）デバイスは、VXLANのカプセル化およびカプセル化解除を実行します。各VTEPには2つのインターフェイスタイプ（VXLAN Network Identifier（VNI）インターフェイスと呼ばれる1つ以上の仮想インターフェイスと、 VTEP間にVNIをトンネリングするVTEP送信元インターフェイスと呼ばれる通常のインターフェイス）がありますVTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

VTEP 送信元インターフェイス

VTEP送信元インターフェイスは、VNIインターフェイスに関連付けられる予定の標準の ASA Virtual インターフェイスです。1 つの VTEP ソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。各 VTEP ソースインターフェイスには、同じサブネット上の IP アドレスがあります。このサブネットは、他のすべてのトラフィックからは隔離し、クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持

する仮想インターフェイスです。設定できる VNI インターフェイスは 1 つだけです。各 VNI インターフェイスは、同じサブネット上の IP アドレスを持ちます。

ピア VTEP

単一の VTEP ピアを許可するデータインターフェイス用の通常の VXLAN とは異なり、ASA Virtual クラスタリングでは複数のピアを設定できます。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンクの障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャット ダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。

（注） ASA 仮想 が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットが DHCP またはクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。クラスタ IP プールを使用している場合、リロードしてもクラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（制御ノードと同じメイン IP アドレスを使用するため）。さらに設定を行う場合は、コンソールポート（使用可能な場合）を使用する必要があります。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

ASA 仮想 クラスタの管理

ASA 仮想 クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのノードを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理用に、管理 0/0 インターフェイスを使用します。

（注） 管理インターフェイスの動的ルーティングを有効にすることはできません。スタティック ルートを使用する必要があります。

管理 IP アドレスには、静的アドレスまたは DHCP を使用できます。

静的 IP アドレスを使用する場合は、常に現在の制御ノードに属するクラスタの固定アドレスであるメインクラスタ IP アドレスを使用できます。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ノード（現在の制御ノードも含まれます）がその範囲内のローカルアドレスを使用できるようになります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。ローカルIPアドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の制御ノードに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、制御ノードを含む各ノードは、ローカル IP アドレスを使用してサーバーに接続します。

DHCP を使用する場合、ローカルアドレスのプールを使用したり、メインクラスタの IP アドレスを使用したりしません。

（注） to-the-box トラフィックをノードの管理IPアドレスに転送する必要があります。to-the-box トラフィックは、クラスタ制御リンクを介して他のノードに転送されません。

制御ノードの管理対データノードの管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。また、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。
- ノードごとのSyslogモニタリング（コンソールレプリケーションが有効な場合にコンソールに送信される Syslog を除く）。
- SNMP
- NetFlow

暗号キー複製

制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメインクラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

サイト間クラスタリング

サイト間インストールの場合、次の推奨ガイドラインに従う限り、ASA仮想クラスタリングを利用できます。

各クラスタ シャーシを、個別のサイト ID に属するように設定できます。サイト ID は、LISP インスペクションを使用するフローモビリティ、データセンターのサイト間クラスタリングのパフォーマンスを向上し、ラウンドトリップ時間の遅延を減少させるためのディレクタ ローカリゼーション、およびトラフィックフローのバックアップオーナーが常にオーナーとは異なるサイトにある接続のサイト冗長性を有効にするために使用されます。

サイト間クラスタリングの詳細については、以下の項を参照してください。

- Data Center Interconnect のサイジング：ASA 仮想クラスタリングの要件と前提条件 （647 ページ）

- サイト間のガイドライン：ASA 仮想クラスタリングに関するガイドライン （648 ページ）
- クラスタ フロー モビリティの設定：クラスタ フロー モビリティの設定 （673 ページ）
- ディレクタ ローカリゼーションの有効化：ディレクタ ローカリゼーションの有効化 （672 ページ）
- サイト冗長性の有効化：ディレクタ ローカリゼーションの有効化 （672 ページ）
- サイト間での例：個別インターフェイス ルーテッド モード ノースサウス サイト間の例 （696 ページ）

ASA 仮想クラスタリングのライセンス

各クラスタノードには、同じモデルライセンスが必要です。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

（注） ASA 仮想 を登録解除してライセンスを解除した場合、ASA 仮想 をリロードすると、重大なレート制限状態に戻ります。ライセンスのない、パフォーマンスの低いクラスタノードは、クラスタ全体のパフォーマンスに悪影響を及ぼします。すべてのクラスタノードのライセンスを保持するか、ライセンスのないノードを削除してください。

ASA 仮想クラスタリングの要件と前提条件

モデルの要件

- ASAv30、ASAv50、ASAv100
- 次のプライベート クラウド サービス：
  - KVM
  - VMware
- 2x8 展開構成に含まれる「2 つ」のホスト上のクラスタ内で最大 16 ノード。2 つのホストのそれぞれに最大 8 つの ASAv を展開（2x8）することをお勧めします。これにより、16 ノードのクラスタになります。

ASA 仮想プラットフォームおよびソフトウェア要件

クラスタ内のすべてのノード：

- 同じモデルである必要があります。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のノードに一致するようにすべてのノードで制限されます。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレスアップグレードがサポートされます。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- コンフィギュレーション複製前の初期クラスタ制御リンク通信のために、新しいクラスタメンバーは、制御ノードと同じ SSL 暗号化設定（**ssl encryption** コマンド）を使用する必要があります。

ASA 仮想クラスタリングに関するガイドライン

フェールオーバー

フェールオーバーは、クラスタリングではサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（ASA 上でのインターフェイスまたはスイッチの有効化または無効化、VSS または vPC を形成するための追加スイッチの追加など）、ヘルスチェック機能を無効にし、無効化したインターフェイスのインターフェイスモニタリングも無効にする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、インターフェイス ヘルスチェック機能を再度有効にできます。
- ノードを既存のクラスタに追加したときや、ノードをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- データインターフェイスの VXLAN はサポートしていません。クラスタ制御リンクのみが VXLAN をサポートします。
- クラスタ内のすべてのノードに変更が複製されるまでには時間がかかります。たとえば、オブジェクトグループを使用するアクセスコントロールルール（展開時に複数のルールに分割される）を追加するなどの大きな変更を行うと、変更の完了に必要な時間がクラスタノードが成功メッセージで応答できるタイムアウトを超える可能性があります。この場合、「failed to replicate command」というメッセージが表示されることがあります。このメッセージは無視できます。

ASA 仮想クラスタリングのデフォルト

- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が5分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- 接続再分散は、デフォルトでは無効になっています。接続再分散を有効にした場合の、デフォルトの負荷情報交換間隔は 5 秒です。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

Day0 設定を使用した ASA 仮想 クラスタリングの設定

制御ノード Day0 設定

制御ノードの次の Day0 設定には、ブートストラップ設定と、それに続くデータノードに複製されるインターフェイス設定が含まれています。太字のテキストは、データノードの Day0 設定で変更する必要がある値を示しています。

（注） この設定には、クラスタ中心の設定のみが含まれます。Day0 設定には、ライセンス、SSH アクセス、ASDM アクセスなどの他の設定も含める必要があります。Day0 設定の詳細については、スタートアップガイドを参照してください。

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
```

```
security-level 0
ip address 10.6.6.51 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
local-unit A
cluster-interface vni1 ip 10.2.2.1 255.255.255.0
priority 1
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

データノード Day0 設定

データノードの次の Day0 設定には、ブートストラップ設定のみが含まれています。太字のテキストは、制御ノードの Day0 設定から変更する必要がある値を示しています。

（注） この設定には、クラスタ中心の設定のみが含まれます。Day0 設定には、ライセンス、SSH アクセス、ASDM アクセスなどの他の設定も含める必要があります。Day0 設定の詳細については、スタートアップガイドを参照してください。

```
!BOOTSTRAP
! Cluster interface mode
cluster interface mode individual
!
! VXLAN peer group
object-group network cluster-peers
network-object host 10.6.6.51
network-object host 10.6.6.52
network-object host 10.6.6.53
network-object host 10.6.6.54
!
! Alternate object group representation
! object-network xyz
! range 10.6.6.51 10.6.6.54
! object-group network cluster-peers
! network-object object xyz
!
! Cluster control link physical interface (VXLAN tunnel endpoint (VTEP) src interface)
interface gigabitethernet 0/7
description CCL VTEP src ifc
nve-only cluster
nameif ccl
security-level 0
ip address 10.6.6.52 255.255.255.0
no shutdown
!
! VXLAN Network Identifier (VNI) interface
interface vni1
segment-id 1
vtep-nve 1
!
! Set the CCL MTU
mtu ccl 1654
!
! Network Virtualization Endpoint (NVE) association with VTEP src interface
nve 1
encapsulation vxlan
source-interface ccl
peer-group cluster-peers
!
! Management Interface Using DHCP
interface management 0/0
nameif management
ip address dhcp setroute
no shutdown
!
! Alternate Management Using Static IP
! ip local pool mgmt_pool 10.1.1.1 10.10.10.4
! interface management 0/0
! nameif management
! ip address 10.1.1.25 255.255.255.0 cluster-pool mgmt_pool
! no shutdown
!
! Cluster Config
cluster group cluster1
```

```
local-unit B
cluster-interface vni1 ip 10.2.2.2 255.255.255.0
priority 2
enable noconfirm
!
! INTERFACES
!
ip local pool inside_pool 10.10.10.11 10.10.10.14
ip local pool outside_pool 10.11.11.11 10.11.11.14
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 10.10.10.10 255.255.255.0 cluster-pool inside_pool
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address 10.11.11.10 255.255.255.0 cluster-pool outside_pool
!
!JUMBO FRAME RESERVATION for CCL MTU
jumbo-frame reservation
```

展開後のASA 仮想クラスタリングの設定

ASA 仮想 の展開後にクラスタリングを設定するには、次のタスクを実行します。

インターフェイスの設定

各ノードのクラスタ インターフェイス モードと、制御ノードのインターフェイスを設定します。インターフェイス構成は、クラスタに参加するときにデータノードに複製されます。クラスタ制御リンクの構成は、ブートストラップ コンフィギュレーション手順で説明されていることに注意してください。

各ノードのでクラスタ インターフェイス モードを設定する

クラスタリングを有効にする前に、個々のインターフェイスを使用するようにファイアウォールを変換する必要があります。クラスタリングによって使用できるインターフェイスの種類が制限されるため、このプロセスでは、既存の設定に互換性のないインターフェイスがあるかどうかを確認し、サポートされていないインターフェイスを設定できないようにします。

始める前に

- モードの設定は、クラスタに追加する各 ASA 仮想 で個別に行う必要があります。
- コンソールポート（使用可能な場合）またはSSH（設定されている場合）のいずれかを使用して、ASA 仮想 CLI に接続します。これらのオプションのいずれも使用できない場合は、ASDM を使用してクラスタリングを設定できます。

手順

ステップ 1 互換性のないコンフィギュレーションを表示し、強制的にインターフェイスモードにして後でコンフィギュレーションを修正できるようにします。このコマンドではモードは変更されません。

cluster interface-mode individual check-details

例：

```
ciscoasa(config)# cluster interface-mode individual check-details
```

注意
インターフェイス モードを設定した後は、SSH を使用して常にインターフェイスに接続できるようになります。ただし、クラスタリング要件に適合するように管理インターフェイスを設定する前に ASA をリロードすると（たとえば、クラスタ IP プールを追加するため、または DHCP から IP アドレスを取得するため）、クラスタと互換性のないインターフェイス コンフィギュレーションが削除されるため、再接続できなくなります。その場合は、可能であればコンソールポートに接続してインターフェイス コンフィギュレーションを修正する必要があります。

ステップ 2 クラスタリング用にインターフェイス モードを設定します。

cluster interface-mode individual force

例：

```
ciscoasa(config)# cluster interface-mode individual force
```

デフォルト設定はありません。明示的にモードを選択する必要があります。モードを設定していない場合は、クラスタリングをイネーブルにできません。

force オプションを指定すると、互換性のないコンフィギュレーションの検査は行わずにモードが変更されます。コンフィギュレーションの問題がある場合は、モードを変更した後に手動で解決する必要があります。インターフェイス コンフィギュレーションの修正ができるのはモードの設定後に限られるので、**force** オプションを使用することを推奨します。このようにすれば、最低でも、既存のコンフィギュレーションの状態から開始できます。さらにガイダンスが必要な場合は、モードを設定した後で **check-details** オプションを再実行します。

force オプションを指定しないと、互換性のないコンフィギュレーションがある場合は、コンフィギュレーションをクリアしてリロードするように求められるので、コンソールポート（可能な場合）に接続して管理アクセスを再設定する必要があります。コンフィギュレーションに互換性の問題がない場合は（まれなケース）、モードが変更され、コンフィギュレーションは維持されます。コンフィギュレーションをクリアしたくない場合は、**n** を入力してコマンドを終了します。

インターフェイス モードを解除するには、**no cluster interface-mode** コマンドを入力します。

個々のインターフェイスの設定

クラスタリングを有効にする前に、現在 IP アドレスが設定されているインターフェイスをクラスタ対応に変更する必要があります。管理に静的 IP アドレスを使用する場合は、少なくとも、SSH が現在接続されている管理インターフェイスを変更する必要がある場合があります。他のインターフェイスについては、クラスタリングを有効化する前またはその後に設定できます。完全なコンフィギュレーションが新しいクラスタノードと同期するように、すべてのインターフェイスを事前に設定することを推奨します。

ここでは、個々のインターフェイスがクラスタリング互換となるようにインターフェイスを設定する方法について説明します。個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用の IP アドレスを IP アドレス プールから取得します。メインクラスタ IP アドレスは、そのクラスタのための固定アドレスであり、常に現在の制御ノードに属します。すべてのデータインターフェイスは個別インターフェイスである必要があります。

管理インターフェイスでは、IP アドレスプールを設定するか、DHCP を使用できます。管理インターフェイスのみが DHCP からのアドレスの取得をサポートしています。DHCP を使用する場合は、この手順を使用しないでください。代わりに、通常どおりに設定します（ルーテッドモードの一般的なインターフェイス パラメータの設定 （933 ページ）を参照）。

始める前に

- （オプション）サブインターフェイスを設定します。
- 管理インターフェイスには、静的アドレスを使用するか、DHCP を使用できます。静的 IP アドレスを使用しており、SSH を使用して管理インターフェイスにリモートに接続している場合は、将来のデータノードの現在の IP アドレスは一時的なものです。
  - 各メンバには、制御ノードで定義されたクラスタ IP プールから IP アドレスが割り当てられます。
  - クラスタ IP プールには、将来のセカンダリ IP アドレスを含む、ネットワークですでに使用中のアドレスを含めることはできません。

    次に例を示します。

    1. 制御ノードに 10.1.1.1 を設定します。
    2. 他のノードには、10.1.1.2、10.1.1.3、10.1.1.4 を使用します。
    3. 制御ノードのクラスタの IP プールを設定する場合、使用中であるために .2、.3、.4 のアドレスをプールに含めることはできません。
    4. 代わりに、.5、.6、.7、.8 のような、ネットワークの他の IP アドレスを使用する必要があります。

（注） プールには、制御ノードを含むクラスタのメンバ数分のアドレスが必要です。元の .1 アドレスはメインクラスタ IP アドレスであり、現在の制御ノードのものです。

5. クラスタに参加すると古い一時的なアドレスは放棄され、他の場所で使用できます。

手順

ステップ 1 ローカル IP アドレス（IPv4 と IPv6 の一方または両方）のプールを設定します。このアドレスの 1 つが、このインターフェイス用に各クラスタノードに割り当てられます。

（IPv4）

ip local pool *poolname first-address — last-address* [**mask** *mask*]

（IPv6）

ipv6 local pool *poolname ipv6-address*/*prefix-length number_of_addresses*

例：

```
ciscoasa(config)# ip local pool ins 192.168.1.2-192.168.1.9
ciscoasa(config-if)# ipv6 local pool insipv6 2001:DB8:45:1003/64 8
```

少なくともクラスタ内のノードと同じ数のアドレスを含めます。クラスタを拡張する予定の場合は、アドレスを増やします。現在の制御ノードに属するメインクラスタ IP アドレスは、このプールの一部ではありません。必ず、同じネットワークの IP アドレスの 1 つをメインクラスタ IP アドレス用に確保してください。

各ノードに割り当てられるローカルアドレスを、事前に正確に特定することはできません。各ノードで使用されているアドレスを表示するには、**show ip**[**v6**] **local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。

ステップ 2 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface gigabitethernet 0/1
```

ステップ 3 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。

ステップ 4 メイン クラスタの IP アドレスを設定し、クラスタ プールを指定します。

（IPv4）

ip address *ip_address* [*mask*] **cluster-pool** *poolname*

（IPv6）

ipv6 address *ipv6-address*/*prefix-length* **cluster-pool** *poolname*

例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ciscoasa(config-if)# ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
```

この IP アドレスは、クラスタ プール アドレスと同じネットワーク上に存在している必要がありますが、プールに含まれていてはなりません。IPv4 アドレスと IPv6 アドレスの一方または両方を設定できます。

DHCP、PPPoE、および IPv6 自動設定はサポートされません。IP アドレスを手動で設定する必要があります。リンクローカルアドレスの手動設定もサポートされていません。

ステップ 5 セキュリティ レベルを設定します。*number* には、0（最低）～ 100（最高）の整数を指定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

ステップ 6 インターフェイスをイネーブルにします。

no shutdown

例

次の例では、管理 0/0、GigabitEthernet 0/0、および GigabitEthernet 0/1 インターフェイスを個別のインターフェイスとして設定します。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
nameif management
ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
```

```
ipv6 address 2001:DB8:45:1001::99/64 cluster-pool mgmtipv6
security-level 100
no shutdown

ip local pool out 209.165.200.225-209.165.200.232
ipv6 local pool outipv6 2001:DB8:45:1002/64 8

interface gigabitethernet 0/0
nameif outside
ip address 209.165.200.233 255.255.255.224 cluster-pool out
ipv6 address 2001:DB8:45:1002::99/64 cluster-pool outipv6
security-level 0
no shutdown

ip local pool ins 192.168.1.2-192.168.1.9
ipv6 local pool insipv6 2001:DB8:45:1003/64 8

interface gigabitethernet 0/1
nameif inside
ip address 192.168.1.1 255.255.255.0 cluster-pool ins
ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
security-level 100
no shutdown
```

ブートストラップ コンフィギュレーションの作成

クラスタ内の各ノードがクラスタに参加するには、ブートストラップ設定が必要です。

制御ノードのブートストラップの設定

クラスタ内の各ノードがクラスタに参加するには、ブートストラップ設定が必要です。一般的には、クラスタに参加するように最初に設定したノードが制御ノードとなります。クラスタリングをイネーブルにした後で、選定期間が経過すると、クラスタの制御ノードが選定されます。最初はクラスタ内に1つのノードしかないため、そのノードが制御ノードになります。クラスタに追加する後続のノードはデータノードになります。

始める前に

- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。
- クラスタ制御リンクと管理インターフェイス（オプションでDHCPを使用可能）を除いて、コンフィギュレーション内のインターフェイスはすべて、クラスタ IP プールを指定して設定されている必要があります。この設定は、クラスタリングを有効化する前に行います。既存のインターフェイス コンフィギュレーションがある場合は、そのインターフェイス コンフィギュレーションをクリアすることも（**clear configure interface**）、インターフェイスをクラスタインターフェイスに変換することもできます。これは、クラスタリングをイネーブルにする前に行います。
- 稼働中のクラスタにノードを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがありますが、これは想定内の動作です。

- クラスタ制御リンクで使用するジャンボフレーム予約を有効にして、クラスタ制御リンクの MTU を推奨値に設定できるようにします。**jumbo-frame reservation** コマンドを参照してください。ジャンボフレームを有効にすると ASA がリロードされるため、この手順を進める前に実行しておく必要があります。

手順

ステップ 1 クラスタに参加する前に、クラスタ制御リンクインターフェイスの VXLAN インターフェイスを設定します。

後でクラスタリングを有効化するときに、このインターフェイスをクラスタ制御リンクとして識別します。

クラスタ制御リンク インターフェイス コンフィギュレーションは、制御ノードからデータ ノードには複製されませんが、同じコンフィギュレーションを各ノードで使用する必要があります。このコンフィギュレーションは複製されないため、クラスタ制御リンクインターフェイスの設定は各ノードで個別に行う必要があります。

a) ネットワーク オブジェクト グループを作成して、VTEP ピアの IP アドレスを識別します。

ネットワーク オブジェクト グループの詳細については、ASA ファイアウォール コンフィギュレーション ガイドの「Objects for Access Control」の章を参照してください。

VTEP 間の基礎となる IP ネットワークは、VNI インターフェイスが使用するクラスタ制御リンクネットワークから独立しています。各 VTEP ソースインターフェイスには、同じサブネット上の IP アドレスがあります。このサブネットは、他のすべてのトラフィックからは隔離し、 クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

例：

次に、インラインで定義されたホストを含むネットワーク オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

次の例では、スタンドアロン ネットワーク オブジェクトを参照するネットワーク オブジェクト グループを作成します。

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54

ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

b) VTEP 送信元インターフェイスを設定します。

interface *interface_id*

nve-only cluster

nameif *name*

ip address *ip_address subnet_mask*

no shutdown

IP アドレスは、ネットワーク オブジェクト グループのピアの 1 つとして含める必要があります。

例：

```
ciscoasa(config)# interface gigabitethernet 0/7
ciscoasa(config-if)# nve-only cluster
ciscoasa(config-if)# nameif ccl
ciscoasa(config-if)# ip address 10.6.6.51 255.255.255.0
ciscoasa(config-if)# no shutdown
```

c) VTEP ソースインターフェイスを NVE インスタンスに関連付けます。

nve 1

source-interface *interface-name*

peer-group *network_object_name*

ID 1 で NVE インスタンスを 1 つだけ指定できます。

encapsulation vxlan コマンドが NVE インスタンスのデフォルトにより追加されます。明示的に追加する必要はありません。

例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface ccl
ciscoasa(cfg-nve)# peer-group cluster-peers
```

d) VTEP ソースインターフェイスの最大伝送ユニットを指定します。データインターフェイスの最大 MTU より少なくとも 154 バイト高い値を指定します。

mtu *interface_name bytes*

クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッド（100 バイト）および VXLAN のオーバーヘッド（54 バイト）にも対応する必要があります。MTU は 1,554 ～ 9,198 バイトの間で設定しますが、その範囲内でも 2,561 ～ 8,362 の間には設定しないでください。ブロック プールの処理により、この MTU サイズはシステム動作に最適ではありません。デフォルトの MTU は 1554 バイトです。データインターフェイスが 1500 に設定されている場合は、クラスタ制御リンクの MTU を 1654 に設定することをお勧めします。この値にはジャンボ フレームの予約が必要です（**jumbo-frame reservation** コマンドを参照）。

たとえばジャンボ フレームを使用している場合、最大 MTU は 9198 バイトであるため、データインターフェイスの最大 MTU は 9044 になり、クラスタ制御リンクは 9198 に設定できます。

このコマンドはデータノードに複製されますが、ブートストラップ設定とともにこの設定を設定することをお勧めします。

クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。

例：

```
ciscoasa(config)# mtu ccl 1654
```

e) （任意） VXLAN UDP ポートを設定します。

vxlan *port number*

デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。ネットワークで標準以外のポートを使用する場合は、それを変更できます。

例：

```
ciscoasa(config)# vxlan port 5678
```

f) VNI インターフェイスを作成します。

interface vni *vni_num*

segment-id *id*

vtep-nve 1

例：

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
```

- 1 ～ 10000 の範囲で VNI 番号を設定します。この ID は内部インターフェイス識別子です。
- 1 ～ 16777215 の範囲でセグメント ID を設定します。セグメント ID は VXLAN タギングに使用されます。

インターフェイスの名前などのパラメータを設定しないでください。

ステップ 2 クラスタに名前を付け、クラスタ コンフィギュレーション モードにします。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

名前は 1 ～ 38 文字の ASCII 文字列であることが必要です。ノードごとに設定できるクラスタグループは1つだけです。クラスタのすべてのメンバが同じ名前を使用する必要があります。

ステップ 3 クラスタのこのメンバの名前を指定します。

local-unit *node_name*

1 ～ 38 文字の一意の ASCII 文字列を使用します。各ノードには一意の名前が必要です。クラスタ内の他のノードと同じ名前を付けることはできません。

例：

```
ciscoasa(cfg-cluster)# local-unit node1
```

ステップ 4 クラスタ制御リンク VNI インターフェイスを指定します。

cluster-interface *vni_interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface vni1 ip 192.168.1.1 255.255.255.0
INFO: Non-cluster interface config is cleared on VNI1
```

IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。ノードごとに、同じネットワーク上の異なる IP アドレスを指定します。VNI ネットワークは、物理 VTEP ネットワーク上で稼働する暗号化された仮想ネットワークです。

ステップ 5 制御ノードの選択に対するこのノードのプライオリティを設定します。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 1
```

プライオリティは 1 ～ 100 であり、1 が最高のプライオリティです。

ステップ 6 （オプション）クラスタ制御リンクの制御トラフィックの認証キーを設定します。

key *shared_secret*

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

共有秘密は、1 ～ 63 文字の ASCII 文字列です。共有秘密は、キーを生成するために使用されます。このコマンドは、データパストラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

ステップ 7 クラスタリングをイネーブルにします。

enable [**noconfirm**]

例：

```
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
 Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

enable コマンドが入力されると、ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルト コンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するように求められます。応答として **No** を入力した場合は、クラスタリングはイネーブルになりません。確認を省略し、互換性のないコマンドを自動的に削除するには、**noconfirm** キーワードを使用します。

最初にイネーブルにしたノードについては、制御ノード選定が発生します。これまでは最初のノードがクラスタの唯一のメンバーである必要があるため、これが制御ノードになります。この期間中にコンフィギュレーション変更を実行しないでください。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注）
クラスタリングをディセーブルにした場合は、すべてのデータインターフェイスがシャットダウンされ、管理インターフェイスだけがアクティブになります。

例

次の例では、管理インターフェイス、内部インターフェイス、外部インターフェイス、およびVXLANクラスタ制御リンクを設定し、その後で、「node1」という名前のASAのクラスタリングを有効化します。これは最初にクラスタに追加されるノードであるため、制御ノードになります。

```
ip local pool mgmt 10.1.1.2-10.1.1.9
ipv6 local pool mgmtipv6 2001:DB8:45:1002/64 8

interface management 0/0
    nameif management
    ip address 10.1.1.1 255.255.255.0 cluster-pool mgmt
    ipv6 address 2001:DB8:45:1001::99/64 cluster-pool mgmtipv6
    security-level 100
```

```
    no shutdown

ip local pool out 209.165.200.225-209.165.200.232
ipv6 local pool outipv6 2001:DB8:45:1002/64 8

interface gigabitethernet 0/0
    nameif outside
    ip address 209.165.200.233 255.255.255.224 cluster-pool out
    ipv6 address 2001:DB8:45:1002::99/64 cluster-pool outipv6
    security-level 0
    no shutdown

ip local pool ins 192.168.1.2-192.168.1.9
ipv6 local pool insipv6 2001:DB8:45:1003/64 8

interface gigabitethernet 0/1
    nameif inside
    ip address 192.168.1.1 255.255.255.0 cluster-pool ins
    ipv6 address 2001:DB8:45:1003::99/64 cluster-pool insipv6
    security-level 100
    no shutdown

object-group network cluster-peers
    network-object host 10.6.6.51
    network-object host 10.6.6.52
    network-object host 10.6.6.53
    network-object host 10.6.6.54

interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

mtu ccl 1654

interface vni 1
    segment-id 1000
    vtep-nve 1

cluster group pod1
    local-unit node1
    cluster-interface vni1 ip 192.168.1.1 255.255.255.0
    priority 1
    key 67impala
    enable noconfirm
```

データノードのブートストラップの設定

データノードを設定するには、次の手順に従います。

始める前に

- コンフィギュレーションをバックアップします。後でクラスタから脱退する必要が生じたときに備えて、コンフィギュレーションを復元できるようにしておくためです。

- クラスタ制御リンクと管理インターフェイス（オプションでDHCPを使用可能）を除いて、コンフィギュレーション内のインターフェイスはすべて、クラスタ IP プールを指定して設定されている必要があります。この設定は、クラスタリングを有効化する前に行います。既存のインターフェイス コンフィギュレーションがある場合は、そのインターフェイス コンフィギュレーションをクリアすることも（**clear configure interface**）、インターフェイスをクラスタ インターフェイスに変換することもできます。これは、クラスタリングをイネーブルにする前に行います。
- 稼働中のクラスタにノードを追加すると、一時的に、限定的なパケット/接続ドロップが発生することがありますが、これは想定内の動作です。
- クラスタ制御リンクで使用するジャンボフレーム予約を有効にして、クラスタ制御リンクの MTU を推奨値に設定できるようにします。**jumbo-frame reservation** コマンドを参照してください。ジャンボフレームを有効にすると ASA がリロードされるため、この手順を進める前に実行しておく必要があります。

手順

ステップ 1 制御ノードに設定したものと同じクラスタ制御リンクインターフェイスを設定します。VTEP ソースインターフェイスに別の IP アドレスを指定してください（**太字**で表示）。

例：

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
ciscoasa(config)# interface gigabitethernet 0/7
ciscoasa(config-if)# nve-only cluster
ciscoasa(config-if)# nameif ccl
ciscoasa(config-if)# ip address 10.6.6.52 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface ccl
ciscoasa(cfg-nve)# peer-group cluster-peers
ciscoasa(config)# mtu ccl 1654
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
```

ステップ 2 制御ノードに設定したものと同じクラスタ名を指定します。

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 3 クラスタのこのメンバに一意の文字列で名前を指定します。

local-unit *node_name*

例：

```
ciscoasa(cfg-cluster)# local-unit node2
```

1 ～ 38 文字の ASCII 文字列を指定します。

各ノードには一意の名前が必要です。クラスタ内の他のノードと同じ名前を付けることはできません。

ステップ 4 制御ノードに設定したものと同じクラスタ制御リンクインターフェイスを指定しますが、ノードごとに同じネットワーク上の異なる IP アドレスを指定します。

cluster-interface *vni_interface_id* **ip** *ip_address mask*

例：

```
ciscoasa(cfg-cluster)# cluster-interface vni1 ip 192.168.1.2 255.255.255.0
INFO: Non-cluster interface config is cleared on VNI1
```

IP アドレスには IPv4 アドレスを指定します。IPv6 は、このインターフェイスではサポートされません。このインターフェイスには、**nameif** を設定することはできません。

ステップ 5 サイト間クラスタリングを使用している場合、このノードのサイト ID を設定し、サイト固有の MAC アドレスが使用されるようにします。

site-id *number*

例：

```
ciscoasa(cfg-cluster)# site-id 2
```

number は 1 ～ 8 です。

ステップ 6 制御ノードの選定に対するこのノードのプライオリティを設定します。通常は、制御ノードより高い値にします。

priority *priority_number*

例：

```
ciscoasa(cfg-cluster)# priority 2
```

プライオリティを 1 ～ 100 に設定します。1 が最高のプライオリティです。

ステップ 7 制御ノードに設定したものと同じ認証キーを設定します。

例：

```
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

ステップ 8 クラスタリングをイネーブルにします。

enable as-data-node

enable as-data-node コマンドを使用することによって、設定に関するすべての非互換性（主にまだクラスタリング用に設定されていないインターフェイスの存在）を回避できます。このコマンドを実行すると、クラスタに参加させるデータノードが現在の選定において制御ノードとなる可能性をなくすことができます。データノードのコンフィギュレーションは、制御ノードから同期されたコンフィギュレーションによって上書きされます。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注）
クラスタリングをディセーブルにした場合は、すべてのデータインターフェイスがシャットダウンされ、管理インターフェイスだけがアクティブになります。

例

次の例には、データノード node2 の設定が含まれています。

```
object-group network cluster-peers
    network-object host 10.6.6.51
    network-object host 10.6.6.52
    network-object host 10.6.6.53
    network-object host 10.6.6.54

interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.52 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

mtu ccl 1654

interface vni 1
    segment-id 1000
    vtep-nve 1

cluster group pod1
    local-unit node2
    cluster-interface vni1 ip 192.168.1.2 255.255.255.0
    priority 2
    key 67impala
    enable noconfirm
```

クラスタリング動作のカスタマイズ

Day 0 設定の一環として、またはクラスタの展開後に、クラスタリング ヘルス モニタリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

制御ノードで次の手順を実行します。

ASA クラスタの基本パラメータの設定

制御ノード上のクラスタ設定をカスタマイズできます。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （任意） データノードから制御ノードへのコンソール複製を有効にします。

console-replicate

この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート 1 つだけです。

ステップ 3 クラスタリング イベントの最小トレース レベルを設定します。

trace-level *level*

必要に応じて最小レベルを設定します。

- **critical**：クリティカル イベント（重大度 = 1）
- **warning**：警告（重大度 = 2）
- **informational**：情報イベント（重大度 = 3）
- **debug**：デバッグ イベント（重大度 = 4）

ステップ 4 フローオーナーからディレクタおよびバックアップオーナーへのフロー状態更新メッセージ（clu_keepalive および clu_update メッセージ）のキープアライブ間隔を設定します。

clu-keepalive-interval *seconds*

- *seconds*：15 ～ 55。デフォルトは 15 です。

クラスタ制御リンクのトラフィック量を減らすために、デフォルトよりも長い間隔を設定することもできます。

ヘルスモニタリングおよび自動再参加設定の設定

この手順では、ノードとインターフェイスのヘルスモニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ヘルスモニタリングはVLANサブインターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

手順

ステップ1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

ステップ2 クラスタノードのヘルスチェック機能をカスタマイズします。

health-check [**holdtime** *timeout*]

ノードのヘルスを確認するため、ASAのクラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。

- **holdtime** *timeout*：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は .3 ～ 45 秒で、デフォルトは 3 秒です。

何らかのトポロジ変更を行うとき（たとえば、データインターフェイスの追加または削除、ASAまたはスイッチ上のインターフェイスの有効化または無効化）は、ヘルスチェック機能を無効にし、無効化したインターフェイスのインターフェイスモニタリングも無効にする必要があります（**no health-check monitor-interface**）。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ3 インターフェイスでインターフェイス ヘルス チェックを無効化します。

no health-check monitor-interface *interface_id*

インターフェイスのヘルス チェックはリンク障害をモニターします。ASA がメンバーをクラスタから削除するまでの時間は、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルスチェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブル（無効）にすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。

- *interface_id*：インターフェイスの監視を無効にします。ヘルスモニタリングはVLANサブインターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

何らかのトポロジ変更を行うとき（たとえば、データインターフェイスの追加または削除、ASAまたはスイッチ上のインターフェイスの有効化または無効化）は、ヘルスチェック機能を無効（**no health-check**）にし、無効化したインターフェイスのインターフェイスモニタリングも無効にする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

ステップ 4 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**：内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
- **unlimited**：（**cluster-interface** のデフォルト）再結合の試行回数を制限しません。
- *auto-rejoin-max*：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。**data-interface** と **system** のデフォルトは 3 です。
- *auto_rejoin_interval*：再結合試行の間隔を 2 ～ 60 の範囲の分単位で定義します。デフォルト値は5分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- *auto_rejoin_interval_variation*：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の2倍、**3**：直前の間隔の3倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタインターフェイスの場合は**1**、データインターフェイスおよびシステムの場合は**2**です。

例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

ステップ 5 ASAがインターフェイスを障害が発生していると見なし、クラスタからノードが削除されるまでのデバウンス時間を設定します。

health-check monitor-interface debounce-time *ms*

例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

デバウンス時間は 300 ～ 9000 ms の範囲の値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASA はインターフェイスを障害としてマークし、クラスタからノードを削除するまで指定されたミリ秒数待機します。

ステップ 6 （任意）トラフィック負荷のモニタリングを設定します。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds*：モニタリングメッセージ間の時間を、10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。
- **intervals** *intervals*： ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

クラスタメンバのトラフィック負荷をモニターできます。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのノードが負荷を処理できる場合は、ノードのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ノードでクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

例

次の例では、ヘルスチェック保留時間を .3 秒に設定し、管理 0/0 インターフェイスのモニタリングを無効にし、データインターフェイスの自動再結合の試行回数を 2 分から開始して前回の間隔の 3 倍増加させる計 4 回に設定し、クラスタ制御リンクの自動再結合の試行回数を 2 分おきの計 6 回に設定しています。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
```

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

接続リバランスおよびクラスタ TCP 複製遅延の設定

接続の再分散を設定できます。アップストリームまたはダウンストリームルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しい TCP フローを過負荷のノードから他のノードにリダイレクトするように設定できます。既存のフローは他のノードには移動されません。

TCP 接続のクラスタ複製の遅延を有効化して、ディレクタ/バックアップ フロー作成の遅延による存続期間が短いフローに関連する「不要な作業」を排除できます。ディレクタ/バックアップフローが作成される前にノードが失敗する場合は、それらのフローを回復することはできません。同様に、フローを作成する前にトラフィックが別のノードに再調整される場合、流れを回復することはできません。TCP のランダム化を無効化するトラフィックの TCP の複製の遅延を有効化しないようにする必要があります。

手順

ステップ 1 TCP 接続のクラスタ複製の遅延を有効化します。

cluster replication delay *seconds* { **http | match tcp {host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*] { **host** *ip_address* | *ip_address mask* | **any | any4 | any6} [{eq | lt | gt}** *port*]}

例：

```
ciscoasa(config)# cluster replication delay 15 match tcp any any eq ftp
ciscoasa(config)# cluster replication delay 15 http
```

1 ～ 15 の範囲で秒数を設定します。**http** 遅延はデフォルトで 5 秒間有効になります。

ステップ 2 クラスタの設定モードを開始します。

cluster group *name*

ステップ 3 （オプション）TCP トラフィックの接続の再分散を有効化します。

conn-rebalance [**frequency** *seconds*]

例：

```
ciscoasa(cfg-cluster)# conn-rebalance frequency 60
```

このコマンドは、デフォルトでディセーブルになっています。有効化されている場合、ASA は、1 秒あたりの接続数に関する情報を定期的に交換し、新しい接続を、1 秒あたりの接続数が多いデバイスから低負荷のデバイスにオフロードします。既存の接続は移動されません。さらに、このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立さ

れた接続の総数は考慮されず、接続の総数は等しくない場合があります。負荷情報を交換する間隔を、1 ～ 360 秒の範囲内で指定します。デフォルトは 5 秒です。

接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタメンバには接続を再分散できません。

サイト間機能の設定

サイト間クラスタリングの場合、冗長性と安定性を高めるために、設定をカスタマイズできます。

ディレクタ ローカリゼーションの有効化

データセンターのサイト間クラスタリングのパフォーマンスを向上させ、ラウンドトリップ時間を短縮するために、ディレクターローカリゼーションをイネーブルにすることができます。通常、新しい接続は特定のサイト内のクラスタ メンバーによってロード バランスされ、所有されています。しかし、ASA は任意のサイトのメンバーにディレクタ ロールを割り当てます。ディレクタ ローカリゼーションにより、所有者と同じサイトのローカル ディレクタ、どのサイトにも存在可能なグローバルディレクタという追加のディレクタ ロールが有効になります。所有者とディレクタが同一サイトに存在すると、パフォーマンスが向上します。また、元の所有者が失敗した場合、ローカルなディレクタは同じサイトで新しい接続の所有者を選択します。グローバルなディレクタは、クラスタ メンバーが別のサイトで所有される接続のパケットを受信する場合に使用されます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。
- 次のトラフィック タイプは、ローカリゼーションをサポートしていません：NAT および PAT トラフィック、SCTP 検査されたトラフィック、フラグメンテーション所有クエリ。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 ディレクタ ローカリゼーションをイネーブルにします。

director-localization

サイト冗長性の有効化

サイトの障害からフローを保護するために、サイトの冗長性を有効にできます。接続バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。

始める前に

- ブートストラップ設定でクラスタ メンバーのサイト ID を設定します。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)#
```

ステップ 2 サイトの冗長性を有効にします。

site-redundancy

クラスタ フロー モビリティの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

LISP インスペクションについて

LISP トラフィックを検査することで、サイト間のフローのモビリティを有効にできます。

LISP について

VMware VMotion などのデータセンター仮想マシンのモビリティによって、サーバはクライアントへの接続を維持すると同時に、データセンター間を移動できます。このようなデータセンター サーバ モビリティをサポートするには、サーバの移動時にサーバへの入力ルートをルータが更新できる必要があります。Cisco Locator/ID Separation Protocol（LISP）のアーキテクチャは、デバイス ID、つまりエンドポイント ID（EID）をその場所、つまりルーティング ロケータ（RLOC）から 2 つの異なるナンバリング スペースに分離し、サーバの移行をクライアント

に対して透過的にします。たとえば、サーバが新しい場所に移動し、クライアントがサーバにトラフィックを送信すると、ルータは新しい場所にトラフィックをリダイレクトします。

LISP では、LISP の出力トンネル ルータ（ETR）、入力トンネル ルータ（ITR）、ファースト ホップ ルータ、マップ リゾルバ（MR）、およびマップ サーバ（MS）などのある一定のロールにおいてルータとサーバが必要です。サーバが別のルータに接続されていることをサーバのファースト ホップ ルータが感知すると、そのルータは他のすべてのルータとデータベースを更新し、クライアントに接続されている ITR がトラフィックを代行受信してカプセル化し、新しいサーバの場所に送信できるようにします。

ASA LISP のサポート

ASA は LISP 自体を実行しませんが、場所の変更に関する LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用できます。LISP の統合を行わない場合、サーバが新しいサイトに移動すると、トラフィックは元のフローオーナーの代わりに、新しいサイトで ASA クラスタ メンバーになります。新しい ASA が古いサイトの ASA にトラフィックを転送した後、古い ASA は、サーバに到達するためにトラフィックを新しいサイトに送り返す必要があります。このトラフィック フローは最適ではなく、「トロンボーニング」または「ヘアピニング」と呼ばれます。

LISP 統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR 間でやり取りされる LISP トラフィックを検査し、フローの所有者を新しいサイトに変更できます。

LISP のガイドライン

- ASA クラスタ メンバーは、サイトのファースト ホップ ルータと ITR または ETR の間に存在している必要があります。ASA クラスタ自体を拡張セグメントのファーストホップ ルータにすることはできません。
- 完全分散されたフローのみがサポートされます。一元化されたフロー、半分散されたフロー、または個々のノードに属しているフローは新しいオーナーには移動されません。半分散されたフローには SIP などのアプリケーションが含まれており、親フローとそのすべての子フローが同じ ASA によって所有されます。
- クラスタはレイヤ 3 および 4 のフロー状態を移動させるだけです。一部のアプリケーション データが失われる可能性があります。
- 短時間のフローまたはビジネスに不可欠でないフローの場合、オーナーの移動は有用でない可能性があります。インスペクション ポリシーを設定するときに、この機能でサポートされるトラフィックのタイプを制御できます。また、フロー モビリティを不可欠なトラフィックに制限する必要があります。

ASA LISP の実装

この機能には、複数の相互に関係する設定が含まれています（それらについてはすべてこの章で説明します）。

1. （任意）ホストまたはサーバ IP アドレスに基づく検査対象 EID の制限：ファースト ホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信する場合があります。このため、クラスタに関連するサーバまたはネット

ワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

2. LISP トラフィック インスペクション：ASA は、ファーストホップルータと ITR または ETR の間で送信される EID 通知メッセージにおいて、UDP ポート 4342 上の LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。LISP トラフィックにはディレクタが割り当てられておらず、LISP トラフィック自体はクラスタ状態の共有に参加しないことに注意してください。
3. 指定されたトラフィック上のフロー モビリティを有効にするサービス ポリシー：フロー モビリティはビジネスクリティカルなトラフィックに対して有効にする必要があります。たとえば、フロー モビリティを HTTPS トラフィックおよび/または特定のサーバへのトラフィックのみに制限できます。
4. サイト ID：ASA は、各クラスタノードのサイト ID を使用して新しいオーナーを特定します。
5. フローモビリティをイネーブルにするためのクラスタレベル設定：フローモビリティは、クラスタ レベルでも有効にする必要があります。このオン/オフ トグルを使用すると、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。

LISP インスペクションの設定

LISP のトラフィックを検査して、サーバーがサイト間を移動する時にフロー モビリティを有効にできます。

始める前に

- 制御ノードのブートストラップの設定 （657 ページ） および データノードのブートストラップの設定 （663 ページ） に従って、各クラスタ ユニットをサイト ID に割り当てます。
- LISP のトラフィックはデフォルト インスペクション トラフィック クラスに含まれないため、この手順の一部として LISP のトラフィック用に別のクラスを設定する必要があります。

手順

ステップ 1 （任意） LISP インスペクション マップを設定して、IP アドレスに基づいて検査済みの EID を制限し、LISP の事前共有キーを設定します。

a) 拡張 ACL を作成します。宛先 IP アドレスのみが EID 組み込みアドレスと照合されます。

access list *eid_acl_name* **extended permit ip** *source_address mask destination_address mask*

IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) LISP インスペクション マップを作成し、パラメータ モードに移行します。

policy-map type inspect lisp *inspect_map_name*

parameters

c) 作成した ACL を識別して、許可された EID を定義します。

allowed-eid access-list *eid_acl_name*

ファースト ホップ ルータまたは ITR/ETR は、ASA クラスタが関与していないホストまたはネットワークに EID 通知メッセージを送信することがあります。このため、クラスタに関連するサーバーまたはネットワークのみに EID を制限できます。たとえば、クラスタが 2 つのサイトのみに関与しているが、LISP が 3 つのサイトで実行されている場合は、クラスタに関与している 2 つのサイトに対してのみ EID を含める必要があります。

d) 必要に応じて、事前共有キーを入力します。

validate-key *key*

例：

```
ciscoasa(config)# access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0
255.255.255.0
ciscoasa(config)# policy-map type inspect lisp LISP_EID_INSPECT
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# allowed-eid access-list TRACKED_EID_LISP
ciscoasa(config-pmap-p)# validate-key MadMaxShinyandChrome
```

ステップ 2 ファースト ホップ ルータとポート 4342 の ITR または ETR の間の UDP トラフィック の LISP インスペクションの設定。

a) 拡張 ACL を設定して LISP のトラフィックを特定します。

access list *inspect_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq 4342**

UDP ポート 4342 を指定する必要があります。IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。

b) ACL のクラス マップを作成します。

class-map *inspect_class_name*

match access-list *inspect_acl_name*

c) ポリシー マップ、クラス マップを指定し、オプションの LISP インスペクション マップを使用してインスペクションを有効化し、サービス ポリシーをインターフェイスに適用します（新規であれば）。

policy-map *policy_map_name*

class *inspect_class_name*

inspect lisp [*inspect_map_name*]

service-policy *policy_map_name* {**global** | **interface** *ifc_name*}

既存のサービス ポリシーある場合は、既存のポリシー マップ名を指定します。デフォルトで、ASA には**global_policy** と呼ばれるグローバル ポリシーが含まれているため、グローバル ポリシーの名前を指定します。ポリシーをグローバルに適用しない場合は、インターフェイスごとに 1 つのサービス ポリシーを作成することもできます。LISP インスペクションは、双方向にトラフィックに適用するため、送信元と宛先の両方のインターフェイスにサービス ポリシーを適用する必要はありません。トラフィックが両方向のクラス マップに一致する場合、ポリシー マップを適用するインターフェイスに入るまたは存在するトラフィックのすべてが影響を受けます。

例：

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

ASAは、ファースト ホップ ルータと ITR または ETR の間で送信される EID 通知メッセージの LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。

ステップ 3 トラフィック クラスのフロー モビリティを有効化します。

a) 拡張 ACL を設定して、サーバーがサイトを変更するときに、最適なサイトに再割り当てするビジネス クリティカルなトラフィックを特定します。

access list *flow_acl_name* **extended permit udp** *source_address mask destination_address mask* **eq** *port*

IPv4 ACL および IPv6 ACL のどちらにも対応しています。厳密な **access-list extended** の構文については、コマンド リファレンスを参照してください。フロー モビリティは、ビジネス クリティカルなトラフィックに対してイネーブルにする必要があります。たとえば、フロー モビリティを HTTPS トラフィックのみ、または特定のサーバへのトラフィックのみに制限できます。

b) ACL のクラス マップを作成します。

class-map *flow_map_name*

match access-list *flow_acl_name*

c) LISP インスペクションを有効化した同じポリシー マップ、フロー クラス マップを指定して、フロー モビリティを有効にします。

policy-map *policy_map_name*

class *flow_map_name*

cluster flow-mobility lisp

例：

```
ciscoasa(config)# access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0
255.255.255.0 eq https
ciscoasa(config)# class-map IMPORTANT-FLOWS-MAP
ciscoasa(config)# match access-list IMPORTANT-FLOWS
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class IMPORTANT-FLOWS-MAP
ciscoasa(config-pmap-c)# cluster flow-mobility lisp
```

ステップ 4 クラスタ グループ コンフィギュレーション モードに移行し、クラスタのフローのモビリティを有効化します。

cluster group *name*

flow-mobility lisp

このオン/オフの切り替えにより、フロー モビリティの有効化や無効化を簡単に行えます。

例

次に例を示します。

- EID を 10.10.10.0/24 ネットワーク上の EID に制限します。
- 192.168.50.89（内部）にある LISP ルータと 192.168.10.8（別の ASA インターフェイス上）にある ITR または ETR ルータの間の LISP トラフィック（UDP 4342）を検査します。
- HTTPS を使用して 10.10.10.0/24 のサーバーに送信されるすべての内部トラフィックに対してフロー モビリティを有効化します。
- クラスタに対してフロー モビリティをイネーブルにします。

```
access-list TRACKED_EID_LISP extended permit ip any 10.10.10.0 255.255.255.0
policy-map type inspect lisp LISP_EID_INSPECT
   parameters
      allowed-eid access-list TRACKED_EID_LISP
      validate-key MadMaxShinyandChrome
!
access-list LISP_ACL extended permit udp host 192.168.50.89 host 192.168.10.8 eq 4342
class-map LISP_CLASS
   match access-list LISP_ACL
policy-map INSIDE_POLICY
   class LISP_CLASS
      inspect lisp LISP_EID_INSPECT
service-policy INSIDE_POLICY interface inside
!
access-list IMPORTANT-FLOWS extended permit tcp any 10.10.10.0 255.255.255.0 eq https
class-map IMPORTANT-FLOWS-MAP
   match access-list IMPORTANT-FLOWS
policy-map INSIDE_POLICY
   class IMPORTANT-FLOWS-MAP
      cluster flow-mobility lisp
```

```
!
cluster group cluster1
   flow-mobility lisp
```

クラスタノードの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタノードを管理できます。

非アクティブノードになる

クラスタの非アクティブなメンバーになるには、クラスタリングコンフィギュレーションは変更せずに、そのノード上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのノードをクラスタから完全に削除します。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

no enable

このノードが制御ノードであった場合は、新しい制御ノードの選定が実行され、別のメンバーが制御ノードになります。

クラスタ コンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

制御ノードからのデータノードの非アクティブ化

ログインしているノード以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

手順

クラスタからノードを削除します。

cluster remove unit *node_name*

ブートストラップ コンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ノードがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各ノードの現在のコンフィギュレーションは（アクティブユニットから同期されて）同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IP アドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

手順

ステップ 1 データノードの場合、クラスタリングを次のように無効化します。

cluster group *cluster_name* **no enable**

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがデータノード上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ 2 クラスタ コンフィギュレーションをクリアします。

clear configure cluster

ASAは、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ 3 クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ 4 バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy *backup_cfg* **running-config**

例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

ステップ 5 コンフィギュレーションをスタートアップに保存します。

write memory

ステップ 6 バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

制御ノードの変更

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

手順

新しいノードを制御ノードとして設定します。

cluster control-node unit*node_name*

例：

```
ciscoasa(config)# cluster control-node unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバー名を表示するには、**cluster control-node unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのノードに、または特定のノードに送信するには、次の手順を実行します。**show** コマンドをすべてのノードに送信すると、すべての出力が収集されて現在のノードのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

手順

すべてのノードにコマンドを送信します。ノード名を指定した場合は、特定のノードに送信します。

cluster exec [**unit** *node_name*] コマンド

例：

```
ciscoasa# cluster exec show xlate
```

ノード名を表示するには、**cluster exec unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャファイルをクラスタ内のすべてのノードから同時に TFTP サーバにコピーするには、制御ノードで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ノードから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にノード名が付加され、capture1_asa1.pcap、

capture1_asa2.pcap などとなります。この例では、asa1 と asa2 はクラスタノード名です。

ASA 仮想クラスタのモニタリング

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info** [**health** [**details**]]

  キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバのステータスが表示されます。

  show cluster info health コマンドは、インターフェイス、ノードおよびクラスタ全体の現在の状態を表示します。**details** キーワードは、ハートビート メッセージの失敗数を表示します。

  show cluster info コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID   : 2
```

```
      Version   : 9.4(1)
Serial No.: P3000000191
CCL IP    : 10.0.0.2
CCL MAC   : 000b.fcf8.c61e
Last join : 19:13:50 UTC Sep 23 2011
Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  時間遅延後にクラスタノードがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルスチェック障害など）がクリアされたかどうかを示します。ノードが永続的に無効になっている場合、またはノードがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。

  show cluster info auto-join コマンドについては次の出力を参照してください。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check
failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp**[**detail**]}

  次のトランスポート関連の統計情報を表示します。

  - **asp**：データ プレーンのトランスポート統計情報。
  - **cp**：コントロール プレーンのトランスポート統計情報。

    detail キーワードを入力すると、クラスタで信頼性の高いトランスポート プロトコルの使用状況が表示され、バッファがコントロールプレーンでいっぱいになったときにパケット ドロップの問題を特定できます。**show cluster info transport cp detail** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
```

```
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent

This unit as a sender
--------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
--------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0
```

```
    total:                  0
    current:                0
    high watermark:         0

    delivered:              0
    deliver failures:       0

    buffer full drops:      0
    message truncate drops: 0

    gate close ref count:   0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        4153         73%
  Route Cluster Client                            419          7%
  RRI Cluster Client                             1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  VPN Clustering HA Client                          1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                          Total messages  Percentage
  Cluster Redirect Client                        3731         91%
  RRI Cluster Client                              328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                          Total messages  Percentage    F   L   R
  Cluster Redirect Client                        3607         91%    0   0   0
  RRI Cluster Client                              317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
```

```
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ------------------------------------------------------------
  Client name                          Total messages  Percentage
  VPN Clustering HA Client                        572         99%
  Cluster VPN Unique ID Client                      1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  クラスタの履歴、およびクラスタノードが参加できなかった理由や、ノードがクラスタを離れた理由に関するエラーメッセージが表示されます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用して制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

クラスタリソースのモニタリング

クラスタリソースのモニタリングについては、次のコマンドを参照してください。

show cluster {**cpu** | **memory** | **resource**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタトラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail]、cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダのどのフローであるかを示します。**cluster exec show conn** コマンドを任意のノードで使用すると、すべての接続が表示されます。このコマンドの表示からは、1 つのフローのトラフィック

がクラスタ内のさまざまなASAにどのように到達するかがわかります。クラスタのスループットは、ロードバランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

また、**show conn detail** コマンドはフローモビリティの影響を受けるフローを表示します。

次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
 uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
 received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
 NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
 Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic
received at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface
NP Identity
Ifc Locally received: 716 (8 byte/s)
```

接続フローのトラブルシューティングを行うには、最初にすべてのノードの接続を一覧表示します。それには、任意のノードで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3 つのすべての ASA での 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が表示されています。ASA1 には z フラグがあり、この接続のフォワーダであることを表しています。ASA3 には Y フラグがあり、この接続のディレクタであることを表しています。ASA2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットはASA2の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパ

ケットはASA1およびASA3の外部インターフェイスに入り、クラスタ制御リンクを介してASA2に転送され、次にASA2の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**************************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**************************************************************
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes
0, flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution コマンドと **show cluster info packet-distribution** コマンドは、すべてのクラスタノードへのトラフィック分散を表示します。これらのコマンドは、外部ロードバランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

  show cluster info flow-mobility counters コマンドは、EIDおよびフローの所有者の動作情報を表示します。**show cluster info flow-mobility counters** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  この**show cluster info load-monitor**コマンドは、最後の間隔のクラスタメンバのトラフィック負荷と、設定された間隔の合計数（デフォルトでは30）を表示します。各間隔の各測定値を表示するには、**details** キーワードを使用します。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14             25
   1           0            0            16             20
Average from last 30 interval:
   0           0            0            12             28
```

```
   1           0           0           13              27

ciscoasa(cfg-cluster)# show cluster info load-monitor details

ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval


Connection count captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0


Buffer drops captured over 30 intervals:

Unit ID  0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

         0          0          0          0          0          0

Unit ID  1

         0          0          0          0          0          0

         0          0          0          0          0          0
```

```
          0          0          0          0          0          0
          0          0          0          0          0          0
          0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35

CPU usage(%) captured over 30 intervals:
Unit ID  0
         25         25         30         30         30         35
         25         25         35         30         30         30
         25         25         30         25         25         35
         30         30         30         25         25         25
         25         20         30         30         30         30
Unit ID  1
         30         25         35         25         30         30
         25         25         35         25         30         35
         30         30         35         30         30         30
         25         20         30         25         25         30
         20         30         35         30         30         35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

show cluster access-list コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのノードでの合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*****************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

  クラスタのルーティング情報を表示します。

- **show lisp eid**

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

  cluster exec show lisp eid コマンドからの、次の出力を参照してください。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):*********************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:*****************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  このコマンドは、トラブルシューティングに役立ちます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ノードは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

クラスタのインターフェイスのモニタリング

クラスタのインターフェイスのモニタリングについては、次のコマンドを参照してください。

- **show cluster interface-mode**

  クラスタ インターフェイスのモードを表示します。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **debug cluster flow-mobility**

  クラスタリング フロー モビリティ関連のイベントを表示します。

- **debug lisp eid-notify-intercept**

  EID 通知メッセージ代行受信時のイベントを表示します。

- **show cluster info trace**

  show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

  show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

  たとえば、同じ**ローカルユニット**名を持つ2つのノードが制御ノードとして機能していることを示す次のメッセージが表示された場合は、2 つのノードの**ローカルユニット**名が同じである（設定を確認してください）か、1つのノードが自身のブロードキャストメッセージを受信している（ネットワークを確認してください）可能性があります。

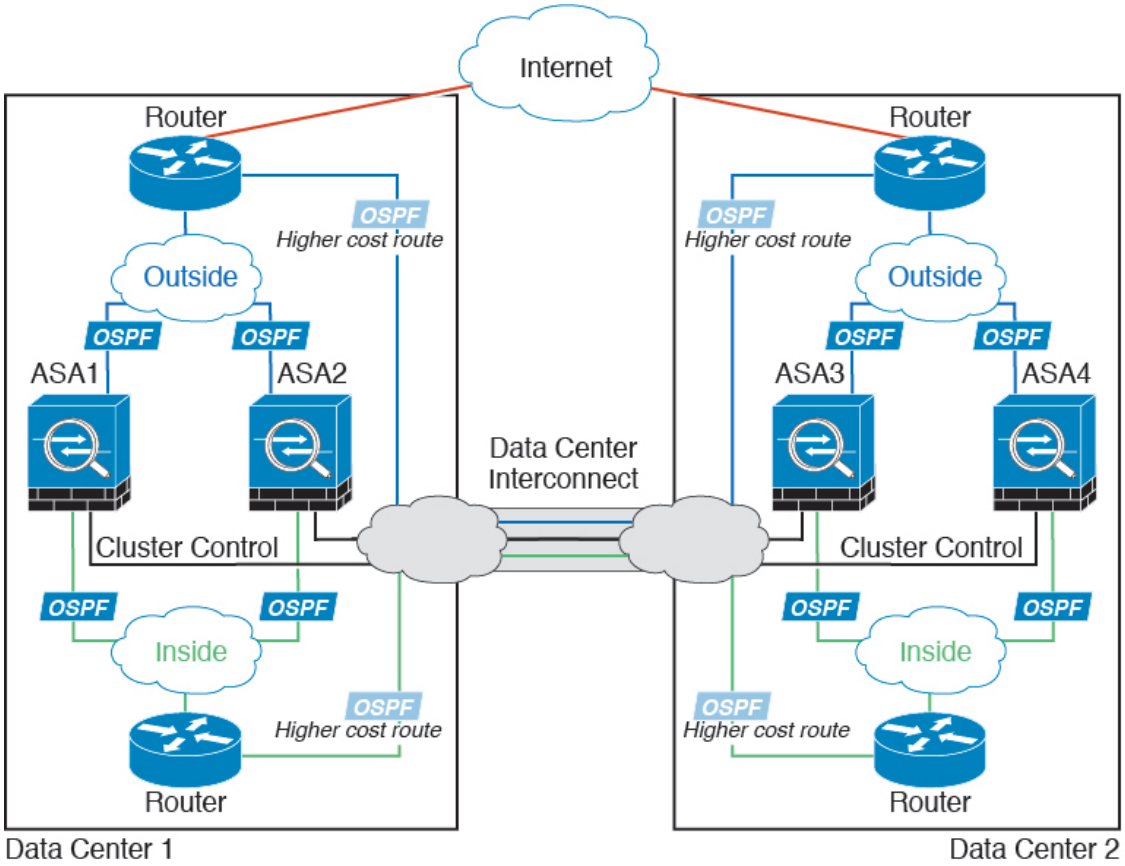
```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node

 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
 Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
 CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

ASA 仮想クラスタリングの例

以下の例には、一般的な導入での ASA のクラスタ関連のすべてのコンフィギュレーションが含まれます。

個別インターフェイス ルーテッド モード ノースサウス サイト間の例

次の例では、内部ルータと外部ルータの間に配置された（ノースサウス挿入）2 つのデータセンターのそれぞれに 2 つの ASA クラスタノードがある場合を示します。クラスタノードは、DCI 経由のクラスタ制御リンクによって接続されています。各データセンターの内部ルータと外部ルータは、OSPF と PBR または ECMP を使用してクラスタ メンバ間でトラフィックをロードバランスします。DCI に高コストルートを割り当てることにより、特定のサイトのすべての ASA クラスタノードがダウンしない限り、トラフィックは各データセンター内に維持されます。1 つのサイトのすべてのクラスタノードに障害が発生した場合、トラフィックは各ルータから DCI 経由で他のサイトの ASA クラスタノードに送られます。



クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- 次のアプリケーション インスペクション：
  - CTIQBE
  - H323、H225、および RAS
  - IPsec パススルー
  - MGCP
  - MMP
  - RTSP
  - SCCP（Skinny）
  - WAAS
  - WCCP
- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- VPN ロード バランシング
- Azure でのフェールオーバー
- 統合ルーティングおよびブリッジング
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP
  - IM
  - NetBIOS
  - PPTP
  - RADIUS
  - RSH
  - SNMP
  - SQLNET
  - SUNRPC
  - TFTP
  - XDMCP
- スタティック ルート モニタリング
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス
- サイト間 VPN
- マルチキャスト ルーティング

個々のノードに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て

行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。

- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。
- リソース管理：マルチコンテキストモードでのリソース管理は、ローカル使用状況に基づいて各ノードに個別に適用されます。
- LISP トラフィック：UDP ポート 4342 上の LISP トラフィックは、各受信ノードによって検査されますが、ディレクタは割り当てられません。各ノードは、クラスタ間で共有される EID テーブルに追加されますが、LISP トラフィック自体はクラスタ状態の共有に参加しません。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証と許可は、クラスタリング制御ノード上で中央集中型機能として実装されており、データ構造がクラスタデータノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるため、フローに対するアカウンティングが設定されている場合、そのフローを所有するクラスタノードがアカウンティング開始と停止のメッセージを AAA サーバに送信します。

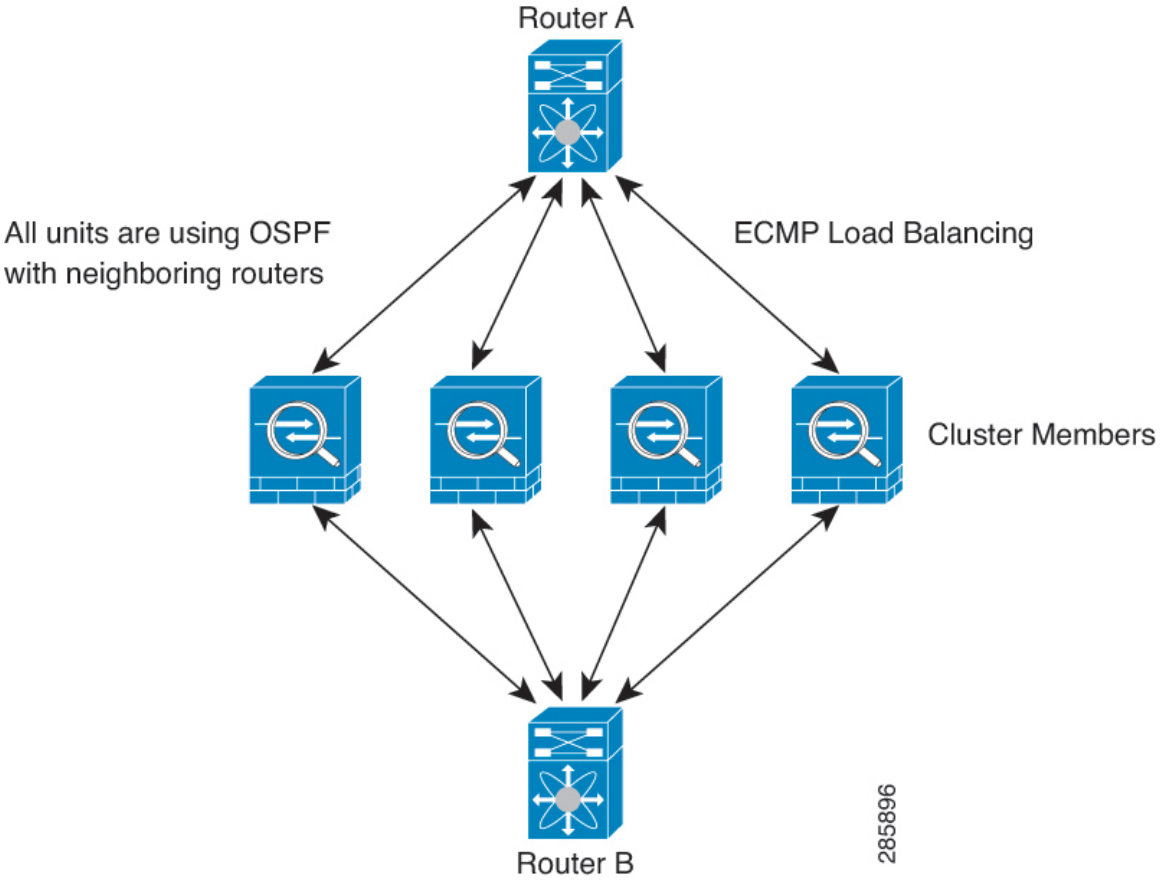
接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます（**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、および **set connection per-client-max** コマンドを参照）。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

ダイナミック ルーティングおよびクラスタリング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *55 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィック ゾーンにこれらすべてのノードインターフェイスをまとめます。トラフィック ゾーンの設定 （995 ページ）を参照してください。

FTP とクラスタリング

- FTPデータ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用する場合、制御チャネルのフローは制御ノードに集中されます。

ICMP インスペクションとクラスタリング

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインスペクションが有効かどうかによって異なります。ICMPインスペクションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インスペクションを使用する場合、ICMP フローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットのディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

マルチキャスト ルーティングとクラスタリング

個別インターフェイスモードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべて制御ユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。こ

れは、スパンドEtherChannelの問題ではありません。クラスタ インターフェイスには関連付けられた IP アドレスが 1 つしかないためです。

- 個別インターフェイスのインターフェイス PAT なし：インターフェイス PAT は、個別インターフェイスではサポートされていません。

- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。
  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。
  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。
  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。
  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは512ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。

- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致

させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。

- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。
- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。
- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。
- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。
- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。たとえば、TCP/443 の HTTPS TLS と比較してずっと優れたパフォーマンスを発揮する代替手段として、UDP/443 を用いる Quick プロトコルの使用が増加している場合、UDP/443 に対し per-session PAT を有効にする必要があります。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。
- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効に

する必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、その 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、STUNインスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。STUN要求の受信後にノードに障害が発生し、別のノードがSTUN応答を受信した場合、STUN応答はドロップされます。

syslog および NetFlow とクラスタリング

- Syslog：クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカルノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。

- NetFlow：クラスタの各ノードは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN 接続を再確立する必要があります。

PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80%になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps（8 ユニット x 10 Gbps）の約 80% で 64 Gbps になります。

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。

3. 45秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

（注） 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。

5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注） ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

ASA 仮想クラスタ内のハイアベイラビリティ

ASA仮想クラスタリングは、ノードとインターフェイスの正常性をモニタリングし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2つのクラスタロケーション間でルータに障害が発生した場合、ロケーション1の元の制御ノードは、ロケーション2のデータノードをクラスタから削除します。一方、ロケーション2のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

詳細については、制御ノードの選定 （705 ページ）を参照してください。

インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェアインターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

ヘルスモニタリングを有効化すると、すべての物理インターフェイスがデフォルトでモニターされるため、オプションでインターフェイスごとのモニタリングを無効化することができます。指名されたインターフェイスのみモニターできます。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ASAがメンバーをクラスタから削除するまでの時間は、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。ASAは、ノードがクラスタに参加する最初の90秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。ノード状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

クラスタ内のノードで障害が発生したときに、そのノードでホストされている接続は他のノードにシームレスに移行されます。トラフィックフローのステート情報は、制御ノードのクラスタ制御リンクを介して共有されます。

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASAが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでノードがまだ非アクティブになっていると、管理インターフェイスは無効になります。さらに設定を行う場合は、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタノードがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：（最初の参加時）クラスタ制御リンクの問題を解決した後、CLI で **cluster group** 名 を入力してから **enable** と入力して、クラスタリングを再び有効化することによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASAは、無限に5分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディ

セーブルにします。データインターフェイスの問題を解決した後、CLIで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動で有効化する必要があります。この動作は設定可能です。

- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングが **enable** コマンドでまだイネーブルになっているなら、ノードは再起動するとクラスタに再参加することを意味します。ASA は 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。ノードは、5 分、10 分、20 分の間隔で自動的にクラスタに再参加しようとします。この動作は設定可能です。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *20*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—
ユーザ アイデンティティ	Yes	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—
Firepower 4100/9300 の分散型 VPN（サイト間）	Yes	バックアップセッションがアクティブセッションになると、新しいバックアップセッションが作成されます。

ASA 仮想クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。

- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

  サイト間クラスタリングのディレクタローカリゼーションを有効にすると、ローカルバックアップとグローバルバックアップの2つのバックアップ オーナー権限があります。オーナーは、常に同じサイトのローカルバックアップをオーナー自身として選択します（サイトIDに基づいて）。グローバルバックアップはどのサイトにあってもよく、ローカルバックアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

  サイトの冗長性を有効にし、バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。シャーシバックアップとサイトバックアップは独立しているため、フローにはシャーシ バックアップとサイト バックアップの両方が含まれている場合があります。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に

対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルディレクタとグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（Site Id に基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにあってもよく、ローカルディレクタと同一ノードとすることもできます。元のオーナーに障害が発生すると、ローカルディレクタはこのサイトで新しい接続オーナーを選択します。

ICMP/ICMPv6 ハッシュの詳細：

- エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
- 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
- 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタのローカリゼーションを有効にすると、フォワーダは常にローカルディレクタに問い合わせます。フォワーダがグローバルディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタ メンバーが受信する場合などです。フォワーダが SYN-ACK パケットを受信した場合、フォワーダはパケットの SYN クッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID の

ハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される5タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

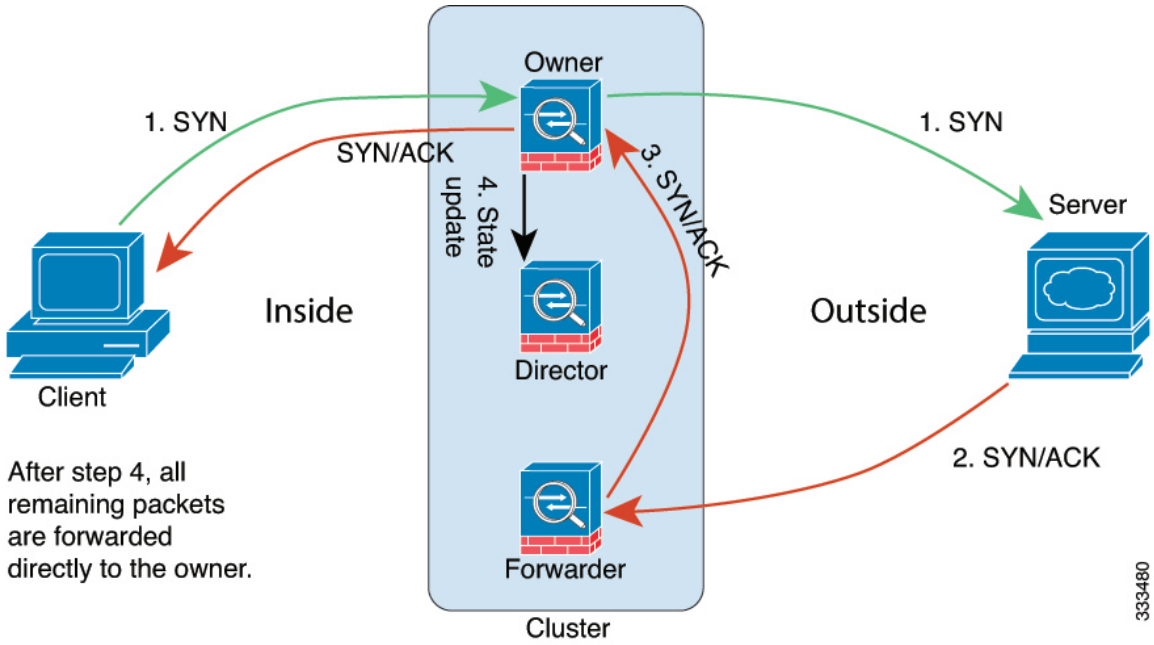
TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そのパケットはクラスタ制御リンクを介してオーナーノードに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1つのフローの両方向が同じノードに到着するとともに、フローがノード間に均等に分散されるようにするためです。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。

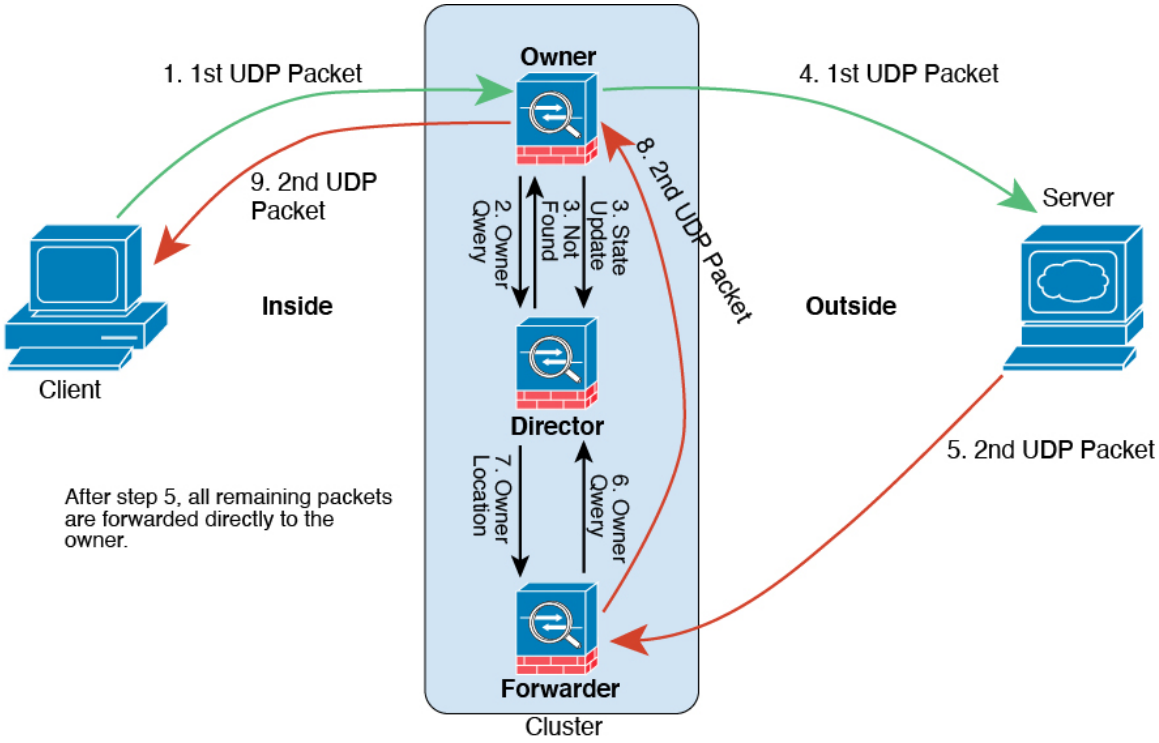


1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。
8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

1. 図 *56 : ICMP* および *UDP* データフロー



UDP パケットがクライアントから発信され、1 つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。
3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。
4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。
5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。
6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。
7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

新しい TCP 接続のクラスタ全体での再分散

アップストリームルータまたはダウンストリームルータによるロードバランシングの結果として、フロー分散に偏りが生じた場合は、新しい接続再分散を設定して、1 秒あたりの新しい接続数が多いノードから他のノードに新しい TCP フローをリダイレクトすることができます。既存のフローは他のノードには移動されません。

このコマンドは1秒あたりの接続数に基づいてのみ再分散するため、各ノードで確立された接続の総数は考慮されず、接続の総数は等しくない場合があります。

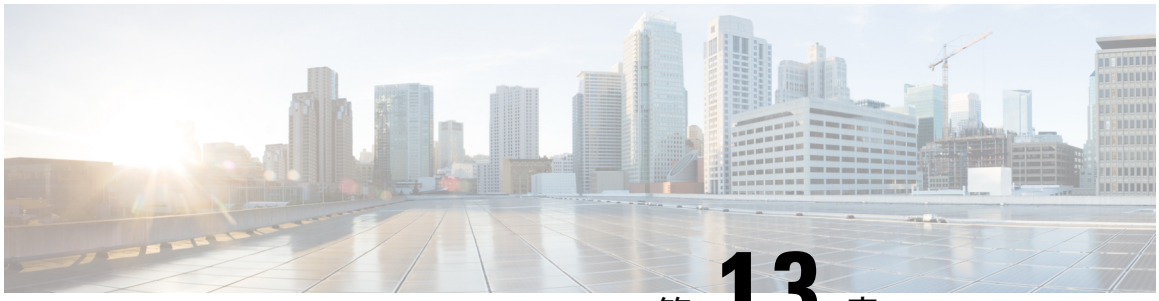
接続が別のノードにオフロードされると、非対称接続になります。

サイト間トポロジに対しては接続の再分散を設定しないでください。異なるサイトのクラスタメンバには新しい接続を再分散できません。

ASA 仮想クラスタリングの履歴

機能名	バージョン	機能情報
ノード参加時の MTU ping テスト	9.23(1)	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
フローステータスの設定可能なクラスタキープアライブ間隔	9.20(1)	フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。 新規/変更されたコマンド： **clu-keepalive-interval**
バイアス言語の除去	9.19(1)	「Master」と「Slave」という用語を含むコマンド、コマンド出力、syslog メッセージは、「Control」と「Control」に変更されました。 新規/変更されたコマンド：**cluster control-node**、**enable as-data-node**、**prompt**、**show cluster history**、**show cluster info**

機能名	バージョン	機能情報
VMware および KVM 用の ASAv30、ASAv50、および ASAv100 クラスタリング	9.17(1)	ASA 仮想 クラスタリングを使用すると、最大 16 の ASA 仮想 を単一の論理デバイスとしてグループ化できます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。ASA 仮想 クラスタリングは、ルーテッド ファイアウォール モードで個別インターフェイスモードをサポートします。スパンド EtherChannels はサポートされていません。ASA 仮想 は、クラスタ制御リンクに VXLAN 仮想インターフェイス（VNI）を使用します。 新規/変更されたコマンド：**cluster-interface vni**、**nve-only cluster**、**peer-group**、**show cluster info**、**show cluster info instance-type**、**show nve 1**



第 13 章

パブリッククラウドにおける ASA Virtual の ASA クラスタ

クラスタリングを利用すると、複数の ASA 仮想 をグループ化して 1 つの論理デバイスとすることができます。クラスタは、単一デバイスのすべての利便性（管理、ネットワークへの統合）を備える一方で、複数デバイスによって高いスループットおよび冗長性を達成します。以下を使用して、パブリッククラウドに ASA 仮想 クラスタを展開できます。

- Amazon Web Services（AWS）
- Microsoft Azure

現在は、ルーテッド ファイアウォール モードのみがサポートされます。

（注） クラスタリングを使用する場合、一部の機能はサポートされません。「クラスタリングでサポートされない機能 （804 ページ）」を参照してください。

- パブリッククラウドにおける ASA Virtual クラスタリングについて （718 ページ）
- ASA Virtual クラスタリングのライセンス （723 ページ）
- ASA Virtual クラスタリングの要件と前提条件 （723 ページ）
- ASA Virtual クラスタリングのガイドライン （725 ページ）
- AWS でクラスタを展開する （726 ページ）
- Azure でクラスタを展開する （747 ページ）
- ASA 仮想 Azure でのクラスタリングのオートスケール ソリューション （760 ページ）
- クラスタリング動作のカスタマイズ （783 ページ）
- クラスタノードの管理 （787 ページ）
- クラスタのモニタリング （792 ページ）
- クラスタリングの参考資料 （804 ページ）
- パブリッククラウドにおける ASA Virtual クラスタリングの履歴 （821 ページ）

パブリッククラウドにおける ASA Virtual クラスタリングについて

ここでは、クラスタリング アーキテクチャとその動作について説明します。

クラスタをネットワークに適合させる方法

クラスタは、複数のファイアウォールで構成され、これらは 1 つのデバイスとして機能します。ファイアウォールをクラスタとして機能させるには、次のインフラストラクチャが必要です。

- クラスタ内通信用の、隔離されたネットワーク。VXLAN インターフェイスを使用したクラスタ制御リンクと呼ばれます。レイヤ 3 物理ネットワーク上でレイヤ 2 仮想ネットワークとして機能する VXLAN により、ASA 仮想はクラスタ制御リンクを介してブロードキャスト/マルチキャストメッセージを送信できます。
- ロードバランサ：外部ロードバランシングには次のオプションがあります。
  - AWS Gateway Load Balancer

    AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。ASA 仮想 は、Geneve インターフェイスのシングルアームプロキシを使用して分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。
  - シスコ クラウド サービス ルータなどの内部および外部ルータを使用した等コスト マルチパス ルーティング（ECMP）

    ECMP ルーティングでは、ルーティング メトリックが同値で最高である複数の「最適パス」を介してパケットを転送できます。EtherChannel のように、送信元および宛先の IP アドレスや送信元および宛先のポートのハッシュを使用してネクスト ホップの 1 つにパケットを送信できます。ECMP ルーティングにスタティックルートを使用する場合は、ASA 仮想 の障害発生時に問題が起きることがあります。ルートは引き続き使用されるため、障害が発生した ASA 仮想へのトラフィックが失われるからです。スタティック ルートを使用する場合は必ず、オブジェクト トラッキングなどのスタティック ルート モニタリング機能を使用してください。ダイナミック ルーティング プロトコルを使用してルートの追加と削除を行うことを推奨します。この場合は、ダイナミック ルーティングに参加するように各 ASA 仮想 を設定する必要があります。

（注） レイヤ 2 スパンド EtherChannels はロードバランシングではサポートされません。

クラスタ ノード

クラスタノードは連携して動作し、セキュリティポリシーおよびトラフィックフローの共有を達成します。ここでは、各ノードのロールの特長について説明します。

ブートストラップ設定

各デバイスで、最小限のブートストラップコンフィギュレーション（クラスタ名、クラスタ制御リンクインターフェイスなどのクラスタ設定）を設定します。通常、クラスタリングを有効にする最初のノードが制御ノードになります。以降のノードに対してクラスタリングをイネーブルにすると、そのノードはデータノードとしてクラスタに参加します。

制御ノードとデータノードの役割

クラスタ内のメンバーの1つが制御ノードになります。複数のクラスタノードが同時にオンラインになる場合、制御ノードは、ブートストラップ コンフィギュレーション内のプライオリティ設定によって決まります。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。他のすべてのメンバーはデータノードです。一般的には、クラスタを作成した後で最初に追加したノードが制御ノードとなります。これは単に、その時点でクラスタに存在する唯一のノードであるからです。

すべてのコンフィギュレーション作業（ブートストラップ コンフィギュレーションを除く）は、制御ノード上のみで実行する必要があります。コンフィギュレーションは、データノードに複製されます。物理的アセット（たとえばインターフェイス）の場合は、制御ノードのコンフィギュレーションがすべてのデータノード上でミラーリングされます。たとえば、内部インターフェイスとしてイーサネット1/2を設定し、外部インターフェイスとしてイーサネット1/1を設定した場合、これらのインターフェイスは内部および外部インターフェイスとしてデータノードでも使用されます。

機能によっては、クラスタ内でスケーリングしないものがあり、そのような機能については制御ノードがすべてのトラフィックを処理します。

個々のインターフェイス

クラスターフェイスを個々のインターフェイスとして設定できます。

個別インターフェイスは通常のルーテッドインターフェイスであり、それぞれが専用のローカルIPアドレスを持ちます。インターフェイス構成は、制御ノードでのみ設定する必要があり、各インターフェイスは DHCP を使用します。

（注） レイヤ 2 スパンド EtherChannels はサポートされません。

クラスタ制御リンク

ノードごとに1つのインターフェイスをクラスタ制御リンク専用のVXLAN（VTEP）インターフェイスにする必要があります。VXLANの詳細については、VXLANインターフェイス（895ページ）を参照してください。

VXLAN トンネル エンドポイント

VXLANトンネルエンドポイント（VTEP）デバイスは、VXLANのカプセル化およびカプセル化解除を実行します。各VTEPには2つのインターフェイスタイプ（VXLAN Network Identifier（VNI）インターフェイスと呼ばれる1つ以上の仮想インターフェイスと、 VTEP間にVNIをトンネリングするVTEP送信元インターフェイスと呼ばれる通常のインターフェイス）がありますVTEP送信元インターフェイスは、VTEP間通信のトランスポートIPネットワークに接続されます。

VTEP 送信元インターフェイス

VTEP送信元インターフェイスは、VNIインターフェイスに関連付けられる予定の標準のASA Virtualインターフェイスです。1つのVTEPソースインターフェイスをクラスタ制御リンクとして機能するように設定できます。ソースインターフェイスは、クラスタ制御リンクの使用専用に予約されています。各VTEPソースインターフェイスには、同じサブネット上のIPアドレスがあります。このサブネットは、他のすべてのトラフィックからは隔離し、クラスタ制御リンクインターフェイスだけが含まれるようにしてください。

VNI インターフェイス

VNIインターフェイスはVLANインターフェイスに似ています。VNIインターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワークトラフィックの分割を維持する仮想インターフェイスです。設定できるVNIインターフェイスは1つだけです。各VNIインターフェイスは、同じサブネット上のIPアドレスを持ちます。

ピア VTEP

単一のVTEPピアを許可するデータインターフェイス用の通常のVXLANとは異なり、ASA Virtualクラスタリングでは複数のピアを設定できます。

クラスタ制御リンク トラフィックの概要

クラスタ制御リンク トラフィックには、制御とデータの両方のトラフィックが含まれます。

制御トラフィックには次のものが含まれます。

- 制御ノードの選択。
- 設定の複製。
- ヘルス モニタリング。

データ トラフィックには次のものが含まれます。

- ステート複製。
- 接続所有権クエリおよびデータ パケット転送。

クラスタ制御リンクの障害

ユニットのクラスタ制御リンク回線プロトコルがダウンした場合、クラスタリングはディセーブルになります。データ インターフェイスはシャット ダウンされます。クラスタ制御リンクの修復後、クラスタリングを再度イネーブルにして手動でクラスタに再参加する必要があります。

（注） ASA 仮想 が非アクティブになると、すべてのデータ インターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのユニットが DHCP またはクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。クラスタ IP プールを使用している場合、リロードしてもクラスタでユニットがまだ非アクティブになっていると、管理インターフェイスはアクセスできません（制御ノードと同じメイン IP アドレスを使用するため）。さらに設定を行う場合は、コンソールポート（使用可能な場合）を使用する必要があります。

コンフィギュレーションの複製

クラスタ内のすべてのノードは、単一の設定を共有します。設定の変更は制御ノードでのみ可能（ブートストラップ設定は除く）で、変更はクラスタに含まれる他のすべてのノードに自動的に同期されます。

ASA 仮想 クラスタの管理

ASA 仮想 クラスタリングを使用することの利点の 1 つは、管理のしやすさです。ここでは、クラスタを管理する方法について説明します。

管理ネットワーク

すべてのノードを単一の管理ネットワークに接続することを推奨します。このネットワークは、クラスタ制御リンクとは別のものです。

管理インターフェイス

管理用に、管理 0/0 インターフェイスを使用します。

（注） 管理インターフェイスの動的ルーティングを有効にすることはできません。スタティック ルートを使用する必要があります。

管理 IP アドレスには、静的アドレスまたは DHCP を使用できます。

静的 IP アドレスを使用する場合は、常に現在の制御ノードに属するクラスタの固定アドレスであるメインクラスタ IP アドレスを使用できます。インターフェイスごとに、管理者はアドレス範囲も設定します。これで、各ノード（現在の制御ノードも含まれます）がその範囲内のローカルアドレスを使用できるようになります。このメインクラスタ IP アドレスによって、管理アクセスのアドレスが一本化されます。制御ノードが変更されると、メインクラスタ IP アドレスは新しい制御ノードに移動するので、クラスタの管理をシームレスに続行できます。ローカルIPアドレスは、ルーティングに使用され、トラブルシューティングにも役立ちます。たとえば、クラスタを管理するにはメインクラスタ IP アドレスに接続します。このアドレスは常に、現在の制御ノードに関連付けられています。個々のメンバを管理するには、ローカル IP アドレスに接続します。TFTP や syslog などの発信管理トラフィックの場合、制御ノードを含む各ノードは、ローカル IP アドレスを使用してサーバーに接続します。

DHCP を使用する場合、ローカルアドレスのプールを使用したり、メインクラスタの IP アドレスを使用したりしません。

（注） to-the-box トラフィックをノードの管理IPアドレスに転送する必要があります。to-the-box トラフィックは、クラスタ制御リンクを介して他のノードに転送されません。

制御ノードの管理対データノードの管理

すべての管理とモニタリングは制御ノードで実行できます。制御ノードから、すべてのノードのランタイム統計情報、リソース使用状況、その他のモニタリング情報を確認できます。また、クラスタ内のすべてのノードに対してコマンドを発行したり、コンソールメッセージをデータノードから制御ノードに複製したりできます。

必要に応じて、データノードを直接モニタできます。制御ノードからも可能ですが、ファイル管理（設定のバックアップやイメージの更新など）をデータノード上で実行できます。次の機能は、制御ノードからは使用できません。

- ノードごとのクラスタ固有統計情報のモニタリング。
- ノードごとのSyslogモニタリング（コンソールレプリケーションが有効な場合にコンソールに送信される Syslog を除く）。
- SNMP
- NetFlow

暗号キー複製

制御ノード上で暗号キーを作成すると、そのキーはすべてのデータノードに複製されます。メインクラスタ IP アドレスへの SSH セッションがある場合、制御ノードで障害が発生すると接続が切断されます。新しい制御ノードでは、SSH接続に対して同じキーが使用されるため、新しい制御ノードに再接続するときに、キャッシュ済みの SSH ホストキーを更新する必要はありません。

ASDM 接続証明書 IP アドレス不一致

デフォルトでは、自己署名証明書は、ローカル IP アドレスに基づいて ASDM 接続に使用されます。ASDM を使用してメインクラスタ IP アドレスに接続すると、IP アドレス不一致に関する警告メッセージが表示される場合があります。これは、証明書で使用されているのがローカル IP アドレスであり、メインクラスタ IP アドレスではないためです。このメッセージは無視して、ASDM 接続を確立できます。ただし、この種の警告を回避するには、新しい証明書を登録し、この中でメイン クラスタ IP アドレスと、IP アドレス プールからのすべてのローカル IP アドレスを指定します。この証明書を各クラスタ メンバに使用します。詳細については、「https://www.cisco.com/c/en/us/td/docs/security/asdm/identity-cert/cert-install.html」を参照してください。

ASA Virtual クラスタリングのライセンス

各クラスタノードには、同じモデルライセンスが必要です。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のメンバーに一致するようにすべてのノードで制限されます。スループットレベルは、一致するように制御ノードから各データノードに複製されます。

（注） ASA 仮想 を登録解除してライセンスを解除した場合、ASA 仮想 をリロードすると、重大なレート制限状態に戻ります。ライセンスのない、パフォーマンスの低いクラスタノードは、クラスタ全体のパフォーマンスに悪影響を及ぼします。すべてのクラスタノードのライセンスを保持するか、ライセンスのないノードを削除してください。

ASA Virtual クラスタリングの要件と前提条件

モデルの要件

- ASAv30、ASAv50、ASAv100
- 以下のパブリッククラウドサービス：
  - Amazon Web Services（AWS）
  - Microsoft Azure
- 最大 16 ノード

『ASA Virtual Getting Started Guide』の ASA virtual の一般的な要件も参照してください。

ハードウェアおよびソフトウェアの要件

クラスタ内のすべてのノード：

- 同じパフォーマンス層である必要があります。すべてのノードに同じ数の CPU とメモリを使用することをお勧めします。そうしないと、パフォーマンスが最小能力のノードに一致するようにすべてのノードで制限されます。
- イメージアップグレード時を除き、同じソフトウェアを実行する必要があります。ヒットレスアップグレードがサポートされます。ソフトウェアバージョンが一致しないとパフォーマンスが低下する可能性があるため、すべてのノードを同じメンテナンス期間でアップグレードするようにしてください。
- 単一の可用性ゾーンの展開がサポートされています。
- クラスタ制御リンクのインターフェイスは同じサブネット内に配置される必要があるため、クラスタは同じサブネットに展開する必要があります。

MTU

クラスタ制御リンクに接続されているポートに適切な MTU 値（高い値）が設定されていること。MTUの不一致がある場合、クラスタの形成に失敗します。クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。

クラスタ制御リンクの MTU は、データインターフェイスよりも 154 バイト大きく設定されているはずです。クラスタ制御リンクのトラフィックにはデータパケット転送が含まれるため、クラスタ制御リンクはデータパケット全体のサイズに加えてクラスタトラフィックのオーバーヘッド（100 バイト）と VXLAN のオーバーヘッド（54 バイト）にも対応する必要があります。

GWLB を使用する AWS の場合、データインターフェイスは Geneve カプセル化を使用します。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。送信元インターフェイス MTU をネットワーク MTU + 306 バイトに設定する必要があります。したがって、標準の 1500 MTU ネットワークパスの場合、送信元インターフェイスの MTU は 1806 であり、クラスタ制御リンクの MTU は +154 の 1960 である必要があります。

GWLB を使用する Azure の場合、データインターフェイスは VXLAN カプセル化を使用します。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。送信元インターフェイス MTU をネットワーク MTU + 54 バイトに設定する必要があります。

次の表は、推奨されるクラスタ制御リンク MTU とデータインターフェイス MTU を示しています。

（注） クラスタ制御リンクの MTU を 2561 ～ 8362 に設定することは推奨されません。ブロックプールの処理が原因で、この MTU サイズはシステム動作に最適ではありません。

表 *21* : 推奨 *MTU*

パブリック クラウド	クラスタ制御リンク MTU	データインターフェイス MTU
GWLB を使用した AWS	1960	1806
AWS	1654	1500
GWLB を使用した Azure	1554	1454
Azure	1554	1400

ASA Virtual クラスタリングのガイドライン

ハイ アベイラビリティ

クラスタリングでは、高可用性はサポートされません。

IPv6

クラスタ制御リンクは、IPv4 のみを使用してサポートされます。

その他のガイドライン

- 大々的なトポロジ変更が発生する場合（EtherChannel インターフェイスの追加または削除、ASA virtual 上でのインターフェイスまたはスイッチの有効化または無効化、冗長スイッチシステムを形成するための追加スイッチの追加など）、ヘルスチェック機能や無効なインターフェイスに対するインターフェイスモニタリングを無効にする必要があります。トポロジの変更が完了して、コンフィギュレーション変更がすべてのユニットに同期されたら、インターフェイスのヘルス チェック機能を再度有効にできます。
- ノードを既存のクラスタに追加したときや、ノードをリロードしたときは、一時的に、限定的なパケット/接続ドロップが発生します。これは予定どおりの動作です。場合によっては、ドロップされたパケットが原因で接続がハングすることがあります。たとえば、FTP 接続の FIN/ACK パケットがドロップされると、FTP クライアントがハングします。この場合は、FTP 接続を再確立する必要があります。
- 復号された TLS/SSL 接続の場合、復号状態は同期されず、接続オーナーに障害が発生すると、復号された接続がリセットされます。新規ノードへの接続を新たに確立する必要があります。復号されていない接続（復号しないルールに一致）は影響を受けず、正しく複製されます。
- ダイナミックスケーリングはサポートされていません。
- 各メンテナンスウィンドウの完了後にグローバル展開を実行します。
- 自動スケールグループ（AWS）やスケールセット（Azure）から一度に複数のデバイスを削除しないでください。また、自動スケールグループ（AWS）やスケールセット（Azure）

からデバイスを削除する前に、デバイスで **cluster disable** コマンドを実行することを推奨します。

- クラスタ内のデータノードと制御ノードを無効にする場合は、制御ノードを無効にする前にデータノードを無効にすることを推奨します。クラスタ内に他のデータノードがあるときに制御ノードが無効になっている場合は、いずれかのデータノードを制御ノードに昇格させる必要があります。ロールの変更はクラスタを妨害する可能性があることに注意してください。
- このガイドに記載されている Day 0 構成スクリプトでは、要件に応じて IP アドレスを変更し、カスタムインターフェイス名を指定して、CCL-Link インターフェイスのシーケンスを変更することができます。

クラスタリングのデフォルト

- cLACP システム ID は自動生成され、システムの優先順位はデフォルトでは 1 になっています。
- クラスタのヘルス チェック機能は、デフォルトで有効になり、ホールド時間は3秒です。デフォルトでは、すべてのインターフェイスでインターネット ヘルス モニタリングが有効になっています。
- 失敗したクラスタ制御リンクのクラスタ再結合機能が 5 分おきに無制限に試行されます。
- 失敗したデータインターフェイスのクラスタ自動再結合機能は、5 分後と、2 に設定された増加間隔で合計で 3 回試行されます。
- HTTP トラフィックでは、5 秒間の接続複製遅延がデフォルトで有効になっています。

AWS でクラスタを展開する

AWS にクラスタを展開する場合、手動で展開するか、スタックを展開する CloudFormation テンプレートを使用できます。AWS ゲートウェイロードバランサ、または Cisco Cloud Services Router などの非ネイティブのロード バランサでクラスタを使用できます。

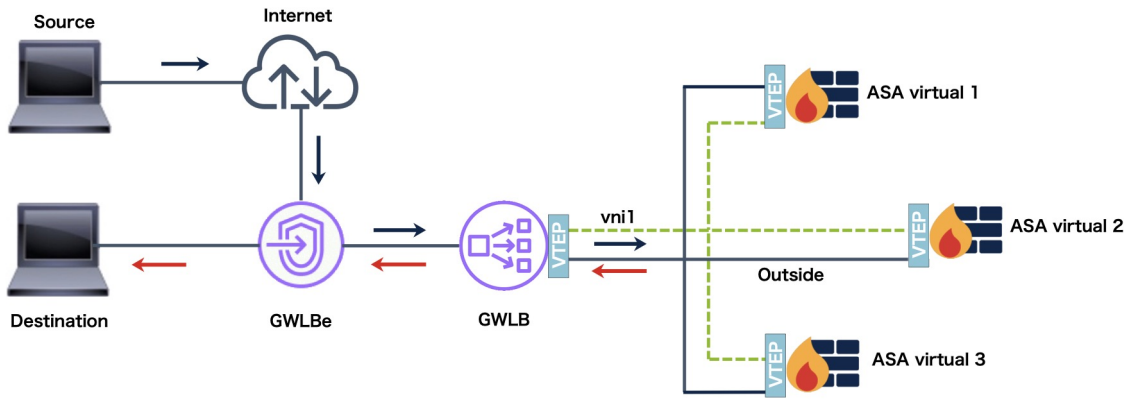
AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ

（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。ASA Virtual は、分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備え

たゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、ゲートウェイロードバランサのエンドポイントからゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の ASA Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、ゲートウェイロードバランサに送り返す（Uターントラフィック）前に検査します。ゲートウェイロードバランサは、トラフィックをゲートウェイロードバランサのエンドポイントと宛先に送り返します。

図 *57 : Geneve* シングルアームプロキシ



トポロジの例

AWS リージョン内の単一および複数の可用性ゾーンにおける自動スケーリングを使用した ASA 仮想 クラスタリング

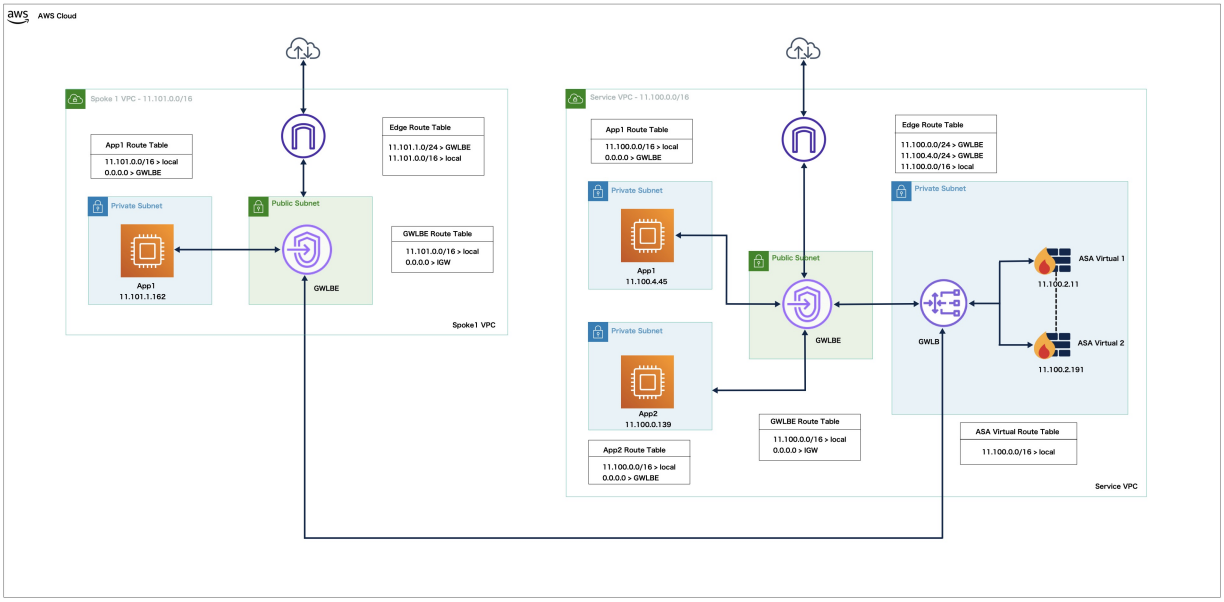
可用性ゾーンは、スタンドアロン データセンター、または独立して動作する AWS リージョン内の一連の独立したデータセンターです。各ゾーンには独自のネットワーク インフラストラクチャ、接続、および電源があり、1 つのゾーンで障害が発生しても他のゾーンには影響しません。冗長性と信頼性を向上させるために、企業は、ディザスタリカバリ計画で複数の可用性ゾーンを使用しています。

複数の可用性ゾーンにASA仮想を展開し、動的拡張を使用してクラスタリングを設定すると、インフラストラクチャの可用性と拡張性が大幅に向上します。さらに、同じリージョン内で複数の可用性ゾーンを利用することにより、冗長性が向上し、障害発生時の高可用性が保証されます。

クラスタ制御リンク（CCL）の IP 割り当てメカニズムを変更して、AWS 上の ASA 仮想 クラスタについて、単一と複数の可用性ゾーンの展開を両方サポートできます。次に示すトポロジは、自動スケーリング機能を備えた単一および複数の可用性ゾーンにおける着信と発信の両方のトラフィックフローを示しています。

単一の可用性ゾーンにおける自動スケーリングを使用した ASA 仮想 クラスタリング

GWLB に接続されているクラスタには、2 つの ASA 仮想 インスタンスがあります。

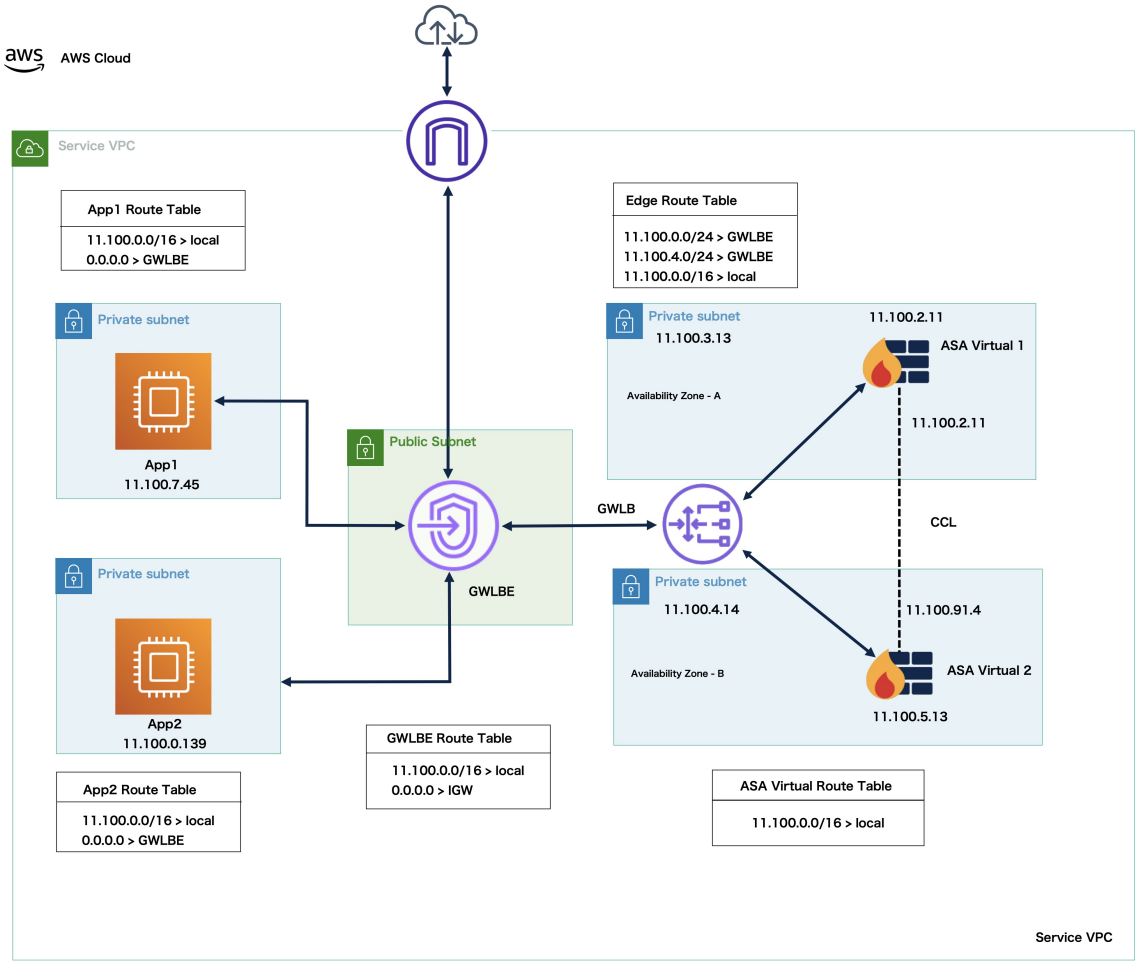


インターネットからの着信トラフィックは、GWLBエンドポイントに送られ、そこからGWLBにトラフィックが送信されます。その後、トラフィックはASA仮想クラスタに転送されます。トラフィックは、クラスタ内のASA仮想インスタンスによって検査された後、アプリケーション VM App1 に転送されます。

App1 からの発信トラフィックは、GWLB エンドポイント > GWLB > ASAv > GWLB > GWLB エンドポイント に送信され、そこからインターネットに送信されます。

自動スケーリング ソリューションを伴う複数の可用性ゾーンにおける自動スケーリングを使用した ASA 仮想 クラスタリング

GWLB に接続されている異なる可用性ゾーンのクラスタには、2 つの ASA 仮想 インスタンスがあります。

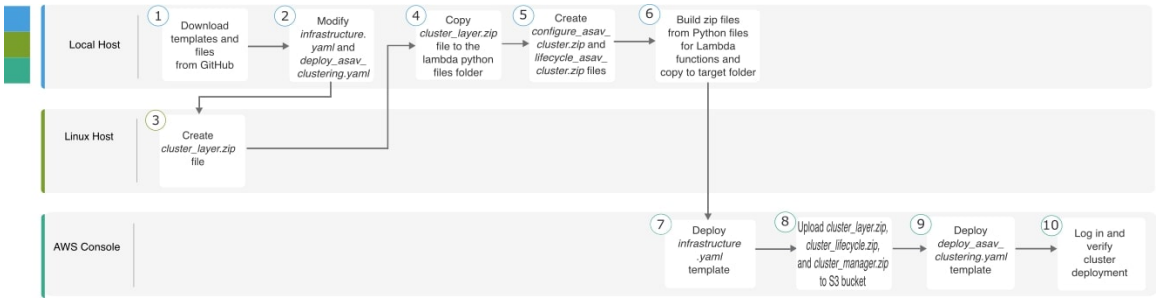


インターネットからの着信トラフィックは、GWLBエンドポイントに送られ、そこからGWLBにトラフィックが送信されます。その後、可用性ゾーンに基づいて、トラフィックがASA仮想クラスタにルーティングされます。トラフィックは、クラスタ内のASA仮想インスタンスによって検査された後、アプリケーションVM App1に転送されます。

AWS で ASA Virtual クラスタを展開するためのエンドツーエンドのプロセス

テンプレートベースの展開

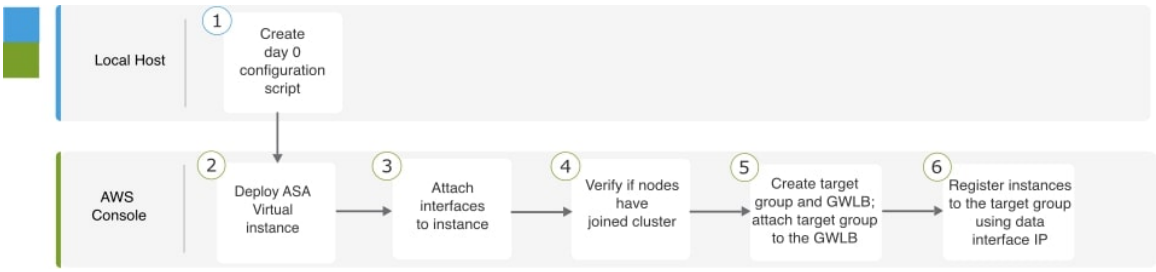
次のフローチャートは、AWS での ASA Virtual クラスタのテンプレートベース展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	GitHub からテンプレートとファイルをダウンロードします。
2	ローカルホスト	infrastructure.yaml および deploying_asav_clustering.yaml テンプレートを変更します。
3	Linux ホスト	cluster_layer.zip ファイルを作成します。
4	ローカルホスト	cluster_layer.zip ファイルを Lambda Python ファイルフォルダにコピーします。
5	ローカルホスト	configure_asav_cluster.zip および lifecycle_asav_cluster.zip ファイルを作成します。
6	ローカルホスト	Lambda 関数の Python ファイルから zip ファイルを作成し、ターゲットフォルダにコピーします。
7	AWS コンソール	Infrastructure.yaml テンプレートを展開します。
8	AWS コンソール	cluster_layer.zip、cluster_lifecycle.zip、および cluster_manager.zip を S3 バケットにアップロードします。
9	AWS コンソール	deploy_asav_clustering.yaml テンプレートを展開します。
10	AWS コンソール	ログインして、クラスタの展開を確認します。

手動展開

次のフローチャートは、AWS での ASA Virtual クラスタの手動展開のワークフローを示しています。



	ワークスペース	手順
1	ローカルホスト	Day 0 構成スクリプトを作成します。
2	AWS コンソール	ASA virtual インスタンスを展開します。
3	AWS コンソール	インスタンスにインターフェイスを接続します。
4	AWS コンソール	ノードがクラスタに参加しているかどうかを確認します。
5	AWS コンソール	ターゲットグループと GWLB を作成します。ターゲットグループを GWLB に割り当てます。
6	AWS コンソール	データインターフェイス IP を使用してターゲットグループにインスタンスを登録します。

テンプレート

以下のテンプレートは GitHub で入手できます。パラメータ値は、テンプレートで指定されたパラメータ名、デフォルト値、使用可能な値、および説明により自明です。

- infrastructure.yaml：インフラストラクチャ展開用のテンプレート。
- deploy_asav_clustering.yaml：クラスタ展開用のテンプレート。

（注） クラスタノードを展開する前に、サポートされている AWS インスタンスタイプのリストを確認してください。このリストは、deploy_asav_clustering.yaml テンプレートのパラメータ InstanceType に使用可能な値の下にあります。

AWS における GWLB を使用した ASA 仮想 クラスタリングのターゲットフェールオーバーの設定

AWS の ASA virtual クラスタリングは、ゲートウェイロードバランサ（GWLB）を使用して、指定された ASA virtual ノードにインスペクション用のネットワークパケットをバランシング

および転送します。GWLBは、ターゲットノードのフェールオーバーまたは登録解除が発生した場合に、ターゲットノードにネットワークパケットを送信し続けるように設計されています。

AWS でターゲットフェールオーバー機能を使用すると、計画メンテナンス中またはターゲットノードの障害時にノードの登録が解除された場合に、GWLBがネットワークパケットを正常なターゲットノードにリダイレクトできるようになります。この機能ではクラスタのステートフル フェールオーバーを利用しています。

（注） GWLB が SSH、SCP、CURL、またはその他のプロトコルを使用してトラフィックをルーティングしている間にターゲットノードに障害が発生した場合、正常なターゲットへのトラフィックのリダイレクトに遅延が発生する可能性があります。この遅延は、トラフィックフローの再調整と再ルーティングが原因で発生します。

AWS では、AWS ELB API または AWS コンソールを介してターゲットフェールオーバーを設定できます。

- AWS API（AWS Elastic Load Balancing（ELB）API 内）の modify-target-group-attributes で、次の2つの新しいパラメータを変更することにより、フロー処理の動作を定義できます。
  - target_failover.on_unhealthy：ターゲットが正常でなくなった場合に GWLB がネットワークフローをどのように処理するかを定義します。
  - target_failover.on_deregistration：ターゲットが登録解除された場合に GWLB がネットワークフローをどのように処理するかを定義します。

  次のコマンドは、これら2つのパラメータを定義するサンプルの API パラメータ設定を示しています。

```
aws elbv2 modify-target-group-attributes \
--target-group-arn arn:aws:elasticloadbalancing:…/my-targets/73e2d6bc24d8a067 \
--attributes \
Key=target_failover.on_unhealthy, Value=rebalance[no_rebalance] \
Key=target_failover.on_deregistration, Value=rebalance[no_rebalance]
```

  詳細については、AWS のマニュアルの「TargetGroupAttribute」を参照してください。

- AWS コンソール：EC2 コンソールでは、次のオプションを設定することにより、[ターゲットグループ（Target Group）]ページの[ターゲットフェールオーバー（Target Failover）]オプションを有効にすることができます。
  - ターゲットグループの属性を編集する
  - ターゲットフェールオーバーを有効にする
  - 再調整フローを確認する

  ターゲットフェールオーバーを有効にする方法の詳細については、「ターゲットフェールオーバー機能を有効にする」を参照してください。

CloudFormation テンプレートを使用した AWS へのスタックの展開

CloudFormation テンプレートを使用して AWS にスタックを展開します。

始める前に

- Python 3 をインストールした Linux コンピューターが必要です。

手順

ステップ 1 テンプレートを準備します。

a) GitHub リポジトリをローカルフォルダに複製します。https://github.com/CiscoDevNet/cisco-asav/tree/master/cluster/aws を参照してください。

b) 必要なパラメータを使用して、**infrastructure.yaml** および **deploy_asav_clustering.yaml** を変更します。

c) **cluster_layer.zip** という名前のファイルを作成して、重要な Python ライブラリを Lambda 関数に提供します。

cluster_layer.zip ファイルを作成するには、Python 3.9 がインストールされた Amazon Linux を使用することをお勧めします。

（注）
Amazon Linux 環境が必要な場合は、Amazon Linux 2023 AMI を使用して EC2 インスタンスを作成するか、Amazon Linux の最新バージョンを実行する AWS Cloudshell を使用できます。

cluster-layer.zip ファイルを作成するには、最初に Python ライブラリパッケージの詳細で構成される **requirements.txt** ファイルを作成してから、シェルスクリプトを実行する必要があります。

1. Python パッケージの詳細を指定して、**requirements.txt** ファイルを作成します。

   以下は、**requirements.txt** ファイルで指定するサンプルパッケージの詳細です。

```
$ cat requirements.txt
pycryptodome
paramiko
requests
scp
jsonschema
cffi
zipp
importlib-metadata
```

2. 次のシェルスクリプトを実行して、**cluster_layer.zip** ファイルを作成します。

```
$ pip3 install --platform manylinux2014_x86_64
--target=./python/lib/python3.9/site-packages
--implementation cp --python-version 3.9 --only-binary=:all:
--upgrade -r requirements.txt
$ zip -r cluster_layer.zip ./python
```

（注）
インストール中にurllib3や暗号化などの依存関係の競合エラーが発生した場合は、競合するパッケージを推奨バージョンと一緒に **requirements.txt** ファイルに含めることをお勧めします。その後、インストールを再度実行して競合を解決できます。

d) 結果の **cluster_layer.zip** ファイルを Lambda Python ファイルフォルダにコピーします。
e) **configure_asav_cluster.zip** および **lifecycle_asav_cluster.zip** ファイルを作成します。

make.py ファイルは、複製されたリポジトリの最上位ディレクトリにあります。これにより、python ファイルが Zip ファイルに圧縮され、ターゲットフォルダにコピーされます。

python3 make.py build

（注）
クラスタを展開する前に、ASAvクラスタリング自動スケール展開に必要なVPC、サブネット、S3バケットなどのインフラストラクチャ要件に合わせて、AWS CFTテンプレートファイル（**infrastructure.yaml** および **deploy_asav_clustering.yaml**）をカスタマイズしていることを確認します。

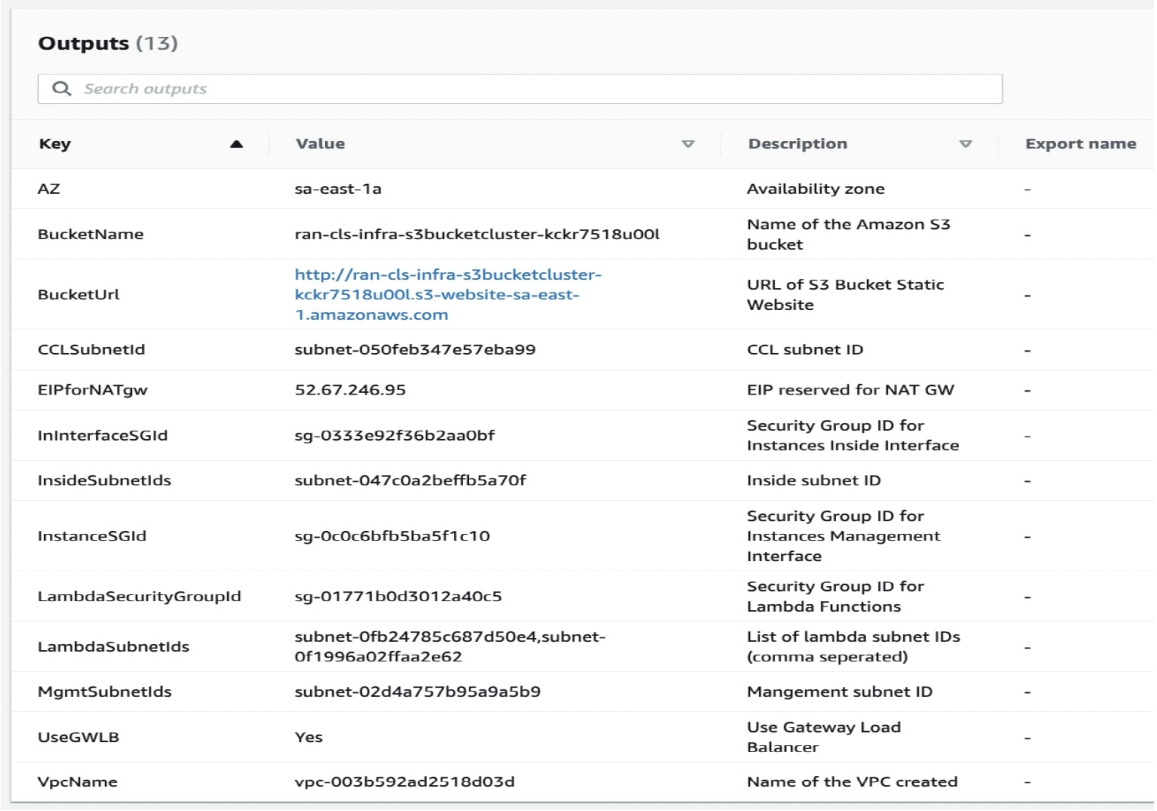
ステップ 2 **Infrastructure.yaml** を展開し、クラスタ展開の出力値をメモします。インフラストラクチャ スタックを展開する前に、使用するAWSリージョンと可用性ゾーンを特定することが重要です。各 AWS リージョンには異なる可用性ゾーンと VPC インフラストラクチャのセットがあるため、展開に適したリージョンと可用性ゾーンを選択することが不可欠です。

a) AWS コンソールで、[CloudFormation] に移動し、[新しいリソース（標準）を使用（With new resources(standard)）] を選択して、[スタックの作成（Create stack）] をクリックします。
b) **[テンプレートファイルのアップロード（Upload a template file）]** を選択し、**[ファイルの選択（Choose file）]** をクリックして、ターゲットフォルダから **infrastructure.yaml** を選択します。
c) [次へ（Next）] をクリックして、必要な情報を入力します。
d) クラスタの一意の**クラスタ名**と**クラスタ番号**を入力します。
e) [可用性ゾーン（Availability Zone）] リストから可用性ゾーンを選択します。このフィールドには、ClusterFormation テンプレートを使用してインフラストラクチャ スタックを展開するために選択した AWS リージョンに基づく可用性ゾーンのみが表示されます。
f) **[内部サブネット CIDR（Inside subnet CIDR）]** にカンマで区切られた事前定義値のサブネット CIDR を入力します。
g) Lambda が AZ 間で通信するために必要な可用性ゾーンを [Lambda AZ のリスト（List of Lambda AZs）] から選択します。
h) **[次へ（Next）]**、**[スタックの作成（Create stack）]** の順にクリックします。

インフラストラクチャ スタックの展開ステータスを示すメッセージ「CREATE_COMPLETE」が表示されます。

i) 展開が完了したら、[出力（Outputs）] に移動し、S3 の **BucketName** を書き留めます。

図 *58 : Infrastructure.yaml* の出力



Outputs (13)

Search outputs

Key	Value	Description	Export name
AZ	sa-east-1a	Availability zone	-
BucketName	ran-cls-infra-s3bucketcluster-kckr7518u00l	Name of the Amazon S3 bucket	-
BucketUrl	http://ran-cls-infra-s3bucketcluster-kckr7518u00l.s3-website-sa-east-1.amazonaws.com	URL of S3 Bucket Static Website	-
CCLSubnetId	subnet-050feb347e57eba99	CCL subnet ID	-
EIPforNATgw	52.67.246.95	EIP reserved for NAT GW	-
InInterfaceSGId	sg-0333e92f36b2aa0bf	Security Group ID for Instances Inside Interface	-
InsideSubnetIds	subnet-047c0a2beffb5a70f	Inside subnet ID	-
InstanceSGId	sg-0c0c6bfb5ba5f1c10	Security Group ID for Instances Management Interface	-
LambdaSecurityGroupId	sg-01771b0d3012a40c5	Security Group ID for Lambda Functions	-
LambdaSubnetIds	subnet-0fb24785c687d50e4,subnet-0f1996a02ffaa2e62	List of lambda subnet IDs (comma seperated)	-
MgmtSubnetIds	subnet-02d4a757b95a9a5b9	Mangement subnet ID	-
UseGWLB	Yes	Use Gateway Load Balancer	-
VpcName	vpc-003b592ad2518d03d	Name of the VPC created	-

ステップ 3 **cluster_layer.zip**、**configure_asav_cluster.zip**、および **lifecycle_asav_cluster.zip** を **infrastructure.yaml** で作成した S3 バケットにアップロードします。

ステップ 4 **deploy_asav_clustering.yaml** を展開します。

a) **[CloudFormation]** に移動し、**[新しいリソース（標準）を使用（With new resources(standard)）]** を選択して、**[スタックの作成（Create stack）]** をクリックします。

b) **[テンプレートファイルのアップロード（Upload a template file）]** を選択し、**[ファイルの選択（Choose file）]** をクリックして、ターゲットフォルダから **deploy_asav_clustering.yaml** を選択します。

c) [次へ（Next）] をクリックして、必要な情報を入力します。

d) 次のクラスタとインフラストラクチャの設定情報を入力します。

パラメータ	使用できる値/タイプ	説明
クラスタの設定		
クラスタ名	文字列	これはクラスタ名のプレフィックスです。クラスタ番号がサフィックスとして追加されます。

パラメータ	使用できる値/タイプ	説明
クラスタ番号	文字列	これはクラスタ番号であり、クラスタ名（msa-asa-infra）のサフィックスとして追加されます。たとえば、この値が「**1**」の場合、グループ名は *msa-asa-infra-1* になります。 1 桁以上 3 桁以下である必要があります。デフォルト：1。
クラスタ サイズ	数字	これは、クラスタ内の ASA Virtual ノードの総数です。 最小値：1 最大値：16
インフラストラクチャの詳細		
可用性ゾーンの数	文字列	これは、ASA Virtual が展開される可用性ゾーンの合計数です（可用性ゾーンの数は 1 ～ 3 でリージョンによって異なります）。 サブネットは、これらの可用性ゾーンに作成されます。 このリストで使用可能な可用性ゾーンは、クラスタの展開用に選択されたリージョンに基づいています。 **（注）** Lambda は、2 つの可用性ゾーンにわたって作成されます。これらのパラメータに基づいて、管理用サブネットと内部用サブネットが 3 つの可用性ゾーンにまたがって作成されます。
有効な可用性ゾーンリストの入力	文字列	可用性ゾーンリストは、展開するリージョンに基づきます。 [可用性ゾーン（Availability Zone）] リストで、有効な可用性ゾーン（1 つの可用性ゾーン、2 つの可用性ゾーン、または 3 つの可用性ゾーン）を選択します。 カウントは、可用性ゾーン数のパラメータの値と一致する必要があります。
クラスタの電子メール通知	文字列	クラスタイベントの電子メールの送信先となる電子メールアドレス。この電子メール通告を受信するには、サブスクリプション電子メール要求を承認する必要があります。 例：admin@company.com

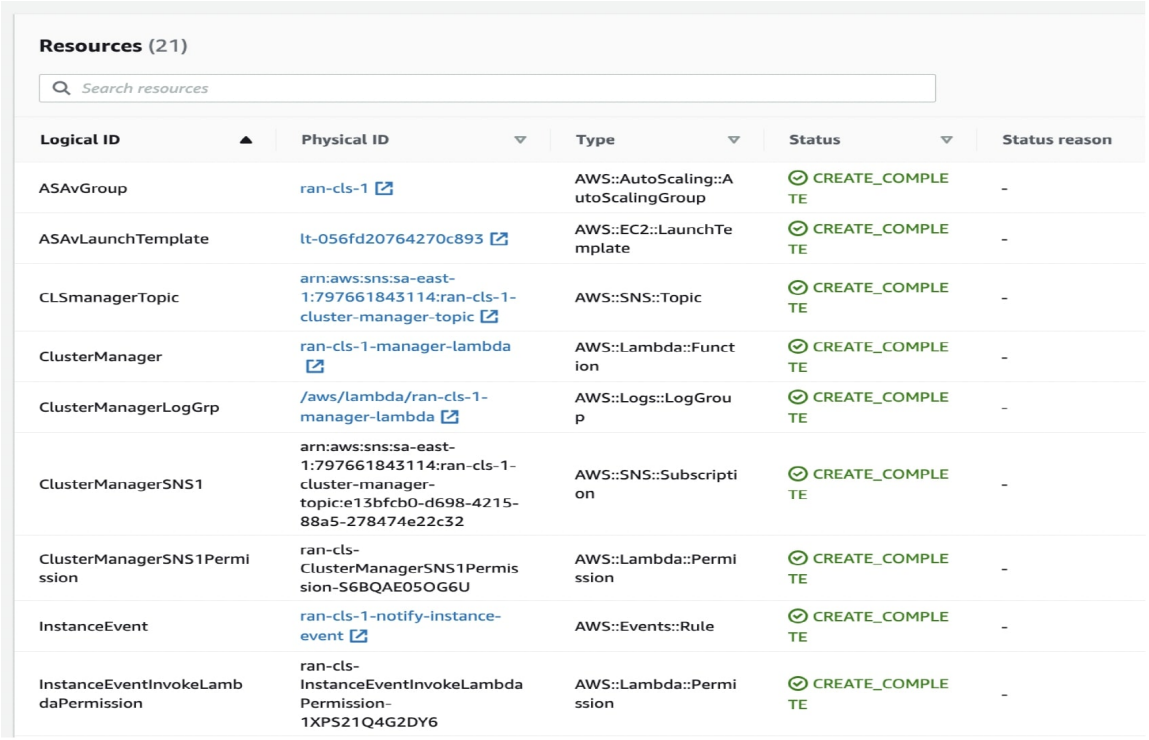
パラメータ	使用できる値/タイプ	説明
GWLB の設定		
GWLB エンドポイントの展開	文字列	**[はい（Yes）]** をクリックして GWLB エンドポイントを展開します。 デフォルトでは、値は [いいえ（No）] に設定されています。
GWLBE の VPC ID	文字列	ゲートウェイロードバランサのエンドポイントを展開する VPC を入力します。 （注） GWLBエンドポイントを展開しない場合は、このフィールドに値を入力しないでください。
GWLBE のサブネット ID	文字列	サブネット ID を 1 つだけ入力します。 （注） GWLBエンドポイントを展開しない場合は、このフィールドに値を入力しないでください。 サブネットが正しい VPC および指定した可用性ゾーンに属していることを確認します。
ターゲットフェールオーバー	文字列	ターゲットに障害が発生した場合または登録解除された場合のターゲット フェールオーバー サポートを有効にします（このパラメータの値はデフォルトで [再調整（rebalance）] に設定されています）。 • [再調整なし（no_rebalance）] : 既存のフローを障害が発生したターゲットに送信し、新しいフローを正常なターゲットに送信し、後方互換性を確保します。 • [再調整（rebalance）] : 新しいフローが正常なターゲットに送られるようにしながら、既存のフローを再配布します。
GWLB の正常性チェックポートの入力	文字列	GWLB の正常性チェックポートを入力します。 （注） デフォルトでは、このポートはトラフィックに使用されません。 指定した値が有効な TCP ポートであることを確認します。デフォルト：80

パラメータ	使用できる値/タイプ	説明
Cisco ASAv インスタンスの設定		
ASAv インスタンスタイプ	文字列	Cisco ASAv EC2 インスタンスタイプ。 選択したインスタンスタイプが AWS リージョンでサポートされていることを確認します。 デフォルトでは、**c5.xlarge** が選択されています。
ASAv インスタンスライセンス タイプ	文字列	Cisco ASAv EC2 インスタンス ライセンス タイプを選択します。**AMI-ID** パラメータに入力する AMI ID が同じライセンスタイプであることを確認します。 デフォルトでは、[BYOL] が選択されています。
ASAv スマート ソフトウェア ライセンス トークン	文字列	（オプション）ASAv デバイスを登録するためのシスコ スマート ソフトウェア ライセンス トークンを指定します。
ASAv AMI-ID	文字列	リージョン、バージョン、およびライセンスタイプ（BYOL または PAYG）に従って正しい AMI ID を選択します。 ASAv バージョン 9.19 以降ではクラスタリングがサポートされ、ASAv バージョン 9.22 以降では自動スケーリングとマルチ AZ の機能拡張がサポートされます。 タイプ：AWS::EC2::Image::Id デフォルト：ami-024f546cb9cbae1bb
ASAv パスワード	文字列	ASAv インスタンスのパスワード。 ASAv にアクセスできるようになると、パスワードがアクティブになります。 文字数は 8 文字以上にする必要があります。パスワードには、プレーンテキストのパスワードまたは KMS 暗号化パスワードを使用できます。
CPU に関するしきい値	カンマ区切りリスト	（任意）ゼロ以外の下限しきい値と上限しきい値を指定すると、スケールポリシーが作成されます。(0,0) を選択すると、CPU スケーリングアラームまたはポリシーは作成されません。評価ポイントとデータポイントは、デフォルト値または推奨値にします。

パラメータ	使用できる値/タイプ	説明
		デフォルトでは、このテンプレートでは**自動スケール**が有効になっています。自動スケールは展開後に無効にできます。

e) [次へ（Next）] をクリックします。
f) クリックしてすべての AWS CloudFormation オプションを確認します。
g) [送信（Submit）] をクリックしてクラスタを展開します。
h) **[次へ（Next）]**、**[スタックの作成（Create stack）]** の順にクリックします。

図 *59 :* 展開されたリソース



Resources (21)

Search resources

Logical ID	Physical ID	Type	Status	Status reason
ASAvGroup	ran-cls-1	AWS::AutoScaling::AutoScalingGroup	CREATE_COMPLETE	-
ASAvLaunchTemplate	lt-056fd20764270c893	AWS::EC2::LaunchTemplate	CREATE_COMPLETE	-
CLSmanagerTopic	arn:aws:sns:sa-east-1:797661843114:ran-cls-1-cluster-manager-topic	AWS::SNS::Topic	CREATE_COMPLETE	-
ClusterManager	ran-cls-1-manager-lambda	AWS::Lambda::Function	CREATE_COMPLETE	-
ClusterManagerLogGrp	/aws/lambda/ran-cls-1-manager-lambda	AWS::Logs::LogGroup	CREATE_COMPLETE	-
ClusterManagerSNS1	arn:aws:sns:sa-east-1:797661843114:ran-cls-1-cluster-manager-topic:e13bfcb0-d698-4215-88a5-278474e22c32	AWS::SNS::Subscription	CREATE_COMPLETE	-
ClusterManagerSNS1Permission	ran-cls-ClusterManagerSNS1Permission-S6BQAE05OG6U	AWS::Lambda::Permission	CREATE_COMPLETE	-
InstanceEvent	ran-cls-1-notify-instance-event	AWS::Events::Rule	CREATE_COMPLETE	-
InstanceEventInvokeLambdaPermission	ran-cls-InstanceEventInvokeLambdaPermission-1XPS21Q4G2DY6	AWS::Lambda::Permission	CREATE_COMPLETE	-

ステータスが CREATE_IN_PROGRESS から CREATE COMPLETE に変わり、展開が成功したことが示されます。

ステップ 5 いずれかのノードにログインし、**show cluster info** コマンドを入力して、クラスタの展開を確認します。

```
show cluster info

Cluster oneclicktest-cluster: On
Interface mode: individual
Cluster Member Limit : 16
```

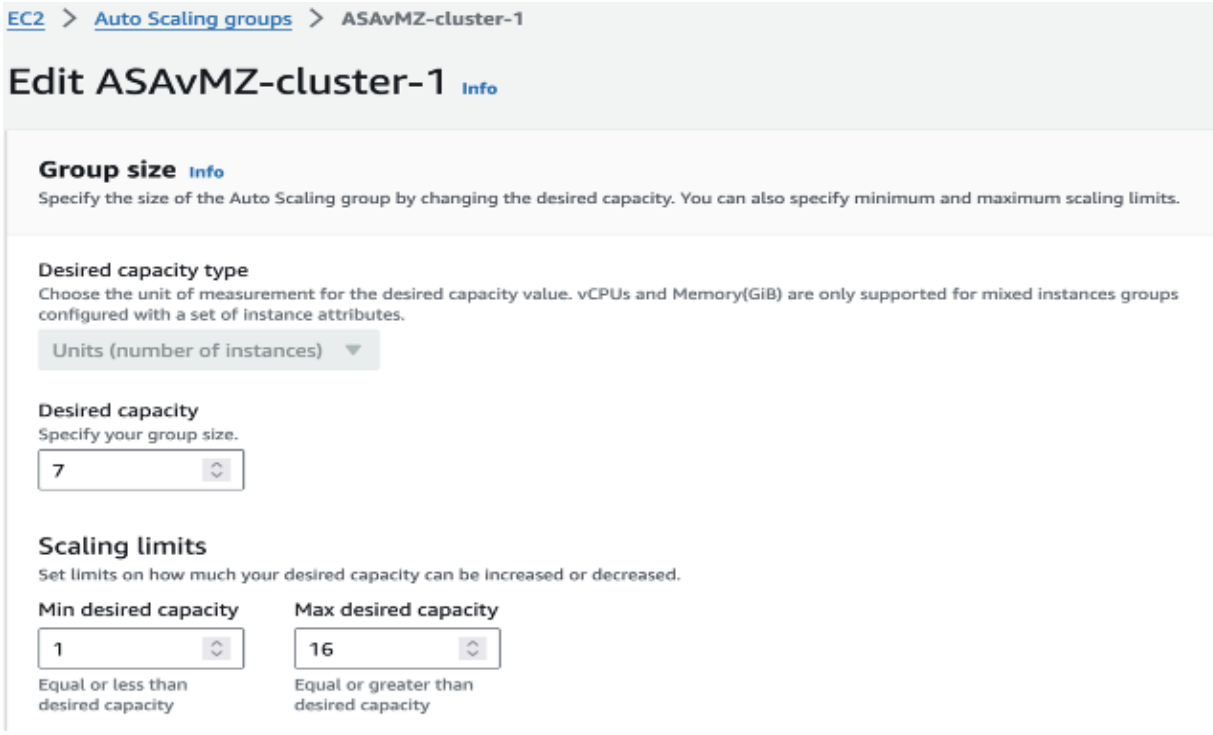
```
This is "200" in state CONTROL_NODE
ID : 0
Version : 9.19.1
Serial No.: 9AU42EN5D1E
CCL IP : 1.1.1.200
CCL MAC : 4201.0a0a.0fc7
Module : ASAv
Resource : 4 cores / 8192 MB RAM
Last join : 15:26:22 UTC Jul 17 2022
Last leave: N/A
Other members in the cluster:
Unit "204" in state DATA_NODE
ID : 1
Version : 9.19.1
Serial No.: 9AJ9N46947R
CCL IP : 1.1.1.204
CCL MAC : 4201.0a0a.0fcb
Module : ASAv
Resource : 4 cores / 8192 MB RAM
Last join : 16:57:42 UTC Jul 17 2022
Last leave: 16:03:25 UTC Jul 17 2022
```

自動スケーリングのパラメータ設定

展開が完了したら、自動スケーリンググループの **[最小容量（Minimum capacity）]**、**[最大容量（Maximum capacity）]**、および **[必要な容量（Desired capacity）]** を指定する必要があります。自動スケーリング機能を検証する必要があります。

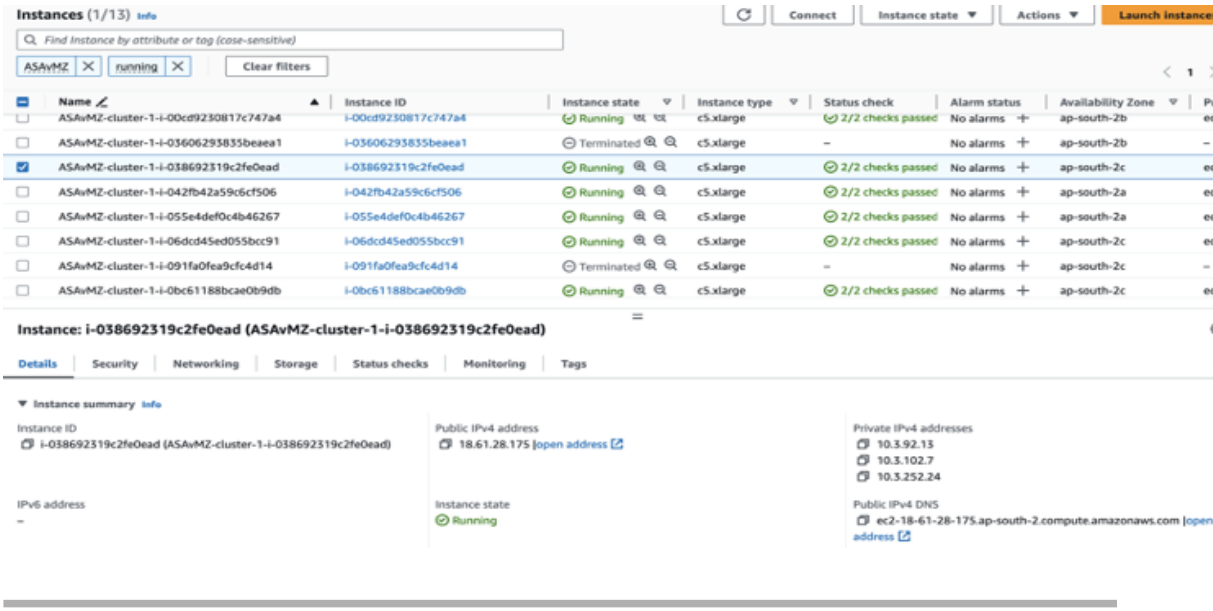
手順

ステップ 1 AWS コンソールから、**[サービス（Services）]** > **[EC2]** > **[自動スケーリンググループ（Auto Scaling groups）]** > **作成された ClusterAutoscale グループ**の順に選択します。



ステップ 2 [必要な容量（Desired capacity）] を設定してから、[スケーリング制限（Scaling limits）] 容量を設定します。

ステップ 3 CPU メトリック データが使用可能かどうかと、AWS Cloudwatch アラームでスケーリングが予期したとおりに発生しているかどうかを確認します。



スタックの更新による ASA Virtual クラスタリングでの IMDSv2 必須モードの設定

AWS にすでに展開されている ASA Virtual の Auto Scale グループ インスタンスの IMDSv2 必須モードを設定できます。

Before you begin

IMDSv2 必須モードは、ASA Virtual バージョン 9.20.3 以降でのみサポートされています。展開に IMDSv2 必須モードを設定する前に、既存のインスタンスのバージョンが IMDSv2 API と互換性がある（バージョン 9.20.3 にアップグレードされている）ことを確認してください。

Procedure

ステップ 1 AWS コンソールで、**[CloudFormation]** に移動し、**[スタック（Stacks）]** をクリックします。

ステップ 2 最初に展開されたクラスタリングインスタンスのスタックを選択します。

ステップ 3 **[更新（Update）]**をクリックします。

ステップ 4 **[スタックの更新（Update stack）]** ページで、**[既存のテンプレートの置換（Replace existing template）]** をクリックします。

ステップ 5 [テンプレートの指定（Specify template）] セクションで、[テンプレートファイルのアップロード（Upload a template file）] をクリックします。

ステップ 6 IMDSv2 をサポートするテンプレートを選択してアップロードします。

ステップ 7 テンプレートの入力パラメータの値を指定します。

ステップ 8 スタックを更新します。

AWS でのクラスタの手動展開

クラスタを手動で展開するには、day0 構成を準備し、各ノードを展開します。

AWS 向け Day 0 構成の作成

次のコマンドを使用して各クラスタノードのブートストラップ設定を指定します。

ゲートウェイロードバランサの例

次の実行コンフィギュレーションの例では、U ターントラフィック用の 1 つの Geneve インターフェイスと、クラスタ制御リンク用の 1 つの VXLAN インターフェイスを備えたゲートウェイロードバランサの構成を作成します。

```
cluster interface-mode individual force
policy-map global_policy
class inspection_default
no inspect h323 h225
no inspect h323 ras
no inspect rtsp
```

```
no inspect skinny

int m0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
no shut

interface TenGigabitEthernet0/0
nameif geneve-vtep-ifc
security-level 0
ip address dhcp
no shutdown

interface TenGigabitEthernet0/1
nve-only cluster
nameif ccl_link
security-level 0
ip address dhcp
no shutdown

interface vni1
description Clustering Interface
segment-id 1
vtep-nve 1

interface vni2
proxy single-arm
nameif ge
security-level 0
vtep-nve 2

object network ccl_link
range 10.1.90.4 10.1.90.254 //Mandatory user input, use same range on all nodes
object-group network cluster_group
network-object object ccl_link
nve 2
encapsulation geneve
source-interface geneve-vtep-ifc
nve 1
encapsulation vxlan
source-interface ccl_link
peer-group cluster_group

cluster group asav-cluster // Mandatory user input, use same cluster name on all nodes
local-unit 1 //Value in bold here must be unique to each node
cluster-interface vni1 ip 1.1.1.1 255.255.255.0 //Value in bold here must be unique to
each node
priority 1
enable noconfirm

mtu geneve-vtep-ifc 1806
mtu ccl_link 1960
aaa authentication listener http geneve-vtep-ifc port 7575 //Use same port number on all
 nodes
jumbo-frame reservation
wr mem
```

（注） AWS ヘルスチェックの設定では、ここで設定した **aaa authentication listener http** ポートを必ず指定してください。

非ネイティブロードバランサの例

次の例では、管理、内部、および外部インターフェイスと、クラスタ制御リンク用の VXLAN インターフェイスを使用して、非ネイティブロードバランサ用の構成を作成します。

```
cluster interface-mode individual force
interface Management0/0
management-only
nameif management
ip address dhcp

interface GigabitEthernet0/0
no shutdown
nameif outside
ip address dhcp

interface GigabitEthernet0/1
no shutdown
nameif inside
ip address dhcp

interface GigabitEthernet0/2
nve-only cluster
nameif ccl_link
ip address dhcp
no shutdown

interface vni1
description Clustering Interface
segment-id 1
vtep-nve 1

jumbo-frame reservation
mtu ccl_link 1654
object network ccl_link
range 10.1.90.4 10.1.90.254          //mandatory user input
object-group network cluster_group
network-object object ccl_link

nve 1
encapsulation vxlan
source-interface ccl_link
peer-group cluster_group

cluster group asav-cluster          //mandatory user input
local-unit 1                        //mandatory user input
cluster-interface vni1 ip 10.1.1.1 255.255.255.0  //mandatory user input
priority 1
enable
```

（注） 上記の設定をコピーして貼り付ける場合は、設定から **//mandatory user input** を必ず削除してください。

クラスタノードの展開

クラスタを形成するためにクラスタノードを展開します。

手順

ステップ 1 必要な数のインターフェイス（ゲートウェイロードバランサ（GWLB）を使用している場合は 3 つのインターフェイス、非ネイティブロードバランサを使用している場合は 4 つのインターフェイス）でクラスタの Day 0 構成を使用することにより、ASA Virtual インスタンスを展開します。これを行うには、[インスタンスの詳細設定（Configure Instance Details）] > [高度な詳細（Advanced Details）] セクションで、クラスタの Day 0 構成に貼り付けます。

（注）
次の順序でインスタンスにインターフェイスを接続していることを確認します。

- AWS ゲートウェイロードバランサの 3 つのインターフェイス：管理、外部、クラスタ制御リンク。
- 非ネイティブロードバランサの 4 つのインターフェイス：管理、内部、外部、クラスタ制御リンク。

AWS での ASA Virtual の展開の詳細については、「Deploy the ASA Virtual on AWS」を参照してください。

ステップ 2 ステップ 1 を繰り返して、必要な数の追加ノードを展開します。

ステップ 3 ASA Virtual コンソールで **show cluster info** コマンドを使用して、すべてのノードがクラスタに正常に参加したかどうかを確認します。

ステップ 4 AWS ゲートウェイロードバランサを設定します。

a) ターゲットグループと GWLB を作成します。

b) ターゲットグループを GWLB に割り当てます。

（注）
正しいセキュリティグループ、リスナー設定、およびヘルスチェック設定を使用するように GWLB を設定していることを確認します。

c) IP アドレスを使用して、データインターフェイス（内部インターフェイス）をターゲットグループに登録します。詳細については、「Create a Gateway Load Balancer」を参照してください。

AWS での ASA virtual のターゲットフェールオーバーの有効化

ASA virtual のデータインターフェイスは、AWS の GWLB のターゲットグループに登録されます。ASA virtual クラスタリングでは、各インスタンスはターゲットグループに関連付けられています。GWLB は、ターゲットグループのターゲットノードとして識別または登録されているこの正常なインスタンスにトラフィックを負荷分散して送信します。

始める前に

手動で、または CloudFormation テンプレートを使用して、AWS で ASA virtual スタックを展開している必要があります。

CloudFormation テンプレートを使用してクラスタを展開する場合、クラスタ展開ファイル `deploy_asav_clustering.yaml` の [GWLBの設定（GWLB Configuration）] セクションで使用可能な [再調整（rebalance）] 属性を割り当てることにより、[ターゲットフェールオーバー（Target Failover）] のパラメータを有効にすることもできます。テンプレートでは、このパラメータの値はデフォルトで [再調整（rebalance）] に設定されています。ただし、AWS コンソールでは、このパラメータのデフォルト値は [再調整なし（no_rebalance）] に設定されています。

それぞれの説明は次のとおりです。

- 再調整なし（no_rebalance）：GWLB は、機能していないターゲットまたは登録解除されたターゲットにネットワークフローを送信し続けます。
- **再調整（rebalance）**：既存のターゲットが機能していないか登録解除された場合、GWLB はネットワークフローを別の正常なターゲットに送信します。

AWS でのスタックの展開については、以下を参照してください。

- AWS でのクラスタの手動展開
- CloudFormation テンプレートを使用した AWS へのスタックの展開

手順

ステップ 1 AWS コンソールで、[サービス（Services）] > [EC2] に移動します。

ステップ 2 [ターゲットグループ（Target Groups）] をクリックして、ターゲットグループのページを表示します。

ステップ 3 ASA virtual インスタンスの IP アドレスが登録されているターゲットグループを選択して開きます。ターゲットグループの詳細ページが表示されます。

ステップ 4 [属性（Attributes）] メニューに移動します。

ステップ 5 [編集（Edit）] をクリックして属性を編集します。

ステップ 6 [フローの再調整（Rebalance Flows）] スライダボタンを右に切り替えます。これによりターゲットフェールオーバーが有効になり、ターゲットフェールオーバーや登録解除の際に既存のネットワークパケットを再調整して正常なターゲットノードに転送するように GWLB が設定されます。

Azure でクラスタを展開する

Azure サービスチェーンでは、ASA virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。Azure での ASA virtual インスタンスのクラスタリングは、単一のデバイスとして抽象化することにより、マルチノード ASAv のスループットをスケールアップするのに役立ちます。

ASAv は、2 つの論理インターフェイスで構成されています。インターネットに向けた**外部インターフェイス**と、顧客サービスに向けた**内部インターフェイス**です。これらのインターフェイスは、ペアリングされたプロキシで VXLAN セグメントを利用することにより、ASAv の単一のネットワーク インターフェイス カード（NIC）で定義されます。

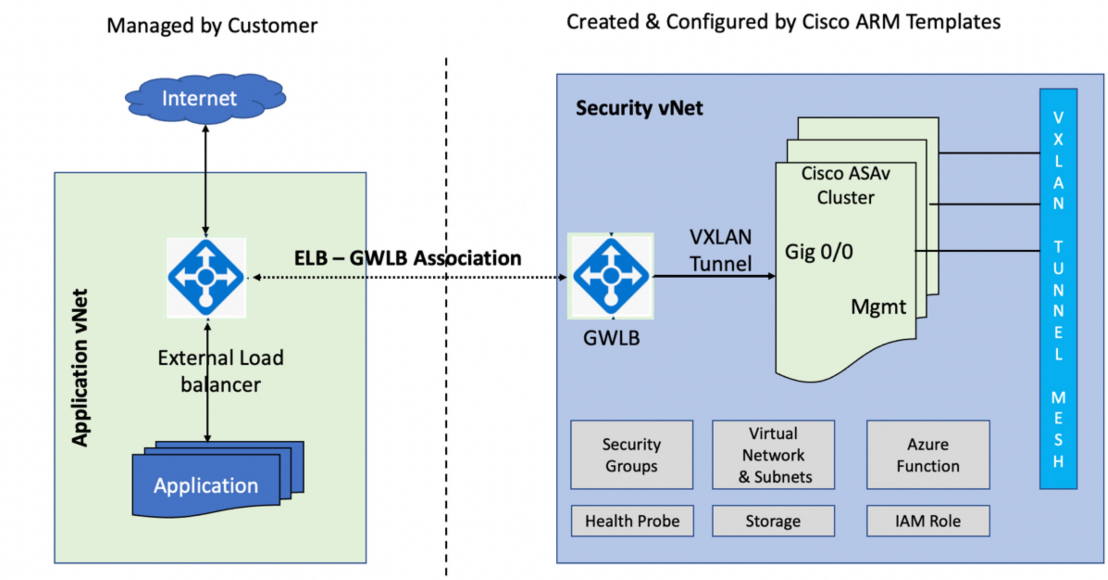
Azure Gateway Load Balancer について

Azure Gateway Load Balancer（GWLB）は、トラフィック検査のために VXLAN セグメントを介して ASAv にルーティングすることにより、着信トラフィックと発信トラフィックのバランスを取り、管理するのに役立ちます。ASAv クラスタ環境では、Azure GWLB はトラフィックの負荷に応じて ASAv ノードのスループットレベルを自動的にスケールアップします。GWLB を使用すると、ルートを手動で更新することなく、ネットワーク仮想アプライアンスへの対称フローまたは一貫性のあるルートを確保できます。この機能により、パケットは同じネットワークパスを双方向で通過できます。

次の図は、外部 VXLAN セグメント上のパブリック ゲートウェイ ロードバランサから Azure GWLB に転送されるトラフィックを示しています。**ゲートウェイロードバランサ**は、まず複数の ASAv の間でトラフィックのバランスを取り、トラフィックをドロップするか、内部の VXLAN セグメント上の GWLB に送り返す前に検査します。Azure GWLB は、トラフィックをパブリック ゲートウェイ ロードバランサと宛先に送り返します。

次の図は、Azure の GWLB と ASAv 間のネットワークフローを示しています。

図 *60 : GWLB* を使用した *Azure* での *ASAv* クラスタリング



Azure でのクラスタ展開について

カスタマイズされた Azure Resource Manager（ARM）テンプレートを使用して、Azure GWLB の仮想マシンスケールセットを展開できます。

クラスタ展開の後、デイゼロ設定を使用して、または Azure portal の Function アプリを介して、クラスタ上の各ノードを手動で設定できます。

Azure Resource Manager テンプレートを使用したクラスタの展開

Azure Resource Manager（ARM）テンプレートを使用してクラスタを形成するようにクラスタノード（仮想マシンスケールセット）を展開します。

始める前に

- Azure クラスタを手動で作成するには、デイゼロ設定で構成テキストファイルを準備する必要があります。「Prepare Configuration File for Cluster deployment on Azure」を参照してください。

手順

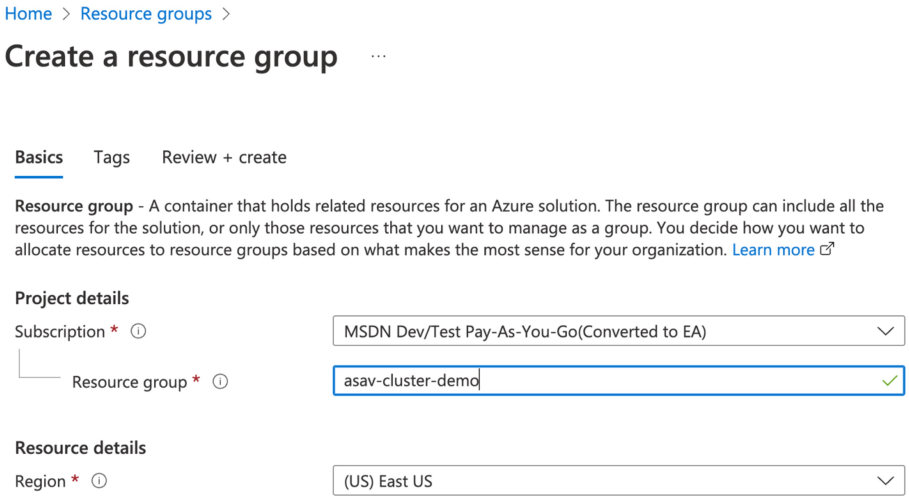
ステップ 1 テンプレートを準備します。

a) GitHub リポジトリをローカルフォルダに複製します。https://github.com/CiscoDevNet/cisco-asav/tree/master/cluster/azure を参照してください。

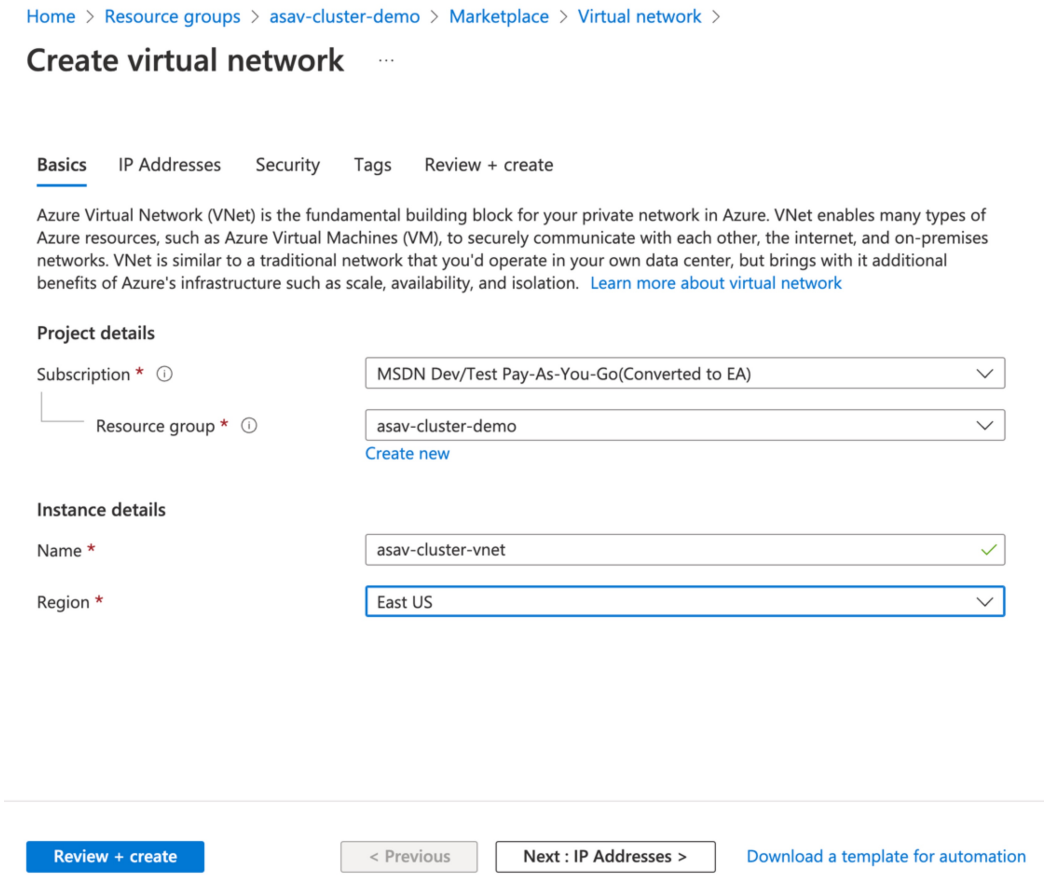
b) GWLB の場合、`azure_asav_gwlb_cluster.json` と `asav-gwlb-cluster-config.txt` を必要なパラメータで変更します。

ステップ 2 Azure ポータル：https://portal.azure.com にログインします。

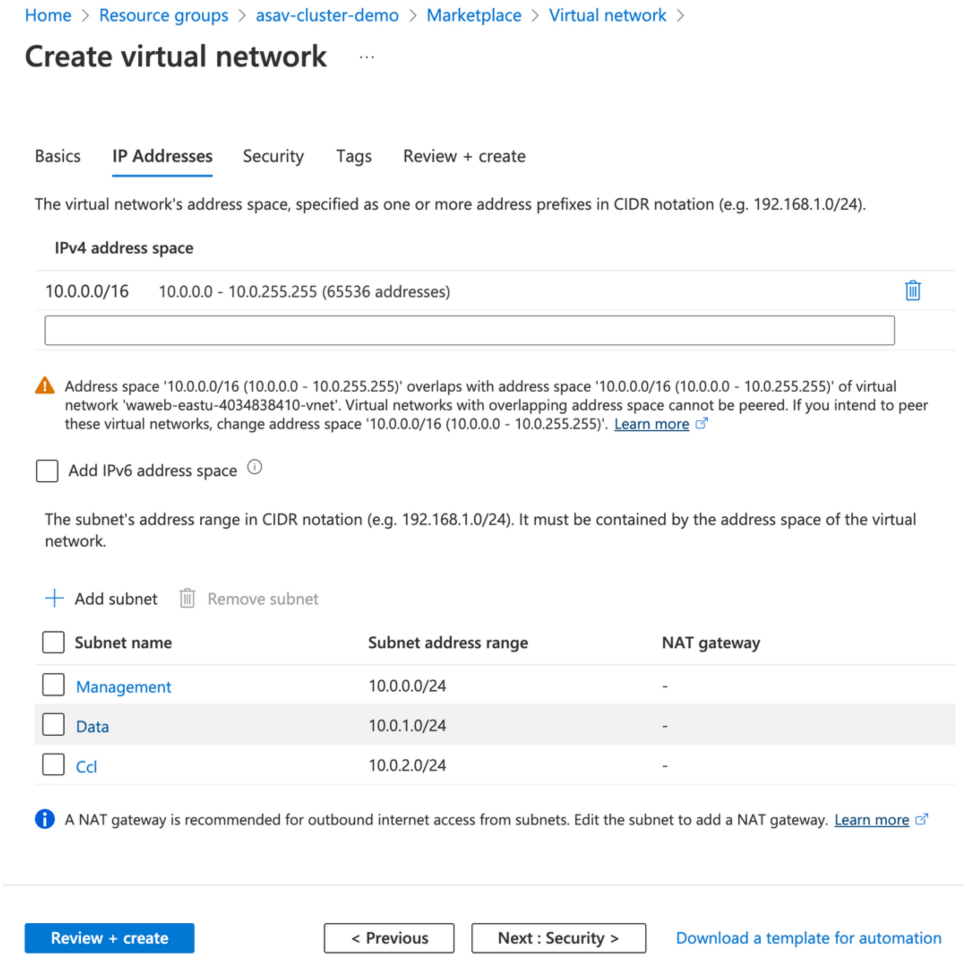
ステップ 3 **リソースグループ**を作成します。



ステップ 4 ASAv クラスタの**管理**、**外部**、および**クラスタ制御リンク**（**CCL**）の 3 つのサブネットを持つ仮想ネットワークを作成します。



ステップ 5　サブネットを追加します。



ステップ 6 カスタムテンプレートを展開します。

a) [作成（Create）] > > [テンプレートの展開（Template deployment）]（カスタムテンプレートを使用して展開）をクリックします。

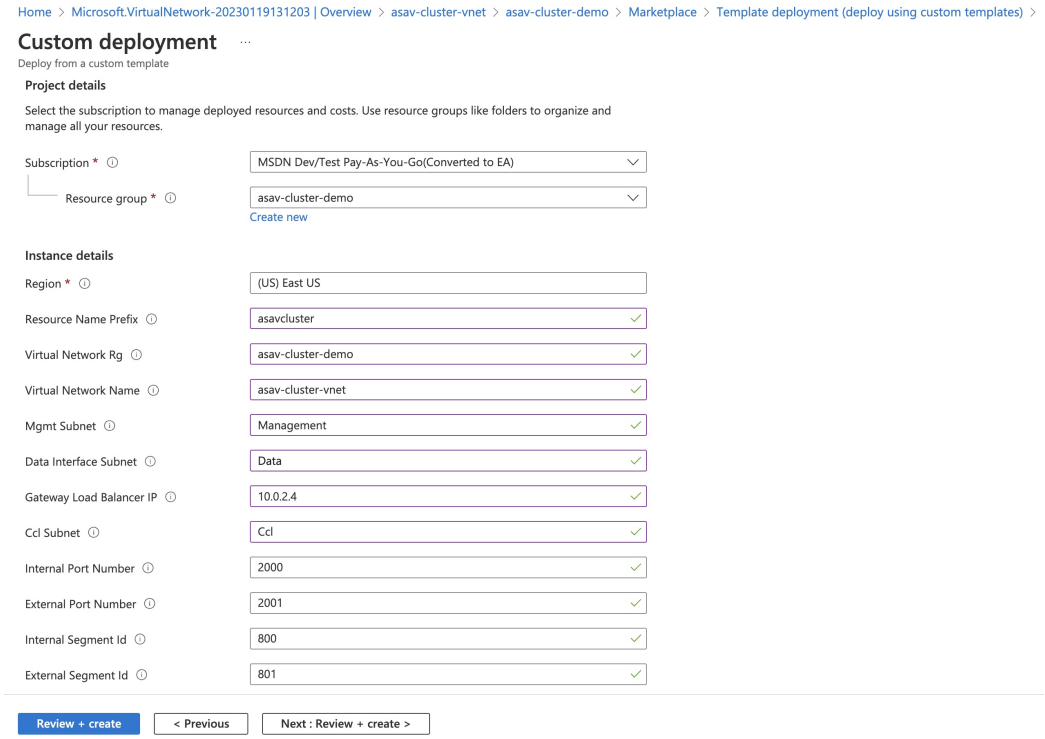
b) [エディタでテンプレートを作成する（Build your template in the editor）] をクリックします。

c) [ファイルのロード（Load File）] をクリックし、Azure で使用しているロードバランサタイプに応じて、`azure_asav_gwlb_cluster.json`。

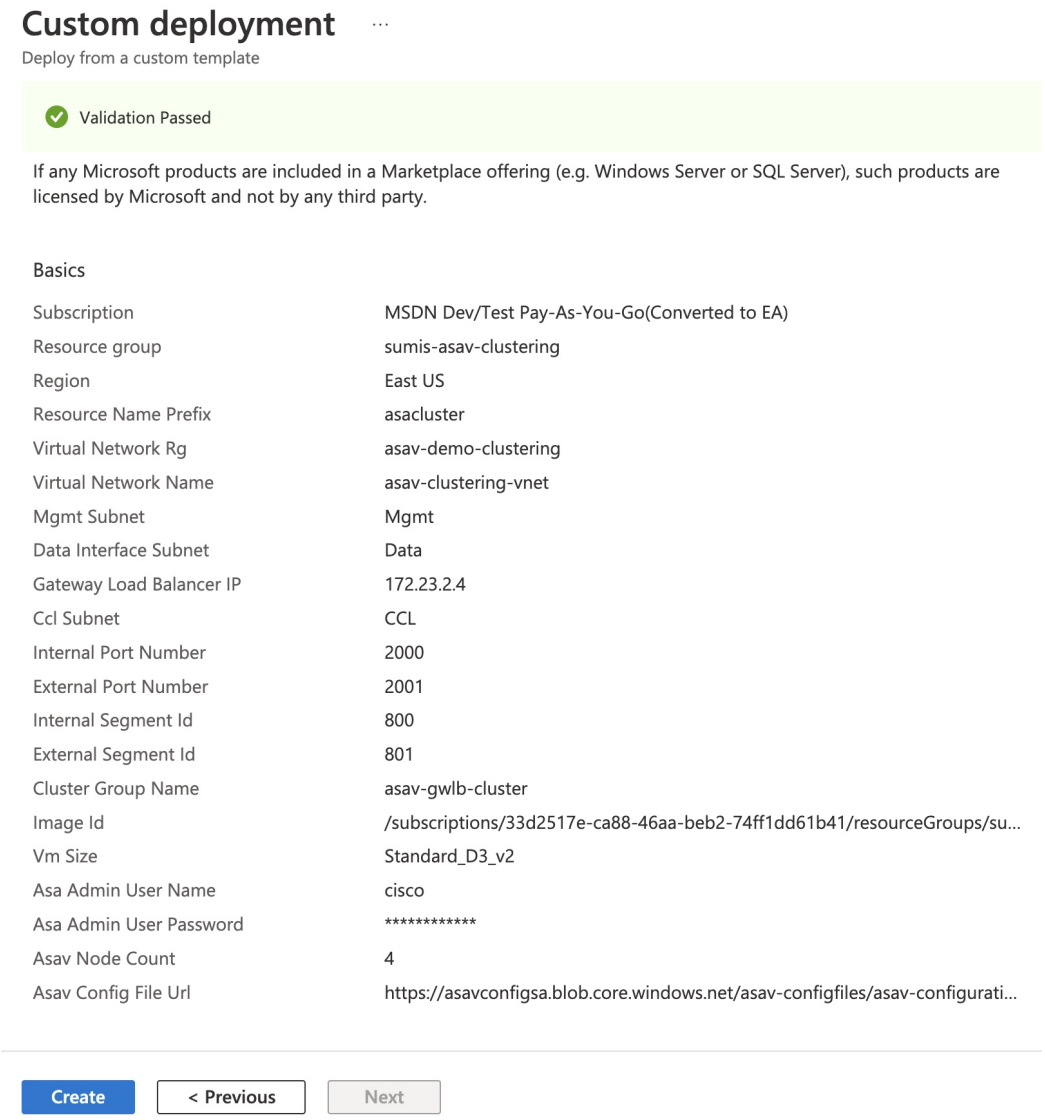
d) [保存（Save）] をクリックします。

ステップ 7 インスタンスの詳細を設定します。

ステップ 8 必要な値を入力し、[確認して作成（Review + create）] をクリックします。



ステップ 9　検証に合格したら、[作成（Create）] をクリックします。



ステップ 10 インスタンスの実行後、いずれかのノードにログインし、**show cluster info** コマンドを入力して、クラスタの展開を確認します。

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
    Interface mode: individual
Cluster Member Limit : 16
    This is "12" in state CONTROL_NODE
        ID        : 0
        Version   : 99.19(1)180
        Serial No.: 9AKGFV8VH4G
        CCL IP    : 10.1.1.12
        CCL MAC   : 000d.3a55.5470
        Module    : NGFWv
        Resource  : 8 cores / 28160 MB RAM
        Last join : 11:13:24 UTC Sep 5 2022
        Last leave: N/A
```

次のタスク

Azure でクラスタを設定する （754 ページ）。

Azure でクラスタを設定する

Azure の ASAv ノードでクラスタを設定するには、構成ファイルを使用するか、Azure Function App を使用して手動で設定できます。ネイティブ GWLB でクラスタを使用できます。

Azure でクラスタを作成するための構成ファイルを準備する

構成ファイルまたは Azure portal の Function App を使用して、ASA 仮想 ノードでクラスタを手動で設定できます。

ASA 仮想 ノードでクラスタを手動で設定するには、`asav-gwlb-cluster-config.txt` を設定しておく必要があります。このファイルでは、クラスタの ASA 仮想 ノードで設定されている範囲オブジェクト、デイゼロ、クラスタグループ名、ライセンスタイプなどのパラメータを定義する必要があります。

このセクションでは、GWLB を使用して Azure の ASA 仮想 ノードを設定するためのクラスタの構成ファイルの作成について説明します。

手順

ステップ 1 Cisco GitHub リポジトリディレクトリ `asav-cluster/sample-config-file` から **asav-gwlb-cluster-config.txt** をダウンロードします。

ステップ 2 クラスタ作成のためにデイゼロ設定を準備できます。

次の day0 構成のサンプルは、GWLB を使用した Azure でのクラスタ作成に必要なパラメータを理解するのに役立ちます。

- **GWLB クラスタ作成用のデイゼロ設定のサンプル**

  以下は、GWLB クラスタ作成に使用される `asav-gwlb-cluster-config.txt` ファイルで必要なデイゼロ設定のサンプルです。

```
cluster interface-mode individual force
            policy-map global_policy
            class inspection_default
            no inspect h323 h225
            no inspect h323 ras
            no inspect rtsp
            no inspect skinny

        interface GigabitEthernet0/0
            nameif vxlan_tunnel
            security-level 0
            ip address dhcp
            no shutdown

        interface GigabitEthernet0/1
            nve-only cluster
```

```
    nameif ccl_link
    security-level 0
    ip address dhcp
    no shutdown

interface vni1
    description ClusterInterface
    segment-id 1
    vtep-nve 1

interface vni2
    proxy paired
    nameif GWLB-backend-pool
    internal-segment-id 800
    external-segment-id 801
    internal-port 2000
    external-port 2001
    security-level 0
    vtep-nve 2

object network ccl#link
    range <CCLSubnetStartAddress> <CClSubnetEndAddress>
    object-group network cluster#group
    network-object object ccl#link

nve 1
    encapsulation vxlan
    source-interface ccl_link
    peer-group cluster#group

nve 2
    encapsulation vxlan
    source-interface vxlan_tunnel
    peer ip <GatewayLoadbalancerIp>

mtu vxlan_tunnel 1454
mtu ccl_link 1374
cluster group <ClusterGroupName>
local-unit <Last Octet of CCL Interface IP>
cluster-interface vni1 ip 1.1.1.<Last Octet of CCL Interface IP> 255.255.255.0

priority 1
enable
```

上記のデイゼロ設定のサンプルでは、カプセル化タイプが **vxlan** としてメンションされている場合、GWLB 関連の設定が有効になります。**InternalPort** と **ExternalPort** は vxlan トンネルインターフェイスの設定に使用され、**InternalSegId** と **ExternalSegId** は内部および外部インターフェイスの識別子として使用されます。

（注）
デイゼロ設定では、開始アドレス（`<CCLSubnetStartAddress>`）とクラスタ制御リンクの終了アドレスを指定する必要があります。したがって、`StartAddress` は常に `x.x.x.4` で開始する必要があり、`EndAddress` は最適な範囲内にある必要があります。広範囲のアドレスを追加するとパフォーマンスに影響する可能性があるため、必要な数のアドレス（最大16）のみを指定することをお勧めします。

例：CCL サブネットが `192.168.3.0/24` の場合、`StartAddress` は `192.168.3.4` になり、`EndAddress` は `192.168.3.30` になります。

以下は、vni インターフェイスに必要な設定のサンプルです。

```
interface vni2
         proxy paired
         nameif GWLB-backend-pool
         internal-segment-id 800
         external-segment-id 801
         internal-port 2000
         external-port 2001
         security-level 0
         vtep-nve 2
```

ステップ 3 構成ファイルを Azure ストレージにアップロードし、この場所のパス（URL）をメモします。この URL パスは、ASA 仮想 ノードでのクラスタの手動設定に必要です。

構成ファイルを使用して手動でクラスタを設定する

構成ファイルを使用して、Azure の ASAv ノードでクラスタを手動で構成するには以下の手順を実行します。

始める前に

構成ファイルを準備し、アップロード先の Azure ストレージの場所をメモしておく必要があります。「Prepare Cluster Configuration File for Azure」を参照してください。

手順

ステップ 1 Azure ポータルにログインします。

ステップ 2 Azure に展開された ASAv インスタンスを開きます。

ステップ 3 次のコマンドを実行して、Azure ストレージコンテナにアップロードしたファイルの URL を指定して、クラスタ構成ファイルを ASAv ノードにコピーします。

copy <Config File URL> running-config

ステップ 4 次のコマンドを実行して、ASAv インスタンスでクラスタを設定します。

```
cluster group <ClusterGroupName>
         local-unit <Last Octet of the Management Interface IP>
         cluster-interface vni1 ip 1.1.1.<Last Octet of the Management Interface IP>
255.255.255.0
         priority 1
         enable
```

ステップ 5 手順 2 ～ 4 を繰り返して、すべての ASAv ノードでクラスタを設定します。

Azure Function App を使用してクラスタを設定する

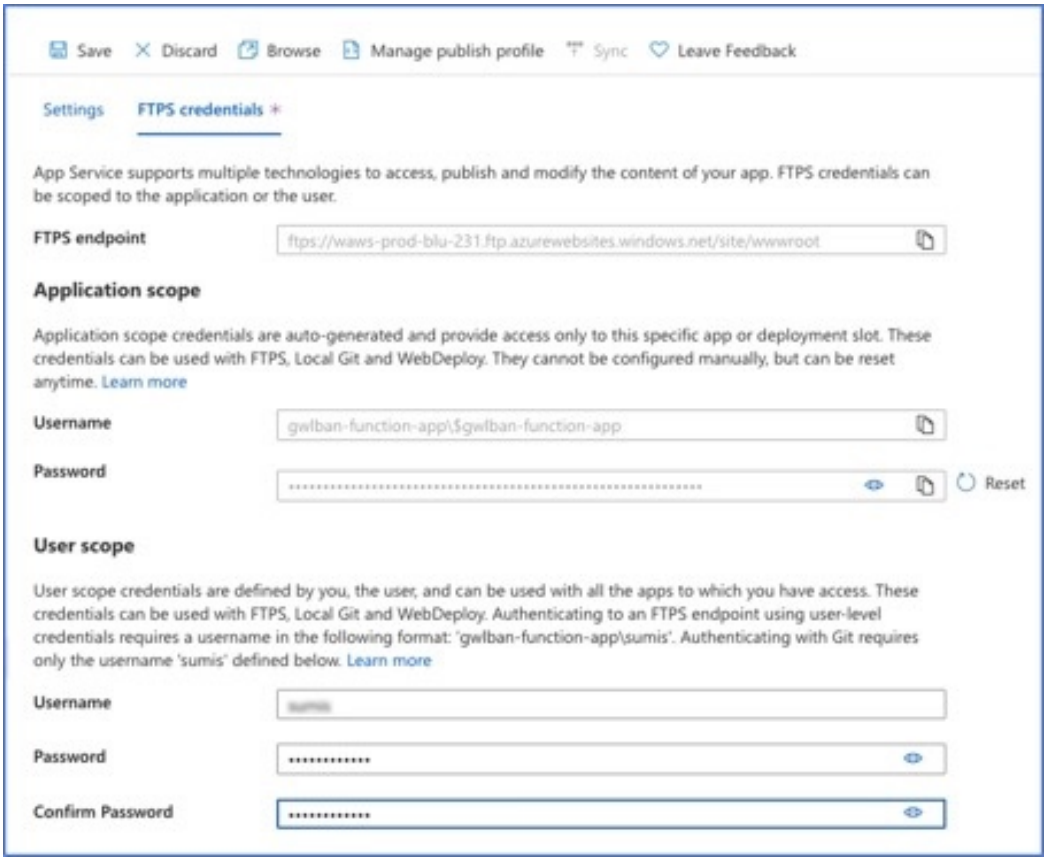
Azure Function App サービスを使用して Azure の ASAv ノードでクラスタを設定するには、以下の手順を実行します。

手順

ステップ 1 Azure ポータルにログインします。

ステップ 2 [Function App] をクリックします。

ステップ 3 **[展開センター（Deployment Center）] > [FTPSの資格情報（FTPS credentials）] > [ユーザースコープ（User scope）] > [ユーザー名とパスワードの設定（Configure Username and Password）] >** をクリックして FTPS の資格情報を作成し、[保存（Save）] をクリックします。



ステップ 4 ローカルのターミナルで次のコマンドを実行して、`Cluster_Function.zip` ファイルを関数アプリにアップロードします。

curl -X POST -u <Userscope_Username> --data-binary @"Cluster_Function.zip" https://<Function_App_Name>.scm.azurewebsites.net/api/zipdeploy

図 *61* : 機能

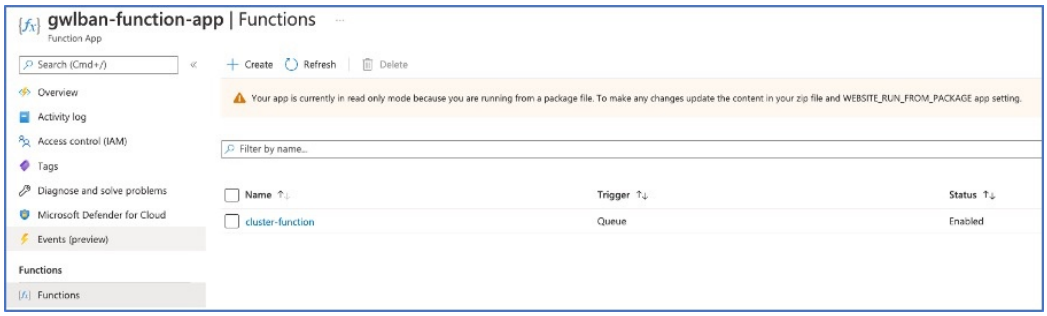


図 *62* : キュー

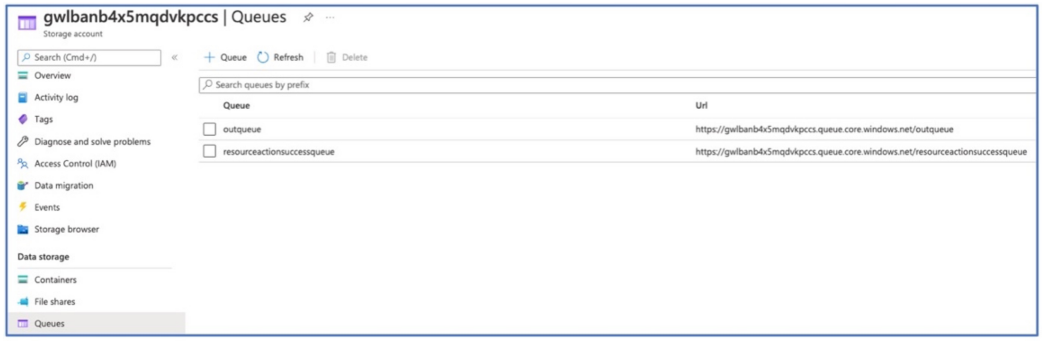
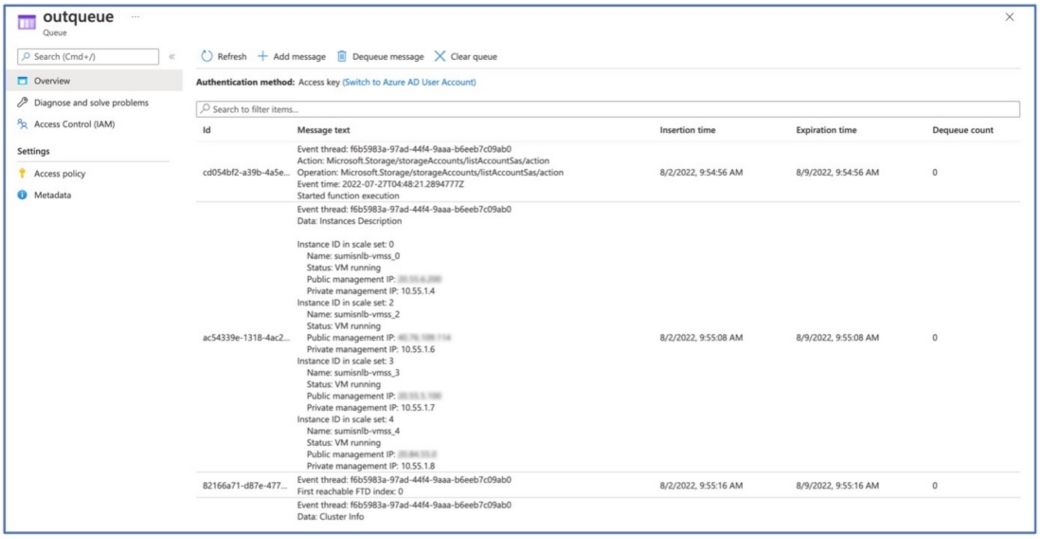


図 *63* : アウトキュー



関数が Function アプリにアップロードされます。関数が開始され、ストレージアカウントのアウトキューにログが表示されます。

関数の実行後、クラスタはすべての ASAv ノードで有効になります。

Azure における ASA Virtual クラスタのトラブルシューティング

トラフィックの問題

トラフィックが機能していない場合は、次のことを確認します。

1. ロードバランサを使用した ASA virtual インスタンスの正常性プローブのステータスが正常であることを確認します。

   ASA virtual インスタンスの正常性プローブのステータスが正常でない場合は、次を実行します。

   1. ASA virtual で設定されたスタティックルートを確認します。
   2. デフォルトゲートウェイがデータサブネットのゲートウェイ IP であることを確認します。
   3. ASA virtual インスタンスが正常性プローブトラフィックを受信していることを確認します。
   4. ASA virtual で設定されているアクセスポリシーが正常性プローブトラフィックを許可していることを確認します。

クラスタの問題

クラスタが形成されていない場合は、次のことを確認してください。

- ネットワーク仮想化エンドポイント（NVE-only）のクラスタインターフェイスの IP アドレス。他のノードの NVE-only のクラスタインターフェイスに ping を実行できることを確認します。
- NVE-only のクラスタインターフェイスの IP アドレスは、オブジェクトグループの一部です。NVE がオブジェクトグループで設定されていることを確認します。
- クラスタグループのクラスタインターフェイスに正しい VNI インターフェイスがあります。この VNI インターフェイスには、対応するオブジェクトグループの NVE があります。
- 各ノードには独自の IP インターフェイスがあります。クラスタ内のノード間の接続を確保するために、ノードが相互に ping できることを確認します。
- テンプレートのデプロイ中に指定された CCL サブネットの開始アドレスと終了アドレスが正しいことを確認します。開始アドレスは、サブネット内で使用可能な最初の IP アドレスで始まる必要があります。たとえばサブネットが 192.168.1.0/24 の場合、開始アドレスは 192.168.1.4 である必要があります（最初の 3 つの IP アドレスは azure によって予約されています）。

ロールに関連する問題

同じリソースグループに再度リソースを展開しているときにロールに関連するエラーが発生した場合は、次の手順を実行します。

特定のロールに関連する問題がある場合、エラーメッセージが表示されます。

エラーメッセージの例を次に示します。

"error": {

"code": "RoleAssignmentUpdateNotPermitted",

"message": "Tenant ID, application ID, principal ID, and scope are not allowed to be updated.”}

ターミナルから以下のコマンドを実行して、以下のロールを削除します。

- ストレージキューデータ寄稿者ロールを削除するコマンド：

  az role assignment delete --resource-group <Resource Group Name> --role "Storage Queue Data Contributor"

- 寄稿者ロールを削除するコマンド：

  az role assignment delete --resource-group <Resource Group Name> --role "Contributor"

ASA 仮想 Azure でのクラスタリングのオートスケール ソリューション

Azure リージョンでの一般的なクラスタ展開には、定義された数の ASA 仮想 インスタンス（ノード）が含まれます。Azure リージョンのトラフィックが変化しても、ノードのダイナミック スケーリング（オートスケール）が行われず、以前からのクラスタ配置のままだと、リソースが十分に活用されなかったり、遅延を引き起こしたりします。Cisco は、Azure リージョンのノードのダイナミック スケーリングをサポートする ASA 仮想 クラスタリング向けにオートスケール ソリューションをバージョン 9.23 以降で提供しています。このソリューションにより、ネットワーク トラフィックに基づいてクラスタからノードを追加または削除して、スケールインまたはスケールアウトを行えます。CPU やメモリのメトリックなどの Azure VMSS メトリックからのリソース使用率の統計に基づくロジックを使用して、クラスタに対してノードを動的に追加または削除します。

Azure の Auto Scale ソリューションを使用した ASA 仮想 クラスタリングは、ネットワーク ロードバランサ（NLB またはサンドイッチ トポロジ）とゲートウェイ ロードバランサ（GWLB）の両方をサポートします。トポロジの例 （761 ページ）を参照してください。

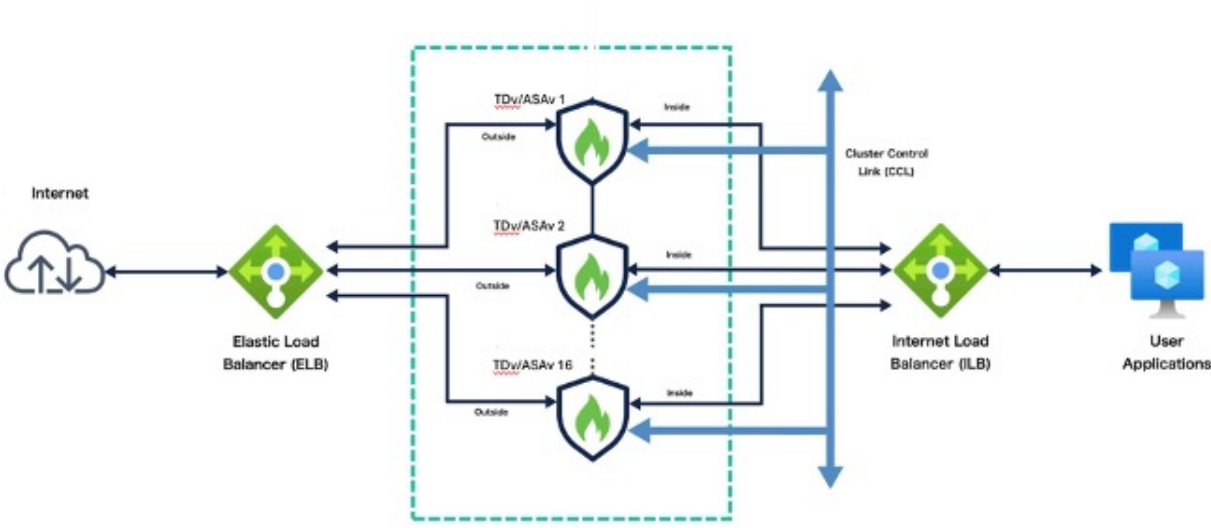
Cisco では、NLB や GWLB を使用して ASA 仮想 クラスタを Azure にオートスケールして展開するための個別の Azure Resource Manager（ARM）テンプレートと、関数アプリや論理アプリなど、Azure サービスを展開するためのインフラストラクチャ テンプレートと構成テンプレートを提供しています。

トポロジの例

ASA 仮想 サンドイッチトポロジ（ネットワーク ロードバランサ）を使用した Azure での Auto Scale のクラスタリング

サンドイッチ トポロジ（NLB）を使用する Azure のオートスケール対応 ASA 仮想 クラスタリングのユースケースは、Azure の内部ロードバランサ（ILB）と Azure の外部ロードバランサ（ELB）にサンドイッチされるように ASA 仮想 スケール セットを配置する、自動水平スケーリング ソリューションです。

このトポロジでは、 ASA 仮想 は、管理、内部、外部、および CCL サブネットの *4* つの インターフェイスのみを使用します。



ASA 仮想 サンドイッチトポロジ（NLB）を使用した Azure での Auto Scale のクラスタリング

以下では、NLB 機能を使用して Azure で の自動スケーリングを行う ASA 仮想 クラスタのフローの概要を示します。

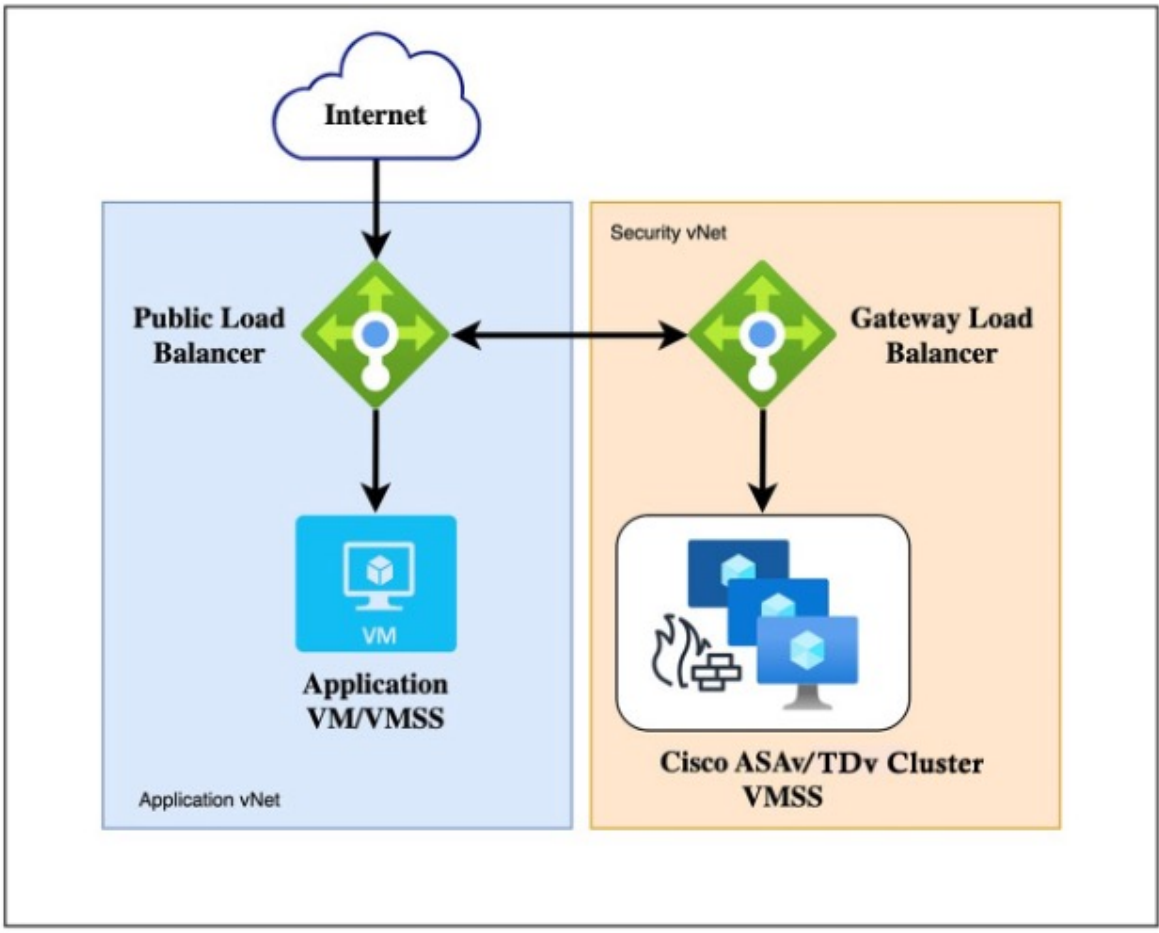
- ELB は、インターネットからのトラフィックをスケールセット内の ASA 仮想 インスタンスに分散させます。その後、ファイアウォールがアプリケーションにトラフィックを転送します。
- ILB は、アプリケーションからのアウトバウンド インターネット トラフィックをスケールセット内の ASA 仮想 インスタンスに分散させます。その後、ファイアウォールがインターネットにトラフィックを転送します。
- ネットワーク パケットが、単一の接続で両方（内部および外部）のロード バランサを通過することはありません。
- スケールセット内の ASA 仮想 インスタンスの数は、負荷条件に基づいて自動的にスケーリングおよび設定されます。

ASA 仮想 ゲートウェイロードバランサを使用した Azure でのオートスケール クラスタリング

オートスケールソリューションを使用した Azure ゲートウェイロードバランサ（GWLB）と ASA 仮想 クラスタの統合により、クラスタセットアップでのインスタンスの展開、管理、およびスケーリングが簡素化されます。Azure ゲートウェイ ロードバランサ（GWLB）は、アプリケーションサーバーなどの Azure VM との間のインターネットトラフィックが、ルーティングの変更を必要とせずに Secure Firewall によって検査されるようにします。また、この統合により、運用の複雑さが軽減され、ファイアウォールでのトラフィックの単一のエントリポイントとエグジットポイントが提供されます。アプリケーションとインフラストラクチャは、送信元 IP アドレスの可視性を維持できます。一部の環境では、この可視性が非常に重要です。

ASA 仮想 は、この使用例では、管理、データ、CCL インターフェイスの *3* つの インターフェイスのみを使用します。

（注）
- Azure GWLB を展開する場合、ネットワークアドレス変換（NAT）は必要ありません。
- IPv4 だけがサポートされます。



以下では、GWLB 機能を使用して、Azure でオートスケーリングを行う ASA 仮想クラスタのフローの概要を説明します。

- インターネットからの着信トラフィックは、GWLB エンドポイントに送られ、そこから GWLB にトラフィックが送信されます。
- その後、トラフィックはASA仮想クラスタにルーティングされます。Auto Scale ソリューションでは、スケールインまたはスケールアウトのロジックを適用して、トラフィック負荷に基づいてクラスタからノードを追加または削除します。
- トラフィックは、クラスタ内のASA仮想インスタンスによって検査された後、アプリケーション VM に転送されます。

Azure での ASA 仮想 クラスタリングの自動スケール ロジック

スケーリングポリシー

自動スケールを備えたクラスタでは、ノードのスケーリングは次のポリシーに基づいて決定されます。

- スケーリングポリシー 1：1 つのクラスタノードがリソース使用率の制限を超える場合。
- スケーリングポリシー 2：すべてのノードの全体的な平均リソース使用率。

スケールアウト

スケールアウトとは、トラフィック負荷のしきい値がクラスタのいずれかのノードに設定されている CPU またはメモリの制限を超えたときに、クラスタに新しいノードを追加するプロセスです。

次に、スケールアウト中にクラスタに新しいノードを追加するプロセスを示します。

1. 新しい ASA 仮想 インスタンスが起動します。
2. ASA 仮想 に適切な設定が適用されています。
3. 適切なライセンスが適用されます。
4. 新しい ASA 仮想 インスタンスがクラスタに追加されます。

スケールアウトプロセス中に新しいASA仮想インスタンスの設定が失敗した場合（低確率）、失敗したインスタンスは終了し、新しいインスタンスが起動して設定されます。

スケールイン

スケールインは、設定されたスケールインしきい値とクラスタ インスタンスの合計数が最小クラスタ サイズを超えた場合に、クラスタからノードを削除するプロセスです。

次に、スケールイン中にクラスタ内のノードを終了するプロセスを示します。

1. CPU またはメモリ使用率が最も低い ASA 仮想 インスタンスは、VMSS メトリックを使用して識別されます。
2. 使用率が同じ最小のインスタンスが複数ある場合、VMSS の VM インデックスが高いインスタンスがスケールイン用に選択されます。
3. このインスタンスへの新しい接続は、適切な設定とポリシーによって無効になります。
4. インスタンスがスマートライセンスから登録解除されます（BYOL に該当）。
5. インスタンスが終了します。

Azure 関数（Function App）

Functionアプリケーションは、ASA 仮想 クラスタの有効化と登録に役立ちます。Functionアプリケーションは、自動スケール展開を使用した ASA 仮想 クラスタリングのホスティング プランを選択するのにも役立ちます。

次の 2 種類のホスティング プランが提供されます。

- 消費
  - これは、自動スケールを使用した ASA 仮想 クラスタリングのデフォルトのホスティング プランです。
  - このプランでは、 リージョンの Azure データセンター IP アドレスへの SSH ポートを開くことにより、Function アプリが ASA 仮想 インスタンスに接続できます。
- プレミアム
  - 展開時に Function アプリに対してこのホスティングプランを選択できます。
  - このプランでは、Functionアプリにネットワーク アドレス変換（NAT）ゲートウェイを追加して、Functionアプリのアウトバウンド IP アドレスを制御できます。このプランでは、NAT ゲートウェイの固定 IP アドレスからのみ ASA 仮想 インスタンスへの SSH アクセスを許可するため、セキュリティが強化されます。

GitHub での展開とインフラストラクチャのテンプレート

Cisco では、Function App、Logic App、自動スケーリンググループなどの複数の Azure サービスを使用して ASA 仮想 クラスタの Virtual Machine Scale Set (VMSS) を展開するための Azure Resource Manager（ARM）テンプレートとスクリプトを提供しています。

ASA 仮想 クラスタの Autoscale ソリューションは、GWLB および NLB ロードバランサのサポートを提供する ARM テンプレートベースの展開です。

ASA 仮想 Autoscale ソリューションテンプレートを使用したクラスタリング

Azure リソース マネージャ（ARM）テンプレート

クラスタに Azure で使用している（NLB または GWLB）ロードバランサに基づいて、autoscale ソリューション用に 2 セットのテンプレートが用意されています。

GitHub では、次のテンプレートを使用できます。

- NLB: `azure_asav_nlb_cluster_autoscale.json` を使用した ASA 仮想 クラスタリング用の Auto Scale ソリューションテンプレートは 、 `azure_autoscale_clustering/asav_cluster/arm_templates/`フォルダにあります。
- GWLB： `azure_asav_gwlb_cluster_autoscale.json` を使用した ASA 仮想 クラスタリング用の autoscale ソリューションテンプレート ：

azure_autoscale_clustering/asav_cluster/arm_templates/フォルダにあります。

GitHub 上の Azure インフラストラクチャおよび構成テンプレート

以下は、Azure での autoscale を使用したクラスタリング用の Azure インフラストラクチャの設定に必要なテンプレートです。

- ASA 仮想インスタンスでクラスタを有効にする機能アプリ：cluster_functions.zip はazure_autoscale_clustering/asav_cluster/azure_function_appフォルダにあります。
- ASA 仮想 の展開、スケールイン、およびスケールアウトのワークフローに使用する Logic App コード：なし（azure_autoscale_clustering/asav_cluster/logic_app/）にある logic_app.txt。

入力パラメータ

次の表に、テンプレートパラメータおよび例を示します。各パラメータの値を決めたら、Azure サブスクリプションに Azure Resource Manager（ARM） テンプレートを展開するときに、各パラメータを使用して ASA 仮想 を作成できます。Azure 向けの GWLB を使用したオートスケールソリューションによるクラスタリングでは、テンプレートで追加の入力パラメータを設定する必要があるため、ネットワーキングインフラストラクチャも作成されます。パラメータの意味は一目瞭然なので説明を省略します。

表 *22:* テンプレートパラメータ

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
resourceNamePrefix	文字列*（3 ～ 10 文字）	すべてのリソースは、このプレフィックスを含む名前で作成されます。 注：小文字のみを使用してください。 例：asav	新規作成
virtualNetworkRg	文字列	仮想ネットワークのリソースグループの名前。 例：cisco-virtualnet-rg	既存
virtualNetworkName	文字列	仮想ネットワーク名（作成済み） 例：cisco-virtualnet	既存

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
mgmtSubnet	文字列	管理サブネット名（作成済み） 例：cisco-mgmt-subnet	既存
dataSubnet	文字列	データ サブネット名（作成済み） 例：cisco-data-subnet	
cclSubnet	文字列	クラスタ制御リンクのサブネット名。 例：cisco-ccl-subnet	
cclSubnetStartAddr	文字列	CCL サブネット IP アドレスの開始範囲。 例：3.4.5.6	
cclSubnetEndAddr	文字列	CCL サブネット IP アドレスの終了範囲。 例：5.6.7.8	
gwlbIP	文字列	GWLB は既存のデータ サブネットに作成されます。 例：10.0.2.4	
dataNetworkGatewayIp	文字列	データ サブネットのゲートウェイ IP アドレス。 例：10.0.2.7	
insideSubnet	文字列	内部サブネット名（作成済み） 例：cisco-inside-subnet	既存
internalLbIp	文字列	内部サブネットの内部ロードバランサの IP アドレス（作成済み）。 例：1.2.3.4	既存
outsideSubnet	文字列	外部サブネット名（作成済み） 例：cisco-outside-subnet	既存

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
softwareVersion	文字列	ASA 仮想バージョン（展開時にドロップダウンから選択）	既存
vmSize	文字列	ASA 仮想インスタンスのサイズ（展開時にドロップダウンから選択）	該当なし
asaAdminUserName	文字列 *	ASA 仮想「admin」ユーザーのユーザー名。 これは「admin」には**できません**。VM 管理者ユーザー名のガイドラインについては、「Azure」を参照してください。 （注） テンプレートには、このパラメータのコンプライアンスチェック機能はありません。	新規作成
asaAdminUserPassword	文字列 *	ASA 仮想 管理者ユーザのパスワード。 パスワードの長さは 12 ー 72 文字で、小文字、大文字、数字、特殊文字を使用する必要があります。また、文字の繰り返しは 2 回までにする必要があります。 （注） テンプレートには、このパラメータのコンプライアンスチェック機能はありません。	新規作成
clusterGroupName	文字列	ASA Virtual デバイスを登録するときに使用されるクラスタグループの名前。 例： asav-cluster	
asaLicensingSku	文字列	ASA Virtual のライセンスモード（PAYG または BYOL）。	

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
healthCheckPortNumber	文字列	ゲートウェイロードバランサで正常性プローブを作成するときに使用されるヘルスチェックのポート番号。 例：8080	
functionHostingPlan	文字列	機能展開のホスティングプラン（コンシューマは消費ホスティングプランを使用、プレミアム：プレミアムホスティングプランを使用）。 デフォルト：消費	
functionAppSubnet	文字列	関数アプリ サブネット名（作成済み）。 例： asav-fapp-subnet	
functionAppSubnetCIDR	文字列	機能アプリサブネットのCIDR（作成済み）。 例：10.0.4.0/24	
scalingMetricsList	文字列	スケーリングおよびスケーリングの決定に使用されるメトリック。 許可: CPU	

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
scalingPolicy	POLICY-1/POLICY-2	**POLICY-1**：設定された期間に、いずれかのASA仮想の平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。 **POLICY-2**：設定された期間に、VMSSのすべてのASA仮想デバイスの平均負荷がスケールアウトしきい値を超えるとスケールアウトがトリガーされます。 どちらの場合も、スケールインロジックは同じままです。設定された期間に、すべてのASA仮想デバイスの平均負荷がスケールインしきい値を下回るとスケールインがトリガーされます。	該当なし
scalingMetricsList	文字列	スケーリングの決定に使用されるメトリック。 許可：CPU デフォルト：CPU	該当なし
scaleInThreshold	文字列	スケールインしきい値（パーセント単位）。 デフォルト：10 ASA仮想メトリックがこの値を下回ると、スケールインがトリガーされます。	該当なし

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
scaleOutThreshold	文字列	スケールアウトしきい値（パーセント単位）。 デフォルト：80 ASA 仮想メトリック（CPU 使用率）がこの値を上回ると、スケールアウトがトリガーされます。 「scaleOutThreshold」は、常に「scaleInThreshold」より**大きく**する必要があります。	該当なし
avClusterSize	文字列	任意の時点でスケールセットで使用可能な ASA Virtual インスタンスのデフォルト ノード数。 例：4	
minAsaCount	整数	任意の時点でスケールセットで使用可能な最小ASA 仮想インスタンス数。 例：2。	該当なし
maxAsaCount	整数	スケールセットで許可される最大 ASA 仮想 インスタンス数。 例：10 （注） Auto Scale ロジックではこの変数の範囲はチェックされないため、慎重に入力してください。	該当なし

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
metricsAverageDuration	整数	ドロップダウンから選択します。 この数値は、メトリックが平均化される時間（分単位）を表します。 この変数の値が5（5分）の場合、Auto Scale Managerがスケジュールされると、メトリックの過去5分間の平均がチェックされ、その結果に基づいてスケーリングの判断が行われます。 （注） Azureの制限により、有効な数値は1、5、15、および30だけです。	該当なし
initDeploymentMode	BULK/STEP	主に最初の展開、またはスケールセットにASA仮想インスタンスが含まれていない場合に適用されます。 BULK：Auto Scale Managerは、「minAsaCount」個のASA仮想 インスタンスを同時に展開しようとします。 STEP：Auto Scale Managerは、スケジュールされた間隔ごとに「minAsaCount」個の ASA仮想デバイスを1つずつ展開します。	
smartLicenseToken	文字列	ASA 仮想を登録するためのスマートライセンストークン。	
licenseThroughput	文字列	ASA 仮想のスマートライセンスの権限付与層。	

パラメータ名	使用できる値/タイプ	説明	リソースの作成タイプ
asavConfigFileUrl	文字列	ASA 仮想 構成ファイルのファイルパス。 例： https://path_to_asav_config_file/config_file 構成ファイルが ASAv からアクセス可能であることを確認します。	該当なし
* Azure には、新しいリソースの命名規則に関する制限があります。制限を確認するか、またはすべて小文字を使用してください**スペースやその他の特殊文字は使用しないでください**。			

ASA 仮想 Auto Scale の展開プロセスとリソースを備えたクラスター

ASA 仮想 Azure での自動スケール展開プロセスを使用した クラスターには、次の作業が含まれます。

- ARM テンプレートを展開します。
- クラスタリング機能を構築して展開します。
- 論理アプリケーションを更新して有効化します。

Azure Resource Manager テンプレート展開リソース

サンドイッチトポロジ（NLB） の ARM テンプレート（`azure_asav_nlb_cluster_autoscale.json`）を使用して、Azure に Auto Scale を使用して ASA 仮想 クラスターを展開すると、リソースグループ内に次のリソースが作成されます。

- 仮想マシンスケールセット（VMSS）
- 外部ロードバランサ
- 内部ロードバランサ
- Azure Function App
- Logic App
- セキュリティグループ（データインターフェイスおよび管理インターフェイス用）

GWLB の ARM テンプレート： `azure_asav_gwlb_cluster_autoscale.json`を使用して、Azure に自動スケールを使用して ASA 仮想 クラスターを展開すると、リソース グループ内に次のリソースが作成されます。

- 仮想マシン（VM）または仮想マシンスケールセット（VMSS）
- ゲートウェイロードバランサ（GWLB）

- Azure Function App
- Logic App
- ネットワーキング インフラストラクチャ
- 展開に必要なセキュリティグループおよびその他のコンポーネント。

Autoscale ソリューションを使用した ASA 仮想 クラスタの展開

ARM テンプレートを使用して、Azure に Auto Scale ソリューションを備えた ASA 仮想 クラスタリングを展開します。トポロジ、サンドイッチ（NLB）または GWLB のユースケースに基づいて、Azure の自動スケールソリューションを使用して ASA 仮想 クラスタリングを展開するための適切な ARM テンプレートをダウンロードして構成する必要があります。

始める前に

GitHub から展開パッケージをダウンロードする

Azure 向けの NLB ソリューションを使用する ASA 仮想 クラスタリング オートスケールは、Azure Resource Manager（ARM）テンプレートベースの展開であり、Azure が提供するサーバーレスインフラストラクチャ（論理アプリ、Azure 関数、ロードバランサ、仮想マシンスケールセットなど）を使用します。

Azure 向けの GWLB ソリューションを使用する ASA 仮想 クラスタリング オートスケールは、ARM テンプレートベースの展開であり、GWLB、ネットワーク インフラストラクチャ、仮想マシン スケール セット、サーバーレス コンポーネント、および他の必要なリソースを作成します。

両方のソリューションの展開手順はほぼ同じです。

Azure 向けのオートスケール ソリューションを使用する ASA 仮想 クラスタリングの起動に必要なファイルをダウンロードします。

該当するバージョン用の展開スクリプトとテンプレートは、GitHub リポジトリから入手できます。

手順

ステップ 1 Microsoft アカウントのユーザー名とパスワードを使用して、Microsoft Azure ポータル（https://portal.azure.com）にログインします。

ステップ 2 **[リソースグループ（Resource Groups）]** ブレードにアクセスするには、サービスのメニューから **[リソースグループ（Resource groups）]** をクリックします。サブスクリプション内のすべてのリソースグループがブレードに一覧表示されます。新しいリソース グループを作成するか、既存の空のリソース グループを選択します。例：**secure-firewall-asav-demo**

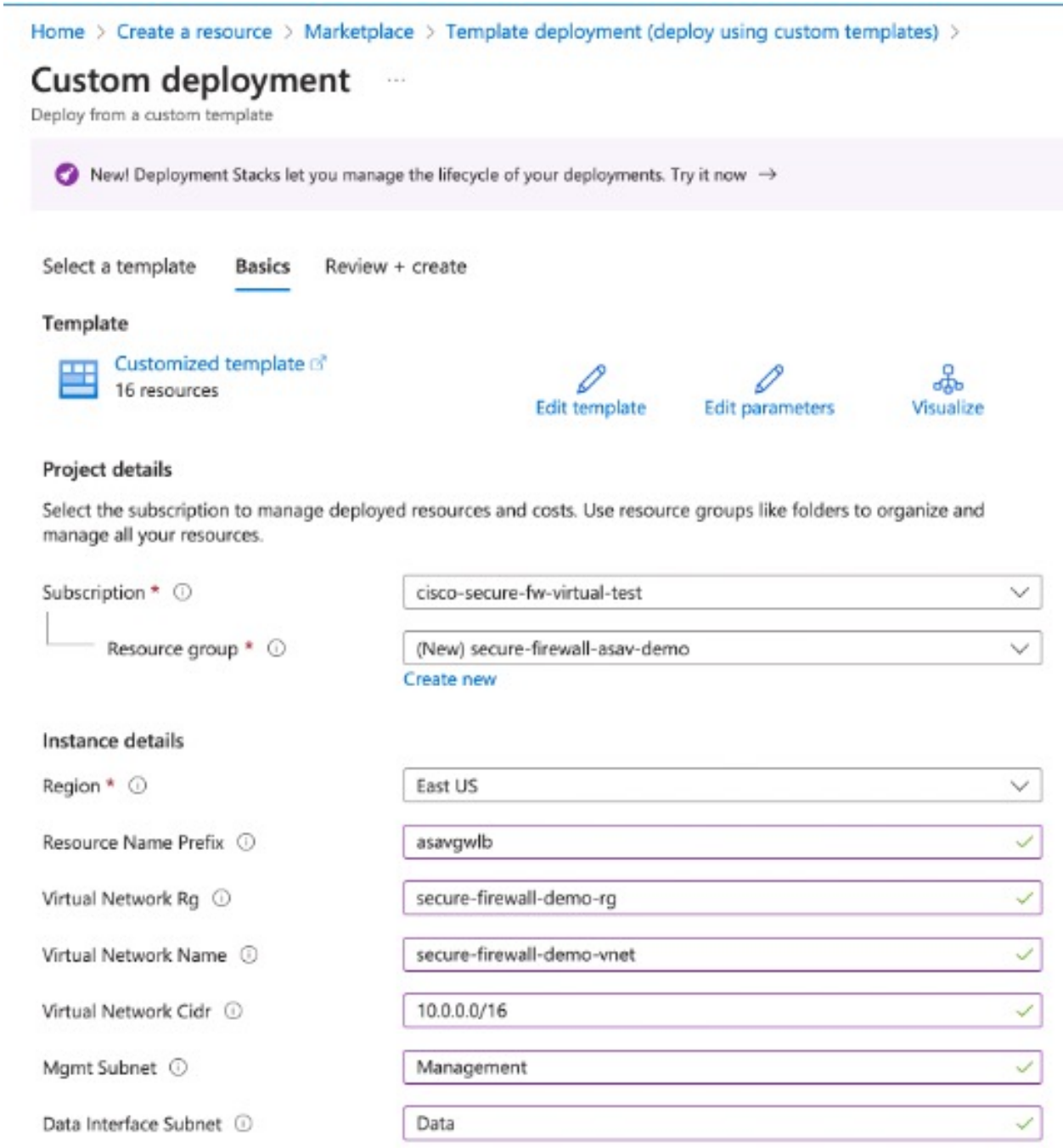
ステップ 3 [リソースの作成（+）（Create a resource (+)）] をクリックして、テンプレート展開用の新しいリソースを作成します。**[リソース グループの作成（Create Resource Group）]** ブレードが表示されます。

ステップ 4 サービスのメニューから **[仮想ネットワーク（Virtual Network）]** をクリックして、仮想ネットワーク ブレードにアクセスします。サブネットを含む仮想ネットワークを作成します。

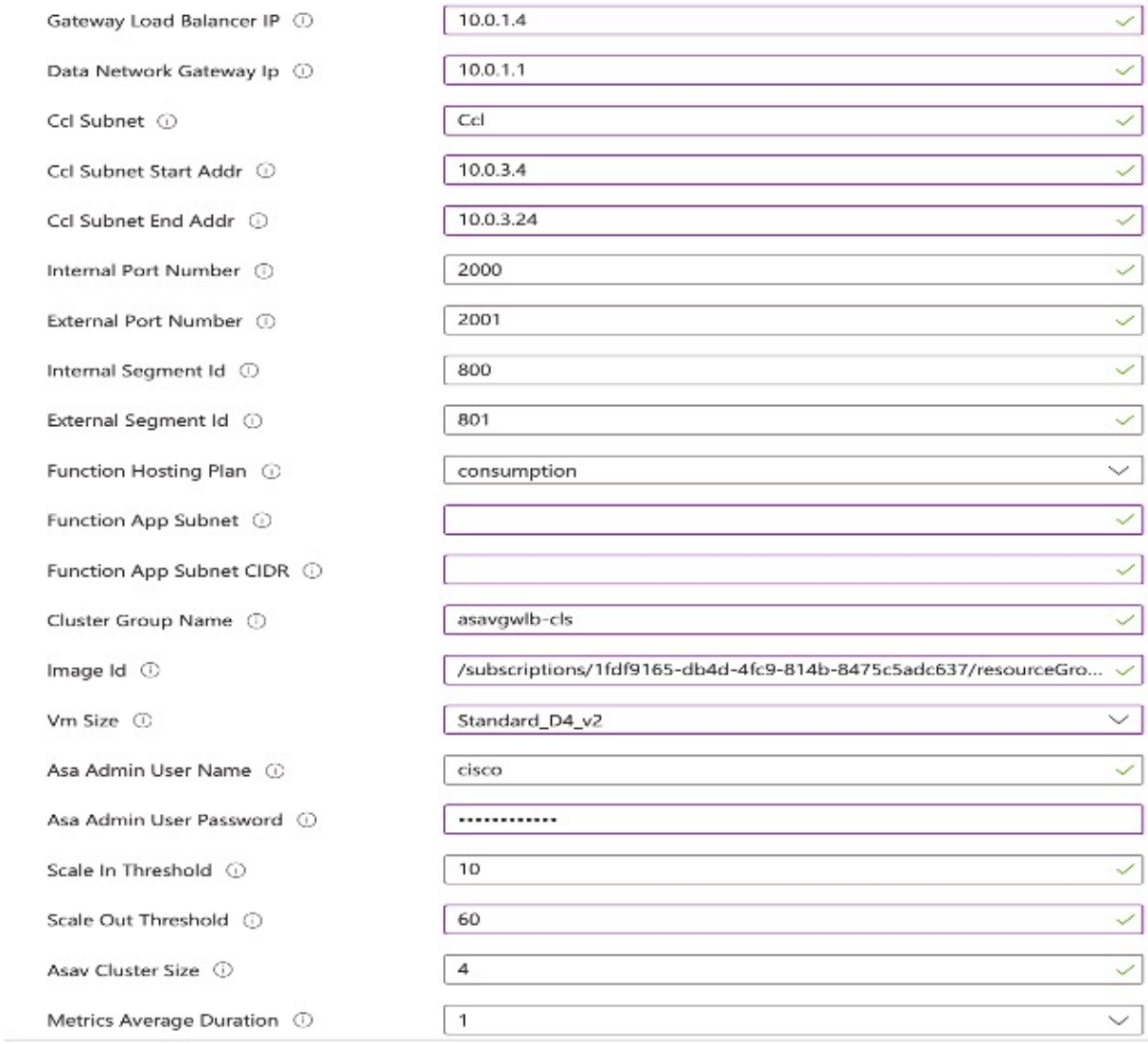
- GWLB 展開の場合、管理、データ、および CCL サブネットを含む仮想ネットワークを作成します。
- NLB 展開の場合、管理、内部、外部、CCL のサブネットを持つ仮想ネットワークを作成します。

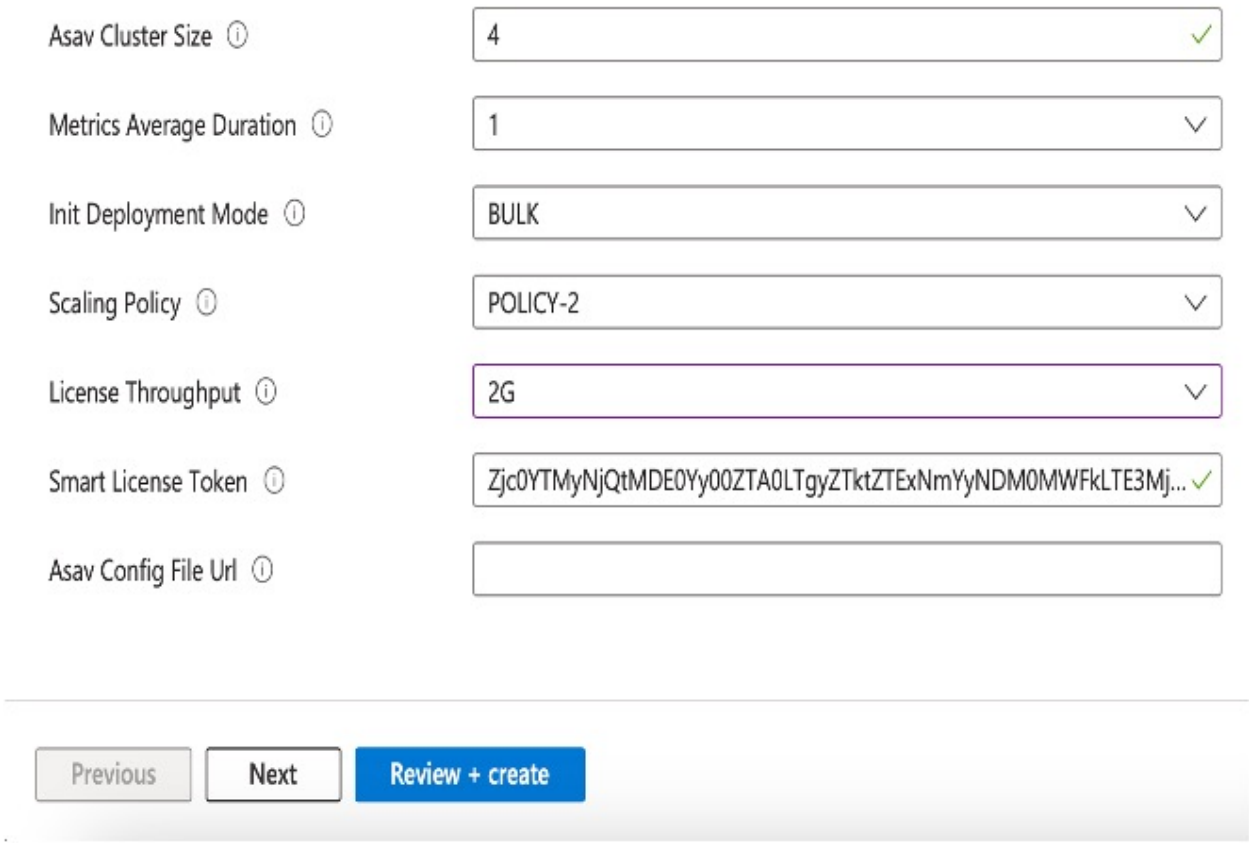
ステップ 5 **[マーケットプレイスの検索（Search the Marketplace）]** で、**[テンプレート展開（`Template deployment`）]**（カスタム テンプレートを使用した展開）と入力し、**Enter** を押します。

ステップ 6 [作成（Create）] をクリックします。テンプレートを作成するためのオプションは複数あります。[エディタで独自のテンプレートを作成する（Build your own template in editor）] を選択します。



ステップ 7 **[テンプレートの編集（Edit template）]** ウィンドウで、すべてのデフォルトコンテンツを削除し、更新した `azure_asav_gwlb_cluster_custom_image.json` または `azure_asav_nlb_cluster_custom_image.json` から（Azure に展開する Auto Scale ソリューションのタイプに応じて）コンテンツをコピーして、**[保存（Save）]** をクリックします。または、**[ファイルの読み込み（Load file）]** をクリックし、コンピュータからこのファイルを参照してアップロードします。


Gateway Load Balancer IP
10.0.1.4
Data Network Gateway Ip
10.0.1.1
Ccl Subnet
Ccl
Ccl Subnet Start Addr
10.0.3.4
Ccl Subnet End Addr
10.0.3.24
Internal Port Number
2000
External Port Number
2001
Internal Segment Id
800
External Segment Id
801
Function Hosting Plan
consumption
Function App Subnet
Function App Subnet CIDR
Cluster Group Name
asavgwlb-cls
Image Id
/subscriptions/1fdf9165-db4d-4fc9-814b-8475c5adc637/resourceGro...
Vm Size
Standard_D4_v2
Asa Admin User Name
cisco
Asa Admin User Password
Scale In Threshold
10
Scale Out Threshold
60
Asav Cluster Size
4
Metrics Average Duration
1



ステップ 8 パラメータ フィールド セクションで、すべてのパラメータを入力します。各パラメータの詳細については、入力パラメータ （766 ページ） を参照してください。次に、**[レビューと作成（Review+Create）]** をクリックします。

ステップ 9 テンプレートの展開が成功すると、Azure 向けのASA 仮想 オートスケール ソリューションに必要なすべてのリソースが作成されます。[タイプ（Type）]列には、Logic App、VMSS、ロードバランサ、パブリック IP アドレスなどの各リソースが示されます。

Function App への Azure Cluster Autoscale 機能の展開

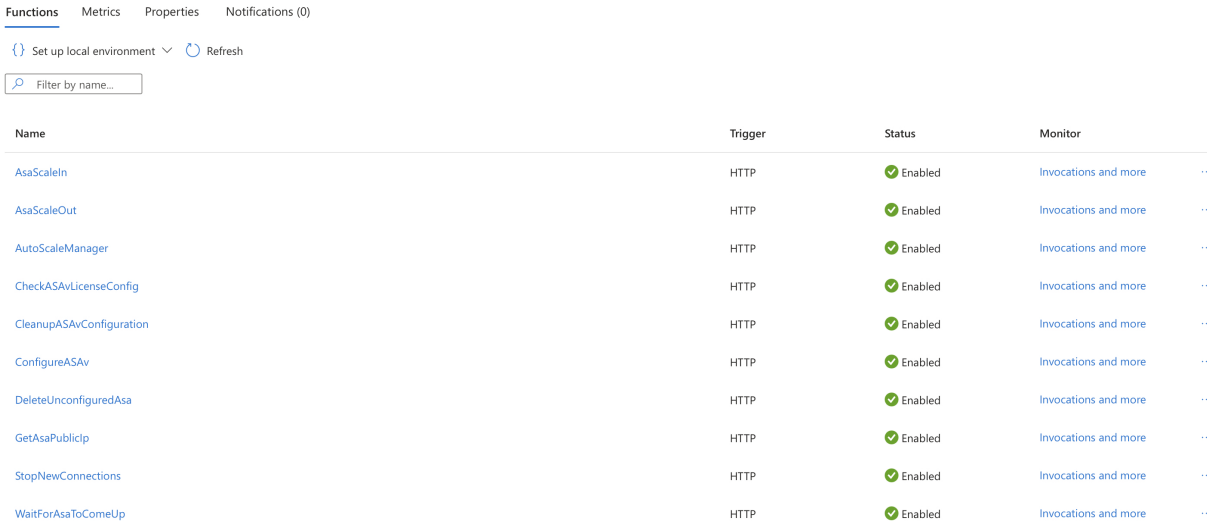
ARM テンプレートの展開が完了すると、次の名前で関数アプリが作成されます。<resourceNamePrefix> *-function-app*。関数アプリを作成したら、次の手順を実行して Azure クラスターの自動スケール機能を関数アプリに展開します。

手順

ステップ 1 ローカルコンピュータで、ターゲットフォルダに移動し、次のコマンドを実行して Azure クラスタ自動スケール機能を機能アプリに展開します。

```
az functionapp deployment source config-zip -g <Resource Group Name> -n <Function App
Name> --src  <cluster_functions.zip> --build-remote true
```

ステップ 2 以下に示すように、アップロードされた機能が機能アプリの **[概要（Overview）]** セクションに表示されているかどうかを確認して、機能が正常に展開されていることを確認します。



Azure Logic App の更新

Logic App は、Auto Scale 機能の Orchestrator として機能します。ARM テンプレートによってスケルトン Logic App が作成されます。このアプリケーションを手動で更新して、Auto Scale Orchestrator として機能するために必要な情報を提供する必要があります。

手順

ステップ 1 リポジトリから、LogicApp.txt ファイルをローカルシステムに取得し、次のように編集します。

重要
手順をすべて読んで理解してから続行してください。

手動の手順は、ARM テンプレートでは自動化されないため、Logic App のみ後で個別にアップグレードできます。

a) 必須: すべての「SUBSCRIPTION_ID」を検索し、サブスクリプション ID 情報に置き換えます。
b) 必須: すべての「RG_NAME」を検索し、リソースグループ名に置き換えます。
c) 必須: すべての「FUNCTIONAPPNAME」を検索し、Function App 名に置き換えます。

次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
  "AutoScaleManager": {
      "inputs": {
          "function": {
              "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/AutoScaleManager"

          }
.
.
                      },
                      "Deploy_Changes_to_ASA": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeployConfiguration"

                              }
.
.
                      "DeviceDeRegister": {
                          "inputs": {
                              "body": "@body('AutoScaleManager')",
                              "function": {
                                  "id":
"/subscriptions/SUBSCRIPTION_ID/resourceGroups/RG_NAME/providers/Microsoft.Web/sites/FUNCTIONAPPNAME/functions/DeviceDeRegister"

                              }
                          },
                          "runAfter": {
                              "Delay_For_connection_Draining": [
```

d) （任意）トリガー間隔を編集するか、デフォルト値（5）のままにします。これは、Auto Scale 機能が定期的にトリガーされる時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
        "triggers": {
            "Recurrence": {
                "conditions": [],
                "inputs": {},
                "recurrence": {
                    "frequency": "Minute",
                    "interval": 5
                },
```

e) （任意）ドレインする時間を編集するか、デフォルト値（5）のままにします。これは、スケールイン操作中にデバイスを削除する前に、ASA Virtual から既存の接続をドレインする時間間隔です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
         "actions": {
              "Branch_based_on_Scale-In_or_Scale-Out_condition": {
                  "actions": {
                      "Delay_For_connection_Draining": {
                          "inputs": {
                              "interval": {
                                  "count": 5,
                                  "unit": "Minute"
```

```
}
```

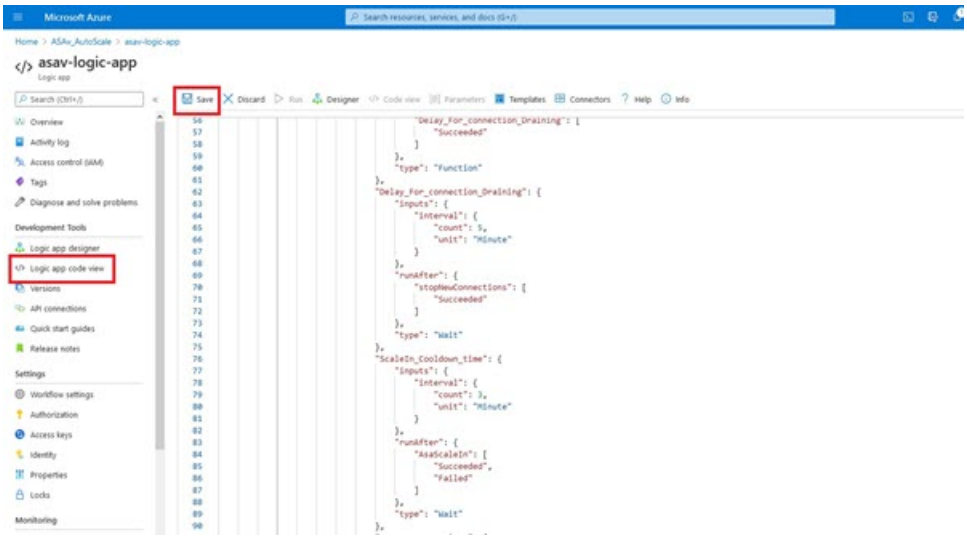
f) （任意）クールダウン時間を編集するか、デフォルト値（10）のままにします。これは、スケールアウト完了後に NO ACTION を実行する時間です。次の例は、LogicApp.txt ファイルの行の一部を示しています。

```
"actions": {
    "Branch_based_on_Scale-Out_or_Invalid_condition": {
        "actions": {
            "Cooldown_time": {
                "inputs": {
                    "interval": {
                        "count": 10,
                        "unit": "Second"
                    }
```

（注）
これらの手順は、Azure ポータルからも実行できます。詳細については、Azure のドキュメントを参照してください。

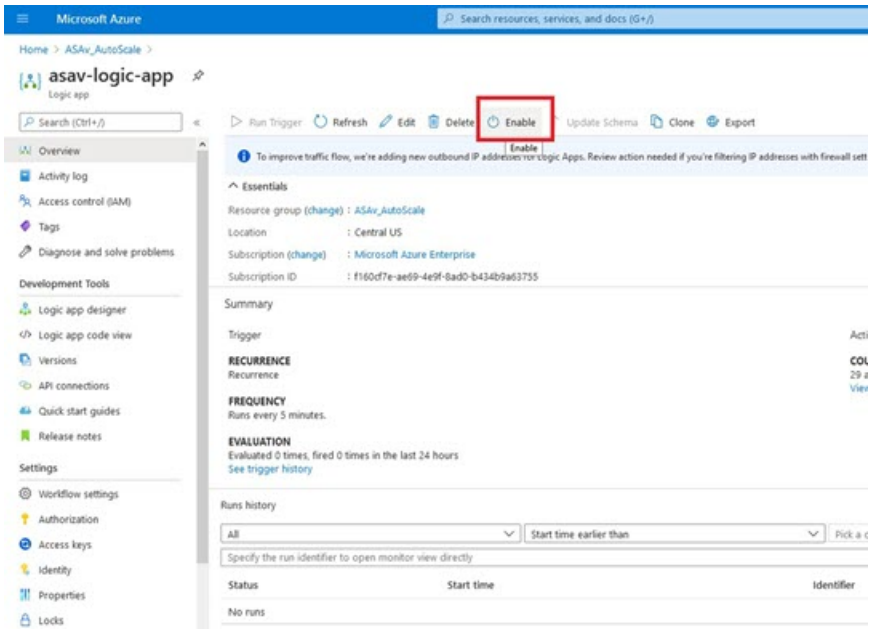
ステップ 2 [Logic Appコードビュー（Logic App code view）] に移動し、デフォルトの内容を削除して、編集した LogicApp.txt ファイルの内容を貼り付け、[保存（Save）] をクリックします。

図 *64 : Logic App* コードビュー



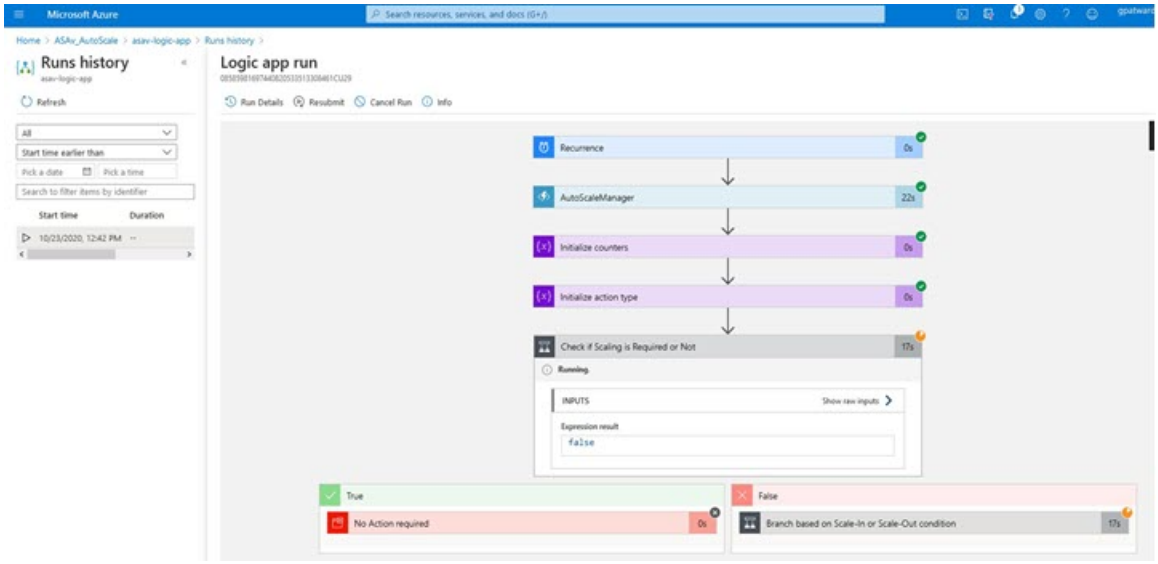
ステップ 3 Logic App を保存すると、[無効（Disabled）] 状態になります。Auto Scale Manager を起動する場合は、[有効化（Enable）] をクリックします。

図 *65 : Logic App* の有効化



ステップ 4 有効にすると、タスクの実行が開始されます。[実行中（Running）] ステータスをクリックしてアクティビティを表示します。

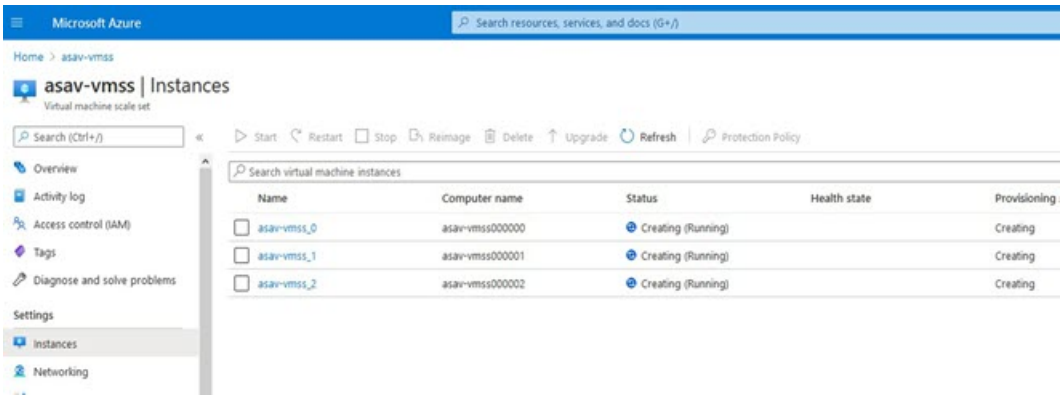
図 *66 : Logic App* の実行ステータス



ステップ 5 Logic App が起動すると、導入関連のすべての手順が完了します。

ステップ 6 ASA Virtual インスタンスが作成されていることを VMSS で確認します。

図 *67* : 稼働中の*ASA Virtual* インスタンス



この例では、ARM テンプレートの展開で「'minAsaCount'」が「3」に設定され、「initDeploymentMode」が「BULK」に設定されているため、3 つの ASA Virtual インスタンスが起動されます。

クラスタリング動作のカスタマイズ

Day 0 設定の一環として、またはクラスタの展開後に、クラスタリング ヘルス モニタリング、TCP 接続複製の遅延、フローのモビリティ、他の最適化をカスタマイズできます。

制御ノードで次の手順を実行します。

ASA クラスタの基本パラメータの設定

制御ノード上のクラスタ設定をカスタマイズできます。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

ステップ 2 （任意） データノードから制御ノードへのコンソール複製を有効にします。

console-replicate

この機能はデフォルトで無効に設定されています。ASA は、特定の重大イベントが発生したときに、メッセージを直接コンソールに出力します。コンソール複製を有効にすると、データノードから制御ノードにコンソールメッセージが送信されるので、モニタする必要があるのはクラスタのコンソールポート 1 つだけです。

ステップ 3 クラスタリング イベントの最小トレース レベルを設定します。

trace-level *level*

必要に応じて最小レベルを設定します。

- **critical**：クリティカル イベント（重大度 = 1）
- **warning**：警告（重大度 = 2）
- **informational**：情報イベント（重大度 = 3）
- **debug**：デバッグ イベント（重大度 = 4）

ステップ 4 フローオーナーからディレクタおよびバックアップオーナーへのフロー状態更新メッセージ（clu_keepalive および clu_update メッセージ）のキープアライブ間隔を設定します。

clu-keepalive-interval *seconds*

- *seconds*：15 ～ 55。デフォルトは 15 です。

クラスタ制御リンクのトラフィック量を減らすために、デフォルトよりも長い間隔を設定することもできます。

ヘルスモニタリングおよび自動再参加設定の設定

この手順では、ノードとインターフェイスのヘルスモニタリングを設定します。

たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルスモニタリングをディセーブルにすることができます。ヘルスモニタリングは VLAN サブインターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)#
```

ステップ 2 クラスタノードのヘルスチェック機能をカスタマイズします。

health-check [**holdtime** *timeout*]

ノードのヘルスを確認するため、ASA のクラスタノードはクラスタ制御リンクで他のノードにハートビートメッセージを送信します。ノードが保留時間内にピアノードからハートビートメッセージを受信しない場合、そのピアノードは応答不能またはデッド状態と見なされます。

- **holdtime** *timeout*：ノードのハートビート ステータス メッセージの時間間隔を指定します。指定できる範囲は .3 ～ 45 秒で、デフォルトは 3 秒です。

何らかのトポロジ変更を行うとき（たとえば、データインターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスの有効化または無効化）は、ヘルスチェック機能を無効にし、無効化したインターフェイスのインターフェイス モニタリングも無効にする必要があります（**no health-check monitor-interface**）。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

例：

```
ciscoasa(cfg-cluster)# health-check holdtime 5
```

ステップ 3 インターフェイスでインターフェイス ヘルス チェックを無効化します。

no health-check monitor-interface *interface_id*

インターフェイスのヘルス チェックはリンク障害をモニターします。ASA がメンバーをクラスタから削除するまでの時間は、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。デフォルトでは、ヘルス チェックはすべてのインターフェイスでイネーブルになっています。このコマンドの **no** 形式を使用してディセーブル（無効）にすることができます。たとえば、管理インターフェイスなど、必須以外のインターフェイスのヘルス モニタリングをディセーブルにすることができます。

- *interface_id*：インターフェイスの監視を無効にします。ヘルスモニタリングは VLAN サブインターフェイスでは実行されません。クラスタ制御リンクのモニタリングは設定できません。このリンクは常にモニターされています。

何らかのトポロジ変更を行うとき（たとえば、データインターフェイスの追加または削除、ASA またはスイッチ上のインターフェイスの有効化または無効化）は、ヘルスチェック機能を無効（**no health-check**）にし、無効化したインターフェイスのインターフェイス モニタリングも無効にする必要があります。トポロジの変更が完了して、設定の変更がすべてのノードに同期されたら、ヘルスチェック機能を再度有効にできます。

例：

```
ciscoasa(cfg-cluster)# no health-check monitor-interface management1/1
```

ステップ 4 ヘルス チェック失敗後の自動再結合クラスタ設定をカスタマイズします。

health-check {**data-interface** | **cluster-interface** | **system**} **auto-rejoin** [**unlimited** | *auto_rejoin_max*] *auto_rejoin_interval auto_rejoin_interval_variation*

- **system**：内部エラー時の自動再結合の設定を行います。内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。
- **unlimited**：（**cluster-interface** のデフォルト）再結合の試行回数を制限しません。
- *auto-rejoin-max*：再結合の試行回数を 0 ～ 65535 の範囲の値に設定します。**0** は自動再結合を無効化します。**data-interface** と **system** のデフォルトは 3 です。

- *auto_rejoin_interval*：再結合試行の間隔を 2 ～ 60 の範囲の分単位で定義します。デフォルト値は5分です。クラスタへの再参加をノードが試行する最大合計時間は、最後の障害発生時から 14400 分（10 日）に制限されます。
- *auto_rejoin_interval_variation*：間隔を増加させるかどうかを定義します。1 ～ 3 の範囲で値を設定します（**1**：変更なし、**2**：直前の間隔の2倍、**3**：直前の間隔の3倍）。たとえば、間隔を 5 分に設定し、変分を 2 に設定した場合は、最初の試行が 5 分後、2 回目の試行が 10 分後（2 x 5）、3 階目の試行が 20 分後（2 x 10）となります。デフォルト値は、クラスタインターフェイスの場合は**1**、データインターフェイスおよびシステムの場合は**2**です。

例：

```
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 10 3 3
```

ステップ 5 ASAがインターフェイスを障害が発生していると見なし、クラスタからノードが削除されるまでのデバウンス時間を設定します。

health-check monitor-interface debounce-time *ms*

例：

```
ciscoasa(cfg-cluster)# health-check monitor-interface debounce-time 300
```

デバウンス時間は 300 ～ 9000 ms の範囲の値を設定します。デフォルトは 500 ms です。値を小さくすると、インターフェイスの障害をより迅速に検出できます。デバウンス時間を短くすると、誤検出の可能性が高くなることに注意してください。インターフェイスのステータス更新が発生すると、ASAはインターフェイスを障害としてマークし、クラスタからノードを削除するまで指定されたミリ秒数待機します。

ステップ 6 （任意）トラフィック負荷のモニタリングを設定します。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

- **frequency** *seconds*：モニタリングメッセージ間の時間を、10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。
- **intervals** *intervals*： ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

クラスタメンバのトラフィック負荷をモニターできます。対象には、合計接続数、CPUとメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのノードが負荷を処理できる場合は、ノードのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ノードでクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例：

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 50 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 25 interval:
   0           0            0            12              28
   1           0            0            13              27
```

例

次の例では、ヘルスチェック保留時間を .3 秒に設定し、管理 0/0 インターフェイスのモニタリングを無効にし、データインターフェイスの自動再結合の試行回数を 2 分から開始して前回の間隔の 3 倍増加させる計 4 回に設定し、クラスタ制御リンクの自動再結合の試行回数を 2 分おきの計 6 回に設定しています。

```
ciscoasa(config)# cluster group test
ciscoasa(cfg-cluster)# health-check holdtime .3
ciscoasa(cfg-cluster)# no health-check monitor-interface management0/0
ciscoasa(cfg-cluster)# health-check data-interface auto-rejoin 4 2 3
ciscoasa(cfg-cluster)# health-check cluster-interface auto-rejoin 6 2 1
```

クラスタノードの管理

クラスタを導入した後は、コンフィギュレーションを変更し、クラスタノードを管理できます。

非アクティブノードになる

クラスタの非アクティブなメンバーになるには、クラスタリングコンフィギュレーションは変更せずに、そのノード上でクラスタリングをディセーブルにします。

（注） ASAが（手動で、またはヘルスチェックエラーにより）非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィックフローを再開させるには、クラスタリングを再びイネーブルにします。または、そのノードをクラスタから完全に削除します。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソールポートを使用する必要があります。

手順

ステップ 1 クラスタの設定モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをディセーブルにします。

no enable

このノードが制御ノードであった場合は、新しい制御ノードの選定が実行され、別のメンバーが制御ノードになります。

クラスタコンフィギュレーションは維持されるので、後でクラスタリングを再度イネーブルにできます。

制御ノードからのデータノードの非アクティブ化

ログインしているノード以外のメンバを非アクティブにするには、次のステップを実行します。

（注） ASAが非アクティブになると、すべてのデータインターフェイスがシャットダウンされます。管理専用インターフェイスのみがトラフィックを送受信できます。トラフィック フローを再開するには、クラスタリングを再度有効にします。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードしてもノードがクラスタ内でまだアクティブではない場合（クラスタリングが無効な状態で設定を保存した場合など）、管理インターフェイスは無効になります。それ以降のコンフィギュレーション作業には、コンソール ポートを使用する必要があります。

手順

クラスタからノードを削除します。

cluster remove unit *node_name*

ブートストラップ コンフィギュレーションは変更されず、制御ノードから最後に同期されたコンフィギュレーションもそのままであるので、コンフィギュレーションを失わずに後でそのノードを再度追加できます。制御ノードを削除するためにデータノードでこのコマンドを入力した場合は、新しい制御ノードが選定されます。

メンバ名を一覧表示するには、**cluster remove unit ?** と入力するか、**show cluster info** コマンドを入力します。

例：

```
ciscoasa(config)# cluster remove unit ?

Current active units in the cluster:
asa2

ciscoasa(config)# cluster remove unit asa2
WARNING: Clustering will be disabled on unit asa2. To bring it back
to the cluster please logon to that unit and re-enable clustering
```

クラスタへの再参加

ノードがクラスタから削除された場合（たとえば、障害が発生したインターフェイスの場合、またはメンバーを手動で非アクティブにした場合）は、クラスタに手動で再参加する必要があります。

手順

ステップ 1 コンソールで、クラスタ コンフィギュレーション モードを開始します。

cluster group *name*

例：

```
ciscoasa(config)# cluster group pod1
```

ステップ 2 クラスタリングをイネーブルにします。

enable

クラスタからの脱退

クラスタから完全に脱退するには、クラスタ ブートストラップ コンフィギュレーション全体を削除する必要があります。各ノードの現在のコンフィギュレーションは（アクティブユニットから同期されて）同じであるため、クラスタから脱退すると、クラスタリング前のコンフィギュレーションをバックアップから復元するか、IPアドレスの競合を避けるためコンフィギュレーションを消去して初めからやり直すことも必要になります。

手順

ステップ 1 データノードの場合、クラスタリングを次のように無効化します。

cluster group *cluster_name* **no enable**

例：

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# no enable
```

クラスタリングがデータノード上でイネーブルになっている間は、コンフィギュレーション変更を行うことはできません。

ステップ 2 クラスタ コンフィギュレーションをクリアします。

clear configure cluster

ASAは、管理インターフェイスとクラスタ制御リンクを含むすべてのインターフェイスをシャットダウンします。

ステップ 3 クラスタ インターフェイス モードをディセーブルにします。

no cluster interface-mode

モードはコンフィギュレーションには保存されないため、手動でリセットする必要があります。

ステップ 4 バックアップ コンフィギュレーションがある場合、実行コンフィギュレーションにバックアップ コンフィギュレーションをコピーします。

copy *backup_cfg* **running-config**

例：

```
ciscoasa(config)# copy backup_cluster.cfg running-config

Source filename [backup_cluster.cfg]?

Destination filename [running-config]?
ciscoasa(config)#
```

ステップ 5 コンフィギュレーションをスタートアップに保存します。

write memory

ステップ 6 バックアップ コンフィギュレーションがない場合は、管理アクセスを再設定します。たとえば、インターフェイス IP アドレスを変更し、正しいホスト名を復元します。

制御ノードの変更

注意 制御ノードを変更する最良の方法は、制御ノードでクラスタリングを無効にし、新しい制御ユニットの選択を待ってから、クラスタリングを再度有効にする方法です。制御ノードにするノードを厳密に指定する必要がある場合は、この項の手順を使用します。ただし、中央集中型機能の場合は、この手順を使用して制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

制御ノードを変更するには、次の手順を実行します。

手順

新しいノードを制御ノードとして設定します。

cluster control-node unit*node_name*

例：

```
ciscoasa(config)# cluster control-node unit asa2
```

メイン クラスタ IP アドレスへの再接続が必要になります。

メンバー名を表示するには、**cluster control-node unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

クラスタ全体でのコマンドの実行

コマンドをクラスタ内のすべてのノードに、または特定のノードに送信するには、次の手順を実行します。**show** コマンドをすべてのノードに送信すると、すべての出力が収集されて現在のノードのコンソールに表示されます。その他のコマンド、たとえば **capture** や **copy** も、クラスタ全体での実行を活用できます。

手順

すべてのノードにコマンドを送信します。ノード名を指定した場合は、特定のノードに送信します。

cluster exec [**unit** *node_name*] コマンド

例：

```
ciscoasa# cluster exec show xlate
```

ノード名を表示するには、**cluster exec unit ?**（現在のノードを除くすべての名前が表示される）と入力するか、**show cluster info** コマンドを入力します。

例

同じキャプチャファイルをクラスタ内のすべてのノードから同時に TFTP サーバにコピーするには、制御ノードで次のコマンドを入力します。

```
ciscoasa# cluster exec copy /pcap capture: tftp://10.1.1.56/capture1.pcap
```

複数の PCAP ファイル（各ノードから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャファイル名には自動的にノード名が付加され、capture1_asa1.pcap、capture1_asa2.pcap などとなります。この例では、asa1 と asa2 はクラスタノード名です。

クラスタのモニタリング

クラスタの状態と接続をモニターおよびトラブルシューティングできます。

クラスタ ステータスのモニタリング

クラスタの状態のモニタリングについては、次のコマンドを参照してください。

- **show cluster info** [**health** [**details**]]

キーワードを指定しないで **show cluster info** コマンドを実行すると、クラスタ内のすべてのメンバのステータスが表示されます。

show cluster info health コマンドは、インターフェイス、ノードおよびクラスタ全体の現在の状態を表示します。**details** キーワードは、ハートビート メッセージの失敗数を表示します。

show cluster info コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info
Cluster stbu: On
  This is "C" in state DATA_NODE
      ID        : 0
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000025
      CCL IP    : 10.0.0.3
      CCL MAC   : 000b.fcf8.c192
      Last join : 17:08:59 UTC Sep 26 2011
      Last leave: N/A
Other members in the cluster:
  Unit "D" in state DATA_NODE
      ID        : 1
      Site ID   : 1
            Version   : 9.4(1)
      Serial No.: P3000000001
      CCL IP    : 10.0.0.4
      CCL MAC   : 000b.fcf8.c162
      Last join : 19:13:11 UTC Sep 23 2011
      Last leave: N/A
  Unit "A" in state CONTROL_NODE
      ID        : 2
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: JAB0815R0JY
      CCL IP    : 10.0.0.1
      CCL MAC   : 000f.f775.541e
      Last join : 19:13:20 UTC Sep 23 2011
      Last leave: N/A
  Unit "B" in state DATA_NODE
      ID        : 3
      Site ID   : 2
            Version   : 9.4(1)
      Serial No.: P3000000191
      CCL IP    : 10.0.0.2
      CCL MAC   : 000b.fcf8.c61e
      Last join : 19:13:50 UTC Sep 23 2011
      Last leave: 19:13:36 UTC Sep 23 2011
```

- **show cluster info auto-join**

  時間遅延後にクラスタノードがクラスタに自動的に再参加するかどうか、および障害状態（ライセンスの待機やシャーシのヘルスチェック障害など）がクリアされたかどうかを示します。ノードが永続的に無効になっている場合、またはノードがすでにクラスタ内にある場合、このコマンドでは出力が表示されません。

  show cluster info auto-join コマンドについては次の出力を参照してください。

```
ciscoasa(cfg-cluster)# show cluster info auto-join
```

```
Unit will try to join cluster in 253 seconds.
Quit reason: Received control message DISABLE

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Control node has application down that data node has up.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Chassis-blade health check failed.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Service chain application became down.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit will try to join cluster when quit reason is cleared.
Quit reason: Unit is kicked out from cluster because of Application health check
failure.

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license entitlement: ent1)

ciscoasa(cfg-cluster)# show cluster info auto-join
Unit join is pending (waiting for the smart license export control flag)
```

- **show cluster info transport**{**asp** |**cp**[**detail**]}

  次のトランスポート関連の統計情報を表示します。

  - **asp**：データ プレーンのトランスポート統計情報。
  - **cp**：コントロール プレーンのトランスポート統計情報。

    detail キーワードを入力すると、クラスタで信頼性の高いトランスポート プロトコルの使用状況が表示され、バッファがコントロールプレーンでいっぱいになったときにパケット ドロップの問題を特定できます。**show cluster info transport cp detail** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info transport cp detail
Member ID to name mapping:
  0 - unit-1-1   2 - unit-4-1   3 - unit-2-1

Legend:
  U    - unreliable messages
  UE   - unreliable messages error
  SN   - sequence number
  ESN  - expecting sequence number
  R    - reliable messages
  RE   - reliable messages error
  RDC  - reliable message deliveries confirmed
  RA   - reliable ack packets received
  RFR  - reliable fast retransmits
  RTR  - reliable timer-based retransmits
  RDP  - reliable message dropped
  RDPR - reliable message drops reported
  RI   - reliable message with old sequence number
  RO   - reliable message with out of order sequence number
  ROW  - reliable message with out of window sequence number
  ROB  - out of order reliable messages buffered
  RAS  - reliable ack packets sent
```

```
This unit as a sender
-------------------------
        all       0         2         3
  U     123301    3867966   3230662   3850381
  UE    0         0         0         0
  SN    1656a4ce  acb26fe   5f839f76  7b680831
  R     733840    1042168   852285    867311
  RE    0         0         0         0
  RDC   699789    934969    740874    756490
  RA    385525    281198    204021    205384
  RFR   27626     56397     0         0
  RTR   34051     107199    111411    110821
  RDP   0         0         0         0
  RDPR  0         0         0         0

This unit as a receiver of broadcast messages
----------------------------------------------
        0         2         3
  U     111847    121862    120029
  R     7503      665700    749288
  ESN   5d75b4b3  6d81d23   365ddd50
  RI    630       34278     40291
  RO    0         582       850
  ROW   0         566       850
  ROB   0         16        0
  RAS   1571      123289    142256

This unit as a receiver of unicast messages
-------------------------------------------
        0         2         3
  U     1         3308122   4370233
  R     513846    879979    1009492
  ESN   4458903a  6d841a84  7b4e7fa7
  RI    66024     108924    102114
  RO    0         0         0
  ROW   0         0         0
  ROB   0         0         0
  RAS   130258    218924    228303

Gated Tx Buffered Message Statistics
------------------------------------
    current sequence number: 0

    total:                   0
    current:                 0
    high watermark:          0

    delivered:               0
    deliver failures:        0

    buffer full drops:       0
    message truncate drops:  0

    gate close ref count:    0

    num of supported clients:45

MRT Tx of broadcast messages
============================
Message high watermark: 3%
  Total messages buffered at high watermark: 5677
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
```

```
  Client name                           Total messages  Percentage
  Cluster Redirect Client                         4153         73%
  Route Cluster Client                             419          7%
  RRI Cluster Client                              1105         19%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 1
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                           Total messages  Percentage    F   L   R
  VPN Clustering HA Client                           1        100%    0   0   0

MRT Tx of unitcast messages(to member_id:0)
===========================================
Message high watermark: 31%
  Total messages buffered at high watermark: 4059
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                           Total messages  Percentage
  Cluster Redirect Client                         3731         91%
  RRI Cluster Client                               328          8%

Current MRT buffer usage: 29%
  Total messages buffered in real-time: 3924
  [Per-client message usage in real-time]
  Legend:
        F - MRT messages sending when buffer is full
        L - MRT messages sending when cluster node leave
        R - MRT messages sending in Rx thread
  ------------------------------------------------------------------------------
  Client name                           Total messages  Percentage    F   L   R
  Cluster Redirect Client                         3607         91%    0   0   0
  RRI Cluster Client                               317          8%    0   0   0

MRT Tx of unitcast messages(to member_id:2)
===========================================
Message high watermark: 14%
  Total messages buffered at high watermark: 578
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                           Total messages  Percentage
  VPN Clustering HA Client                         578        100%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0

MRT Tx of unitcast messages(to member_id:3)
===========================================
Message high watermark: 12%
  Total messages buffered at high watermark: 573
  [Per-client message usage at high watermark]
  ----------------------------------------------------------------
  Client name                           Total messages  Percentage
  VPN Clustering HA Client                         572         99%
  Cluster VPN Unique ID Client                       1          0%

Current MRT buffer usage: 0%
  Total messages buffered in real-time: 0
```

- **show cluster history**

  クラスタの履歴、およびクラスタノードが参加できなかった理由や、ノードがクラスタを離れた理由に関するエラーメッセージが表示されます。

クラスタ全体のパケットのキャプチャ

クラスタでのパケットのキャプチャについては、次のコマンドを参照してください。

cluster exec capture

クラスタ全体のトラブルシューティングをサポートするには、**cluster exec capture** コマンドを使用して制御ノード上でのクラスタ固有トラフィックのキャプチャを有効にします。これで、クラスタ内のすべてのデータノードでも自動的に有効になります。

クラスタリソースのモニタリング

クラスタリソースのモニタリングについては、次のコマンドを参照してください。

show cluster {**cpu** | **memory** | **resource**} [*options*]

クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

クラスタ トラフィックのモニタリング

クラスタトラフィックのモニタリングについては、次のコマンドを参照してください。

- **show conn [detail]、cluster exec show conn**

  show conn コマンドは、フローがディレクタ、バックアップ、またはフォワーダのどのフローであるかを示します。**cluster exec show conn** コマンドを任意のノードで使用すると、すべての接続が表示されます。このコマンドの表示からは、1 つのフローのトラフィックがクラスタ内のさまざまなASAにどのように到達するかがわかります。クラスタのスループットは、ロードバランシングの効率とコンフィギュレーションによって異なります。このコマンドを利用すると、ある接続のトラフィックがクラスタ内をどのように流れるかが簡単にわかります。また、ロードバランサがフローのパフォーマンスにどのように影響を与えるかを理解するのに役立ちます。

  また、**show conn detail** コマンドはフローモビリティの影響を受けるフローを表示します。

  次に、**show conn detail** コマンドの出力例を示します。

```
ciscoasa/ASA2/data node# show conn detail
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, b - TCP state-bypass or nailed,
       C - CTIQBE media, c - cluster centralized,
       D - DNS, d - dump, E - outside back connection, e - semi-distributed,
       F - outside FIN, f - inside FIN,
```

```
       G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
       i - incomplete, J - GTP, j - GTP data, K - GTP t3-response
       k - Skinny media, L - LISP triggered flow owner mobility,
       M - SMTP data, m - SIP media, n - GUP
       O - outbound data, o - offloaded,
       P - inside back connection,
       Q - Diameter, q - SQL*Net data,
       R - outside acknowledged FIN,
       R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up,
       V - VPN orphan, W - WAAS,
       w - secondary domain backup,
       X - inspected by service module,
       x - per session, Y - director stub flow, y - backup stub flow,
       Z - Scansafe redirection, z - forwarding stub flow
ESP outside: 10.1.227.1/53744 NP Identity Ifc: 10.1.226.1/30604, , flags c, idle 0s,
 uptime
1m21s, timeout 30s, bytes 7544, cluster sent/rcvd bytes 0/0, owners (0,255) Traffic
 received
at interface outside Locally received: 7544 (93 byte/s) Traffic received at interface
 NP
Identity Ifc Locally received: 0 (0 byte/s) UDP outside: 10.1.227.1/500 NP Identity
 Ifc:
10.1.226.1/500, flags -c, idle 1m22s, uptime 1m22s, timeout 2m0s, bytes 1580, cluster
sent/rcvd bytes 0/0, cluster sent/rcvd total bytes 0/0, owners (0,255) Traffic
received at
interface outside Locally received: 864 (10 byte/s) Traffic received at interface
NP Identity
Ifc Locally received: 716 (8 byte/s)
```

接続フローのトラブルシューティングを行うには、最初にすべてのノードの接続を一覧表示します。それには、任意のノードで **cluster exec show conn** コマンドを入力します。ディレクタ（Y）、バックアップ（y）、およびフォワーダ（z）のフラグを持つフローを探します。次の例には、3 つのすべての ASA での 172.18.124.187:22 から 192.168.103.131:44727 への SSH 接続が表示されています。ASA1 には z フラグがあり、この接続のフォワーダであることを表しています。ASA3 には Y フラグがあり、この接続のディレクタであることを表しています。ASA2 には特別なフラグはなく、これがオーナーであることを表しています。アウトバウンド方向では、この接続のパケットは ASA2 の内部インターフェイスに入り、外部インターフェイスから出ていきます。インバウンド方向では、この接続のパケットは ASA1 および ASA3 の外部インターフェイスに入り、クラスタ制御リンクを介して ASA2 に転送され、次に ASA2 の内部インターフェイスから出ていきます。

```
ciscoasa/ASA1/control node# cluster exec show conn
ASA1(LOCAL):**********************************************************
18 in use, 22 most used
Cluster stub connections: 0 in use, 5 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags z


ASA2:**********************************************************************
12 in use, 13 most used
Cluster stub connections: 0 in use, 46 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:00, bytes
37240828, flags UIO


ASA3:**********************************************************************
```

```
10 in use, 12 most used
Cluster stub connections: 2 in use, 29 most used
TCP outside  172.18.124.187:22 inside  192.168.103.131:44727, idle 0:00:03, bytes
0, flags  Y
```

- **show cluster info** [**conn-distribution** | **packet-distribution** | **loadbalance** | **flow-mobility counters**]

  show cluster info conn-distribution コマンドと **show cluster info packet-distribution** コマンドは、すべてのクラスタノードへのトラフィック分散を表示します。これらのコマンドは、外部ロードバランサを評価し、調整するのに役立ちます。

  show cluster info loadbalance コマンドは、接続再分散の統計情報を表示します。

  show cluster info flow-mobility counters コマンドは、EIDおよびフローの所有者の動作情報を表示します。**show cluster info flow-mobility counters** コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info flow-mobility counters
EID movement notification received  : 4
EID movement notification processed : 4
Flow owner moving requested         : 2
```

- **show cluster info load-monitor** [**details**]

  この**show cluster info load-monitor**コマンドは、最後の間隔のクラスタメンバのトラフィック負荷と、設定された間隔の合計数（デフォルトでは30）を表示します。各間隔の各測定値を表示するには、**details** キーワードを使用します。

```
ciscoasa(cfg-cluster)# show cluster info load-monitor
ID  Unit Name
0  B
1  A_1
Information from all units with 20 second interval:
Unit     Connections    Buffer Drops   Memory Used   CPU Used
Average from last 1 interval:
   0           0            0            14              25
   1           0            0            16              20
Average from last 30 interval:
   0           0            0            12              28
   1           0            0            13              27


ciscoasa(cfg-cluster)# show cluster info load-monitor details


ID  Unit Name

 0  B

 1  A_1

Information from all units with 20 second interval



Connection count captured over 30 intervals:

Unit ID  0
```

```
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
Unit ID  1
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0

Buffer drops captured over 30 intervals:
Unit ID  0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
Unit ID  1
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0
        0          0          0          0          0          0

Memory usage(%) captured over 30 intervals:
Unit ID  0
       25         25         30         30         30         35
       25         25         35         30         30         30
       25         25         30         25         25         35
       30         30         30         25         25         25
```

```
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35


CPU usage(%) captured over 30 intervals:
Unit ID  0
        25          25          30          30          30          35
        25          25          35          30          30          30
        25          25          30          25          25          35
        30          30          30          25          25          25
        25          20          30          30          30          30
Unit ID  1
        30          25          35          25          30          30
        25          25          35          25          30          35
        30          30          35          30          30          30
        25          20          30          25          25          30
        20          30          35          30          30          35
```

- **show cluster** {**access-list** | **conn** | **traffic** | **user-identity** | **xlate**} [*options*]

  クラスタ全体の集約データを表示します。使用可能な *options* はデータのタイプによって異なります。

  show cluster access-list コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster access-list
hitcnt display order: cluster-wide aggregated result, unit-A, unit-B,  unit-C, unit-D
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096) alert-interval
 300
access-list 101; 122 elements; name hash: 0xe7d586b5
access-list 101 line 1 extended permit tcp 192.168.143.0 255.255.255.0 any eq www
(hitcnt=0, 0, 0, 0, 0) 0x207a2b7d
access-list 101 line 2 extended permit tcp any 192.168.143.0 255.255.255.0 (hitcnt=0,
 0, 0, 0, 0) 0xfe4f4947
access-list  101 line 3 extended permit tcp host 192.168.1.183 host 192.168.43.238
(hitcnt=1, 0, 0, 0, 1) 0x7b521307
access-list 101 line 4 extended permit tcp host 192.168.1.116 host 192.168.43.238
(hitcnt=0, 0, 0, 0, 0) 0x5795c069
```

```
access-list 101 line 5 extended permit tcp host 192.168.1.177 host 192.168.43.238
(hitcnt=1, 0, 0, 1, 0) 0x51bde7ee
access list 101 line 6 extended permit tcp host 192.168.1.177 host 192.168.43.13
(hitcnt=0, 0, 0, 0, 0) 0x1e68697c
access-list 101 line 7 extended permit tcp host 192.168.1.177 host 192.168.43.132
(hitcnt=2, 0, 0, 1, 1) 0xc1ce5c49
access-list 101 line 8 extended permit tcp host 192.168.1.177 host 192.168.43.192
(hitcnt=3, 0, 1, 1, 1) 0xb6f59512
access-list 101 line 9 extended permit tcp host 192.168.1.177 host 192.168.43.44
(hitcnt=0, 0, 0, 0, 0) 0xdc104200
access-list 101 line 10 extended permit tcp host 192.168.1.112 host 192.168.43.44
(hitcnt=429, 109, 107, 109, 104)
0xce4f281d
access-list 101 line 11 extended permit tcp host 192.168.1.170 host 192.168.43.238
(hitcnt=3, 1, 0, 0, 2) 0x4143a818
access-list 101 line 12 extended permit tcp host 192.168.1.170 host 192.168.43.169
(hitcnt=2, 0, 1, 0, 1) 0xb18dfea4
access-list 101 line 13 extended permit tcp host 192.168.1.170 host 192.168.43.229
(hitcnt=1, 1, 0, 0, 0) 0x21557d71
access-list 101 line 14 extended permit tcp host 192.168.1.170 host 192.168.43.106
(hitcnt=0, 0, 0, 0, 0) 0x7316e016
access-list 101 line 15 extended permit tcp host 192.168.1.170 host 192.168.43.196
(hitcnt=0, 0, 0, 0, 0) 0x013fd5b8
access-list 101 line 16 extended permit tcp host 192.168.1.170 host 192.168.43.75
(hitcnt=0, 0, 0, 0, 0) 0x2c7dba0d
```

使用中の接続の、すべてのノードでの合計数を表示するには、次のとおりに入力します。

```
ciscoasa# show cluster conn count
Usage Summary In Cluster:*********************************************
  200 in use (cluster-wide aggregated)
     cl2(LOCAL):************************************************************
  100 in use, 100 most used

  cl1:********************************************************************
  100 in use, 100 most used
```

- **show asp cluster counter**

  このコマンドは、データパスのトラブルシューティングに役立ちます。

クラスタのルーティングのモニタリング

クラスタのルーティングについては、次のコマンドを参照してください。

- **show route cluster**
- **debug route cluster**

  クラスタのルーティング情報を表示します。

- **show lisp eid**

  EIDs とサイト ID を示す ASA EID テーブルを表示します。

  cluster exec show lisp eid コマンドからの、次の出力を参照してください。

```
ciscoasa# cluster exec show lisp eid
L1(LOCAL):**********************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1             4
    11.22.11.2             4
L2:**********************************************************************
     LISP EID       Site ID
    33.44.33.105        2
    33.44.33.201        2
    11.22.11.1   4
    11.22.11.2  4
```

- **show asp table classify domain inspect-lisp**

  このコマンドは、トラブルシューティングに役立ちます。

クラスタリングのロギングの設定

クラスタリングのロギングの設定については、次のコマンドを参照してください。

logging device-id

クラスタ内の各ノードは、syslog メッセージを個別に生成します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるノードからのメッセージのように見せることができます。

クラスタのインターフェイスのモニタリング

クラスタのインターフェイスのモニタリングについては、次のコマンドを参照してください。

- **show cluster interface-mode**

  クラスタ インターフェイスのモードを表示します。

クラスタリングのデバッグ

クラスタリングのデバッグについては、次のコマンドを参照してください。

- **debug cluster [ccp | datapath | fsm | general | hc | license | rpc | transport]**

  クラスタリングのデバッグ メッセージを表示します。

- **debug cluster flow-mobility**

  クラスタリング フロー モビリティ関連のイベントを表示します。

- **debug lisp eid-notify-intercept**

  EID 通知メッセージ代行受信時のイベントを表示します。

- **show cluster info trace**

show cluster info trace コマンドは、トラブルシューティングのためのデバッグ情報を表示します。

show cluster info trace コマンドについては次の出力を参照してください。

```
ciscoasa# show cluster info trace
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Receive CCP message: CCP_MSG_LOAD_BALANCE
 Feb 02 14:19:47.456 [DBUG]Send CCP message to all: CCP_MSG_KEEPALIVE from 80-1 at
CONTROL_NODE
```

たとえば、同じ**ローカルユニット**名を持つ2つのノードが制御ノードとして機能していることを示す次のメッセージが表示された場合は、2 つのノードの**ローカルユニット**名が同じである（設定を確認してください）か、1つのノードが自身のブロードキャストメッセージを受信している（ネットワークを確認してください）可能性があります。

```
ciscoasa# show cluster info trace
 May 23 07:27:23.113 [CRIT]Received datapath event 'multi control_nodes' with parameter
 1.
 May 23 07:27:23.113 [CRIT]Found both unit-9-1 and unit-9-1 as control_node units.
Control_node role retained by unit-9-1, unit-9-1 will leave then join as a Data_node

 May 23 07:27:23.113 [DBUG]Send event (DISABLE, RESTART | INTERNAL-EVENT, 5000 msecs,
 Detected another Control_node, leave and re-join as Data_node) to FSM. Current state
 CONTROL_NODE
 May 23 07:27:23.113 [INFO]State machine changed from state CONTROL_NODE to DISABLED
```

クラスタリングの参考資料

このセクションには、クラスタリングの動作に関する詳細情報が含まれます。

ASA の各機能とクラスタリング

ASA の一部の機能は ASA クラスタリングではサポートされず、一部の機能は制御ノードだけでサポートされます。その他の機能については適切な使用に関する警告がある場合があります。

クラスタリングでサポートされない機能

次の各機能は、クラスタリングが有効なときは設定できず、コマンドは拒否されます。

- TLS プロキシを使用するユニファイド コミュニケーション機能
- リモート アクセス VPN（SSL VPN および IPSec VPN）
- 仮想トンネルインターフェイス（VTI）
- 次のアプリケーション インスペクション：

- CTIQBE
- H323、H225、および RAS
- IPsec パススルー
- MGCP
- MMP
- RTSP
- SCCP（Skinny）
- WAAS
- WCCP

- ボットネット トラフィック フィルタ
- Auto Update Server
- DHCP クライアント、サーバー、およびプロキシ。DHCP リレーはサポートされています。
- VPN ロード バランシング
- Azure でのフェールオーバー
- 統合ルーティングおよびブリッジング
- FIPS モード

クラスタリングの中央集中型機能

次の機能は、制御ノード上だけでサポートされます。クラスタの場合もスケーリングされません。

（注） 中央集中型機能のトラフィックは、クラスタ制御リンク経由でメンバーノードから制御ノードに転送されます。

再分散機能を使用する場合は、中央集中型機能のトラフィックが中央集中型機能として分類される前に再分散が行われて、制御ノード以外のノードに転送されることがあります。この場合は、トラフィックが制御ノードに送り返されます。

中央集中型機能については、制御ノードで障害が発生するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

- 次のアプリケーション インスペクション：
  - DCERPC
  - ESMTP

- IM
- NetBIOS
- PPTP
- RADIUS
- RSH
- SNMP
- SQLNET
- SUNRPC
- TFTP
- XDMCP

- スタティック ルート モニタリング
- ネットワーク アクセスの認証および許可。アカウンティングは非集中型です。
- フィルタリング サービス
- サイト間 VPN
- マルチキャスト ルーティング

個々のノードに適用される機能

これらの機能は、クラスタ全体または制御ノードではなく、各 ASA ノードに適用されます。

- QoS：QoS ポリシーは、コンフィギュレーション複製の一部としてクラスタ全体で同期されます。ただし、ポリシーは各ノードに個別に適用されます。たとえば、出力に対してポリシングを設定する場合は、適合レートおよび適合バースト値は、特定の ASA から出て行くトラフィックに適用されます。3 ノードから成るクラスタがあり、トラフィックが均等に分散している場合、適合レートは実際にクラスタのレートの 3 倍になります。
- 脅威検出：脅威検出はノードごとに個別に機能します。たとえば、上位統計情報はノード固有です。たとえば、ポートスキャン検出が機能しないのは、スキャントラフィックが全ノード間でロードバランシングされ、1 つのノードですべてのトラフィックを確認できないためです。

ネットワーク アクセス用の AAA とクラスタリング

ネットワーク アクセス用の AAA は、認証、許可、アカウンティングの 3 つのコンポーネントで構成されます。認証と許可は、クラスタリング制御ノード上で中央集中型機能として実装されており、データ構造がクラスタデータノードに複製されます。制御ノードが選択された場合、確立済みの認証済みユーザおよびユーザに関連付けられた許可を引き続き中断なく運用するために必要なすべての情報を新しい制御ノードが保有します。ユーザ認証のアイドルおよび絶対タイムアウトは、制御ノードが変更されたときも維持されます。

アカウンティングは、クラスタ内の分散型機能として実装されています。アカウンティングはフロー単位で実行されるため、フローに対するアカウンティングが設定されている場合、そのフローを所有するクラスタノードがアカウンティング開始と停止のメッセージを AAA サーバに送信します。

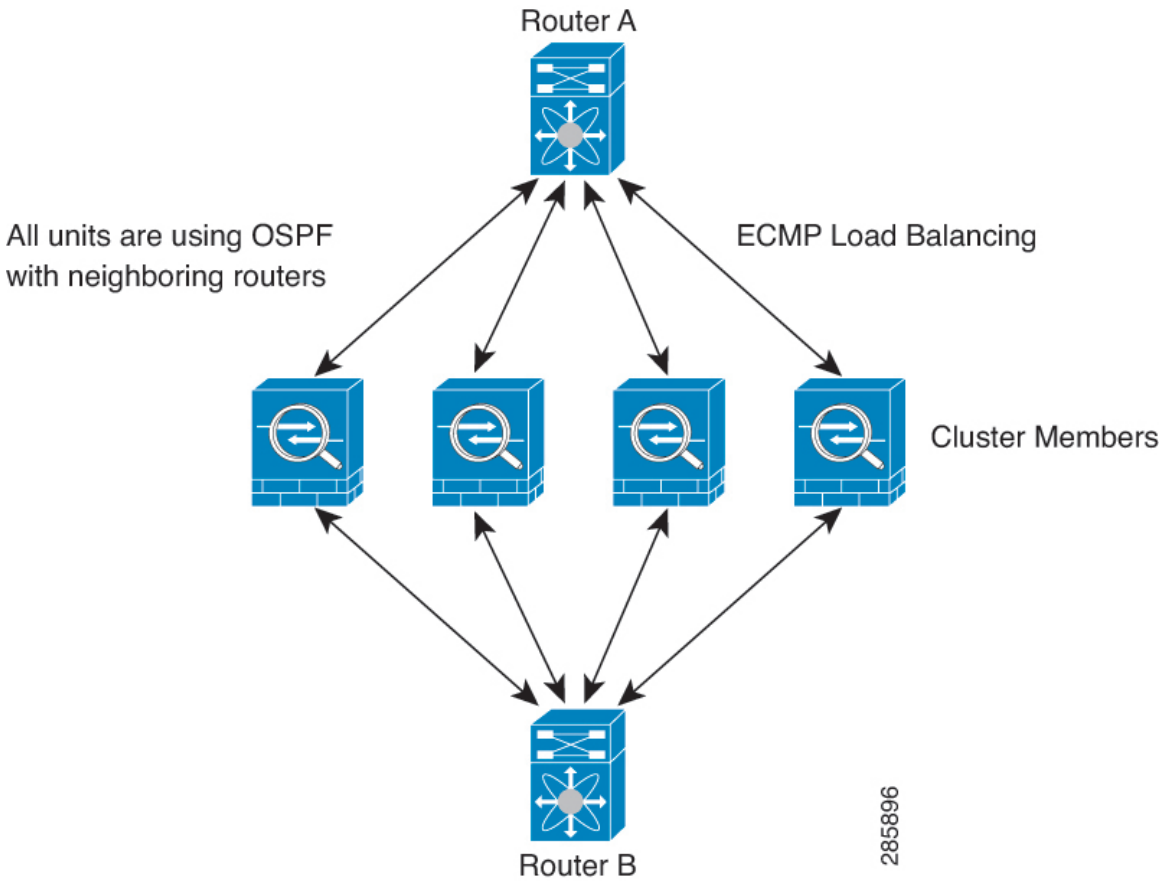
接続設定とクラスタリング

接続制限は、クラスタ全体に適用されます（**set connection conn-max**、**set connection embryonic-conn-max**、**set connection per-client-embryonic-max**、および **set connection per-client-max** コマンドを参照）。各ノードには、ブロードキャストメッセージに基づくクラスタ全体のカウンタの推定値があります。クラスタ全体で接続制限を設定しても、効率性を考慮して、厳密に制限数で適用されない場合があります。各ノードでは、任意の時点でのクラスタ全体のカウンタ値が過大評価または過小評価される可能性があります。ただし、ロードバランシングされたクラスタでは、時間の経過とともに情報が更新されます。

ダイナミック ルーティングおよびクラスタリング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *68* : 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィックゾーンにこれらすべてのノードインターフェイスをまとめます。トラフィック ゾーンの設定 （995 ページ）を参照してください。

FTP とクラスタリング

- FTP データ チャネルとコントロール チャネルのフローがそれぞれ別のクラスタ メンバよって所有されている場合は、データ チャネルのオーナーは定期的にアイドル タイムアウト アップデートをコントロール チャネルのオーナーに送信し、アイドル タイムアウト値を更新します。ただし、コントロール フローのオーナーがリロードされて、コントロール フローが再ホスティングされた場合は、親子フロー関係は維持されなくなります。したがって、コントロール フローのアイドル タイムアウトは更新されません。
- FTP アクセスに AAA を使用する場合、制御チャネルのフローは制御ノードに集中されます。

ICMP インスペクションとクラスタリング

クラスタを通過する ICMP および ICMP エラーパケットのフローは、ICMP/ICMP エラーインスペクションが有効かどうかによって異なります。ICMP インスペクションを使用しない場合、ICMP は一方向のフローであり、ディレクタフローはサポートされません。ICMP インスペクションを使用する場合、ICMP フローは双方向になり、ディレクタ/バックアップフローによってバックアップされます。検査された ICMP フローの違いの 1 つは、転送されたパケットのディレクタ処理にあります。ディレクタは、パケットをフォワーダに返す代わりに、フローオーナーに ICMP エコー応答パケットを転送します。

マルチキャスト ルーティングとクラスタリング

個別インターフェイス モードでは、マルチキャストに関してユニットが個別に動作することはありません。データおよびルーティングのパケットはすべて制御ユニットで処理されて転送されるので、パケットレプリケーションが回避されます。

NAT とクラスタリング

NAT は、クラスタの全体的なスループットに影響を与えることがあります。インバウンドおよびアウトバウンドの NAT パケットが、それぞれクラスタ内の別の ASA に送信されることがあります。ロード バランシング アルゴリズムは IP アドレスとポートに依存していますが、NAT が使用されるときは、インバウンドとアウトバウンドとで、パケットの IP アドレスやポートが異なるからです。NAT オーナーではない ASA に到着したパケットは、クラスタ制御リンクを介してオーナーに転送されるため、クラスタ制御リンクに大量のトラフィックが発生します。NAT オーナーは、セキュリティおよびポリシーチェックの結果に応じてパケットの接続を作成できない可能性があるため、受信側ノードは、オーナーへの転送フローを作成しないことに注意してください。

それでもクラスタリングで NAT を使用する場合は、次のガイドラインを考慮してください。

- プロキシ ARP なし：個別インターフェイスの場合は、マッピング アドレスについてプロキシ ARP 応答が送信されることはありません。これは、クラスタに存在しなくなった可能性のある ASA と隣接ルータとがピア関係を維持することを防ぐためです。アップストリーム ルータは、メイン クラスタ IP アドレスを指すマッピング アドレスについてはスタティック ルートまたは PBR とオブジェクト トラッキングを使用する必要があります。これは、スパンド EtherChannel の問題ではありません。クラスタ インターフェイスには関連付けられた IP アドレスが 1 つしかないためです。

- ポート ブロック割り当てによる PAT：この機能については、次のガイドラインを参照してください。

  - ホストあたりの最大制限は、クラスタ全体の制限ではなく、ノードごとに個別に適用されます。したがって、ホストあたりの最大制限が 1 に設定されている 3 ノードクラスタでは、ホストからのトラフィックが 3 つのノードすべてにロードバランシングされている場合、3 つのブロックを各ノードに 1 つずつ割り当てることができます。

  - バックアッププールからバックアップノードで作成されたポートブロックは、ホストあたりの最大制限の適用時には考慮されません。

  - PAT プールが完全に新しい IP アドレスの範囲で変更される On-the-fly PAT ルールの変更では、新しいプールが有効になっていてもいまだ送信中の xlate バックアップ要求に対する xlate バックアップの作成が失敗します。この動作はポートのブロック割り当て機能に固有なものではなく、プールが分散されトラフィックがクラスタノード間でロードバランシングされるクラスタ展開でのみ見られる一時的な PAT プールの問題です。

  - クラスタで動作している場合、ブロック割り当てサイズを変更することはできません。新しいサイズは、クラスタ内の各デバイスをリロードした後にのみ有効になります。各デバイスのリロードの必要性を回避するために、すべてのブロック割り当てルールを削除し、それらのルールに関連するすべての xlate をクリアすることをお勧めします。その後、ブロックサイズを変更し、ブロック割り当てルールを再作成できます。

- ダイナミック PAT の NAT プールアドレス配布：PAT プールを設定すると、クラスタはプール内の各 IP アドレスをポートブロックに分割します。デフォルトでは、各ブロックは 512 ポートですが、ポートブロック割り当てルールを設定すると、代わりにユーザのブロック設定が使用されます。これらのブロックはクラスタ内のノード間で均等に分散されるため、各ノードには PAT プール内の IP アドレスごとに 1 つ以上のブロックがあります。したがって、想定される PAT 接続数に対して十分である場合には、クラスタの PAT プールに含める IP アドレスを 1 つだけにすることができます。PAT プールの NAT ルールで予約済みポート 1 ～ 1023 を含めるようにオプションを設定しない限り、ポートブロックは 1024 ～ 65535 のポート範囲をカバーします。

- 複数のルールにおける PAT プールの再利用：複数のルールで同じ PAT プールを使用するには、ルールにおけるインターフェイスの選択に注意を払う必要があります。すべてのルールで特定のインターフェイスを使用するか、あるいはすべてのルールで「任意の」インターフェイスを使用するか、いずれかを選択する必要があります。ルール全般にわたって特定のインターフェイスと「任意」のインターフェイスを混在させることはできません。混在させると、システムがリターントラフィックとクラスタ内の適切なノードを一致させることができなくなる場合があります。ルールごとに固有の PAT プールを使用することは、最も信頼性の高いオプションです。

- ラウンドロビンなし：PAT プールのラウンドロビンは、クラスタリングではサポートされません。

- 拡張 PAT なし：拡張 PAT はクラスタリングでサポートされません。

- 制御ノードによって管理されるダイナミック NAT xlate：制御ノードが xlate テーブルを維持し、データノードに複製します。ダイナミック NAT を必要とする接続をデータノードが受信したときに、その xlate がテーブル内にない場合、データノードは制御ノードに xlate を要求します。データノードが接続を所有します。

- 旧式の xlate：接続所有者の xlate アイドル時間が更新されません。したがって、アイドル時間がアイドルタイムアウトを超える可能性があります。refcnt が 0 で、アイドルタイマー値が設定されたタイムアウトより大きい場合は、旧式の xlate であることを示します。

- per-session PAT 機能：クラスタリングに限りませんが、per-session PAT 機能によって PAT の拡張性が向上します。クラスタリングの場合は、各データノードが独自の PAT 接続を持てます。対照的に、multi-session PAT 接続は制御ノードに転送する必要があり、制御ノードがオーナーとなります。デフォルトでは、すべての TCP トラフィックおよび UDP DNS トラフィックは per-session PAT xlate を使用します。これに対し、ICMP および他のすべての UDP トラフィックは multi-session を使用します。TCP および UDP に対しこれらのデフォルトを変更するように per-session NAT ルールを設定できますが、ICMP に per-session PAT を設定することはできません。たとえば、TCP/443 の HTTPS TLS と比較してずっと優れたパフォーマンスを発揮する代替手段として、UDP/443 を用いる Quick プロトコルの使用が増加している場合、UDP/443 に対し per-session PAT を有効にする必要があります。H.323、SIP、または Skinny などの multi-session PAT のメリットを活用できるトラフィックでは、関連付けられている TCP ポートに対し per-session PAT を無効にできます（それらの H.323 および SIP の UDP ポートはデフォルトですでに multi-session になっています）。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

- 次のインスペクション用のスタティック PAT はありません。
  - FTP
  - PPTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- 1 万を超える非常に多くの NAT ルールがある場合は、デバイスの CLI で **asp rule-engine transactional-commit nat** コマンドを使用してトランザクション コミット モデルを有効にする必要があります。有効にしないと、ノードがクラスタに参加できない可能性があります。

SCTP とクラスタリング

SCTP アソシエーションは、（ロードバランシングにより）任意のノードに作成できますが、マルチホーミング接続は同じノードに存在する必要があります。

SIP インスペクションとクラスタリング

制御フローは、（ロードバランシングにより）任意のノードに作成できますが、子データフローは同じノードに存在する必要があります。

TLS プロキシ設定はサポートされていません。

SNMP とクラスタリング

SNMP エージェントは、個々の ASA を、その 診断インターフェイスのローカル IP アドレスによってポーリングします。クラスタの統合データをポーリングすることはできません。

SNMP ポーリングには、メイン クラスタ IP アドレスではなく、常にローカル アドレスを使用してください。SNMP エージェントがメインクラスタ IP アドレスをポーリングする場合、新しい制御ノードが選択されると、新しい制御ノードのポーリングは失敗します。

クラスタリングでSNMPv3を使用している場合、最初のクラスタ形成後に新しいクラスタノードを追加すると、SNMPv3ユーザは新しいノードに複製されません。SNMPv3ユーザは、制御ノードに再追加して、新しいノードに強制的に複製するようにするか、データノードに直接追加する必要があります。ユーザを削除して再追加し、設定を再展開して、ユーザを新しいノードに強制的に複製する必要があります。

STUN とクラスタリング

ピンホールが複製されるとき、STUNインスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はノード間で複製されません。

STUN 要求の受信後にノードに障害が発生し、別のノードが STUN 応答を受信した場合、STUN 応答はドロップされます。

syslog とクラスタリング

- Syslog：クラスタの各ノードは自身の syslog メッセージを生成します。ロギングを設定して、各ノードの syslog メッセージ ヘッダー フィールドで同じデバイス ID を使用するか、別の ID を使用するかを設定できます。たとえば、ホスト名設定はクラスタ内のすべてのノードに複製されて共有されます。ホスト名をデバイス ID として使用するようにロギングを設定した場合、すべてのノードで生成される syslog メッセージが 1 つのノードから生成されているように見えます。クラスタブートストラップ設定で割り当てられたローカル ノード名をデバイス ID として使用するようにロギングを設定した場合、syslog メッセージはそれぞれ別のノードから生成されているように見えます。
- NetFlow：クラスタの各ノードは自身の NetFlow ストリームを生成します。NetFlow コレクタは、各 ASA を独立した NetFlow エクスポータとしてのみ扱うことができます。

Cisco TrustSec とクラスタリング

制御ノードだけがセキュリティグループタグ（SGT）情報を学習します。その後、制御ノードからデータノードに SGT が渡されるため、データノードは、セキュリティポリシーに基づいて SGT の一致を判断できます。

VPN とクラスタリング

サイト間 VPN は、中央集中型機能です。制御ノードのみが VPN 接続をサポートします。

（注） リモート アクセス VPN は、クラスタリングではサポートされません。

VPN 機能を使用できるのは制御ノードだけであり、クラスタの高可用性機能は活用されません。制御ノードで障害が発生した場合は、すべての既存の VPN 接続が失われ、VPN ユーザにとってはサービスの中断となります。新しい制御ノードが選定されたときに、VPN 接続を再確立する必要があります。

PBR または ECMP を使用するときの個別インターフェイスへの接続については、ローカル アドレスではなく、常にメイン クラスタ IP アドレスに接続する必要があります。

VPN 関連のキーと証明書は、すべてのノードに複製されます。

パフォーマンス スケーリング係数

複数のユニットをクラスタに結合すると、期待できる合計クラスタパフォーマンスは、最大合計スループットの約 80%になります。

たとえば、モデルが単独稼働で約 10 Gbps のトラフィックを処理できる場合、8 ユニットのクラスタでは、最大合計スループットは 80 Gbps（8 ユニット x 10 Gbps）の約 80% で 64 Gbps になります。

制御ノードの選定

クラスタのノードは、クラスタ制御リンクを介して通信して制御ノードを選定します。方法は次のとおりです。

1. ノードに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのノードは選定要求を 3 秒間隔でブロードキャストします。
2. プライオリティの高い他のノードがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。
3. 45 秒経過しても、プライオリティの高い他のノードからの応答を受信していない場合は、そのノードが制御ノードになります。

（注） 最高のプライオリティを持つノードが複数ある場合は、クラスタノード名、次にシリアル番号を使用して制御ノードが決定されます。

4. 後からクラスタに参加したノードのプライオリティの方が高い場合でも、そのノードが自動的に制御ノードになることはありません。既存の制御ノードは常に制御ノードのままです。ただし、制御ノードが応答を停止すると、その時点で新しい制御ノードが選定されます。
5. 「スプリットブレイン」シナリオで一時的に複数の制御ノードが存在する場合、優先順位が最も高いノードが制御ノードの役割を保持し、他のノードはデータノードの役割に戻ります。

（注） ノードを手動で強制的に制御ノードにすることができます。中央集中型機能については、制御ノード変更を強制するとすべての接続がドロップされるので、新しい制御ノード上で接続を再確立する必要があります。

クラスタ内のハイアベイラビリティ

クラスタリングは、ノードとインターフェイスの正常性をモニターし、ノード間で接続状態を複製することにより、ハイアベイラビリティを実現します。

ノードヘルスモニタリング

各ノードは、クラスタ制御リンクを介してブロードキャスト ハートビート パケットを定期的に送信します。設定可能なタイムアウト期間内にデータノードからハートビートパケットまたはその他のパケットを受信しない場合、制御ノードはクラスタからデータノードを削除します。データノードが制御ノードからパケットを受信しない場合、残りのノードから新しい制御ノードが選択されます。

ノードで実際に障害が発生したためではなく、ネットワークの障害が原因で、ノードがクラスタ制御リンクを介して相互に通信できない場合、クラスタは「スプリットブレイン」シナリオに移行する可能性があります。このシナリオでは、分離されたデータノードが独自の制御ノードを選択します。たとえば、2 つのクラスタロケーション間でルータに障害が発生した場合、ロケーション 1 の元の制御ノードは、ロケーション 2 のデータノードをクラスタから削除します。一方、ロケーション2のノードは、独自の制御ノードを選択し、独自のクラスタを形成します。このシナリオでは、非対称トラフィックが失敗する可能性があることに注意してください。クラスタ制御リンクが復元されると、より優先順位の高い制御ノードが制御ノードの役割を保持します。

インターフェイス モニタリング

各ノードは、使用中のすべての指名されたハードウェアインターフェイスのリンクステータスをモニタし、ステータス変更を制御ノードに報告します。

ヘルスモニタリングを有効化すると、すべての物理インターフェイスがデフォルトでモニターされるため、オプションでインターフェイスごとのモニタリングを無効化することができます。指名されたインターフェイスのみモニターできます。

ノードのモニタ対象のインターフェイスが失敗した場合、そのノードはクラスタから削除されます。ASAがメンバーをクラスタから削除するまでの時間は、そのノードが確立済みメンバーであるか、またはクラスタに参加しようとしているかによって異なります。ASAは、ノードがクラスタに参加する最初の90秒間はインターフェイスを監視しません。この間にインターフェイスのステータスが変化しても、ASA はクラスタから削除されません。ノード状態に関係なく、ノードは 500 ミリ秒後に削除されます。

障害後のステータス

制御ノードで障害が発生した場合、そのクラスタの他のメンバーのうち、優先順位が最高（番号が最小）のメンバーが制御ノードになります。

障害イベントに応じて、ASA は自動的にクラスタへの再参加を試みます。

（注） ASAが非アクティブになり、クラスタへの自動再参加に失敗すると、すべてのデータインターフェイスがシャットダウンされ、管理専用インターフェイスのみがトラフィックを送受信できます。管理インターフェイスは、そのノードがクラスタ IP プールから受け取った IP アドレスを使用して引き続き稼働状態となります。ただし、リロードする場合、クラスタでノードがまだ非アクティブになっていると、管理インターフェイスは無効になります。さらに設定を行う場合は、コンソールポートを使用する必要があります。

クラスタへの再参加

クラスタノードがクラスタから削除された後、クラスタに再参加するための方法は、削除された理由によって異なります。

- クラスタ制御リンクの障害：（最初の参加時）クラスタ制御リンクの問題を解決した後、CLI で **cluster group** 名 を入力してから **enable** と入力して、クラスタリングを再び有効化することによって、手動でクラスタに再参加する必要があります。
- クラスタに参加した後に障害が発生したクラスタ制御リンク：ASA は、無限に 5 分ごとに自動的に再参加を試みます。この動作は設定可能です。
- データ インターフェイスの障害：ASA は自動的に最初は 5 分後、次に 10 分後、最終的に 20 分後に再参加を試みます。20 分後に参加できない場合、ASA はクラスタリングをディセーブルにします。データインターフェイスの問題を解決した後、CLIで **cluster group** *name* と入力してから **enable** と入力して、クラスタリングを手動で有効化する必要があります。この動作は設定可能です。
- ノードの障害：ノードがヘルスチェック失敗のためクラスタから削除された場合、クラスタへの再参加は失敗の原因によって異なります。たとえば、一時的な電源障害の場合は、クラスタ制御リンクが稼働していて、クラスタリングが **enable** コマンドでまだイネーブルになっているなら、ノードは再起動するとクラスタに再参加することを意味します。ASA は 5 秒ごとにクラスタへの再参加を試みます。
- 内部エラー：内部の障害には、アプリケーション同期のタイムアウト、矛盾したアプリケーション ステータスなどがあります。ノードは、5 分、10 分、20 分の間隔で自動的にクラスタに再参加しようとします。この動作は設定可能です。

データ パス接続状態の複製

どの接続にも、1 つのオーナーおよび少なくとも 1 つのバックアップ オーナーがクラスタ内にあります。バックアップ オーナーは、障害が発生しても接続を引き継ぎません。代わりに、TCP/UDP のステート情報を保存します。これは、障害発生時に接続が新しいオーナーにシームレスに移管されるようにするためです。バックアップ オーナーは通常ディレクタでもあります。

トラフィックの中には、TCP または UDP レイヤよりも上のステート情報を必要とするものがあります。この種類のトラフィックに対するクラスタリングのサポートの可否については、次の表を参照してください。

表 *23*：クラスタ全体で複製される機能

Traffic	状態のサポート	注意
Up time	Yes	システムアップタイムをトラッキングします。
ARP Table	あり	—
MAC アドレス テーブル	あり	—

Traffic	状態のサポート	注意
ユーザ アイデンティティ	Yes	AAA ルール（uauth）が含まれます。
IPv6 ネイバー データベース	○	—
ダイナミック ルーティング	○	—
SNMP エンジン ID	**[いいえ（No）]**	—
Firepower 4100/9300 の分散型 VPN（サイト間）	Yes	バックアップセッションがアクティブセッションになると、新しいバックアップセッションが作成されます。

クラスタが接続を管理する方法

接続をクラスタの複数のノードにロードバランシングできます。接続のロールにより、通常動作時とハイ アベイラビリティ状況時の接続の処理方法が決まります。

接続のロール

接続ごとに定義された次のロールを参照してください。

- オーナー：通常、最初に接続を受信するノード。オーナーは、TCP状態を保持し、パケットを処理します。1 つの接続に対してオーナーは 1 つだけです。元のオーナーに障害が発生すると、新しいノードが接続からパケットを受信したときにディレクタがそれらのノードの新しいオーナーを選択します。
- バックアップオーナー：オーナーから受信したTCP/UDPステート情報を格納するノード。障害が発生した場合、新しいオーナーにシームレスに接続を転送できます。バックアップオーナーは、障害発生時に接続を引き継ぎません。オーナーが使用不可能になった場合、（ロードバランシングに基づき）その接続からのパケットを受信する最初のノードがバックアップオーナーに問い合わせて、関連するステート情報を取得し、そのノードが新しいオーナーになります。

  ディレクタ（下記参照）がオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  1 台のシャーシに最大 3 つのクラスタノードを搭載できる Firepower 9300 のクラスタリングでは、バックアップオーナーがオーナーと同じシャーシにある場合、シャーシ障害からフローを保護するために、別のシャーシから追加のバックアップオーナーが選択されます。

  サイト間クラスタリングのディレクタ ローカリゼーションを有効にすると、ローカルバックアップとグローバルバックアップの2つのバックアップ オーナー権限があります。オーナーは、常に同じサイトのローカルバックアップをオーナー自身として選択します（サイトIDに基づいて）。グローバルバックアップはどのサイトにあってもよく、ローカルバッ

クアップと同一ノードとすることもできます。オーナーは、両方のバックアップへ接続ステート情報を送信します。

サイトの冗長性を有効にし、バックアップ オーナーがオーナーと同じサイトにある場合は、サイトの障害からフローを保護するために、追加のバックアップ オーナーが別のサイトから選択されます。シャーシバックアップとサイトバックアップは独立しているため、フローにはシャーシ バックアップとサイト バックアップの両方が含まれている場合があります。

- ディレクタ：フォワーダからのオーナールックアップ要求を処理するノード。オーナーは、新しい接続を受信すると、送信元/宛先 IP アドレスおよびポートのハッシュに基づいてディレクタを選択し、新しい接続を登録するためにそのディレクタにメッセージを送信します。パケットがオーナー以外のノードに到着した場合、そのノードはどのノードがオーナーかをディレクタに問い合わせることで、パケットを転送できます。1 つの接続に対してディレクタは1つだけです。ディレクタが失敗すると、オーナーは新しいディレクタを選択します。

  ディレクタがオーナーと同じノードでない限り、ディレクタはバックアップオーナーでもあります（上記参照）。オーナーがディレクタとして自分自身を選択すると、別のバックアップ オーナーが選択されます。

  サイト間クラスタリングのディレクタローカリゼーションを有効にすると、ローカルディレクタとグローバルディレクタの2つのディレクタ権限が区別されます。オーナーは、同一サイト（Site Idに基づき）のローカルディレクタとして、常にオーナー自身を選択します。グローバルディレクタはどのサイトにあってもよく、ローカルディレクタと同一ノードとすることもできます。元のオーナーに障害が発生すると、ローカルディレクタはこのサイトで新しい接続オーナーを選択します。

  ICMP/ICMPv6 ハッシュの詳細：

  - エコーパケットの場合、送信元ポートは ICMP 識別子であり、宛先ポートは 0 です。
  - 応答パケットの場合、送信元ポートは 0 で、宛先ポートは ICMP 識別子です。
  - 他のパケットの場合、送信元ポートと宛先ポートの両方が 0 です。

- フォワーダ：パケットをオーナーに転送するノード。フォワーダが接続のパケットを受信したときに、その接続のオーナーが自分ではない場合は、フォワーダはディレクタにオーナーを問い合わせてから、そのオーナーへのフローを確立します。これは、この接続に関してフォワーダが受信するその他のパケット用です。ディレクタは、フォワーダにもなることができます。ディレクタのローカリゼーションを有効にすると、フォワーダは常にローカルディレクタに問い合わせます。フォワーダがグローバルディレクタに問い合わせを行うのは、ローカルディレクタがオーナーを認識していない場合だけです。たとえば、別のサイトで所有されている接続のパケットをクラスタ メンバーが受信する場合などです。フォワーダがSYN-ACKパケットを受信した場合、フォワーダはパケットのSYNクッキーからオーナーを直接取得できるので、ディレクタに問い合わせる必要がないことに注意してください（TCP シーケンスのランダム化を無効にした場合は、SYN Cookie は使用されないので、ディレクタへの問い合わせが必要です）。存続期間が短いフロー（たとえばDNSやICMP）の場合は、フォワーダは問い合わせの代わりにパケットを即座にディレ

クタに送信し、ディレクタがそのパケットをオーナーに送信します。1つの接続に対して、複数のフォワーダが存在できます。最も効率的なスループットを実現できるのは、フォワーダが1つもなく、接続のすべてのパケットをオーナーが受信するという、優れたロードバランシング方法が使用されている場合です。

（注） クラスタリングを使用する場合は、TCP シーケンスのランダム化を無効にすることは推奨されません。SYN/ACK パケットがドロップされる可能性があるため、一部の TCP セッションが確立されない可能性があります。

- フラグメントオーナー：フラグメント化されたパケットの場合、フラグメントを受信するクラスタノードは、フラグメントの送信元と宛先の IP アドレス、およびパケット ID のハッシュを使用してフラグメントオーナーを特定します。その後、すべてのフラグメントがクラスタ制御リンクを介してフラグメント所有者に転送されます。スイッチのロードバランスハッシュで使用される 5 タプルは、最初のフラグメントにのみ含まれているため、フラグメントが異なるクラスタノードにロードバランシングされる場合があります。他のフラグメントには、送信元ポートと宛先ポートは含まれず、他のクラスタノードにロードバランシングされる場合があります。フラグメント所有者は一時的にパケットを再アセンブルするため、送信元/宛先 IP アドレスとポートのハッシュに基づいてディレクタを指定できます。新しい接続の場合は、フラグメントの所有者が接続所有者として登録されます。既存の接続の場合、フラグメント所有者は、クラスタ制御リンクを介して、指定された接続所有者にすべてのフラグメントを転送します。その後、接続所有者はすべてのフラグメントを再構築します。

接続でポート アドレス変換（PAT）を使用すると、PAT のタイプ（per-session または multi-session）が、クラスタのどのメンバが新しい接続のオーナーになるかに影響します。

- per-session PAT：オーナーは、接続の最初のパケットを受信するノードです。

  デフォルトでは、TCP および DNS UDP トラフィックは per-session PAT を使用します。

- multi-session PAT：オーナーは常に制御ノードです。multi-session PAT 接続がデータノードで最初に受信される場合、データノードがその接続を制御ノードに転送します。

  デフォルトでは、UDP（DNS UDP を除く）および ICMP トラフィックは multi-session PAT を使用するため、それらの接続は常に制御ノードによって所有されています。

TCP および UDP の per-session PAT デフォルトを変更できるので、これらのプロトコルの接続は、その設定に応じて per-session または multi-session で処理されます。ICMP の場合は、デフォルトの multi-session PAT から変更することはできません。per-session PAT の詳細については、『ファイアウォールの構成ガイド』を参照してください。

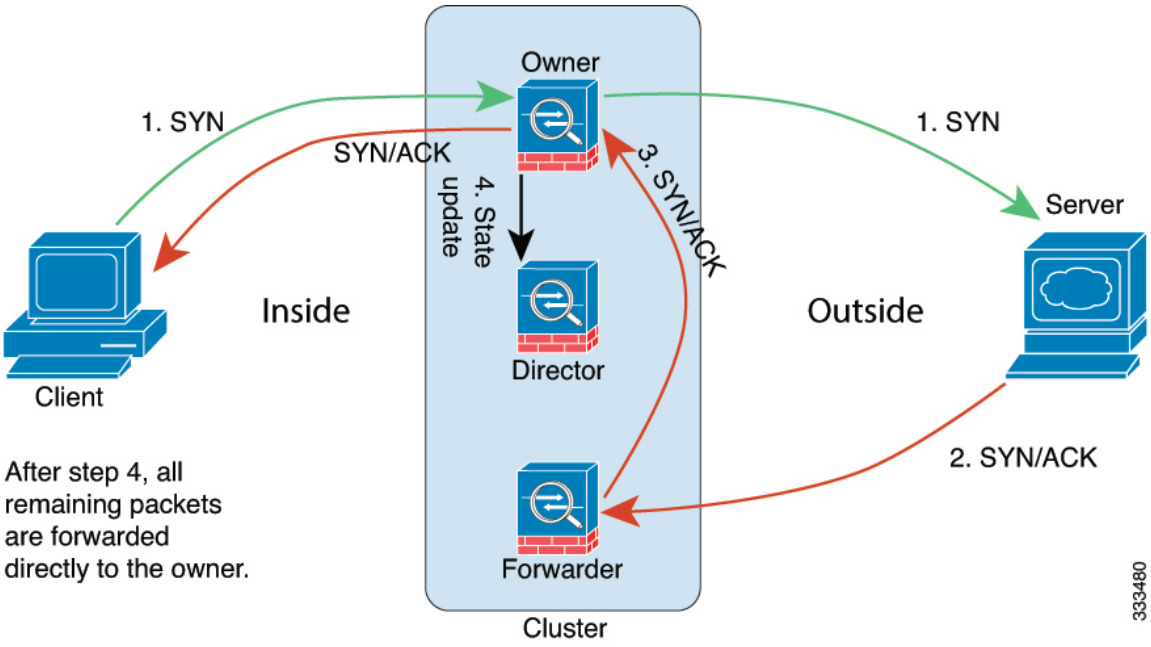
新しい接続の所有権

新しい接続がロードバランシング経由でクラスタのノードに送信される場合は、そのノードがその接続の両方向のオーナーとなります。接続のパケットが別のノードに到着した場合は、そ

のパケットはクラスタ制御リンクを介してオーナーノードに転送されます。最適なパフォーマンスを得るには、適切な外部ロードバランシングが必要です。1つのフローの両方向が同じノードに到着するとともに、フローがノード間に均等に分散されるようにするためです。逆方向のフローが別のノードに到着した場合は、元のノードにリダイレクトされます。

TCP のサンプルデータ フロー

次の例は、新しい接続の確立を示します。



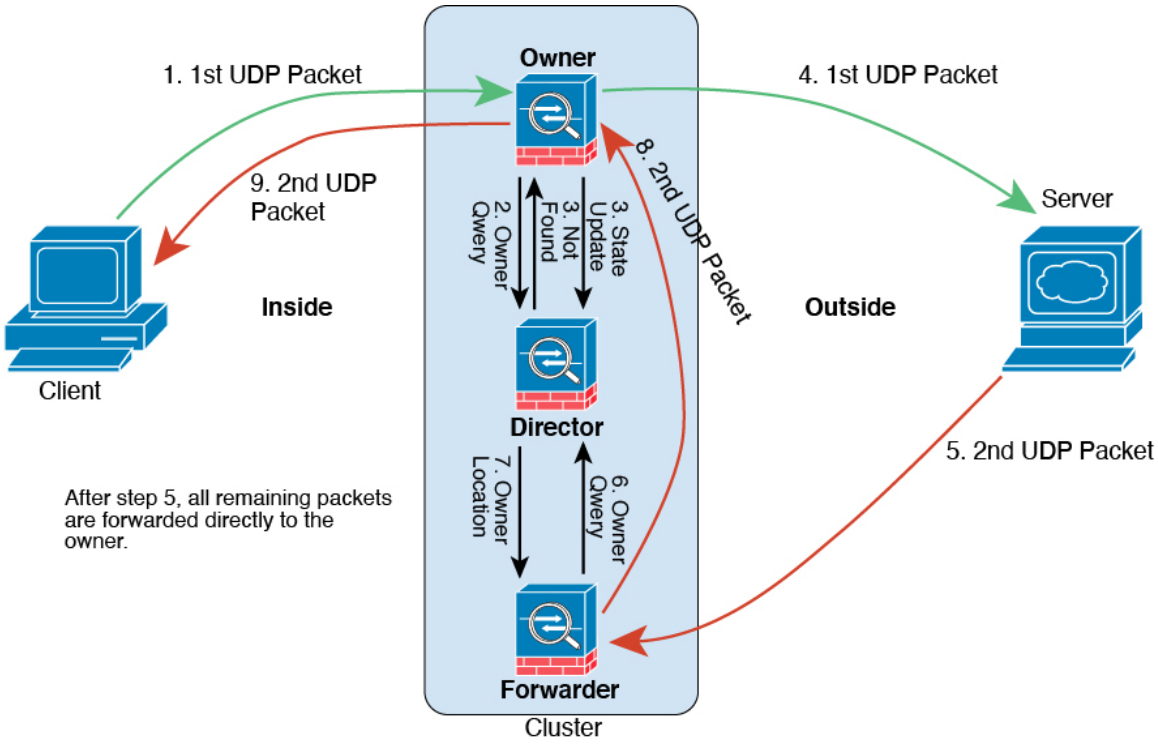
1. SYN パケットがクライアントから発信され、ASA の 1 つ（ロード バランシング方法に基づく）に配信されます。これがオーナーとなります。オーナーはフローを作成し、オーナー情報をエンコードして SYN Cookie を生成し、パケットをサーバに転送します。
2. SYN-ACK パケットがサーバから発信され、別の ASA（ロード バランシング方法に基づく）に配信されます。この ASA はフォワーダです。
3. フォワーダはこの接続を所有してはいないので、オーナー情報を SYN Cookie からデコードし、オーナーへの転送フローを作成し、SYN-ACK をオーナーに転送します。
4. オーナーはディレクタに状態アップデートを送信し、SYN-ACK をクライアントに転送します。
5. ディレクタは状態アップデートをオーナーから受信し、オーナーへのフローを作成し、オーナーと同様に TCP ステート情報を記録します。ディレクタは、この接続のバックアップ オーナーとしての役割を持ちます。
6. これ以降、フォワーダに配信されたパケットはすべて、オーナーに転送されます。
7. パケットがその他のノードに配信された場合、そのノードはディレクタに問い合わせてオーナーを特定し、フローを確立します。

8. フローの状態が変化した場合は、状態アップデートがオーナーからディレクタに送信されます。

ICMP および UDP のサンプルデータフロー

次の例は、新しい接続の確立を示します。

1. 図 *69 : ICMP および UDP データフロー*



UDP パケットがクライアントから発信され、1 つの ASA（ロードバランシング方法に基づく）に配信されます。

2. 最初のパケットを受信したノードは、送信元/宛先 IP アドレスとポートのハッシュに基づいて選択されたディレクタノードをクエリします。

3. ディレクタは既存のフローを検出せず、ディレクタフローを作成して、以前のノードにパケットを転送します。つまり、ディレクタがこのフローのオーナーを選択したことになります。

4. オーナーはフローを作成し、ディレクタに状態アップデートを送信して、サーバにパケットを転送します。

5. 2 番目の UDP パケットはサーバから発信され、フォワーダに配信されます。

6. フォワーダはディレクタに対して所有権情報をクエリします。存続期間が短いフロー（DNS など）の場合、フォワーダはクエリする代わりにパケットを即座にディレクタに送信し、ディレクタがそのパケットをオーナーに送信します。

7. ディレクタは所有権情報をフォワーダに返信します。
8. フォワーダは転送フローを作成してオーナー情報を記録し、パケットをオーナーに転送します。
9. オーナーはパケットをクライアントに転送します。

パブリッククラウドにおける ASA Virtual クラスタリングの履歴

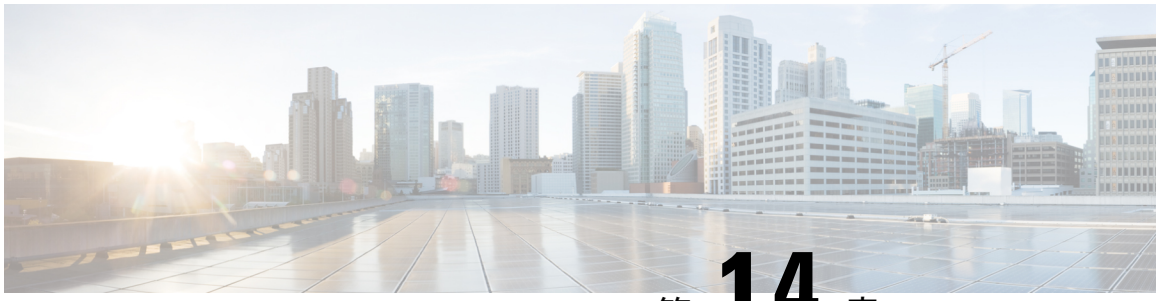
機能	バージョン	詳細
ノード参加時の MTU ping テスト	9.23(1)	クラスタに参加したノードは、クラスタ制御リンク MTU と一致するパケットサイズで制御ノードに ping を送信することで MTU の互換性をチェックします。ping が失敗すると、通知が生成されるため、接続スイッチの MTU 不一致を修正して再試行することができます。
Azure 上の ASA Virtual：ゲートウェイ ロード バランシングによるクラスタリング	9.20(2)	Azure Resource Manager（ARM）テンプレートを使用した Azure での ASA Virtual クラスタリングの展開がサポートされるようになり、ネットワークトラフィックのロードバランシングにゲートウェイロードバランサ（GWLB）を使用するように ASAv クラスタが設定されています。
AWS における GWLB を使用した ASA Virtual クラスタリングのターゲットフェールオーバーの設定	9.20(2)	AWS でターゲットフェールオーバー機能を使用すると、計画メンテナンス中またはターゲットノードの障害時にノードの登録が解除された場合に、GWLB がネットワークパケットを正常なターゲットノードにリダイレクトできるようになります。この機能ではクラスタのステートフル フェールオーバーを利用しています。
フローステータスの設定可能なクラスタキープアライブ間隔	9.20(2)	フローオーナーは、キープアライブ（clu_keepalive メッセージ）と更新（clu_update メッセージ）をディレクタおよびバックアップオーナーに送信して、フローの状態を更新します。キープアライブ間隔を設定できるようになりました。デフォルトは 15 秒で、15 ～ 55 秒の範囲で間隔を設定できます。クラスタ制御リンクのトラフィック量を減らすために長い間隔を設定できます。 新規/変更されたコマンド： **clu-keepalive-interval**
ASA Virtual Amazon Web Services（AWS）クラスタリング	9.19(1)	ASA Virtual は AWS で最大 16 ノードの個別インターフェイスのクラスタリングをサポートします。AWS ゲートウェイロードバランサ の有無にかかわらず、クラスタリングを使用できます。

機能	バージョン	詳細
Amazon Web Services（AWS）クラスタリングでの ASA virtual IMDSv2 サポート	9.22	ASA Virtual は、AWS での IMDSv2 をサポートしています。スタックを更新することで、IMDSv2 必須モードを有効にすることができます。

第 III 部

インターフェイス

- 基本的なインターフェイス設定 （825 ページ）
- Firepower 1010 と Cisco Secure Firewall 1210/1220 スイッチポートの基本インターフェイス設定 （845 ページ）
- EtherChannel インターフェイスインターフェイス （865 ページ）
- ループバック インターフェイス （881 ページ）
- VLAN サブインターフェイス （887 ページ）
- VXLAN インターフェイス （895 ページ）
- ルーテッド モードおよびトランスペアレント モードのインターフェイス （927 ページ）
- 高度なインターフェイス設定 （973 ページ）
- トラフィック ゾーン （985 ページ）



第 14 章

基本的なインターフェイス設定

この章では、イーサネット設定、ジャンボ フレーム設定などの基本的なインターフェイス設定について説明します。

（注） マルチコンテキスト モードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

（注） プラットフォーム モードの Firepower 4100/9300 シャーシ では、FXOS オペレーティング システムで基本的なインターフェイス設定を行います。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

- 基本的なインターフェイス設定について （825 ページ）
- 基本インターフェイスの設定のガイドライン （828 ページ）
- 基本インターフェイスのデフォルト設定 （829 ページ）
- 物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 （830 ページ）
- ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000） （833 ページ）
- Cisco Secure Firewall 3100/4200 のネットワークモジュールの管理 （834 ページ）
- インターフェイスのモニタリング （840 ページ）
- 基本インターフェイスの例 （840 ページ）
- 基本インターフェイスの設定の履歴 （841 ページ）

基本的なインターフェイス設定について

この項では、インターフェイスの機能と特殊なインターフェイスについて説明します。

Auto-MDI/MDIX 機能

RJ-45 インターフェイスでは、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレートケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。ギガビット イーサネットの速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常にイネーブルになり、ディセーブルにできません。

管理インターフェイス

管理インターフェイスは、使用しているモデルに応じて、管理トラフィック専用の個別インターフェイスとなります。

管理インターフェイスの概要

次のインターフェイスに接続して ASA を管理できます。

- 任意の通過トラフィック インターフェイス
- 専用の管理スロット/ポート インターフェイス（使用しているモデルで使用できる場合）

管理アクセス（1495 ページ）の説明に従って、管理アクセスへのインターフェイスを設定する必要がある場合があります。

管理スロット/ポート インターフェイス

次の表に、モデルごとの管理インターフェイスを示します。

表 *24*：モデルごとの管理インターフェイス

モデル	管理 0/0	管理 1/1	管理 1/2	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 1000	—	対応	—	○	○
Cisco Secure Firewall 1200	—	対応	—	○	○
Cisco Secure Firewall 3100	—	対応	—	○	○
Cisco Secure Firewall 4200	—	○	○	○	○

モデル	管理 0/0	管理 1/1	管理 1/2	通過トラフィックに対して設定可能	サブインターフェイスを使用可能
Firepower 4100/9300	N/A インターフェイス ID は ASA 論理デバイスに割り当てた物理 mgmt タイプ インターフェイスに基づいています。	—	—	—	対応
ISA 3000	—	対応	—	—	—
ASAv	対応	—	—	対応	—

管理専用トラフィックに対する任意のインターフェイスの使用

任意のインターフェイスを、管理トラフィック用として設定することによって管理専用インターフェイスとして使用できます。これには、EtherChannel インターフェイスも含まれます（**management-only** コマンドを参照）。

トランスペアレント モードの管理インターフェイス

トランスペアレント ファイアウォール モードでは、許可される最大通過トラフィック インターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）のいずれか）を個別の管理専用インターフェイスとして使用できます。

他のインターフェイスタイプは管理インターフェイスとして使用できません。

Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。

（注） 管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

Management-Only Traffic

管理インターフェイスは to-the-box トラフィックおよび from-the-box トラフィック専用で、トラフィックのパススルーはできません。いずれの場合も、ブリッジグループは他のブリッジグループと通信できないため、トラフィックによるサポートがあった場合でも、管理インターフェイスからブリッジグループに、またはその逆にルーティングすることはできません。

共有 MAC アドレス テーブルおよびスイッチ接続

トランスペアレント ファイアウォール モードでは、管理インターフェイスによってデータ インターフェイスと同じ方法でMACアドレス テーブルがアップデートされます。したがって、いずれかのスイッチ ポートをルーテッド ポートとして設定しない限り、管理インターフェイスおよびデータ インターフェイスを同じスイッチに接続しないでください（デフォルトでは、Catalyst スイッチがすべての VLAN スイッチ ポートの MAC アドレスを共有します）。そうしないと、物理的に接続されたスイッチから管理インターフェイスにトラフィックが到着すると、ASA によって、データ インターフェイスではなく、管理インターフェイスを使用してスイッチにアクセスするようにMACアドレス テーブルがアップデートされます。この処理が原因で、一時的にトラフィックが中断します。セキュリティ上の理由から、少なくとも 30 秒間は、スイッチからデータ インターフェイスへのパケットのために MAC アドレス テーブルが ASA によって再アップデートされることはありません。

マルチ コンテキスト モード

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。サポートされるモデルのコンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。一部のモデルでは管理インターフェイスのサブインターフェイスが許可されないため、それらのモデルでコンテキスト単位の管理を行うには、データ インターフェイスに接続する必要があります。Firepower 4100/9300 シャーシでは、管理インターフェイスとそのサブインターフェイスは、コンテキスト内で特別に許可された管理インターフェイスとして認識されません。この場合、管理サブインターフェイスをデータインターフェイスとして扱い、BVI に追加する必要があります。

基本インターフェイスの設定のガイドライン

トランスペアレント ファイアウォール モード

マルチコンテキストのトランスペアレントモードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。

フェールオーバー

データインターフェイスと、フェールオーバーまたはステートのインターフェイスを共有することはできません。

その他のガイドライン

一部の管理関連のサービスは、管理対象外のインターフェイスが有効になり、ASAが「システム レディ」状態になるまで使用できません。ASA が「System Ready」状態になると、次の syslog メッセージを生成します。

```
%ASA-6-199002: Startup completed.  Beginning operation.
```

基本インターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。
- VXLAN VNI インターフェイス：イネーブル。
- EtherChannel ポートチャネル インターフェイス（ISA 3000）：有効。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。
- EtherChannel ポートチャネル インターフェイス（その他のモデル）：無効。

（注） Firepower 4100/9300 の場合、管理上、シャーシおよび ASA の両方で、インターフェイスを有効および無効にできます。インターフェイスを動作させるには、両方のオペレーティング システムで、インターフェイスを有効にする必要があります。インターフェイスの状態は個別に制御されるので、シャーシと ASA の間の不一致が生じることがあります。

デフォルトの速度および二重通信

- デフォルトでは、銅線（RJ-45）インターフェイスの速度とデュプレックスは、オートネゴシエーションに設定されます。

デフォルトのコネクタ タイプ

2 つのコネクタ タイプ（copper RJ-45 と fiber SFP）を持つモデルもあります。RJ-45 がデフォルトです。ASA にファイバ SFP コネクタを使用するように設定できます。

デフォルトの MAC アドレス

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。

物理インターフェイスのイネーブル化およびイーサネット パラメータの設定

ここでは、次の方法について説明します。

- 物理インターフェイスをイネーブルにする。
- 特定の速度と二重通信（使用できる場合）を設定する。
- （Cisco Secure Firewall 1200/3100/4200）フロー制御のポーズフレームをイネーブルにする。
- （Cisco Secure Firewall 3100/4200）前方誤り訂正を設定する。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 設定するインターフェイスを指定します。

interface *physical_interface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID には、タイプ、スロット、およびポート番号（type[slot/]port）が含まれます。

物理インターフェイスのタイプには、次のものがあります。

- **ethernet**

  gigabitethernet

- **tengigabitethernet**
- **management**

タイプに続けてスロット/ポートを入力します。たとえば、**gigabitethernet0/1** というようになります。タイプとスロット/ポートの間のスペースは任意です。

ステップ 2 （任意） 速度を選択します（モデルによって異なります）。

speed {**auto** | *speed* | **nonegotiate** | **sfp-detect**}

例：

```
ciscoasa(config-if)# speed 100
```

Firepower 1100 光ファイバインターフェイスの場合、**speed nonegotiate** を指定すると速度が 1,000 Mbps に設定され、フロー制御パラメータとリモート障害情報のリンクネゴシエーションがディセーブルになります。Cisco Secure Firewall 1200/3100/4200 については、**negotiate-auto** コマンドを参照してください。

（Cisco Secure Firewall 1200/3100/4200 のみ）**sfp-detect** を選択してインストールされている SFP モジュールの速度を検出し、適切な速度を使用します。デュプレックスは常に全二重で、自動ネゴシエーションは常に有効です。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。Cisco Secure Firewall 1250には、2500 Mbps の最大速度を設定できます。

ステップ 3 （Cisco Secure Firewall 1200/3100/4200）自動ネゴシエーションを設定します。

negotiate-auto

自動ネゴシエーションは、速度とは別に設定されます。

例：

```
ciscoasa(config-if)# negotiate-auto
```

ステップ 4 （任意） RJ-45 インターフェイスのデュプレックスを設定します。

duplex {**auto** | **full** | **half**}

SFP インターフェイスは全二重のみをサポートします。

例：

```
ciscoasa(config-if)# duplex full
```

ステップ 5 （任意）（Cisco Secure Firewall 3100/4200）25 Gbps 以上のインターフェイスの場合は、前方誤り訂正（FEC）を設定します。

fec {**auto** | **cl108-rs** | **cl74-fc** | **cl91-rs** | **disable**}

EtherChannel メンバーインターフェイスの場合は、EtherChannel に追加する前に FEC を設定する必要があります。**自動**を使用する場合に選択する設定は、トランシーバのタイプと、インターフェイスが固定（内蔵）かネットワークモジュールかによって異なります。

（注）
インターフェイスが EtherChannel から削除された場合、ASA の再起動後に、FEC および自動ネゴシエーションの設定が変更されます。これは予期される動作であるため、FECおよび自動ネゴシエーションを手動で再設定する必要があります。

表 *25 :* 自動設定のデフォルト *FEC*

トランシーバ タイプ	固定ポートのデフォルト **FEC**（イーサネット **1/9** ～ **1/16**）	ネットワークモジュールのデフォルト **FEC**
25G-SR	cl108-rs	cl108-rs
25G-LR	cl108-rs	cl108-rs
10/25G-CSR	cl108-rs	cl74-fc
25G-AOC*x*M	cl74-fc	cl74-fc
25G-CU2.5/3M	自動ネゴシエーション	自動ネゴシエーション
25G-CU4/5M	自動ネゴシエーション	自動ネゴシエーション
25/50/100G	cl91-rs	cl91-rs

ステップ 6 （任意）（Cisco Secure Firewall 1200/3100/4200）1 ギガビット以上のインターフェイスでフロー制御のポーズ（XOFF）フレームをイネーブルにします。

flowcontrol send on

例：

```
ciscoasa(config-if)# flowcontrol send on
```

フロー制御により、接続しているイーサネットポートは、輻輳しているノードがリンク動作をもう一方の端で一時停止できるようにすることによって、輻輳時のトラフィック レートを制御できます。ASA ポートで輻輳が生じ（内部スイッチでキューイングリソースが枯渇）、それ以上はトラフィックを受信できなくなった場合、ポーズフレームを送信することによって、その状態が解消されるまで送信を中止するように、そのポートから相手ポートに通知します。ポーズ フレームを受信すると、送信側デバイスはデータ パケットの送信を中止するので、輻輳時のデータ パケット損失が防止されます。

（注）
ASA は、リモートピアがトラフィックをレート制御できるように、ポーズ フレームの送信をサポートしています。

ただし、ポーズフレームの受信はサポートされていません。

内部スイッチには、それぞれ 250 バイトの 8000 バッファのグローバルプールがあり、スイッチはバッファを各ポートに動的に割り当てます。バッファ使用量がグローバル ハイ ウォーターマーク（2 MB（8000 バッファ））を超えると、フロー制御が有効になっているすべてのインターフェイスからポーズフレームが送信されます。また、バッファがポートのハイ ウォーター

マーク（.3125 MB（1250 バッファ））を超えると、特定のインターフェイスからポーズフレームが送信されます。ポーズの送信後、バッファ使用量が低ウォーターマークよりも下回ると、XON フレームを送信できます（グローバルでは 1.25MB（5000 バッファ）、ポートごとに 25 MB（1000 バッファ））リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。

802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティベースのフロー制御はサポートされていません。

ステップ 7 インターフェイスをイネーブルにします。

no shutdown

例：

```
ciscoasa(config-if)# no shutdown
```

インターフェイスをディセーブルにするには、**shutdown** コマンドを入力します。**shutdown** コマンドを入力すると、すべてのサブインターフェイスもシャットダウンします。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでシャットダウンします。

ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000）

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび VLAN ヘッダーを含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネットフレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボ フレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。ASA MTU はレイヤ 2（14 バイト）および VLAN ヘッダー（4 バイト）を含まずにペイロードサイズを設定するので、モデルによっては MTU 最大値が 9198 になることに注意してください。

この手順は、ISA 3000、および ASA 仮想 にのみ適用できます。その他のモデルは、デフォルトでジャンボフレームをサポートしています。

ジャンボフレームは、8GB RAM 未満の ASAv5 および ASAv10 ではサポートされません。

始める前に

- マルチ コンテキスト モードでは、システム実行スペースでこのオプションを設定します。
- この設定を変更した場合は、ASA のリロードが必要です。

- ジャンボフレームを送信する必要のある各インターフェイスの MTU を、デフォルト値の 1500 より大きい値に設定してください。たとえば、**mtu** コマンドを使用して値を 9198 に設定します。マルチ コンテキスト モードでは、各コンテキスト内で MTU を設定します。
- Be sure to adjust the TCP MSS, either to disable it for non-IPsec traffic (use the **sysopt connection tcpmss 0** command), or to increase it in accord with the MTU.

手順

ジャンボ フレーム サポートをイネーブルにします。

jumbo-frame reservation

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5

70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

Cisco Secure Firewall 3100/4200 のネットワークモジュールの管理

最初にファイアウォールの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。

初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、次の手順を参照してください。

ブレークアウトポートの設定

40GB 以上のインターフェイスごとに 10GB のブレークアウトポートを設定できます。この手順では、ポートの分割と再参加の方法について説明します。ブレークアウトポートは、EtherChannel への追加を含め、他の物理イーサネットポートと同じように使用できます。

設定でインターフェイスがすでに使用されている場合は、存在しなくなるインターフェイスに関連する設定を手動で削除する必要があります。

始める前に

- サポートされているブレークアウトケーブルを使用する必要があります。詳細については、ハードウェア設置ガイドを参照してください。
- クラスタリングまたはフェールオーバーの場合、クラスタ/フェールオーバーリンクで（分割用の）親インターフェイスか（再結合用の）子インターフェイスが使用されていないことを確認してください。クラスタ/フェールオーバーリンクに使用されている場合、インターフェイスを変更することはできません。

手順

ステップ 1 40GB 以上のインターフェイスから 10GB ポートを分割します。

breakout *slot port*

たとえば、Ethernet2/1 40GB インターフェイスを分割するには、スロットに **2**、ポートに **1** を指定します。分割後の子インターフェイスは、Ethernet2/1/1、Ethernet2/1/2、Ethernet2/1/3、および Ethernet2/1/4 として識別されます。

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。インターフェイスの変更は他のノードに複製されます。

例：

```
ciscoasa(config)# breakout 2 1
ciscoasa(config)# breakout 2 2
ciscoasa(config)# breakout 2 3
ciscoasa(config)# breakout 2 4
```

ステップ 2 インターフェイスを復元するには、ブレークアウトポートを再結合します。

no breakout *slot port*

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

インターフェイスのすべての子ポートを再結合する必要があります。

例：

```
ciscoasa(config)# no breakout 2 1
```

ネットワークモジュールの追加

初回起動後にファイアウォールにネットワークモジュールを追加するには、次の手順を実行します。新しいモジュールを追加するには、リロードが必要です。クラスタリングまたはフェールオーバーの場合、ゼロダウンタイムはサポートされないため、この手順は必ずメンテナンスウィンドウ中に実行してください。

手順

ステップ 1 ハードウェア設置ガイドに従ってネットワークモジュールをインストールします。ファイアウォールの電源がオンの状態でネットワークモジュールをインストールできます。

クラスタリングまたはフェールオーバーの場合は、すべてのノードにネットワークモジュールをインストールします。

ステップ 2 ファイアウォールをリロードします。ASA のリロード （46 ページ）[ツール（Tools）] > [システムのリロード（System Reload）] を参照してください。

クラスタリングまたはフェールオーバーの場合は、すべてのノードをリロードします。ネットワークモジュールが異なるノードはクラスタ/フェールオーバーペアに参加できないため、クラスタ/フェールオーバーペアを再作成する前に、新しいモジュールですべてのノードをリロードする必要があります。

ステップ 3 ネットワークモジュールを有効化します。

no netmod 2 disable

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

例：

```
ciscoasa(config)# no netmod 2 disable
```

ネットワークモジュールの交換方法

リロードすることなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。この手順では、古いモジュールをシャットダウンし、新しいモジュールをインストールして有効にする方法について説明します。

クラスタリングまたはフェールオーバーの場合、クラスタ制御リンク/フェールオーバーリンクがモジュール上にあると、ネットワークモジュールを無効化できません。

手順

ステップ 1 クラスタリングまたはフェールオーバーの場合は、次の手順を実行します。

- **クラスタリング**：ホットスワップを実行するユニットがデータノードであることを確認します（「制御ノードの変更（472 ページ）」を参照）。次に、そのノードでクラスタリングを無効化します。非アクティブノードになる（468 ページ）またはノードの非アクティブ化（469 ページ）を参照してください。

  クラスタ制御リンクがネットワークモジュール上にある場合は、クラスタから脱退する必要があります。クラスタからの脱退（471 ページ）を参照してください。アクティブなクラスタ制御リンクがあるネットワークモジュールを無効化することはできません。

- **フェールオーバー**：ホットスワップを実行するユニットがスタンバイノードであることを確認します。フェールオーバーの強制実行（369 ページ）を参照してください。

  フェールオーバーリンクがネットワークモジュール上にある場合は、フェールオーバーを無効化する必要があります。フェールオーバーのディセーブル化（370 ページ）を参照してください。アクティブなフェールオーバーリンクがあるネットワークモジュールを無効化することはできません。

ステップ 2 ネットワークモジュールを無効化します。

netmod 2 disable

例：

```
ciscoasa(config)# netmod 2 disable
```

ステップ 3 ハードウェア設置ガイドに従ってネットワークモジュールを交換します。ファイアウォールの電源がオンの状態でネットワークモジュールを交換できます。

ステップ 4 ネットワークモジュールを有効化します。

no netmod 2 disable

例：

```
ciscoasa(config)# no netmod 2 disable
```

ステップ 5 クラスタリングまたはフェールオーバーの場合は、次の手順を実行します。

- **クラスタリング**：ノードをクラスタに追加して戻します。クラスタへの再参加（470 ページ）を参照してください。

- **フェールオーバー**：フェールオーバーを無効化した場合は、もう一度フェールオーバーを実行します。

ネットワークモジュールを別のタイプに交換する

ネットワークモジュールを別のタイプに交換する場合は、リロードが必要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。クラスタリングまたはフェールオーバーの場合、ゼロダウンタイムはサポートされないため、この手順は必ずメンテナンスウィンドウ中に実行してください。

手順

ステップ 1 ネットワークモジュールを無効化します。

netmod 2 disable

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。設定を保存しないでください。リロードすると、保存された設定でモジュールが有効になります。

例：

```
ciscoasa(config)# netmod 2 disable
```

ステップ 2 ハードウェア設置ガイドに従ってネットワークモジュールを交換します。ファイアウォールの電源がオンの状態でネットワークモジュールを交換できます。

クラスタリングまたはフェールオーバーの場合は、すべてのノードにネットワークモジュールをインストールします。

ステップ 3 ファイアウォールをリロードします。ASA のリロード （46 ページ）[ツール（Tools）] > [システムのリロード（System Reload）] を参照してください。

クラスタリングまたはフェールオーバーの場合は、すべてのノードをリロードします。ネットワークモジュールが異なるノードはクラスタ/フェールオーバーペアに参加できないため、クラスタ/フェールオーバーペアを再作成する前に、新しいモジュールですべてのノードをリロードする必要があります。

ステップ 4 再ロードの前に設定を保存した場合は、モジュールを再有効化する必要があります。

ネットワーク モジュールの取り外し

ネットワークモジュールを完全に削除する場合は、次の手順に従います。ネットワークモジュールを削除するには、リロードが必要です。クラスタリングまたはフェールオーバーの場合、ゼロダウンタイムはサポートされないため、この手順は必ずメンテナンスウィンドウ中に実行してください。

始める前に

クラスタリングまたはフェールオーバーの場合、クラスタ/フェールオーバーリンクがネットワークモジュール上にないことを確認してください。この場合、モジュールを削除することはできません。

手順

ステップ 1 ネットワークモジュールを無効にして設定を保存します。

netmod 2 disable

write memory

クラスタリングまたはフェールオーバーの場合は、制御ノード/アクティブユニットでこの手順を実行します。モジュールの状態は他のノードに複製されます。

例：

```
ciscoasa(config)# netmod 2 disable
ciscoasa(config)# write memory
```

ステップ 2 ハードウェア設置ガイドに従ってネットワークモジュールを削除します。ファイアウォールの電源がオンの状態でネットワークモジュールを削除できます。

クラスタリングまたはフェールオーバーの場合は、すべてのノードのネットワークモジュールを削除します。

ステップ 3 ファイアウォールをリロードします。ASA のリロード （46 ページ）[ツール（Tools）] > [システムのリロード（System Reload）] を参照してください。

クラスタリングまたはフェールオーバーの場合は、すべてのノードをリロードします。ネットワークモジュールが異なるノードはクラスタ/フェールオーバーペアに参加できないため、クラスタ/フェールオーバーペアを再作成する前に、モジュールのないすべてのノードをリロードする必要があります。

インターフェイスのモニタリング

次のコマンドを参照してください。

（注） Firepower 、および Secure Firewall モデルの場合、一部の統計は ASA コマンドで表示されません。FXOS コマンドを使用して、より詳細なインターフェイス統計情報を表示する必要があります。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

詳細については、『FXOS troubleshooting guide』を参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- （Secure Firewall 1200）**show interface egress shaper**

  出力シェーパーの統計情報を表示します。

基本インターフェイスの例

次の設定例を参照してください。

物理インターフェイス パラメータの例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
```

マルチ コンテキスト モードの例

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
interface gigabitethernet 0/1
speed 1000
duplex full
no shutdown
interface gigabitethernet 0/1.1
vlan 101
context contextA
allocate-interface gigabitethernet 0/1.1
```

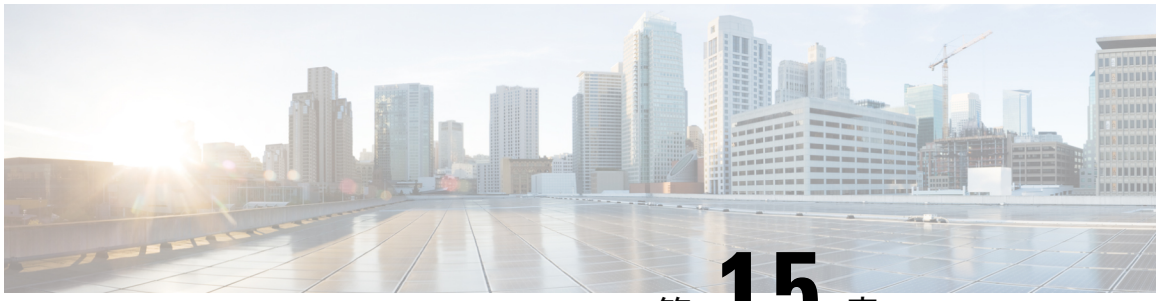
基本インターフェイスの設定の履歴

表 *26 :* インターフェイスの履歴

機能名	リリース	機能情報
Cisco Secure Firewall 1200 シリーズのサポート	9.22(1)	フロー制御、FEC、SFP の検出、自動ネゴシエーションなどの機能がサポートされています。
Secure Firewall 3100 固定ポートのデフォルトの前方誤り訂正（FEC）が、25 GB+ SR、CSR、および LR トランシーバの cl74-fc から cl108-rs に変更されました	9.18(3)/9.19(1)	Secure Firewall 3100 の固定ポートで FEC を Auto に設定すると、25 GB SR、CSR、および LR トランシーバのデフォルトのタイプが cl74-fc ではなく cl108-rs に設定されるようになりました。 新規/変更されたコマンド： **fec**
Cisco Secure Firewall 3100 のフロー制御に対応するためのフレームの一時停止	9.18(1)	トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。 新規/変更されたコマンド： **flowcontrol send on**
Secure Firewall 3130 および 3140 のブレークアウトポート	9.18(1)	Cisco Secure Firewall 3130 および 3140 の 40 GB インターフェースごとに 4 つの 10 GB ブレークアウトポートを構成できるようになりました。 新規/変更されたコマンド： **breakout**

機能名	リリース	機能情報
Cisco Secure Firewall 3100 におけるネットワークモジュールのホットスワップのサポート	9.17(1)	Cisco Secure Firewall 3100 では、ファイアウォールの電源がオンの状態でネットワークモジュールを追加または削除できます。モジュールを同じタイプの別のモジュールに交換する場合、再起動は必要ありません。最初の起動の後にモジュールを追加するか、モジュールを完全に削除するか、モジュールを新しいタイプのモジュールに交換する場合は、再起動が必要です。 新規/変更されたコマンド： **netmod**
Cisco Secure Firewall 3100 における前方誤り訂正のサポート	9.17(1)	Cisco Secure Firewall 3100 25 Gbps インターフェイスは、前方誤り訂正（FEC）をサポートします。FECはデフォルトで有効になっており、[自動（Auto）] に設定されています。 新規/変更されたコマンド： **fec**
Cisco Secure Firewall 3100 における SFP に基づく速度設定のサポート	9.17(1)	Cisco Secure Firewall 3100 は、インストールされている SFP に基づくインターフェイスの速度検出をサポートします。SFPの検出はデフォルトで有効になっています。このオプションは、後でネットワークモジュールを別のモデルに変更し、速度を自動的に更新する場合に便利です。 新規/変更されたコマンド： **speed sfp-detect**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	9.17(1)	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスについて、速度とは別に有効または無効にすることができます。 新規/変更されたコマンド：**negotiate-auto**
Firepower 1100 および 2100 の光ファイバインターフェイスでの速度の自動ネゴシエーションの無効化	9.14(1)	自動ネゴシエーションを無効にするように Firepower 1100 または 2100 光ファイバインターフェイスを設定できるようになりました。10GB インターフェイスの場合、自動ネゴシエーションなしで速度を 1GB に設定できます。速度が 10 GB に設定されているインターフェイスの自動ネゴシエーションは無効にできません。 新規/変更されたコマンド： **speed nonegotiate**
ASA 仮想 の管理 0/0 インターフェイスでの通過トラフィックサポート	9.6(2)	ASA 仮想 の管理 0/0 インターフェイスでトラフィックを通過させることができるようになりました。以前は、Microsoft Azure 上の ASA 仮想 のみで通過トラフィックをサポートしていました。今後は、すべての ASA 仮想 で通過トラフィックがサポートされます。任意で、このインターフェイスを管理専用に設定できますが、デフォルトでは管理専用に設定されていません。 次のコマンドが変更されました。 **management-only**

機能名	リリース	機能情報
ギガビットイーサネットインターフェイスでのフロー制御のポーズフレームのサポート	8.2(5)/8.4(2)	すべてのASAモデルでギガビットイーサネットインターフェイスのフロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 **flowcontrol** コマンドが変更されました。
ASA 5580 10 ギガビット イーサネット インターフェイスでのフロー制御のポーズ フレームのサポート	8.2(2)	フロー制御のポーズ（XOFF）フレームをイネーブルにできるようになりました。 この機能は、ASA 5585-X でもサポートされます。 **flowcontrol** コマンドが導入されました。
ASA 5580 に対するジャンボ パケット サポート	8.1(1)	ASA 5580 はジャンボフレームをサポートします。ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび FCS を含む）より大きく、9216 バイトまでのイーサネット パケットのことです。イーサネット フレームを処理するためのメモリ容量を増やすことにより、すべてのインターフェイスに対してジャンボフレームのサポートをイネーブルにできます。ジャンボ フレームに割り当てるメモリを増やすと、他の機能（ACL など）の最大使用量が制限される場合があります。 この機能は、ASA 5585-X でもサポートされます。 **jumbo-frame reservation** コマンドが導入されました。
ASA 5510 Security Plus ライセンスに対するギガビット イーサネット サポート	7.2(3)	ASA 5510 は、GE（ギガビット イーサネット）を Security Plus ライセンスのあるポート 0 および 1 でサポートするようになりました。ライセンスを Base から Security Plus にアップグレードした場合、外部 Ethernet 0/0 および Ethernet 0/1 ポートの容量は、元の FE（ファスト イーサネット）の 100 Mbps から GE の 1000 Mbps に増加します。インターフェイス名は Ethernet 0/0 および Ethernet 0/1 のままです。**speed** コマンドを使用してインターフェイスの速度を変更します。また、**show interface** コマンドを使用して各インターフェイスの現在の設定速度を確認します。
ASA 5510 上の基本ライセンスに対する増加したインターフェイス	7.2(2)	ASA 5510 上の基本ライセンスについて、最大インターフェイス数が 3 プラス管理インターフェイスから無制限のインターフェイスに増加しました。



第 15 章

Firepower 1010 と Cisco Secure Firewall 1210/1220 スイッチポートの基本インターフェイス設定

Firepower 1010 または Cisco Secure Firewall 1210/1220 の各インターフェイスは、通常のファイアウォールインターフェイスとしてまたはレイヤ2ハードウェアスイッチポートとして実行するように設定できます。この章では、スイッチモードの有効化と無効化、VLANインターフェイスの作成、そのインターフェイスのスイッチポートへの割り当てなど、スイッチポート設定を開始するためのタスクについて説明します。また、サポート対象のインターフェイスでPower on Ethernet（PoE）をカスタマイズする方法についても説明します。

- スイッチ ポートについて （845 ページ）
- スイッチポートの注意事項および制約事項 （847 ページ）
- スイッチ ポートと Power Over Ethernet の設定 （849 ページ）
- スイッチポートのモニタリング （858 ページ）
- スイッチポートの例 （860 ページ）
- スイッチポートの履歴 （864 ページ）

スイッチ ポートについて

この項では、Firepower 1010/1210/1220 のスイッチ ポートについて説明します。

スイッチポートおよびインターフェイスについて

ポートとインターフェイス

1010/1210/1220 の物理インターフェイスごとに、その動作をファイアウォールインターフェイスまたはスイッチポートとして設定できます。物理インターフェイスとポートタイプ、およびスイッチポートを割り当てる論理 VLAN インターフェイスについては、次の情報を参照してください。

- 物理ファイアウォールインターフェイス：ルーテッドモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールと VPN サービスを適用することによって、レイヤ3のネットワーク間でトラフィックを転送します。トランスペアレントモードでは、これらのインターフェイスは、設定済みのセキュリティポリシーを使用してファイアウォールサービスを適用することによって、レイヤ2の同じネットワーク上のインターフェイス間でトラフィックを転送するブリッジグループメンバーです。ルーテッドモードでは、一部のインターフェイスでブリッジグループメンバーとして、その他のインターフェイスでレイヤ3インターフェイスとして、統合ルーティングおよびブリッジングを使用することもできます。デフォルトでは、イーサネット1/1インターフェイスはファイアウォールインターフェイスとして設定されます。
- 物理スイッチポート：スイッチポートは、ハードウェアのスイッチ機能を使用して、レイヤ 2 でトラフィックを転送します。同じ VLAN 上のスイッチポートは、ハードウェアスイッチングを使用して相互に通信できます。トラフィックには、ASA セキュリティポリシーは適用されません。アクセスポートはタグなしトラフィックのみを受け入れ、それらを単一のVLANに割り当てることができます。トランクポートはタグなしおよびタグ付きトラフィックを受け入れ、複数のVLANに属することができます。デフォルトでは、イーサネット 1/2 ～ 1/8 （1010 および 1210）または 1/2 ー 1/10（1220）は VLAN 1 のアクセススイッチポートとして設定されています。管理インターフェイスをスイッチポートとして設定することはできません。
- 論理 VLAN インターフェイス：これらのインターフェイスは物理ファイアウォール インターフェイスと同じように動作しますが、サブインターフェイス、またはEtherChannelインターフェイスを作成できないという例外があります。スイッチポートが別のネットワークと通信する必要がある場合、ASA デバイスは VLAN インターフェイスにセキュリティポリシーを適用し、別の論理 VLAN インターフェイスまたはファイアウォール インターフェイスにルーティングします。ブリッジグループメンバーとして VLAN インターフェイスで統合ルーティングおよびブリッジングを使用することもできます。同じ VLAN 上のスイッチポート間のトラフィックに ASA セキュリティポリシーは適用されませんが、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、ブリッジグループとスイッチポートを階層化して特定のセグメント間にセキュリティポリシーを適用できます。

Power Over Ethernet

PoE は 次のように使用できます：

- Firepower 1010：イーサネット 1/7 および 1/8 で、IEEE 802.3af（PoE）および 802.3at（PoE+）を使用して、ポートあたり最大 30 ワット、合計で最大 60 ワット供給。
- Cisco Secure Firewall 1210CP：イーサネット 1/5、1/6、1/7、および 1/8 で、IEEE 802.3af（PoE）、802.3at（PoE+）、および 802.3bt（PoE++ および Hi-PoE） を使用して、ポートあたり最大 90 ワット、 合計で最大 120 W 供給。

PoE + およびそれ以降の規格では、リンク層検出プロトコル（Link Layer Discovery Protocol、LLDP）を使用して、電力レベルをネゴシエートします。電力は必要な場合にのみ提供されます。

インターフェイスをシャットダウンすると、デバイスへの電源がディセーブルになります。

Auto-MDI/MDIX 機能

すべてのスイッチポートで、デフォルトの自動ネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルを検出すると、内部クロスオーバーを実行することでクロス ケーブルによる接続を不要にします。インターフェイスの Auto-MDI/MDIX をイネーブルにするには、速度とデュプレックスのいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックスの両方に明示的に固定値を指定すると、両方の設定でオートネゴシエーションがディセーブルにされ、Auto-MDI/MDIX もディセーブルになります。速度と二重通信をそれぞれ 1000 と全二重に設定すると、インターフェイスでは常にオートネゴシエーションが実行されるため、Auto-MDI/MDIX は常に有効になり、無効にできません。

スイッチポートの注意事項および制約事項

コンテキスト モード

- Firepower 1010 はマルチ コンテキスト モードをサポートしません。
- Secure Firewall 1210/1220 でスイッチ ポートを使用しない場合、マルチ コンテキスト モードのみがサポートされます。

フェールオーバー とクラスタリング

- クラスタはサポートされません。
- アクティブ/スタンバイのフェールオーバーのみサポートされます。
- フェールオーバー を使用する場合は、スイッチポート機能を使用しないでください。スイッチポートはハードウェアで動作するため、アクティブユニットとスタンバイユニットの両方でトラフィックを通過させ続けます。フェールオーバーは、トラフィックがスタンバイユニットを通過するのを防ぐように設計されていますが、この機能はスイッチポートには拡張されていません。通常の フェールオーバー のネットワーク設定では、両方のユニットのアクティブなスイッチ ポートがネットワーク ループにつながります。スイッチング機能には外部スイッチを使用することをお勧めします。VLAN インターフェイスはフェールオーバーによってモニタできますが、スイッチポートはモニタできません。理論的には、1 つのスイッチ ポートを VLAN に配置して、フェールオーバー を正常に使用することができますが、代わりに物理ファイアウォールインターフェイスを使用する設定の方が簡単です。
- ファイアウォールインターフェイスはフェールオーバー リンクとしてのみ使用できます。

論理 VLAN インターフェイス（SVI）

- 最大 60 個の VLAN インターフェイスを作成できます。
- また、ファイアウォール インターフェイスで VLAN サブインターフェイスを使用する場合、論理 VLAN インターフェイスと同じ VLAN ID は使用できません。
- MAC アドレス：
  - ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが 1 つの MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。MAC アドレスの手動設定 （978 ページ） を参照してください。
  - トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。MAC アドレスの手動設定 （978 ページ）を参照してください。

ブリッジ グループ

同じブリッジ グループ内に論理 VLAN インターフェイスと物理ファイアウォール インターフェイスを混在させることはできません。

VLAN インターフェイスおよびスイッチ ポートでサポートされていない機能

VLAN インターフェイスおよびスイッチポートは、次の機能をサポートしていません。

- ダイナミック ルーティング
- マルチキャスト ルーティング
- ポリシーベース ルーティング
- 等コストマルチパス（ECMP）ルーティング
- VXLAN
- EtherChannel：スイッチのポートを EtherChannel の一部にはできません。PoE も、EtherChannel のポートではサポートされません。
- フェールオーバーおよびステートリンク
- トラフィック ゾーン
- セキュリティグループタグ（SGT）

その他の注意事項と制約事項

- Firepower 1010 および Cisco Secure Firewall 1210/1220 には、最大 60 個の名前付きインターフェイスを設定できます。

- 管理 インターフェイスをスイッチポートとして設定することはできません。

デフォルト設定

- イーサネット 1/1 はファイアウォール インターフェイスです。
- 1010/1210 では、イーサネット 1/2 ～ 1/8 が、VLAN 1 に割り当てられたスイッチ ポートです。
- 1220 では、イーサネット 1/2 ～ 1/10 が、VLAN 1 に割り当てられたスイッチ ポートです。
- デフォルトの速度とデュプレックス：デフォルトでは、速度とデュプレックスは自動ネゴシエーションに設定されます。

スイッチ ポートと Power Over Ethernet の設定

スイッチ ポートおよび PoE を設定するには、次のタスクを実行します。

スイッチ ポート モードの有効化または無効化

各インターフェイスは、ファイアウォール インターフェイスまたはスイッチ ポートのいずれかになるように個別に設定できます。デフォルトでは、イーサネット 1/1 はファイアウォール インターフェイスで、残りのイーサネット インターフェイスはスイッチ ポートとして設定されます。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface ethernet1/*port*

- *port*：ポート （1 ～ 8）を設定します。

管理 1/1 インターフェイスをスイッチポートモードに設定することはできません。

例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

ステップ 2 スイッチポートモードを有効にします。

switchport

このインターフェイスがすでにスイッチポートモードの場合、モードを変更する代わりにスイッチポートパラメータを入力するように求められます。

```
ciscoasa(config-if)# switchport
ciscoasa(config-if)# switchport ?
interface mode commands/options:
  access         Set access mode characteristics of the interface
  mode           Set trunking mode of the interface
  monitor        Monitor another interface
  protected      Configure an interface to be a protected port
  trunk          Set trunking characteristics of the interface
<cr>
ciscoasa(config-if)#
```

ステップ 3 スイッチポートモードを無効にします。

no switchport

```
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# switchport ?

interface mode commands/options:
<cr>
```

例

次に、イーサネット 1/3 および 1/4 をファイアウォールモードに設定する例を示します。

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)# interface ethernet1/3
ciscoasa(config-if)# no switchport
ciscoasa(config-if)#
```

VLAN インターフェイスの設定

ここでは、関連付けられたスイッチポートで使用するための VLAN インターフェイス（SVI）の設定方法について説明します。スイッチ ポートを関連付けられた最大 60 個の VLAN インターフェイスを作成できます。

手順

ステップ 1 VLAN インターフェイスを追加します。

interface vlan *id*

- *id*：このインターフェイスの VLAN ID を 1 ～ 4070 の範囲で設定します。ただし、内部使用のために予約されている 3968 ～ 4047 の範囲の ID は除きます。

例：

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)#
```

ステップ 2 （任意） 別の VLAN への転送を無効にします。

no forward interface *vlan_id*

- *vlan_id*：この VLAN インターフェイスでトラフィックの開始を禁止する先の VLAN ID を指定します。

たとえば、1 つの VLAN をインターネット アクセスの外部に、もう 1 つを内部ビジネス ネットワーク内に、そして 3 つ目をホーム ネットワークにそれぞれ割り当てます。ホームネットワークはビジネスネットワークにアクセスする必要がないので、ホーム VLAN で **no forward interface** コマンドを使用できます。ビジネスネットワークはホームネットワークにアクセスできますが、その反対はできません。

例：

```
ciscoasa(config-if)# no forward interface 200
ciscoasa(config-if)#
```

スイッチ ポートのアクセス ポートとしての設定

1 つの VLAN にスイッチ ポートを割り当てるには、アクセス ポートとして設定します。アクセス ポートは、タグなしのトラフィックのみを受け入れます。Firepower 1010 および Cisco Secure Firewall 1210 では、イーサネット 1/2 ～ 1/8 スイッチ ポートが、デフォルトで VLAN 1 に割り当てられています。Cisco Secure Firewall 1220 では、イーサネット 1/2 ～ 1/10 スイッチ ポートが、デフォルトで VLAN 1 に割り当てられています。

（注） デバイスは、ネットワーク内のループ検出に使用されるスパニングツリープロトコルをサポートしていません。したがって、ASA との接続はいずれもネットワークループ内で終わらないようにする必要があります。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface ethernet1/*port*

- *port*：ポート （1 ～ 8）を設定します。

例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

ステップ 2 このスイッチポートを VLAN に割り当てます。

switchport access vlan *number*

- *number*：VLAN ID を 1 ～ 4070 の間で設定します。デフォルトは VLAN 1 です。

例：

```
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)#
```

ステップ 3 （任意）このスイッチポートを保護対象として設定します。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

switchport protected

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに **switchport protected** コマンドを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

例：

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

ステップ 4 （任意） 速度を設定します。

speed {**auto** | **10** | **100** | **1000**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

ステップ 5 （任意） 二重通信を設定します。

duplex {**auto** | **full** | **half**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

ステップ 6 スイッチポートをイネーブルにします。

no shutdown

スイッチポートをディセーブルにするには、**shutdown** コマンドを入力します。

例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

例

次の例では、イーサネット 1/3、イーサネット 1/4、およびイーサネット 1/5 を VLAN 101 に割り当て、イーサネット 1/3 とイーサネット 1/4 を保護対象として設定します。

```
ciscoasa(config)# interface ethernet1/3
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/4
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet1/5
ciscoasa(config-if)# switchport access vlan 101
ciscoasa(config-if)# no shutdown
```

スイッチ ポートのトランク ポートとしての設定

この手順では、802.1Q タグ付けを使用して複数の VLAN を伝送するトランク ポートの作成方法について説明します。トランクポートは、タグなしトラフィックとタグ付きトラフィックを受け入れます。許可された VLAN のトラフィックは、トランクポートを変更せずに通過します。

トランクは、タグなしトラフィックを受信すると、そのトラフィックをネイティブ VLAN ID にタグ付けして、ASA が正しいスイッチポートにトラフィックを転送したり、別のファイアウォールインターフェイスにルーティングしたりできるようにします。ASA は、トランクポートからネイティブ VLAN ID トラフィックを送信する際に VLAN タグを削除します。タグなしトラフィックが同じ VLAN にタグ付けされるように、他のスイッチのトランク ポートに同じネイティブ VLAN を設定してください。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface ethernet1/*port*

- *port*：ポート （1 ～ 8）を設定します。

例：

```
ciscoasa(config)# interface ethernet1/4
ciscoasa(config-if)#
```

ステップ 2 このスイッチポートをトランクポートにします。

switchport mode trunk

このポートをアクセスモードに復元するには、**switchport mode access** コマンドを入力します。

例：

```
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)#
```

ステップ 3 このトランクに VLAN を割り当てます。

switchport trunk allowed vlan *vlan_range*

- *vlan_range*：VLAN ID を 1 ～ 4070 の間で設定します。次のいずれかの方法で最大 20 個の ID を指定できます。
  - 単一の番号（n）
  - 範囲（n-x）
  - 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。

    5,7-10,13,45-100

  カンマの代わりにスペースを入力できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。

  このコマンドにネイティブ VLAN を含めても無視されます。トランクポートは、ネイティブ VLAN トラフィックをポートから送信するときに、常に VLAN タグを削除します。また、まだネイティブ VLAN タグが付いているトラフィックを受信しません。

例：

```
ciscoasa(config-if)# switchport trunk allowed vlan 100,200,300
ciscoasa(config-if)#
```

ステップ 4 ネイティブ VLAN を選択します。

switchport trunk native vlan *vlan_id*

- *vlan_range*：VLAN ID を 1 ～ 4070 の間で設定します。デフォルト値は VLAN 1 です。

各ポートのネイティブ VLAN は 1 つのみですが、すべてのポートに同じネイティブ VLAN または異なるネイティブ VLAN を使用できます。

例：

```
ciscoasa(config-if)# switchport trunk native vlan 2
ciscoasa(config-if)#
```

ステップ 5 （任意）このスイッチポートを保護対象として設定します。これにより、スイッチポートが同じ VLAN 上の他の保護されたスイッチポートと通信するのを防ぐことができます。

switchport protected

スイッチ ポート上のデバイスが主に他の VLAN からアクセスされる場合、VLAN 内アクセスを許可する必要がない場合、および感染やその他のセキュリティ侵害に備えてデバイスを相互に分離する場合に、スイッチ ポートが相互に通信しないようにします。たとえば、3 つの Web サーバーをホストする DMZ がある場合、各スイッチポートに **switchport protected** コマンドを適用すると、Web サーバーを相互に分離できます。内部ネットワークと外部ネットワークはいずれも 3 つの Web サーバーすべてと通信でき、その逆も可能ですが、Web サーバーは相互に通信できません。

例：

```
ciscoasa(config-if)# switchport protected
ciscoasa(config-if)#
```

ステップ 6 （任意）速度を設定します。

speed {**auto** | **10** | **100** | **1000**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# speed 100
ciscoasa(config-if)#
```

ステップ 7 （任意）二重通信を設定します。

duplex {**auto** | **full** | **half**}

デフォルトは **auto** です。

例：

```
ciscoasa(config-if)# duplex half
ciscoasa(config-if)#
```

ステップ 8 スイッチポートをイネーブルにします。

no shutdown

スイッチポートをディセーブルにするには、**shutdown** コマンドを入力します。

例：

```
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)#
```

例

次に、イーサネット 1/6 を VlAN 20 ～ 30 のトランクポートとして設定し、ネイティブ VLAN を 4 に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/6
ciscoasa(config-if)# switchport mode trunk
ciscoasa(config-if)# switchport trunk allowed vlan 20-30
ciscoasa(config-if)# switchport trunk native vlan 4
ciscoasa(config-if)# no shutdown
```

Power over Ethernet の設定

Power over Ethernet（PoE）ポートは、IP 電話や無線アクセスポイントなどのデバイスに電力を供給します。PoE はデフォルトでイネーブルです。この手順では、PoE を無効および有効にする方法と、オプションパラメータを設定する方法について説明します。

始める前に

マルチ コンテキスト モードでこの手順をシステム実行スペースで実行します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface ethernet1/*port_number*

例：

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)#
```

ステップ 2 PoE を有効または無効にします。

power inline {**auto** | **never** | **consumption wattage** *milliwatts*}

- **auto**：給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。ファイアウォールはLLDPを使用して、さらに適切なワット数をネゴシエートします。特定クラスのデバイスを接続すると、より多くの電力を使用する必要がある場合に備えて、そのクラスの最大値までプロビジョニングが行われます。たとえば、12.95W を要求するクラス 4 デバイスを追加した場合、そのデバイスが現在その電力すべてを使用していなくても、30Wが割り当てられます。一部のデバイスは、電力要件を再ネゴシエートできます。デバイスに必要な電力が割り当てられている電力よりも少ないことがわかっている場合は、代わりに **consumption wattage** を手動で設定して、他のデバイス用に電力を解放できます。
- **never**：PoE を無効にします。
- **consumption wattage** *milliwatts*：4000 から 30000（1010）または 90000（1210CP）のワット数をミリワット単位で手動で指定します。ワット数を手動で設定し、LLDPネゴシエーションを無効にする場合は、このコマンドを使用します。手動割り当ての場合、 出力にクラスが n/a と表示されます。これは、クラスが消費電力の決定に使用されないためです。

show power inline コマンドを使用して、現在の PoE ステータスを表示します。

（注）
コンテキスト内で、そのコンテキストに割り当てられているインターフェイスのPoEステータスを表示できます。

例：

1210CP

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
Total:120.000 (W) Used:79.000 (W) Remaining:41.000 (W)
Interface    Admin       Oper       Class  Current(mA) Voltage(V) Requested Allocated
Utilized
             State       State                                   Power(W)  Power(W)
Power(W)
---------    -----       -----      -----  ----------  ---------- --------- ---------
---------
Ethernet1/5  auto        on         1      17.212      54.523     4.000     4.000
0.932
Ethernet1/6  never       off        na     0.000       0.000      0.000     0.000
0.000
Ethernet1/7  consumption power-deny na     0.000       0.000      90.000    0.000
0.000
Ethernet1/8  auto        on         4D,5D  944.330     54.200     75.000    75.000
51.180
```

例：

Firepower 1010

```
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
```

```
Ethernet1/3   n/a     n/a     n/a           n/a
Ethernet1/4   n/a     n/a     n/a           n/a
Ethernet1/5   n/a     n/a     n/a           n/a
Ethernet1/6   n/a     n/a     n/a           n/a
Ethernet1/7   On      4       121.00        53.00
Ethernet1/8   On      4       88.00         53.00
```

例

次に、イーサネット 1/7 のワット数を手動で設定し、イーサネット 1/8 の電力を auto に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

スイッチポートのモニタリング

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show switch vlan**

  VLAN とスイッチポートの関連付けを表示します。

```
ciscoasa# show switch vlan
VLAN Name                    Status    Ports
---- --------------------- --------- --------------------
1    -                      down      Ethernet1/3,
                                      Ethernet1/4,
                                      Ethernet1/5,
                                      Ethernet1/6
                                      Ethernet1/7,
                                      Ethernet1/8
10   inside                 up        Ethernet1/1
20   outside                up        Ethernet1/2
```

- **show switch mac-address-table**

  スタティックおよびダイナミック MAC アドレス エントリを表示します。

```
ciscoasa# show switch mac-address-table
Legend: Age - entry expiration time in seconds
  Mac Address  | VLAN |       Type       | Age | Port
-------------------------------------------------------
```

```
0c75.bd11.c504 | 0010 |     dynamic      | 330 | In0/0
885a.92f6.c6e3 | 0010 |     dynamic      | 330 | Et1/1
0c75.bd11.c504 | 0020 |     dynamic      | 330 | In0/0
885a.92f6.c45b | 0020 |     dynamic      | 330 | Et1/2
```

- **show arp**

  ダイナミック、スタティック、およびプロキシ ARP エントリを表示します。ダイナミック ARP エントリには、ARP エントリの秒単位のエージングが含まれています。エージングの代わりに、スタティック ARP エントリにはダッシュ（-）が、プロキシ ARP エントリには「alias」という状態が含まれています。次に、**show arp** コマンドの出力例を示します。1 つめのエントリは、2 秒間エージングされているダイナミック エントリです。2 つめのエントリはスタティック エントリ、3 つめのエントリはプロキシ ARP のエントリです。

```
ciscoasa# show arp
outside 10.86.194.61 0011.2094.1d2b 2
outside 10.86.194.1 001a.300c.8000 -
outside 10.86.195.2 00d0.02a8.440a alias
```

- **show power inline**

  PoE+ ステータスを表示します。

  1210CP：

```
ciscoasa(config-if)# show power inline
Total:120.000 (W) Used:79.000 (W) Remaining:41.000 (W)
Interface    Admin      Oper       Class  Current(mA) Voltage(V) Requested Allocated
 Utilized
             State       State                                    Power(W)  Power(W)
  Power(W)
---------    -----      -----      -----  ----------  ---------- --------- ---------
 ---------
Ethernet1/5  auto        on         1      17.212      54.523     4.000     4.000
   0.932
Ethernet1/6  never       off        na     0.000       0.000      0.000     0.000
   0.000
Ethernet1/7  consumption power-deny na     0.000       0.000      90.000    0.000
   0.000
Ethernet1/8  auto        on         4D,5D  944.330     54.200     75.000    75.000
   51.180
```

  1010：

```
ciscoasa# show power inline
   Interface     Power   Class   Current (mA)   Voltage (V)
   ---------     -----   -----   ------------   -----------
   Ethernet1/1   n/a     n/a     n/a            n/a
   Ethernet1/2   n/a     n/a     n/a            n/a
   Ethernet1/3   n/a     n/a     n/a            n/a
   Ethernet1/4   n/a     n/a     n/a            n/a
   Ethernet1/5   n/a     n/a     n/a            n/a
   Ethernet1/6   n/a     n/a     n/a            n/a
   Ethernet1/7   On      4       121.00         53.00
   Ethernet1/8   On      4       88.00          53.00
```

スイッチポートの例

次のトピックでは、ルーテッドモードおよびトランスペアレントモードでスイッチポートを設定する例を示します。

ルーテッドモードの例

次の例では、2 つの VLAN インターフェイスを作成し、2 つのスイッチポートを内部インターフェイスに、もう 1 つを外部インターフェイスに割り当てます。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

トランスペアレントモードの例

次の例では、ブリッジグループ 1 に 2 つの VLAN インターフェイスを作成し、2 つのスイッチポートを内部インターフェイスに、もう 1 つを外部インターフェイスに割り当てます。

```
firewall transparent
!
interface BVI1
ip address 10.20.20.1 255.255.255.0
!
interface Vlan11
bridge-group 1
nameif inside
security-level 100
no shutdown
!
```

```
interface Vlan20
bridge-group 1
nameif outside
security-level 0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
```

ファイアウォール インターフェイス/スイッチポートの混合の例

次の例では、内部インターフェイス用の 1 つの VLAN インターフェイスと、外部および dmz 用の 2 つのファイアウォール インターフェイスを作成します。

```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/4
nameif outside
security-level 0
ip address 10.12.11.1 255.255.255.0
no shutdown
!
interface Ethernet1/5
nameif dmz
security-level 50
ip address 10.13.11.1 255.255.255.0
no shutdown
```

統合ルーティングおよびブリッジングの例

次の例では 2 つのブリッジグループを作成します。ブリッジグループ 1 に 2 つの VLAN インターフェイス（inside_1 と inside_2）、ブリッジグループ 2 に 1 つの VLAN インターフェイス（outside）を含めます。4 番目の VLAN インターフェイスはブリッジグループの一部ではなく、通常のルーテッドインターフェイスです。同じ VLAN 上のスイッチポート間のトラフィックは、ASA のセキュリティポリシーの対象にはなりません。ただし、ブリッジグループ内の VLAN 間のトラフィックにはセキュリティポリシーが適用されるため、特定のセグメント間のレイヤブリッジグループとスイッチポートを選択することができます。

```
interface BVI1
nameif inside_bvi
security-level 100
ip address 10.30.1.10 255.255.255.0
!
interface BVI2
nameif outside_bvi
security-level 0
ip address 10.40.1.10 255.255.255.0
!
interface Vlan10
bridge-group 1
nameif inside_1
security-level 100
no shutdown
!
interface Vlan20
bridge-group 2
nameif outside
security-level 0
no shutdown
!
interface Vlan30
bridge-group 1
nameif inside_2
security-level 100
no shutdown
!
interface Vlan 100
nameif dmz
security-level 0
ip address 10.1.1.1 255.255.255.0
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/4
```

```
switchport
switchport access vlan 20
security-level 100
no shutdown
!
interface Ethernet1/5
switchport
switchport access vlan 100
no shutdown
!
interface Ethernet1/6
switchport
switchport access vlan 10
no shutdown
!
interface Ethernet1/7
switchport
switchport access vlan 30
no shutdown
!
interface Ethernet1/8
switchport
switchport access vlan 100
no shutdown
```

フェールオーバーの例

次に、イーサネット 1/3 をフェールオーバー インターフェイスとして設定する例を示します。

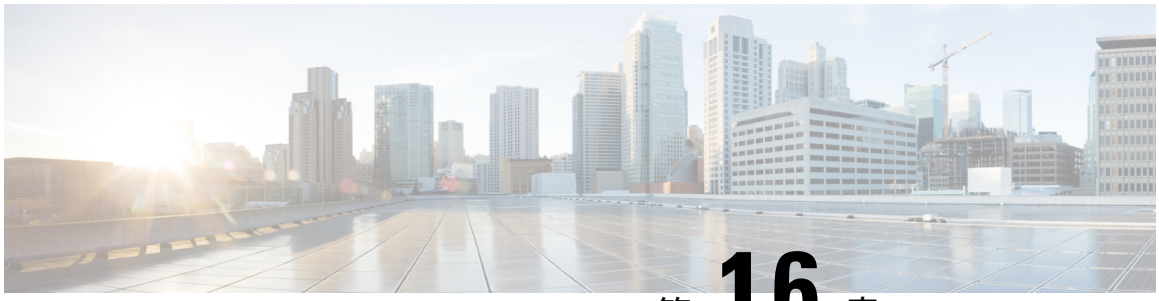
```
interface Vlan11
nameif inside
security-level 100
ip address 10.11.11.1 255.255.255.0 standby 10.11.11.2
no shutdown
!
interface Vlan20
nameif outside
security-level 0
ip address 10.20.20.1 255.255.255.0 standby 10.20.20.2
no shutdown
!
interface Ethernet1/1
switchport
switchport access vlan 11
no shutdown
!
interface Ethernet1/2
switchport
switchport access vlan 20
no shutdown
!
interface Ethernet1/3
description LAN/STATE Failover Interface
no shutdown
!
failover
failover lan unit primary
failover lan interface folink Ethernet1/3
failover replication http
failover link folink Ethernet1/3
```

```
failover interface ip folink 10.90.90.1 255.255.255.0 standby 10.90.90.2
```

スイッチポートの履歴

表 *27*：スイッチポートの履歴

機能名	バージョン	機能情報
Cisco Secure Firewall 1210CP IEEE 802.3bt のサポート（PoE++ および Hi-PoE）	9.23(1)	IEEE 802.3bt のサポートに関連する次の改善を確認してください。 • PoE++ と Hi-PoE：ポートあたり最大 90 W。 • シングルシグネチャおよびデュアルシグネチャの受電デバイス（PD）。 • パワーバジェットが先着順で行われます。 • **show power inline** にパワーバジェットフィールドが追加されました。 新規/変更されたコマンド：**power inline**、**show power inline**
Cisco Secure Firewall 1210/1220 ハードウェアスイッチのサポート	9.22(1)	Cisco Secure Firewall 1210/1220 では、各イーサネット インターフェイスをスイッチポートまたはファイアウォール インターフェイスとして設定できます。
Cisco Secure Firewall 1210CP PoE+ は、イーサネットポート 1/5 ～ 1/8 でサポートされます	9.22(1)	Cisco Secure Firewall 1210CP は、イーサネットポート 1/5 ～ 1/8 で Power over Ethernet+（PoE+）をサポートします。
Firepower 1010 ハードウェア スイッチのサポート	9.13(1)	Firepower 1010 では、各イーサネット インターフェイスをスイッチ ポートまたはファイアウォール インターフェイスとして設定できます。 新しい/変更されたコマンド：**forward interface**、**interface vlan**、**show switch mac-address-table**、**show switch vlan**、**switchport**、**switchport access vlan**、**switchport mode**、**switchport trunk allowed vlan**
イーサネット 1/7 およびイーサネット 1/8 での Firepower 1010 PoE+ のサポート	9.13(1)	Firepower 1010 は、イーサネット 1/7 およびイーサネット 1/8 での Power over Ethernet+（PoE+） をサポートしています。 新しい/変更されたコマンド：**power inline**、**show power inline**



第 16 章

EtherChannel インターフェイスインターフェイス

この章では、EtherChannel インターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

特殊な必須要件を保有する ASA クラスタ インターフェイスについては、Cisco Secure Firewall 3100/4200 の ASA クラスタ （407 ページ） を参照してください。

（注） Firepower 4100/9300 シャーシ、EtherChannel インターフェイスは FXOS オペレーティングシステムで設定されます。詳細については、お使いのシャーシの設定または導入ガイドを参照してください。

- EtherChannel インターフェイスについて （865 ページ）
- EtherChannel インターフェイスのガイドライン （869 ページ）
- EtherChannel インターフェイスのデフォルト設定 （872 ページ）
- EtherChannel の設定 （872 ページ）
- EtherChannel のモニタリング （877 ページ）
- EtherChannel の例 （878 ページ）
- EtherChannel インターフェイスの履歴 （879 ページ）

EtherChannel インターフェイスについて

ここでは、EtherChannel インターフェイスについて説明します。

EtherChannel について

802.3ad EtherChannel は、単一のネットワークの帯域幅を増やすことができるように、個別のイーサネット リンク（チャネル グループ）のバンドルで構成される論理インターフェイスです（ポートチャネル インターフェイスと呼びます）。ポートチャネル インターフェイスは、インターフェイス関連の機能を設定するときに、物理インターフェイスと同じように使用します。

モデルでサポートされているインターフェイスの数に応じて、最大 48 個の Etherchannel を設定できます。

チャネル グループのインターフェイス

各チャネルグループには、最大 8 個のアクティブインターフェイスを持たせることができます。ただし、ISA 3000 は、16 個のアクティブインターフェイスをサポートしています。8 個のアクティブインターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

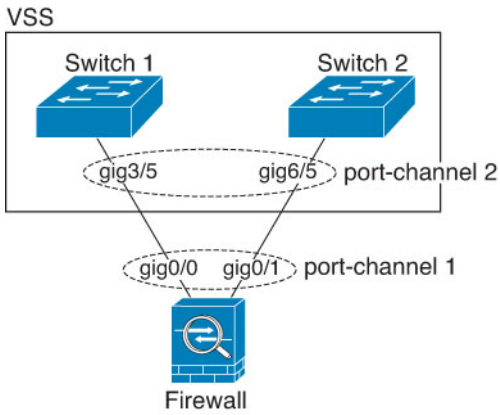
EtherChannel によって、チャネル内の使用可能なすべてのアクティブインターフェイスのトラフィックが集約されます。インターフェイスは、送信元または宛先 MAC アドレス、IP アドレス、TCP および UDP ポート番号、および VLAN 番号に基づいて、独自のハッシュ アルゴリズムを使用して選択されます。

別のデバイスの EtherChannel への接続

ASA EtherChannelの接続先のデバイスも802.3ad EtherChannelをサポートしている必要があります。たとえば、Catalyst 6500スイッチまたはCisco Nexus 7000に接続できます。

スイッチが仮想スイッチングシステム（VSS）または仮想ポートチャネル（vPC）の一部である場合、同じ EtherChannel 内の ASA インターフェイスを VSS/vPC 内の個別のスイッチに接続できます。個別のスイッチは単一のスイッチのように動作するため、スイッチインターフェイスは同じ EtherChannel ポートチャネル インターフェイスのメンバです。

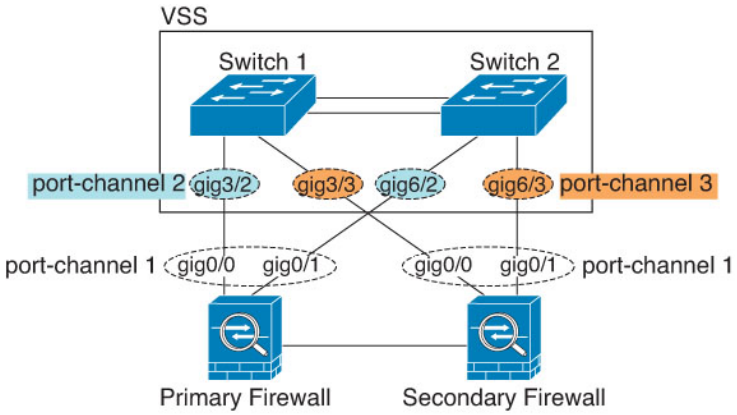
図 *70 : VSS/vPC*への接続



（注） ASA デバイスがトランスペアレント ファイアウォール モードになっており、2 組の VSS/vPC スイッチ間に ASA デバイスを配置する場合は、EtherChannel 内で ASA デバイスに接続されたすべてのスイッチポートで単方向リンク検出（UDLD）を無効にしてください。UDLDを有効にすると、スイッチポートは他のVSS/vPCペアの両方のスイッチから送信されたUDLDパケットを受信する場合があります。受信側スイッチは、"UDLDネイバーの不一致" という理由で受信側インターフェイスをダウン状態にします。

ASA デバイスをアクティブ/スタンバイフェールオーバー展開で使用する場合、ASA デバイスごとに 1 つ、VSS/vPC 内のスイッチで個別の EtherChannel を作成する必要があります。各 ASA デバイスで、1 つの EtherChannel が両方のスイッチに接続します。すべてのスイッチインターフェイスを両方の ASA デバイスに接続する単一の EtherChannel にグループ化できる場合でも（この場合、個別の ASA システム ID のため、EtherChannel は確立されません）、単一の EtherChannel は望ましくありません。これは、トラフィックをスタンバイ ASA デバイスに送信しないようにするためです。

図 *71 : アクティブ/スタンバイ フェールオーバーと VSS/vPC*



Link Aggregation Control Protocol

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。

EtherChannel 内の各物理インターフェイスを次のように設定できます。

- アクティブ：LACP アップデートを送信および受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。
- パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。ハードウェアモデルではサポートされていません。
- オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ロード バランシング

ASA デバイスは、パケットの送信元および宛先 IP アドレスをハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します（この基準は設定可能です）。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links*の結果が0となるすべてのパケットは、EtherChannel内の最初のインターフェイスへ送信され、以降は結果が1となるものは2番目のインターフェイスへ、結果が2となるものは3番目のインターフェイスへ、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

クラスタリングのスパンド EtherChannel では、ロードバランシングは ASA ごとに行われます。たとえば、8台のASAにわたるスパンドEtherChannel内に32個のアクティブインターフェイスがあり、EtherChannel内の1台のASAあたり4個のインターフェイスがある場合、ロードバランシングは1台のASAの4個のインターフェイス間でのみ行われます。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

関連トピック

EtherChannel のカスタマイズ（ISA 3000） （875 ページ）

EtherChannel MAC アドレス

1 つのチャネル グループに含まれるすべてのインターフェイスは、同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。

Firepower および Secure Firewall ハードウェア

ポートチャネル インターフェイスは、内部インターフェイスの内部データ 0/1 の MAC アドレスを使用します。または、ポート チャネル インターフェイスの MAC アドレスを手動で設定することもできます。マルチコンテキストモードでは、固有の MAC アドレスを共有インターフェイス（EtherChannel ポートインターフェイスを含む）に自動的に割り当てることができます。シャーシ上のすべての EtherChannel インターフェイスは同じ MAC アドレスを使用するため、たとえば、SNMP ポーリングを使用する場合、複数のインターフェイスが同じ MAC アドレスを持つことに注意してください。

（注） メンバーインターフェイスは、再起動後に内部データ 0/1 MAC アドレスのみを使用します。再起動する前に、メンバーインターフェイスは独自の MAC アドレスを使用するた再起動後に新しいメンバーインターフェイスを追加する場合、MAC アドレスを更新するためにもう一度再起動する必要があります。

EtherChannel インターフェイスのガイドライン

ブリッジグループ

ルーテッドモードでは、ASA 定義の EtherChannel はブリッジグループメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。

フェールオーバー

- EtherChannel インターフェイスを フェールオーバー リンクとして使用する場合、フェールオーバーペアの両方のユニットでその事前設定を行う必要があります。プライマリユニットで設定し、セカンダリユニットに複製されることは想定できません。これは、複製にはフェールオーバー リンク自体が必要であるためです。
- EtherChannel インターフェイスをステートリンクに対して使用する場合、特別なコンフィギュレーションは必要ありません。コンフィギュレーションは通常どおりプライマリユニットから複製されます。Firepower 4100/9300 シャーシ では、EtherChannel を含むすべてのインターフェイスを、両方のユニットで事前に設定する必要があります。
- フェールオーバー の EtherChannel インターフェイスをモニターできます。そのときには、**monitor-interface** コマンドを使用します。アクティブなメンバーインターフェイスがスタ

ンバイインターフェイスにフェールオーバーした場合、デバイスレベルのフェールオーバーをモニタしているときには、EtherChannel インターフェイスで障害が発生しているようには見えません。すべての物理インターフェイスで障害が発生した場合にのみ、EtherChannel インターフェイスで障害が発生しているように見えます（EtherChannel インターフェイスでは、障害の発生が許容されるメンバインターフェイスの数を設定できます）。

- EtherChannelインターフェイスをフェールオーバー リンクまたはステートリンクに対して使用する場合、異常なパケットを防止するために、EtherChannel 内の 1 つのインターフェイスのみが使用されます。そのインターフェイスで障害が発生した場合は、EtherChannel 内の次のリンクが使用されます。フェールオーバーリンクとして使用中のEtherChannelの設定は変更できません。設定を変更するには、フェールオーバーを一時的に無効にする必要があります。これにより、その期間中は フェールオーバー が発生することはありません。

サポート モデル

- Firepower 4100/9300、または ASA 仮想 の場合、ASA に EtherChannel を追加することはできません。Firepower 4100/9300 は EtherChannel をサポートしていますが、シャーシの FXOS で EtherChannel のすべてのハードウェア設定を実行する必要があります。
- EtherChannel で Firepower 1010 または Cisco Secure Firewall 1210/1220 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

クラスタリング

- EtherChannel インターフェイスをクラスタ制御リンクとして使用するときは、クラスタのすべてのユニットでそのリンクを事前に設定する必要があります。プライマリユニットで設定し、その設定がメンバーユニットに複製されると期待することはできません。これは、クラスタ制御リンク自体が複製に必要であるためです。
- スパンドEtherChannelまたは個々のクラスタインターフェイスを設定するには、「クラスタリング」の章を参照してください。

EtherChannelの一般的なガイドライン

- モデルで利用可能なインターフェイスの数に応じて、最大48個のEtherchannelを設定できます。
- 各チャネルグループには、最大8個のアクティブインターフェイスを持たせることができます。ただし、ISA 3000は、16個のアクティブインターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネルグループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは8個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。

- チャネルグループ内のすべてのインターフェイスは、メディアタイプと速度が同じでなければなりません。また、同じ速度とデュプレックスに設定する必要があります。メディアタイプはRJ-45またはSFPのいずれかです。異なるタイプ（銅と光ファイバ）のSFPを混在させることができます。大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GBと10GBのインターフェイスなど）を混在させることはできません。ただし、Cisco Secure Firewall 1200/3100/4200の場合は、速度が [SFPを検出（Detect SFP）] に設定されている限り、異なるインターフェイス容量をサポートします。この場合、最も低い共通速度が使用されます。
- ASA の EtherChannel の接続先デバイスも 802.3ad EtherChannel をサポートしている必要があります。
- ASAデバイスは、VLANタグ付きのLACPDUをサポートしていません。Cisco IOS **vlan dot1Q tag native** コマンドを使用して隣接スイッチのネイティブ VLAN タギングを有効にすると、ASAデバイスはタグ付きのLACPDUをドロップします。隣接スイッチのネイティブVLANタギングは、必ず無効にしてください。マルチ コンテキスト モードでは、これらのメッセージはパケット キャプチャに含まれていないため、問題を効率的に診断できません。
- LACP レートはモデルによって異なります。レート（通常または高速）を設定すると、デバイスは接続中のスイッチにそのレートを要求します。デバイスの方も接続中のスイッチによって要求されたレートで送信します。両側で同じレートを設定することを推奨します。
  - Firepower 4100/9300：LACP レートは、FXOS ではデフォルトで高速に設定されていますが、通常（低速とも呼ばれる）に設定することもできます。
  - Cisco Secure Firewall 3100/4200：LACP レートは、デフォルトで通常（低速）に設定されていますが、デバイスで高速に設定することもできます。
  - 他のすべてのモデル：LACP レートが通常（低速とも呼ばれる）に設定されており、変更できません。つまり、デバイスは接続中のスイッチに常に低速レートを要求します。スイッチのレートを低速に設定して、両側が同じレートでLACPメッセージを送信するように設定することを推奨します。
- 15.1(1)S2以前のCisco IOSソフトウェアバージョンを実行するASAでは、スイッチスタックへのEtherChannelの接続がサポートされていませんでした。デフォルトのスイッチ設定では、ASA EtherChannelがクロススタックに接続されている場合、プライマリスイッチの電源がオフになると、残りのスイッチに接続されているEtherChannelは起動しません。互換性を高めるため、**stack-mac persistent timer** コマンドを設定して、十分なリロード時間を確保できる大きな値、たとえば8分、0（無制限）などを設定します。または、15.1(1)S2など、より安定したスイッチ ソフトウェア バージョンにアップグレードできます。
- すべての ASA コンフィギュレーションは、メンバー物理インターフェイスではなく論理 EtherChannel インターフェイスを参照します。
- ブレークアウトポートを持つポートチャネルを削除する前に、まず、ポート チャネル メンバーシップからブレークアウトポートを削除する必要があります。そうしないと、ポートチャネルを削除した後にブレークアウトポートに再参加するときに、ブレークアウト

ポートが関連付けられていないものとして表示されます。これは、ポートチャネルに固定ポートのみがあり、ブレークアウトポートがない場合には、適用されません。

EtherChannel インターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- EtherChannel ポートチャネル インターフェイス：イネーブル。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。

EtherChannel の設定

ここでは、EtherChannel ポートチャネル インターフェイスの作成、インターフェイスの EtherChannel への割り当て、EtherChannel のカスタマイズ方法について説明します。

EtherChannel へのインターフェイスの追加

ここでは、EtherChannel ポートチャネル インターフェイスを作成し、インターフェイスを EtherChannel に割り当てる方法について説明します。デフォルトでは、ポートチャネル インターフェイスはイネーブルになっています。

始める前に

- 使用しているモデルに設定されているインターフェイスの数に応じて、最大 48 個の EtherChannel を設定できます。

- 各チャネルグループには、最大 8 個のアクティブインターフェイスを持たせることができます。ただし、ISA 3000 は、16 個のアクティブインターフェイスをサポートしています。8 個のアクティブ インターフェイスだけをサポートするスイッチの場合、1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。インターフェイスは 8 個のみアクティブにできるため、残りのインターフェイスは、インターフェイスの障害が発生した場合のスタンバイ リンクとして動作できます。
- クラスタリング用にスパンド EtherChannel を設定するには、この手順の代わりにクラスタリングの章を参照してください。
- チャネルグループ内のすべてのインターフェイスは、同じメディアタイプと容量である必要があり、同じ速度とデュプレックスに設定する必要があります。メディアタイプは RJ-45 または SFP のいずれかです。異なるタイプ（銅と光ファイバ）の SFP を混在させることができます。速度が [SFPを検出（Detect SFP）] に設定されている限り、さまざまなインターフェイス容量をサポートする Cisco Secure Firewall 3100/4200 を除いて（この場合は共通の最低速度が使用されます）、大容量のインターフェイスで速度を低く設定することでインターフェイス容量（1GB と 10GB のインターフェイスなど）を混在させることはできません。。
- 名前が設定されている場合は、物理インターフェイスをチャネル グループに追加できません。最初に、**no nameif** コマンドを使用して、名前を削除する必要があります。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

⚠

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

手順

ステップ 1 チャネル グループに追加するインターフェイスを指定します。

interface *physical_interface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
```

physical_interface ID には、タイプ、スロット、およびポート番号（type[slot/]port）が含まれます。チャネル グループのこの最初のインターフェイスによって、グループ内の他のすべてのインターフェイスのタイプと速度が決まります。

トランスペアレント モードで、複数の管理インターフェイスがあるチャネル グループを作成する場合は、この EtherChannel を管理専用インターフェイスとして使用できます。

ステップ 2 この物理インターフェイスを EtherChannel に割り当てます。

channel-group *channel_id* **mode** {**active** | **passive** | **on**}

例：

```
ciscoasa(config-if)# channel-group 1 mode active
```

channel_id は 1 ～ 48 の整数（Firepower 1010 には 1 と 8）です。このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合、ポートチャネル インターフェイスが作成されます。

interface port-channel *channel_id*

active モードを使用することを推奨します。**パッシブ** モードは ISA 3000 でのみ使用できます。

ステップ 3 （任意）（Secure Firewall 3100/4200 のみ）チャネルグループの物理インターフェイスの LACP データ ユニット受信レートを設定します。

lacp rate {**normal** | **fast**}

デフォルトは **normal**（低速、30 秒ごと）です。 **fast** オプションは、1 秒ごとに LACP データ ユニットを受信します。接続されているスイッチの設定と一致させる必要があります。

ステップ 4 （任意）（ISA 3000 モデルのみ）チャネル グループの物理インターフェイスのプライオリティを設定します。

lacp port-priority *number*

例：

```
ciscoasa(config-if)# lacp port-priority 12345
```

プライオリティの *number* は、1 ～ 65535 の整数です。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポートプライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、**lacp port-priority** の値を、1/3 インターフェイスでは 12345 とし、0/7 インターフェイスではデフォルトの 32768 とします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。**lacp system-priority** コマンドを参照してください。

ステップ 5 （オプション）ポートチャネル インターフェイスのイーサネット プロパティを設定します。この設定は、個別インターフェイスに対して設定されたプロパティよりも優先されます。

interface port-channel *channel_id*

イーサネットのコマンドについては、物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 （830 ページ）を参照してください。これらのパラメータはチャネル グループのすべてのインターフェイスで一致している必要があるため、この方法はこれらのパラメータを設定するショートカットになります。

ステップ 6 チャネル グループに追加するインターフェイスごとに、ステップ 1 ～ 3 を繰り返します。

チャネル グループの各インターフェイスのタイプと速度が同一であることが必要です。半二重はサポートされません。一致しないインターフェイスを追加すると、一時停止状態になります。

ステップ 7 （任意） （Secure Firewall 3100/4200 のみ）チャネルグループの物理インターフェイスの LACP データユニット受信レートを設定します。

a) [Interfaces] テーブルで物理インターフェイスを選択し、[Edit] をクリックします。

[Edit Interface] ダイアログボックスが表示されます。

b) [Advanced] タブをクリックします。

c) **[EtherChannel]** 領域で、**[Rate]** ドロップダウンリストから、**[Normal]** または **[Fast]** を選択します。

デフォルトは **[通常（Normal）]**（低速、30 秒ごと）です。**[Fast]** オプションは、LACP 更新を毎秒受信します。接続されているスイッチの設定と一致させる必要があります。

関連トピック

Link Aggregation Control Protocol （868 ページ）
EtherChannel のカスタマイズ（ISA 3000） （875 ページ）

EtherChannel のカスタマイズ（ISA 3000）

この項では、EtherChannel のインターフェイスの最大数、EtherChannel をアクティブにするための動作インターフェイスの最小数、ロード バランシング アルゴリズム、およびその他のオプション パラメータを設定する方法について説明します。これらのパラメータは、ISA 3000 にのみ適用されます。

手順

ステップ 1 ポートチャネル インターフェイスを指定します。

interface port-channel *channel_id*

例：

```
ciscoasa(config)# interface port-channel 1
```

このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。まだインターフェイスを追加していない場合は、このコマンドを実行するとポートチャネル インターフェイスが作成されます。

少なくとも 1 つのメンバー インターフェイスをポートチャネル インターフェイスに追加してからでなければ、インターフェイスの論理パラメータ（名前など）は設定できません。

ステップ 2 チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。

lacp max-bundle *number*

例：

```
ciscoasa(config-if)# lacp max-bundle 6
```

number には、1 ～ 16 の範囲内の値を入力します。デフォルトは 16 です。スイッチが 16 個のアクティブインターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。

ステップ 3 ポートチャネルインターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。

port-channel min-bundle *number*

例：

```
ciscoasa(config-if)# port-channel min-bundle 2
```

number には、1 ～ 16 の範囲内の値を入力します。デフォルトは 1 です。チャネル グループ内のアクティブ インターフェイス数がこの値よりも小さい場合、ポートチャネル インターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。

ステップ 4 ロード バランシング アルゴリズムを設定します。

port-channel load-balance {**dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port**}

例：

```
ciscoasa(config-if)# port-channel load-balance src-dst-mac
```

デフォルトでは、ASA はパケットの送信元および宛先 IP アドレス（**src-dst-ip**）に従ってインターフェイスでのパケットの負荷を分散します。パケットの分類の基準となるプロパティを変更する場合は、このコマンドを使用します。たとえば、トラフィックが同じ送信元および宛先 IP アドレスに大きく偏っている場合、EtherChannel 内のインターフェイスに対するトラフィックの割り当てがアンバランスになります。別のアルゴリズムに変更すると、トラフィックはより均等に分散される場合があります。

ステップ 5 LACP システム プライオリティを設定します。

lacp system-priority *number*

例：

```
ciscoasa(config)# lacp system-priority 12345
```

number には、1 ～ 65535 の範囲内の値を入力します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。このコマンドは、ASA に対してグローバルです。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。EtherChannel 内でのインターフェイス プライオリティについては、**lacp port-priority** コマンドを参照してください。

関連トピック

ロード バランシング （868 ページ）
EtherChannel へのインターフェイスの追加 （872 ページ）

EtherChannel のモニタリング

次のコマンドを参照してください。

（注） Firepower 、および Secure Firewall モデルの場合、一部の統計は ASA コマンドで表示されません。FXOS コマンドを使用して、より詳細なインターフェイス統計情報を表示する必要があります。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

詳細については、『FXOS troubleshooting guide』を参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- （ISA 3000 のみ）**show lacp** {[*channel_group_number*] {**counters** | **internal** | **neighbor**} | **sys-id**}

  EtherChannel の場合は、LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。

- （ISA 3000 のみ）**show port-channel** [*channel_group_number*] [**brief** | **detail** | **port** | **protocol** | **summary**]

  EtherChannel の場合は、EtherChannel 情報が、詳細な 1 行サマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。

- （ISA 3000 のみ）**show port-channel** *channel_group_number* **load-balance** [**hash-result** {**ip** | **ipv6** | **l4port** | **mac** | **mixed** | **vlan-only**} *parameters*]

  EtherChannel の場合は、ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

EtherChannel の例

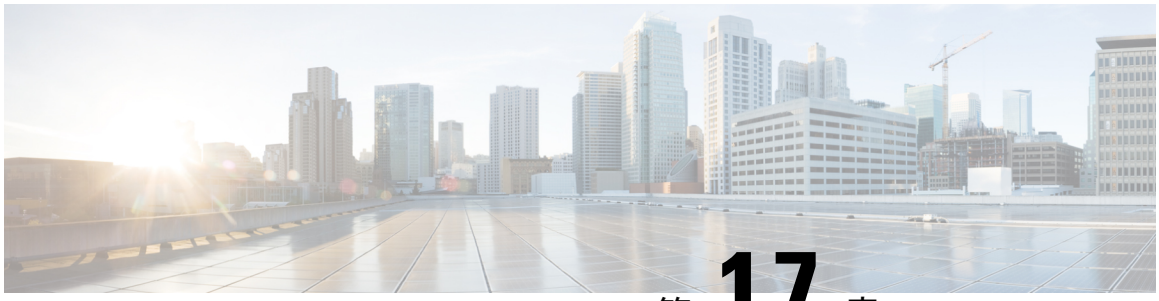
次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

```
lacp system-priority 1234
interface GigabitEthernet0/0
  channel-group 1 mode active
interface GigabitEthernet0/1
  channel-group 1 mode active
interface GigabitEthernet0/2
  lacp port-priority 1234
  channel-group 1 mode passive
interface Port-channel1
  lacp max-bundle 4
  port-channel min-bundle 2
  port-channel load-balance dst-ip
```

EtherChannel インターフェイスの履歴

表 *28 : EtherChannel* インターフェイスの履歴

機能名	リリース	機能情報
EtherChannel サポート	8.4(1)	最大 48 個の 802.3ad EtherChannel（1 つあたりのアクティブ インターフェイス 8 個）を設定できます。 **channel-group**、**lacp port-priority**、**interface port-channel**、**lacp max-bundle**、**port-channel min-bundle**、**port-channel load-balance**、**lacp system-priority**、**clear lacp counters**、**show lacp**、**show port-channel** の各コマンドが導入されました。 （注） EtherChannel は ASA 5505 ではサポートされません。
EtherChannel あたり 16 個のアクティブ リンクのサポート	9.2(1)	EtherChannel あたり最大で 16 個のアクティブ リンクを設定できるようになりました。これまでは、8 個のアクティブ リンクと 8 個のスタンバイ リンクが設定できました。スイッチは、16 個のアクティブ リンクをサポート可能である必要があります（たとえば、Cisco Nexus 7000 と F2 シリーズ 10 ギガビット イーサネット モジュール）。 （注） 旧バージョンの ASA からアップグレードする場合、互換性を得るために、アクティブなインターフェイスの最大数を 8 に設定します（**lacp max-bundle** コマンド）。 次のコマンドが変更されました。**lacp max-bundle** および **port-channel min-bundle**。



第 17 章

ループバック インターフェイス

この章では、ループバック インターフェイスを設定する方法について説明します。

- ループバック インターフェイスについて （881 ページ）
- ループバック インターフェイスの概要 （882 ページ）
- ループバック インターフェイスの設定 （882 ページ）
- ループバック インターフェイスへのトラフィックのレート制限 （883 ページ）
- ループバック インターフェイスのモニタリング （884 ページ）
- ループバック インターフェイスの履歴 （885 ページ）

ループバック インターフェイスについて

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、複数の物理インターフェイスを介して IPv4 および IPv6 に到達できます。ループバック インターフェイスはパス障害の克服に役立ちます。任意の物理インターフェイスからアクセスできるため、1 つがダウンした場合、別のインターフェイスからループバック インターフェイスにアクセスできます。

ループバック インターフェイスは、次の目的で使用できます。

- AAA
- BGP
- DNS
- HTTP
- ICMP
- SNMP
- SSH
- スタティックおよびダイナミック VTI トンネル
- Syslog
- Telnet

ASA は、ダイナミック ルーティング プロトコルを使用してループバックアドレスを配布できます。または、ピアデバイスでスタティックルートを設定して、 ASA のいずれかの物理インターフェイスを介してループバック IP アドレスに到達できます。ASA では、ループバック インターフェイスを指定するスタティックルートを設定できません。

ループバック インターフェイスの概要

フェールオーバー とクラスタリング

- クラスタリングはサポートされません。

コンテキスト モード

- VTIはシングルコンテキストモードでのみサポートされます。マルチコンテキストモードでは、他のループバックの使用がサポートされます。

その他のガイドラインと制限事項

- 物理インターフェイスからループバック インターフェイスへのトラフィックでは、TCP シーケンスのランダム化は常に無効になっています。

ループバック インターフェイスの設定

ループバック インターフェイスを追加します。

手順

ステップ 1 ループバック インターフェイスを作成します。

interface loopback *number*

0 ー 10413 の値を指定できます。

例：

```
ciscoasa(config)# interface loopback 10
```

ステップ 2 名前と IP アドレスを設定します。ルーテッド モードおよびトランスペアレント モードのインターフェイス （927 ページ）を参照してください。

ステップ 3 ループバックトラフィックのレート制限を設定します。「ループバック インターフェイスへのトラフィックのレート制限 （883 ページ）」を参照してください。

ループバック インターフェイスへのトラフィックのレート制限

システムに過剰な負荷がかからないように、ループバック インターフェイス IP アドレスに送信されるトラフィックのレートを制限する必要があります。グローバルサービスポリシーに接続制限ルールを追加できます。この手順では、デフォルトのグローバルポリシー（global_policy）への追加を示します。

手順

ステップ 1 ループバック インターフェイス IP アドレスへのトラフィックを識別するアクセスリストを作成します。

access-list *name* **extended permit ip any host** *loopback_ip*

ループバック インターフェイス IP アドレスごとに ACE を作成します。**any** の代わりに送信元 IP アドレスを指定して、このアクセスリストを絞り込むこともできます。

例：

```
ciscoasa(config)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
```

ステップ 2 アクセスリストを識別するクラスマップを作成します。

class-map *name*

match access-list *acl_name*

例：

```
ciscoasa(config)# class-map rate-limit-loopback
ciscoasa(config-cmap)# match access-list loop
```

ステップ 3 グローバルポリシーマップの一部として、最大接続数および最大初期接続数をクラスマップに適用します。

policy-map global_policy

class *class_map_name*

set connection conn-max *conns* **embryonic-conn-max** *conns*

最大接続数をループバック インターフェイスの予期される接続数に設定し、初期接続数をより低い数に設定します。予期される必要なループバック インターフェイス セッション数に応じて、たとえば、5/2、10/5、または 1024/512 に設定できます。

初期接続制限を設定するとTCP代行受信が有効になります。この代行受信によって、TCP SYNパケットを使用してインターフェイスをフラッディングするDoS攻撃からシステムを保護します。

例：

```
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class rate-limit-loopback
ciscoasa(config-pmap-c)# set connection conn-max 5 embryonic-conn-max 2
```

例

次の例では、2つのループバック インターフェイス（10.1.1.1と10.2.1.1）に送信されるすべてのトラフィックに適用されるデフォルトグローバルポリシーの最大接続数と初期接続数を10と5に設定します。

```
ciscoasa(config)# interface loopback 1
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop1
ciscoasa(config-if)# interface loopback 2
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# nameif loop2
ciscoasa(config-if)# access-list loop extended permit ip any host 10.1.1.1
ciscoasa(config)# access-list loop extended permit ip any host 10.2.1.1
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match access-list loop
ciscoasa(config-cmap)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
ciscoasa(config-pmap-c)# set connection conn-max 10 embryonic-conn-max 5
```

ループバック インターフェイスのモニタリング

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

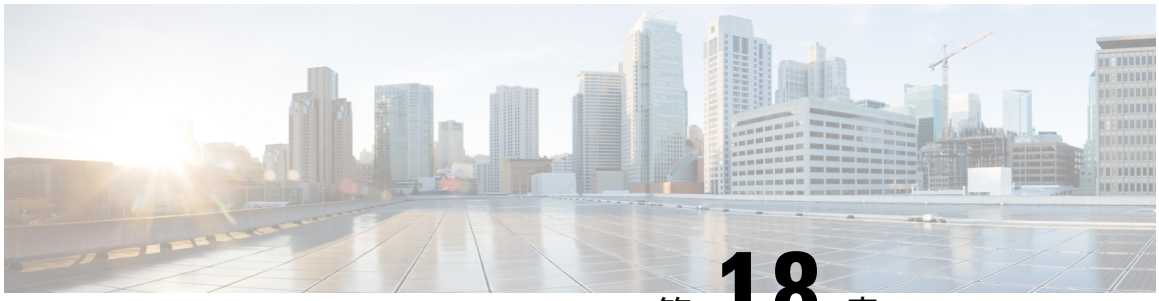
- **show interface ip brief**

  インターフェイスのIPアドレスとステータスを表示します。

ループバック インターフェイスの履歴

表 *29 :* ループバック インターフェイスの履歴

機能名	バージョン	機能情報
DNS、HTTP、ICMP、IPsec フローオフロードのループバック インターフェイスのサポート	9.20(1)	ループバック インターフェイスを追加して、以下に使用できるようになりました。 • DNS • HTTP • ICMP • IPsec フローのオフロード
VTI のループバック インターフェイス サポート	9.19(1)	ループバック インターフェイスは、静的および動的 VTI VPN トンネルの冗長性を提供します。ループバック インターフェイスを VTI の送信元インターフェイスとして設定できるようになりました。VTI インターフェイスは、静的に設定された IP アドレスの代わりに、ループバック インターフェイスの IP アドレスを継承することもできます。ループバック インターフェイスは、パス障害の克服に役立ちます。インターフェイスがダウンした場合、ループバック インターフェイスの IP アドレスを使用してすべてのインターフェイスにアクセスできます。 新規/変更されたコマンド：**tunnel source interface**、**ip unnumbered**、**ipv6 unnumbered**
ループバック インターフェイスのサポート	9.18(2)	ループバック インターフェイスを追加して、以下に使用できるようになりました。 • BGP • AAA • SNMP • Syslog • SSH • Telnet 新規/変更されたコマンド：**interface loopback**、**logging host**、**neighbor update-source**、**snmp-server host**、**ssh**、**telnet**



第 18 章

VLAN サブインターフェイス

この章では、VLAN サブインターフェイスを設定する方法について説明します。

（注） マルチコンテキストモードでは、この項のすべてのタスクをシステム実行スペースで実行してください。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。。

- VLAN サブインターフェイスについて （887 ページ）
- VLAN サブインターフェイスのライセンス （888 ページ）
- VLAN サブインターフェイスのガイドラインと制限事項 （889 ページ）
- VLAN サブインターフェイスのデフォルト設定 （890 ページ）
- VLAN サブインターフェイスと 802.1Q トランキングの設定 （890 ページ）
- VLAN サブインターフェイスのモニタリング （892 ページ）
- VLAN のサブインターフェイスの例 （892 ページ）
- VLAN サブインターフェイスの履歴 （893 ページ）

VLAN サブインターフェイスについて

VLAN サブインターフェイスを使用すると、1 つの物理インターフェイスまたは EtherChannel インターフェイスを、異なる VLAN ID でタグ付けされた複数の論理インターフェイスに分割できます。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。VLAN では、所定の物理インターフェイス上でトラフィックを分離しておくことができるため、物理インターフェイスまたは ASA を追加しなくても、ネットワーク上で使用できるインターフェイスの数を増やすことができます。この機能は、各コンテキストに固有のインターフェイスを割り当てることができるので、マルチコンテキストモードで特に便利です。

1 つのプライマリ VLAN と 1 つまたは複数のセカンダリ VLAN を設定できます。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。

VLAN サブインターフェイスのライセンス

モデル	ライセンス要件
Firepower 1010	Essentials ライセンス：60
Firepower 1120	Essentials ライセンス：512
Firepower 1140、1150	Essentials ライセンス：1024
Secure Firewall 1210、1220	Essentials ライセンス：1024
Secure Firewall 1230、1240、1250	Essentials ライセンス：1024
Cisco Secure Firewall 3100	Essentials ライセンス：1024
Firepower 4100	Essentials ライセンス：1024
Cisco Secure Firewall 4200	Essentials ライセンス：1024
Firepower 9300	Essentials ライセンス：1024
ASA 仮想	スループット機能： 100 Mbps：25 1 Gbps：50 2 Gbps：200 10 Gbps：1024
ISA 3000	Essentials ライセンス: 5 Security Plus ライセンス：100

（注） VLAN 制限の対象としてカウントするインターフェイスに、VLAN を割り当てます。 たとえば、次のようになります。

```
interface gigabitethernet 0/0.100
  vlan 100
```

VLAN サブインターフェイスのガイドラインと制限事項

モデルのサポート

- Firepower 1010 および Cisco Secure Firewall 1210/1220：VLAN サブインターフェイスは、スイッチポートおよび VLAN インターフェイスではサポートされていません。
- ASA モデルでは、管理インターフェイスのサブインターフェイスを設定できません。サブインターフェイスのサポートについては、管理スロット/ポート インターフェイス （826 ページ）を参照してください。

その他のガイドライン

- 物理インターフェイス上のタグなしパケットの禁止：サブインターフェイスを使用する場合、物理インターフェイスでトラフィックを通過させないようにすることもよくあります。物理インターフェイスはタグのないパケットを通過させることができるためです。この特性は、アクティブな物理インターフェイスと EtherChannel リンクにも当てはまります。トラフィックがサブインターフェイスを通過するには、物理インターフェイスまたは EtherChannel インターフェイスがイネーブルになっている必要があるため、トラフィックが物理インターフェイスまたは EtherChannel インターフェイスを通過しないように、**nameif** コマンドを除外してください。物理インターフェイスまたは EtherChannel インターフェイスでタグのないパケットを通過させる場合は、通常どおり **amenameif** コマンドを設定できます。
- 同じ親インターフェイスのすべてのサブインターフェイスは、ブリッジグループメンバーかルーテッドインターフェイスのいずれかである必要があります。混在および一致はできません。
- ASA は Dynamic Trunking Protocol（DTP）をサポートしていないため、接続されているスイッチポートを無条件にトランキングするように設定する必要があります。
- 親インターフェイスの同じ Burned-In MAC Address を使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。一意の MAC アドレスを自動的に生成できます。MAC アドレスの自動割り当て （979 ページ）を参照してください。

（注） MAC アドレスを手動で割り当てる場合は、予期しない動作や停止を避けるために、同じ物理インターフェイス上のすべてのサブインターフェイスに MAC アドレスを割り当てるようにしてください。

VLAN サブインターフェイスのデフォルト設定

この項では、工場出荷時のデフォルトコンフィギュレーションが設定されていない場合のインターフェイスのデフォルト設定を示します。

インターフェイスのデフォルトの状態

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

マルチ コンテキスト モードでは、システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。

シングルモードまたはシステム実行スペースでは、インターフェイスのデフォルトの状態は次のとおりです。

- 物理インターフェイス：ディセーブル。
- VLANサブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

VLAN サブインターフェイスと 802.1Q トランキングの設定

VLANサブインターフェイスを物理インターフェイスまたはEtherChannelインターフェイスに追加します。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

ステップ 1 新しいサブインターフェイスを指定します。

interface {*physical_interface* | **port-channel** *number*}.*subinterface*

例：

```
ciscoasa(config)# interface gigabitethernet 0/1.100
```

port-channel *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。

subinterface ID は、1 ～ 4294967293 の整数です。

ステップ 2 サブインターフェイスの VLAN を指定します。

vlan *vlan_id* [**secondary** *vlan_range*]

例：

```
ciscoasa(config-subif)# vlan 101 secondary 52 64,66-74
```

vlan_id は、1 ～ 4094 の整数です。VLAN ID には、接続されているスイッチで予約されているものがあります。詳細については、スイッチのマニュアルを参照してください。

セカンダリ VLAN は、（連続する範囲について）スペース、カンマ、およびダッシュで区切ることができます。ASA はセカンダリ VLAN でトラフィックを受信すると、そのトラフィックをプライマリ VLAN にマップします。

同じ VLAN を複数のサブインターフェイスに関連付けることはできません。VLAN を物理インターフェイスに割り当てることはできません。トラフィックがサブインターフェイスを通過するには、各サブインターフェイスに VLAN ID が必要となります。VLAN ID を変更するために **no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を指定して **vlan** コマンドを入力すると、ASA によって古い ID が変更されます。リストからいくつかのセカンダリ VLAN を削除するには、**no** コマンドを使用して削除する VLAN のみをリストすることができます。リストされた VLAN のみを選択的に削除できます。たとえば、範囲内の 1 つの VLAN を削除することはできません。

例

次に、一連のセカンダリ VLAN を VLAN 200 にマップする例を示します。

```
interface gigabitethernet 0/6.200
   vlan 200 secondary 500 503 600-700
```

次に、リストからセカンダリ VLAN 503 を削除する例を示します。

```
no vlan 200 secondary 503
show running-config interface gigabitethernet0/6.200
!
interface GigabitEthernet0/6.200
 vlan 200 secondary 500 600-700
 no nameif
 no security-level
 no ip address
```

関連トピック

VLAN サブインターフェイスのライセンス （888 ページ）

VLAN サブインターフェイスのモニタリング

次のコマンドを参照してください。

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show vlan mapping**

  マップされるインターフェイス、セカンダリ VLAN およびプライマリ VLAN を表示します。

VLAN のサブインターフェイスの例

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
interface gigabitethernet 0/1
  no nameif
  no security-level
  no ip address
  no shutdown
interface gigabitethernet 0/1.1
  vlan 101
  nameif inside
  security-level 100
  ip address 192.168.6.6 255.255.255.0
  no shutdown
```

次に、Catalyst 6500 でどのように VLAN マッピングが機能するのかを示します。ノードを PVLANS に接続する方法については、Catalyst 6500 の設定ガイドを参照してください。

```
ASA Configuration

interface GigabitEthernet1/1
  description Connected to Switch GigabitEthernet1/5
  no nameif
  no security-level
  no ip address
  no shutdown
!
interface GigabitEthernet1/1.70
  vlan 70 secondary 71 72
  nameif vlan_map1
  security-level 50
  ip address 10.11.1.2 255.255.255.0
```

```
  no shutdown
!
interface GigabitEthernet1/2
  nameif outside
  security-level 0
  ip address 172.16.171.31 255.255.255.0
  no shutdown
```

Catalyst 6500 Configuration

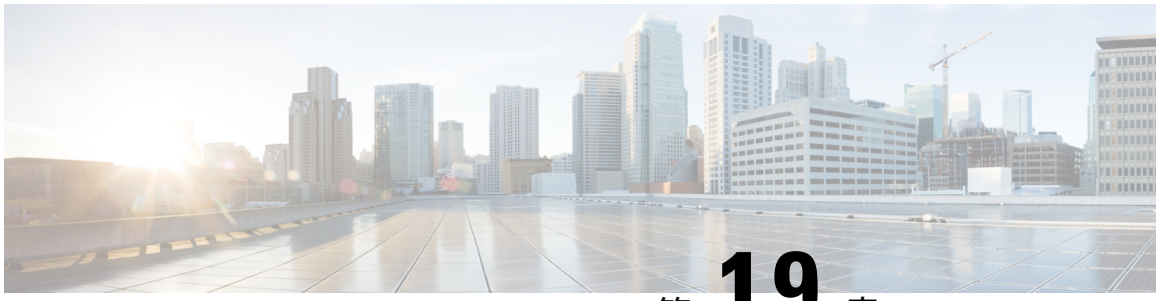
```
vlan 70
  private-vlan primary
  private-vlan association 71-72
!
vlan 71
  private-vlan community
!
vlan 72
  private-vlan isolated
!
interface GigabitEthernet1/5
  description Connected to ASA GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 70-72
  switchport mode trunk
!
```

VLAN サブインターフェイスの履歴

表 *30 : VLAN* サブインターフェイスの履歴

機能名	バージョン	機能情報
VLAN 数の増加	7.0(5)	次の制限値が増加されました。 • ASA 5510 基本ライセンスの VLAN 数が 0 から 10 に増えました。 • ASA 5510 Security Plus ライセンスの VLAN 数が 10 から 25 に増えました。 • ASA 5520 の VLAN 数が 25 から 100 に増えました。 • ASA 5540 の VLAN 数が 100 から 200 に増えました。
VLAN 数の増加	7.2(2)	VLAN の制限値が変更されました。ASA 5510 の基本ライセンスでは 10 から 50 に、Security Plus ライセンスでは 25 から 100 に、ASA 5520 では 100 から 150 に、ASA 5550 では 200 から 250 に増えています。
ASA 5580 の VLAN 数の増加	8.1(2)	ASA 5580 上でサポートされる VLAN 数が 100 から 250 に増加されました。

機能名	バージョン	機能情報
セカンダリ VLAN のプライマリ VLAN へのマッピングのサポート	9.5(2)	サブ インターフェイスで、1 つ以上のセカンダリ VLAN を設定できるようになりました。ASA はセカンダリ VLAN でトラフィックを受信すると、それをプライマリ VLAN にマップします。 次のコマンドを導入または変更しました。**vlan secondary**、**show vlan mapping**
ISA 3000 の VLAN 数の増加	9.13(1)	Security Plus ライセンスが有効な ISA 3000 について、最大 VLAN 数が 25 から 100 に増えました。



第 19 章

VXLAN インターフェイス

この章では、仮想拡張 LAN（VXLAN）インターフェイスを設定する方法について説明します。VXLAN は、レイヤ 2 ネットワークを拡張するためにレイヤ 3 物理ネットワーク上のレイヤ 2 仮想ネットワークとして機能します。

- VXLAN インターフェイスの概要 （895 ページ）
- VXLAN インターフェイスの要件と前提条件 （905 ページ）
- VXLAN インターフェイスのガイドライン （906 ページ）
- VXLAN インターフェイスのデフォルト設定 （907 ページ）
- VXLAN インターフェイスの設定 （907 ページ）
- Geneve インターフェイスの設定 （914 ページ）
- ゲートウェイロードバランサのヘルスチェックの許可 （917 ページ）
- VXLAN インターフェイスのモニタリング （919 ページ）
- VXLAN インターフェイスの例 （921 ページ）
- VXLAN インターフェイスの履歴 （926 ページ）

VXLAN インターフェイスの概要

VXLAN は、VLAN の場合と同じイーサネットレイヤ 2 ネットワークサービスを提供しますが、より優れた拡張性と柔軟性を備えています。VLAN と比較して、VXLAN には次の利点があります。

- データセンター全体でのマルチテナントセグメントの柔軟な配置。
- より多くのレイヤ 2 セグメント（最大 1600 万の VXLAN セグメント）に対応するための高度なスケーラビリティ。

ここでは、VXLAN の動作について説明します。VXLAN の詳細については、RFC 7348 を参照してください。Geneve の詳細については、RFC 8926 を参照してください。

カプセル化

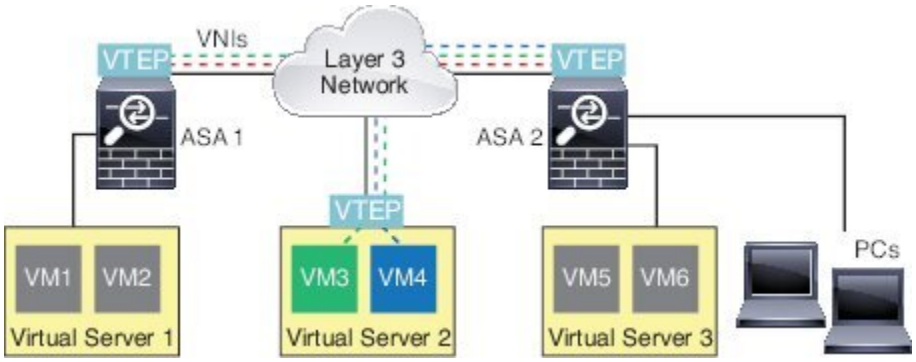
ASA は、次の 2 種類の VXLAN カプセル化をサポートしています。

- VXLAN（すべてのモデル）：VXLAN は、MAC Address-in-User Datagram Protocol（MAC-in-UDP）のカプセル化を使用します。元のレイヤ 2 フレームに VXLAN ヘッダーが追加され、UDP-IP パケットに置かれます。
- Geneve（ASA 仮想 のみ）：Geneve には、MAC アドレスに限定されない柔軟な内部ヘッダーがあります。Geneve カプセル化は、Amazon Web Services（AWS）ゲートウェイロードバランサとアプライアンス間のパケットの透過的なルーティング、および追加情報の送信に必要です。

VXLAN トンネル エンドポイント

VXLAN トンネルエンドポイント（VTEP）デバイスは、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP には 2 つのインターフェイス タイプ（セキュリティ ポリシーを適用する VXLAN Network Identifier（VNI）インターフェイスと呼ばれる 1 つ以上の仮想インターフェイスと、 VTEP 間に VNI をトンネリングする VTEP 送信元インターフェイスと呼ばれる通常のインターフェイス）があります。VTEP 送信元インターフェイスは、VTEP 間通信のトランスポート IP ネットワークに接続されます。

次の図に、レイヤ 3 ネットワークで VTEP として機能し、サイト間の VNI 1、2、3 を拡張する 2 つの ASA と仮想サーバ 2 を示します。ASA は、VXLAN と VXLAN 以外のネットワークの間のブリッジまたはゲートウェイとして機能します。



VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。カプセル化されたパケットは、発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてルーティングされます。VXLAN カプセル化の場合：宛先 IP アドレスは、リモート VTEP が不明な場合、マルチキャストグループにすることができます。Geneve では、ASA はスタティックピアのみをサポートします。デフォルトでは、 VXLAN の宛先ポートは UDP ポート 4789 です（ユーザ設定可能）。Geneve の宛先ポートは 6081 です。

VTEP 送信元インターフェイス

VTEP 送信元インターフェイスは、すべての VNI インターフェイスに関連付けられる予定の標準の ASA インターフェイス（物理、EtherChannel、または VLAN）です。ASA/セキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。設定できる VTEP

送信元インターフェイスは1つだけであるため、VXLANインターフェイスとGeneveインターフェイスの両方を同じデバイスに設定することはできません。AWS または Azure での ASA 仮想クラスタリングには例外があり、2 つの VTEP ソースインターフェイスを使用することができます。VXLANインターフェイスはクラスタ制御リンクに使用され、Geneve（AWS）またはVXLAN（Azure）インターフェイスはゲートウェイロードバランサに使用できます。

VTEP 送信元インターフェイスは、VXLAN トラフィック専用にすることができますが、その使用に制限されません。必要に応じて、インターフェイスを通常のトラフィックに使用し、そのトラフィックのインターフェイスにセキュリティポリシーを適用できます。ただし、VXLANトラフィックの場合は、すべてのセキュリティ ポリシーを VNI インターフェイスに適用する必要があります。VTEP インターフェイスは、物理ポートとしてのみ機能します。

トランスペアレントファイアウォールモードでは、VTEP送信元インターフェイスは、BVIの一部ではないため、そのIPアドレスを設定しません。このインターフェイスは、管理インターフェイスが処理される方法に似ています。

VNI インターフェイス

VNI インターフェイスは VLAN インターフェイスに似ています。VNI インターフェイスは、タギングを使用して特定の物理インターフェイスでのネットワーク トラフィックの分割を維持する仮想インターフェイスです。各VNI インターフェイスにセキュリティ ポリシーを直接適用します。

追加できる VTEP インターフェイスは 1 つだけで、すべての VNI インターフェイスは、同じ VTEP インターフェイスに関連付けられます。AWS または Azure での ASA Virtual クラスタリングには例外があります。AWS クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、Geneve インターフェイスは AWS ゲートウェイロードバランサに使用できます。Azure クラスタリングの場合、2 つの VTEP ソースインターフェイスを使用することができます。VXLAN インターフェイスはクラスタ制御リンクに使用され、2 つ目の VXLAN インターフェイスは Azure ゲートウェイロードバランサに使用できます。

VXLAN パケット処理

VXLAN

VTEP 送信元インターフェイスを出入りするトラフィックは、VXLAN 処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP送信元インターフェイスにより、VXLANヘッダーが含まれている内部MACフレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP がリモート VTEP IP ルックアップによって決定されます。

カプセル化解除については、次の場合に ASA によって VXLAN パケットのみがカプセル化解除されます。

- これが、宛先ポートが 4789 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- VXLAN パケット形式が標準に準拠します。

Geneve

VTEP送信元インターフェイスを出入りするトラフィックは、Geneve処理、特にカプセル化または非カプセル化の対象となります。

カプセル化処理には、次のタスクが含まれます。

- VTEP 送信元インターフェイスにより、Geneve ヘッダーが含まれている内部 MAC フレームがカプセル化されます。
- UDP チェックサム フィールドがゼロに設定されます。
- 外部フレームの送信元 IP がVTEP インターフェイスの IP に設定されます。
- 外部フレームの宛先 IP には、設定したピア IP アドレスが設定されます。

カプセル化解除については、次の場合にASAによってGeneveパケットのみがカプセル化解除されます。

- これが、宛先ポートが 6081 に設定された UDP パケットである場合（この値はユーザー設定可能です）。
- 入力インターフェイスが VTEP 送信元インターフェイスである場合。
- 入力インターフェイスの IP アドレスが宛先 IP アドレスと同じになります。
- Geneve パケット形式が標準に準拠します。

ピア VTEP

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA はVNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VXLAN ピア

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

  手動で複数のピアを定義することはできません。

  IPv4 の場合：ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンドノードの MAC アドレスを取得します。

  IPv6 の場合：ASA は IPv6 ネイバー要請メッセージを IPv6 要請ノード マルチキャスト アドレスに送信します。ピア VTEP は、そのリンクローカルアドレスを使用して IPv6 ネイバー アドバタイズメント メッセージで応答します。

- マルチキャスト グループは、VNI インターフェイスごとに（または VTEP 全体に）設定できます。

（注） このオプションは、Geneve ではサポートされていません。

  IPv4 の場合：ASA は、IP マルチキャストパケット内の VXLAN カプセル化 ARP ブロードキャストパケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

  IPv6 の場合：ASA は、VTEP 送信元インターフェイスを経由してマルチキャストリスナー検出（MLD）レポートメッセージを送信し、ASA が VTEP インターフェイスでマルチキャスト アドレス トラフィックをリッスンしていることを示します。

Geneve ピア

ASA 仮想 は、静的に定義されたピアのみをサポートします。AWS ゲートウェイロードバランサで ASA 仮想 ピアの IP アドレスを定義できます。ASA 仮想 はゲートウェイロードバランサへのトラフィックを開始しないため、ASA 仮想 でゲートウェイロードバランサの IP アドレスを指定する必要はありません。Geneve トラフィックを受信すると、ピア IP アドレスを学習します。マルチキャストグループは、Geneve ではサポートされていません。

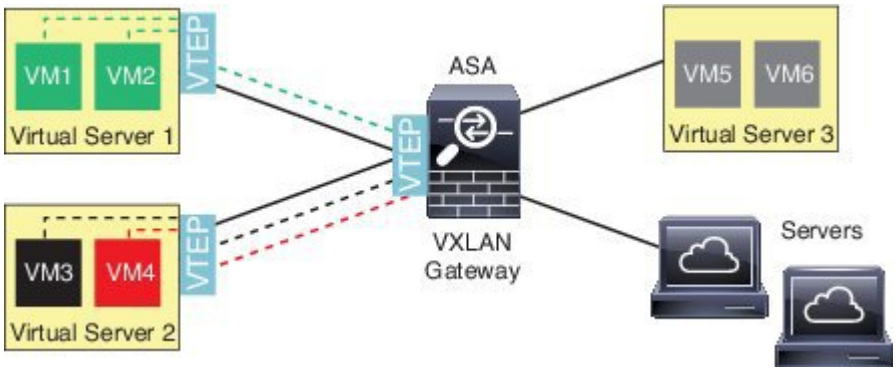
VXLAN 使用例

ここでは、ASA 上への VXLAN の実装事例について説明します。

VXLAN ブリッジまたはゲートウェイの概要

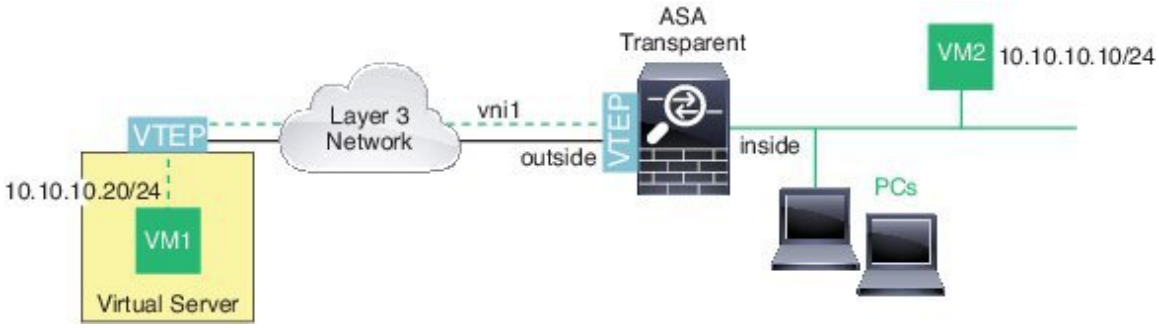
各 ASA の VTEP は、VM、サーバ、PC、VXLANのオーバーレイ ネットワークなどのエンドノード間のブリッジまたはゲートウェイとして機能します。VTEP 送信元インターフェイスを介して VXLAN カプセル化で受信した受信フレームの場合、ASA は VXLAN ヘッダーを除去して、内部イーサネット フレームの宛先 MAC アドレスに基づいて非 VXLAN ネットワークに接続されている物理インターフェイスに転送します。

ASA は、常に VXLAN パケットを処理します。つまり、他の 2 つの VTEP 間で VXLAN パケットをそのまま転送する訳ではありません。



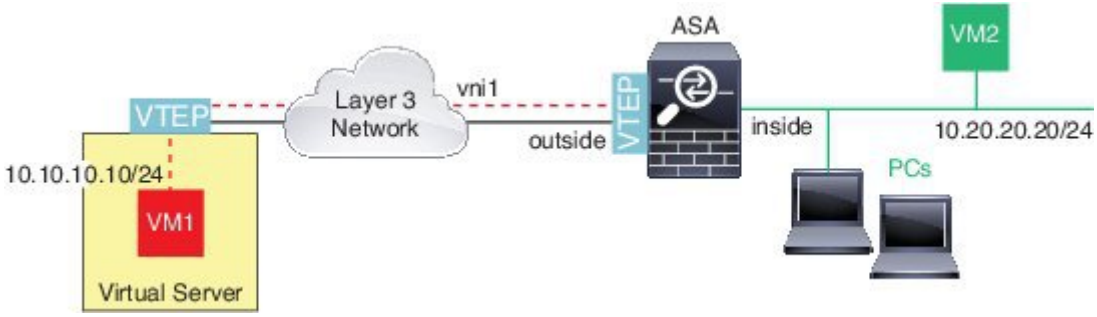
VXLAN ブリッジ

ブリッジグループ（トランスペアレント ファイアウォール モードまたは任意ルーテッドモード）を使用する場合、ASA は、同じネットワークに存在する（リモート）VXLAN セグメントとローカルセグメント間の VXLAN ブリッジとして機能できます。この場合、ブリッジグループのメンバーは通常インターフェイス 1 つのメンバーが通常のインターフェイスで、もう 1 つのメンバーが VNI インターフェイスです。



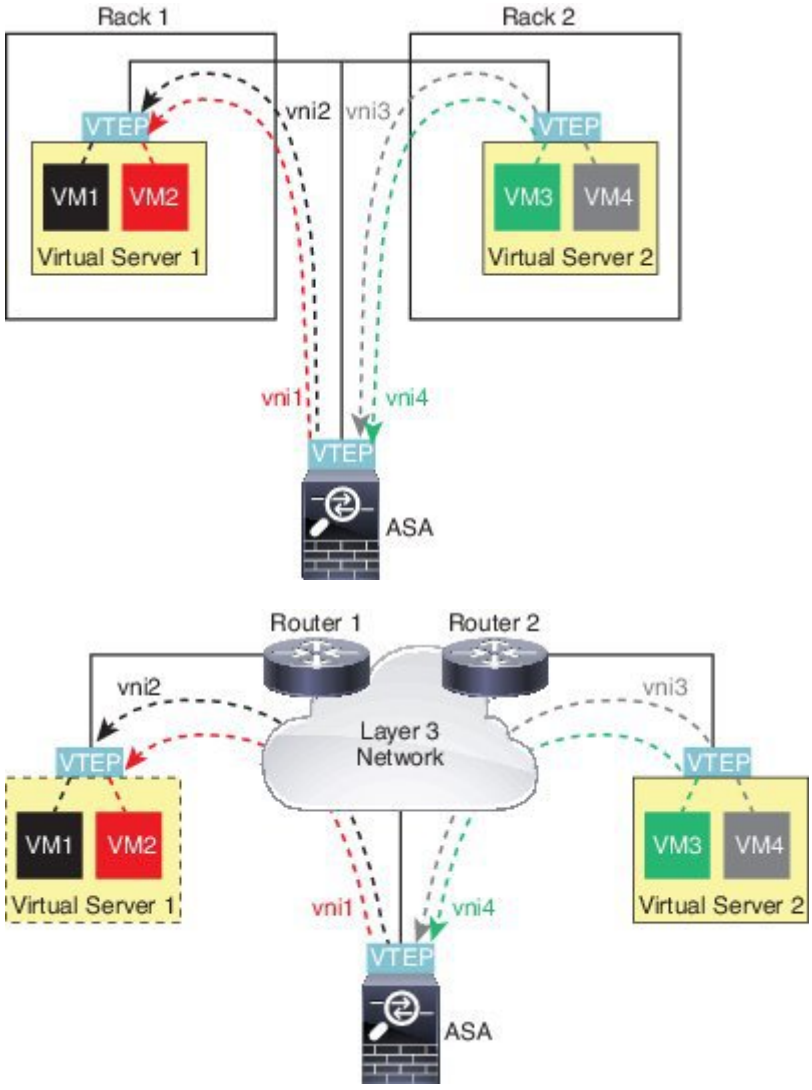
VXLAN ゲートウェイ（ルーテッド モード）

ASA は、VXLAN ドメインと非 VXLAN ドメイン間のルータとして機能し、異なるネットワーク上のデバイスを接続します。



VXLAN ドメイン間のルータ

VXLAN 拡張 レイヤ 2 ドメインを使用すると、VM は、ASA が同じラックにないとき、あるいは ASA がレイヤ 3 ネットワーク上の離れた場所にあるときにsのゲートウェイとして ASA を指し示すことができます。



このシナリオに関する次の注意事項を参照してください。

1. VM3 から VM1 へのパケットでは、ASA がデフォルトゲートウェイであるため、宛先 MAC アドレスは ASA の MAC アドレスです。
2. 仮想サーバー 2 の VTEP 送信元インターフェイスは、VM3 からパケットを受信してから、VNI 3 の VXLAN タグでパケットをカプセル化して ASA に送信します。
3. ASA は、パケットを受信すると、そのパケットをカプセル化解除して内部フレームを取得します。

4. ASA は、ルート ルックアップに内部フレームを使用して、宛先が VNI 2 上であることを認識します。VM1 のマッピングがまだない場合、ASA は、VNI 2 カプセル化された ARP ブロードキャストを VNI 2 のマルチキャスト グループ IP で送信します。

（注） このシナリオでは複数の VTEP ピアがあるため、ASA は、複数のダイナミック VTEP ピア ディスカバリを使用する必要があります。

5. ASA は、VNI 2 の VXLAN タグでパケットを再度カプセル化し、仮想サーバ 1 に送信します。カプセル化の前に、ASA は、内部フレームの宛先 MAC アドレスを変更して VM1 の MAC にします（ASA で VM1 の MAC アドレスを取得するためにマルチキャスト カプセル化 ARP が必要な場合があります）。

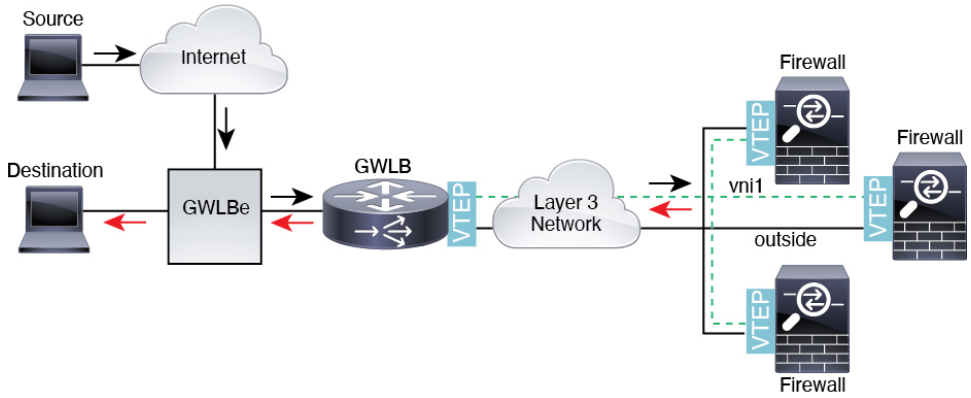
6. 仮想サーバー 1 は、VXLAN パケットを受信すると、パケットをカプセル化解除して内部フレームを VM1 に配信します。

AWS ゲートウェイロードバランサおよび Geneve シングルアームプロキシ

（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。ASA Virtual は、分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、ゲートウェイロードバランサのエンドポイントからゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の ASA Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、ゲートウェイロードバランサに送り返す（U ターントラフィック）前に検査します。ゲートウェイロードバランサは、トラフィックをゲートウェイロードバランサのエンドポイントと宛先に送り返します。

図 *72 : Geneve* シングルアームプロキシ



AWS ゲートウェイロードバランサおよび Geneve デュアルアームプロキシ

（注） この使用例は、現在サポートされている Geneve インターフェイスの唯一の使用例です。

ASA Virtual は、シングルアームまたはデュアルアームモードの分散データプレーン（ゲートウェイ ロード バランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。次の図は、GWLB および GWLB エンドポイントへのトラフィックホップを必要とせずに宛先（インターネット）に直接転送されるアウトバウンドトラフィック（ASA Virtual によって検査されるトラフィック）を示しています。 ASA Virtual はアウトバウンドを検査し、トラフィックの NAT を実行してから、トラフィックをドロップするか、NAT ゲートウェイを介してインターネットに送り返します。デュアルアームプロキシは、マルチ VPC 展開に共通の出力パスを提供します。ファイアウォールは、複数の VPC からのアウトバウンドトラフィックを検査し、トラフィックは単一のポイントからインターネットに出るため、費用対効果の高いインフラストラクチャ ソリューションです。

図 *73 : Geneve* デュアルアームプロキシ：単一 *VPC* からの出力トラフィック

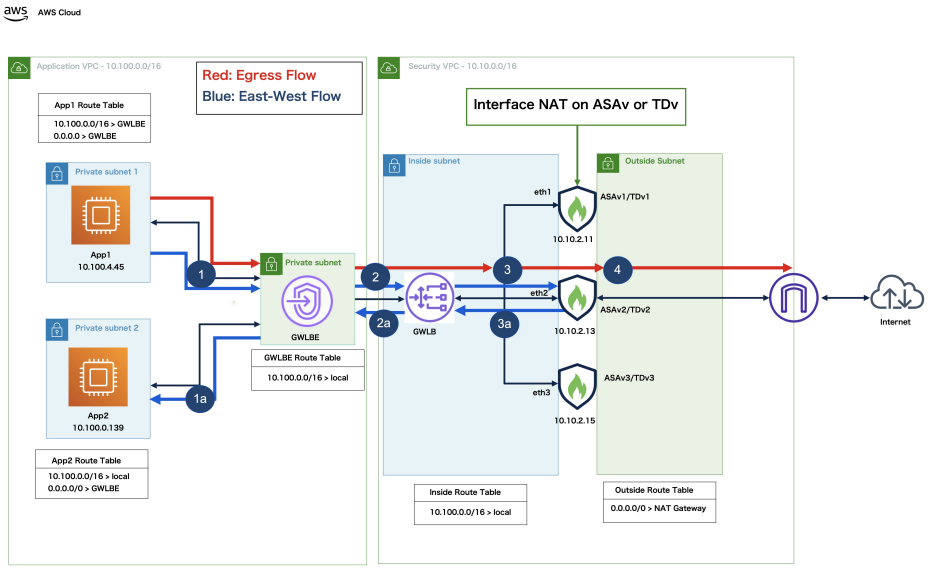
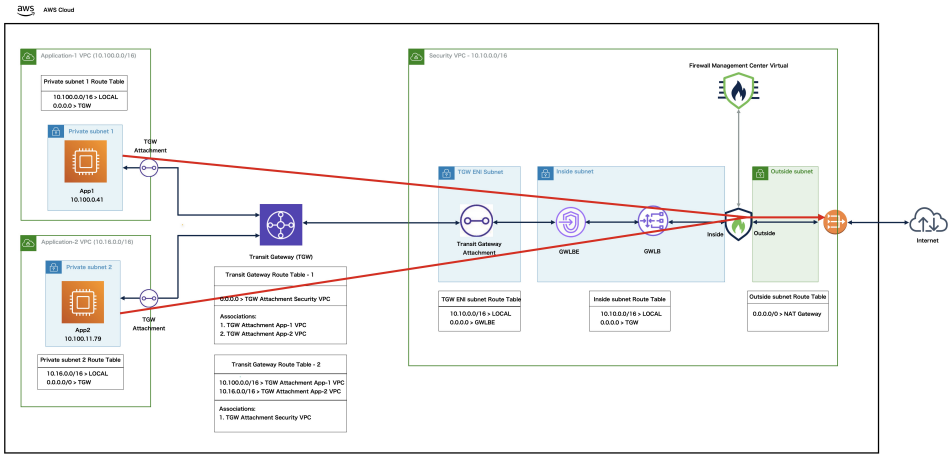


図 *74 : Geneve* デュアルアームプロキシ：複数の *VPC* からの出力トラフィック



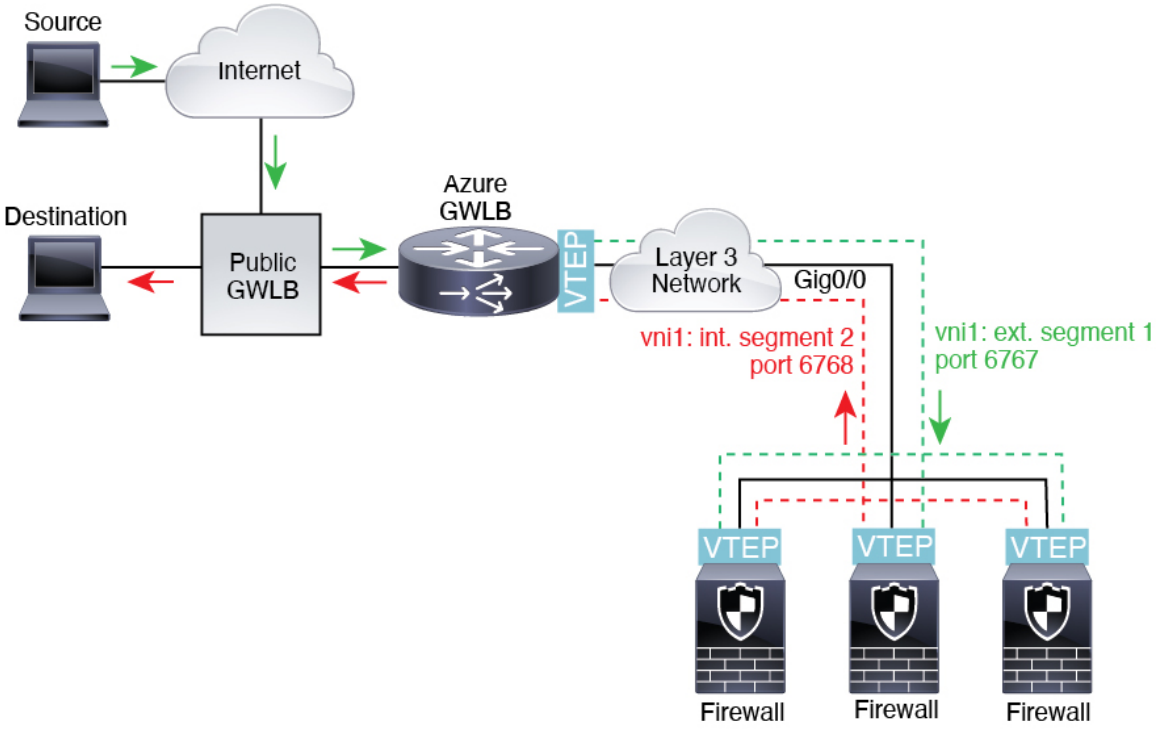
Azure ゲートウェイロードバランサおよびペアプロキシ

Azure サービスチェーンでは、ASA Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。ASA Virtual は、ペアリングされたプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

次の図は、外部 VXLAN セグメント上のパブリックゲートウェイロードバランサから Azure ゲートウェイロードバランサに転送されるトラフィックを示しています。ゲートウェイロードバランサは、複数の ASA Virtual の間でトラフィックのバランスをとり、トラフィックをドロップするか、外部 VXLAN セグメント上のゲートウェイロードバランサに送り返す前に検査しま

す。Azure ゲートウェイロードバランサは、トラフィックをパブリックゲートウェイロードバランサと宛先に送り返します。

図 *75* : ペアリングされたプロキシを使用した *Azure Gateway* ロードバランサ



VXLAN インターフェイスの要件と前提条件

モデルの要件

- Firepower 1010 および Cisco Secure Firewall 1210/1220：スイッチポートおよび VLAN インターフェイスは、VTEP インターフェイスとしてサポートされていません。
- Geneve カプセル化は、Amazon Web Services（AWS）の ASAv30、ASAv50、ASAv100 のモデルでサポートされています。
- ペアプロキシモードの VXLAN は、次のモデルでサポートされています。
  - Azure での ASA Virtual

VXLAN インターフェイスのガイドライン

ファイアウォール モード

- Geneve インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。
- ペアプロキシの VXLAN インターフェイスは、ルーテッド ファイアウォール モードでのみサポートされています。

IPv6

- VNI インターフェイスは、IPv4 と IPv6 の両方のトラフィックをサポートします。
- VXLAN カプセル化の場合、VTEP 送信元インターフェイスは IPv4 と IPv6 の両方をサポートします。ASA 仮想 クラスタ制御リンクの VTEP 送信元インターフェイスは、IPv4 のみをサポートします。

  Geneve の場合、VTEP 送信元インターフェイスは IPv4 のみをサポートします。

クラスタリングとマルチコンテキストモード

- ASA クラスタリングは、クラスタ制御リンク（ASA 仮想 のみ）を除いて、個別インターフェイスモードの VXLAN をサポートしません。スパンド EtherChannel モードでのみ VXLAN をサポートしています。

  GWLB で使用する追加の Geneve インターフェイスを使用できる AWS の ASA 仮想 と、GWLB で使用する追加のペアプロキシの VXLAN インターフェイスを使用できる Azure の場合は例外です。

- Geneve インターフェイスは、のシングルコンテキストモードでのみサポートされます。マルチコンテキストモードではサポートされません。

Routing

- VNI インターフェイスでは、スタティック ルーティングまたはポリシー ベース ルーティングのみをサポートします。ダイナミック ルーティング プロトコルはサポートされません。

VPN

VPN に VTEP 送信元インターフェイスを設定したり、VTI として使用したりすることはできません。

MTU

- VXLAN カプセル化：送信元インターフェイスの MTU が 1554 バイト未満（IPv4 の場合）または 1574 バイト未満（IPv6 の場合）の場合、ASA は自動的に MTU を増やします。この場合、イーサネットデータグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きなMTUが必要になります。他のデバイスが使用するMTUの方が大きい場合、送信元インターフェイス MTU を、ネットワーク MTU＋54 バイト（IPv4 の場合）または＋64 バイト（IPv6 の場合）に設定する必要があります。この MTU は、一部のフレームでジャンボ フレーム予約を有効にする必要があります。ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000） （833 ページ） を参照してください。
- Geneve カプセル化：送信元インターフェイスの MTU が 1806 バイト未満の場合、ASA は自動的に MTU を 1806 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。他のデバイスが使用するMTUの方が大きい場合、送信元インターフェイスMTUを、ネットワークMTU+306バイトに設定する必要があります。このMTUは、一部のフレームでジャンボ フレーム予約を有効にする必要があります。ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000） （833 ページ） を参照してください。

VXLAN インターフェイスのデフォルト設定

デフォルトでは、VNI インターフェイスはイネーブルになっています。

VXLAN インターフェイスの設定

VXLAN を設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます（ASA 仮想 のみ）。Geneve インターフェイスについては、Geneve インターフェイスの設定 （914 ページ）を参照してください。

手順

ステップ 1 VTEP 送信元インターフェイスの設定 （908 ページ）を使用して無効にすることができます。
ステップ 2 VNI インターフェイスの設定 （910 ページ）
ステップ 3 「（オプション）VXLAN UDP ポートの変更 （913 ページ）」を参照してください。
ステップ 4 （Azure GWLB）ゲートウェイロードバランサのヘルスチェックの許可 （917 ページ）。

VTEP 送信元インターフェイスの設定

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。Azure のASA 仮想 でのクラスタリングには例外があり、1 つの VTEP ソースインターフェイスをクラスタ制御リンクに使用し、2 つ目のソースインターフェイスを Azure GWLB に接続されたデータインターフェイスに使用できます。

始める前に

マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。設定したいコンテキストを変更するには、**changeto context***name* コマンドを入力します。

手順

ステップ 1 （トランスペアレント モード）送信元インターフェイスが NVE 専用であることを指定します。

interface *id*

nve-only

例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

この設定により、インターフェイスの IP アドレスを設定することができます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されるルーテッド モードではオプションです。

ステップ 2 送信元インターフェイス名と IPv4 および/または IPv6 アドレスを設定します。

ASA 仮想 クラスタ制御リンクは IPv6 をサポートしません。

例：

（ルーテッド モード）

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64
```

例：

（トランスペアレント モード）

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

```
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64
```

ステップ 3 NVE インスタンスを指定します。

nve 1

ID 1 で NVE インスタンスを 1 つだけ指定できます。

例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

ステップ 4 VXLAN カプセル化を指定します。

encapsulation vxlan

例：

```
ciscoasa(cfg-nve)# encapsulation vxlan
```

ステップ 5 ステップ 2 で設定した送信元インターフェイス名を指定します。

source-interface *interface-name*

例：

```
ciscoasa(cfg-nve)# source-interface outside
```

（注）
VTEP インターフェイスの MTU が 1554 バイト（IPv4 の場合）または 1574 バイト（IPv6 の場合）未満の場合、ASA は自動的に MTU を 1554 バイトまたは 1574 バイトに増やします。

ステップ 6 （マルチ コンテキスト モード（シングル モードではオプション）手動でピア VTEP の IP アドレスを指定します。

peer ip *ip_address*

例：

IPv4 ピア

```
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

例：

IPv6 ピア：

```
ciscoasa(cfg-nve)# peer ip 2001:0DB8:BA98::1234
```

ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

ステップ 7 （オプション、シングル モードのみ）関連付けられたすべての VNI インターフェイスにデフォルトのマルチキャスト グループを指定します。

default-mcast-group *mcast_ip*

例：

IPv4 グループ

```
ciscoasa(cfg-nve)# default-mcast-group 236.0.0.100
```

例：

IPv6 グループ

```
ciscoasa(cfg-nve)# default-mcast-group ff0e::100
```

VNI インターフェイスごとにマルチキャスト グループを設定していない場合は、このグループが使用されます。その VNI インターフェイス レベルでグループを設定している場合は、そのグループがこの設定よりも優先されます。

VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

Azure の ASA virtual の場合、通常の VXLAN インターフェイスを設定するか、Azure GWLB で使用するペアプロキシモードの VXLAN インターフェイスを設定できます。ペアプロキシモードは、クラスタリングでサポートされる唯一のモードです。

手順

ステップ 1 VNI インターフェイスを作成します。

interface vni *vni_num*

例：

```
ciscoasa(config)# interface vni 1
```

1 ～ 10000 の範囲で ID を設定します。この ID は内部インターフェイス識別子です。

ステップ 2 （通常の VXLAN）VXLAN セグメント ID を指定します。

segment-id *id*

例：

```
ciscoasa(config-if)# segment-id 1000
```

1 ～ 16777215 の範囲で ID を設定します。セグメント ID は VXLAN タギングに使用されます。

ステップ 3 （Azure GWLB のペアプロキシ VXLAN）プロキシペアモードを有効にして、必要なパラメータを設定します。

a) プロキシペアモードを有効にします。

proxy paired

例：

```
ciscoasa(config-if)# proxy paired
```

b) 内部ポートを設定します。

internal-port *port_number*

port_number は *1024* ～ *65535* です。

例：

```
ciscoasa(config-if)# internal-port 2000
```

c) 内部セグメント ID を設定します。

internal-segment-id *id_number*

id_number は 1 ～ 16777215 です。

例：

```
ciscoasa(config-if)# internal-segment-id 101
```

d) 外部ポートを設定します。

external-port *port_number*

port_number は *1024* ～ *65535* です。

例：

```
ciscoasa(config-if)# external-port 2001
```

e) 外部セグメント ID を設定します。

external-segment-id *id_number*

id_number は 1 ～ 16777215 です。

例：

```
ciscoasa(config-if)# external-segment-id 102
```

f) トラフィックが同じインターフェイスに出入りすることを許可します。

same-security-traffic permit intra-interface

例：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

ステップ 4 （トランスペアレント モードの場合は必須）このインターフェイスを関連付けるブリッジ グループを指定します。

bridge-group *number*

例：

```
ciscoasa(config-if)# bridge-group 1
```

BVIインターフェイスを設定して通常のインターフェイスをこのブリッジグループに関連付けるには、ブリッジグループ インターフェイスの設定 （937 ページ）を参照してください。

ステップ 5 このインターフェイスを VTEP 送信元インターフェイスに関連付けます。

vtep-nve 1

ステップ 6 インターフェイスの名前を指定します。

nameif *vni_interface_name*

例：

```
ciscoasa(config-if)# nameif vxlan1000
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 7 （ルーテッド モード）IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てます。

ip address {*ip_address* [*mask*] [**standby** *ip_address*] | **dhcp** [**setroute**] | **pppoe** [**setroute**]}

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address*]}

例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

ステップ 8 セキュリティ レベルを設定します。

security-level *level*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

ステップ 9 （シングル モード）マルチキャスト グループ アドレスを設定します。

mcast-group *multicast_ip*

例：

IPv4 グループ：

```
ciscoasa(config-if)# mcast-group 236.0.0.100
```

例：

IPv6 グループ：

```
ciscoasa(config-if)# mcast-group ff0e::101
```

VNI インターフェイスに対してマルチキャスト グループを設定しない場合は、VTEP 送信元インターフェイス設定のデフォルト グループが使用されます（使用可能な場合）。VTEP 送信元インターフェイスに対して手動でVTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャスト グループを指定することはできません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

（オプション）VXLAN UDP ポートの変更

デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。ネットワークで標準以外のポートを使用する場合は、それを変更できます。

始める前に

マルチ コンテキスト モードでは、システム実行スペースで次のタスクを実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

VXLAN UDP ポートを設定します。

vxlan *port number*

例：

```
ciscoasa(config)# vxlan port 5678
```

Geneve インターフェイスの設定

ASA 仮想 の Geneve インターフェイスを設定するには、次の手順を実行します。

（注） VXLAN または Geneve を設定できます。VXLAN インターフェイスについては、VXLAN インターフェイスの設定 （907 ページ）を参照してください。

手順

ステップ 1 Geneve の VTEP 送信元インターフェイスの設定 （914 ページ）。

ステップ 2 Geneve の VNI インターフェイスの設定 （915 ページ）

ステップ 3 ゲートウェイロードバランサのヘルスチェックの許可 （917 ページ）。

Geneve の VTEP 送信元インターフェイスの設定

ASA 仮想 ごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。

手順

ステップ 1 （任意） 送信元インターフェイスが NVE 専用であることを指定します。

interface *id*

nve-only

例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
```

この設定によって、トラフィックがこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されます。

ステップ 2 送信元インターフェイス名と IPv4 アドレスを設定します。

例：

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

ステップ 3 NVE インスタンスを指定します。

nve 1

ID 1 で NVE インスタンスを 1 つだけ指定できます。

例：

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)#
```

ステップ 4 Geneve カプセル化を指定します。

encapsulation geneve

[Geneveポート（Geneve Port）] は変更しないでください。AWS にはポート 6081 が必要です。

例：

```
ciscoasa(cfg-nve)# encapsulation geneve
```

ステップ 5 ステップ 2 で設定した送信元インターフェイス名を指定します。

source-interface *interface-name*

例：

```
ciscoasa(cfg-nve)# source-interface outside
```

（注）
送信元インターフェイスの MTU が 1806 バイト未満の場合、ASA は自動的に MTU を 1806 バイトに増やします。

Geneve の VNI インターフェイスの設定

VNI インターフェイスを追加してそれを VTEP 送信元インターフェイスに関連付けて、基本インターフェイス パラメータを設定します。

手順

ステップ 1 VNI インターフェイスを作成します。

interface vni *vni_num*

例：

```
ciscoasa(config)# interface vni 1
```

1 ～ 10000 の範囲で ID を設定します。この ID は内部インターフェイス識別子です。

ステップ 2 このインターフェイスを VTEP 送信元インターフェイスに関連付けます。

vtep-nve 1

ステップ 3 インターフェイスの名前を指定します。

nameif *vni_interface_name*

例：

```
ciscoasa(config-if)# nameif geneve1000
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 4 IPv4 アドレスと IPv6 アドレスの一方または両方を割り当てます。

ip address {*ip_address* [*mask*] [**standby** *ip_address*]}

ipv6 address {**autoconfig** | *ipv6-address*/*prefix-length* [**standby** *ipv6-address*]}

Geneve は静的 IP アドレスのみをサポートします。

例：

```
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

ステップ 5 セキュリティ レベルを設定します。

security-level *level*

level には、0（最下位）～ 100（最上位）の整数を指定します。

例：

```
ciscoasa(config-if)# security-level 50
```

ステップ 6 シングルアームプロキシまたはを有効にします。

proxy single-arm

例：

```
ciscoasa(config-if)# proxy single-arm
```

proxy dual-arm

例：

```
ciscoasa(config-if)# proxy single-arm | dual-arm
```

それぞれの説明は次のとおりです。

プロキシ は、実行するモード VNI インターフェイスを指定するキーワードです。

single-arm または dual-arm は、AWS シングルアームまたはデュアルアーム展開モードを指定するキーワードです。

ステップ 7 トラフィックが同じインターフェイスに出入りすることを許可します。

same-security-traffic permit intra-interface

例：

```
ciscoasa(config)# same-security-traffic permit intra-interface
```

ゲートウェイロードバランサのヘルスチェックの許可

AWS または Azure ゲートウェイロードバランサでは、アプライアンスがヘルスチェックに正しく応答する必要があります。AWS ゲートウェイロードバランサは、正常と見なされるアプライアンスにのみトラフィックを送信します。

SSH、Telnet、HTTP、または HTTPS のヘルスチェックに応答するように ASA 仮想 を設定する必要があります。

SSH 接続

SSH の場合、ゲートウェイロードバランサからの SSH を許可します。ゲートウェイロードバランサは、ASA 仮想 への接続の確立を試行し、ログインの ASA 仮想 のプロンプトが正常性の証拠として取得されます。

（注） SSH ログインの試行は 1 分後にタイムアウトします。このタイムアウトに対応するには、ゲートウェイロードバランサでより長いヘルスチェック間隔を設定する必要があります。

例

```
! Allow SSH connections from GWLB network: 10.0.1.0/24
ssh 10.0.1.0 255.255.255.0 outside
```

Telnet 接続

Telnet の場合、ゲートウェイロードバランサからの Telnet を許可します。ゲートウェイロードバランサは、ASA 仮想 への接続の確立を試行し、ASA 仮想 のログインのプロンプトが正常性の証拠として取得されます。

（注） 最も低いセキュリティレベルのインターフェイスに Telnet で接続できないため、この方法は実用的ではありません。

例

```
! Allow Telnet connections from GWLB network: 10.0.1.0/24
telnet 10.0.1.0 255.255.255.0 outside
```

HTTP（S）カットスループロキシ

ゲートウェイロードバランサに HTTP（S）ログインを要求するように ASA を設定できます。

例

```
! Identify health probe HTTP traffic from GWLB nw 10.0.1.0/24 to ASAv interface 10.2.2.2
access-list gwlb extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.2 eq www
! Enable HTTP authentication
aaa authentication http console LOCAL
! Require authentication for the health probe traffic
aaa authentication match gwlb outside LOCAL
! Use an HTTP login page on the ASA
aaa authentication listener http outside port www
```

ポート変換を設定したスタティック インターフェイス NAT を使用した HTTP（S）リダイレクト

ヘルスチェックをメタデータ HTTP(S) サーバーにリダイレクトするように ASA 仮想 を設定できます。HTTP（S）ヘルスチェックの場合、HTTP（S）サーバは 200 ー 399 の範囲のステータスコードでゲートウェイロードバランサに応答する必要があります。ASA 仮想 では同時管理接続の数に制限があるため、ヘルスチェックを外部サーバーにオフロードすることもできます。

ポート変換を設定したスタティック インターフェイス NAT を使用すると、ポート（ポート 80 など）への接続を別の IP アドレスにリダイレクトできます。たとえば、ASA 仮想 外部インターフェイスの宛先を持つゲートウェイロードバランサからの HTTP パケットを、HTTP サーバーの宛先を持つ ASA 仮想 外部インターフェイスからのように変換します。次に ASA 仮想 はパケットをマッピングされた宛先アドレスに転送します。HTTP サーバーは ASA 仮想 外部インターフェイスに応答し、ASA 仮想 はゲートウェイロードバランサに応答を転送します。ゲートウェイロードバランサから HTTP サーバへのトラフィックを許可するアクセスルールが必要です。

例

```
! Permit HTTP traffic from GWLB nw 10.0.1.0/24 to HTTP server 10.2.2.3
access-list gwlb-health extended permit tcp 10.0.1.0 255.255.255.0 host 10.2.2.3 eq www
access-group gwlb-health in interface outside

! Create network objects
object network gwlb-subnet
 subnet 10.0.1.0 255.255.255.0
object-group network gwlb
    network-object object gwlb-subnet
object-group network http-server
    network-object host 10.2.2.3
object service http80
    service tcp destination eq www

! For HTTP, translate src GWLB IP to outside IP; translate dest of outside IP to HTTP
Server IP
nat (outside,outside) source static gwlb interface destination static interface http-server
 service http80 http80
```

VXLAN インターフェイスのモニタリング

VTEPインターフェイスおよびVNIインターフェイスをモニターするには、次のコマンドを参照してください。

- **show nve** [*id*] [**summary**]

  このコマンドは、NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。**summary** オプションを指定すると、このコマンドは、the status of the NVE インターフェイスのステータス、NVE インターフェイスの背後にある VNI の数、 検出された VTEP の数を表示します。

  show nve 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1
ciscoasa(config-if)# show nve
nve 1, source-interface "inside" is up
IP address 15.1.2.1, subnet mask 255.255.255.0
Encapsulation: vxlan
Encapsulated traffic statistics:
6701004 packets input, 3196266002 bytes
6700897 packets output, 3437418084 bytes
1 packets dropped
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Discovered peer VTEPs:
IP address 15.1.2.3
Number of VNIs attached to nve 1: 2
VNIs attached:
vni 2: segment-id 5002, mcast-group 239.1.2.3
vni 1: segment-id 5001, mcast-group 239.1.2.3
```

  show nve 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show nve 1 summary
nve 1, source-interface "inside" is up
Encapsulation: vxlan
Number of configured static peer VTEPs: 0
Number of discovered peer VTEPs: 1
Default multicast group: 239.1.2.3
Number of VNIs attached to nve 1: 2
```

- **show interface vni** *id* [**summary**]

  このコマンドは、VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。**summary** オプションを指定すると、VNI インターフェイスのパラメータのみが表示されます。

  show interface vni 1 コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group 239.1.3.3
Traffic Statistics for "vni-inside":
235 packets input, 23606 bytes
524 packets output, 32364 bytes
14 packets dropped
1 minute input rate 0 pkts/sec, 0 bytes/sec
1 minute output rate 0 pkts/sec, 2 bytes/sec
1 minute drop rate, 0 pkts/sec
5 minute input rate 0 pkts/sec, 0 bytes/sec
5 minute output rate 0 pkts/sec, 0 bytes/sec
5 minute drop rate, 0 pkts/sec
```

  show interface vni 1 summary コマンドについては、次の出力を参照してください。

```
ciscoasa# show interface vni 1 summary
Interface vni1 "vni-inside", is up, line protocol is up
VTEP-NVE 1
Segment-id 5001
Tag-switching: disabled
MTU: 1500
MAC: aaaa.bbbb.1234
IP address 192.168.0.1, subnet mask 255.255.255.0
Multicast group not configured
```

- **show vni vlan-mapping**

  このコマンドは、VNIセグメントIDと、VLANインターフェイスまたは物理インターフェイス間のマッピングを表示します。このコマンドは、ルーテッドモードでは、VXLANとVLAN間ののマッピングに表示する値を大量に含めることができるため、トランスペアレント ファイアウォール モードでのみ有効です。

show vni vlan-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show vni vlan-mapping
vni1: segment-id: 6000, interface: 'g0110', vlan 10, interface: 'g0111', vlan 11
vni2: segment_id: 5000, interface: 'g01100', vlan 1, interface: 'g111', vlan 3,
interface: 'g112', vlan 4
```

- **show arp vtep-mapping**

  このコマンドは、リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。

  show arp vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show arp vtep-mapping
vni-outside 192.168.1.4 0012.0100.0003 577 15.1.2.3
vni-inside 192.168.0.4 0014.0100.0003 577 15.1.2.3
```

- **show mac-address-table vtep-mapping**

  このコマンドは、リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレス テーブル）を表示します。

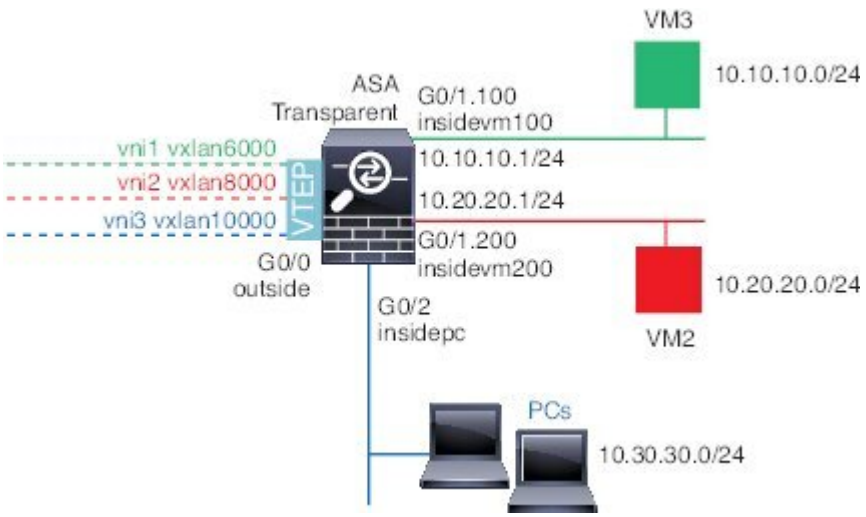
  show mac-address-table vtep-mapping コマンドについては、次の出力を参照してください。

```
ciscoasa# show mac-address-table vtep-mapping
interface                  mac  address       type     Age(min)   bridge-group
VTEP
-------------------------------------------------------------------------------------------
vni-outside                00ff.9200.0000      dynamic      5         1
10.9.1.3
vni-inside                0041.9f00.0000      dynamic      5         1      10.9.1.3
```

VXLAN インターフェイスの例

次の VXLAN の設定例を参照してください。

トランスペアレント VXLAN ゲートウェイの例



この例の次の説明を参照してください。

- GigabitEthernet 0/0 の外部インターフェイスは、VTEP 送信元インターフェイスとして使用され、レイヤ 3 ネットワークに接続されます。
- GigabitEthernet 0/1.100 の insidevm100 VLAN サブインターフェイスは、VM3 が存在する 10.10.10.0/24 ネットワークに接続されます。VM3 が VM1 と通信する場合（表示されません。両方とも、10.10.10.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 6000 を使用します。
- GigabitEthernet 0/1.200 の insidevm200 VLAN サブインターフェイスは、VM2 が存在する 10.20.20.0/24 ネットワークに接続されます。VM2 が VM4 と通信する場合（表示されません。両方とも、10.20.20.0/24 の IP アドレスを持つ）、ASA は VXLAN タグ 8000 を使用します。
- GigabitEthernet 0/2 の insidepc インターフェイスは、数台の PC が存在する 10.30.30.0/24 ネットワークに接続されます。それらの PC が、同じネットワーク（すべて 10.30.30.0/24 の IP アドレスを持つ）に属するリモート VTEP の裏の VMs/PCs（表示されません）と通信する場合、ASA は VXLAN タグ 10000 を使用します。

ASA の設定

```
firewall transparent
vxlan port 8427
!
interface gigabitethernet0/0
  nve-only
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
```

```
  source-interface outside
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  bridge-group 1
  vtep-nve 1
  mcast-group 235.0.0.100
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  bridge-group 2
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface vni3
  segment-id 10000
  nameif vxlan10000
  security-level 0
  bridge-group 3
  vtep-nve 1
  mcast-group 236.0.0.100
!
interface gigabitethernet0/1.100
  nameif insidevm100
  security-level 100
  bridge-group 1
!
interface gigabitethernet0/1.200
  nameif insidevm200
  security-level 100
  bridge-group 2
!
interface gigabitethernet0/2
  nameif insidepc
  security-level 100
  bridge-group 3
!
interface bvi 1
  ip address 10.10.10.1 255.255.255.0
!
interface bvi 2
  ip address 10.20.20.1 255.255.255.0
!
interface bvi 3
  ip address 10.30.30.1 255.255.255.0
```

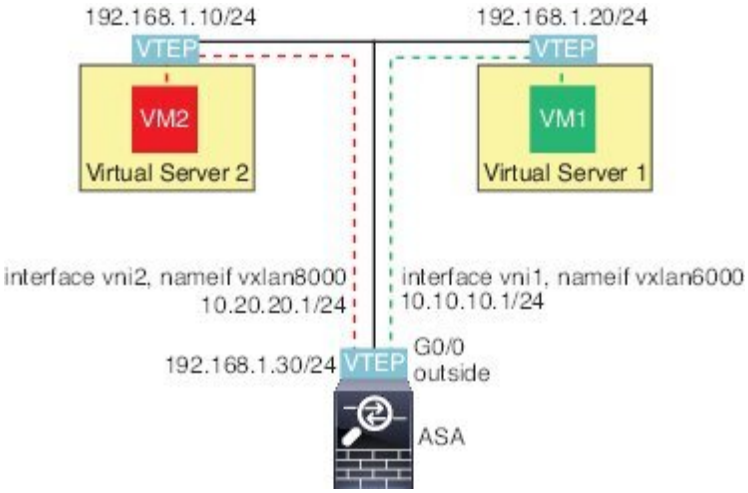
注意

- VNI インタフェース vni1 と vni2 の場合、カプセル化時に内部 VLAN タグが削除されます。
- VNI インターフェイス vni2 と vni3 は、マルチキャストでカプセル化された ARP に対して同じマルチキャスト IP アドレスを共有します。この共有は許可されます。
- ASA は、上記の BVI とブリッジグループ設定に基づいて VXLAN トラフィックを非 VXLAN でサポートされているインターフェイスにブリッジします。拡張されたレイヤ 2 ネット

ワークの各セグメント（10.10.10.0/24、10.20.20.0/24、10.30.30.0/24）の場合、ASA はブリッジとして機能します。

- 複数の VNI または複数の通常のインターフェイス（VLAN または単に物理インターフェイス）をブリッジ グループに設定できます。VXLAN セグメント ID から VLAN ID（物理インターフェイス） の転送または関連付けは、宛先 MAC アドレスによって決定され、どちらかのインターフェイスが宛先に接続されます。
- VTEP 送信元インターフェイスは、インターフェイス設定で **nve-only** によって示されるトランスペアレント ファイアウォール モードのレイヤ 3 インターフェイスです。VTEP 送信元インターフェイスは、BVI インターフェイスまたは管理インターフェイスではありませんが、IP アドレスがあり、ルーティング テーブルを使用します。

VXLAN ルーティングの例



この例の次の説明を参照してください。

- VM1（10.10.10.10）は仮想サーバー 1 にホストされ、VM2（10.20.20.20）は仮想サーバー 2 にホストされます。
- VM1 のデフォルト ゲートウェイは ASA であり、仮想サーバー 1 と同じのポッドにありませんが、VM1 はそれを認識しません。VM1 は、そのデフォルト ゲートウェイの IP アドレスが 10.10.10.1 であることだけを認識します。同様に、VM2 はデフォルト ゲートウェイの IP アドレスが10.20.20.1 であることだけを認識します。
- 仮想サーバー 1 および 2 の VTEP サポート型ハイパーバイザは、同じサブネットまたはレイヤ 3 ネットワーク（表示なし。この場合、ASA と仮想サーバーのアップリンクに異なるネットワーク アドレスがある）経由で ASA と通信できます。
- VM1 のパケットは、そのハイパーバイザの VTEP によってカプセル化され、VXLAN トンネリングを使用してそのデフォルト ゲートウェイに送信されます。

- VM1 がパケットを VM2 に送信すると、パケットはその観点からデフォルト ゲートウェイ 10.10.10.1 を介して送信されます。仮想サーバー 1 は 10.10.10.1 がローカルにないことを認識しているので、VTEP は VXLAN 経由でパケットをカプセル化し、ASA の VTEP に送信します。
- ASA で、パケットはカプセル化解除されます。VXLAN セグメント ID は、カプセル化解除時に取得されます。次に、ASA は、VXLAN セグメント ID に基づいて、VNI インターフェイス（vni1）に対応する内部フレームを再投入します。その後に、ASA はルート ルックアップを実行し、別の VNI インターフェイス（vni2）経由で内部パケットを送信します。vni2 を経由するすべての出力パケットは、VXLAN セグメント 8000 でカプセル化され、VTEP 経由で外部に送信されます。
- 最後に、カプセル化されたパケットが仮想サーバー 2 の VTEP によって受信され、カプセル化解除され、VM2 に転送されます。

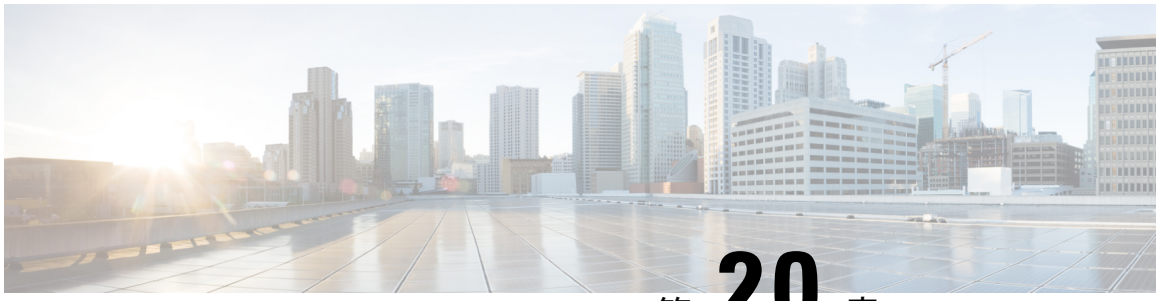
ASA の設定

```
interface gigabitethernet0/0
  nameif outside
  ip address 192.168.1.30 255.255.255.0
  no shutdown
!
nve 1
  encapsulation vxlan
  source-interface outside
  default-mcast-group 235.0.0.100
!
interface vni1
  segment-id 6000
  nameif vxlan6000
  security-level 0
  vtep-nve 1
  ip address 10.20.20.1 255.255.255.0
!
interface vni2
  segment-id 8000
  nameif vxlan8000
  security-level 0
  vtep-nve 1
  ip address 10.10.10.1 255.255.255.0
!
```

VXLAN インターフェイスの履歴

表 *31 : VXLAN* インターフェイスの履歴

機能名	リリース	機能情報
VXLAN VTEP IPv6 のサポート	9.20(1)	VXLAN VTEP インターフェイスに IPv6 アドレスを指定できるようになりました。IPv6 では、ASA 仮想 クラスタ制御リンクまたは Geneve カプセル化がサポートされていません。 新規/変更されたコマンド：**default-mcast-group**、**mcast-group**、**peer ip**
Azure ゲートウェイロードバランサーの ASA Virtual のペアプロキシ VXLAN	9.19(1)	Azure ゲートウェイ ロードバランサ（GWLB）で使用するために、Azure の ASA Virtual のペアプロキシモード VXLAN インターフェイスを構成できます。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。 新規/変更されたコマンド：**external-port**、**external-segment-id**、**internal-port**、**internal-segment-id**、**proxy paired**
AWS ゲートウェイロードバランサの AWS での ASA 仮想 の Geneve サポート	9.17(1)	AWS ゲートウェイロードバランサのシングルアームプロキシをサポートするために、ASAv30、ASAv50、および ASAv100 の Geneve カプセル化サポートが追加されました。 新規/変更されたコマンド：**debug geneve**、**debug nve**、**debug vxlan**、**encapsulation**、**packet-tracer geneve**、**proxy single-arm**、**show asp drop**、**show capture**、**show interface**、**show nve**、
VXLAN のサポート	9.4(1)	VXLAN のサポートが追加されました（VXLAN トンネル エンドポイント（VTEP）のサポートを含む）。ASA またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを定義できます。 次のコマンドが導入されました。**debug vxlan**、**default-mcast-group**、**encapsulation vxlan**、**inspect vxlan**、**interface vni**、**mcast-group**、**nve**、**nve-only**、**peer ip**、**segment-id**、**show arp vtep-mapping**、**show interface vni**、**show mac-address-table vtep-mapping**、**show nve**、**show vni vlan-mapping**、**source-interface**、**vtep-nve**、**vxlan port**



第 20 章

ルーテッド モードおよびトランスペアレント モードのインターフェイス

この章では、ルーテッドまたはトランスペアレント ファイアウォール モードですべてのモデルのインターフェイス設定を完了するためのタスクについて説明します。

（注） マルチ コンテキスト モードでは、この項のタスクをコンテキスト実行スペースで実行してください。設定したいコンテキストを変更するには、**changeto context***name* コマンドを入力します。

- ルーテッド モード インターフェイスとトランスペアレント モード インターフェイスについて （927 ページ）
- ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項 （930 ページ）
- ルーテッド モードのインターフェイスの設定 （932 ページ）
- ブリッジグループ インターフェイスの設定 （937 ページ）
- IPv6 アドレスの設定 （944 ページ）
- ルーテッド モードおよびトランスペアレント モードのインターフェイスのモニタリング （959 ページ）
- ルーテッド モードおよびトランスペアレント モードのインターフェイスの例 （964 ページ）
- ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴 （968 ページ）

ルーテッドモードインターフェイスとトランスペアレント モード インターフェイスについて

ASA は、ルーテッドおよびブリッジという 2 つのタイプのインターフェイスをサポートします。

各レイヤ 3 ルーテッド インターフェイスに、固有のサブネット上の IP アドレスが必要です。

ブリッジされたインターフェイスはブリッジ グループに属しており、すべてのインターフェイスは同じネットワーク上にあります。ブリッジ グループは、ブリッジ ネットワーク上の IP アドレスを持つブリッジ仮想インターフェイス（BVI）によって表わされます。ルーテッド モードは、ルーテッド インターフェイスとブリッジ インターフェイスの両方をサポートし、ルーテッド インターフェイスと BVI との間のルーティングが可能です。トランスペアレント ファイアウォール モードでは、ブリッジ グループと BVI インターフェイスのみがサポートされます。

セキュリティ レベル

ブリッジグループ メンバー インターフェイスを含む各インターフェイスには、0（最下位）～100（最上位）のセキュリティ レベルを設定する必要があります。たとえば、内部ホスト ネットワークなど、最もセキュアなネットワークにはレベル 100 を割り当てる必要があります。一方、インターネットなどに接続する外部ネットワークにはレベル 0 が割り当てられる場合があります。DMZ など、その他のネットワークはその中間に設定できます。複数のインターフェイスを同じセキュリティ レベルに割り当てることができます。

BVI にセキュリティ レベルを割り当てるかどうかは、ファイアウォール モードに応じて異なります。トランスペアレント モードでは、BVI インターフェイスはインターフェイス間のルーティングに参加しないため、BVI インターフェイスにはセキュリティ レベルが割り当てられていません。ルーテッド モードでは、BVI 間や他のインターフェイスとの間のルーティングを選択した場合、BVI インターフェイスはセキュリティ レベルを所有します。ルーテッド モードでは、ブリッジ グループ メンバー インターフェイスのセキュリティ レベルは、ブリッジ グループ内の通信にのみ適用されます。同様に、BVI のセキュリティ レベルは、BVI/レイヤ 3 インターフェイス通信にのみ適用されます。

レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトで、高いセキュリティ レベルのインターフェイスから低いセキュリティ レベルのインターフェイスへの通信（発信）は暗黙的に許可されます。高いセキュリティ レベルのインターフェイス上のホストは、低いセキュリティ レベルのインターフェイス上の任意のホストにアクセスできます。ACL をインターフェイスに適用して、アクセスを制限できます。

  同じセキュリティ レベルのインターフェイスの通信をイネーブルにすると、同じセキュリティ レベルまたはそれより低いセキュリティ レベルの他のインターフェイスにアクセスするインターフェイスは、暗黙的に許可されます。

- インスペクション エンジン：一部のアプリケーション インスペクション エンジンはセキュリティ レベルに依存します。同じセキュリティ レベルのインターフェイス間では、インスペクション エンジンは発信と着信のいずれのトラフィックに対しても適用されます。
  - NetBIOS インスペクション エンジン：発信接続に対してのみ適用されます。
  - SQL*Net インスペクション エンジン：SQL*Net（旧称 OraServ）ポートとの制御接続が一対のホスト間に存在する場合、着信データ接続だけが ASA を通過することが許可されます。

デュアル IP スタック（IPv4 および IPv6）

ASA は、インターフェイスで IPv6 アドレスと IPv4 アドレスの両方をサポートしています。IPv4 と IPv6 の両方で、デフォルト ルートを設定してください。

31 ビット サブネット マスク

ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバーリンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP または Syslog を実行する管理ステーションを直接接続することもできます。

31 ビットのサブネットとクラスタリング

管理インターフェイスとクラスタ制御リンクを除き、スパンドクラスタリング モードで31 ビットのサブネットマスクを使用できます。

インターフェイス上では、クラスタリングモードで 31 ビットのサブネット マスクを使用できません。

31 ビットのサブネットとフェールオーバー

フェールオーバーに関しては、ASA インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバーインターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、ASA はネットワークのテストを実行できず、リンクステートのみしか追跡できません。

ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。

31 ビットのサブネットと管理

直接接続される管理ステーションがあれば、ASA 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。

31 ビットのサブネットをサポートしていない機能

次の機能は、31 ビットのサブネットをサポートしていません。

- ブリッジ グループ用 BVI インターフェイス - ブリッジ グループには BVI、2 つのブリッジ グループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/ 29 サブネット以下を使用する必要があります。
- マルチキャスト ルーティング

ルーテッドモードおよびトランスペアレントモードのインターフェイスに関するガイドラインと制限事項

コンテキスト モード

- マルチ コンテキスト モードで設定できるのは、マルチ コンテキストの設定 （277 ページ）に従ってシステム コンフィギュレーションでコンテキストにすでに割り当てられているコンテキスト インターフェイスだけです。
- PPPoE は、マルチ コンテキスト モードではサポートされていません。
- トランスペアレント モードのマルチ コンテキスト モードでは、各コンテキストが別個のインターフェイスを使用する必要があります。コンテキスト間でインターフェイスを共有することはできません。
- トランスペアレント モードのマルチ コンテキスト モードでは、通常、各コンテキストが別個のサブネットを使用します。重複するサブネットを使用することもできますが、ルーティング スタンドポイントから可能にするため、ネットワーク トポロジにルータと NAT コンフィギュレーションが必要です。
- DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。
- ルーテッド ファイアウォール モードでは、ブリッジ グループ インターフェイスはマルチ コンテキスト モードでサポートされません。

フェールオーバー、クラスタリング

- フェールオーバー リンクは、この章の手順で設定しないでください。詳細については、「フェールオーバー」の章を参照してください。
- クラスタインターフェイスの場合は、クラスタリングの章で要件を確認してください。
- フェールオーバー を使用する場合、データ インターフェイスの IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP および PPPoE はサポートされません。

IPv6

- IPv6 はすべてのインターフェイスでサポートされます。
- トランスペアレント モードでは、IPv6 アドレスは手動でのみ設定できます。

- ASAは、IPv6 エニーキャスト アドレスはサポートしません。
- DHCPv6およびプレフィックス委任オプションは、マルチコンテキストモード、トランスペアレントモード、クラスタリング、またはフェールオーバーではサポートされません。

モデルのガイドライン

- ASAv50 の場合、ブリッジグループは透過的モードまたはルーテッドモードのいずれでもサポートされません。

トランスペアレント モードとブリッジ グループのガイドライン

- 64 のインターフェイスをもつブリッジ グループを 250 まで作成できます。
- 直接接続された各ネットワークは同一のサブネット上にある必要があります。
- ASA では、セカンダリ ネットワーク上のトラフィックはサポートされていません。BVI IP アドレスと同じネットワーク上のトラフィックだけがサポートされています。
- デバイスとデバイス間の管理トラフィック、および ASA を通過するデータトラフィックの各ブリッジグループに対し、BVI の IP アドレスが必要です。IPv4 トラフィックの場合は、IPv4 アドレスを指定します。IPv6 トラフィックの場合は、IPv6 アドレスを指定します。
- IPv6 アドレスは手動でのみ設定できます。
- BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。サブネットにホスト サブネット（255.255.255.255）を設定することはできません。
- 管理インターフェイスはブリッジ グループのメンバーとしてサポートされません。
- ブリッジされた ixgbevf インターフェイスを備えた VMware の ASAv50 の場合、トランスペアレントモードはサポートされておらず、ブリッジグループはルーテッドモードではサポートされていません。
- Firepower 1010 および Secure Firewall 1210/20 では、同じブリッジグループ内に論理 VLAN インターフェイスと物理ファイアウォールインターフェイスを混在させることはできません。
- トランスペアレント モードでは、少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があります。
- トランスペアレントモードでは、接続されたデバイス用のデフォルトゲートウェイとして BVI IP アドレスを指定しないでください。デバイスは ASA の他方側のルータをデフォルトゲートウェイとして指定する必要があります。
- トランスペアレント モードでは、管理トラフィックの戻りパスを指定するために必要な *default* ルートは、1 つのブリッジ グループ ネットワークからの管理トラフィックにだけ適用されます。これは、デフォルト ルートはブリッジ グループのインターフェイスとブリッジ グループ ネットワークのルータ IP アドレスを指定しますが、ユーザは 1 つのデフォルト ルートしか定義できないためです。複数のブリッジ グループ ネットワークから

の管理トラフィックが存在する場合は、管理トラフィックの発信元ネットワークを識別する標準のスタティック ルートを指定する必要があります。

- トランスペアレント モードでは、PPPoE は 管理 インターフェイスでサポートされません。
- ルーテッドモードでは、ブリッジグループと他のルーテッドインターフェイスの間をルーティングするために、BVI を指定する必要があります。
- ルーテッド モードでは、ASA 定義の EtherChannel および VNI インターフェイスがブリッジ グループのメンバーとしてサポートされません。Firepower 4100/9300 上の Etherchannel は、ブリッジグループメンバーにすることができます。
- Bidirectional Forwarding Detection（BFD）エコー パケットは、ブリッジ グループ メンバを使用するときに、ASA を介して許可されません。BFD を実行している ASA の両側に 2 つのネイバーがある場合、ASA は BFD エコー パケットをドロップします。両方が同じ送信元および宛先 IP アドレスを持ち、LAND 攻撃の一部であるように見えるからです。

デフォルトのセキュリティ レベル

デフォルトのセキュリティ レベルは 0 です。インターフェイスに「inside」という名前を付けて、明示的にセキュリティ レベルを設定しないと、ASA はセキュリティ レベルを 100 に設定します。

（注） インターフェイスのセキュリティレベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear conn** コマンドを使用して接続をクリアできます。

その他のガイドラインと要件

- ASA では、パケットで 802.1Q ヘッダーが 1 つだけサポートされ、複数のヘッダー（Q-in-Q）はサポートされません。
- 頻繁なアップ/ダウンステータスの変化などのインターフェイスの問題があると、フローティング接続タイマーが、インターフェイスを通過する接続に正しく適用されない場合があります。インターフェイスのステータスに問題がある場合は、無効な接続をクリアするするため、ステータスが安定した後にすべての接続をクリアすることを検討してください。

ルーテッド モードのインターフェイスの設定

ルーテッド モードのインターフェイスを設定するには、次の手順を実行します。

ルーテッド モードの一般的なインターフェイス パラメータの設定

この手順では、名前、セキュリティ レベル、IPv4 アドレス、およびその他のオプションを設定する方法について説明します。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

インターフェイス ID には、次のものがあります。

- **port-channel**
- *physical*：**ethernet**、**gigabitethernet**、**tengigabitethernet**、**management** など。インターフェイス名については、使用しているモデルのハードウェア インストール ガイドを参照してください。
- *physical.subinterface*：**gigabitethernet0/0.100** など。
- **vni**
- **vlan**
- **loopback**
- *mapped_name*：マルチ コンテキスト モードの場合。

（注）
Firepower 1010 の場合、スイッチポートをルーテッド モード インターフェイスとして設定することはできません。

ステップ 2 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3 次のいずれかの方法を使用して IP アドレスを設定します。

フェールオーバーやクラスタリング、およびループバック インターフェイスの場合は、IP アドレスを手動で設定する必要があります。DHCP と PPPoE はサポートされません。

- IP アドレスを手動で設定します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  standby *ip_address* 引数は、フェールオーバーで使用します。スタンバイ IP アドレスを設定しない場合、アクティブ ユニットはネットワーク テストを使用してスタンバイ インターフェイスをモニターできず、リンク ステートをトラックすることしかできません。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。ポイントツーポイント接続の場合、31 ビットのサブネット マスク（255.255.255.254）を指定できます。この場合、ネットワークまたはブロードキャスト アドレス用の IP アドレスは予約されません。この場合、スタンバイ IP アドレスを設定できません。

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.0 255.255.255.254
  ```

- DHCP サーバーから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute キーワードを指定すると、ASA が DHCP サーバーから渡されたデフォルト ルートを使用できるようになります。

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  （注）
  ip address dhcp コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

- PPPoE サーバから IP アドレスを取得します。

  ip address pppoe [**setroute**]

例：

```
ciscoasa(config-if)# ip address pppoe setroute
```

または、IP アドレスを手動で入力して PPPoE を有効化することができます。

ip address *ip_address mask* **pppoe**

例：

```
ciscoasa(config-if)# ip address 10.1.1.78 255.255.255.0 pppoe
```

setroute オプションを指定すると、PPPoE クライアントが接続をまだ確立していない場合に、デフォルトルートが設定されます。**setroute** オプションを使用する場合は、スタティックに定義されたルートをコンフィギュレーションに含めることはできません。

（注）
2 つのインターフェイス（プライマリとバックアップのインターフェイスなど）で PPPeE が有効化されているときに、デュアル ISP サポートを設定しない場合、ASA では、最初のインターフェイスに限り、IP アドレスを取得するためにトラフィックを送信できます。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

（注）
ループバック インターフェイスの場合、インターフェイスはデバイス間のトラフィックに対してのみサポートされるため、セキュリティ レベルは設定しません。

ステップ 5 （オプション）インターフェイスを管理専用モードに設定してトラフィックが通過しないようにします。

management-only

デフォルトでは、管理インターフェイスは管理専用として設定されます。

（注）
ループバック インターフェイスの場合、インターフェイスはデバイス間のトラフィックに対してのみサポートされるため、管理モードは設定しません。

例

次に、VLAN 101 のパラメータの設定例を示します。

```
ciscoasa(config)# interface vlan 101
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
```

次に、マルチコンテキストモードでコンテキストコンフィギュレーションにパラメータを設定する例を示します。インターフェイス ID はマップ名です。

```
ciscoasa/contextA(config)# interface int1
ciscoasa/contextA(config-if)# nameif outside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
```

関連トピック

IPv6 アドレスの設定 （944 ページ）
物理インターフェイスのイネーブル化およびイーサネット パラメータの設定 （830 ページ）
PPPoE の設定 （936 ページ）

PPPoE の設定

インターフェイスが DSL、ケーブル モデム、またはその他の手段で ISP に接続されていて、ISP が PPPoE を使用して IP アドレスを割り当てる場合は、次のパラメータを設定します。

手順

ステップ 1 この接続を表す任意のバーチャルプライベート ダイヤルアップ ネットワーク（VPDN）グループ名を定義します。

vpdn group *group_name* **request dialout pppoe**

例：

```
ciscoasa(config)# vpdn group pppoe-sbc request dialout pppoe
```

ステップ 2 ISP が認証を要求する場合は、認証プロトコルを選択します。

vpdn group *group_name* **ppp authentication** {**chap** | **mschap** | **pap**}

例：

```
ciscoasa(config)# vpdn group pppoe-sbc ppp authentication chap
```

ISP で使用する認証方式に応じた適切なキーワードを入力します。

CHAP または MS-CHAP を使用する場合は、ユーザー名がリモート システム名として参照され、パスワードが CHAP シークレットとして参照されます。

ステップ 3 ISP で割り当てられたユーザー名を VPDN グループに関連付けます。

vpdn group *group_name* **localname** *username*

例：

```
ciscoasa(config)# vpdn group pppoe-sbc localname johncrichton
```

ステップ 4 PPPoE 接続用のユーザー名とパスワードのペアを作成します。

vpdn username *username* **password** *password* [**store-local**]

例：

```
ciscoasa(config)# vpdn username johncrichton password moya
```

store-local オプションを指定すると、ユーザー名とパスワードが ASA の NVRAM の特別な場所に保存されます。Auto Update Server が **clear config** コマンドを ASA に送信し、その後に接続が中断された場合、ASA は、ユーザー名とパスワードを NVRAM から読み取り、アクセス コンセントレータに対して再認証できます。

ブリッジグループ インターフェイスの設定

ブリッジ グループは、ASA がルーティングではなくブリッジするインターフェイスのグループです。ブリッジグループはトランスペアレント ファイアウォール モード、ルーテッド ファイアウォール モードの両方でサポートされています。ブリッジグループの詳細については、ブリッジグループについて （233 ページ）を参照してください。

ブリッジグループと関連インターフェイスを設定するには、次の手順を実行します。

ブリッジ仮想インターフェイス（BVI）の設定

ブリッジ グループごとに、IP アドレスを設定する BVI が必要です。ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの IP アドレスを使用します。BVI IP アドレスは、接続されたネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、BVI IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。

ルーテッドモードの場合、BVIに名前を指定すると、BVIがルーティングに参加します。名前を指定しなければ、ブリッジ グループはトランスペアレント ファイアウォール モードの場合と同じように隔離されたままになります。

一部のモデルでは、デフォルト コンフィギュレーションにブリッジ グループと BVI が含まれています。追加のブリッジグループおよびBVIを作成して、グループの間でメンバーインターフェイスを再割り当てすることもできます。

（注） トランスペアレントモードの個別の管理インターフェイスでは（サポートされているモデルの場合）、設定できないブリッジグループ（ID 301）がコンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

手順

ステップ 1 BVI を作成します。

interface bvi *bridge_group_number*

例：

```
ciscoasa(config)# interface bvi 2
```

bridge_group_number は、1 ～ 250 の整数です。このブリッジ グループ メンバーには、後で物理インターフェイスを割り当てます。

ステップ 2 （トランスペアレント モード）BVI の IP アドレスを指定します。

ip address *ip_address* [*mask*] [**standby** *ip_address*]

例：

```
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

BVI にはホスト アドレス（/32 または 255.255.255.255）を割り当てないでください。また、/30 サブネットなど（255.255.255.252）、ホストアドレスが 3 つ未満の他のサブネットを使用しないでください（ホストアドレスは、アップストリーム ルータ、ダウンストリーム ルータ、BVI にそれぞれ 1 つずつです）。ASA は、サブネットの先頭アドレスと最終アドレスで送受信されるすべての ARP パケットをドロップします。このため、/30 サブネットを使用し、このサブネットからアップストリーム ルータに予約済みアドレスを割り当てると、ASA はダウンストリーム ルータからアップストリーム ルータへの ARP 要求をドロップします。

フェールオーバーには、**standby** キーワードおよびアドレスを使用します。

ステップ 3 （ルーテッド モード）次のいずれかの方法を使用して IP アドレスを設定します。

フェールオーバーやクラスタリングの場合は、IPアドレスを手動で設定する必要があります。DHCP はサポートされません。

- IP アドレスを手動で設定します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

  standby *ip_address* 引数は、フェールオーバーで使用します。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。

- DHCP サーバーから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

  ```
  ciscoasa(config-if)# ip address dhcp
  ```

  setroute キーワードを指定すると、ASA が DHCP サーバーから渡されたデフォルト ルートを使用できるようになります。

  DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

  ip address dhcp コマンドを入力する前に、no shutdown コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

ステップ 4 （ルーテッド モード）インターフェイスに名前を付けます。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside
```

トラフィックをブリッジ グループ メンバーの外部（たとえば、外部インターフェイスや他のブリッジグループのメンバー）にルーティングする必要がある場合は、BVIに名前を付ける必要があります。*name* は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 5 （ルーテッド モード）セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

例

次の例では、BVI 2 アドレスとスタンバイ アドレスを設定します。

```
ciscoasa(config)# interface bvi 2
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

ブリッジ グループ メンバーの一般的なインターフェイス パラメータの設定

この手順は、ブリッジ グループ メンバー インターフェイスの名前、セキュリティ レベル、およびブリッジ グループを設定する方法について説明します。

始める前に

- 同じブリッジグループで、さまざまな種類のインターフェイス（物理インターフェイス、VLAN サブインターフェイス、VNI インターフェイス、EtherChannel インターフェイス）を含めることができます。管理インターフェイスはサポートされていません。ルーテッド モードでは、EtherChannel と VNI はサポートされません。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。
- トランスペアレント モードの場合、管理インターフェイスにはこの手順を使用しないでください。管理インターフェイスを設定する場合は、トランスペアレント モードの管理インターフェイスの設定 （942 ページ）を参照してください。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

インターフェイス ID には、次のものがあります。

- **port-channel**
- *physical*：**ethernet**、**gigabitethernet**、**tengigabitethernet** など。管理インターフェイスはサポートされていません。インターフェイス名については、使用しているモデルのハードウェア インストール ガイドを参照してください。
- *physical_or_port-channel.subinterface*：たとえば、**gigabitethernet0/0.100**または **port-channel1.100** など。
- **vni**
- **vlan**
- *mapped_name*：マルチ コンテキスト モードの場合。

（注）
Firepower 1010 では、スイッチポートをブリッジグループメンバーとして設定することはできません。

同じブリッジグループ内に論理 VLAN インターフェイスと物理ルータインターフェイスを混在させることはできません。

（注）
ルーテッドモードでは、**port-channel** および **vni** インターフェイスはブリッジグループのメンバーとしてサポートされません。

ステップ 2 インターフェイスをブリッジ グループに割り当てます。

bridge-group *number*

例：

```
ciscoasa(config-if)# bridge-group 1
```

number は 1 ~ 250 の整数で、BVI インターフェイス番号に一致する必要があります。ブリッジグループには最大 64 個のインターフェイスを割り当てることができます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。

ステップ 3 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif inside1
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 50
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

関連トピック

MTUおよび TCP MSS の設定 （980 ページ）

トランスペアレント モードの管理インターフェイスの設定

トランスペアレント ファイアウォール モードでは、すべてのインターフェイスがブリッジ グループに属している必要があります。唯一の例外は管理インターフェイス（物理インターフェイス、サブインターフェイス（ご使用のモデルでサポートされている場合）、または管理インターフェイスを構成する EtherChannel インターフェイス（複数の管理インターフェイスがある場合）のいずれか）です。管理インターフェイスは個別の管理インターフェイスとして設定できます。Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt タイプ インターフェイスに基づいています。他のインターフェイス タイプは管理インターフェイスとして使用できません。シングル モードまたはコンテキストごとに 1 つの管理インターフェイスを設定できます。詳細については、トランスペアレント モードの管理インターフェイス （827 ページ）を参照してください。

管理インターフェイスは to-the-box トラフィックおよび from-the-box トラフィック専用で、トラフィックのパススルーはできません。

始める前に

- このインターフェイスをブリッジ グループに割り当てないでください。設定できないブリッジ グループ（ID 301）は、コンフィギュレーションに自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。
- Firepower 4100/9300 シャーシ では、管理インターフェイス ID は ASA 論理デバイスに割り当てた mgmt-type インターフェイスに基づいています。
- マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。データ インターフェイスに接続する必要があります。
- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface {{**port-channel** *number* | **management** *slot*/*port* | *mgmt-type_interface_id* }[**.** *subinterface*] | *mapped_name*}

例：

```
ciscoasa(config)# interface management 0/0.1
```

port-channel *number* 引数は、**port-channel 1** などの EtherChannel インターフェイス ID です。EtherChannel インターフェイスには、管理メンバーインターフェイスのみが設定されている必要があります。

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用して割り当てた場合、*mapped_name* を入力します。

Firepower 4100/9300 シャーシでは、ASA 論理デバイスに割り当てた mgmt タイプ インターフェイス（個別インターフェイスまたは EtherChannel インターフェイス）のインターフェイス ID を指定します。

ステップ 2 インターフェイスの名前を指定します。

nameif *name*

例：

```
ciscoasa(config-if)# nameif management
```

name は最大 48 文字のテキスト文字列です。大文字と小文字は区別されません。名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、**no** 形式は入力しないでください。

ステップ 3 次のいずれかの方法を使用して IP アドレスを設定します。

- IP アドレスを手動で設定します。

  フェールオーバーとともに使用する場合は、IP アドレスとスタンバイ アドレスを手動で設定する必要があります。DHCP はサポートされません。

  ip_address 引数および *mask* 引数には、インターフェイスの IP アドレスとサブネット マスクを設定します。

  standby *ip_address* 引数は、フェールオーバーで使用します。

  ip address *ip_address* [*mask*] [**standby** *ip_address*]

  例：

  ```
  ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
  ```

- DHCP サーバーから IP アドレスを取得します。

  ip address dhcp [**setroute**]

  例：

```
ciscoasa(config-if)# ip address dhcp
```

setroute キーワードを指定すると、ASA が DHCP サーバーから渡されたデフォルト ルートを使用できるようになります。

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

ip address dhcp コマンドを入力する前に、no shutdown コマンドを使用してインターフェイスを有効化していない場合、一部の DHCP 要求が送信されないことがあります。

ステップ 4 セキュリティ レベルを設定します。

security-level *number*

例：

```
ciscoasa(config-if)# security-level 100
```

number には、0（最下位）～ 100（最上位）の整数を指定します。

IPv6 アドレスの設定

この項では、IPv6 アドレッシングを設定する方法について説明します。

IPv6 について

このセクションには、IPv6 に関する情報が含まれています。

IPv6 アドレッシング

IPv6 に対して次の 2 種類のユニキャスト アドレスを設定できます。

- グローバル：グローバル アドレスは、パブリック ネットワークで使用可能なパブリック アドレスです。ブリッジ グループの場合、このアドレスは各メンバー インターフェイスごとに設定するのではなく、BVI 用に設定する必要があります。また、トランスペアレント モードで管理インターフェイスのグローバルな IPv6 アドレスを設定することもできます。
- リンクローカル：リンクローカルアドレスは、直接接続されたネットワークだけで使用できるプライベート アドレスです。ルータは、リンクローカル アドレスを使用してパケットを転送するのではなく、特定の物理ネットワーク セグメント上で通信だけを行います。ルータは、アドレス設定またはアドレス解決などのネイバー探索機能に使用できます。ブリッジ グループでは、メンバー インターフェイスのみがリンクローカル アドレスを所有しています。BVI にはリンクローカル アドレスはありません。

最低限、IPv6 が動作するようにリンクローカル アドレスを設定する必要があります。グローバル アドレスを設定すると、リンクローカル アドレスがインターフェイスに自動的に設定されるため、リンクローカル アドレスを個別に設定する必要はありません。ブリッジ グループ インターフェイスでは、BVI でグローバル アドレスを設定した場合、ASA が自動的にメンバー インターフェイスのリンクローカル アドレスを生成します。グローバル アドレスを設定しない場合は、リンクローカル アドレスを自動的にするか、手動で設定する必要があります。

（注） リンクローカル アドレスの設定だけを行う場合は、コマンド リファレンスの **ipv6 enable** コマンド（自動設定）または **ipv6 address link-local** コマンド（手動設定）を参照してください。

Modified EUI-64 インターフェイス ID

RFC 3513「Internet Protocol Version 6 (IPv6) Addressing Architecture」（インターネット プロトコル バージョン 6 アドレッシング アーキテクチャ）では、バイナリ値 000 で始まるものを除き、すべてのユニキャスト IPv6 アドレスのインターフェイス識別子部分は長さが 64 ビットで、Modified EUI-64 形式で組み立てることが要求されています。ASA では、ローカル リンクに接続されたホストにこの要件を適用できます。

この機能がインターフェイスで有効化されていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカル リンク上のホストに対してのみ実行できます。

IPv6 プレフィックス委任クライアントの設定

ASA は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアント インターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASA はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。

IPv6 プレフィックス委任の概要

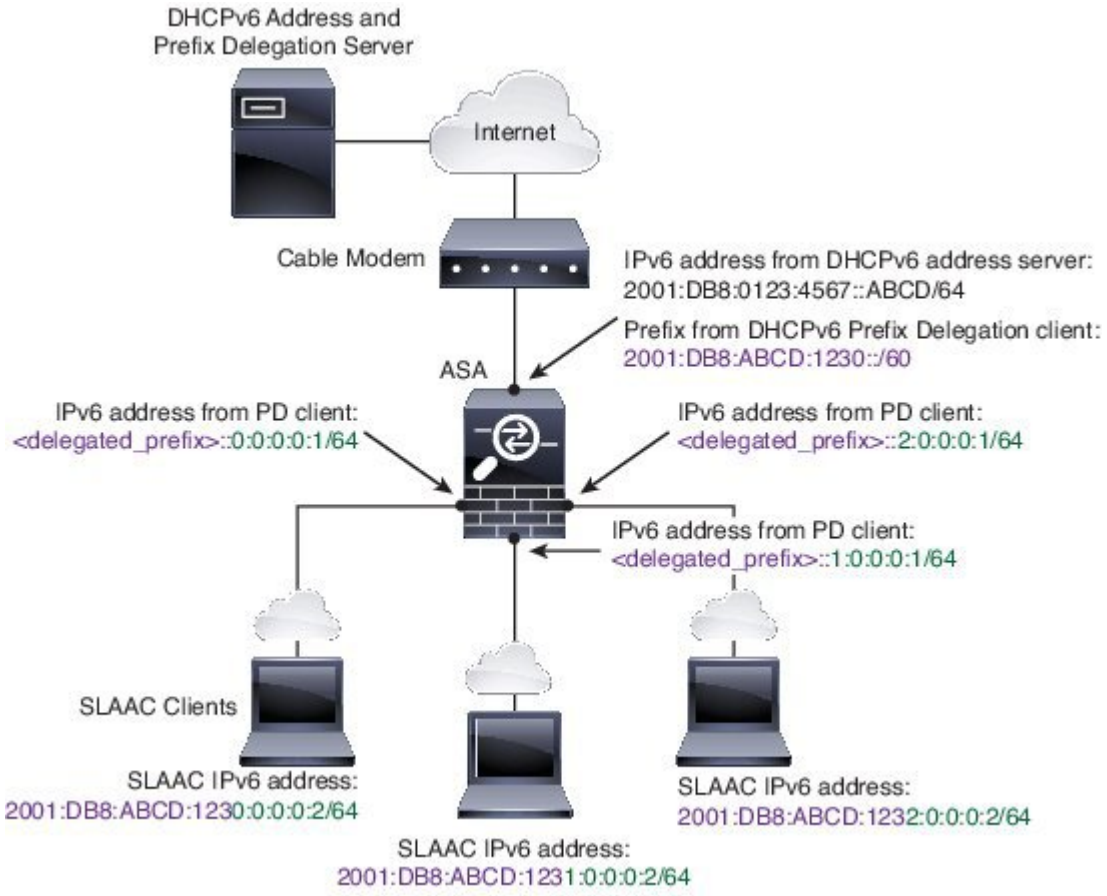
ASA は、（ケーブルモデムに接続された外部インターフェイスなどの）クライアント インターフェイスが 1 つ以上の IPv6 プレフィックスを受け取れるように DHPCv6 プレフィックス委任クライアントとして機能することができ、ASA はそのプレフィックスをサブネット化して内部インターフェイスに割り当てることが可能です。これにより、内部インターフェイスに接続されているホストは、StateLess Address Auto Configuration（SLAAC）を使用してグローバル IPv6

アドレスを取得できます。ただし、内部ASAインターフェイスはプレフィックス委任サーバーとして機能しないため注意してください。ASAは、SLAACクライアントにグローバルIPアドレスを提供することしかできません。たとえば、ルータが ASA に接続されている場合、ASAはSLAACクライアントとして機能し、IPアドレスを取得できます。しかし、ルータの背後のネットワークに代理プレフィックスのサブネットを使用したい場合、ルータの内部インターフェイス上でそれらのアドレスを手動で設定する必要があります。

ASA には軽量 DHCPv6 サーバーが含まれており、SLAAC クライアントが情報要求（IR）パケットを ASA に送信した場合、ASA は DNS サーバーやドメイン名などの情報を SLAAC クライアントに提供できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（ASA がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

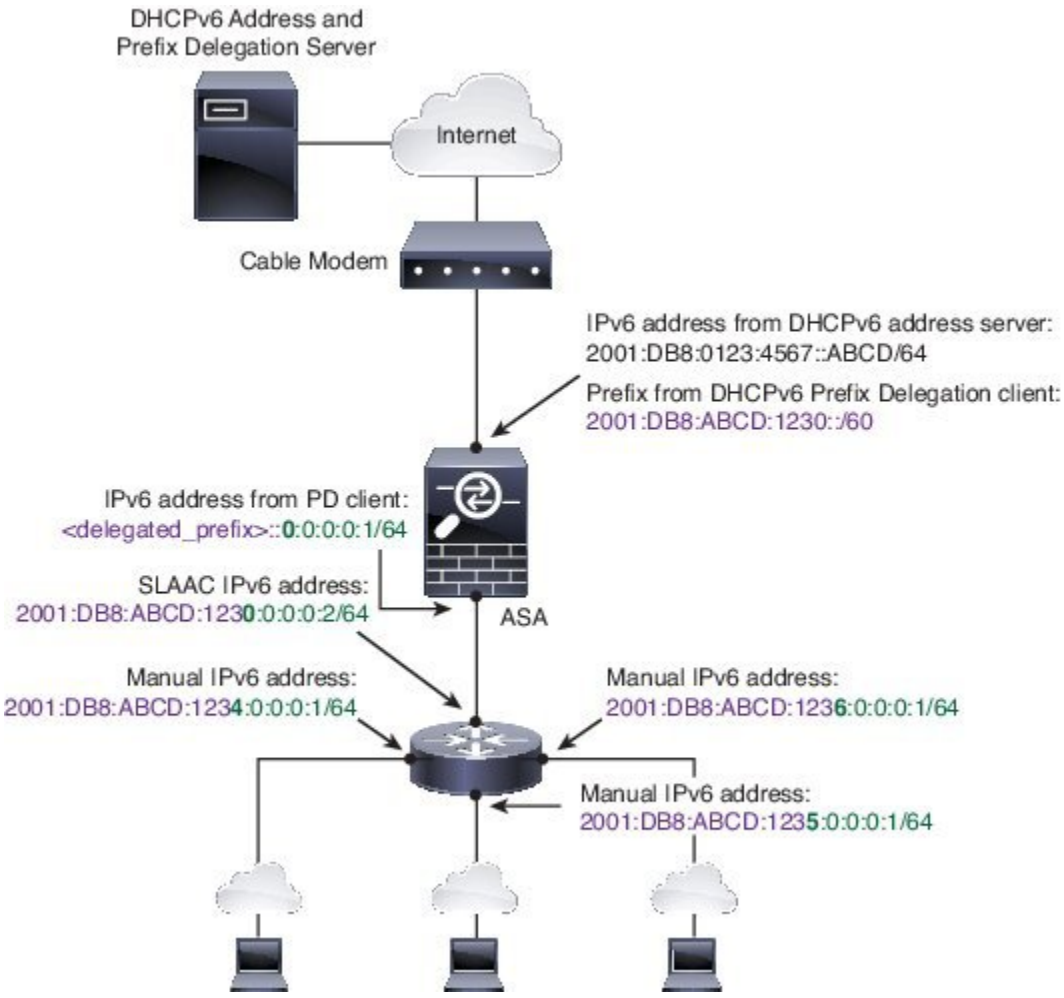
IPv6 プレフィックス委任 /64 サブネットの例

次の例では、ASA が DHCPv6 アドレスクライアントを使用して、外部インターフェイス上で IP アドレスを受け取るところを示しています。また、ASA は DHCPv6 プレフィックス委任クライアントを使用して代理プレフィックスを取得します。ASAは、委任されたプレフィックスを /64 ネットワークにサブネット化し、委任されたプレフィックスと手動で設定されたサブネット（::0、::1、または ::2）と各インターフェイスの IPv6 アドレス（0:0:0:1）を使用して、動的に内部インターフェイスにグローバル IPv6 アドレスを割り当てます。これらの内部インターフェイスに接続されている SLAAC クライアントは、各 /64 サブネットの IPv6 アドレスを取得します。



IPv6 プレフィックス委任 /62 サブネットの例

次の例は、ASA が 4/62 サブネットにプレフィックスをサブネット化するところを示しています。2001:DB8:ABCD:123**0**::/62、2001:DB8:ABCD:123**4**::/62、2001:DB8:ABCD:123**8**::/62、2001:DB8:ABCD:123**C**::/62。ASA は、内部ネットワーク（::0）に 2001:DB8:ABCD:1230::/62 の利用可能な 64 サブネット 4 つのいずれかを使用します。ダウンストリーム ルータには、手動で追加の /62 サブネットを使用できます。図のルータは、内部インターフェイス（::4, ::5, and ::6）に 2001:DB8:ABCD:1234::/62 の利用可能な 4 つの /64 サブネットのうちの 3 つを使用します。この場合、内部ルータインターフェイスは委任されたプレフィックスを動的に取得できないため、ASA 上で委任されたプレフィックスを表示し、ルータ設定にそのプレフィックスを使用する必要があります。通常、リースが期限切れになった場合、ISP は既定のクライアントに同じプレフィックスを委任しますが、ASA が新しいプレフィックスを受け取った場合、新しいプレフィックスを使用するようルータ設定を変更する必要があります。DHCP の一意識別子（DUID）は、再起動後も存続します。



IPv6 プレフィックス委任クライアントの有効化

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

始める前に

- この機能は、ルーテッド ファイアウォール モードに限りサポートされています。
- この機能はマルチ コンテキスト モードではサポートされません。
- この機能は、クラスタリングではサポートされていません。
- この機能は管理専用インターフェイスでは設定できません。

- プレフィックス委任を使用する場合は、IPv6 トラフィックの中断を防ぐために、ASA IPv6 ネイバー探索のルータ アドバタイズメント間隔を DHCPv6 サーバによって割り当てられるプレフィックスの推奨有効期間よりもはるかに小さい値に設定する必要があります。たとえば、DHCPv6 サーバがプレフィックス委任の推奨有効期間を 300 秒に設定している場合は、ASA RA の間隔を 150 秒に設定する必要があります。推奨有効期間を設定するには、**show ipv6 general-prefix** コマンドを使用します。ASA RA の間隔を設定するには、IPv6 ネイバー探索の設定 （954 ページ）を参照してください。デフォルトは 200 秒です。

手順

ステップ 1 DHCPv6 サーバー ネットワークに接続されるインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

ステップ 2 DHCPv6プレフィックス委任クライアントを有効にし、このインターフェイスで取得したプレフィックスに名前を付けます。

ipv6 dhcp client pd *name*

例：

```
ciscoasa(config-if)# ipv6 dhcp client pd Outside-Prefix
```

name には最大 200 文字を使用できます。

ステップ 3 受信する委任されたプレフィックスに関する 1 つ以上のヒントを提供します。

ipv6 dhcp client pd hint*ipv6_prefix/ prefix_length*

例：

```
ciscoasa(config-if)# ipv6 dhcp client pd hint 2001:DB8:ABCD:1230::/60
```

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバによって決定されます。

ステップ 4 ASA インターフェイスのグローバル IP アドレスとしてプレフィックスのサブネットを割り当てるには、グローバル IPv6 アドレスの設定 （950 ページ） を参照してください。

ステップ 5 （任意） SLAAC クライアントにドメイン名とサーバー パラメータを提供するには、DHCPv6 ステートレス サーバーの設定 （1042 ページ） を参照してください。

ステップ 6 （任意）BGP でプレフィックスをアドバタイズするには、IPv6 ネットワークの設定 （1230 ページ） を参照してください。

例

次に、GigabitEthernet 0/0 で DHCPv6 アドレスクライアントおよびプレフィックス委任クライアントを設定した後に、アドレスをプレフィックスとともに GigabitEthernet 0/1 および 0/2 に割り当てる例を示します。

```
interface gigabitethernet 0/0
  ipv6 address dhcp default
  ipv6 dhcp client pd Outside-Prefix
  ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

グローバル IPv6 アドレスの設定

ルーテッド モードの任意のインターフェイスとトランスペアレント モードまたはルーテッド モードの BVI に対してグローバル IPv6 アドレスを設定するには、次の手順を実行します。

DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。

（注） グローバルアドレスを設定すると、リンクローカルアドレスは自動的に設定されるため、別々に設定する必要はありません。ブリッジ グループについて、BVI でグローバル アドレスを設定すると、すべてのメンバー インターフェイスのリンクローカル アドレスが自動的に設定されます。

サブインターフェイスの場合、親インターフェイスの同じ Burned-In MAC Address を使用するので、MAC アドレスも手動で設定することをお勧めします。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。を参照してください。MAC アドレスの手動設定 （978 ページ）

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

トランスペアレント モード、またはルーテッド モードのブリッジ グループの場合、BVI を指定します。

例：

```
ciscoasa(config)# interface bvi 1
```

トランスペアレントモードでは、BVIに加え、管理インターフェイスを指定することもできます。

例：

```
ciscoasa(config)# interface management 1/1
```

ステップ 2 （ルーテッド インターフェイス）次のいずれかの方法を使用して IP アドレスを設定します。

フェールオーバーやクラスタリング、およびループバック インターフェイスの場合は、IP アドレスを手動で設定する必要がありますクラスタリングの場合、リンクローカルアドレスの手動設定はサポートされていません。

- インターフェイスでステートレスな自動設定をイネーブルにします。

  ipv6 address autoconfig [**default trust** {**dhcp** |**ignore**}]

  インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。ステートレスな自動設定が有効になっている場合、インターフェイスのリンクローカルアドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。

  （注）
  RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定していますが、ASA はこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、**ipv6 nd suppress-ra** コマンドを参照してください。

デフォルトルートをインストールするには、 **default trust dhcp** か **ignore** を指定します。**dhcp** を指定すると、ASA は信頼できる送信元から（IPv6 アドレスを提供した同じサーバーから）取得されたルータアドバタイズメントからのデフォルトルートのみを使用します。**ignore** を指定すると、別のネットワークからルータアドバタイズメントを取得できるようになります（この方法では、リスクが高くなる可能性があります）。

- DHCPv6 を使用してアドレスを取得します。

  ipv6 address dhcp [**default**]

  例：

  ```
  ciscoasa(config-if)# ipv6 address dhcp default
  ```

  default キーワードを指定すると、ルータ アドバタイズメントからデフォルト ルートが取得されます。

- インターフェイスに手動でグローバル アドレスを割り当てます。

  ipv6 address *ipv6_address*/*prefix-length* [**standby** *ipv6_address*]

  例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
  ```

  グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。

  standby は、フェールオーバーペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

- Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。

  ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

  例：

  ```
  ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
  ```

  グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。

  スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。

- 委任されたプレフィックスを使用します。

  ipv6 address *prefix_name ipv6_address*/*prefix_length*

  例：

```
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

この機能は、ASA に別のインターフェイスで DHCPv6 プレフィックス委任クライアントを有効にさせるために必要です。IPv6 プレフィックス委任クライアントの有効化 （948 ページ）を参照してください。通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。

ステップ 3 （BVIインターフェイス）BVIに手動でグローバルアドレスを割り当てます。トランスペアレント モードの管理インターフェイスでも、この方法を使用します。

ipv6 address *ipv6_address/prefix-length* [**standby** *ipv6_address*]

例：

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。

standby は、フェールオーバー ペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

ステップ 4 （オプション）ローカル リンクの IPv6 アドレスに Modified EUI-64 形式のインターフェイス識別子の使用を適用します。

ipv6 enforce-eui64 *if_name*

例：

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

if_name 引数には、**nameif** コマンドで指定したインターフェイスの名前を指定します。このインターフェイスに対してアドレス形式を適用できます。

IPv6 ネイバー探索の設定

IPv6 ネイバー探索プロセスは、ICMPv6 メッセージおよび要請ノード マルチキャスト アドレスを使用して、同じネットワーク（ローカル リンク）上のネイバーのリンク層アドレスを特定し、ネイバーの読み出し可能性を確認し、隣接ルータを追跡します。

ノード（ホスト）はネイバー探索を使用して、接続リンク上に存在することがわかっているネイバーのリンク層アドレスの特定や、無効になったキャッシュ値の迅速なパージを行います。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送しようとしている隣接ルータを検出します。さらに、ノードはこのプロトコルを使用して、どのネイバーが到達可能でどのネイバーがそうでないかをアクティブに追跡するとともに、変更されたリンク層アドレスを検出します。ルータまたはルータへのパスが失われると、ホストは機能している代替ルータまたは代替パスをアクティブに検索します。

手順

ステップ 1 設定する IPv6 インターフェイスを指定します。

interface *name*

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)#
```

ステップ 2 重複アドレス検出（DAD）の試行回数を指定します。

ipv6 nd dad attempts *value*

value 引数の有効な値の範囲は 0 ～ 600 です。この値が 0 の場合、指定されたインターフェイスでの DAD 処理が無効化されます。デフォルト値は 1 件です。

DAD は、割り当てられる前に、新しいユニキャスト IPv6 アドレスの一意性を確認し、ネットワークに重複する IPv6 アドレスが検出されていないかをリンク ベースで確認します。ASA は、ネイバー送信要求メッセージを使用して、DAD を実行します。

重複アドレスが検出されると、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用対象外となり、次のエラー メッセージが生成されます。

```
325002: Duplicate address ipv6_address/MAC_address on interface
```

重複アドレスがインターフェイスのリンクローカルアドレスであれば、インターフェイス上で IPv6 パケットの処理は無効になります。重複アドレスがグローバル アドレスであれば、そのアドレスは使用されません。

例：

```
ciscoasa(config-if)# ipv6 nd dad attempts 20
```

ステップ 3 IPv6 ネイバー送信要求の再送信する間隔を設定します。

ipv6 nd ns-interval *value*

value 引数の有効な値は、1000 ～ 3600000 ミリ秒です。

ローカル リンク上にある他のノードのリンクレイヤ アドレスを検出するため、ノードからネイバー送信要求メッセージ（ICMPv6 Type 135）がローカル リンクに送信されます。ネイバー送信要求メッセージを受信すると、宛先ノードは、ネイバー アドバタイズメント メッセージ（ICPMv6 Type 136）をローカル リンク上に送信して応答します。

送信元ノードがネイバーアドバタイズメントを受信すると、送信元ノードと宛先ノードが通信できるようになります。ネイバー送信要求メッセージは、ネイバーのリンク層アドレスが識別された後に、ネイバーの到達可能性の確認にも使用されます。ノードがあるネイバーの到達可能性を検証する場合、ネイバー送信要求メッセージ内の宛先アドレスとして、そのネイバーのユニキャスト アドレスを使用します。

ネイバー アドバタイズメント メッセージは、ローカル リンク上のノードのリンク層アドレスが変更されたときにも送信されます。

例：

```
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

ステップ 4 リモートの IPv6 ノードに到達可能な時間を設定します。

ipv6 nd reachable-time *value*

value 引数の有効な値は、0 ～ 3600000 ミリ秒です。value に 0 を使用すると、到達可能時間が判定不能として送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

ネイバー到達可能時間を設定すると、使用できないネイバーを検出できます。時間を短く設定すると、使用できないネイバーをより早く検出できます。ただし、時間を短くするほど、IPv6 ネットワーク帯域幅とすべての IPv6 ネットワーク デバイスの処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

例：

```
ciscoasa config-if)# ipv6 nd reachable-time 1700000
```

ステップ 5 IPv6 ルータ アドバタイズメントの送信間隔を設定します。

ipv6 nd ra-interval [**msec**] *value*

msec キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードが存在しない場合、値は秒単位で指定されます。*value* 引数の有効な値の範囲は 3 ～ 1800 秒、**msec** キーワードが指定されている場合は 500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

送信間隔の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

ASA がデフォルト ルータとして設定されている場合、送信間隔は IPv6 ルータ アドバタイズメント ライフタイム以下にする必要があります。

他の IPv6 ノードと同期しないように、ASA は設定値（ジッター）をランダムに調整します。

例：

```
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

ステップ 6 ローカル リンク上のノードが、ASA をリンク上のデフォルト ルータと見なす時間の長さを指定します。

ipv6 nd ra-lifetime [**msec**] *value*

オプションの **msec** キーワードは、この値がミリ秒単位で指定されることを示します。このキーワードを指定しない場合、値は秒単位です。*value* 引数の有効な値は 0 ～ 9000 秒です。0 を入力すると、ASA は選択したインターフェイスのデフォルト ルータと見なされません。

ルータの有効期間の値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイス上のデフォルトルータとしての ASA の有用性を示します。

例：

```
ciscoasa(config-if)# ipv6 nd ra-lifetime 2000
```

ステップ 7 ルータ アドバタイズメントを抑制します。

ipv6 nd suppress-ra

ルータ要請メッセージ（ICMPv6 Type 133）に応答して、ルータ アドバタイズメント メッセージ（ICMPv6 Type 134）が自動的に送信されます。ルータ要請メッセージは、システムの起動時にホストから送信されるため、ホストは、次にスケジュールされているルータ アドバタイズメント メッセージを待つことなくただちに自動設定を行うことができます。

ASA で IPv6 プレフィックスを提供する必要がないインターフェイス（外部インターフェイスなど）では、これらのメッセージを無効にできます。

このコマンドを入力すると、ASA がリンク上では IPv6 ルータではなく、通常の IPv6 ネイバーのように見えるようになります。

ステップ 8 取得されるステートレス自動設定のアドレス以外の IPv6 アドレスの取得に DHCPv6 を使用するように IPv6 自動設定クライアントに通知するには、IPv6 ルータ アドバタイズメントにフラグを追加します。

ipv6 nd managed-config-flag

このオプションは、IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定します。

ステップ 9 DNS サーバー アドレスや他の情報の取得に DHCPv6 を使用するように IPv6 自動設定クライアントに通知するには、IPv6 ルータ アドバタイズメントにフラグを追加します。

ipv6 nd other-config-flag

このオプションは、IPv6 ルータ アドバタイズメント パケットのその他のアドレス設定フラグを設定します。

ステップ 10 IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定します。

ipv6 nd prefix{*ipv6_prefix*/*prefix_length* |**default**} [*valid_lifetime preferred_lifetime* | **at** *valid_date preferred_date*] [**no-advertise**] [**no-autoconfig**] [ ] [**off-link**]

ネイバー デバイスは、プレフィックス アドバタイズメントを使用して、そのインターフェイス アドレスを自動設定できます。ステートレス自動設定では、ルータ アドバタイズメント メッセージで提供される IPv6 プレフィックスを使用して、リンクローカル アドレスからグローバル ユニキャスト アドレスを作成します。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してプレフィックスをアドバタイズメント用に設定すると、これらのプレフィックスだけがアドバタイズされます。

ステートレス自動設定が正しく機能するには、ルータ アドバタイズメント メッセージでアドバタイズされるプレフィックス長が常に 64 ビットでなければなりません。

- **default**: デフォルトのプレフィックスが使用されていることを示します。
- *valid_lifetime preferred_lifetime* ：指定した IPv6 プレフィックスを有効かつ優先されるものとしてアドバタイズする時間を指定します。優先の有効期間中には、アドレスの制限はありません。優先有効期間を過ぎると、アドレスは廃止状態になります。廃止状態のアドレスの使用は推奨されませんが、固く禁じられているわけではありません。有効期間の期限が切れた後に、アドレスは無効になり、使用できません。有効ライフタイムは優先ライフタイムと同じかそれより長い必要があります。値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定することもできます。デフォルトの有効期間は 2592000（30 日間）です。デフォルトの優先有効期間は 604800（7 日間）です。
- **at** *valid_date preferred_date*：プレフィックスの有効期限が切れる特定の日付と時刻を示します。日付は *month_name day hh*:*mm* と指定します。たとえば、**dec 1 13:00** と入力します。
- **no-advertise**：プレフィックスのアドバタイズメントを無効にします。**default** プレフィックスの場合、この設定はオンリンク プレフィックスにのみ適用されます。特定のオフリンク プレフィックスに **no-advertise** を指定しない限り、オフリンクプレフィックスは引き続きアドバタイズされます。
- **no-autoconfig**：プレフィックスは IPv6 自動設定には使用できないことを指定します。
- **off-link**：指定したプレフィックスをオフリンクとして設定します。プレフィクスはL ビット クリアでアドバタイズされます。プレフィックスは、接続されたプレフィックスとしてルーティング テーブルに挿入されません。

onlink がオン（デフォルト）のときは、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

例：

```
ciscoasa(config-if)# ipv6 nd prefix 2001:DB8::/32 1000 900
```

ステップ 11 IPv6 ネイバー探索キャッシュのスタティック エントリを設定します。

ipv6 neighbor *ipv6_address if_name mac_address*

次のガイドラインと制限事項は、スタティック IPv6 ネイバーの設定に適用されます。

- **ipv6 neighbor** コマンドは **arp** コマンドに似ています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。これらのエントリは、copy コマンドを使用して設定を保存するときに設定に保存されます。
- IPv6 ネイバー探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。
- **clear ipv6 neighbor** コマンドにより、スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリをネイバー探索キャッシュから削除します。このコマンドは、IPv6 ネイバー探索プロセスから認識されるエントリであるダイナミック エントリはキャッシュから削除しません。**no ipv6 enable** コマンドを使用してインターフェイスで IPv6 をディセーブルにすると、スタティック エントリを除いて、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュ エントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。
- IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。
- **clear ipv6 neighbor** コマンドを実行しても、スタティック エントリが IPv6 ネイバー探索キャッシュから削除されることはありません。ダイナミック エントリのクリアだけが行われます。
- 生成された ICMP syslog は、IPv6 ネイバー エントリの定期的な更新に起因します。IPv6 ネイバー エントリの ASA デフォルト タイマーは 30 秒であるため、ASA は 30 秒おきに ICMPv6 ネイバー探索および応答パケットを生成します。ASA にフェールオーバー LAN および IPv6 アドレスで設定された状態インターフェイスの両方がある場合は、30 秒ごとに、ICMPv6 ネイバー探索および応答パケットが、設定済みのリンクローカル IPv6 アドレスの 両方の ASA で生成されます。また、各パケットは複数の syslog（ICMP 接続およびローカル ホストの作成またはティアダウン）を生成するため、連続 ICMP syslog が生成されているように見えることがあります。IPV6 ネイバー エントリのリフレッシュ時間は、通常のデータ インターフェイスに設定可能ですが、フェールオーバー インターフェイスでは設定可能ではありません。ただし、この ICMP ネイバー探索トラフィックの CPU の影響はわずかです。

例：

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 002.7D1A.9472
```

ルーテッドモードおよびトランスペアレントモードのインターフェイスのモニタリング

インターフェイスの統計情報、ステータス、PPPoE をモニターできます。

（注） Firepower 、および Secure Firewall モデルの場合、一部の統計は ASA コマンドで表示されません。FXOS コマンドを使用して、より詳細なインターフェイス統計情報を表示する必要があります。

- /eth-uplink/fabric# **show interface**
- /eth-uplink/fabric# **show port-channel**
- /eth-uplink/fabric/interface# **show stats**

詳細については、『FXOS troubleshooting guide』を参照してください。

インターフェイス統計情報

- **show interface**

  インターフェイス統計情報を表示します。

- **show interface ip brief**

  インターフェイスの IP アドレスとステータスを表示します。

- **show bridge-group**

  指定されたインターフェイス、MAC アドレスと IP アドレスなどのブリッジグループ情報を表示します。

DHCP Information

- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface コマンドは、すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバー構成用に設定されている場合（DHCPv6 ステートレス サーバーの設定 （1042 ページ） を参照）、このコマンドはサー

バーによって使用されているDHCPv6プールをリストします。インターフェイスにDHCPv6アドレスクライアントまたはプレフィックス委任クライアントの設定がある場合、このコマンドは各クライアントの状態とサーバーから受信した値を表示します。特定のインターフェイスについて、DHCPサーバーまたはクライアントのメッセージの統計情報を表示できます。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
```

```
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp client [pd] statistics**

  show ipv6 dhcp client statistics コマンドは、DHCPv6 クライアント統計情報を表示し、送受信されたメッセージ数の出力を表示します。**show ipv6 dhcp client pd statistics** コマンドは、プレフィックス委任クライアントの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config)# show ipv6 dhcp client statistics

Protocol Exchange Statistics:
  Total number of Solicit messages sent:              4
  Total number of Advertise messages received:        4
  Total number of Request messages sent:              4
  Total number of Renew messages sent:                92
  Total number of Rebind messages sent:               0
  Total number of Reply messages received:            96
  Total number of Release messages sent:              6
  Total number of Reconfigure messages received:      0
  Total number of Information-request messages sent:  0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  8
  Total number of Message Validation errors in received messages: 0


ciscoasa(config)# show ipv6 dhcp client pd statistics

Protocol Exchange Statistics:
```

```
 Total number of Solicit messages sent:              1
 Total number of Advertise messages received:        1
 Total number of Request messages sent:              1
 Total number of Renew messages sent:                92
 Total number of Rebind messages sent:               0
 Total number of Reply messages received:            93
 Total number of Release messages sent:              0
 Total number of Reconfigure messages received:      0
 Total number of Information-request messages sent:  0

Error and Failure Statistics:


 Total number of Re-transmission messages sent:                   1
 Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics コマンドは、DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバーユニット間のトランザクションの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

  アクティブ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  スタンドバイ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

- **show ipv6 general-prefix**

  show ipv6 general-prefix コマンドは、DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスとそのプレフィックスの他のプロセスへの ASA 配布（「コンシューマ リスト」）を表示します。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config)# show ipv6 general-prefix
IPv6 Prefix Sample-PD, acquired via DHCP PD
  2005:abcd:ab03::/48 Valid lifetime 524, preferred lifetime 424
   Consumer List                Usage count
```

```
    BGP network command         1
    inside (Address command)    1
```

PPPoE

- **show ip address** *interface_name* **pppoe**

  現在の PPPoE クライアントの設定情報を表示します。

- **debug pppoe** {**event** | **error** | **packet**}

  PPPoE クライアントのデバッグをイネーブルにします。

- **show vpdn session**[**l2tp** |**pppoe**] [**id** *sess_id* |**packets** |**state** | **window**]

  PPPoE セッションのステータスを表示します。

  次に、このコマンドで提供される情報例を示します。

```
ciscoasa# show vpdn

Tunnel id 0, 1 active sessions
     time since change 65862 secs
     Remote Internet Address 10.0.0.1
    Local Internet Address 199.99.99.3
     6 packets sent, 6 received, 84 bytes sent, 0 received
Remote Internet Address is 10.0.0.1
     Session state is SESSION_UP
       Time since event change 65865 secs, interface outside
       PPP interface id is 1
       6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn session
PPPoE Session Information (Total tunnels=1 sessions=1)
Remote Internet Address is 10.0.0.1
  Session state is SESSION_UP
    Time since event change 65887 secs, interface outside
    PPP interface id is 1
    6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
ciscoasa# show vpdn tunnel
PPPoE Tunnel Information (Total tunnels=1 sessions=1)
Tunnel id 0, 1 active sessions
   time since change 65901 secs
   Remote Internet Address 10.0.0.1
   Local Internet Address 199.99.99.3
   6 packets sent, 6 received, 84 bytes sent, 0 received
ciscoasa#
```

IPv6 ネイバー探索

IPv6 ネイバー探索パラメータをモニターするには、次のコマンドを入力します。

- **show ipv6 interface**

このコマンドは、「外部」などのインターフェイス名を含む、IPv6用に設定されているインターフェイスのユーザビリティ状態を表示し、指定されたインターフェイスの設定を表示します。しかし、このコマンドは名前を除外し、IPv6が有効になっているすべてのインターフェイスの設定を表示します。コマンドの出力では、次の項目が表示されます。

- インターフェイスの名前とステータス
- リンクローカルおよびグローバルなユニキャスト アドレス
- インターフェイスが属するマルチキャスト グループ
- ICMP リダイレクトおよびエラー メッセージの設定
- ネイバー探索の設定
- コマンドが 0 に設定されているときの実際の時間
- 使用されているネイバー探索の到達可能時間

ルーテッドモードおよびトランスペアレントモードのインターフェイスの例

2 つのブリッジグループを含むトランスペアレント モードの例

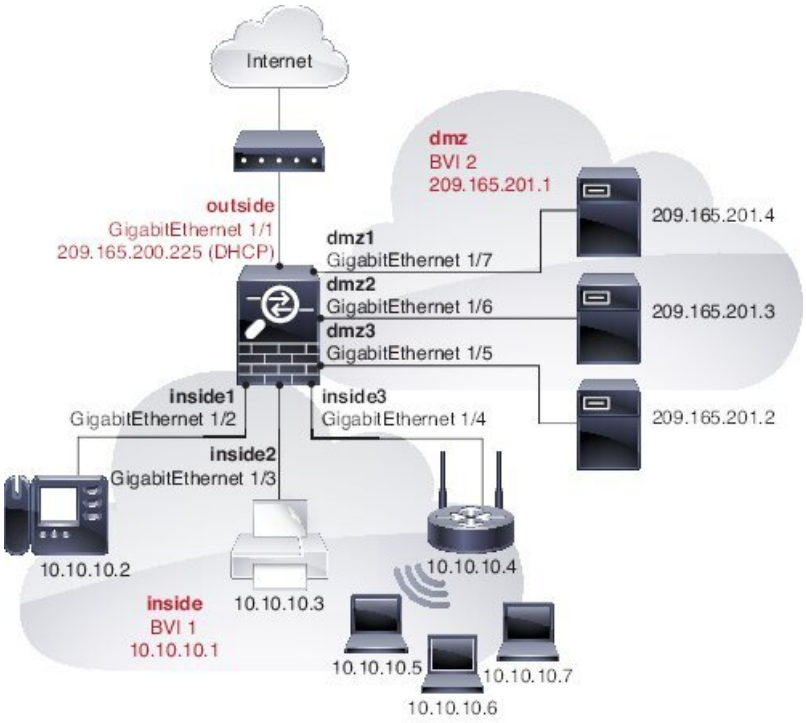
トランスペアレント モードの次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジグループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 0/1
  nameif outside1
  security-level 0
  bridge-group 1
  no shutdown
interface gigabitethernet 0/2
  nameif dmz1
  security-level 50
  bridge-group 1
  no shutdown
interface bvi 1
  ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2

interface gigabitethernet 1/0
  nameif inside2
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/1
  nameif outside2
```

```
  security-level 0
  bridge-group 2
  no shutdown
interface gigabitethernet 1/2
  nameif dmz2
  security-level 50
  bridge-group 2
  no shutdown
interface bvi 2
  ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9

interface management 0/0
  nameif mgmt
  security-level 100
  ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
  no shutdown
```

2 つのブリッジグループを含むスイッチド LAN セグメントの例

次の例では、3 つのインターフェイスのそれぞれと 1 つの通常の外部用ルーテッド インターフェイスに 2 つのブリッジグループを設定します。ブリッジグループ 1 は内部であり、ブリッジグループ 2 はパブリック Web サーバーが設定された dmz です。ブリッジグループのメンバーインターフェイスは、各メンバーのセキュリティ レベルが等しく、同一のセキュリティ通信が可能になっているため、ブリッジグループ内で自由に通信できます。内部メンバーのセキュリティ レベルが 100 で、dmz メンバーのセキュリティ レベルも 100 ですが、これらのセキュリティ レベルは BVI 間通信には適用されません。BVI のセキュリティ レベルのみ、BVI 間のトラフィックに影響します。BVI と外部のセキュリティ レベル（100、50、および 0）は、内部から dmz と内部から外部、および dmz から外部へのトラフィックを暗黙的に許可します。dmz 上のサーバーに対するトラフィックを許可するために、アクセス ルールが外部に適用されます。




```
interface gigabitethernet 1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface gigabitethernet 1/2
  nameif inside1
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/3
  nameif inside2
  security-level 100
  bridge-group 1
  no shutdown
interface gigabitethernet 1/4
  nameif inside3
  security-level 100
  bridge-group 1
  no shutdown
!
interface bvi 1
  nameif inside
  security-level 100
  ip address 10.10.10.1 255.255.255.0
!
interface gigabitethernet 1/5
  nameif dmz1
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/6
  nameif dmz2
```

```
  security-level 100
  bridge-group 2
  no shutdown
interface gigabitethernet 1/7
  nameif dmz3
  security-level 100
  bridge-group 2
  no shutdown
!
interface bvi 2
  nameif dmz
  security-level 50
  ip address 209.165.201.1 255.255.255.224
!
same-security-traffic permit inter-interface
!
# Assigns IP addresses to inside hosts
dhcpd address 10.10.10.2-10.10.10.200 inside
dhcpd enable inside
!
# Applies interface PAT for inside traffic going outside
nat (inside1,outside) source dynamic any interface
nat (inside2,outside) source dynamic any interface
nat (inside3,outside) source dynamic any interface
!
# Allows outside traffic to each server for specific applications
object network server1
  host 209.165.201.2
object network server2
  host 209.165.201.3
object network server3
  host 209.165.201.4
!
# Defines mail services allowed on server3
object-group service MAIL
  service-object tcp destination eq pop3
  service-object tcp destination eq imap4
  service-object tcp destination eq smtp
!
# Allows access from outside to servers on the DMZ
access-list SERVERS extended permit tcp any object server1 eq www
access-list SERVERS extended permit tcp any object server2 eq ftp
access-list SERVERS extended permit tcp any object server3 object-group MAIL
access-group SERVERS in interface outside
```

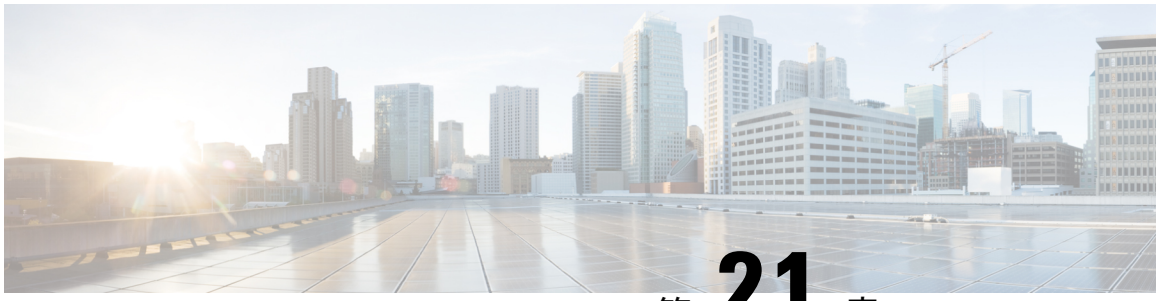
ルーテッドモードおよびトランスペアレントモードのインターフェイスの履歴

機能名	プラットフォーム リリース	機能情報
IPv6 ネイバー探索	7.0(1)	この機能が導入されました。 **ipv6 nd ns-interval**、**ipv6 nd ra-lifetime**、**ipv6 nd suppress-ra**、**ipv6 neighbor**、**ipv6 nd prefix**、**ipv6 nd dad-attempts**、**ipv6 nd reachable-time**、**ipv6 address**、および **ipv6 enforce-eui64** コマンドが導入されました。
トランスペアレント モードの IPv6 のサポート	8.2(1)	トランスペアレント ファイアウォール モードの IPv6 サポートが導入されました。
トランスペアレント モードのブリッジ グループ	8.4(1)	セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジグループにグループ化し、各ネットワークに1つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離されます。シングル モードまたはコンテキストごとに、それぞれ 4 つのインターフェイスからなる最大 8 個のブリッジ グループを設定できます。 次のコマンドが導入されました。**interface bvi**、**show bridge-group**
IPv6 DHCP リレーのアドレス設定フラグ	9.0(1)	コマンド **ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag** が導入されました。
トランスペアレント モードのブリッジ グループの最大数が 250 に増加	9.3(1)	ブリッジ グループの最大数が 8 個から 250 個に増えました。シングル モードでは最大 250 個、マルチ モードではコンテキストあたり最大 8 個のブリッジ グループを設定でき、各ブリッジ グループには最大 4 個のインターフェイスを追加できます。 **interface bvi** および **bridge-group** コマンドが変更されました。
トランスペアレント モードで、ブリッジ グループごとのインターフェイス数が最大で 64 に増加	9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	機能情報
IPv6 DHCP	9.6(2)	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバーから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバー：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次のコマンドが追加または変更されました。**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address autoconfig**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**

機能名	プラットフォーム リリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASAがルートの代わりにブリッジするインターフェイスのグループのことです。ASAは、ASAがファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレントファイアウォールモードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジグループの設定と、ブリッジグループ間およびブリッジグループとルーテッド インターフェイス間のルーティングを実行できます。ブリッジグループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジグループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ2スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVI は名前付きインターフェイスとなり、アクセス ルールやDHCPサーバーなどの一部の機能に、メンバーインターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッド モードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次のコマンドが変更されました。**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**

機能名	プラットフォーム リリース	機能情報
31 ビット サブネット マスク	9.7(1)	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネット に IP アドレスを設定できます。31 ビット サブネットには2つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバー リンクに必要なアドレスは2つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。この機能は、ブリッジグループ用のBVI、またはマルチキャストルーティングではサポートされていません。 次のコマンドを変更しました。**ip address**、**http**、**logging host**、**snmp-server**、**ssh**



第 21 章

高度なインターフェイス設定

この章では、インターフェイスのMACアドレスを設定する方法、最大伝送ユニット（MTU）を設定する方法、TCP最大セグメントサイズ（TCP MSS）を設定する方法、および同じセキュリティ レベルの通信を許可する方法について説明します。最高のネットワーク パフォーマンスを実現するには、正しい MTU と最大 TCP セグメント サイズの設定が不可欠です。

- インターフェイスの詳細設定について （973 ページ）
- MAC アドレスの手動設定 （978 ページ）
- MAC アドレスの自動割り当て （979 ページ）
- MTUおよび TCP MSS の設定 （980 ページ）
- 同一のセキュリティ レベル通信の許可 （982 ページ）
- インターフェイスの詳細設定の履歴 （983 ページ）

インターフェイスの詳細設定について

ここでは、インターフェイスの詳細設定について説明します。

MAC アドレスについて

手動でMACアドレスを割り当てて、デフォルトを上書きすることができます。マルチコンテキストモードでは、（コンテキストに割り当てられているすべてのインターフェイスの）一意の MAC アドレスと（サブインターフェイスの）シングルコンテキストモードを自動的に生成できます。.

（注） 親インターフェイスと同じ組み込みのMACアドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービスプロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスはMACアドレスに基づいて生成されるため、サブインターフェイスに一意のMACアドレスを割り当てることで、一意のIPv6 リンクローカルアドレスが可能になり、ASA デバイスで特定のインスタンスでのトラフィックの中断を回避できます。

デフォルトの MAC アドレス

デフォルトのMACアドレスの割り当ては、インターフェイスのタイプによって異なります。

- 物理インターフェイス：物理インターフェイスでは、Burned-In MAC Address を使用します。
- VLAN インターフェイス（Firepower 1010 および Secure Firewall 1210/1220）：ルーテッド ファイアウォール モード：すべての VLAN インターフェイスが MAC アドレスを共有します。接続スイッチがどれもこのシナリオをサポートできるようにします。接続スイッチに固有の MAC アドレスが必要な場合、手動で MAC アドレスを割り当てることができます。を参照してくださいMAC アドレスの手動設定 （978 ページ）。

  トランスペアレント ファイアウォール モード：各 VLAN インターフェイスに固有の MAC アドレスがあります。必要に応じて、手動で MAC アドレスを割り当てて、生成された MAC アドレスを上書きできます。を参照してくださいMAC アドレスの手動設定 （978 ページ）。
- EtherChannel（Firepower モデル）：EtherChannel の場合、そのチャネルグループに含まれるすべてのインターフェイスが同じ MAC アドレスを共有します。この機能によって、EtherChannel はネットワーク アプリケーションとユーザに対して透過的になります。ネットワーク アプリケーションやユーザから見えるのは 1 つの論理接続のみであり、個々のリンクのことは認識しないからです。ポートチャネルインターフェイスは、プールにある一意の MAC アドレスを使用します。インターフェイス メンバーシップは MAC アドレスに影響しません。
- EtherChannel（ASA モデル）：ポートチャネル インターフェイスは、最も小さいチャネル グループ インターフェイスの MAC アドレスをポートチャネル MAC アドレスとして使用します。または、ポートチャネル インターフェイスの MAC アドレスを設定することもできます。グループ チャネル インターフェイスのメンバーシップが変更された場合に備えて、一意の MAC アドレスを設定することをお勧めします。ポートチャネル MAC アドレスを提供していたインターフェイスを削除すると、そのポートチャネルの MAC アドレスは次に番号が小さいインターフェイスに変わるため、トラフィックが分断されます。
- サブインターフェイス: 物理インターフェイスのすべてのサブインターフェイスは同じ Burned-In MAC Addressを使用します。サブインターフェイスに一意のMACアドレスを割り当てることが必要になる場合があります。たとえば、サービス プロバイダーによっては、MACアドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、サブインターフェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカル アドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

自動 MAC アドレス

マルチコンテキストモードでは、自動生成によって、コンテキストに割り当てられたすべてのインターフェイスに一意のMACアドレスが割り当てられます。

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます（有効になっている場合）。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。

自動生成されたアドレス（プレフィックスを使用するとき）は A2 で始まるため、自動生成も使用する予定のときは手動 MAC アドレスを A2 で始めることはできません。

ASAは、次の形式を使用して MACアドレスを生成します。

A2*xx.yyzz.zzzz*

*xx.yy*はユーザ定義プレフィックスまたはインターフェイスMACアドレスの最後の2バイトに基づいて自動生成されたプレフィックスであり、*zz.zzzz* はASAによって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例としてたとえば、プレフィックス77を設定すると、ASAは77を16進数値004D (*yyxx*)に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように逆転されます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

（注） プレフィックスのないMACアドレス形式は、従来のバージョンです。従来の形式に関する詳細については、コマンドリファレンスの**mac-address auto**コマンドを参照してください。

MTU について

MTU は、ASA が特定のイーサネット インターフェイスで送信可能な最大フレームペイロードサイズを指定します。MTU の値は、イーサネット ヘッダー、VLAN タギング、またはその他のオーバーヘッドを含まないフレーム サイズです。たとえば、MTU を 1500 に設定すると、予想されるフレーム サイズはヘッダーを含めて 1518 バイトで、VLAN を使用する場合は 1522 です。これらのヘッダーに対応するために MTU 値を高く設定しないでください。

VXLAN または Geneve については、イーサネットデータグラム全体がカプセル化されるため、新しい IP パケットは大きくなり、より大きな MTU が必要となります。そのため、ASA VTEP 送信元インターフェイスの MTU をネットワーク MTU + 54 バイト（VXLAN）、または + 306 バイト（Geneve）に設定する必要があります。

パス MTU ディスカバリ

ASA は、Path MTU Discovery（RFC 1191 の定義に従う）をサポートします。つまり、2 台のホスト間のネットワーク パス内のすべてのデバイスで MTU を調整できます。したがってパスの最小 MTU の標準化が可能です。

デフォルト MTU

ASA のデフォルト MTU は、1500 バイトです。この値には、イーサネット ヘッダー、VLAN タギングや他のオーバーヘッド分の 18～22 バイトは含まれません。

VTEP 送信元インターフェイスの VXLAN を有効にし、MTU が 1554 バイト未満の場合、ASA は自動的に MTU を 1554 バイトに増やします。この場合、イーサネット データグラム全体がカプセル化されるため、新しいパケットのサイズが大きくなるため、より大きな MTU が必要になります。一般的には、ASA 送信元インターフェイス MTU をネットワーク MTU + 54 バイトに設定する必要があります。

MTU とフラグメンテーション

IPv4 の場合、出力 IP パケットが、指定された MTU より大きい場合、2 つ以上のフレームにフラグメント化されます。フラグメントは送信先（場合によっては中継先）で組立て直されます。フラグメント化はパフォーマンス低下の原因となります。IPv6 の場合、通常、パケットのフラグメント化は許可されません。したがってフラグメント化を避けるために、IP パケットを MTU サイズ以内におさめる必要があります。

TCP パケットの場合、通常、エンドポイントが MTU を使用して、TCP 最大セグメント サイズ（たとえば、MTU - 40 など）を判別します。途中で TCP ヘッダーが追加される場合（たとえば、サイト間 VPN トンネルなど）、トンネリング エンティティによって TCP MSS を調整する必要があります。TCP MSS について （977 ページ）を参照してください。

UDP または ICMP の場合、アプリケーションは、フラグメンテーションを避けるために、MTU を考慮する必要があります。

（注） ASA はメモリに空きがある限り、設定された MTU よりも大きいフレームを受信します。

MTU とジャンボ フレーム

MTU が大きくなると、より大きなパケットを送信できます。大きなパケットはネットワークにとってより効率的です。次のガイドラインを参照してください。

- トラフィックパスの MTU の一致：すべての ASA インターフェイスの MTU と、トラフィックパス上のその他のデバイスインターフェイスの MTU を同じ値に設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボフレームへの対応：ジャンボフレームが有効な場合、MTU を 9,000 バイト以上に設定できます。最大値はモデルによって異なります。

TCP MSS について

TCP 最大セグメント サイズ（MSS）とは、あらゆる TCP と IP ヘッダーが追加される前の TCP ペイロードのサイズです。UDP パケットは影響を受けません。接続を確立するときのスリーウェイ ハンドシェイク中に、クライアントとサーバは TCP MSS 値を交換します。

」を参照してください。デフォルトで、最大 TCP MSS は 1,380 バイトに設定されます。この設定は、ASA が IPsec VPN カプセル化のパケットサイズを大きくする必要がある場合に役立ちます。ただし、非 IPsec エンドポイントでは、ASA の最大 TCP MSS を無効化する必要があります。

最大 TCP MSS を設定すると、接続のいずれかのエンドポイントが ASA で設定した値よりも大きな TCP MSS を要求した場合に、ASA は要求パケットの TCP MSS を ASA の最大値で上書きします。ホストやサーバが TCP MSS を要求しない場合、ASA は RFC 793 のデフォルト値 536 バイト（IPv4）または 1220 バイト（IPv6）を想定しますが、パケットを変更することはありません。たとえば、MTU をデフォルトの 1500 バイトのままにします。ホストは、1500 バイトの MSS から TCP および IP のヘッダー長を減算して、MSS を 1460 バイトに設定するように要求します。ASA の最大 TCP MSS が 1380（デフォルト）の場合は、ASA は TCP 要求パケットの MSS 値を 1380 に変更します。サーバは、1380 バイトのペイロードを含むパケットを送信します。ASA はさらに 120 バイトのヘッダーをパケットに追加しますが、それでも 1500 の MTU サイズに収まります。

TCP の最小 MSS も設定できます。ホストまたはサーバが非常に小さい TCP MSS を要求した場合、ASA は値を調整します。デフォルトでは、最小 TCP MSS は有効ではありません。

SSL VPN 接続用を含む to-the-box トラフィックには、この設定は適用されません。ASA は MTU を使用して、TCP MSS を導き出します。MTU - 40（IPv4）または MTU - 60（IPv6）となります。

デフォルト TCP MSS

デフォルトでは、ASA の最大 TCP MSS は 1380 バイトです。このデフォルトは、ヘッダーが最大 120 バイトの IPv4 IPsec VPN 接続に対応しています。この値は、MTU の デフォルトの 1500 バイト内にも収まっています。

TCP MSS の推奨最大設定

デフォルトでは TCP MSS は、ASA が IPv4 IPsec VPN エンドポイントとして機能し、MTU が 1500 バイトであることを前提としています。ASA が IPv4 IPsec VPN エンドポイントとして機能している場合は、最大 120 バイトの TCP および IP ヘッダーに対応する必要があります。

MTU 値を変更して、IPv6 を使用するか、または IPsec VPN エンドポイントとして ASA を使用しない場合は、。

次のガイドラインを参照してください。

- 通常のトラフィック：TCP MSS の制限を無効にし、接続のエンドポイント間で確立された値を受け入れます。一般に接続エンドポイントは MTU から TCP MSS を取得するため、非 IPsec パケットは通常この TCP MSS を満たしています。

- IPv4 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 120 に設定します。たとえば、ジャンボ フレームを使用しており、MTU を 9000 に設定すると、新しい MTU を使用するために、TCP MSS を 8880 に設定する必要があります。
- IPv6 IPsec エンドポイント トラフィック：最大 TCP MSS を MTU - 140 に設定します。

インターフェイス間通信

同じセキュリティ レベルのインターフェイスで相互通信を許可する利点としては、次のものがあります。

- 101 より多い数の通信インターフェイスを設定できます。

  各インターフェイスで異なるセキュリティ レベルを使用したときに、同一のセキュリティ レベルにインターフェイスを割り当てないと、各レベル（0～100）に1つのインターフェイスしか設定できません。

- ACL がなくても同じセキュリティ レベルのインターフェイスすべての間で自由にトラフィックが流れるようにできます。

同じセキュリティ インターフェイス通信をイネーブルにした場合でも、異なるセキュリティ レベルで通常どおりインターフェイスを設定できます。

インターフェイス内通信（ルーテッド ファイアウォール モード）

インターフェイス内通信は、インターフェイスに入ってくる VPN トラフィックに対して使用できますが、その場合は同じインターフェイスのルートから外されます。この場合、VPN トラフィックは暗号化解除されたり、別の VPN 接続のために再度暗号化されたりする場合があります。たとえば、ハブアンドスポーク VPN ネットワークがあり、ASA がハブ、リモート VPN ネットワークがスポークの場合、あるスポークが別のスポークと通信するためには、トラフィックは ASA に入ってから他のスポークに再度ルーティングされる必要があります。

（注） この機能で許可されたすべてのトラフィックは、引き続きファイアウォール規則に従います。リターン トラフィックが ASA を通過できない原因となるため、非対称なルーティング状態にしないよう注意してください。

MAC アドレスの手動設定

MAC アドレスを手動で割り当てる必要がある場合は、この手順を使用して実行できます。

親インターフェイスと同じ組み込みの MAC アドレスを使用するので、ASA で定義されたサブインターフェイスに一意の MAC アドレスを割り当てることもできます。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス制御を行う場合があります。また、IPv6 リンクローカルアドレスは MAC アドレスに基づいて生成されるため、サブインター

フェイスに一意の MAC アドレスを割り当てることで、一意の IPv6 リンクローカルアドレスが可能になり、ASA で特定のインスタンスでのトラフィックの中断を避けることができます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
```

ステップ 2 プライベート MAC アドレスをこのインターフェイスに割り当てます。

mac-address *mac_address* [**standby** *mac_address*]

例：

```
ciscoasa(config-if)# mac-address 000C.F142.4CDE
```

mac_address は、H.H.H 形式で指定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。MAC アドレスはマルチキャスト ビット セットを持つことはできません。つまり、左から 2 番目の 16 進数字を奇数にすることはできません。

自動生成された MAC アドレスも使用する場合、手動で割り当てる MAC アドレスの最初の 2 バイトには A2 を使用できません。

フェールオーバーで使用する場合は、**スタンバイ** MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

MAC アドレスの自動割り当て

この項では、MAC アドレスの自動生成の設定方法について説明します。マルチ コンテキスト モードの場合、この機能によって、コンテキストに割り当てられたすべてのインターフェイス

タイプに一意の MAC アドレスが割り当てられます。 シングル モードでは、この機能によって、VLAN サブインターフェイスに一意の MAC アドレスが割り当てられます。

始める前に

- インターフェイスの **nameif** コマンドを設定すると、ただちに新規MACアドレスが生成されます。インターフェイスを設定した後でこの機能をイネーブルにした場合は、イネーブルにした直後に、すべてのインターフェイスの MAC アドレスが生成されます。この機能をディセーブルにすると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。
- 生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、インターフェイスの MAC アドレスを手動で設定できます。
- マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。

手順

プライベート MAC アドレスを各インターフェイスに自動的に割り当てます。

mac-address auto [**prefix** *prefix*]

プレフィックスを入力しない場合は、ASA によって、インターフェイス MAC アドレスの最後の 2 バイトに基づいてプレフィックスが自動生成されます。

手動でプレフィックスを入力する場合は、*prefix* に 0 ～ 65535 の 10 進数値を指定します。このプレフィックスは 4 桁の 16 進数値に変換され、MAC アドレスの一部として使用されます。

例：

```
ciscoasa(config)# mac-address auto prefix 19
```

MTUおよび TCP MSS の設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

- MTU を 1500 より多く増やすには、ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000）（833 ページ）に従って、ジャンボ フレームをイネーブルにします。

手順

ステップ 1 MTU を設定します。最小値と最大値は、プラットフォームによって異なります。

mtu *interface_name bytes*

例：

```
ciscoasa(config-if)# mtu inside ?

configure mode commands/options:
  <64-9198>  MTU bytes
ciscoasa(config)# mtu inside 9000
```

デフォルトは 1500 バイトです。

（注）
ポートチャネル インターフェイスに MTU を設定すると、ASA は、この設定をすべてのメンバー インターフェイスに適用します。

ジャンボフレームをサポートする一部のモデルでは、インターフェイスに 1500 よりも大きな値を入力する場合、ジャンボフレームのサポートをイネーブルにする必要があります。ジャンボフレームサポートの有効化（ASA 仮想、ISA 3000）（833 ページ）を参照してください。

ステップ 2 最大 TCP セグメントサイズをバイト単位で設定します（48 ～任意の最大値）。

sysopt connection tcpmss [**minimum**] バイト

例：

```
ciscoasa(config)# sysopt connection tcpmss 8500
ciscoasa(config)# sysopt connection tcpmss minimum 1290
```

デフォルト値は 1380 バイトです。この機能は、**0** バイトに設定することによって無効にできます。

minimum キーワードには、48 ～ 65535 の間で *bytes* の値未満にならないように最大セグメントサイズを設定します。minimum 機能は、デフォルトでディセーブルです（0 に設定）。

ステップ 3 未処理 TCP セグメントの最大数を設定します。

sysopt connection tcp-max-unprocessed-seg *unprocessed segments*

例：

```
ciscoasa(config)# sysopt connection tcp-max-unprocessed-seg 7
```

デフォルト値は、6 です。範囲は 6 ～ 24 です。

例

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、非 VPN トラフィックの TCP MSS をディセーブルにします（TCP MSS を 0 に設定、すなわち無制限とすることによって行います）。

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 0
```

下記の例では、ジャンボ フレームをイネーブルにし、すべてのインターフェイスの MTU を増加し、VPN トラフィックの TCP MSS を 9078 に変更します（MTU から 120 を差し引きます）。

```
mtu inside 9198
mtu outside 9198
sysopt connection tcpmss 9078
```

同一のセキュリティ レベル通信の許可

デフォルトでは、同じセキュリティ レベルのインターフェイスは相互に通信することができません。また、パケットは同じインターフェイスを出入りすることができません。この項では、複数のインターフェイスが同じセキュリティ レベルの場合にインターフェイス間通信をイネーブルにする方法と、インターフェイス内通信をイネーブルにする方法について説明します。

手順

ステップ 1 相互通信を可能にするために同じセキュリティ レベルのインターフェイスをイネーブルにします。

same-security-traffic permit inter-interface

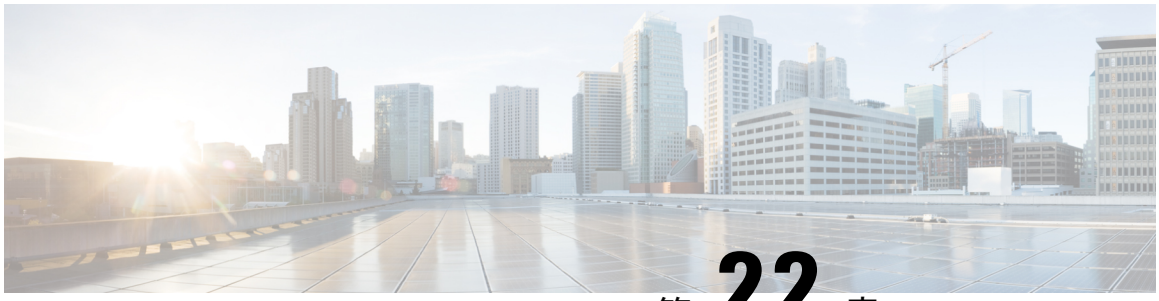
ステップ 2 同じインターフェイスに接続されたホスト間の通信をイネーブルにします。

same-security-traffic permit intra-interface

インターフェイスの詳細設定の履歴

表 *32 :* インターフェイスの詳細設定の履歴

機能名	リリース	機能情報
最大 MTU が 9198 バイトになりました	9.1(6)、9.2(1)	ASA で使用できる最大の MTU は 9198 バイトです（CLI のヘルプでご使用のモデルの正確な最大値を確認してください）。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。 次のコマンドが変更されました。**mtu**
Firepower 4100/9300 シャーシ の ASA のMTU サイズ増加	9.6(2)	Firepower 4100 および 9300 で、最大 MTU を 9184 バイトに設定できます。これまでは 9000 バイトが最大でした。この MTU は FXOS 2.0.1.68 以降でサポートされます。 次のコマンドが変更されました。**mtu**
シングル コンテキスト モード用の一意の MAC アドレス生成	9.8(3), 9.8(4), 9.9(2)	シングル コンテキスト モードで VLAN サブインターフェイスの一意の MAC アドレス生成を有効にできるようになりました。通常、サブインターフェイスはメインインターフェイスと同じ MAC アドレスを共有します。IPv6 リンクローカル アドレスは MAC アドレスに基づいて生成されるため、この機能により一意の IPv6 リンクローカル アドレスが許可されます。 新規または変更されたコマンド：**mac-address auto**
Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。	9.17(1)	Secure Firewall 3100 の自動ネゴシエーションは、1 ギガビット以上のインターフェイスで有効または無効にすることができます。他のモデルの SFP ポートの場合、**no speed nonegotiate** オプションは速度を 1000 Mbps に設定します。新しいコマンドは、自動ネゴシエーションと速度を個別に設定できることを意味します。 新規/変更されたコマンド：**negotiate-auto**



第 22 章

トラフィック ゾーン

トラフィック ゾーンに複数のインターフェイスを割り当てることができます。これにより、既存のフローのトラフィックがゾーン内のインターフェイスで ASA に出入りできるようになります。この機能により、ASA 上での等コスト マルチパス（ECMP）のルーティングや、ASA へのトラフィックの複数のインターフェイスにわたる外部ロードバランシングが可能になります。

- トラフィック ゾーンの概要 （985 ページ）
- トラフィック ゾーンの前提条件 （992 ページ）
- トラフィック ゾーンのガイドライン （994 ページ）
- トラフィック ゾーンの設定 （995 ページ）
- トラフィック ゾーンのモニタリング （996 ページ）
- トラフィック ゾーンの例 （999 ページ）
- トラフィック ゾーンの履歴 （1002 ページ）

トラフィック ゾーンの概要

この項では、ネットワークでトラフィック ゾーンを使用する方法について説明します。

ゾーン分割されていない動作

アダプティブ セキュリティ アルゴリズムは、トラフィックの許可または拒否を決定する際に、パケットの状態を考慮します。フローに適用されたパラメータの 1 つは、トラフィックが同じインターフェイスに出入りすることです。異なるインターフェイスに入る既存のフローのトラフィックは、ASA によってドロップされます。

トラフィック ゾーンにより、複数のインターフェイスを 1 つにまとめることができるため、ゾーン内の任意のインターフェイスに出入りするトラフィックがアダプティブ セキュリティ アルゴリズムのセキュリティ チェックを満たすことができるようになります。

関連トピック

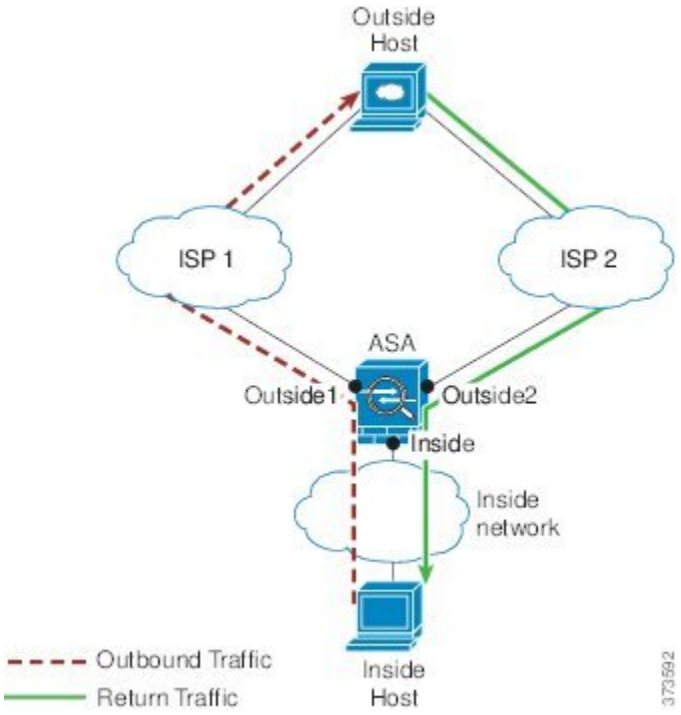
ステートフル インスペクションの概要 （8 ページ）

ゾーンを使用する理由

ゾーンを使用して、複数のルーティングのシナリオに対応することができます。

非対称ルーティング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。宛先ネットワークの非対称ルーティングが原因で、Outside2 インターフェイスの ISP 2 からリターン トラフィックが到達しています。

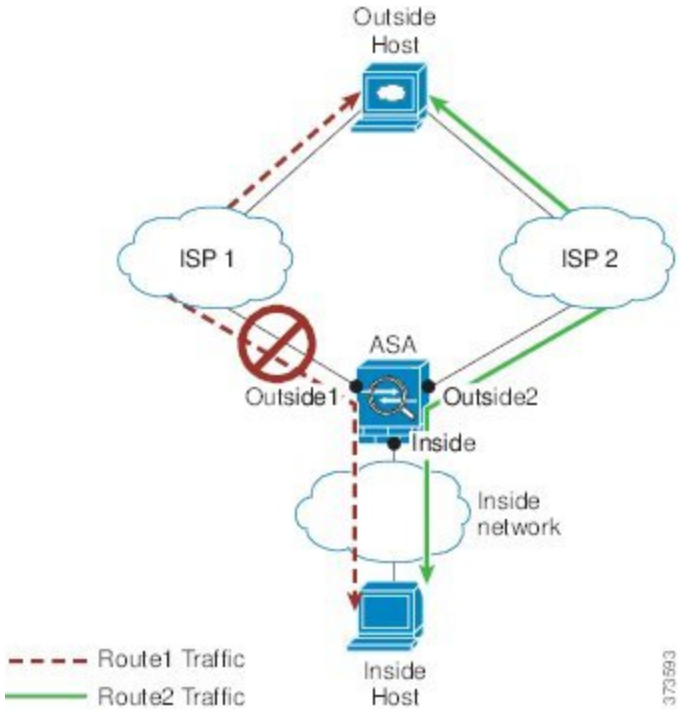


ゾーン分割されていない場合の問題：ASA は、インターフェイスごとに接続テーブルを保持します。リターン トラフィックが Outside2 に到達すると、そのトラフィックは、接続テーブルに一致しないため、ドロップされます。ASA クラスタに関しては、クラスタが同一ルータに対して複数の隣接関係（アジャセンシー）を持つ場合、非対称ルーティングは許容できないトラフィック紛失の原因となることがあります。

ゾーン分割されたソリューション：ASAは、ゾーンごとに接続テーブルを保持します。Outside1 と Outside2 を 1 つのゾーンにグループ化した場合、リターン トラフィックが Outside2 に到達すると、ゾーンごとの接続テーブルに一致するため、接続が許可されます。

紛失したルート

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。Outside1 と ISP 1 間でルートが紛失または移動したため、トラフィックは ISP 2 を経由する別のルートを通る必要があります。

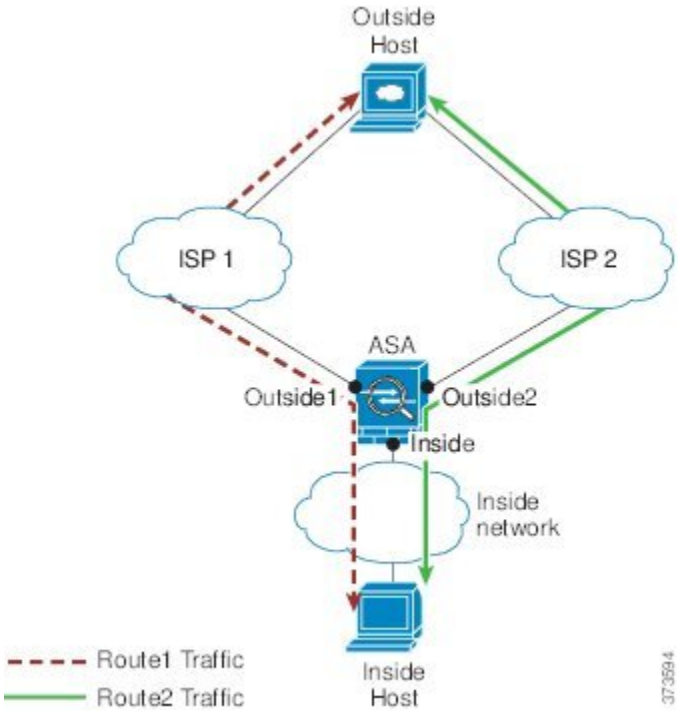


ゾーン分割されていない場合の問題：内部ホストと外部ホスト間の接続が削除されるため、新しい次善のルートを使用して新しい接続を確立する必要があります。UDP の場合、1 つのパケットがドロップダウンすると新しいルートが使用され、UDP がない場合は、新しい接続を再確立する必要があります。

ゾーン分割されたソリューション：ASA は、紛失したルートを検出し、フローを ISP 2 経由の新しいパスに切り替えます。トラフィックは、パケットがドロップすることなくシームレスに転送されます。

ロード バランシング

次のシナリオでは、Outside1 インターフェイスの ISP 1 を経由する内部ホストと外部ホストの間に接続が確立されています。2 番目の接続が Outside2 の ISP 2 を経由する等コスト ルートを介して確立されています。



ゾーン分割されていない場合の問題：インターフェイス間でロードバランシングを行うことができません。可能なのは、1つのインターフェイスの等コストルートによるロードバランスだけです。

ゾーン分割されたソリューション：ASAは、ゾーン内のすべてのインターフェイスで最大8つの等コスト ルート間の接続をロードバランスすることができます。

ゾーンごとの接続テーブルおよびルーティング テーブル

ASAは、トラフィックがゾーンのインターフェイスのいずれかに到達できるようにゾーンごとの接続テーブルを保持します。また、ASAは、ECMPサポート用にゾーンごとのルーティングテーブルも保持します。

ECMP ルーティング

ASA では、等コスト マルチパス（ECMP）ルーティングをサポートしています。

ゾーン分割されていない ECMP サポート

ゾーンがない場合は、インターフェイスごとに最大8つの等コストのスタティック ルートタまたはダイナミック ルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスに 3 つのデフォルト ルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
```

```
route outside 0 0 10.1.1.4
```

この場合、トラフィックは10.1.1.2、10.1.1.3、および10.1.1.4間の外部インターフェイスでロードバランシングされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

ECMPは複数のインターフェイス間ではサポートされないため、異なるインターフェイスで同じ宛先へのルートを定義することはできません。上記のルートのいずれかを設定すると、次のルートは拒否されます。

```
route outside2 0 0 10.2.1.1
```

ゾーン分割された ECMP サポート

ゾーンがある場合は、ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストのスタティック ルートまたはダイナミック ルートを設定できます。たとえば、次のようにゾーン内の 3 つのインターフェイ間に 3 つのデフォルト ルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、自動的に等コスト ルートを設定できます。ASA では、より堅牢なロード バランシング メカニズムを使用してインターフェイス全体でトラフィックをロードバランスします。

ルートが紛失した場合、ASA はフローをシームレスに別のルートに移動させます。

接続のロード バランス方法

ASA では、パケットの 6 タプル（送信元 IP アドレス、宛先 IP アドレス、送信元ポート、宛先ポート、プロトコル、入力インターフェイス）から生成されたハッシュを使用して、等コスト ルート間の接続をロードバランスします。ルートが紛失しない限り、接続は接続期間中、インターフェイスで継続されます。

接続内のパケットは、ルート間でロードバランスされません。接続では、そのルートが紛失しない限り、単一ルートを使用します。

ASA では、ロード バランシング時にインターフェイス帯域幅やその他のパラメータを考慮しません。同じゾーン内のすべてのインターフェイスが MTU、帯域幅などの同じ特性を持つことを確認します。

ロード バランシング アルゴリズムは、ユーザー設定可能ではありません。

別のゾーンのルートへのフォール バック

ルートがインターフェイスで紛失したときにゾーン内で使用可能な他のルートがない場合、ASA では、異なるインターフェイス/ゾーンからのルートを使用します。このバックアップ

ルートを使用した場合、ゾーン分割されていないルーティングのサポートと同様にパケットのドロップが発生することがあります。

インターフェイスベースのセキュリティ ポリシーの設定

ゾーンを使用すると、トラフィックはゾーン内のすべてのインターフェイスで出入りを許可されますが、セキュリティ ポリシー自体（アクセス ルール、NAT など）は、ゾーン単位ではなく、インターフェイス単位で適用されます。ゾーン内のすべてのインターフェイスに同じセキュリティ ポリシーを設定すると、そのトラフィックの ECMP およびロード バランシングを適切に実装できます。必須のパラレルインターフェイス設定の詳細については、トラフィック ゾーンの前提条件 （992 ページ）を参照してください。

トラフィック ゾーンでサポートされるサービス

次のサービスがゾーンでサポートされています。

- アクセル ルール
- NAT
- QoS トラフィック ポリシングを除くサービス ルール。
- Routing

完全にゾーン分割されたサポートは利用できませんが、To-the-Box および From-the-Box トラフィック （991 ページ）に示した to-the-box サービスおよび from-the-box サービスを設定することもできます。

トラフィック ゾーンのインターフェイスに他のサービス（VPN、ボットネット トラフィック フィルタなど）を設定しないでください。これらのサービスは、想定どおりに機能または拡張しないことがあります。

（注） セキュリティ ポリシーの設定方法の詳細については、トラフィック ゾーンの前提条件 （992 ページ）を参照してください。

セキュリティ レベル

ゾーンに最初に追加するインターフェイスによってゾーンのセキュリティ レベルが決まります。追加のインターフェイスは、すべて同じセキュリティ レベルにする必要があります。ゾーン内のインターフェイスのセキュリティ レベルを変更するには、1 つのインターフェイスを除くすべてのインターフェイスを削除してからセキュリティ レベルを変更し、インターフェイスを再度追加します。

フローのプライマリおよび現在のインターフェイス

各接続フローは、最初の入出力インターフェイスに基づいて構築されます。これらのインターフェイスは、プライマリ インターフェイスです。

ルート変更または非対称ルーティングにより、新しい出力インターフェイスが使用されている場合は、新しいインターフェイスが現在のインターフェイスになります。

ゾーンの追加または削除

ゾーンにインターフェイスを割り当てる場合、そのインターフェイスのすべての接続が削除されます。接続を再確立する必要があります。

ゾーンからインターフェイスを削除する場合、そのインターフェイスをプライマリ インターフェイスとしているすべての接続が削除されます。接続を再確立する必要があります。そのインターフェイスが現在のインターフェイスの場合、ASA は接続をプライマリ インターフェイスに戻します。ゾーンのルート テーブルも更新されます。

ゾーン内トラフィック

トラフィックがあるインターフェイスに入り、同じゾーンの別のインターフェイスから出ることができるようにするには、**same-security permit intra-interface** コマンドをイネーブルにしてトラフィックが同じインターフェイスを出入りできるようにし、さらに、**same-security permit inter-interface** コマンドをイネーブルにして same-security インターフェイス間のトラフィックを許可します。このように設定しない場合、フローは同じゾーンの2つのインターフェイス間をルーティングできません。

To-the-Box および From-the-Box トラフィック

- management-only インターフェイスまたは management-access インターフェイスをゾーンに追加することはできません。
- ゾーンの通常のインターフェイスでの管理トラフィックでは、既存のフローの非対称ルーティングのみがサポートされます。ECMP サポートはありません。
- 1 つのゾーン インターフェイスにのみ管理サービスを設定できますが、非対称ルーティング サポートを利用するには、すべてのインターフェイスでそれを設定する必要があります。構成がすべてのインターフェイスでパラレルである場合でも、ECMP はサポートされません。
- ASA は、ゾーンで次の To-the-Box および From-the-Box サービスをサポートします。
  - Telnet
  - SSH
  - HTTPS
  - SNMP

- Syslog

ゾーン内の IP アドレスのオーバーラップ

ゾーン分割されていないインターフェイスの場合、ASA では、NAT が正しく設定されていれば、インターフェイスでの IP アドレス ネットワークのオーバーラップをサポートします。ただし、同じゾーンのインターフェイスでは、ネットワークのオーバーラップはサポートされていません。

トラフィック ゾーンの前提条件

- 名前、IPアドレス、およびセキュリティ レベルを含むすべてのインターフェイスパラメータを設定します。ゾーンのすべてのインターフェイスでセキュリティ レベルが一致する必要があることに注意してください。帯域幅および他のレイヤ2のプロパティについては、インターフェイスのようにグループ化する計画を立てる必要があります。
- 次のサービスをゾーンのすべてのインターフェイスで一致するように設定します。
  - アクセス ルール：同じアクセス ルールをゾーンのすべてのメンバー インターフェイスに適用するか、グローバル アクセス ルールを使用します。

    次に例を示します。

    ```
    access-list ZONE1 extended permit tcp any host WEBSERVER1 eq 80
    access-group ZONE1 in interface outside1
    access-group ZONE1 in interface outside2
    access-group ZONE1 in interface outside3
    ```

  - NAT：ゾーンのすべてのメンバー インターフェイスで同じ NAT ポリシーを設定するか、グローバル NAT ルールを使用します（つまり、「any」を使用して NAT ルールでゾーンのインターフェイスを表します）。

    インターフェイス PAT はサポートされていません。

    次に例を示します。

    ```
    object network WEBSERVER1
      host 10.9.9.9 255.255.255.255
      nat (inside,any) static 209.165.201.9
    ```

（注） インターフェイス固有の NAT および PAT プールを使用したときに元のインターフェイスの障害が発生した場合、ASA は接続を切り替えることはできません。

インターフェイス固有の PAT プールを使用する場合、同じホストからの複数の接続は、別のインターフェイスにロードバランスし、別のマッピング IP アドレスを使用することがあります。この場合、複数の同時接続を使用するインターネット サービスが正しく機能しないことがあります。

- サービス ルール：グローバル サービス ポリシーを使用するか、ゾーンの各インターフェイスに同じポリシーを割り当てます。

  QoS トラフィック ポリシングはサポートされていません。

  次に例を示します。

```
service-policy outside_policy interface outside1
service-policy outside_policy interface outside2
service-policy outside_policy interface outside3
```

（注） VoIP インスペクションでは、ゾーンのロード バランシングにより、順序が正しくないパケットが増加する可能性があります。この状況は、異なるパスを通る先行パケットの前に後行パケットが ASA に到達する可能性があるために発生することがあります。順序が正しくないパケットには、次のような症状があります。

- キューイングを使用した場合に、中間ノード（ファイアウォールと IDS）および受信エンド ノードでメモリ使用率が高い。
- ビデオまたは音声の品質が低い。

これらの影響を軽減するには、VoIP トラフィックのロード分散にのみ IP アドレスを使用することを推奨します。

- ECMP ゾーン機能を考慮してルーティングを設定します。

トラフィック ゾーンのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでだけサポートされています。トランスペアレント ファイアウォール モードまたはルーテッド モードのブリッジグループ インターフェイスはサポートされません。

フェールオーバー

- フェールオーバー リンクまたはステート リンクをゾーンに追加することはできません。
- アクティブ/アクティブ フェールオーバー モードでは、各コンテキストのインターフェイスを非対称ルーティング（ASR）グループに割り当てることができます。このサービスにより、ピア装置の同様のインターフェイスに戻るトラフィックを元の装置に復元することができます。コンテキスト内に ASR グループとトラフィック ゾーンの両方を設定することはできません。コンテキスト内にゾーンを設定した場合、どのコンテキスト インターフェイスも ASR グループに含めることはできません。ASR グループに関する詳細については、非対称にルーティングされたパケットのサポートの設定（アクティブ/アクティブ モード）（365 ページ）を参照してください。
- 各接続のプライマリ インターフェイスのみがスタンバイ装置に 複製されます。現在のインターフェイスは複製されません。スタンバイ装置がアクティブになると、その装置によって必要に応じて現在の新しいインターフェイスが割り当てられます。

クラスタ

- クラスタ制御リンクをゾーンに追加することはできません。

モデルのガイドライン

EtherChannel で Firepower 1010 または Cisco Secure Firewall 1210/1220 のスイッチポートまたは VLAN インターフェイスを使用することはできません。

その他のガイドライン

- 最大 256 ゾーンを作成できます。
- 次のタイプのインターフェイスをゾーンに追加できます。
  - 物理
  - VLAN
  - EtherChannel
- 次のタイプのインターフェイスは追加できません。

- 管理専用
- 管理アクセス
- フェールオーバーまたはステート リンク
- クラスタ制御リンク
- EtherChannel インターフェイスのメンバーインターフェイス
- VNI（さらに、通常のデータ インターフェイスが nve 専用としてマークされている場合、ゾーンのメンバーにすることはできません）
- BVI、またはブリッジグループ メンバー インターフェイス。

- 1 つのインターフェイスがメンバーになることができるゾーンは 1 つだけです。
- ゾーンごとに最大 8 つのインターフェイスを含めることができます。
- ECMP の場合、ゾーンのすべてのインターフェイス間で、ゾーンごとに最大 8 つの等コスト ルートを追加できます。また、8 ルート制限の一部として 1 つのインターフェイスに複数のルートを設定することもできます。
- ゾーンにインターフェイスを追加すると、それらのインターフェイスのすべてのスタティック ルートが削除されます。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。
- ASA では、個別のインターフェイスにロードバランシングされるフラグメントについて、フラグメント化されたパケットのリアセンブルはサポートしていません。これらのフラグメントはドロップされます。
- PIM/IGMP マルチキャストルーティングは、ゾーン内のインターフェイスではサポートされません。

トラフィック ゾーンの設定

名前を付けたゾーンを設定し、インターフェイスをそのゾーンに割り当てます。

手順

ステップ 1 ゾーンを追加します。

zone *name*

例：

```
zone outside
```

ゾーン名は最大 48 文字です。

ステップ 2 インターフェイスをゾーンに追加します。

interface *id* **zone-member** *zone_name*

例：

```
interface gigabitethernet0/0
  zone-member outside
```

ステップ 3 インターフェイスをさらにゾーンに追加します。これらのインターフェイスのセキュリティ レベルが、追加した最初のインターフェイスのセキュリティ レベルと同じであることを確認します。

例：

```
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

例

次の例では、4 つのメンバー インターフェイスを含む外部ゾーンを設定します。

```
zone outside
interface gigabitethernet0/0
  zone-member outside
interface gigabitethernet0/1
  zone-member outside
interface gigabitethernet0/2
  zone-member outside
interface gigabitethernet0/3
  zone-member outside
```

トラフィック ゾーンのモニタリング

この項では、トラフィック ゾーンをモニターする方法について説明します。

ゾーン情報

- **show zone** [*name*]

  ゾーン ID、コンテキスト、セキュリティ レベル、およびメンバーを表示します。

show zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show zone outside-zone

Zone: zone-outside id: 2
Security-level: 0
Context: test-ctx
 Zone Member(s) : 2
  outside1       GigabitEthernet0/0
  outside2       GigabitEthernet0/1
```

- **show nameif zone**

  インターフェイス名およびゾーン名を表示します。

  show nameif zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show nameif zone
Interface                Name                   zone-name      Security
GigabitEthernet0/0       inside-1               inside-zone     100
GigabitEthernet0/1.21    inside                 inside-zone     100
GigabitEthernet0/1.31    4                                        0
GigabitEthernet0/2       outside                outside-zone   0
Management0/0            lan                                      0
```

ゾーン接続

- **show conn** [**long** | **detail**] [**zone** *zone_name* [**zone** *zone_name*] [...]]

  show conn zone コマンドは、ゾーンの接続を表示します。**long** キーワードと **detail** キーワードは、接続が構築されたプライマリ インターフェイスと、トラフィックの転送に使用される現在のインターフェイスを表示します。したがって、複数のインターフェイスからの接続の場合、現在のインターフェイスは、show conn コマンドが発行されたタイミングに応じて、異なる時点で異なるインターフェイスを表示できます。

  show conn long zone コマンドの次の出力を参照してください。

```
ciscoasa# show conn long zone zone-inside zone zone-outside

TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

- **show asp table zone**

  デバッグ目的で高速セキュリティ パス テーブルを表示します。

- **show local-host** [**zone** *zone_name* [**zone** *zone_name*] [...]]

  ゾーン内のローカル ホストのネットワーク状態を表示します。

  show local-host zone コマンドについては、次の出力を参照してください。プライマリ インターフェイスが最初に表示され、現在のインターフェイスがカッコに囲まれています。

```
ciscoasa# show local-host zone outside-zone

Zone:outside-zone: 4 active, 5 maximum active, 0 denied
local host: <10.122.122.1>,
    TCP flow count/limit = 3/unlimited
    TCP embryonic count to host = 0
    TCP intercept watermark = unlimited
    UDP flow count/limit = 0/unlimited

  Conn:
 TCP outside-zone:outside1(outside2): 10.122.122.1:1080
inside-zone:inside1(inside2): 10.121.121.1:34254, idle 0:00:02, bytes 10, flags UO
```

ゾーン ルーティング

- **show route zone**

  ゾーン インターフェイスのルートを表示します。

  show route zone コマンドについては、次の出力を参照してください。

```
ciscoasa# show route zone

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

S    192.168.105.1 255.255.255.255 [1/0] via 172.16.1.1, outside-zone:outside1
C    192.168.212.0 255.255.255.0 is directly connected, lan-zone:inside,
C    172.16.1.0 255.255.255.0 is directly connected, wan-zone:outside2
S    10.5.5.0 255.255.255.0 [1/0] via 172.16.1.1, wan-zone:outside2
O    10.2.2.1 255.255.255.255 [110/11] via 192.168.212.3, 2:09:24, lan-zone:inside
O    10.1.1.1 255.255.255.255 [110/11] via 192.168.212.2, 2:09:24, lan-zone:inside
```

- **show asp table routing**

  デバッグ目的で高速セキュリティ パス テーブルを表示し、各ルートに関連付けられたゾーンを表示します。

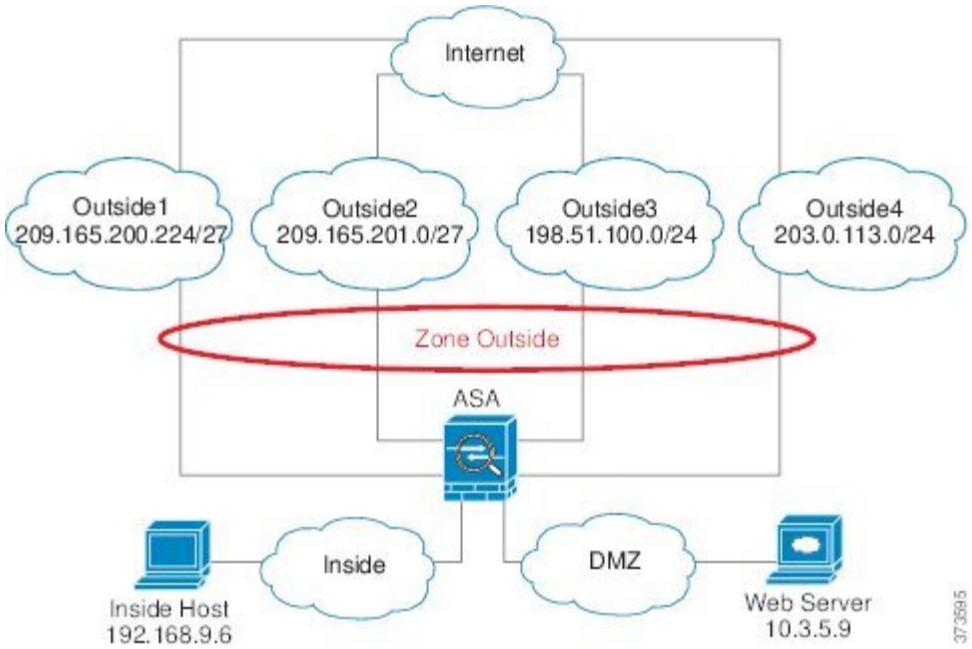
  show asp table routing コマンドについては次の出力を参照してください。

```
ciscoasa# show asp table routing
route table timestamp: 60
in   255.255.255.255 255.255.255.255 identity
in   10.1.0.1       255.255.255.255 identity
in   10.2.0.1       255.255.255.255 identity
in   10.6.6.4         255.255.255.255 identity
in   10.4.4.4         255.255.255.255 via 10.4.0.10 (unresolved, timestamp: 49)
in   172.0.0.67       255.255.255.255 identity
in   172.0.0.0       255.255.255.0   wan-zone:outside2
in   10.85.43.0      255.255.255.0   via 10.4.0.3 (unresolved, timestamp: 50)
```

```
in   10.85.45.0      255.255.255.0   via 10.4.0.20 (unresolved, timestamp: 51)
in   192.168.0.0        255.255.255.0   mgmt
in   192.168.1.0       255.255.0.0     lan-zone:inside
out  255.255.255.255 255.255.255.255 mgmt
out  172.0.0.67       255.255.255.255 mgmt
out  172.0.0.0        255.255.255.0   mgmt
out  10.4.0.0       240.0.0.0       mgmt
out  255.255.255.255 255.255.255.255 lan-zone:inside
out  10.1.0.1       255.255.255.255 lan-zone:inside
out  10.2.0.0       255.255.0.0     lan-zone:inside
out  10.4.0.0       240.0.0.0       lan-zone:inside
```

トラフィック ゾーンの例

次に、4 つの VLAN インターフェイスを外部ゾーンに割り当てて、4 つの等コストのデフォルト ルートを設定する例を示します。PAT は内部インターフェイスに設定され、Web サーバーはスタティック NAT を使用して DMZ インターフェイスで使用できます。




```
interface gigabitethernet0/0
  no shutdown
  description outside switch 1
interface gigabitethernet0/1
  no shutdown
  description outside switch 2

interface gigabitethernet0/2
  no shutdown
  description inside switch

zone outside

interface gigabitethernet0/0.101
```

```
  vlan 101
  nameif outside1
  security-level 0
  ip address 209.165.200.225 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/0.102
  vlan 102
  nameif outside2
  security-level 0
  ip address 209.165.201.1 255.255.255.224
  zone-member outside
  no shutdown

interface gigabitethernet0/1.201
  vlan 201
  nameif outside3
  security-level 0
  ip address 198.51.100.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/1.202
  vlan 202
  nameif outside4
  security-level 0
  ip address 203.0.113.1 255.255.255.0
  zone-member outside
  no shutdown

interface gigabitethernet0/2.301
  vlan 301
  nameif inside
  security-level 100
  ip address 192.168.9.1 255.255.255.0
  no shutdown

interface gigabitethernet0/2.302
  vlan 302
  nameif dmz
  security-level 50
  ip address 10.3.5.1 255.255.255.0
  no shutdown

# Static NAT for DMZ web server on any destination interface
object network WEBSERVER
  host 10.3.5.9 255.255.255.255
  nat (dmz,any) static 209.165.202.129 dns

# Dynamic PAT for inside network on any destination interface
object network INSIDE
  subnet 192.168.9.0 255.255.255.0
  nat (inside,any) dynamic 209.165.202.130

# Global access rule for DMZ web server
access-list WEB-SERVER extended permit tcp any host WEBSERVER eq 80
access-group WEB-SERVER global

# 4 equal cost default routes for outside interfaces
route outside1 0 0 209.165.200.230
route outside2 0 0 209.165.201.10
route outside3 0 0 198.51.100.99
route outside4 0 0 203.0.113.87
```

```
# Static routes for NAT addresses - see redistribute static command
route dmz 209.165.202.129 255.255.255.255 10.3.5.99
route inside 209.165.202.130 255.255.255.255 192.168.9.99

# The global service policy
class-map inspection_default
  match default-inspection-traffic
policy-map type inspect dns preset_dns_map
  parameters
    message-length maximum client auto
    message-length maximum 512
    dns-guard
    protocol-enforcement
    nat-rewrite
policy-map global_policy
  class inspection_default
    inspect dns preset_dns_map
    inspect ftp
    inspect h323 h225 _default_h323_map
    inspect h323 ras _default_h323_map
    inspect ip-options _default_ip_options_map
    inspect netbios
    inspect rsh
    inspect rtsp
    inspect skinny
    inspect esmtp _default_esmtp_map
    inspect sqlnet
    inspect sunrpc
    inspect tftp
    inspect sip
    inspect xdmcp
service-policy global_policy global
```

トラフィック ゾーンの履歴

機能名	プラットフォーム リリース	説明
トラフィック ゾーン	9.3(2)	インターフェイスをトラフィック ゾーンにグループ化することで、トラフィックのロードバランシング（等コスト マルチパス（ECMP）ルーティングを使用）、ルートの冗長性、および複数のインターフェイス間での非対称ルーティングを実現できます。 （注） 名前付きゾーンにはセキュリティ ポリシーを適用できません。セキュリティ ポリシーはインターフェイスに基づきます。ゾーン内のインターフェイスが同じアクセス ルール、NAT、およびサービス ポリシーを使用して設定されていれば、ロード バランシングおよび非対称ルーティングは正しく動作します。 **zone**、**zone-member**、**show running-config zone**、**clear configure zone**、**show zone**、**show asp table zone**、**show nameif zone**、**show conn long**、**show local-host zone**、**show route zone**、**show asp table routing**、**clear conn zone**、**clear local-host zone** の各コマンドが導入または変更されました。
clear local-host コマンド	9.14(1)	**clear local-host** コマンドおよびそのすべての属性とキーワードが廃止されました。今後のリリースで削除される予定です。

第 IV 部

基本設定

- 基本設定 （1005 ページ）
- DHCP サービスと DDNS サービス （1033 ページ）
- デジタル証明書 （1063 ページ）
- ARP インスペクションおよび MAC アドレス テーブル （1109 ページ）

第 23 章

基本設定

この章では、ASA 上でコンフィギュレーションを機能させるために通常必要な基本設定を行う方法について説明します。

- ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （1005 ページ）
- 日時の設定 （1008 ページ）
- マスター パスフレーズの設定 （1015 ページ）
- DNS サーバーの設定 （1020 ページ）
- ハードウェア バイパスおよびデュアル電源（Cisco ISA 3000）の設定 （1023 ページ）
- ASP（高速セキュリティ パス）のパフォーマンスと動作の調整 （1025 ページ）
- DNS キャッシュのモニタリング （1028 ページ）
- 基本設定の履歴 （1028 ページ）

ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定

ホスト名、ドメイン名、イネーブルパスワード、Telnetパスワードを設定するには、次の手順を実行します。

始める前に

ホスト名、ドメイン名、イネーブルパスワード、Telnetパスワードを設定する前に、次の要件を確認します。

- マルチ コンテキスト モードでは、コンテキスト実行スペースとシステム実行スペースの両方のホスト名とドメイン名を設定できます。
- イネーブル パスワードと Telnet パスワードは、各コンテキストで設定します。システムでは使用できません。
- システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ASA またはコンテキストのホスト名を指定します。デフォルトのホスト名は「asa」です。

hostname *name*

例：

```
ciscoasa(config)# hostname myhostnamexample12345
```

名前には、63 文字以下の文字を使用できます。ホスト名はアルファベットまたは数字で開始および終了する必要があります。使用できるのはアルファベット、数字、ハイフンのみです。

ASA のホスト名を設定すると、そのホスト名がコマンドラインのプロンプトに表示されます。このホスト名によって、複数のデバイスとのセッションを確立する場合に、コマンドを入力する場所が常に把握できます。

マルチ コンテキスト モードでは、システム実行スペースに設定したホスト名がすべてのコンテキストのコマンドラインプロンプトに表示されます。コンテキスト内で任意に設定したホスト名はコマンドラインには表示されませんが、**banner** コマンド**$(hostname)** トークンによって使用できます。

ステップ 2 ASA のドメイン名を指定します。デフォルト ドメイン名は default.domain.invalid です。

domain-name *name*

例：

```
ciscoasa(config)# domain-name example.com
```

ASA は、修飾子を持たない名前のサフィックスとして、ドメイン名を追加します。たとえば、ドメイン名を「example.com」に設定し、syslog サーバーとして非修飾名「jupiter」を指定した場合は、ASA によって名前が修飾されて「jupiter.example.com」となります。

ステップ 3 イネーブル パスワードを変更します。デフォルトではイネーブル パスワードは空白ですが、**enable** コマンドを最初に入力したときに変更するように求められます。

enable password *password*

例：

```
ciscoasa(config)# enable password Pa$$w0rd
```

enable 認証を設定しない場合、イネーブル パスワードによって特権 EXEC モードが開始されます。HTTP 認証を設定しない場合、イネーブル パスワードによって空のユーザー名で ASDM にログインできます。

password 引数は、大文字と小文字が区別される 8 ～ 127 文字のパスワードです。以下を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

- スペースは使用できません。
- 疑問符は使用できません。
- 3 文字以上連続した、順番に並んだ ASCII 文字または繰り返される ASCII 文字は使用できません。たとえば、次のパスワードは拒否されます。
  - **abc**user1
  - user**543**
  - user**aaaa**
  - user2**666**

このコマンドによって最高の特権レベル（15）のパスワードが変更されます。ローカル コマンド許可を設定すると、次の構文を使用して 0 ～ 15 の各特権レベルにイネーブル パスワードを設定できます。

enable password *password* **level** *number*

encrypted キーワード（9.6 以前の場合は 32 文字以内のパスワード用）または **pbkdf2** キーワード（9.6 以降では 32 文字を超えるパスワード用、9.7 以降では長さを問わずすべてのパスワード用）は、（MD5 ベースのハッシュまたは SHA-512 を使用する PBKDF2（Password-Based Key Derivation Function 2）ハッシュを使用して）パスワードが暗号化されていることを示します。新しいパスワードを入力しない限り、既存のパスワードは MD5 ベースのハッシュを使用し続けることに注意してください。**enable password** コマンドのパスワードを定義すると、ASA はセキュリティを維持するために、そのパスワードを設定に保存するときに暗号化します。**show running-config** コマンドを入力すると、**enable password** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **encrypted** または **pbkdf2** キーワードが示されます。たとえば、パスワードに「test」と入力すると、**show running-config** コマンドの出力には次のように表示されます。

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

実際に CLI で **encrypted** または **pbkdf2** キーワードを入力するのは、同じパスワードを使用して、ある設定ファイルを他の ASA で使用するためにカット アンド ペーストする場合だけです。

パスワードを空白の値にリセットすることはできません。

ステップ 4 Telnetアクセスのためのログイン パスワードを設定します。デフォルトのパスワードはありません。

Telnet 認証を設定しない場合、ログイン パスワードは Telnet アクセスに使用されます。

passwd *password* [**encrypted**]

例：

```
ciscoasa(config)# passwd cisco12345
```

password は、大文字と小文字が区別されるパスワードです。英数字と特殊記号を 16 文字まで使用できます。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由で別の ASA にパスワードをコピーする必要があるが、元のパスワードがわからない場合、暗号化されたパスワードと、**encrypted** キーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力するときにだけ表示されます。

日時の設定

（注） Firepower 4100/9300 の日時を設定しないでください。ASA はシャーシから日時の設定を受信します。

タイムゾーンと夏時間の日付の設定

タイムゾーンおよび夏時間の日付範囲を設定するには、次の手順を実行します。

手順

ステップ 1 タイム ゾーンを設定します。デフォルトでは、タイムゾーンは UTC です。

- Firepower および Secure Firewall モデル：

  clock timezone *zone*

  - *zone*：使用可能なタイムゾーン名のリストを表示するには、**clock timezone ?** コマンドを入力します。

  例：

```
ciscoasa(config)# clock timezone ?
Available timezones:
CET
CST6CDT
Cuba
EET
Egypt
Eire
EST
EST5EDT
Factory
GB
GB-Eire
```

```
GMT
GMT0
GMT-0
GMT+0
Greenwich
Hongkong
HST
Iceland
Iran
Israel
Jamaica
Japan
[...]

ciscoasa(config)# clock timezone US/?

configure mode commands/options:
  US/Alaska          US/Aleutian    US/Arizona    US/Central
  US/East-Indiana    US/Eastern     US/Hawaii     US/Indiana-Starke
  US/Michigan        US/Mountain    US/Pacific

ciscoasa(config)# clock timezone US/Mountain
```

- その他のすべてのモデルについては次を実行します。

  clock timezone *zone* [-]*hours* [*minutes*]

  - *zone*：タイムゾーンを文字列で指定します（太平洋標準時の PST など）。
  - [-]*hours*：UTC からのオフセットの時間数を設定します。たとえば、PST は -8 時間です。
  - *minutes*：UTC からのオフセットの分数を設定します。

  例：

```
ciscoasa(config)# clock timezone PST -8
```

ステップ 2 （ASA 仮想、および ISA 3000）次のいずれかのコマンドを入力して、夏時間の日付範囲をデフォルトから変更します。デフォルトの定期的な日付範囲は、3 月の第 2 日曜日の午前 2 時～ 11 月の第 1 日曜日の午前 2 時です。

- 夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このコマンドを使用する場合は、日付を毎年再設定する必要があります。

  clock summer-time *zone* **date** {*day month* | *month day*} *year hh*:*mm* {*day month* | *month day*} *year hh*:*mm* [*offset*]

  - *zone*：タイムゾーンを文字列で指定します（太平洋夏時間の PDT など）。
  - *day*：1 ～ 31 の日付を設定します。標準の日付形式に応じて、月日を **April 1** または 1 April のように入力できます。
  - *month*：月を文字列で設定します。標準の日付形式に応じて、月日を April 1 または 1 April のように入力できます。
  - *year*：4 桁で年を設定します（2004 など）。年の範囲は 1993 ～ 2035 です。

- *hh:mm*：24 時間形式で、時間と分を設定します。
- *offset*：夏時間用に時間を変更する分数を設定します。デフォルト値は 60 分です。

例：

```
ciscoasa(config)# clock summer-time PDT 1 April 2010 2:00 60
```

- 夏時間の開始日と終了日を、年の特定の日付ではなく、月の日時の形式で指定します。このコマンドを使用すると、毎年変更する必要がない、繰り返される日付範囲を設定できます。

  clock summer-time *zone* **recurring** [*week weekday month hh*:*mm week weekday month hh*:*mm*] [*offset*]

  - *zone*：タイムゾーンを文字列で指定します（太平洋夏時間の PDT など）。
  - *week*：月の特定の週を 1 から 4 までの整数で指定するか、first または last という単語で指定します。たとえば、日付が 5 週目に当たる場合は、last を指定します。
  - *weekday*：Monday、Tuesday、Wednesday などのように曜日を指定します。
  - *month*：月を文字列で設定します。
  - *hh:mm*：24 時間形式で、時間と分を設定します。
  - *offset*：夏時間用に時間を変更する分数を設定します。デフォルト値は 60 分です。

  例：

```
ciscoasa(config)# clock summer-time PDT recurring first Monday April 2:00 60
```

NTP サーバを使用した日付と時刻の設定

NTP を利用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバを設定できます。ASA は一番下の階層からサーバを選択し、データ信頼度の尺度にします。

手動で設定した時刻はすべて、NTP サーバーから取得された時刻によって上書きされます。

ASA は NTPv4 をサポートします。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

ステップ 1 （任意） NTP サーバーによる認証を有効にします。

a) 認証をイネーブルにします。

ntp authenticate

例：

```
ciscoasa(config)# ntp authenticate
```

NTP 認証を有効にする場合は、さらに **ntp trusted-key** コマンドでキー ID を指定し、そのキーを **ntp server key** コマンドでサーバーに関連付ける必要があります。**ntp authentication-key** コマンドを使用して ID の実際のキーを設定します。複数のサーバーがある場合は、サーバーごとに個別の ID を設定します。

b) 認証キー ID が信頼できるキーであると指定します。この信頼できるキーは、NTP サーバーでの認証に必要です。

ntp trusted-key *key_id*

例：

```
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
```

key_id 引数は、1 ～ 4294967295 の値です。複数のサーバで使用できるように複数の信頼できるキーを入力できます。

c) NTP サーバーの認証を行うためのキーを設定します。

ntp authentication-key *key_id* {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} *key*

例：

```
ciscoasa(config)# ntp authentication-key 1 md5 aNiceKey1
ciscoasa(config)# ntp authentication-key 2 md5 aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
```

- *key_id*：**ntp trusted-key** コマンドを使用して設定した ID を設定します。
- {**md5** | **sha1** | **sha256** | **sha512** | **cmac**} ：アルゴリズムを設定します。
- *key*：キーを最大 32 文字の文字列で設定します。

ステップ 2 NTP サーバーを指定します。

ntp server {*ipv4_address* | *ipv6_address* }[**key** *key_id*] [**source** *interface_name*] [**prefer**]

例：

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

NTP 認証（**ntp authenticate**）をイネーブルにした場合は、**ntp trusted-key** コマンドを使って設定した ID を使用して **key** *keykey_id* 引数を指定する必要があります。

source *interface_name* キーワード引数ペアは、NTP パケットの発信インターフェイスを識別します（ルーティングテーブル内のデフォルトのインターフェイスを使用しない場合）。マルチコンテキストモードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。

prefer キーワードは、精度が類似する複数のサーバーがある場合に、この NTP サーバーを優先サーバーに設定します。NTP では、どのサーバーの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバーに同期します。サーバーの精度に差がない場合は、**prefer** キーワードで使用するサーバーを指定します。ただし、優先サーバーよりも精度が大幅に高いサーバーがある場合、ASA は精度の高いそのサーバーを使用します。たとえば、ASA では、優先サーバの stratum 3 の代わりに、サーバ stratum 2 を使用します。

複数のサーバーを指定できます。その中から ASA は最も精度の高いサーバーを使用します。

手動での日時の設定

日付と時刻を手動で設定するには、次の手順を実行します。

始める前に

マルチ コンテキスト モードでは、時刻はシステム コンフィギュレーションに対してだけ設定できます。

手順

日付と時刻を手動で設定します。

clock set *hh*:*mm*:*ss* {*month day* | *day month*} *year*

例：

```
ciscoasa# clock set 20:54:00 april 1 2004
```

hh:*mm*:*ss* 引数には、時、分、秒を 24 時間形式で設定します。たとえば、午後 8:54 の場合は、20:54:00 と入力します。

day 値は、月の日付として 1 ～ 31 を設定します。標準の日付形式に応じて、月日を april 1 または 1 april のように入力できます。

month 値は、月を設定します。標準の日付形式に応じて、月日を april 1 または 1 april のように入力できます。

year 値は、4 桁で年を設定します（2004 など）。年の範囲は 1993 ～ 2035 です。

デフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して、 **clock set** コマンドの入力後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、clock set コマンドを使用して新しい時刻を設定する必要があります。

Precision Time Protocol の設定（ISA 3000）

高精度時間プロトコル（PTP）は、パケットベース ネットワーク内のさまざまなデバイスのクロックを同期するために開発された時間同期プロトコルです。それらのデバイスクロックは、一般的に精度と安定性が異なります。このプロトコルは、産業用のネットワーク化された測定およびコントロールシステム向けに設計されており、必要な帯域幅は最小限で、処理オーバーヘッドが少ないため、分散システムでの使用に最適です。

PTP システムは、PTP デバイスと非 PTP デバイスの組み合わせで構成される分散ネットワークシステムです。PTP デバイスには、オーディナリクロック、境界クロック、およびトランスペアレントクロックが含まれます。非 PTP デバイスには、ネットワークスイッチ、ルータ、およびその他のインフラストラクチャ デバイスが含まれます。

ASA デバイスは、トランスペアレントクロックとして設定できます。ASA デバイスは、自身のクロックを PTP クロックと同期しません。ASA デバイスは、PTP クロックで定義されている PTP のデフォルトプロファイルを使用します。

PTP デバイスを設定する場合は、連携させるデバイスのドメイン番号を定義します。したがって、複数の PTP ドメインを設定し、特定の 1 つのドメインに PTP クロックを使用するように PTP 以外の各デバイスを設定できます。

始める前に

- この機能は、ISA 3000 のみで使用できます。
- PTP の使用は、シングルコンテキストモードでのみサポートされます。
- Cisco PTP は、マルチキャスト PTP メッセージのみをサポートしています。
- デフォルトでは、トランスペアレント モードのすべての ISA 3000 インターフェイスで PTP がイネーブルになっています。ルーテッドモードでは、PTP パケットがデバイスを通過できるようにするために必要な設定を追加する必要があります。

- PTP は IPv6 ネットワークではなく、IPv4 ネットワークでのみ使用できます。
- PTP設定は、スタンドアロンかブリッジグループメンバーかを問わず、物理イーサネットインターフェイスでサポートされます。次のものではサポートされません。
  - 管理インターフェイス。
  - サブインターフェイス、EtherChannel、BVI、その他の仮想インターフェイス。
- VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。
- PTPパケットが確実にデバイスを通過できるようにする必要があります。トランスペアレントファイアウォールモードでは、PTPトラフィックを許可するアクセスリストがデフォルトで設定されています。PTP トラフィックは UDP ポート 319 と 320、および宛先 IP アドレス 224.0.1.129 によって識別されます。そのためルーテッド ファイアウォール モードでは、このトラフィックを許可するすべての ACL が受け入れられます。
- さらにルーテッド ファイアウォール モードでは、PTP マルチキャストグループ用のマルチキャストルーティングを次のようにイネーブルにする必要もあります。
  - グローバル コンフィギュレーション モードのコマンド **multicast-routing** を入力します。
  - また、ブリッジグループメンバーではなく、PTPが有効になっているインターフェイスごとに、インターフェイス コンフィギュレーション コマンド **igmp join-group 224.0.1.129** を入力して、PTP マルチキャスト グループ メンバーシップを静的に有効にします。このコマンドは、ブリッジグループメンバーに対してはサポートされておらず、必要もありません。

手順

ステップ 1 デバイスのすべてのポートのドメイン番号を指定します。

ptp domain *domain_num*

例：

```
ciscoasa(config)# ptp domain 54
```

domain_num 引数は、デバイスのすべてのポートのドメイン番号です。異なるドメインで受信されたパケットは、通常のマルチキャストパケットのように扱われるため、PTP処理は行われません。この値の範囲は 0 ～ 255、デフォルト値は 0 です。ネットワーク内の PTP デバイスに設定されているドメイン番号を入力します。

ステップ 2 （オプション）デバイスの PTP クロック モードを設定します。

ptp mode e2etransparent

例：

```
ciscoasa(config)# ptp mode e2etransparent
```

このコマンドは、PTP がイネーブルになっているすべてのインターフェイスでエンド ツー エンド トランスペアレント モードをイネーブルにします。

ステップ 3 インターフェイスでの PTP をイネーブルにします。

ptp enable

システムが設定ドメイン内のPTPクロックに接続できる各インターフェイスで、PTPを有効にします。

例：

```
ciscoasa(config)# interface gigabitethernet1/2
ciscoasa(config-if)# ptp enable
```

マスター パスフレーズの設定

マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。マスターパスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)
- フェールオーバー
- AAA サーバ
- Logging
- 共有ライセンス

マスター パスフレーズの追加または変更

マスター パスフレーズを追加または変更するには、次の手順を実行します。

始める前に

- この手順を実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。
- フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスター パスフレーズを変更すると、エラー メッセージが表示されます。こ

のメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

- アクティブ/スタンバイ フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行されます。これは、アクティブな構成をスタンバイ ユニットに複製します。この複製が行われない場合、スタンバイ ユニットの暗号化されたパスワードは、同じパスフレーズを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されます。アクティブ/アクティブ フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、アクティブ/アクティブ モードでトラフィックの中断を引き起こす場合があります。これは、新しい構成が同期される前に、セカンダリ ユニットで構成が消去されるためです。**failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、**write standby** を入力してから、**no failover active group 2** コマンドを使用してセカンダリ ユニットにグループ 2 コンテキストを復元する必要があります。

手順

ステップ 1 暗号キーの生成に使用されるパスフレーズを設定します。パスフレーズの長さは、8 ～ 128 文字にする必要があります。パスフレーズには、バックスペースと二重引用符を除くすべての文字を使用できます。コマンドに新しいパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。パスフレーズを変更するには、古いパスフレーズを入力する必要があります。

key config-key password-encryption [*new_passphrase* [*old_passphrase*]]

例：

```
ciscoasa(config)# key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
```

（注）
インタラクティブ プロンプトを使用してパスワードを入力し、パスワードがコマンド履歴バッファに記録されないようにします。

暗号化されたパスワードがプレーン テキスト パスワードに変換されるため、**no key config-key password-encrypt** コマンドは注意して使用してください。パスワードの暗号化がサポートされていないソフトウェア バージョンにダウングレードするときは、このコマンドの **no** 形式を使用できます。

ステップ 2 パスワード暗号化をイネーブルにします。

password encryption aes

例：

```
ciscoasa(config)# password encryption aes
```

パスワードの暗号化がイネーブルになり、マスターパスワードが使用可能になると、ただちにすべてのユーザーパスワードが暗号化されます。実行コンフィギュレーションには、パスワードは暗号化された形式で表示されます。

パスワードの暗号化をイネーブルにしたときに、パスフレーズが設定されていない場合、パスフレーズが将来的に使用可能になるものとしてコマンドは正常に実行されます。

後から **no password encryption aes** コマンドを使用してパスワードの暗号化をディセーブルにすると、暗号化された既存のパスワードは変更されず、マスター パスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号化されます。

ステップ 3 マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

このコマンドを入力しなければ、スタートアップ コンフィギュレーションのパスワードは引き続き可読状態となります（過去に暗号化された状態で保存されていない場合）。また、マルチ コンテキスト モードでは、マスター パスフレーズはシステム コンテキスト コンフィギュレーション内で変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザー コンテキストではなく、システム コンテキスト モードで write memory コマンドを入力しないと、ユーザー コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで write memory all コマンドを使用します。

例

次の例は、これまでにキーが何も存在していないことを示します。

```
ciscoasa(config)# key config-key password-encryption 12345678
```

次の例は、キーがすでに存在することを示します。

```
ciscoasa(config)# key config-key password-encryption 23456789
Old key: 12345678
```

次の例では、パラメータを指定しないでコマンドを入力して、キーの入力を求めるプロンプトが表示されるようにします。キーがすでに存在するため、入力を求めるプロンプトが表示されます。

```
ciscoasa(config)# key config-key password-encryption
```

```
Old key: 12345678
New key: 23456789
Confirm key: 23456789
```

次の例では、既存のキーがないため、入力を求めるプロンプトが表示されません。

```
ciscoasa(config)# key config-key password-encryption
New key: 12345678
Confirm key: 12345678
```

マスター パスフレーズの無効化

マスター パスフレーズをディセーブルにすると、暗号化されたパスワードがプレーン テキストパスワードに戻ります。暗号化されたパスワードをサポートしていない以前のソフトウェアバージョンにダウングレードする場合は、パスフレーズを削除しておくと便利です。

始める前に

- ディセーブルにする現在のマスターパスフレーズがわかっていなければなりません。パスフレーズが不明の場合は、マスターパスフレーズの削除（1019ページ）を参照してください。
- この手順が機能するのは、HTTPS を介した Telnet、SSH、または ASDM によるセキュアセッションだけです。

  マスター パスフレーズをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 マスターパスフレーズを削除します。コマンドにパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。

no key config-key password-encryption [*old_passphrase*]]

例：

```
ciscoasa(config)# no key config-key password-encryption

Warning! You have chosen to revert the encrypted passwords to plain text.
This operation will expose passwords in the configuration and therefore
exercise caution while viewing, storing, and copying configuration.

Old key: bumblebee
```

ステップ 2 マスター パスフレーズのランタイム値と結果のコンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

パスフレーズを含む不揮発性メモリは消去され、0xFF パターンで上書きされます。

マルチ モードでは、システム コンテキスト コンフィギュレーション内のマスター パスフレーズが変更されます。その結果、すべてのコンテキスト内のパスワードが影響を受けます。すべてのユーザー コンテキストではなく、システム コンテキスト モードで write memory コマンドを入力すると、ユーザー コンテキストで暗号化されたパスワードは失効する可能性があります。また、すべての設定を保存するには、システム コンテキストで write memory all コマンドを使用します。

マスター パスフレーズの削除

マスター パスフレーズは回復できません。マスター パスフレーズがわからなくなった場合や不明な場合は、削除できます。

マスター パスフレーズを削除するには、次の手順を実行します。

手順

ステップ 1 マスターキーと、暗号化されたパスワードが含まれているコンフィギュレーションを削除します。

write erase

例：

```
ciscoasa(config)# write erase
```

ステップ 2 マスター キーや暗号化パスワードのないスタートアップ コンフィギュレーションを使用して ASA をリロードします。

reload

例：

```
ciscoasa(config)# reload
```

DNS サーバーの設定

DNS サーバーを設定して、ASA がホスト名を IP アドレスに解決できるようにする必要があります。また、アクセスルールに完全修飾ドメイン名（FQDN）ネットワークオブジェクトを使用するように、DNS サーバーを設定する必要があります。

一部の ASA 機能では、ドメイン名で外部サーバにアクセスするために DNS サーバを使用する必要があります。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバーと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。

デフォルトでは、DefaultDNS と呼ばれるデフォルトの DNS サーバーグループがあります。複数の DNS サーバーグループを作成できます。1 つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。PN トンネル グループ用に他の DNS サーバー グループを設定できます。詳細については、コマンドリファレンスの **tunnel-group** コマンドを参照してください。

（注） ASA では、機能に応じて DNS サーバーの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、names コマンドを使用して名前の使用を有効にした場合だけです。

始める前に

DNS ドメインルックアップをイネーブルにするすべてのインターフェイスに対して適切なルーティングおよびアクセス ルールを設定し、DNS サーバーに到達できるようにしてください。

手順

ステップ 1 サポートされているコマンドに対してネーム ルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。

dns domain-lookup *interface_name*

インターフェイスで DNS ルックアップを有効にしない場合、ASA はそのインターフェイスの DNS サーバーと通信しません。DNS サーバーへのアクセスに使用されるすべてのインターフェイスで DNS ルックアップを有効にしてください。

例：

```
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns domain-lookup outside
```

ステップ 2 1 つ以上の DNS サーバーグループを作成し、そのグループにサーバーを追加します。

a) DNS サーバーグループに名前を付けます。

dns server-group *name*

デフォルトの DefaultDNS サーバーグループを設定するには、名前に DefaultDNS を指定します。

例：

```
ciscoasa(config)# dns server-group DefaultDNS
```

b) グループの 1 つ以上の DNS サーバーを指定します。

name-server *ip_address* [*ip_address2*] [*...*] [*ip_address6*] *[interface_name]*

同じコマンドで 6 つの IP アドレスすべてをスペースで区切って入力するか、各コマンドを別々に入力できます。

（任意）ASA がサーバーとの通信に使用する *interface_name* を指定します。インターフェイスを指定しなかった場合、ASA はデータ ルーティング テーブルを確認し、一致するものが見つからなければ、管理専用ルーティング テーブルを確認します。

ASA では、応答を受信するまで各 DNS サーバを順に試します。

例：

```
ciscoasa(config-dns-server-group)# name-server 10.1.1.5 192.168.1.67 209.165.201.6
outside
```

c) （デフォルト グループのみの場合）完全修飾されていない場合、ホスト名に追加するドメイン名を構成します。

domain-name *name*

例：

```
ciscoasa(config-dns-server-group)# domain-name example.com
```

d) （任意） DNS サーバー グループの追加プロパティを設定します。

デフォルト設定がネットワークに適さない場合は、次のコマンドを使用してグループの特性を変更します。

- **timeout** *seconds*：次の DNS サーバーを試行する前に待機する秒数（1 ～ 30）。デフォルト値は 2 秒です。ASA がサーバーのリストを再試行するたびに、このタイムアウトは倍増します。

- **retries** *number*：ASA が応答を受信しないときに、DNS サーバーのリストを再試行する回数（0 ～ 10）。
- **expire-entry-timer minutes** *number*：DNS エントリの最小 TTL（分単位）。有効期限タイマーがエントリの TTL よりも長い場合、TTL は有効期限エントリ時間値まで増加します。TTL が有効期限タイマーよりも長い場合、有効期限エントリ時間値は無視されます。この場合、TTL に追加の時間は追加されません。有効期限が切れると、DNS ルックアップテーブルからエントリが削除されます。エントリの削除にはテーブルをコンパイルする必要があります。したがって、削除を頻繁に行うとデバイス上の処理負荷が増加する可能性があります。DNS エントリによっては TTL が極端に短い（3 秒程度）場合があるため、この設定を使用して TTL を実質的に延長できます。デフォルトは 1 分です（つまり、すべての解像度の最小 TTL は 1 分です）。指定できる範囲は 1 ～ 65535 分です。このオプションは、FQDN ネットワーク オブジェクトの解決時にのみ使用されます。
- **poll-timer minutes** *number*：FQDN ネットワーク/ホスト オブジェクトを IP アドレスに解決するために使用されるポーリング サイクルの時間（分単位）。FQDN オブジェクトはファイアウォール ポリシーで使用される場合にのみ解決されます。タイマーによって、解決間隔の最大時間が決定されます。また、DNS エントリの存続可能時間（TTL）の値を使用しても、IP アドレス解決に更新するタイミングを決定できます。したがって、個々の FQDN がポーリング サイクルよりも頻繁に解決される可能性があります。デフォルトは 240 （4 時間）です。指定できる範囲は 1 ～ 65535 分です。

e) さらに DNS サーバーグループを追加したい場合は、上記の手順を繰り返します。

ステップ 3 （任意） ドメインを特定の DNS サーバーグループにマッピングします。

dns-group-map

dns-to-domain *dns_group_name domain*

最大 30 のドメインをマッピングできます。同じドメインを複数の DNS サーバーグループにマッピングすることはできませんが、複数のドメインを同じサーバーグループにマッピングすることは可能です。（DefaultDNS などの）デフォルトに使用するグループにドメインをマッピングしないでください。

例：

```
ciscoasa(config)# dns-group-map
ciscoasa(config-dns-group-map)# dns-to-domain group1 eng.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group1 hr.cisco.com
ciscoasa(config-dns-group-map)# dns-to-domain group2 example.com
```

ステップ 4 デフォルトの DNS グループを指定します。

dns-group *name*

デフォルトでは、DefaultDNS が指定されています。他のグループを設定した場合は、このコマンドを使用して別のデフォルトグループを指定できます。 DNS グループマップで関連付けられているドメインをデフォルトグループに含めることはできません。

例：

```
ciscoasa(config)# dns-group new_default_group
```

ハードウェア バイパスおよびデュアル電源（Cisco ISA 3000）の設定

ハードウェア バイパスを有効化して、停電時にもインターフェイス ペア間のトラフィックのフローを継続することができます。サポートされているインターフェイス ペアは、銅線 GigabitEthernet 1/1 と 1/2 および GigabitEthernet 1/3 と 1/4 です。ハードウェア バイパスがアクティブな場合はファイアウォール機能が設定されていません。したがって、トラフィックの通過を許可しているリスクをご自身が理解していることを確認してください。次のハードウェア バイパスのガイドラインを参照してください。

- この機能は、Cisco ISA 3000 アプライアンスのみで使用できます。
- 光ファイバ イーサネット モデルがある場合は、銅線イーサネット ペア（GigabitEthernet 1/1 および 1/2）のみがハードウェア バイパスをサポートします。
- ISA 3000 への電源が切断され、ハードウェア バイパス モードに移行すると、通信できるのはサポートされているインターフェイス ペアだけになります。つまり、デフォルトの設定を使用している場合、inside1 と inside2 間および outside1 と outside2 間は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。
- シスコでは、TCP シーケンスのランダム化を無効にすることを推奨しています（下記の手順を参照）。ランダム化が有効化されている場合（デフォルト）、ハードウェア バイパスを有効化するときに TCP セッションを再確立する必要があります。デフォルトでは、ISA 3000 を通過する TCP 接続の最初のシーケンス番号（ISN）が乱数に書き換えられます。ハードウェア バイパスが有効化されると、ISA 3000 はデータ パスに存在しなくなり、シーケンス番号を変換しません。受信するクライアントは予期しないシーケンス番号を受信し、接続をドロップします。TCP シーケンスのランダム化が無効になっていても、スイッチオーバーの際に一時的にダウンしたリンクのために、一部の TCP 接続は再確立される必要があります。
- ハードウェアのバイパス インターフェイスでの Cisco TrustSec の接続は、ハードウェアのバイパスが有効化されているときにはドロップされます。ISA 3000 の電源がオンになり、ハードウェアのバイパスが非アクティブ化されている場合、接続は再ネゴシエートされます。
- ハードウェア バイパスを非アクティブ化し、トラフィックが ISA 3000 のデータ パスを経由することを再開した場合、スイッチオーバー時に一時的にダウンしたリンクがあるために、既存の TCP セッションの一部を再確立する必要があります。

- ハードウェア バイパスをアクティブにすると、イーサネット PHY が切断され、ASA はインターフェイスのステータスを判断できなくなります。インターフェイスはダウン状態であるかのように表示されます。

ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。

始める前に

- ハードウェア バイパス インターフェイスはスイッチのアクセス ポートに接続する必要があります。トランク ポートには接続しないでください。

手順

ステップ 1 停電時にハードウェア バイパスが有効化されるように設定します。

hardware-bypass GigabitEthernet {**1/1-1/2** | **1/3-1/4**} [**sticky**]

例：

```
ciscoasa(config)# hardware-bypass GigabitEthernet 1/1-1/2
ciscoasa(config)# hardware-bypass GigabitEthernet 1/3-1/4
```

sticky キーワードによって、電源が回復してアプライアンスが起動した後に、アプライアンスがハードウェア バイパス モードに保たれます。この場合、準備が整った時点でハードウェア バイパスを手動でオフにする必要があります。このオプションを使用すると、トラフィックへの短時間の割り込みがいつ発生するかを制御できます。

ステップ 2 手動でハードウェア バイパスを有効化または非アクティブ化します。

[**no**] **hardware-bypass manual GigabitEthernet** {**1/1-1/2** |**1/3-1/4**}

例：

```
ciscoasa# hardware-bypass manual GigabitEthernet 1/1-1/2
ciscoasa# no hardware-bypass manual GigabitEthernet 1/1-1/2
```

ステップ 3 （任意）ハードウェア バイパスを設定して、ASA FirePOWER モジュールが起動するまでアクティブに維持します。

hardware-bypass boot-delay module-up sfr

ブート遅延が動作するには、**sticky** オプションを使用せずにハードウェア バイパスを有効化する必要があります。**hardware-bypass boot-delay** を使用しないと、ASA FirePOWER モジュールが起動を完了する前にハードウェア バイパスが非アクティブになる可能性があります。たとえば、モジュールをフェールクローズに設定していた場合、このような状況では、トラフィックがドロップされる可能性があります。

ステップ 4 TCP シーケンスのランダム化のディセーブルこの例では、デフォルト設定に設定を追加することによって、すべてのトラフィックのランダム化を無効化する方法を示します。

policy-map global_policy

class sfrclass

set connection random-sequence-number disable

後でオンに戻す場合は、「disable」を **enable** に置き換えます。

ステップ 5 予期する構成としてデュアル電源を設定します。

power-supply dual

ステップ 6 設定を保存します。

write memory

システムがオンラインになった後のハードウェアバイパスの動作は、スタートアップ コンフィギュレーションの設定によって決定されるため、実行コンフィギュレーションを保存する必要があります。

ASP（高速セキュリティ パス）のパフォーマンスと動作の調整

ASP はポリシーおよび設定を利用可能にする実装レイヤです。Cisco Technical Assistance Center とのトラブルシューティング時以外は直接影響することはありません。ただし、パフォーマンスと信頼性に関連するいくつかの動作を調節することができます。

ルール エンジンのトランザクション コミット モデルの選択

デフォルトでは、ルールベースのポリシー（アクセス ルールなど）を変更した場合、変更はただちに有効になります。ただし、この即時性によりパフォーマンスにわずかな負担がかかります。パフォーマンス コストは、1 秒あたりの接続数が多い環境で大量のルール リストがある場合に顕著です。たとえば、ASA が 1 秒あたり 18,000 個の接続を処理しながら、25,000 個のルールがあるポリシーを変更する場合などです。

パフォーマンスに影響するのは、ルール検索を高速化するためにルール エンジンがルールをコンパイルするためです。デフォルトでは、システムは接続試行の評価時にコンパイルされていないルールも検索して、新しいルールが適用されるようにします。ルールがコンパイルされていないため、検索に時間がかかります。

この動作を変更して、ルール エンジンがトランザクション モデルを使用してルールの変更を導入し、新しいルールがコンパイルされて使用可能な状態になるまで古いルールを引き続き使用するようにできます。トランザクション モデルを使用することで、ルールのコンパイル中にパフォーマンスが落ちることはありません。次の表は、その動作の違いを明確にします。

モデル	コンパイル前	コンパイル中	コンパイル後
デフォルト	古いルールに一致します。	新しいルールに一致します （接続数/秒のレートは減少します）。	新しいルールに一致します。
トランザクション	古いルールに一致します。	古いルールに一致します （接続数/秒のレートは影響を受けません）。	新しいルールに一致します。

トランザクション モデルのその他のメリットには、インターフェイス上の ACL を交換するときに、古い ACL を削除して新しいポリシーを適用するまでに時間差がないことがあります。この機能により受け入れ可能な接続が操作中にドロップされる可能性が削減されます。

始める前に

- 解決が頻繁に変わる可能性があるホスト名にFQDNオブジェクトを使用する場合、トランザクション コミットはアクセス制御ルールでは推奨されません。これは、DNS のチャーンが原因でアクセス グループのコンパイルが完全に解決されない可能性があるためです。引き続きトランザクションコミットを使用する場合は、DNSの有効期限の延長を検討してください。
- ルール タイプのトランザクション モデルをイネーブルにする場合、コンパイルの先頭と末尾をマークする Syslog が生成されます。これらの Syslog には 780001 ～ 780004 までの番号が付けられます。

手順

ルール エンジンのトランザクション コミット モデルを有効にします。

asp rule-engine transactional-commit *option*

オプションは次のとおりです。

- **access-group**：グローバルにまたはインターフェイスに適用されるアクセス ルール。
- **nat**：ネットワーク アドレス変換ルール。

例：

```
ciscoasa(config)# asp rule-engine transactional-commit access-group
```

ASP ロード バランシングの有効化

ASP のロード バランシング機能によって、次の問題を回避しやすくなります。

- フロー上での突発的なトラフィックの増加によって発生するオーバーラン
- 特定のインターフェイス受信リングをオーバーサブスクライブするバルク フローによるオーバーラン
- 比較的高過負荷のインターフェイス受信リングによるオーバーラン（シングル コアでは負荷を維持できません）

ASP ロードバランシングにより、1 つのインターフェイス受信リングから受信したパケットを複数のコアが同時に処理できます。システムがパケットをドロップし、**show cpu** コマンドの出力が 100% を大きく下回る場合、互いに関連のない多数の接続にパケットが属しているのであれば、この機能によってスループットが向上することがあります。

（注） ASP ロードバランシングは、ASA 仮想 で無効になっています。ASA 仮想 の高速セキュリティ パス（ASP）に対する DPDK（データプレーン開発キット）の統合により、ASA 仮想 でこの機能を無効にしたときのパフォーマンスが向上します。

手順

ステップ 1 ASP ロード バランシングの自動オン/オフ切り替えを次のようにイネーブルにします。

asp load-balance per-packet auto

ステップ 2 次のように手動で ASP ロード バランシングをイネーブルにします。

asp load-balance per-packet

ASP ロード バランシングは、**auto** コマンドを有効にしている場合でも、手動で無効化するまでは有効です。

ステップ 3 次のように ASP ロード バランシングを手動でディセーブルにします。

no asp load-balance per-packet

このコマンドは、手動で ASP ロード バランシングをイネーブルにした場合にのみ適用されます。**auto** コマンドも有効にしている場合、ASP ロード バランシングは自動的に有効または無効な状態に戻ります。

DNS キャッシュのモニタリング

ASA では、特定のクライアントレス SSL VPN および certificate コマンドに送信された外部 DNS クエリーの DNS 情報のローカル キャッシュを提供します。各 DNS 変換要求は、ローカル キャッシュで最初に検索されます。ローカル キャッシュに情報がある場合、結果の IP アドレスが戻されます。ローカル キャッシュで要求を解決できない場合、設定されているさまざまな DNS サーバーに DNS クエリーが送信されます。外部 DNS サーバーによって要求が解決された場合、結果の IP アドレスが、対応するホスト名とともにローカル キャッシュに格納されます。

DNS キャッシュのモニタリングについては、次のコマンドを参照してください。

- **show dns-hosts**

  DNS キャッシュを表示します。これには、DNS サーバーからダイナミックに学習したエントリと name コマンドを使用して手動で入力された名前および IP アドレスが含まれます。

基本設定の履歴

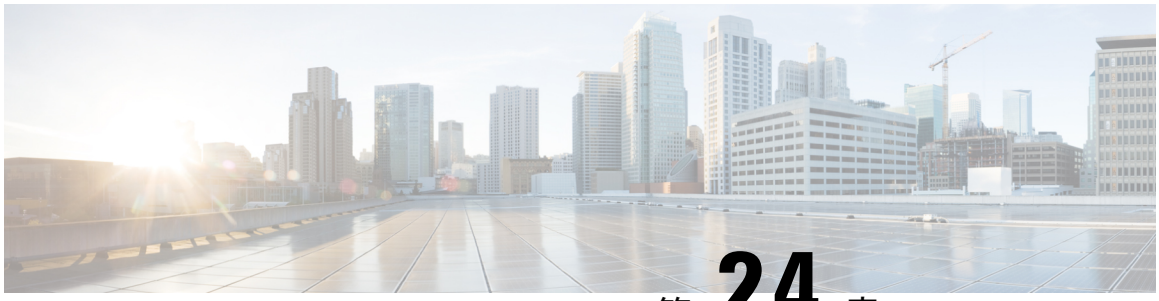
機能名	プラットフォーム リリース	説明
複数の DNS サーバー グループ	9.18(1)	複数の DNS サーバーグループを使用できるようになりました。1 つのグループがデフォルトで、他のグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。 新規/変更されたコマンド：**dns-group-map**、**dns-to-domain**
ネットワーク サービス オブジェクト ドメイン解決用の信頼された DNS サーバ。	9.17(1)	ネットワーク サービス オブジェクトのドメイン名を解決するときに、システムが信頼する DNS サーバを指定できます。この機能により、すべての DNS ドメイン名解決が、信頼された送信元から IP アドレスを取得するようになります。 新規/変更されたコマンド：**dns trusted-source**、**show dns trusted-source**

機能名	プラットフォームリリース	説明
DNS エントリの TTL 動作の変更	9.17(1)	以前は、設定値は各エントリの既存の TTL に追加されていました（デフォルトは 1 分でした）。現在は、有効期限タイマーがエントリの TTL よりも長い場合、TTL は有効期限エントリ時間値まで増加します。TTL が有効期限タイマーよりも長い場合、有効期限エントリ時間値は無視されます。この場合、TTL に追加の時間は追加されません。 新規/変更されたコマンド： **expire-entry-timer minutes**
より強力なローカルユーザーと有効なパスワード要件	9.17(1)	ローカルユーザーと有効なパスワードについて、次のパスワード要件が追加されました。 • パスワードの長さ：8 文字以上。以前は、最小値が 3 文字でした。 • 繰り返し文字と連続文字：3 つ以上の連続した ASCII 文字または繰り返しの ASCII 文字は許可されません。たとえば、次のパスワードは拒否されます。 • **abc**user1 • user**543** • user**aaaa** • user2**666** 新規/変更されたコマンド：**enable password**、**username**
NTPv4 のサポート	9.14(1)	ASA が NTPv4 をサポートするようになりました。 変更されたコマンドはありません。
追加の NTP 認証アルゴリズム	9.13(1)	以前は、NTP 認証では MD5 だけがサポートされていました。ASA は、次のアルゴリズムをサポートするようになりました。 • MD5 • SHA-1 • SHA-256 • SHA-512 • AES-CMAC 新規/変更されたコマンド： **ntp authentication-key**
IPv6 での NTP サポート	9.12(1)	NTP サーバーに IPv6 アドレスを指定できるようになりました。 新規/変更されたコマンド： **ntp server**

機能名	プラットフォーム リリース	説明
enable ログイン時のパスワードの変更が必須に	9.12(1)	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 ～ 127 文字の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブル パスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 新規/変更されたコマンド： **enable password**
ASP ロードバランシングは、ASA 仮想 で無効になっています。	9.10(1)	ASA 仮想の高速セキュリティパス（ASP）に対する最近の DPDK（データプレーン開発キット）の統合により、ASA 仮想 でこの機能を無効にしたときのパフォーマンスが向上します。
自動 ASP ロードバランシングが ASA 仮想 でサポートされるようになりました。	9.8(1)	以前は、ASP ロード バランシングは手動でのみ有効または無効にできました。 次のコマンドを変更しました。**asp load-balance per-packet-auto**
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	9.7(1)	長さ制限内のすべてのローカル **username** および **enable** パスワードは、SHA-512 を使用する PBKDF2（パスワードベースキー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザーが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次のコマンドを変更しました。**enable**、**username**
ISA 3000 のデュアル電源サポート	9.6(1)	ISA 3000 のデュアル電源では、ASA OS に望ましい構成としてデュアル電源を設定できます。1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA は単一電源を想定していますが、装備される電源のいずれかが機能しているかぎりアラームを発しません。 次のコマンドが導入されました。**power-supply dual**

機能名	プラットフォーム リリース	説明
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次のコマンドを変更しました。**enable**、**username**
ISA 3000 ハードウェア バイパス	9.4(1.225)	ISA 3000 は、トラフィックが電源喪失時にアプライアンスを通過し続けるようにするハードウェア バイパス機能をサポートします。 次のコマンドが導入されました。**hardware-bypass**、**hardware-bypass manual**、**hardware-bypass boot-delay**、**show hardware-bypass** この機能は、バージョン *9.5(1)* では使用できません。
自動 ASP ロード バランシング	9.3(2)	ASP ロードバランシング機能の自動切替を有効または無効に設定できるようになりました。 （注） 自動機能は ASA 仮想 ではサポートされません。手動による有効化または無効化のみがサポートされます。 次のコマンドが導入されました。**asp load-balance per-packet-auto**
デフォルトの Telnet パスワードの削除	9.0(2)、9.1(2)	ASA への管理アクセスのセキュリティ向上のために、Telnet のデフォルト ログイン パスワードが削除されました。Telnet を使用してログインする前に、パスワードを手動で設定する必要があります。 （注） ログイン パスワードが使用されるのは、Telnet ユーザー認証（**aaa authentication telnet console** コマンド）を設定しない場合の Telnet に対してのみです。 以前はパスワードをクリアすると、ASA がデフォルト「cisco」を復元していました。今ではパスワードをクリアすると、パスワードは削除されるようになりました。 ログイン パスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。最初 ASASM のアクセスでは、ログイン パスワードを設定するまで、**service-module session** コマンドを使用します。 **password** コマンドが変更されました。
パスワード暗号化の可視性	8.4(1)	**show password encryption** コマンドが変更されました。

機能名	プラットフォーム リリース	説明
マスターパスフレーズ	8.3(1)	この機能が導入されました。マスター パスフレーズを利用すると、プレーン テキストのパスワードが安全に、暗号化形式で保存され、1 つのキーを使用してすべてのパスワードを一様に暗号化またはマスキングできるようになります。このようにしても、機能は一切変更されません。 次のコマンドが導入されました。**key config-key password-encryption**、**password encryption aes**、**clear configure password encryption aes**、**show running-config password encryption aes**、**show password encryption**



第 24 章

DHCP サービスと DDNS サービス

この章では、ダイナミック DNS（DDNS）のアップデート方式のほか、DHCP サーバーまたは DHCP リレーを設定する方法について説明します。

- DHCP サービスと DDNS サービスについて （1033 ページ）
- DHCP サービスと DDNS サービスのガイドライン （1036 ページ）
- DHCP サーバーの設定 （1038 ページ）
- DHCP リレー エージェントの設定 （1044 ページ）
- ダイナミック DNS の設定 （1048 ページ）
- DHCP および DDNS サービスのモニタリング （1054 ページ）
- DHCP および DDNS サービスの履歴 （1060 ページ）

DHCP サービスと DDNS サービスについて

次の項では、DHCP サーバ、DHCP リレー エージェント、および DDNS 更新について説明します。

DHCPv4 サーバについて

DHCP は、IP アドレスなどのネットワーク構成パラメータを DHCP クライアントに提供します。ASA は、ASA インターフェイスに接続されている DHCP クライアントに、DHCP サーバーを提供します。DHCP サーバは、ネットワーク設定パラメータを DHCP クライアントに直接提供します。

IPv4 DHCP クライアントは、サーバに到達するために、マルチキャストアドレスよりもブロードキャストを使用します。DHCP クライアントは UDP ポート 68 でメッセージをリッスンし、DHCP サーバは UDP ポート 67 でメッセージをリッスンします。

DHCP オプション

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータは DHCP メッセージの Options フィールドにストアされているタグ付けされたア

イテムにより送信され、このデータはオプションとも呼ばれます。ベンダー情報も Options に保存され、ベンダー拡張情報はすべて DHCP オプションとして使用できます。

たとえば、Cisco IP Phone が TFTP サーバから設定をダウンロードする場合を考えます。Cisco IP Phone の起動時に、IP アドレスと TFTP サーバの IP アドレスの両方が事前に設定されていない場合、Cisco IP Phone ではオプション 150 または 66 を伴う要求を DHCP サーバに送信して、この情報を取得します。

- DHCP オプション 150 では、TFTP サーバのリストの IP アドレスが提供されます。
- DHCP オプション 66 では、1 つの TFTP サーバの IP アドレスまたはホスト名が与えられます。
- DHCP オプション 3 では、デフォルト ルートが設定されます。

1 つの要求にオプション 150 と 66 の両方が含まれている場合があります。この場合、両者が ASA ですでに設定されていると、DHCP サーバは、その応答で両方のオプションに対する値を提供します。

高度な DHCP オプションを使用すれば、DHCP クライアントに DNS、WINS、およびドメイン名の各パラメータを提供できます。DHCP オプション 15 は DNS ドメインのサフィックスに使用されます。DHCP 自動コンフィギュレーションの設定を使用して、これらの値を取得したり、これらを手動で定義したりできます。この情報の定義に 2 つ以上の方法を使用すると、次の優先順位で情報が DHCP クライアントに渡されます。

1. 手動で行われた設定
2. 高度な DHCP オプションの設定
3. DHCP 自動構成設定

たとえば、DHCP クライアントが受け取るドメイン名を手動で定義し、次に DHCP 自動構成を有効にできます。DHCP 自動構成によって、DNS サーバーおよび WINS サーバーとともにドメインが検出されても、手動で定義したドメイン名が、検出された DNS サーバー名および WINS サーバー名とともに DHCP クライアントに渡されます。これは、DHCP 自動構成プロセスで検出されたドメイン名よりも、手動で定義されたドメイン名の方が優先されるためです。

DHCPv6 ステートレス サーバーについて

ステートレスアドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6 プレフィックス委任クライアントの有効化（948 ページ））については、これらのクライアントが情報要求（IR）パケットを ASA に送信する際に（DNS サーバー、ドメイン名などの）情報を提供するように ASA を設定できます。ASA は IR パケットのみを受け付け、アドレスをクライアントに割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（ASA がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

DHCP リレー エージェントについて

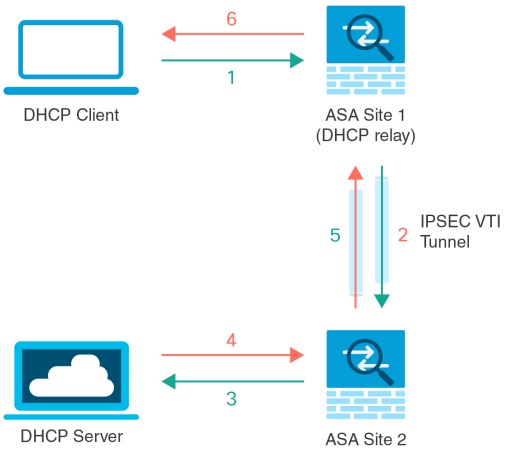
インターフェイスで受信した DHCP 要求を 1 つまたは複数の DHCP サーバに転送するように DHCP リレー エージェントを設定できます。DHCP クライアントは、最初の DHCPDISCOVER メッセージを送信するために UDP ブロードキャストを使用します。接続されたネットワークについての情報がクライアントにはないためです。サーバを含まないネットワーク セグメントにクライアントがある場合、ASA はブロードキャスト トラフィックを転送しないため、UDP ブロードキャストは通常転送されません。DHCP リレー エージェントを使用して、ブロードキャストを受信している ASA のインターフェイスが DHCP 要求を別のデバイスの DHCP サーバーに転送するように設定できます。

VTI での DHCP リレーサーバーのサポート

DHCP クライアントと DHCP サーバーの間で DHCP メッセージを受信して転送するように、ASA インターフェイスで DHCP リレーエージェントを設定できます。ただし、論理インターフェイスを介してメッセージを転送する DHCP リレーサーバーはサポートされていませんでした。

次の図は、VTI VPN 経由の DHCP リレーを使用した DHCP クライアントと DHCP サーバーの DISCOVER プロセスを示しています。ASA サイト 1 の VTI インターフェイスに設定された DHCP リレーエージェントは、DHCP クライアントから DHCPDISCOVER パケットを受信し、VTI トンネルを介してパケットを送信します。ASA サイト 2 は DHCPDISCOVER パケットを DHCP サーバーに転送します。DHCP サーバーは ASA サイト 2 に DHCPOFFER で応答します。この応答が ASA サイト 2 から DHCP リレー（ASA サイト 1）に転送され、そこから DHCP クライアントに転送されます。

図 *76 : VTI* を介した *DHCP* リレーサーバー



DHCPREQUEST および DHCPACK/NACK の要件についても同じ手順に従います。

DHCP サービスと DDNS サービスのガイドライン

この項では、DHCPおよびDDNSサービスを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モード

- DHCPv6 ステートレス サーバは、マルチ コンテキスト モードではサポートされません。

ファイアウォール モード

- DHCPリレーは、トランスペアレントファイアウォールモード、BVI上のルーテッドモードまたはブリッジ グループ メンバー インターフェイスではサポートされません。
- DHCP サーバーは、ブリッジ グループ メンバー インターフェイス上のトランスペアレント ファイアウォール モードでサポートされます。 ルーテッド モードでは、DHCP サーバーは BVI インターフェイスでサポートされますが、ブリッジ グループ メンバー インターフェイスではサポートされません。DHCP サーバーを動作させるために、BVI には名前が必要です。
- DDNS は、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。
- DHCPv6 ステートレス サーバーは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスではサポートされません。

クラスタリング

- DHCPv6 ステートレス サーバは、クラスタリングではサポートされません。

IPv6

DHCP ステートレス サーバーの IPv6 と DHCP リレーをサポートします。

DHCPv4 サーバ

- 使用可能な DHCP の最大プールは 256 アドレスです。
- 名前とIPアドレスを持つ任意のインターフェイス（物理インターフェイス、サブインターフェイス、ルーテッドモードの BVIなど）で DHCP サーバーを設定できます。
- インターフェイスごとに 1 つの DHCP サーバのみを設定できます。各インターフェイスは、専用のアドレス プールのアドレスを使用できます。しかし、DNS サーバー、ドメイン名、オプション、ping のタイムアウト、WINS サーバーなど他の DHCP 設定はグローバルに設定され、すべてのインターフェイス上の DHCP サーバーによって使用されます。

- インターフェイスで DHCP サーバーも有効になっている場合、そのインターフェイスを DHCP クライアントとして設定することはできません。スタティック IP アドレスを使用する必要があります。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- インターフェイスの DHCP アドレスを予約できます。ASA で、クライアントの MAC アドレスに基づいて、アドレスプールから DHCP クライアントに特定のアドレスが割り当てられます。
- ASA は、QIP DHCP サーバーと DHCP プロキシサービスとの併用をサポートしません。
- DHCP サーバーは、BOOTP 要求をサポートしていません。

DHCPv6 サーバ

DHCPv6 ステートレス サーバは、DHCPv6 アドレス、プレフィックス委任クライアントまたは DHCPv6 リレーが設定されているインターフェイス上で設定できません。

DHCP リレー

- 10 台までの DHCPv4 リレーサーバーを設定できます。インターフェイスごとには、4 台まで設定できます。
- 10 台までの DHCPv6 リレーサーバーを設定できます。IPv6 のインターフェイス固有のサーバーはサポートされません。
- 別々のインターフェイスで有効にする場合でも、同じデバイスで DHCP サーバーと DHCP リレーの両方を設定することはできません。いずれかのサービスタイプのみを設定できます。
- DHCP リレー サービスは、トランスペアレント ファイアウォール モード、BVI 上のルーテッド モードまたはブリッジ グループ メンバー インターフェイスでは利用できません。ただし、アクセス ルールを使用して DHCP トラフィックを通過させることはできます。DHCP 要求と応答が ASA を通過できるようにするには、2 つのアクセス ルールを設定する必要があります。1 つは内部インターフェイスから外部（UDP 宛先ポート 67）への DCHP 要求を許可するもので、もう 1 つは逆方向（UDP 宛先ポート 68）に向かうサーバーからの応答を許可するためのものです。
- IPv4 の場合、クライアントは直接 ASA に接続する必要があり、他のリレー エージェントやルータを介して要求を送信できません。IPv6 の場合、ASA は別のリレー サーバーからのパケットをサポートします。
- DHCP クライアントは、ASA が要求をリレーする DHCP サーバーとは別のインターフェイスに存在する必要があります。
- トラフィック ゾーン内のインターフェイスで DHCP リレーを有効にできません。

DDNS サービス

ファイアウォールの DDNS は、DynDNS サービスのみをサポートします。したがって、DDNS が次のシンタックスの更新 URL で設定されていることを確認します。

https://*username***:***password***@***provider-domain***/***path***?hostname=<h>&myip=<a>**

DHCP サーバーの設定

ここでは、ASA の DHCP サーバーを設定する方法について説明します。

手順

ステップ 1 DHCPv4 サーバーの有効化 （1038 ページ）。
ステップ 2 高度な DHCPv4 オプションの設定 （1040 ページ）。
ステップ 3 DHCPv6 ステートレス サーバーの設定 （1042 ページ）。

DHCPv4 サーバーの有効化

ASA のインターフェイスで DHCP サーバーをイネーブルにするには、次の手順を実行します。

手順

ステップ 1 インターフェイスの DHCP アドレス プールを作成します。ASA は各クライアントにこのプールのアドレスを 1 つ割り当て、このアドレスを一定時間だけ使用できます。これらのアドレスは、直接接続されているネットワークのための、変換されていないローカル アドレスです。

dhcpd address *ip_address_start-ip_address_end if_name*

例：

```
ciscoasa(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
```

アドレス プールは、ASA インターフェイスと同じサブネット内にある必要があります。トランスペアレント モードでは、ブリッジ グループ メンバー インターフェイスを指定します。ルーテッド モードでは、ルーテッド インターフェイスまたは BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。

ステップ 2 （任意）（ルーテッド モード）DHCP または PPPoE クライアントを実行するインターフェイスから、または VPN サーバーから取得される DNS、WINS、およびドメイン名の値を自動的に構成します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

例：

```
ciscoasa(config)# dhcpd auto_config outside interface inside
```

次のコマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定で取得されたパラメータが上書きされます。

ステップ 3 （任意）クライアントの DHCP アドレスを予約します。ASA で、クライアントの MAC アドレスに基づいて、設定されたアドレスプールから DHCP クライアントに特定のアドレスが割り当てられます。

dhcpd reserve-address *ip_address mac_address if_name*

例：

```
ciscoasa(config)# dhcpd reserve-address 10.0.1.109 030c.f142.4cde inside
```

予約済みアドレスは設定済みのアドレスプールから取得する必要があり、アドレスプールは ASA インターフェイスと同じサブネット上にある必要があります。トランスペアレント モードでは、ブリッジ グループ メンバー インターフェイスを指定します。ルーテッド モードでは、ルーテッドインターフェイスまたは BVI を指定します。ブリッジ グループ メンバー インターフェイスは指定しないでください。

ステップ 4 （オプション）DNS サーバーの IP アドレスを指定します。

dhcpd dns *dns1* [*dns2*]

例：

```
ciscoasa(config)# dhcpd dns 209.165.201.2 209.165.202.129
```

ステップ 5 （オプション）WINS サーバーの IP アドレスを指定します。WINS サーバーは最大 2 つまでです。

dhcpd wins *wins1* [*wins2*]

例：

```
ciscoasa(config)# dhcpd wins 209.165.201.5
```

ステップ 6 （任意）クライアントに許可するリース期間を変更します。リース期間とは、割り当てられた IP アドレスをクライアントが使用できる時間の長さ（秒）であり、この時間が経過するとリースは失効します。0 ～ 1,048,575 の範囲の数を入力してください。デフォルト値は 3600 秒です。

dhcpd lease *lease_length*

例：

```
ciscoasa(config)# dhcpd lease 3000
```

ステップ 7 （オプション）ドメイン名を設定します。

dhcpd domain *domain_name*

例：

```
ciscoasa(config)# dhcpd domain example.com
```

ステップ 8 （オプション）ICMP パケットの DHCP ping タイムアウト値を設定します。アドレスの競合を避けるために、ASA はアドレスを DHCP クライアントに割り当てる前に 2 つの ICMP ping パケットをそのアドレスに送信します。デフォルト値は 50 ミリ秒です。

dhcpd ping timeout *milliseconds*

例：

```
ciscoasa(config)# dhcpd ping timeout 20
```

ステップ 9 DHCP クライアントに送信するデフォルト ゲートウェイを定義します。ルーテッド モードで **dhcpd option 3 ip** コマンドを使用しない場合、ASA は、DHCP サーバーがイネーブルになっているインターフェイス IP アドレスをデフォルト ゲートウェイとして送信します。トランスペアレント モードでデフォルト ゲートウェイを設定する場合には **dhcpd option 3 ip** を設定する必要があります。ASA 自体はデフォルト ゲートウェイとして動作できません。

dhcpd option 3 ip *gateway_ip*

例：

```
ciscoasa(config)# dhcpd option 3 ip 10.10.1.1
```

ステップ 10 ASA 内の DHCP デーモンをイネーブルにし、イネーブルになったインターフェイス上で DHCP クライアント要求をリッスンします。

dhcpd enable *interface_name*

例：

```
ciscoasa(config)# dhcpd enable inside
```

dhcpd address 範囲と同じインターフェイスを指定します。

高度な DHCPv4 オプションの設定

ASA は、RFC 2132、RFC 2562、および RFC 5510 に記載されている情報を送信する DHCP オプションをサポートしています。オプション 1、12、50 ～ 54、58 ～ 59、61、67、82 を除き、すべての DHCP オプション（1 ～ 255）がサポートされています。

手順

ステップ 1 1 つまたは 2 つの IP アドレスを返す DHCP オプションを設定します。

dhcpd option *code* **ip** *addr_1* [*addr_2*]

例：

```
ciscoasa(config)# dhcpd option 150 ip 10.10.1.1
ciscoasa(config)# dhcpd option 3 ip 10.10.1.10
```

オプション 150 では、Cisco IP Phone で使用する 1 台または 2 台の TFTP サーバーの IP アドレスまたは名前を指定します。オプション 3 では、Cisco IP Phone のデフォルト ルートを設定します。

ステップ 2 テキスト文字列を返す DHCP オプションを設定します。

dhcpd option *code* **ascii** *text*

例：

```
ciscoasa(config)# dhcpd option 66 ascii exampleserver
```

オプション 66 では、Cisco IP Phone で使用する TFTP サーバーの IP アドレスまたは名前を指定します。

ステップ 3 16 進数値を返す DHCP オプションを設定します。

dhcpd option code hex *value*

例：

```
ciscoasa(config)# dhcpd option 2 hex 22.0011.01.FF1111.00FF.0000.AAAA.1111.1111.1111.11
```

（注）
ASA は、指定されたオプションのタイプおよび値が、RFC 2132 に定義されているオプションコードに対して期待されているタイプおよび値と一致するかどうかは確認しません。たとえば、**dhcpd option 46 ascii hello** というコマンドを入力することは可能であり、ASA はこのコンフィギュレーションを受け入れますが、RFC 2132 の定義では、オプション 46 には 1 桁の 16 進数値を指定することになっています。オプション コードと、コードに関連付けられたタイプおよび期待値の詳細については、RFC 2132 を参照してください。

次の表に、**dhcpd option** コマンドでサポートされていない DHCP オプションを示します。

表 *33 :* サポートされていない *DHCP* オプション

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

DHCPv6 ステートレス サーバーの設定

ステートレス アドレス自動設定（SLAAC）をプレフィックス委任機能と併せて使用するクライアント（IPv6 プレフィックス委任クライアントの有効化（948 ページ））については、これらのクライアントが情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけでクライアントにアドレスを割り当てません。クライアントが独自の IPv6 アドレスを生成するように設定するには、クライアントで IPv6 自動設定を有効にします。クライアントでステートレスな自動設定を有効にすると、ルータ アドバタイズメント メッセージで受信したプレフィックス（ASA がプレフィックス委任を使用して受信したプレフィックス）に基づいて IPv6 アドレスが設定されます。

始める前に

この機能は、シングル ルーテッド モードでのみサポートされます。この機能は、クラスタリングではサポートされていません。

手順

ステップ 1 DHCPv6 サーバーに提供させる情報が含まれる IPv6 DHCP プールを設定します。

ipv6 dhcp pool *pool_name*

例：

```
ciscoasa(config)# ipv6 dhcp pool Inside-Pool
ciscoasa(config)#
```

必要に応じてインターフェイスごとに個別のプールを設定できます。また、複数のインターフェイスで同じプールを使用することもできます。

ステップ 2 次のうち、IR メッセージに対する応答でクライアントに提供するパラメータを 1 つ以上設定します。

dns-server *dns_ipv6_address*

domain-name *domain_name*

nis address *nis_ipv6_address*

nis domain-name *nis_domain_name*

nisp address *nisp_ipv6_address*

nisp domain-name *nisp_domain_name*

sip address *sip_ipv6_address*

sip domain-name *sip_domain_name*

sntp address *sntp_ipv6_address*

import{[**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**]}

例：

```
ciscoasa(config-dhcpv6)# domain-name example.com
ciscoasa(config-dhcpv6)# import dns-server
```

import コマンドは、プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用します。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じパラメータを手動で設定し、かつ **import** コマンドで設定することはできません。

ステップ 3 ASA に IR メッセージをリッスンさせるインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabithethernet 0/0
ciscoasa(config-if)#
```

ステップ 4 DHCPv6 サーバーをイネーブルにします。

ipv6 dhcp server *pool_name*

例：

```
ciscoasa(config-if)# ipv6 dhcp server Inside-Pool
ciscoasa(config-if)#
```

ステップ 5 DHCPv6 サーバーに関する情報を SLAAC クライアントに提供するためのルータ アドバタイズメントを設定します。

ipv6 nd other-config-flag

このフラグは、DHCPv6 から DNS サーバー アドレスなどの追加情報の取得に DHCPv6 を使用する必要があることを IPv6 自動設定クライアントに通知します。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
  domain-name eng.example.com
  import dns-server
ipv6 dhcp pool IT-Pool
  domain-name it.example.com
  import dns-server
interface gigabitethernet 0/0
  ipv6 address dhcp setroute default
  ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
  ipv6 address Outside-Prefix ::1:0:0:0:1/64
  ipv6 dhcp server Eng-Pool
  ipv6 nd other-config-flag
interface gigabitethernet 0/2
  ipv6 address Outside-Prefix ::2:0:0:0:1/64
  ipv6 dhcp server IT-Pool
  ipv6 nd other-config-flag
```

DHCP リレー エージェントの設定

インターフェイスに DHCP 要求が届くと、ユーザーの設定に基づいて、ASA からその要求がリレーされる DHCP サーバーが決定されます。設定できるサーバーのタイプは次のとおりです。

- インターフェイス固有の DHCP サーバー：特定のインターフェイスに DHCP 要求が届くと、ASA はその要求をインターフェイス固有のサーバーにだけリレーします。
- グローバル DHCP サーバー：インターフェイス固有のサーバーが設定されていないインターフェイスに DHCP 要求が届くと、ASA はその要求をすべてのグローバル サーバーにリレーします。インターフェイスにインターフェイス固有のサーバーが設定されている場合、グローバル サーバーは使用されません。

DHCPv4 リレー エージェントの設定

DHCP 要求がインターフェイスに届くと、ASA はその要求を DHCP サーバーにリレーします。

手順

ステップ 1 次のいずれかまたは両方を実行します。

- グローバル DHCP サーバーの IP アドレスおよびそのサーバーに到達可能なインターフェイスを指定します。

  dhcprelay server *ip_address if_name*

  例：

```
ciscoasa(config)# dhcprelay server 209.165.201.5 outside
ciscoasa(config)# dhcprelay server 209.165.201.8 outside
ciscoasa(config)# dhcprelay server 209.165.202.150 it
```

- DHCP クライアント ネットワークに接続されているインターフェイス ID、およびそのインターフェイスで受信した DHCP 要求に対して使用される DHCP サーバーの IP アドレスを指定します。

```
interface interface_id
  dhcprelay server ip_address
```

  例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config)# dhcprelay server 209.165.201.6
ciscoasa(config)# dhcprelay server 209.165.201.7
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config)# dhcprelay server 209.165.202.155
ciscoasa(config)# dhcprelay server 209.165.202.156
```

  グローバル **dhcprelay server** コマンドとは異なり、要求の出力インターフェイスは指定しないことに注意してください。代わりに、ASA はルーティング テーブルを使用して出力インターフェイスを決定します。

ステップ 2 DHCP クライアントに接続されたインターフェイス上で DHCP リレー サービスをイネーブルにします。複数のインターフェイス上で DHCP リレーをイネーブルにできます。

dhcprelay enable *interface*

例：

```
ciscoasa(config)# dhcprelay enable inside
ciscoasa(config)# dhcprelay enable dmz
ciscoasa(config)# dhcprelay enable eng1
ciscoasa(config)# dhcprelay enable eng2
ciscoasa(config)# dhcprelay enable mktg
```

ステップ 3 （オプション）DHCP リレーのアドレス処理のために許容する時間を秒数で設定します。

dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# dhcprelay timeout 25
```

ステップ 4 （オプション）DHCP サーバーから送信されたパケットの最初のデフォルト ルータ アドレスを、ASA インターフェイスのアドレスに変更します。

dhcprelay setroute *interface_name*

例：

```
ciscoasa(config)# dhcprelay setroute inside
```

このアクションを行うと、クライアントは、自分のデフォルトルートを設定して、DHCP サーバーで異なるルータが指定されている場合でも、ASA をポイントすることができます。

パケット内にデフォルトのルータ オプションがなければ、ASA は、そのインターフェイスのアドレスを含んでいるデフォルト ルータを追加します。

ステップ 5 （オプション）インターフェイスを信頼できるインターフェイスとして設定します。次のいずれかを実行します。

- 信頼する DHCP クライアント インターフェイスを指定します。

```
interface interface_id
  dhcprelay information trusted
```

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# dhcprelay information trusted
```

DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できます。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP

リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレーエージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。

- すべてのクライアント インターフェイスを信頼するインターフェイスとして設定します。

  dhcprelay information trust-all

  例：

```
ciscoasa(config)# dhcprelay information trust-all
```

DHCPv6 リレー エージェントの設定

インターフェイスに DHCPv6 要求が届くと、ASA はその要求をすべての DHCPv6 グローバル サーバーにリレーします。

手順

ステップ 1 クライアント メッセージの転送先となる IPv6 DHCP サーバーの宛先アドレスを指定します。

ipv6 dhcprelay server *ipv6_address* [*interface*]

例：

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701
```

ipv6-address 引数には、リンク スコープのユニキャスト、マルチキャスト、サイト スコープのユニキャスト、またはグローバル IPv6 アドレスを指定できます。リレー宛先の指定は必須です。ループバックやノードローカルのマルチキャストアドレスは指定できません。オプションの *interface* 引数では、宛先に対する出力インターフェイスを指定します。クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。指定したアドレスがリンク スコープのアドレスである場合は、インターフェイスを指定する必要があります。

ステップ 2 インターフェイス上で DHCPv6 リレー サービスをイネーブルにします。

ipv6 dhcprelay enable *interface*

例：

```
ciscoasa(config)# ipv6 dhcprelay enable inside
```

ステップ 3 （オプション）リレーアドレスの処理のために、リレーバインディングを通してDHCPv6サーバからの応答を DHCPv6 クライアントに渡すときに許容する時間を秒数で指定します。

ipv6 dhcprelay timeout *seconds*

例：

```
ciscoasa(config)# ipv6 dhcprelay timeout 25
```

seconds 引数の有効な値の範囲は 1 ～ 3600 です。デフォルトは 60 秒です。

ダイナミック DNS の設定

インターフェイスでDHCP IPアドレッシングを使用している場合、DHCP リースが更新されると、割り当てられたIPアドレスが変更されることがあります。完全修飾ドメイン名（FQDN）を使用してインターフェイスに到達できる必要がある場合、この IP アドレスの変更が原因で DNS サーバーのリソースレコード（RR）が古くなる可能性があります。ダイナミック DNS（DDNS）は、IPアドレスまたはホスト名が変更されるたびにDNSのRRを更新するメカニズムです。DDNS はスタティックまたは PPPoE IP アドレッシングにも使用できます。

DDNS では DNS サーバーの A RR と PTR RR を更新します。A RR には名前から IP アドレスへのマッピングが含まれ、PTR RR でアドレスが名前にマッピングされます。

ASA では、次の DDNS 更新方式をサポートしています。

- 標準の DDNS：標準の DDNS 更新方式は RFC 2136 で定義されています。

  この方式では、ASA と DHCP サーバーで DNS 要求を使用して DNS の RR を更新します。ASA または DHCP サーバーは、ローカル DNS サーバーにホスト名に関する情報を求める DNS 要求を送信し、その応答に基づいて RR を所有するメイン DNS サーバーを特定します。その後、ASA または DHCP サーバーからメイン DNS サーバーに更新要求が直接送信されます。一般的なシナリオを次に示します。

  - ASA で A RR を更新し、DHCP サーバーで PTR RR を更新する。

    通常、ASA が A RR を「所有」し、DHCP サーバーが PTR RR を「所有」するため、両方のエンティティで個別に更新を要求する必要があります。IPアドレスまたはホスト名が変更されると、ASA から DHCP サーバーに DHCP 要求（FQDN オプションを含む）が送信され、PTR RR の更新を要求する必要があることが通知されます。

  - DHCP サーバーで A RR と PTR RR の両方を更新する。

    このシナリオは、ASA に A RR を更新する権限がない場合に使用します。IPアドレスまたはホスト名が変更されると、ASA から DHCP サーバーに DHCP 要求（FQDN オプションを含む）が送信され、A RR と PTR RR の更新を要求する必要があることが通知されます。

セキュリティのニーズやメイン DNS サーバーの要件に応じて、異なる所有権を設定できます。たとえば、スタティックアドレスの場合、ASA で両方のレコードの更新を所有します。

- Web：Web 更新方式では、DynDNS リモート API 仕様（https://help.dyn.com/remote-access-api/）を使用します。

  この方式では、IP アドレスまたはホスト名が変更されると、ASA からアカウントを持っている DNS プロバイダーに HTTP 要求が直接送信されます。

（注） DDNS は BVI またはブリッジグループのメンバーインターフェイスではサポートされません。

始める前に

- **[Configuration]** > **[Device Management]** > **[DNS]** > **[DNS Client]** で DNS サーバーを設定します。「DNS サーバーの設定 （1020 ページ）」を参照してください。
- **[Configuration]** > **[Device Setup]** > **[Device Name/Password]** でデバイスのホスト名とドメイン名を設定します。「ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （1005 ページ）」を参照してください。インターフェイスごとにホスト名を指定しない場合は、デバイスのホスト名が使用されます。FQDN を指定しない場合、スタティックまたは PPPoE IP アドレッシングにおいては、システムのドメイン名または DNS サーバーのドメイン名がホスト名に追加されます。

手順

ステップ 1 標準の DDNS 方式：ASA からの DNS 要求を有効にするように DDNS 更新方式を設定します。

すべての要求を DHCP サーバーで実行する場合は、DDNS 更新方式を設定する必要はありません。

a) 更新方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method ddns1
ciscoasa(DDNS-update-method)#
```

b) 標準の DDNS 方式を指定します。

ddns [**both**]

デフォルトでは、ASA は A RR のみを更新します。DHCP サーバーで PTR RR を更新する場合は、この設定を使用します。ASA で A RR と PTR RR の両方を更新する場合は、**both**

を指定します。スタティックまたは PPPoE IP アドレッシングには、**both** キーワードを使用します。

例：

```
ciscoasa(DDNS-update-method)# ddns
```

c) （任意） DNS 要求の更新間隔を設定します。

interval maximum *days hours minutes seconds*

デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、*days*（0 ～ 364）、*hours*、*minutes*、*seconds* で間隔を設定します。

例：

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

d) この方式をインターフェイスに関連付けます。「ステップ 3（1051 ページ）」を参照してください。

ステップ 2 Web 方式：ASA からの HTTP 更新要求を有効にするように DDNS 更新方式を設定します。

a) 更新方式を作成します。

ddns update method *name*

例：

```
ciscoasa(config)# ddns update method web1
ciscoasa(DDNS-update-method)#
```

b) DDNS サーバー証明書の ID を検証するための参照 ID 名を指定します。ASA は、ホスト名の一致を見つけようとします。ホストの解決に失敗するか一致するものが見つからない場合、接続は終了します。

例：

```
ciscoasa(DDNS-update-method)# web reference-identity dyndns
```

c) Web 方式と更新 URL を指定します。

web update-url https://*username***:***password***@***provider-domain/path***?hostname=<h>&myip=<a>**

疑問符（?）文字を入力する前に、キーボードの Ctrl キーと v キーを一緒に押します。これにより、? がソフトウェアでヘルプ照会と解釈されなくなり、? を入力できます。

例：

```
ciscoasa(DDNS-update-method)#
web update-url
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
```

d) （任意） 更新するアドレスタイプ（IPv4 または IPv6）を指定します。

デフォルトでは、ASA はすべての IPv4 アドレスと IPv6 アドレスを更新します。アドレスを制限する場合は、次のコマンドを入力します。

web update-type {**ipv4** | **ipv6** [**all**] | **both** [**all**]}

- **both all**：（デフォルト）すべての IPv4 アドレスと IPv6 アドレスを更新します。
- **both**：IPv4 アドレスと最新の IPv6 アドレスを更新します。
- **ipv4**：IPv4 アドレスのみを更新します。
- **ipv6**：最新の IPv6 アドレスのみを更新します。
- **ipv6 all**：すべての IPv6 アドレスを更新します。

例：

```
ciscoasa(DDNS-update-method)# web update-type ipv4
```

e) （任意） DNS 要求の更新間隔を設定します。

interval maximum *days hours minutes seconds*

デフォルトでは、すべての値が 0 に設定され、IP アドレスまたはホスト名が変更されるたびに更新要求が送信されます。要求を定期的に送信するには、*days*（0 ～ 364）、*hours*、*minutes*、*seconds* で間隔を設定します。

例：

```
ciscoasa(DDNS-update-method)# interval maximum 0 0 15 0
```

f) この方式をインターフェイスに関連付けます。「ステップ 3 （1051 ページ）」を参照してください。

g) Web タイプ方式の DDNS の場合は、HTTPS 接続用の DDNS サーバ証明書の検証のために DDNS サーバのルート CA も識別する必要があります。ステップ 4 （1053 ページ）を参照してください。

ステップ 3 DDNS のインターフェイス設定として、このインターフェイスの更新方式、DHCP クライアント設定、ホスト名などを設定します。

a) インターフェイス コンフィギュレーション モードを開始します。

interface *id*

例：

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)#
```

b) 更新方式を割り当てます。

ddns update *name*

標準の DDNS 方式：すべての更新を DHCP サーバーで実行する場合は、方式を割り当てる必要はありません。 このコマンドは、Web アップデート方式の場合に必要です。

例：

```
ciscoasa(config-if)# ddns update ddns1
```

c) このインターフェイスのホスト名を割り当てます。

ddns update hostname *hostname*

ホスト名を設定しない場合は、デバイスのホスト名が使用されます。FQDN を指定しない場合、システムのドメイン名または DNS サーバーグループのデフォルトのドメイン（スタティックまたは PPPoE IP アドレッシングの場合）、または DHCP サーバーのドメイン名（DHCP IP アドレッシングの場合）が追加されます。

例：

```
ciscoasa(config-if)# ddns update hostname asa1.example.com
```

d) 標準の DDNS 方式：DHCP サーバーで更新するレコードを指定します。

dhcp client update dns [**server** {**both** | **none**}]

ASA から DHCP サーバーに DHCP クライアント要求が送信されます。DHCP サーバーも DDNS をサポートするように設定する必要があることに注意してください。サーバーはクライアント要求を受け入れるように設定できるほか、クライアントをオーバーライドすることもできます（この場合、サーバーで実行している更新をクライアントで実行しないようにクライアントに応答します）。クライアントで DDNS 更新を要求しなくても、DHCP サーバーから更新を送信するように設定できます。

スタティックまたは PPPoE IP アドレッシングの場合、これらの設定は無視されます。

（注）
これらの値は、**dhcp-client update dns** コマンドを使用して、すべてのインターフェイスに対してグローバルに設定することもできます。インターフェイスごとの設定は、グローバル設定よりも優先されます。

- デフォルト（キーワードなし）：DHCP サーバーで PTR RR の更新を実行するように要求します。この設定は、**ddns** で A レコードを有効にした DDNS 更新方式と連携して機能します。
- **server both**：DHCP サーバーで A RR と PTR RR の両方の更新を実行するように要求します。この設定では、DDNS 更新方式をインターフェイスに関連付ける必要はありません。
- **server none**：DHCP サーバで更新を実行しないように要求します。この設定は、**ddns both** で A レコードと PTR レコードを有効にした DDNS 更新方式と連携して機能します。

例：

```
ciscoasa(config-if)# ddns client update dns
```

ステップ 4 Web 方式の DDNS の場合は、HTTPS 接続用の DDNS サーバー証明書の検証のために DDNS サーバーのルート CA も識別する必要があります。「トラストポイントの設定（1078ページ）」を参照してください。

例：

```
crypto ca trustpoint DDNS_Trustpoint
  enrollment terminal
crypto ca authenticate DDNS_Trustpoint nointeractive
   MIIFWjCCA0KgAwIBAgIQbkepxUtHDA3sM9CJuRz04TANBgkqhkiG9w0BAQwFADBH
   MQswCQYDVQQGEwJVUzEiMCAGA1UEChMZR29vZ2xlIFRydXN0IFNlcnZpY2VzIExM
   [...]
   quit
```

スタティック IP アドレスの標準の DDNS 方式

次に、スタティック IP アドレスで使用する標準の DDNS 方式を設定する例を示します。このシナリオでは、DHCP クライアント設定は設定しません。

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
 ddns both
interface gigabitethernet1/1
 ip address 209.165.200.225
! Associate the method with the interface:
 ddns update ddns-2
 ddns update hostname asa1.example.com
```

例：標準の DDNS 方式：ASA で A RR を更新し、DHCP サーバーで PTR RR を更新する

次に、ASA で A RR を更新し、DHCP サーバーで PTR RR を更新するように設定する例を示します。

```
! Define the DDNS method to update the A RR:
ddns update method ddns-1
 ddns
interface gigabitethernet1/1
  ip address dhcp
! Associate the method with the interface:
  ddns update ddns-1
  ddns update hostname asa
! Set the client to update the A RR, and the server to update the PTR RR:
  dhcp client update dns
```

例：標準の DDNS 方式：DHCP サーバーで RR を更新しない

次に、ASA で A RR と PTR RR の両方を更新するように設定し、DHCP サーバーで RR を更新しないように要求する例を示します。

```
! Define the DDNS method to update both RRs:
ddns update method ddns-2
  ddns both
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update ddns-2
  ddns update hostname asa1.example.com
! Set the client to update both RRs, and the server to update none:
  dhcp client update dns server none
```

例：標準の DDNS 方式：DHCP サーバーで両方の RR を更新する

次に、DHCP クライアントからの要求に応じて DHCP サーバーで A RR と PTR RR の両方を更新するように設定する例を示します。すべての更新をサーバーで実行するため、更新方式をインターフェイスに関連付ける必要はありません。

```
interface gigabitethernet1/1
  ip address dhcp
  ddns update hostname asa
! Configure the DHCP server to update both RRs:
  dhcp client update dns server both
```

例：Web タイプ

次に、Web タイプ方式を設定する例を示します。

```
! Define the web type method:
ddns update method web-1
  web update-url
https://captainkirk:enterpr1s3@domains.cisco.com/ddns?hostname=<h>&myip=<a>
! Associate the method with the interface:
interface gigabitethernet1/1
  ip address dhcp
  ddns update web-1
  ddns update hostname asa2.example.com
```

DHCP および DDNS サービスのモニタリング

この項では、DHCPおよびDDNSの両方のサービスをモニターする手順について説明します。

DHCP サービスのモニタリング

- **show dhcpd** {**binding** [*IP_address*] | **state** | **statistics**}

  このコマンドは、現在の DHCP サーバー クライアント バインディング、状態と統計情報を示します。

- **show dhcprelay** {**state** | **statistics**}

  このコマンドは、DHCP リレー ステータスと統計情報を表示します。

- **show ipv6 dhcprelay binding**

  このコマンドは、リレー エージェントによって作成されたリレー バインディング エントリを表示します。

- **show ipv6 dhcprelay statistics**

  このコマンドは、IPv6 の DHCP リレー エージェントの統計情報を表示します。

- **show ipv6 dhcp server statistics**

  このコマンドは、DHCPv6 ステートレス サーバーの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config)# show ipv6 dhcp server statistics

Protocol Exchange Statistics:
  Total number of Solicit messages received:             0
  Total number of Advertise messages sent:               0
  Total number of Request messages received:             0
  Total number of Renew messages received:               0
  Total number of Rebind messages received:              0
  Total number of Reply messages sent:                   10
  Total number of Release messages received:             0
  Total number of Reconfigure messages sent:             0
  Total number of Information-request messages received: 10
  Total number of Relay-Forward messages received:       0
  Total number of Relay-Reply messages sent:             0

Error and Failure Statistics:
  Total number of Re-transmission messages sent:                  0
  Total number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp pool** [*pool_name*]
- **show ipv6 dhcp interface** [*ifc_name* [**statistics**]]

  show ipv6 dhcp interface コマンドは、すべてのインターフェイスの DHCPv6 情報を表示します。インターフェイスが DHCPv6 ステートレス サーバー構成用に設定されている場合（DHCPv6 ステートレス サーバーの設定 （1042 ページ） を参照）、このコマンドはサーバーによって使用されている DHCPv6 プールをリストします。インターフェイスに DHCPv6 アドレス クライアントまたはプレフィックス委任クライアントの設定がある場合、このコマンドは各クライアントの状態とサーバーから受信した値を表示します。特定のインターフェイスについて、DHCP サーバーまたはクライアントのメッセージの統計情報を表示できます。次に、このコマンドで提供される情報例を示します。

```
ciscoasa(config-if)# show ipv6 dhcp interface
GigabitEthernet1/1 is in server mode
  Using pool: Sample-Pool

GigabitEthernet1/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:03:46
  Address State is OPEN
  Renew for address will be sent in 00:03:47
  List of known servers:
    Reachable via address: fe80::20c:29ff:fe96:1bf4
    DUID: 000100011D9D1712005056A07E06
```

```
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00030001, T1 250, T2 400
        Prefix: 2005:abcd:ab03::/48
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      IA NA: IA ID 0x00030001, T1 250, T2 400
        Address: 2004:abcd:abcd:abcd:abcd:abcd:abcd:f2cb/128
                preferred lifetime 500, valid lifetime 600
                expires at Nov 26 2014 03:11 PM (577 seconds)
      DNS server: 2004:abcd:abcd:abcd::2
      DNS server: 2004:abcd:abcd:abcd::4
      Domain name: relay.com
      Domain name: server.com
      Information refresh time: 0
  Prefix name: Sample-PD

Management1/1 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 11:26:44
  List of known servers:
    Reachable via address: fe80::4e00:82ff:fe6f:f6f9
    DUID: 000300014C00826FF6F8
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x000a0001, T1 43200, T2 69120
        Address: 2308:2308:210:1812:2504:1234:abcd:8e5a/128
                preferred lifetime INFINITY, valid lifetime INFINITY
      Information refresh time: 0


ciscoasa(config-if)# show ipv6 dhcp interface outside statistics

DHCPV6 Client PD statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0

DHCPV6 Client address statistics:

Protocol Exchange Statistics:


 Number of Solicit messages sent:              1
 Number of Advertise messages received:        1
 Number of Request messages sent:              1
 Number of Renew messages sent:                45
```

```
 Number of Rebind messages sent:               0
 Number of Reply messages received:            46
 Number of Release messages sent:              0
 Number of Reconfigure messages received:      0
 Number of Information-request messages sent:  0

Error and Failure Statistics:


 Number of Re-transmission messages sent:                 1
 Number of Message Validation errors in received messages: 0
```

- **show ipv6 dhcp ha statistics**

  show ipv6 dhcp ha statistics コマンドは、DUID 情報がフェールオーバー ユニット間で同期された回数を含め、フェールオーバーユニット間のトランザクションの統計情報を表示します。次に、このコマンドで提供される情報例を示します。

  アクティブ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              1
  DUID sync messages received:          0

DHCPv6 HA error statistics:
  Send errors:                          0
```

  スタンドバイ ユニット上：

```
ciscoasa(config)# show ipv6 dhcp ha statistics

DHCPv6 HA global statistics:
  DUID sync messages sent:              0
  DUID sync messages received:          1

DHCPv6 HA error statistics:
  Send errors:                          0
```

VTI を介した DHCP リレーのトラブルシューティング

DHCP クライアントで IP アドレスを取得できない場合は、次の手順を実行します。

- 両方の ASA サイトのトンネルインターフェイス/VTI 設定を確認します。
- **show crypto ipsec sa** コマンドを使用して、サイト間で転送されたパケットを確認します。

  例

```
ciscoasa(config)# show crypto ipsec sa
interface: outside
Crypto map tag: cmap, seq num: 10, local addr: 192.168.2.111
access-list CSM_IPSEC_ACL_0 extended permit ip any4 any4
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
current_peer: 192.168.2.110
#pkts encaps: 1, #pkts encrypt: 1, #pkts digest: 1
#pkts decaps: 2, #pkts decrypt: 2, #pkts verify: 2
```

デバッグコマンドの有効化

DHCP リレーのデバッグを有効にすると、DISCOVER/REQUEST パケットが DHCP リレーサーバーに転送されたかどうかを確認できます。

- **debug dhcprelay event 255**
- **debug dhcprelay packet 255**
- **debug dhcprelay error 255**

例

```
ciscoasa(config)# DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
DHCP: Received a BOOTREQUEST from interface 2 (size = 548)
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPRA: setting giaddr to 192.168.1.111. dhcpd_forward_request: request from xxxx.xxxx.xxxx
forwarded to 192.168.3.112.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on vti interface
DHCP: Received a BOOTREPLY from relay interface 5 (size = 300, xid = xxxxxxxxx) at
04:40:52
UTC Tue Sep 10 2019
DHCPRA: relay binding found for client xxxx.xxxx.xxxx.
DHCPD/RA: creating ARP entry (192.168.1.88, xxxx.xxxx.xxxx).
DHCPRA: Adding rule to allow client to respond using offered address 192.168.1.95
DHCPRA: forwarding reply to client xxxx.xxxx.xxxx.
DHCPD/RA: Relay msg received, fip=ANY, fport=0 on inside interface
```

DDNS ステータスのモニタリング

DDNS ステータスのモニタリングについては、次のコマンドを参照してください。

- **show ddns update** { **interface** *if_name* | **method** [*name*]}

  このコマンドは、DDNS 更新ステータスを表示します。

  次の例は、DDNS 更新方式の詳細を示しています。

```
ciscoasa# show ddns update method ddns1

Dynamic DNS Update Method: ddns1
  IETF standardized Dynamic DNS 'A' record update
```

  次の例は、Web 更新方式の詳細を示しています。

```
ciscoasa# show ddns update method web1

Dynamic DNS Update Method: web1
 Dynamic DNS updated via HTTP(s) protocols
  URL used to update record:
https://cdarwin:*****@ddns.cisco.com/update?hostname=<h>&myip=<a>
```

次の例は、DDNS インターフェイスに関する情報を示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available
```

次の例は、Web タイプの更新が成功したことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Success
FQDN : asa1.example.com
IP addresses(s): 10.10.32.45,2001:DB8::1
```

次の例は、Web タイプの更新が失敗したことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Could not establish a connection to the server
```

次の例は、DNS サーバーから Web タイプの更新のエラーが返されたことを示しています。

```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update attempted on 09:01:52.729 UTC Mon Mar 23 2020
Status : Failed
Reason : Server error (Error response from server)
```

次の例は、IP アドレスが設定されていないか DHCP 要求が失敗したために、Web 更新がまだ試行されていないことを示しています。

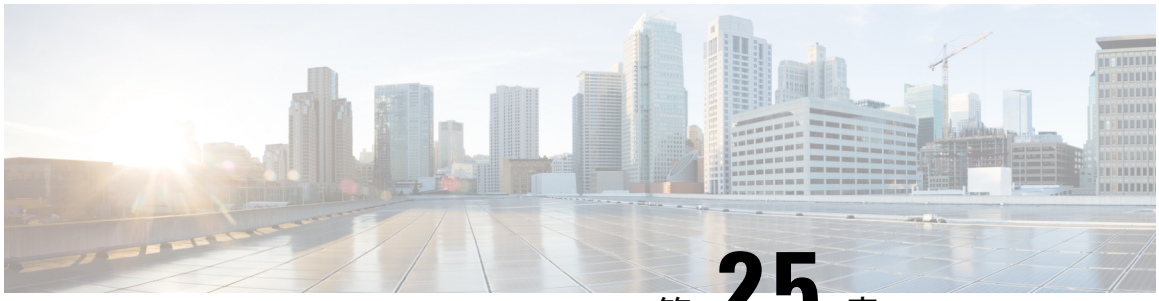
```
ciscoasa# show ddns update interface outside

Dynamic DNS Update on outside:
  Update Method Name            Update Destination
  test                          not available

Last Update Not attempted
```

DHCP および DDNS サービスの履歴

機能名	プラットフォーム リリース	説明
DDNS の Web 更新方式のサポート	9.15(1)	DDNS の Web 更新方式を使用するようにインターフェイスを設定できるようになりました。 新規/変更されたコマンド： **show ddns update interface**、**show ddns update method**、**web update-url**、**web update-type**
VTI での DHCP リレーサーバーのサポート	9.14(1)	VTI で DHCP リレーを有効にできるようになりました。 新規/変更されたコマンド： **dhcprelay server**
DHCP の予約	9.13(1)	ASA で DHCP の予約がサポートされます。DHCP サーバーで、クライアントの MAC アドレスに基づいて、定義されたアドレスプールから DHCP クライアントにスタティック IP アドレスが割り当てられます。 新規/変更されたコマンド： **dhcpd reserve-address**
IPv6 DHCP	9.6(2)	ASA で IPv6 アドレッシングの次の機能がサポートされました。 • DHCPv6 アドレス クライアント：ASA は DHCPv6 サーバーから IPv6 グローバル アドレスとオプションのデフォルト ルートを取得します。 • DHCPv6 プレフィックス委任クライアント：ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。 • 委任プレフィックスの BGP ルータ アドバタイズメント • DHCPv6 ステートレス サーバー：SLAAC クライアントが ASA に情報要求（IR）パケットを送信すると、ASA はドメインインネームなどの他の情報を SLAAC クライアントに提供します。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。 次のコマンドが追加または変更されました。**clear ipv6 dhcp statistics**、**domain-name**、**dns-server**、**import**、**ipv6 address**、**ipv6 address dhcp**、**ipv6 dhcp client pd**、**ipv6 dhcp client pd hint**、**ipv6 dhcp pool**、**ipv6 dhcp server**、**network**、**nis address**、**nis domain-name**、**nisp address**、**nisp domain-name**、**show bgp ipv6 unicast**、**show ipv6 dhcp**、**show ipv6 general-prefix**、**sip address**、**sip domain-name**、**sntp address**
DHCPv6 モニタリング	9.4(1)	IPv6 の DHCP 統計情報および IPv6 の DHCP バインディングをモニターできます。

機能名	プラットフォーム リリース	説明
DHCP リレー サーバーは、応答用の DHCP サーバー識別子を確認します。	9.2(4)/ 9.3(3)	ASA DHCP リレー サーバーが不適切な DHCP サーバーから応答を受信すると、応答を処理する前に、その応答が適切なサーバーからのものであることを確認するようになりました。導入または変更されたコマンドはありません。変更された ASDM 画面はありません。 導入または変更されたコマンドはありません。
DHCP 再バインド機能	9.1(4)	DHCP 再バインド フェーズに、クライアントはトンネル グループ リスト内の他の DHCP サーバーへの再バインドを試みるようになりました。このリリース以前には、DHCP リースの更新に失敗した場合、クライアントは代替サーバーへ再バインドしませんでした。 導入または変更されたコマンドはありません。
DHCP の信頼できるインターフェイス	9.1(2)	DHCP Option 82 を維持するために、インターフェイスを信頼できるインターフェイスとして設定できるようになりました。DHCP Option 82 は、DHCP スヌーピングおよび IP ソース ガードのために、ダウンストリームのスイッチおよびルータによって使用されます。通常、ASA DHCP リレー エージェントが Option 82 をすでに設定した DHCP パケットを受信しても、giaddr フィールド（サーバーにパケットを転送する前に、リレー エージェントによって設定された DHCP リレー エージェント アドレスを指定するフィールド）が 0 に設定されている場合は、ASA はそのパケットをデフォルトで削除します。インターフェイスを信頼できるインターフェイスとして指定することで、Option 82 を維持したままパケットを転送できます。 **dhcprelay information trusted**、**dhcprelay information trust-all**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
インターフェイスごとの DHCP リレー サーバー（IPv4 のみ）	9.1(2)	DHCP リレー サーバーをインターフェイスごとに設定できるようになりました。特定のインターフェイスに届いた要求は、そのインターフェイス用に指定されたサーバーに対してのみリレーされます。インターフェイス単位の DHCP リレーでは、IPv6 はサポートされません。 **dhcprelay server**（インターフェイス設定モード）、**clear configure dhcprelay**、**show running-config dhcprelay** の各コマンドが導入または変更されました。
DHCP relay for IPv6 (DHCPv6)	9.0(1)	DHCP リレーに IPv6 サポートが追加されました。 **ipv6 dhcprelay server**、**ipv6 dhcprelay enable**、**ipv6 dhcprelay timeout**、**clear config ipv6 dhcprelay**、**ipv6 nd managed-config-flag**、**ipv6 nd other-config-flag**、**debug ipv6 dhcp**、**debug ipv6 dhcprelay**、**show ipv6 dhcprelay binding**、**clear ipv6 dhcprelay binding**、**show ipv6 dhcprelay statistics**、**clear ipv6 dhcprelay statistics** の各コマンドが導入されました。

機能名	プラットフォーム リリース	説明
DDNS	7.0(1)	この機能が導入されました。 **ddns**、**ddns update**、**dhcp client update dns**、**dhcpd update dns**、**show running-config ddns**、および **show running-config dns server-group** の各コマンドが導入されました。
DHCP	7.0(1)	ASA は、DHCP サーバーまたは DHCP リレー サービスを ASA のインターフェイスに接続されている DHCP クライアントに提供することができます。 次のコマンドを導入しました。**dhcp client update dns**、 **dhcpd address**、 **dhcpd domain**、**dhcpd enable**、 **dhcpd lease**、**dhcpd option**、**dhcpd ping timeout**、**dhcpd update dns**、**dhcpd wins**、**dhcp-network-scope**、**dhcprelay enable**、**dhcprelay server**、**dhcprelay setroute**、**dhcp-server**、**show running-config dhcpd**、および **show running-config dhcprelay**。



第 25 章

デジタル証明書

この章では、デジタル証明書の設定方法について説明します。

- デジタル証明書の概要 （1063 ページ）
- デジタル証明書のガイドライン （1072 ページ）
- デジタル証明書の設定 （1075 ページ）
- 特定の証明書タイプの設定方法 （1099 ページ）
- 証明書の有効期限アラートの設定（ID 証明書または CA 証明書用） （1101 ページ）
- デジタル証明書のモニタリング （1101 ページ）
- 証明書管理の履歴 （1104 ページ）

デジタル証明書の概要

デジタル証明書は、認証に使用されるデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、または IP アドレスなど、ユーザまたはデバイスを識別する情報が含まれます。CA は、証明書要求の管理とデジタル証明書の発行を行います。CA は、証明書に「署名」してその認証を確認することで、デバイスまたはユーザーのアイデンティティを保証する、信頼できる機関です。

デジタル証明書には、ユーザーまたはデバイスの公開キーのコピーも含まれています。CA は、信頼できるサードパーティ（VeriSign など）の場合もあれば、組織内に設置したプライベート CA（インハウス CA）の場合もあります。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。

デジタル証明書を使用して認証を行う場合は、ASA に 1 つ以上の ID 証明書と、その発行元の CA 証明書が必要です。この設定では、複数のアイデンティティ、ルート、および証明書の階層が許可されます。ASA では CRL（認証局の失効リストとも呼ばれます）に照らしてサードパーティの証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

次に、使用可能な各種デジタル証明書について説明します。

- CA 証明書は、他の証明書に署名するために使用されます。これは自己署名され、ルート証明書と呼ばれます。別の CA 証明書により発行される証明書は、下位証明書と呼ばれます。

- ID証明書は、特定のシステムまたはホストの証明書です。この証明書もCAにより発行されます。
- コード署名者証明書は、コードに署名するためのデジタル署名を作成する際に使用される特殊な証明書であり、署名されたコードそのものが証明書の作成元を示しています。

ルートCA証明書と2つの中間CA証明書を持つ階層では、ID証明書が1つの中間CAによって署名されているが、CRLが別の中間CAによって署名されている場合、9.13以降を実行しているヘッドエンドでリモートアクセスのCRL検証が失敗します。障害は、ヘッドエンドが両方の中間を信頼しており、両方が同じルートによって署名されている場合でも発生します。

したがって、各署名者は独自のCRLを維持する必要があります。各署名者は、署名する各証明書のURLリスト内でCRLの場所を指定します。または、正しいCRLの場所を指している各署名者のトラストポイントで、URLオーバーライドを設定することもできます。

ローカルCAは、ASAの独立認証局機能を統合したもので、証明書の配布と、発行された証明書に対するセキュアな失効チェックを行います。Webサイトのログインページからユーザー登録を行う場合には、ローカルCAにより実現されるセキュアで設定可能な内部認証局機能によって、証明書の認証を行うことができます。

（注） CA証明書およびID証明書は、サイトツーサイトVPN接続およびリモートアクセスVPN接続の両方に適用されます。このマニュアルに記載の手順は、ASDM GUIでリモートアクセスVPNを使用する場合の手順です。

ヒント 証明書コンフィギュレーションおよびロードバランシングの例は、次のURLを参照してください。https://supportforums.cisco.com/docs/DOC-5964

公開キー暗号化

デジタル署名は、公開キー暗号化によってイネーブルになり、デバイスおよびユーザーを認証する手段です。RSA暗号化システムなどの公開キー暗号化では、各ユーザは、公開キーと秘密キーの両方を含むキーペアを使用します。これらのキーはお互い補足しあい、一方のキーで暗号化されたものは、もう一方のキーで復号できます。

簡単に言えば、データが秘密キーで暗号化されると、署名が形成されます。署名はデータに付加されて受信者に送信されます。受信者は送信者の公開キーをデータに適用します。データとともに送信された署名が、公開キーをデータに適用した結果と一致した場合、メッセージの有効性が確立されます。

このプロセスは、受信者が送信者の公開キーのコピーを持っていること、およびその公開キーが送信者になりすました別人のものではなく、送信者本人のものであることを受信者が強く確信していることに依存しています。

通常、送信者の公開キーは外部で取得するか、インストール時の操作によって取得します。たとえば、ほとんどの Web ブラウザでは、いくつかの CA のルート証明書がデフォルトで設定されています。VPN の場合、IKE プロトコルは IPsec のコンポーネントであり、デジタル署名を使用してピア デバイスを認証した後で、セキュリティ アソシエーションをセットアップできます。

証明書のスケーラビリティ

デジタル証明書がない場合、通信するピアごとに各 IPsec ピアを手動で設定する必要があります。そのため、ネットワークにピアを新たに追加するたびに、安全に通信するために各ピアで設定変更を行わなければなりません。

デジタル証明書を使用している場合、各ピアは CA に登録されます。2 つのピアは、通信を試みるときに、証明書とデジタル署名されたデータを交換して、相互の認証を行います。新しいピアがネットワークに追加された場合は、そのピアを CA に登録するだけで済みます。他のピアを修正する必要はありません。新しいピアが IPSec 接続を試みると、証明書が自動的に交換され、そのピアの認証ができます。

CA を使用した場合、ピアはリモート ピアに証明書を送り、公開キー暗号化を実行することによって、そのリモート ピアに対して自分自身を認証します。各ピアから、CA によって発行された固有の証明書が送信されます。このプロセスが機能を果たすのは、関連付けられているピアの公開キーが各証明書にカプセル化され、各証明書が CA によって認証され、参加しているすべてのピアによって CA が認証権限者として認識されるためです。このプロセスは、RSA 署名付きの IKE と呼ばれます。

ピアは、証明書が期限満了になるまで、複数の IPSec セッションに対して、および複数の IPSec ピア宛てに証明書を送り続けることができます。証明書が期限満了になったときは、ピアの管理者は新しい証明書を CA から入手する必要があります。

CA は、IPSec に参加しなくなったピアの証明書を無効にすることもできます。無効にされた証明書は、他のピアからは有効な証明書とは認識されなくなります。無効にされた証明書は CRL に記載され、各ピアは別のピアの証明書を受け取る前に、CRL をチェックします。

CA の中には、実装の一部として RA を持つものもあります。RA は CA のプロキシの役割を果たすサーバーであるため、CA が使用できないときも CA 機能は継続しています。

キーペア

キー ペアは、RSA または楕円曲線署名アルゴリズム（ECDSA）キーであり、次の特性があります。

- RSA キーは SSH や SSL に使用できます。
- SCEP 登録は、RSA キーの証明書をサポートしています。
- RSA キー サイズの最大値は 4096 で、デフォルトは 2048 です。
- ECDSA キー長の最大値は 521 で、デフォルトは 384 です。

- 署名にも暗号化にも使用できる汎用 RSA キー ペアを生成することも、署名用と暗号化用に別々の RSA キー ペアを生成することもできます。SSL では署名用ではなく暗号化用のキーが使用されるので、署名用と暗号化用にキーを分けると、キーが公開される頻度を少なくすることができます。ただし、IKE では暗号化用ではなく署名用のキーが使用されます。キーを用途別に分けることで、キーの公開頻度が最小化されます。

トラストポイント

トラストポイントを使用すると、CA と証明書の管理およびトラックを行えます。トラストポイントとは、CA または ID ペアを表現したものです。トラストポイントには、CA の ID、CA 固有のコンフィギュレーション パラメータ、登録されている ID 証明書とのアソシエーションが含まれています。

トラストポイントの定義が完了したら、CA の指定を必要とするコマンドで、名前によってトラストポイントを参照できます。トラストポイントは複数設定できます。

（注） ASA に同じ CA を共有するトラストポイントが複数ある場合、CA を共有するトラストポイントのうち、ユーザー証明書の検証に使用できるのは 1 つだけです。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザー証明書を検証するかを制御するには、**support-user-cert-validation** コマンドを使用します。

自動登録の場合は、登録 URL がトラストポイントに設定されている必要があり、また、トラストポイントが示す CA がネットワーク上で使用可能であり、SCEP をサポートしている必要があります。

キーペアと、トラストポイントに関連付けられている発行済み証明書は、PKCS12 形式でエクスポートとインポートができます。この形式は、異なる ASA 上のトラストポイント コンフィギュレーションを手動でコピーする場合に便利です。

認証登録

ASA は、トラストポイントごとに 1 つの CA 証明書が必要で、セキュリティ アプライアンス自体には、トラストポイントで使用するキーのコンフィギュレーションに応じて 1 つまたは 2 つの証明書が必要です。トラストポイントが署名と暗号化に別々の RSA キーを使用する場合、ASA には署名用と暗号化用の 2 つの証明書が必要になります。署名用と暗号化用のキーが同じである場合、必要な証明書は 1 つだけです。

ASA は、SCEP を使用した自動登録と、base-64-encoded 証明書を直接端末に貼り付けられる手動登録をサポートしています。サイトツーサイト VPN の場合は、各 ASA を登録する必要があります。リモート アクセス VPN の場合は、各 ASA と各リモート アクセス VPN クライアントを登録する必要があります。

ASA トラストポイントに自動証明書管理環境（ACME）プロトコルを設定して、TLS デバイス証明書を管理できます。ACME 対応トラストポイントは、手動の証明書登録もサポートしてい

ます。ACME サーバーは、ASA ポート 80 を使用してドメイン所有権を検証します。ACME は、非クラスタ化シングルコンテキスト ASA 展開でのみサポートされます。

SCEP 要求のプロキシ

ASA は、セキュアクライアント とサードパーティ CA 間の SCEP 要求のプロキシとして動作することができます。プロキシとして動作する場合に必要なのは CA が ASA からアクセス可能であることのみです。ASA のこのサービスが機能するには、ASA が登録要求を送信する前に、ユーザーが AAA でサポートされているいずれかの方法を使用して認証されている必要があります。また、ホスト スキャンおよびダイナミック アクセス ポリシーを使用して、登録資格のルールを適用することもできます。

ASA は、セキュアクライアント SSL または IKEv2 VPN セッションでのみこの機能をサポートしています。これは、Cisco IOS CS、Windows Server 2003 CA、および Windows Server 2008 CA を含む、すべての SCEP 準拠 CA をサポートしています。

クライアントレス（ブラウザベース）アクセスは SCEP プロキシをサポートしていませんが、WebLaunch（クライアントレス起動 セキュアクライアント）はサポートしています。

ASA は、証明書のポーリングはサポートしていません。

ASA はこの機能に対するロード バランシングをサポートしています。

失効チェック

証明書は発行されると、一定期間有効です。CA は、安全上の問題や名前またはアソシエーションの変更などの理由で、期限が切れる前に証明書を無効にすることがあります。CA は、無効になった証明書の署名付きリストを定期的に発行します。失効確認を有効にすることにより、CA が認証にその証明書を使用するたびに、その証明書が無効にされていないかどうか、ASA によってチェックされます。

失効確認を有効にすると、PKI 証明書検証プロセス時に ASA によって証明書の失効ステータスがチェックされます。これには、CRL チェック、OCSP、またはその両方が使用されます。OCSP は、最初の方式がエラーを返した場合に限り使用されます（たとえば、サーバーが使用不可であることを示すエラー）。

CRL チェックを使用すると、ASA によって、無効になった（および失効解除された）証明書とその証明書シリアル番号がすべてリストされている CRL が取得、解析、およびキャッシュされます。ASA は CRL（認証局の失効リストとも呼ばれます）に基づいて証明書を検証します。検証は、ID 証明書から下位証明書チェーンの認証局までさかのぼって行われます。

OCSP は、検証局に特定の証明書のステータスを問い合わせ、チェックを検証局が扱う範囲に限定するため、よりスケーラブルな方法を提供します。

サポート対象の CA サーバー

ASA は次の CA サーバーをサポートしています。

Cisco IOS CS、ASA ローカル CA、およびサードパーティの X.509 準拠 CA ベンダー（次のベンダーが含まれますが、これらに限定はされません）。

- Baltimore Technologies
- Entrust
- Digicert
- Geotrust
- GoDaddy
- iPlanet/Netscape
- Microsoft Certificate Services
- RSA Keon
- Thawte
- VeriSign

CRL

CRL は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための1つの方法です。CRL コンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

証明書を認証するときに必ず **revocation-check crl** コマンドを使用して CRL チェックを行うように、ASA を設定できます。また、**revocation-check crl none** コマンドを使用して、CRL チェックをオプションにすることもできます。オプションにすると、更新された CRL データが CA から提供されない場合でも、証明書認証は成功します。

（注） 9.13(1) で削除された **revocation-check crl none** が復元されました。

ASA は HTTP、SCEP、または LDAP を使用して、CA から CRL を取得できます。トラストポイントごとに取得された CRL は、トラストポイントごとに設定可能な時間だけキャッシュされます。

（注） CRL サーバは HTTP フラグ「Connection: Keep-alive」で応答して永続的な接続を示しますが、ASA は永続的な接続のサポートを要求しません。リストの送信時に「Connection: Close」と応答するように、CRL サーバの設定を変更します。

CRL のキャッシュに設定された時間を超過して ASA にキャッシュされている CRL がある場合、ASA はその CRL を、古すぎて信頼できない、つまり「失効した」と見なします。ASA は、次回の証明書認証で失効した CRL のチェックが必要な場合に、より新しいバージョンの CRL を取得しようとします。

CRL の 16 MB のサイズ制限を超えると、ユーザー接続/証明書で失効チェックエラーが表示されることがあります。

ASA によって CRL がキャッシュされる時間は、次の 2 つの要素によって決まります。

- **cache-time** コマンドで指定される分数。デフォルト値は 60 分です。
- 取得した CRL 中の NextUpdate フィールド。このフィールドが CRL にない場合もあります。ASA が NextUpdate フィールドを必要とするかどうか、およびこのフィールドを使用するかどうかは、**enforcenextupdate** コマンドで制御します。

ASA では、これらの 2 つの要素が次のように使用されます。

- NextUpdate フィールドが不要の場合、**cache-time** コマンドで指定された時間が経過すると、ASA は CRL に失効のマークを付けます。
- NextUpdate フィールドが必要な場合、ASA は、**cache-time** コマンドと NextUpdate フィールドで指定されている 2 つの時間のうち短い方の時間で、CRL に失効のマークを付けます。たとえば、**cache-time** コマンドによってキャッシュ時間が 100 分に設定され、NextUpdate フィールドによって次のアップデートが 70 分後に指定されている場合、ASA は 70 分後に CRL に失効のマークを付けます。

ASA がメモリ不足で、特定のトラストポイント用にキャッシュされた CRL をすべて保存することができない場合、使用頻度が最も低い CRL が削除され、新しく取得した CRL 用の空き領域が確保されます。大規模な CRL では、解析に大量の計算オーバーヘッドが必要です。したがって、パフォーマンスを向上させるには、少数の大規模な CRL ではなく、小さいサイズの CRL を多数使用するか、または OCSP を使用することを推奨します。

キャッシュサイズは次のとおりです。

- シングルコンテキストモード：128 MB
- マルチコンテキストモード：コンテキストあたり 16 MB

OCSP

OCSP は、有効期間内の証明書が発行元の CA によって無効にされているかどうかを ASA が判断するための 1 つの方法です。OCSP のコンフィギュレーションは、トラストポイントのコンフィギュレーションの一部です。

OCSP によって、証明書のステータスをチェックする範囲が検証局（OCSP サーバー、応答側とも呼ばれます）に限定され、ASA によって検証局に特定の証明書のステータスに関する問い合わせが行われます。これは、CRL チェックよりもスケーラブルで、最新の失効ステータスを確認できる方法です。この方法は、PKI の導入規模が大きい場合に便利で、安全なネットワークを拡大できます。

（注） ASA では、OCSP 応答に 5 秒間のスキューを許可します。

証明書を認証するときに必ず **revocation-check ocsp** コマンドを使用して OCSP チェックを行うように、ASA を設定できます。また、**revocation-check ocsp none** コマンドを使用して、OCSP

チェックをオプションにすることもできます。オプションにすると、更新されたOCSPデータが検証局から提供されない場合でも、証明書認証は成功します。

（注） 9.13(1) で削除された **revocation-check ocsp none** が復元されました。

OCSP を利用すると、OCSP サーバーの URL を 3 つの方法で定義できます。ASA は、これらのサーバーを次の順に使用します。

1. **match certificate** コマンドの使用による証明書の照合の上書きルールで定義されているOCSP サーバーの URL
2. **ocsp url** コマンドを使用して設定されている OCSP サーバーの URL
3. クライアント証明書の AIA フィールド

（注） トラストポイントでOCSPの応答側の自己署名した証明書を検証するように設定するには、信頼できる CA 証明書として、この自己署名した応答側の証明書をそのトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSP の応答側の自己署名された証明書を含むトラストポイントを使用するようにします。クライアント証明書の検証パスの外部にある応答側の証明書を検証する場合も、同じ手順で設定します。

通常、OCSP サーバー（応答側）の証明書によって、OCSP 応答が署名されます。ASA が応答を受け取ると、応答側の証明書を検証しようとします。通常、CA は、侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。ただし、この拡張がない場合、ASAはトラストポイントで指定されている方法で失効ステータスをチェックします。応答側の証明書を検証できない場合、失効ステータスをチェックできなくなります。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。

証明書とユーザー ログイン クレデンシャル

この項では、認証と認可に証明書およびユーザー ログイン クレデンシャル（ユーザー名とパスワード）を使用する、さまざまな方法について説明します。これらの方式は、IPsec、セキュアクライアント、およびクライアントレス SSL VPN に適用されます。

すべての場合において、LDAP認可では、パスワードをクレデンシャルとして使用しません。RADIUS認可では、すべてのユーザーの共通パスワードまたはユーザー名のいずれかを、パスワードとして使用します。

ユーザー ログイン クレデンシャル

認証および認可のデフォルトの方法では、ユーザー ログイン クレデンシャルを使用します。

- 認証
  - トンネル グループ（ASDM接続プロファイルとも呼ばれます）の認証サーバー グループ設定によりイネーブルにされます。
  - ユーザー名とパスワードをクレデンシャルとして使用します。
- 認証
  - トンネル グループ（ASDM接続プロファイルとも呼ばれます）の認可サーバー グループ設定によりイネーブルにされます。
  - ユーザー名をクレデンシャルとして使用します。

証明書

ユーザーデジタル証明書が設定されている場合、ASAによって最初に証明書が検証されます。ただし、証明書の DN は認証用のユーザー名として使用されません。

認証と認可の両方がイネーブルになっている場合、ASAによって、ユーザーの認証と認可の両方にユーザー ログイン クレデンシャルが使用されます。

- 認証
  - 認証サーバー グループ設定によってイネーブルにされます。
  - ユーザー名とパスワードをクレデンシャルとして使用します。
- 認証
  - 認可サーバー グループ設定によってイネーブルにされます。
  - ユーザー名をクレデンシャルとして使用します。

認証がディセーブルで認可がイネーブルになっている場合、ASA によって認可にプライマリ DN のフィールドが使用されます。

- 認証
  - 認証サーバー グループ設定によってディセーブル（[None] に設定）になります。
  - クレデンシャルは使用されません。
- 認証
  - 認可サーバー グループ設定によってイネーブルにされます。
  - 証明書のプライマリ DN フィールドのユーザー名の値をクレデンシャルとして使用します。

（注） 証明書にプライマリ DN のフィールドが存在しない場合、ASA では、セカンダリ DN のフィールド値が認可要求のユーザ名として使用されます。

次のサブジェクト DN フィールドと値が含まれるユーザー証明書を例に挙げます。

```
Cn=anyuser,OU=sales;O=XYZCorporation;L=boston;S=mass;C=us;ea=anyuser@example.com
```

プライマリ DN = EA（電子メール アドレス）およびセカンダリ DN = CN（一般名）の場合、許可要求で使われるユーザー名は anyuser@example.com になります。

デジタル証明書のガイドライン

この項では、デジタル証明書を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

- サードパーティ CA ではシングル コンテキスト モードでのみサポートされています。

フェールオーバーのガイドライン

- ステートフル フェールオーバーではセッションの複製はサポートされません。
- ローカル CA のフェールオーバーはサポートされません。
- ステートフル フェールオーバーを設定すると、証明書は自動的にスタンバイユニットにコピーされます。証明書がない場合は、アクティブユニットで **write standby** コマンドを使用します。

IPv6 のガイドライン

IPv6 OCSP および CRL URL をサポートします。IPv6 アドレスは角カッコで囲む必要があります（例：*http://[0:0:0:0:0.18:0a01:7c16]*）。

ローカル CA 証明書

- 証明書をサポートするように ASA が正しく設定されていることを確認します。ASA の設定が正しくないと、登録に失敗したり、不正確な情報を含む証明書が要求されたりする可能性があります。
- ASA のホスト名とドメイン名が正しく設定されていることを確認します。現在設定されているホスト名とドメイン名を表示するには、**show running-config** コマンドを入力します。
- CA を設定する前に、ASA のクロックが正しく設定されていることを確認します。証明書には、有効になる日時と満了になる日時が指定されています。ASA が CA に登録して証明

書を取得するとき、ASAは現在の時刻が証明書の有効期間の範囲内であるかどうかをチェックします。現在の時刻が有効期間の範囲外の場合、登録は失敗します。

- ローカルCA証明書の有効期限の30日前に、ロールオーバー代替証明書が生成され、syslogメッセージ情報で管理者にローカルCAのロールオーバーの時期であることが知らされます。新しいローカルCA証明書は、現在の証明書が有効期限に達する前に、必要なすべてのデバイスにインポートする必要があります。管理者が、新しいローカルCA証明書としてロールオーバー証明書をインストールして応答しない場合、検証が失敗する可能性があります。
- ローカルCA証明書は、同じキーペアを使用して期限満了後に自動的にロールオーバーします。ロールオーバー証明書は、base 64形式でエクスポートに使用できます。

  次に、base 64で符号化されたローカルCA証明書の例を示します。

```
MIIXlwIBAzCCF1EGCSqGSIb3DQEHAaCCF0IEghc+MIIXOjCCFzYGCSqGSIb3DQEHBqCCFycwghcjAgEAMIIXHA
YJKoZIhvcNAQcBMBsGCiqGSIb3DQEMAQMwDQQIjph4SxJoyTgCAQGAghbw3v4bFy+GGG2dJnB4OLphsUM+IG3S
DOiDwZG9n1SvtMieoxd7Hxknxbum06JDrujWKtHBIqkrm+td34qlNE1iGeP2YC94/NQ2z+4kS+uZzwcRhl1KEZ
TS1E4L0fSaC3uMTxJq2NUHYWmoc8pi4CIeLj3h7VVMy6qbx2AC8I+q57+QG5vG5l5Hi5imwtYfaWwPEdPQxaWZ
PrzoG1J8BFqdPa1jBGhAzzuSmElm3j/2dQ3Atro1G9nIsRHgV39fcBgwz4fEabHG7/Vanb+fj81d5nlOiJjDYY
bP86tvbZ2yOVZR6aKFVI0b2AfCr6PbwfC9U8Z/aF3BCyM2sN2xPJrXva94CaYrqyotZdAkSYA5KWScyEcgdqmu
BeGDKOncTknfgy0XM+fG5rb3qAXy1GkjyFI5Bm9Do6RUROoG1DSrQrKeq/hj….

END OF CERTIFICATE
```

SCEP プロキシ サポート

- ASA と Cisco ISE ポリシー ノードが、同じ NTP サーバーを使用して同期されていることを確認します。
- セキュアクライアント 3.0 以降がエンドポイントで実行されている必要があります。
- グループ ポリシーの接続プロファイルで設定される認証方式は、AAA 認証と証明書認証の両方を使用するように設定する必要があります。
- SSL ポートが、IKEv2 VPN 接続用に開いている必要があります。
- CA は、自動許可モードになっている必要があります。

その他のガイドライン

- 使用できる証明書のタイプは、証明書を使用するアプリケーションでサポートされている証明書タイプによって制約されます。RSA証明書は通常、証明書を使用するすべてのアプリケーションでサポートされます。ただし、EDDSA証明書は、ワークステーションのオペレーティングシステム、ブラウザ、ASDM、または セキュアクライアント ではサポートされない場合があります。たとえば、リモートアクセスVPNのIDおよび認証にはRSA証明書を使用する必要があります。ASAが証明書を使用するアプリケーションであるサイト間 VPN の場合は、EDDSA がサポートされます。
- ASA が CA サーバーまたはクライアントとして設定されている場合、推奨される終了日（2038 年 1 月 19 日 03:14:08 UTC）を超えないよう、証明書の有効期を制限してくださ

い。このガイドラインは、サードパーティベンダーからインポートした証明書にも適用されます。

- ASA は、次の認定条件のいずれかが満たされている場合にのみ LDAP/SSL 接続を確立します。
  - LDAP サーバー証明書が信頼されていて（トラストポイントまたは ASA トラストプールに存在する）、有効であること。
  - チェーンを発行しているサーバーからの CA 証明書が信頼されていて（トラストポイントまたは ASA トラストプールに存在する）、チェーン内のすべての下位 CA 証明書が完全かつ有効であること。
- 証明書の登録が完了すると、ASA により、ユーザのキー ペアと証明書チェーンを含む PKCS12 ファイルが保存されます。これには、登録ごとに約 2 KB のフラッシュ メモリまたはディスク領域が必要です。実際のディスク領域の量は、設定されている RSA キー サイズと証明書フィールドによって異なります。使用できるフラッシュ メモリの量が限られている ASA に、保留中の証明書登録を多数追加する場合には、このガイドラインに注意してください。これらの PKCS12 ファイルは、設定されている登録の取得タイムアウトの間、フラッシュ メモリに保存されます。キー サイズは 2048 以上を使用することをお勧めします。
- 管理インターフェイスへの ASDM トラフィックと HTTPS トラフィックを保護するために、アイデンティティ証明書を使用するよう ASA を設定する必要があります。SCEP により自動的に生成される ID 証明書はリブートのたびに再生成されるため、必ず独自の ID 証明書を手動でインストールしてください。SSL のみに適用されるこのプロシージャの例については、次の URL を参照してください。
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00809fcf91.shtml。
- ASA と セキュアクライアント で検証できるのは、[X520Serialnumber] フィールド（[サブジェクト名（Subject Name）] のシリアル番号）が PrintableString 形式である証明書のみです。シリアル番号の形式に UTF8 などのエンコーディングが使用されている場合、証明書認証は失敗します。
- ASA でのインポート時は、有効な文字と値だけを証明書パラメータに使用してください。ASA では、これらの証明書が復号化されて内部データ構造に組み込まれます。空白のフィールドがある証明書は、復号化標準に準拠していないと解釈されるため、インストールの検証は失敗します。ただし、バージョン 9.16 以降、オプションフィールドの空白値は、復号化およびインストールの検証基準に影響しません。
- ワイルドカード（*）記号を使用するには、文字列値でこの文字を使用できるエンコードを CA サーバーで使用していることを確認してください。RFC 5280 では UTF8String または PrintableString を使用することを推奨していますが、PrintableString ではこのワイルドカード文字を有効であると認識しないため UTF8String を使用する必要があります。ASA は、インポート中に無効な文字または値が見つかると、インポートした証明書を拒否します。次に例を示します。

```
ERROR: Failed to parse or verify imported certificate ciscoasa(config)# Read 162*H÷ytes
 as CA certificate:0U0= \Ivr"phÕV°3é¼þ0 CRYPTO_PKI(make trustedCerts list)
```

```
CERT-C: E ../cert-c/source/certlist.c(302): Error #711h
CRYPTO_PKI: Failed to verify the ID certificate using the CA certificate in trustpoint
 mm.
CERT-C: E ../cert-c/source/p7contnt.c(169): Error #703h
crypto_certc_pkcs7_extract_certs_and_crls failed (1795):
crypto_certc_pkcs7_extract_certs_and_crls failed
CRYPTO_PKI: status = 1795: failed to verify or insert the cert into storage
```

- ACME を正常に登録できるようにデバイスで DNS サーバを設定します。DNS サーバの設定手順については、DNS サーバーの設定 （1020 ページ）を参照してください。

デジタル証明書の設定

ここでは、デジタル証明書の設定方法について説明します。

キーペアの設定

キー ペアを作成または削除するには、次の手順を実行します。

手順

ステップ 1 1 つのデフォルト汎用 RSA キー ペアを生成します。

crypto key generate rsa modulus 2048

例：

```
ciscoasa(config)# crypto key generate rsa modulus 2048
```

デフォルト キー モジュラスは 2048 ですが、必要なサイズを確実に取得するために、明示的にモジュラスを指定する必要があります。キーの名前は Default-RSA-Key になります。

RSA キーの場合、モジュラスは 2048または 4096 ビットのいずれかです。

楕円曲線デジタル署名アルゴリズム（ECDSA）キーも必要な場合は、Default-ECDSA-Key を生成できます。デフォルトの長さは 384 ですが、256 または 521 も使用できます。

crypto key generate ecdsa elliptic-curve 384

エドワーズ曲線署名アルゴリズム（EdDSA）キーも必要な場合は、Default-EdDSA-Key を生成できます。デフォルトの長さは 256 ビットです。

（注）
タイプ EdDSA（Ed25519）のキーペアを使用した ASA での EST 登録はサポートされていません。EST 登録では、RSA または ECDSA キーのみを使用できます。

crypto key generate eddsa edward-curve Ed25519

ステップ 2 （オプション）一意の名前で追加のキーを作成します。

crypto key generate rsa label *key-pair-label* **modulus** *size*

crypto key generate ecdsa label *key-pair-label* **elliptic-curve** *size*

例：

```
ciscoasa(config)# crypto key generate rsa label exchange modulus 2048
```

このラベルは、キー ペアを使用するトラストポイントによって参照されます。

ステップ 3 生成したキー ペアを検証します。

show crypto key mypubkey {**rsa** | **ecdsa**}

例：

```
ciscoasa/contexta(config)# show crypto mypubkey key rsa
```

ステップ 4 生成したキー ペアを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 5 必要に応じて、新しいキー ペアを生成できるように既存のキー ペアを削除します。

crypto key zeroize {**rsa** | **ecdsa**}

例：

```
ciscoasa(config)# crypto key zeroize rsa
```

ステップ 6 （オプション）ローカル CA サーバー証明書およびキー ペアをアーカイブします。

copy

例：

```
ciscoasa# copy LOCAL-CA-SERVER_0001.pl2 tftp://10.1.1.22/user6/
```

このコマンドは、FTP または TFTP を使用して、ローカル CA サーバー証明書とキー ペア、および ASA からのすべてのファイルをコピーします。

（注）
すべてのローカル CA ファイルをできるだけ頻繁にバックアップしてください。

ステップ 7 自動登録をサポートする登録方式の場合、キーペアは自動的に生成され、登録時にフラッシュに保存されます。このサポートを有効にするには、トラストポイントで次の主要なパラメータを指定します。

次の例は、ECDSA キーペアの設定を示しています。

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

crypto-ca-trustpoint mode commands/options:
  256  256 bits
  384  384 bits
  521  521 bits
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve 521
ciscoasa(config-ca-trustpoint)#
```

次の例は、RSA キーペアの設定を示しています。

```
ciscoasa(config-ca-trustpoint)# keypair ?

crypto-ca-trustpoint mode commands/options:
  WORD < 129 char  Name of key pair
  ecdsa            Generate ECDSA keys
  eddsa            Generate EDDSA keys
  rsa              Generate RSA keys
ciscoasa(config-ca-trustpoint)# keypair ecdsa elliptic-curve ?

ciscoasa(config-ca-trustpoint)# keypair rsa modulus ?

crypto-ca-trustpoint mode commands/options:
  2048  2048 bits
  3072  3072 bits
  4096  4096 bits
ciscoasa(config-ca-trustpoint)# keypair rsa modulus 2048
ciscoasa(config-ca-trustpoint)#
```

（注）
EdDSA キーは ACME に対してサポートされていません。ACME 登録プロトコルがトラストポイントに追加され、ACME 用に設定されたトラストポイントに EDDSA キーペアを追加しようとしたときに、EDDSA キーペアの選択がすでに存在している場合、CLI エラーが発生します。

ステップ 8 登録要求で現在使用されているキー ペアと同じキー ペアを使用するか、新しいキー ペアを生成するかを指定するには、次のコマンドを実行します。

crypto ca enroll my_acme_tp regenerate

次に、現在使用中の同じキー ペアを保持するトラストポイントの登録の設定例を示します。

例：

```
ciscoasa(config)# crypto ca enroll my_acme_tp ?
configure mode commands/options:
  noconfirm   Specify this keyword to suppress all interactive prompting.
  regenerate  Regenerate the key pair to be used for enrollment
  <cr>
ciscoasa(config)# crypto ca enroll my_acme_tp noconfirm
```

ステップ 9 次のコマンドを実行して、キー ペアを削除できます。

crypto key zeroize rsa

次に、キー ペアを削除する例を示します。

例：

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
```

トラストポイントの設定

トラストポイントを設定するには、次の手順を実行します。

手順

ステップ 1 ASA が証明書を受け取る必要のある CA に対応するトラストポイントを作成します。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa/contexta(config)# crypto ca trustpoint Main
```

crypto ca トラストポイント コンフィギュレーション モードに入り、ステップ 3 から設定できる CA 固有のトラストポイント パラメータを制御します。

ステップ 2 CA 証明書の送信元インターフェイスを指定します。

enrollment interface *interface-name*

```
ciscoasa(config-ca-trustpoint)#  enrollment interface mgmt
```

ステップ 3 次のいずれかのオプションを選択します。

- ACME と指定のトラストポイントを使用して自動登録を要求し、登録用 URL を設定します。

  1. 次のコマンドを実行して、登録 URL を設定します。

     enrollment protocol acme *url*

     例：

```
ciscoasa(config-ca-trustpoint)# enrollment protocol acme ?
crypto-ca-trustpoint mode commands/options:
  authentication  ACME authentication method
  url             CA server enrollment URL
ciscoasa(config-ca-trustpoint)# enrollment protocol acme url ?
crypto-ca-trustpoint mode commands/options:
  LINE < 477 char  URL
  LetsEncrypt      Use the Let's Encrypt CA
```

```
ciscoasa(config-ca-trustpoint)#  enrollment protocol acme url
https://mytest.com:8443/acme/acme/directory
```

2. 次のコマンドを実行して、証明書を要求する認証方式とインターフェイスを設定します。

   enrollment protocol acme authentication http01 *inf-name*

```
ciscoasa(config-ca-trustpoint)# enrollment protocol acme ?
crypto-ca-trustpoint mode commands/options:
  authentication  ACME authentication method
  url             CA server enrollment URL

ciscoasa(config-ca-trustpoint)# enrollment protocol acme authentication ?
crypto-ca-trustpoint mode commands/options:
  http01  Use the HTTP-01 method, which opens port 80 on the specified interface

ciscoasa(config-ca-trustpoint)#  enrollment protocol acme authentication http01
 mgmt
```

- SCEP と指定のトラストポイントを使用して自動登録を要求し、次のコマンドを実行っすることにより、登録用 URL を設定します。

  enrollment protocol scep *url*

  例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment protocol scep url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

- CMP と指定のトラストポイントを使用して自動登録を要求し、登録用 URL を設定します。

  enrollment protocol cmp *url*

  例

```
ciscoasa/ contexta(config-ca-trustpoint)# enrollment protocol cmp url
http://10.29.67.142:80/certsrv/mscep/mscep.dll
```

  （注）
  CMP 登録を有効にするには、キャリア ライセンスが含まれている必要があります。

- CA から取得した証明書を端末に貼り付けることによって、指定したトラストポイントで手動登録を要求します。

  enrollment terminal

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment terminal
```

- 次のコマンドを実行して自己署名済み証明書を要求します。

  enrollment self

- EST と指定のトラストポイントを使用して自動登録を要求し、登録用URLを設定します。

enrollment protocol est *url*

例

```
asa(config-ca-trustpoint)# enrollment protocol est ?

crypto-ca-trustpoint mode commands/options:
  url CA server enrollment URL
asa(config-ca-trustpoint)# enrollment protocol est url ?
 crypto-ca-trustpoint mode commands/options:
  LINE < 477 char  URL
asa(config-ca-trustpoint)# enrollment protocol est url https://xyz.com/est
```

ステップ 4 上記のステップで CMP または ACME を使用するようにトラストポイントを設定した場合、オプションで自動的に証明書を要求する機能をイネーブルにすることができます。証明書の絶対ライフタイムのうち、自動登録が必要になるまでの期間をパーセンテージで入力し、証明書の再生成中に新しいキーを生成するかどうかを指定します。

```
[no] auto-enroll [<percent>] [regenerate]
```

ステップ 5 使用可能な CRL コンフィギュレーション オプションを指定します。

revocation-check crl none

（注）
9.13(1) で削除された **revocation-check crl none** が復元されました。

例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation-check crl
ciscoasa/contexta(config-ca-trustpoint)# revocation-check none
```

（注）
必須または任意の CRL チェックをイネーブルにするには、証明書を取得してから、CRL 管理用のトラストポイントを設定します。

ステップ 6 基本制約の拡張および CA フラグを有効または無効にします。

[**no**] **ca-check**

基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。

ca-check コマンドはデフォルトで有効になっているため、このコマンドは、基本制約と CA フラグを無効にする場合にのみ入力する必要があります。

例：

```
ciscoasa/contexta(config-ca-trustpoint)# no ca-check
```

ステップ 7 （ACME に適用不可）登録時に、指定された電子メール アドレスを、証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。

email *address*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# email example.com
```

ステップ 8 （オプション）再試行間隔を分単位で指定し、SCEP 登録だけに適用します。

enrollment retry period

例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 5
```

ステップ 9 （オプション）許可される再試行の最大数を指定し、SCEP 登録だけに適用します。

enrollment retry count

例：

```
ciscoasa/contexta(config-ca-trustpoint)# enrollment retry period 2
```

ステップ 10 登録時に、指定された完全修飾ドメイン名を証明書の Subject Alternative Name 拡張子に含めるように CA に要求します。

fqdn *fqdn*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn example.com
```

ステップ 11 登録時に、複数の完全修飾ドメイン名の値を証明書（または手動、SCEP、CMP、EST、ACME、および自己署名証明書の要求）の Subject Alternative Name 拡張に含めるように CA に要求します。FQDN 値の最大長は 128 文字です。

alt-fqdn *fqdn*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# fqdn primary example.com
ciscoasa/contexta(config-ca-trustpoint)# alt-fqdn example1.com
ciscoasa/contexta(config-ca-trustpoint)# alt-fqdn example2.com
ciscoasa/contexta(config-ca-trustpoint)# alt-fqdn example3.com
```

ステップ 12 （ACME に推奨されない）登録時に、ASA の IP アドレスを証明書に含めるように CA に要求します。

ip-address *ip-address*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# ip-address 10.10.100.1
```

ステップ 13 公開キーが認証の対象となるキー ペアを指定します。

keypair *name*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# keypair exchange
```

ステップ 14 CMP または ACME にトラストポイントを設定した場合、任意の手動および自動登録に EDDSA キー、EDCSA キーまたは RSA キーを生成するかどうかを決定します。

```
no keypair name | [rsa modulus 2048|4096] | [edcsa elliptic-curve 256|384|521] | [ eddsa
 edwards-curve Ed25519 ]
```

（注）
タイプ EDDSA（Ed25519）のキーペアを使用した ASA での EST 登録はサポートされていません。EST 登録では、RSA キーと ECDSA キーのみを使用できます。キーペア タイプ EDDSA での ACME 登録はサポートされていません。

（注）
ECDHE_ECDSA 暗号グループを使用する場合は、ECDSA 対応キーを含む証明書を使用してトラストポイントを設定します。RSA キーを含む証明書は、ECDSA 暗号と互換性がありません。

ステップ 15 OCSP の URL の上書きと、OCSP の応答側の証明書の検証に使用するトラストポイントを設定します。

match certificate map-name override ocsp

例：

```
ciscoasa/contexta(config-ca-trustpoint)# match certificate examplemap override ocsp
```

ステップ 16 OCSP に到達するように ASA の送信元インターフェイスを設定します。

interface *nameif*

例：

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
```

ステップ 17 OCSP要求のnonce拡張をディセーブルにします。nonce拡張は、リプレイ攻撃を防ぐために、要求と応答を暗号化してバインドします。

ocsp disable-nonce

例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp disable-nonce
```

ステップ 18 ASA で、トラストポイントに関連するすべての証明書をチェックするときに使用する OCSP サーバーを設定します。クライアント証明書の AIA 拡張で指定されているサーバーは使用しません。

ocsp url

例：

```
ciscoasa/contexta(config-ca-trustpoint)# ocsp url
```

ASA は、IPv4 と IPv6 両方の OCSP URL をサポートします。IPv6 アドレスは角カッコで囲みます（例：*http://[0:0:0:0:0.18:0a01:7c16/]*）。

ステップ 19 登録時に CA に登録されるチャレンジ フレーズを指定します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。

password *string*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# password mypassword
```

ステップ 20 失効チェックの方法（CRL、OCSP、および none）を 1 つまたは複数設定します。

（注）
失効チェックに OCSP URL を割り当てる場合、OCSP が到達可能なインターフェイス（管理インターフェイスを含む）を指定できます。このインターフェイス値によってルーティングの判断が決まります。

revocation check

例：

```
ciscoasa/contexta(config-ca-trustpoint)# revocation check
```

ステップ 21 登録時に、指定されたサブジェクト DN を証明書に含めるように CA に要求します。DN 文字列にカンマが含まれている場合、この値文字列を二重引用符で囲みます（例：O="Company, Inc."）。

subject-name *X.500 name*

例：

```
ciscoasa/contexta(config-ca-trustpoint)# myname X.500 examplename
```

ステップ 22 登録時に、ASA のシリアル番号を証明書に含めるように CA に要求します。

serial-number

例：

```
ciscoasa/contexta(config-ca-trustpoint)# serial number JMX1213L2A7
```

ステップ 23 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa/contexta(config)# write memory
```

トラストポイントの CRL の設定

証明書の認証時に必須またはオプションの CRL チェックを行うには、トラストポイントごとに CRL を設定する必要があります。トラストポイントの CRL を設定するには、次の手順を実行します。

手順

ステップ 1 CRL コンフィギュレーションを変更するトラストポイントに対して、crypto ca trustpoint コンフィギュレーション モードに入ります。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa (config)# crypto ca trustpoint Main
```

（注）
このコマンドを入力する前に、CRLがイネーブルであることを確認してください。また、認証が成功するためには、CRL が使用可能である必要があります。

ステップ 2 現在のトラストポイントで、crl コンフィギュレーション モードを開始します。

crl configure

例：

```
ciscoasa(config-ca-trustpoint)# crl configure
```

ヒント
すべての CRL コンフィギュレーションのパラメータをデフォルト値に設定するには、**default** コマンドを使用します。CRLの設定中は、いつでもこのコマンドを入力して手順をやり直すことができます。

ステップ 3 取得ポリシーを設定するには、次のいずれかを選択します。

（注）
ASA は、IPv4 または IPv6 ベースの CDP およびスタティック URL をサポートします。IPv6 アドレスは角カッコで囲みます（例：*http://[0:0:0:0:0.18:0a01:7c16/]*）。

- CRL は、認証済みの証明書で指定されている CRL 分散ポイント（CDP）URL だけから取得できます。

  policy cdp

  ```
  ciscoasa(config-ca-crl)# policy cdp
  ```

  （注）
  SCEP の取得は、証明書で指定されている分散ポイントではサポートされていません。

- CRL は、設定した証明書マップ一致ルールだけから取得できます。

  policy static

  ```
  ciscoasa(config-ca-crl)# policy static
  ```

- CRL は、認証済みの証明書で指定されている CRL 分散ポイントと、設定した証明書マップ一致ルールの両方から取得できます。

  policy both

  ```
  ciscoasa(config-ca-crl)# policy both
  ```

ステップ 4 CRL ポリシーの設定時に **static** または **both** キーワードを使用する場合、CRL 取得用の証明書マップ一致ルールを設定する必要があります。1つのマップに複数のスタティック CDP を設定できるようになりました。

enrollment terminal

特定のインスタンスを削除するには、コマンドの **no** 形式でシーケンス番号または URL を含めます。指定した値が設定値と一致することを確認してください。マップのすべてのエントリを削除するには、**no** コマンドを使用します。

例：

```
ciscoasa(crypto ca trustpoint)#enrollment terminal
```

```
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  10 url
http://192.0.2.10
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  20 url
http://192.0.2.12
ciscoasa(crypto ca trustpoint)#match certificate Main override cdp  30 url
http://192.0.2.13
```

ステップ 5 CRL 取得方式として HTTP、LDAP、または SCEP を指定します。

protocol http | **ldap** | **scep**

例：

```
ciscoasa(config-ca-crl)# protocol http
```

ステップ 6 ASA が現在のトラストポイントの CRL をキャッシュしている時間を設定します。*refresh-time* 引数は、CRL を失効と判断するまで ASA が待機する時間（分）です。

cache-time *refresh-time*

例：

```
ciscoasa(config-ca-crl)# cache-time 420
```

ステップ 7 次のいずれかを選択します。

- CRL に NextUpdate フィールドが存在する必要があります。これがデフォルト設定です。

  enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# enforcenextupdate
  ```

- CRL に NextUpdate フィールドが存在しないことを許可します。

  no enforcenextupdate

  ```
  ciscoasa(config-ca-crl)# no enforcenextupdate
  ```

ステップ 8 LDAP が取得プロトコルとして指定されている場合に ASA に LDAP サーバーを指定します。LDAP サーバーは、DNS ホスト名または IP アドレスで指定できます。LDAP サーバーがデフォルトの 389 以外のポートで LDAP クエリーを受信する場合は、ポート番号も指定できます。

ldap-defaults *server*

例：

```
ciscoasa (config-ca-crl)# ldap-defaults ldap1
```

（注）
LDAP サーバーを指定するために、IP アドレスの代わりにホスト名を使用する場合は、ASA が DNS を使用するように設定されていることを確認します。

ステップ 9 LDAP サーバーでクレデンシャルを必要としている場合に、CRL の取得を許可します。

ldap-dn *admin-DN password*

例：

```
ciscoasa (config-ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering c00lRunZ
```

ステップ 10 指定したトラストポイントによって示される CA から現在の CRL を取得し、現在のトラストポイントの CRL コンフィギュレーションをテストします。

crypto ca crl request *trustpoint*

例：

```
ciscoasa (config-ca-crl)# crypto ca crl request Main
```

ステップ 11 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa (config)# write memory
```

トラストポイント設定のエクスポートまたはインポート

トラストポイント設定をエクスポート/インポートするには、次の手順を実行します。

手順

ステップ 1 トラストポイント設定を関連するすべてのキーと PKCS12 形式の証明書とともにエクスポートします。

crypto ca export *trustpoint*

例：

```
ciscoasa(config)# crypto ca export Main
```

ASA は PKCS12 データを端末に表示します。この表示されたデータはコピーできます。トラストポイントデータはパスワードで保護されますが、このデータをファイルに保存する場合は、そのファイルがセキュアな場所にあることを確認してください。

ステップ 2 キー ペアと、トラスト ポイント設定に関連付けられている発行済み証明書をインポートします。

crypto ca import *trustpoint* **pkcs12***passphrase*

例：

```
ciscoasa(config)# crypto ca import Main pkcs12 ?
```

Base-64 形式で端末にテキストを貼り付けるよう ASA によって促されます。トラストポイントとともにインポートされるキーペアには、作成するトラストポイントの名前と一致するラベルが割り当てられます。

（注）
同じ CA を共有するトラストポイントが ASA 内に複数ある場合、CA を共有するトラストポイントのうち 1 つだけを使用してユーザー証明書を検証できます。CA を共有するどのトラストポイントを使用して、その CA が発行したユーザー証明書を検証するかを制御するには、**support-user-cert-validation** キーワードを使用します。

例

次の例では、トラストポイント Main の PKCS12 データをパスフレーズ Wh0zits とともにエクスポートしています。

```
ciscoasa(config)# crypto ca export Main pkcs12 Wh0zits

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---
```

次の例では、パスフレーズ Wh0zits とともに PKCS12 データを手動でトラストポイント Main にインポートしています。

```
ciscoasa (config)# crypto ca import Main pkcs12 Wh0zits

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
```

次に、トラストポイント Main の証明書を手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import Main certificate
% The fully qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word “quit” on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

CA 証明書マップ ルールの設定

証明書の [Issuer] フィールドと [Subject] フィールドに基づいて、ルールを設定できます。作成したルールを使用すると、**tunnel-group-map** コマンドによって、IPsec ピアの証明書をトンネル グループにマッピングできます。

CA 証明書マップ規則を設定するには、次の手順を実行します。

手順

ステップ 1 設定するルールの CA 証明書マップ コンフィギュレーション モードを開始し、ルールのシーケンス番号を指定します。

crypto ca certificate map [*map_name*]*sequence-number*

例：

```
ciscoasa(config)# crypto ca certificate map test-map 10
```

マップ名を指定しない場合、ルールはデフォルト マップ（DefaultCertificateMap）に追加されます。ルール番号ごとに、一致させるフィールドを 1 つ以上指定できます。

ステップ 2 発行元の名前またはサブジェクト名を指定します。

{**issuer-name** | **subject-name**} [**attr** *attribute*] *operator string*

例：

```
ciscoasa(config-ca-cert-map)# issuer-name cn=asa.example.com
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr uid eq jcrichton
```

値全体と一致させることも、一致させる属性を指定することもできます。有効な値は次のとおりです。

- c：国
- cn：共通名
- dc：ドメイン コンポーネント
- dnq：DN 修飾子
- emailAddress：電子メールアドレス
- genq：世代修飾子
- gn：名
- i：イニシャル
- ip：IP アドレス

- l：局所性
- n：名前
- o：組織名
- ou：組織単位
- ser：シリアル番号

（注）
subject-name でシリアル番号属性を指定していることを確認します。証明書マップは、subject-name で指定されたシリアル番号属性とのみ一致します。

- sn：姓
- sp：都道府県
- t：役職
- uid：ユーザー ID
- uname：非構造化名

有効な演算子は次のとおりです。

- eq：フィールドまたは属性が所定の値と一致する。
- ne：フィールドまたは属性が所定の値と一致しない。
- co：フィールドまたは属性の一部または全部が所定の値と一致する。
- nc：フィールドまたは属性の全部が所定の値と一致しない。

ステップ 3 サブジェクト代替名を指定します。

alt-subject-name *operator string*

例：

```
ciscoasa(config-ca-cert-map)# alt-subject-name eq happydays
```

有効な演算子は次のとおりです。

- eq：フィールドが所定の値と一致する。
- ne：フィールドが所定の値と一致しない。
- co：フィールドの一部または全部が所定の値と一致する。
- nc：フィールドの全部が所定の値と一致しない。

ステップ 4 拡張キーの使用法を指定します。

extended-key-usage *operator OID_string*

例：

```
ciscoasa(config-ca-cert-map)# extended-key-usage nc clientauth
```

有効な演算子は次のとおりです。

- co：フィールドの一部または全部が所定の値と一致する。
- nc：フィールドの全部が所定の値と一致しない。

有効な OID 文字列は次のとおりです。

- [string]：ユーザー定義の文字列。
- clientauth：クライアント認証（1.3.6.1.5.5.7.3.2）
- codesigning：コード署名（1.3.6.1.5.5.7.3.3）
- emailprotection：セキュア電子メール保護（1.3.6.1.5.5.7.3.4）
- ocspsigning：OCSP 署名（1.3.6.1.5.5.7.3.9）
- serverauth：サーバー認証（1.3.6.1.5.5.7.3.1）
- timestamping：タイムスタンプ（1.3.6.1.5.5.7.3.8）

参照 ID の設定

ASA が TLS クライアントとして動作する場合、ASA は RFC 6125 で定義されているアプリケーション サーバーの ID の検証ルールをサポートします。この RFC では、参照 ID を表現（ASA 上で設定）し、（アプリケーション サーバーから送信）提示された ID に対して参照 ID を照合する手順を示しています。提示された ID が設定済みの参照 ID と一致しなければ、接続は確立されず、エラーがログに記録されます。

接続の確立中、サーバーは自身の ID を提示するために、1 つ以上の識別子を含めたサーバー証明書を ASA に提示します。ASA で設定される参照 ID は、接続の確立中にサーバー証明書で提示される ID と比較されます。これらの ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。4 つの ID タイプは次のとおりです。

- CN_ID：証明書のサブジェクト フィールドに設定される、共通名（CN）タイプの 1 つの属性タイプと値のペアだけが含まれる相対識別名（RDN）。この値は、完全な形のドメイン名と一致します。CN 値は自由形式のテキストにすることはできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
- DNS-ID：dNSName タイプの subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
- SRV-ID：RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス

タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。

- URI-ID：uniformResourceIdentifier タイプの subjectAltName エントリ。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。

参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。参照 ID には、DNS ドメイン名を特定する情報が含まれている必要があります。また、アプリケーション サービスを特定する情報も含めることができます。

始める前に

- 参照 ID は、syslog サーバーおよびスマート ライセンス サーバーへの接続時にのみ使用されます。その他の ASA SSL クライアント モードの接続では、現時点では、参照 ID の設定や使用はサポートされていません。
- 対話式クライアントの固定証明書およびフォールバックを除き、ASA は RFC 6125 で説明されている ID と一致させるためのすべてのルールを実装します。
- 証明書を固定する機能は実装されません。したがって、「`No Match Found, Pinned Certificate`」メッセージが発生することはありません。また、シスコで実装するクライアントは対話式クライアントではないため、一致が見つからない場合にユーザーが証明書を固定することもできません。

手順

ステップ 1 ASA を ca-reference-identity モードにするには、グローバル コンフィギュレーション モードで **[no] crypto ca reference-identity** コマンドを入力します。

[no] crypto ca reference-identity *reference-identity-name*

この *reference-identity-name* が使用されている参照 ID が見つからない場合、新しい参照 ID が作成されます。使用中の参照 ID に対してこのコマンドの **no** 形式を発行すると、警告メッセージが表示されて、参照 ID は削除されません。

ステップ 2 ca-reference-identity モードで、参照 ID を入力します。参照 ID には、任意のタイプの複数の参照 ID を追加できます。

- **[no] cn-id** *value*
- **[no] dns-id** *value*

- **[no] srv-id** *value*
- **[no] uri-id** *value*

参照 ID を削除するには、このコマンドの no 形式を使用します。

例

syslog サーバーの RFC 6125 サーバー証明書の検証に使用する参照 ID を設定します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

次のタスク

設定した参照 ID は、syslog および Smart Call Home サーバー接続を設定する際に使用します。

手動での証明書の取得

証明書を手動で取得するには、次の手順を実行します。

始める前に

トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得しておく必要があります。

手順

ステップ 1 設定したトラストポイントの CA 証明書をインポートします。

crypto ca authenticate *trustpoint*

例：

```
ciscoasa(config)# crypto ca authenticate Main
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself
MIIDRTCCAu+gAwIBAgIQKVcqP/KW74VP0NZzL+JbRTANBgkqhkiG9w0BAQUFADCB
[ certificate data omitted ]
/7QEM8izy0EOTSErKu7Nd76jwf5e4qttkQ==
quit

INFO: Certificate has the following attributes:
Fingerprint:     24b81433 409b3fd5 e5431699 8d490d34
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

トラストポイントの証明書を手動で取得する必要があるかどうかは、そのトラストポイントの設定時に **enrollment terminal** コマンドを使用するかどうかによって決まります。

ステップ 2 このトラストポイントを持つ ASA を登録します。

crypto ca enroll *trustpoint*

例：

```
ciscoasa(config)# crypto ca enroll Main
% Start certificate enrollment ..

% The fully-qualified domain name in the certificate will be: securityappliance.example.com

% Include the device serial number in the subject name? [yes/no]: n

Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:

MIIBoDCCAQkCAQAwIzEhMB8GCSqGSIb3DQEJAhYSRmVyYWxQaXguY2lzY28uY29t
[ certificate request data omitted ]
jF4waw68eOxQxVmdgMWeQ+RbIOYmvt8g6hnBTrd0GdqjjVLt

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: n
```

このコマンドは、署名データの証明書を生成し、設定したキーのタイプによっては暗号化データの証明書も生成します。署名と暗号化に別々の RSA キーを使用する場合、**crypto ca enroll** コマンドは 2 つの証明書要求（キーごとに 1 つ）を表示します。署名と暗号化の両方に汎用の RSA キーを使用する場合、**crypto ca enroll** コマンドでは証明書要求が 1 つ表示されます。

登録を完了するには、該当するトラストポイントで示される CA から **crypto ca enroll** コマンドで生成されたすべての証明書要求に対する証明書を取得します。証明書が base-64 形式であることを確認してください。

ステップ 3 トラストポイントが CMP 用に設定されている場合、共有秘密値（ir）またはリクエストに署名する証明書を含むトラストポイントの名前（cr）のどちらかを指定できますが、両方を指定することはできません。ASA と交換されるメッセージの信頼性と整合性を確認するための CA からのアウトオブバンド値を指定するか、あるいは CMP 登録要求の署名用に以前に発行されたデバイス証明書をトラストポイントの名前に指定します。共有秘密または署名証明書のキーワードは、トラストポイント登録プロトコルが CMP に設定されている場合にのみ使用できます。

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate
<value>
```

ステップ 4 登録要求を作成する前に、新しい鍵ペアを生成すべきかどうかを判断します。

```
crypto ca enroll trustpoint [regenerate] [shared-secret <value> | signing-certificate
<value>
```

ステップ 5 CA から受信する各証明書をインポートして、証明書を base-64 形式で端末に貼り付けていることを確認します。

crypto ca import *trustpoint* **certificate**

例：

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be: securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
```

ステップ 6 ASAに発行された証明書の詳細とトラストポイントのCA証明書を表示して、登録プロセスが成功したことを確認します。

show crypto ca certificate

例：

```
ciscoasa(config)# show crypto ca  certificate Main
```

ステップ 7 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 8 手動登録を設定したトラストポイントごとに、これらの手順を繰り返します。

SCEP を使用した証明書の自動取得

この項では、SCEP を使用して証明書を自動的に取得する方法について説明します。

始める前に

トラストポイントで示されている CA から、base-64 encoded CA 証明書を取得しておく必要があります。

手順

ステップ 1 設定したトラストポイントの CA 証明書を取得します。

crypto ca authenticate *trustpoint*

例：

```
ciscoasa/contexta(config)# crypto ca authenticate Main
```

トラストポイントを設定するときに、**enrollment url** コマンドを使用すると、SCEP を使用して証明書を自動的に取得する必要があるかどうかを判断できます。

ステップ 2 このトラストポイントを持つ ASA を登録します。このコマンドは、署名データの証明書を取得し、設定したキーのタイプによっては暗号化データの証明書も取得します。CA の管理者は、CA が証明書を付与する前に手動で登録要求を認証しなければならない場合があるため、このコマンドを入力する前に CA の管理者に連絡してください。

crypto ca enroll *trustpoint*

例：

```
ciscoasa/contexta(config)# crypto ca enroll Main
```

ASA が証明書要求を送信してから 1 分（デフォルト）以内に CA から証明書を受け取らなかった場合は、証明書要求が再送信されます。ASA によって、証明書を受信するまで 1 分ごとに証明書要求が送信されます。

トラストポイントの完全修飾ドメイン名が ASA の完全修飾ドメイン名と一致しなかった場合（完全修飾ドメイン名が文字の場合も含む）、警告が表示されます。この問題を解決するには、登録プロセスを終了し、必要な修正を行ってから、**crypto ca enroll** コマンドを再入力します。

（注）
crypto ca enroll コマンドを発行した後、証明書を受信する前に ASA がリブートされた場合は、**crypto ca enroll** コマンドを再入力して、CA 管理者に連絡してください。

ステップ 3 ASA に発行された証明書の詳細とトラストポイントの CA 証明書を表示して、登録プロセスが成功したことを確認します。

show crypto ca certificate

例：

```
ciscoasa/contexta(config)# show crypto ca certificate Main
```

ステップ 4 実行コンフィギュレーションを保存します。

write memory

例：

```
ciscoasa/contexta(config)# write memory
```

SCEP 要求のプロキシ サポートの設定

サードパーティの CA を使用してリモート アクセスのエンド ポイントを認証するように ASA を設定するには、次の手順を実行します。

手順

ステップ 1 トンネル グループ ipsec 属性コンフィギュレーション モードを開始します。

tunnel-group *name* **ipsec-attributes**

例：

```
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
```

ステップ 2 クライアント サービスをイネーブルにします。

crypto ikev2 enable outside client-services port *portnumber*

例：

```
ciscoasa(config-tunnel-ipsec)# crypto ikev2 enable outside client-services
```

デフォルトのポート番号は 443 です。

（注）
このコマンドは、IKEv2 をサポートする場合にのみ必要です。

ステップ 3 トンネル グループ general 属性コンフィギュレーション モードを開始します。

tunnel-group *name* **general-attributes**

例：

```
ciscoasa(config)# tunnel-group 209.165.200.225 general-attributes
```

ステップ 4 トンネル グループの SCEP 登録をイネーブルにします。

scep-enrollment enable

例：

```
ciscoasa(config-tunnel-general)# scep-enrollment enable
INFO: 'authentication aaa certificate' must be configured to complete setup of this
option.
```

ステップ 5 グループ ポリシー属性コンフィギュレーション モードを開始します。

group-policy *name* **attributes**

例：

```
ciscoasa(config)# group-policy FirstGroup attributes
```

ステップ 6 グループ ポリシー用の SCEP CA を登録します。このコマンドは、サードパーティのデジタル証明書をサポートするグループ ポリシーごとに 1 回入力します。

scep-forwarding-url value *URL*

例：

```
ciscoasa(config-group-policy)# scep-forwarding-url value http://ca.example.com:80/
```

URL は CA の SCEP URL です。

ステップ 7 証明書が SCEP プロキシの WebLaunch のサポートに使用できない場合は、共通のセカンデリ パスワードを使用します。

secondary-pre-fill-username clientless hide use-common-password *password*

例：

```
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username clientless hide
use-common-password secret
```

SCEP プロキシをサポートするには、**hide** キーワードを使用する必要があります。

たとえば、証明書は、それを要求するエンドポイントでは使用できません。エンドポイントに証明書が存在する場合、セキュアクライアント は ASA への接続を切断し、その後再接続して内部ネットワークリソースへのアクセスを提供する DAP ポリシーに適合するようにします。

ステップ 8 セキュアクライアント VPN セッションの事前入力されているセカンダリユーザー名を非表示にします。

secondary-pre-fill-username ssl-client hide use-common-password *password*

例：

```
ciscoasa(config-tunnel-webvpn)# secondary-pre-fill-username ssl-client hide
use-common-password secret
```

以前のリリースから継承した **ssl-client** キーワードに関係なく、IKEv2 または SSL を使用するセキュアクライアント セッションをサポートするには、このコマンドを使用します。

SCEP プロキシをサポートするには、**hide** キーワードを使用する必要があります。

ステップ 9 証明書が使用できないときにはユーザー名を指定します。

secondary-username-from-certificate {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]

例：

```
ciscoasa(config-tunnel-webvpn)# secondary-username-from-certificate CN
no-certificate-fallback cisco-secure-desktop machine-unique-id
```

特定の証明書タイプの設定方法

信頼できる証明書を確立すると、アイデンティティ証明書の確立などの基本的なタスクや、ローカル CA 証明書やコード署名証明書の確立などのさらに高度な設定を行なえるようになります。

始める前に

デジタル証明書情報に目を通し、信頼できる証明書を確立します。秘密キーが設定されていない CA 証明書は、すべての VPN プロトコルと webvpn で使用され、トラストポイントで着信クライアント証明書を検証するように設定されています。また、トラストポイントとは、HTTPS サーバーにプロキシ接続された接続を検証し、smart-call-home 証明書を検証する、webvpn 機能によって使用される信頼できる証明書の一覧のことです。

手順

ローカル CA を設定すると、VPN クライアントが ASA から証明書を直接登録できるようになります。この高度な設定により、ASA は CA に変換されます。CA を設定するには、CA 証明書 （1099 ページ） を参照してください。

次のタスク

証明書の有効期限にアラートを設定するか、デジタル証明書や証明書の管理履歴をモニターします。

CA 証明書

このページで、CA 証明書を管理します。次のトピックでは、実行できることについて説明します。

CA サーバー管理

trustpool 証明書の自動インポートの設定

スマートライセンスでは、Smart Call Home インフラストラクチャが使用されます。ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行した CA の証明書を含むトラストポイントを自動的に作成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層の変更を調整する必要はありません。CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。この機能はマルチコンテキスト展開ではサポートされません。

trustpoolの証明書バンドルを自動的にインポートするには、ASAがバンドルのダウンロードとインポートに使用するURLを指定する必要があります。次のコマンドを入力すると、デフォルトのCisco URLとデフォルトの時間（22時間）を使用して、毎日一定の間隔でインポートが実行されます。

```
ciscoasa(config-ca-trustpool)# auto-import-url Default
```

また、次のコマンドを使用して、カスタムURLによる自動インポートをイネーブルにできます。

```
ciscoasa(config-ca-trustpool)# auto-import url http://www.thawte.com
```

オフピーク時またはその他の都合のよい時間帯に柔軟にダウンロードを設定できるようにするには、次のコマンドを入力して、カスタム時間によるインポートをイネーブルにします。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23
```

カスタムURLとカスタム時間の両方による自動インポートを設定するには、次のコマンドを使用する必要があります。

```
ciscoasa(config-ca-trustpool)# auto-import time 23:23:23 url http://www.thawte.com
```

trustpool ポリシーのステータスの表示

trustpool ポリシーの現在のステータスを表示するには、次のコマンドを使用します。

```
show crypto ca trustpool policy
```

このコマンドは次のような情報を返します。

```
0 trustpool certificates installed
Trustpool auto renewal statistics:
 State: Not in progress
 Last import result: Not attempted N/A
 Current Jitter: 0

Trustpool auto import statistics:
 Last import result: N/A
 Next schedule import at 22:00:00 Tues Jul 21 2015

Trustpool Policy

 Trustpool revocation checking is disabled.
 CRL cache time: 60 seconds
 CRL next update field: required and enforced
 Auto import of trustpool is enabled
 Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
 Download time: 22:00:00

Policy Overrides:
 None configured
```

CA Trustpool のクリア

trustpool ポリシーをデフォルト状態にリセットするには、次のコマンドを使用します。

```
clear configure crypto ca trustpool
```

トラストポイント証明書の自動インポートはデフォルトでオフになるので、次のコマンドを使用して機能をディセーブルにします。

証明書の有効期限アラートの設定（ID 証明書または CA 証明書用）

ASA は、トラストポイントの CA 証明書および ID 証明書について有効期限を24時間ごとに 1 回チェックします。証明書の有効期限がまもなく終了する場合、syslog がアラートとして発行されます。

リマインダおよび繰り返し間隔を設定するためにCLIが提供されます。デフォルトでは、リマインダは有効期限の 60 日前に開始され、7 日ごとに繰り返されます。次のコマンドを使用して、最初のアラートが送信される有効期限までの日数を設定し、リマインダが送信される間隔を設定します。

```
[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]
```

アラートの設定に関係なく、有効期限の直前の週はリマインダが毎日送信されます。次の **show** コマンドと **clear** コマンドも追加されています。

```
clear conf crypto ca alerts
show run crypto ca alerts
```

更新リマインダに加え、コンフィギュレーションに期限が切れた証明書が見つかった場合、その証明書を更新するか、または削除することで、コンフィギュレーションを修正するために syslog が毎日 1 回生成されます。

たとえば、有効期限アラートが 60 日に開始され、その後 6 日ごとに繰り返すように設定されているとします。ASAが 40 日に再起動されると、アラートはその日に送信され、次のアラートは 36 日目に送信されます。

（注） 有効期限チェックは、トラストプールの証明書では実行されません。ローカルCA トラストポイントは、有効期限チェックの通常のトラストポイントとしても扱われます。

デジタル証明書のモニタリング

デジタル証明書ステータスのモニタリングについては、次のコマンドを参照してください。

- **show crypto ca server**

  このコマンドは、ローカル CA のコンフィギュレーションとステータスを表示します。

- **show crypto ca server cert-db**

  このコマンドは、ローカル CA によって発行されたユーザー証明書を表示します。

- **show crypto ca server certificate**

このコマンドは、コンソールに base 64 形式でローカル CA 証明書を表示し、使用可能な場合は、他のデバイスへのインポート時に新しい証明書の検証に使うためのロールオーバー証明書のサムプリントを含むロールオーバー証明書の情報を表示します。

- **show crypto ca server crl**

  このコマンドは、CRL を表示します。

- **show crypto ca server user-db**

  このコマンドは、ユーザーとユーザーのステータスを表示します。この情報に次の修飾子を使用して、表示されるレコード数を減らすことができます。

  - allowed：現在登録が許可されているユーザーだけを表示します。
  - enrolled：登録され、有効な証明書を持つユーザーだけを表示します。
  - expired：期間満了になった証明書を持つユーザーだけを表示します。
  - on-hold：証明書を持たず現在登録が許可されていないユーザーだけを表示します。

- **show crypto ca server user-db allowed**

  このコマンドは、登録できるユーザーを表示します。

- **show crypto ca server user-db enrolled**

  このコマンドは、有効な証明書を持つ登録済みユーザーを表示します。

- **show crypto ca server user-db expired**

  このコマンドは、期間満了した証明書を持つユーザーを表示します。

- **show crypto ca server user-db on-hold**

  このコマンドは、証明書がなく、登録が許可されていないユーザーを表示します。

- **show crypto key** *name of key*

  このコマンドは、生成したキー ペアを表示します。

- **show running-config**

  このコマンドは、ローカル CA 証明書マップ ルールを表示します。

例

次の例では、汎用 RSA キーを表示します。

```
ciscoasa/contexta(config)# show crypto key mypubkey rsa
Key pair was generated at: 16:39:47 central Feb 10 2010
Key name: <Default-RSA-Key>
 Usage: General Purpose Key
 Modulus Size (bits): 2048
 Storage: config
 Key Data:

  30820122 300d0609 2a864886 f70d0101 01050003 82010f00 3082010a 02820101
```

```
  00ea2c38 df9c606e ddb7b08a e8b0a1a8 65592d85 0711cac5 fceddee1 fa494297
  525fffc0 90da8a4c e696e44e 0646c661 48b3602a 960d7a3a 52dae14a 5f983603
  e1f33e40 a6ce04f5 9a812894 b0fe0403 f8d7e05e aea79603 2dcd56cc 01261b3e
  93bff98f df422fb1 2066bfa4 2ff5d2a4 36b3b1db edaebf16 973b2bd7 248e4dd2
  071a978c 6e81f073 0c4cd57b db6d9f40 69dc2149 e755fb0f 590f2da8 b620efe6
  da6e8fa5 411a841f e72bb8ea cf4bdb79 f4e57ff3 a940ce3b 4a2c7052 56c1d17b
  af8fe2e2 e58718c6 ed1da0f0 1c6f36eb 79eb1aeb f098b5c4 79e07658 a52d8c7a
  51ceabfb f8ade096 7217cf2d 3728077e 89441d89 9bf5f875 c8d2db39 c858bb7a
  7d020301 0001
```

次に、ローカル CA CRL を表示する例を示します。

```
ciscoasa(config)# show crypto ca server crl
Certificate Revocation List:
    Issuer: cn=xx5520-1-3-2007-1
    This Update: 13:32:53 UTC Jan 4 2010
    Next Update: 13:32:53 UTC Feb 3 2010
    Number of CRL entries: 2
    CRL size: 270 bytes
Revoked Certificates:
    Serial Number: 0x6f
    Revocation Date: 12:30:01 UTC Jan 4 2010
    Serial Number: 0x47
    Revocation Date: 13:32:48 UTC Jan 4 2010
```

次に、1 人の保留中のユーザーを表示する例を示します。

```
ciscoasa(config)# show crypto ca server user-db on-hold
username: wilma101
email:    <None>
dn:       <None>
allowed:  <not allowed>
notified: 0
ciscoasa(config)#
```

次に、**show running-config** コマンドの出力例を示します。この出力には、ローカル CA 証明書マップ ルールが表示されています。

```
crypto ca certificate map 1
 issuer-name co asc
 subject-name attr ou eq Engineering
```

証明書管理の履歴

表 *34 :* 証明書管理の履歴

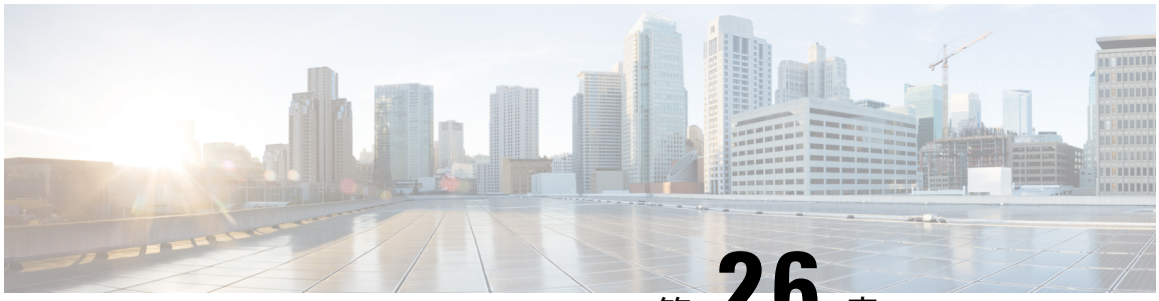
機能名	プラットフォーム リリース	説明
証明書管理	7.0(1)	デジタル証明書（CA 証明書、ID 証明書、およびコード署名者証明書など）は、認証用のデジタル ID を提供します。デジタル証明書には、名前、シリアル番号、会社、部門、またはIPアドレスなど、ユーザーまたはデバイスを識別する情報が含まれます。CAは、証明書に「署名」してその認証を確認することで、デバイスまたはユーザのアイデンティティを保証する、信頼できる機関です。CA は、公開キーまたは秘密キーの暗号化を使用してセキュリティを保証する PKI コンテキストで、デジタル証明書を発行します。
証明書管理	7.2(1)	次のコマンドを導入しました。 **issuer-name** *DN-string*、**revocation-check crl none**、**revocation-check crl**、**revocation-check none**。 **crl** {**required** | **optional** | **nocheck**} コマンドが非推奨になりました。

機能名	プラットフォーム リリース	説明
証明書管理	8.0(2)	次のコマンドを導入しました。 **cdp-url**、**crypto ca server**、**crypto ca server crl issue**、**crypto ca server revoke** *cert-serial-no*、**crypto ca server unrevoke** *cert-serial-no*、**crypto ca server user-db add** *user* [**dn** *dn*] [**email** *e-mail-address*]、**crypto ca server user-db allow** {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]、**crypto ca server user-db email-otp** {*username* | **all-unenrolled** | **all-certholders**}、**crypto ca server user-db remove** *username*、**crypto ca server user-db show-otp** {*username* | **all-certholders** | **all-unenrolled**}、**crypto ca server user-db write**、[**no**] **database path** *mount-name directory-path*、**debug crypto ca server** [*level*]、**lifetime** {**ca-certificate** | **certificate** | **crl**} *time*、**no shutdown**、**otp expiration** *timeout*、**renewal-reminder** *time*、**show crypto ca server**、**show crypto ca server cert-db** [**user** *username* | **allowed** | **enrolled** | **expired** | **on-hold**] [**serial** *certificate-serial-number*]、**show crypto ca server certificate**、**show crypto ca server crl**、**show crypto ca server user-db** [**expired** | **allowed** | **on-hold** | **enrolled**]、**show crypto key** *name of key*、**show running-config**、**shutdown**
SCEP プロキシ	8.4(1)	サードパーティ CA からのデバイス証明書を安全に構成できる機能を導入しました。 次のコマンドを導入しました。 **crypto ikev2 enable outside client-services port** *portnumber*、**scep-enrollment enable**、**scep-forwarding-url value** *URL*、**secondary-pre-fill-username clientless hide use-common-password** *password*、**secondary-pre-fill-username ssl-client hide use-common-password** *password*、**secondary-username-from-certificate** {**use-entire-name** | **use-script** | {*primary_attr* [*secondary-attr*]}} [**no-certificate-fallback cisco-secure-desktop machine-unique-id**]。

機能名	プラットフォーム リリース	説明
参照 ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 確認は syslog サーバーとスマート ライセンス サーバーへの TLS 接続の PKI 確認中に行われます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のコマンドが追加または変更されました。**crypto ca reference-identity**、**logging host**、**call home profile destination address**
ローカル CA サーバー	9.12(1)	ASA の構成済み FQDN を使用する代わりに設定可能な登録用 URL の FQDN を作成するため、新しい CLI オプションが導入されました。この新しいオプションは、crypto ca server の smpt モードに追加されます。 We deprecated Local CA Server and will be removing in a later release—When ASA is configured as local CA server, it is enabled to issue digital certificates, publish Certificate Revocation Lists（CRLs), and securely revoke issued certificates. この機能は古くなったため、crypto ca server コマンドは廃止されています。
ローカル CA サーバー	9.13(1)	ローカル CA サーバーのサポートが削除されました。したがって、**crypto ca server** コマンドとそのサブコマンドは削除されています。 **crypto ca server** コマンドとそのすべてのサブコマンドが削除されました。
CRL 分散ポイント コマンドの変更	9.13(1)	スタティック CDP URL コンフィギュレーション コマンドが削除され、match certificate コマンドに移行しました。 新規/変更されたコマンド：**crypto-ca-trustpoint crl** と **crl url** はその他の関連ロジックで削除され、**match-certificate override-cdp** が導入されました。

機能名	プラットフォーム リリース	説明
CRL キャッシュサイズの拡張	9.13(1)	大規模な CRL ダウンロードの失敗を防ぐため、キャッシュサイズを拡張し、また、個別の CRL 内のエントリ数の制限を取り除きました。 • マルチ コンテキスト モードの場合、コンテキストごとの合計 CRL キャッシュサイズが 16 MB に増加しました。 • シングル コンテキスト モードの場合、合計 CRL キャッシュサイズが 128 MB に増加しました。
証明書有効性チェックをバイパスするオプションの復元	9.15(1)	CRL または OCSP サーバーとの接続問題に起因する失効チェックをバイパスする 9.13(1) で削除されたオプションが復元されました。 新規/変更されたコマンド：**revocation-check crl none**、**revocation-check ocsp none**、**revocation-check crl ocsp none**、**revocation-check ocsp crl none** が復元されました。
スタティック CRL 分散ポイント URL をサポートするための match certificate コマンドの変更	9.15(1)	スタティック CDP URL コンフィギュレーション コマンドでは、スタティック CDP を検証中のチェーン内の各証明書に一意にマッピングできます。ただし、このようなマッピングは各証明書で 1 つだけサポートされていました。今回の変更で、静的に設定された CDP を認証用の証明書チェーンにマッピングできるようになりました。 新規/変更されたコマンド：**match certificate** *map* **override cdp** *seq* **url** *url* and **no match certificate** *map* **override cdp** *seq* **url** *url*
トラストポイントキーペアおよび暗号キー生成コマンドの変更	9.16(1)	2048 より小さいキーサイズの証明書のサポートが削除されました。512、768、または 1024 ビットのオプションを使用する設定は、必要性の通知とともに 2048 に移行されます。 認証に SHA1 ハッシュアルゴリズムを使用するサポートが削除されました。 （注） これらの制限を上書きする **crypto ca permit-weak-crypto** コマンドが導入されました。 新しいキーオプション EDDSA が、既存の RSA および ECDSA オプションに追加されました。

機能名	プラットフォーム リリース	説明
OCSP および CRL IPv6 URL のサポート	9.20(1)	IPv6 OCSP および CRL URL を使用するためのサポートが追加されました。IPv6 アドレスは角カッコで囲む必要があります。



第 26 章

ARP インスペクションおよび MAC アドレス テーブル

この章では、MACアドレステーブルのカスタマイズ方法、およびブリッジグループのARPインスペクションの設定方法について説明します。

- ARP インスペクションと MAC アドレス テーブルについて （1109 ページ）
- デフォルト設定 （1111 ページ）
- ARP インスペクションと MAC アドレス テーブルのガイドライン （1111 ページ）
- ARP インスペクションとその他の ARP パラメータの設定 （1111 ページ）
- トランスペアレントモードのブリッジグループにおけるMACアドレステーブルの （1114 ページ）
- ARP インスペクションと MAC アドレス テーブルのモニタリング （1116 ページ）
- ARP インスペクションと MAC アドレス テーブルの履歴 （1117 ページ）

ARP インスペクションと MAC アドレス テーブルについて

ブリッジ グループのインターフェイスでは、ARP インスペクションは「中間者」攻撃を防止します。他の ARP の設定をカスタマイズすることも可能です。ブリッジ グループの MAC アドレス テーブルのカスタマイズができます。これには、MAC スプーフィングに対する防御としてのスタティック ARP エントリの追加が含まれます。

ブリッジグループ トラフィックの ARP インスペクション

デフォルトでは、ブリッジグループのメンバーの間ですべてのARPパケットが許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。

ARPインスペクションによって、悪意のあるユーザが他のホストやルータになりすます（ARP スプーフィングと呼ばれる）のを防止できます。ARP スプーフィングが許可されていると、「中間者」攻撃を受けることがあります。たとえば、ホストが ARP 要求をゲートウェイ ルータに送信すると、ゲートウェイ ルータはゲートウェイ ルータのMACアドレスで応答します。

ただし、攻撃者は、ルータの MAC アドレスではなく攻撃者の MAC アドレスで別の ARP 応答をホストに送信します。これで、攻撃者は、すべてのホストトラフィックを代行受信してルータに転送できるようになります。

ARP インスペクションを使用すると、正しい MAC アドレスとそれに関連付けられた IP アドレスがスタティック ARP テーブル内にある限り、攻撃者は攻撃者の MAC アドレスで ARP 応答を送信できなくなります。

ARPインスペクションを有効化すると、ASAは、すべてのARPパケット内のMACアドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較し、次のアクションを実行します。

- IPアドレス、MACアドレス、および送信元インターフェイスがARPエントリと一致する場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間で不一致がある場合、ASAはパケットをドロップします。
- ARPパケットがスタティックARPテーブル内のどのエントリとも一致しない場合、パケットをすべてのインターフェイスに転送（フラッディング）するか、またはドロップするようにASAを設定できます。

（注） 専用の 管理 インターフェイスは、このパラメータが flood に設定されている場合でもパケットをフラッディングしません。

MAC アドレス テーブル

ブリッジ グループを使用する場合、ASA は、通常のブリッジまたはスイッチと同様に、MAC アドレスを学習して MAC アドレス テーブルを作成します。デバイスがブリッジ グループ経由でパケットを送信すると、ASA が MAC アドレスをアドレス テーブルに追加します。テーブルで MAC アドレスと発信元インターフェイスが関連付けられているため、ASAは、パケットが正しいインターフェイスからデバイスにアドレス指定されていることがわかります。ブリッジ グループ メンバー間のトラフィックには ASA セキュリティ ポリシーが適用されるため、パケットの宛先 MAC アドレスがテーブルに含まれていなくても、通常のブリッジのように、すべてのインターフェイスに元のパケットを ASA がフラッディングすることはありません。代わりに、直接接続されたデバイスまたはリモートデバイスに対して次のパケットを生成します。

- 直接接続されたデバイスへのパケット：ASA は宛先 IP アドレスに対して ARP 要求を生成し、ARP 応答を受信したインターフェイスを学習します。
- リモート デバイスへのパケット：ASA は宛先 IP アドレスへの ping を生成し、ping 応答を受信したインターフェイスを学習します。

元のパケットはドロップされます。

ルーテッドモードでは、すべてのインターフェイスで非 IP パケットのフラッディングをオプションで有効にできます。

デフォルト設定

- ARP インスペクションを有効にした場合、デフォルト設定では、一致しないパケットはフラッディングします。
- ダイナミック MAC アドレス テーブル エントリのデフォルトのタイムアウト値は 5 分です。
- デフォルトでは、各インターフェイスはトラフィックに入る MAC アドレスを自動的に学習し、ASAは対応するエントリを MAC アドレス テーブルに追加します。

（注） Secure Firewall ASA はリセットパケットを生成し、ステートフル検査エンジンによって拒否された接続をリセットします。リセットパケットでは、パケットの宛先 MAC アドレスが ARP テーブルのルックアップに基づいて決定されるのではなく、拒否されるパケット（接続）から直接取得されます。

ARP インスペクションと MAC アドレス テーブルのガイドライン

- ARP インスペクションは、ブリッジ グループでのみサポートされます。
- MAC アドレス テーブル構成は、ブリッジ グループでのみサポートされます。

ARP インスペクションとその他の ARP パラメータの設定

ブリッジ グループでは、ARP インスペクションをイネーブルにすることができます。その他の ARP パラメータは、ブリッジ グループとルーテッド モードのインターフェイスの両方で設定できます。

手順

ステップ 1 スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ（1112 ページ）に従って、スタティック ARP エントリを追加します。ARP インスペクションは ARP パケットを

ARP テーブルのスタティック ARP エントリと比較するので、この機能にはスタティック ARP エントリが必要です。その他の ARP パラメータも設定できます。

ステップ 2 ARP インスペクションの有効化 （1114 ページ）に従って ARP インスペクションを有効にします。

スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ

ブリッジグループのデフォルトでは、ブリッジ グループ メンバー インターフェイス間の ARP パケットはすべて許可されます。ARP パケットのフローを制御するには、ARP インスペクションをイネーブルにします。ARP インスペクションは、ARP パケットを ARP テーブルのスタティック ARP エントリと比較します。

ルーテッド インターフェイスの場合、スタティック ARP エントリを入力できますが、通常はダイナミック エントリで十分です。ルーテッド インターフェイスの場合、直接接続されたホストにパケットを配送するために ARP テーブルが使用されます。送信者は IP アドレスでパケットの宛先を識別しますが、イーサネットにおける実際のパケット配信は、イーサネット MAC アドレスに依存します。ルータまたはホストは、直接接続されたネットワークでパケットを配信する必要がある場合、IP アドレスに関連付けられた MAC アドレスを要求する ARP 要求を送信し、ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータには ARP テーブルが保管されるため、配信が必要なパケットごとに ARP 要求を送信する必要はありません。ARP テーブルは、ARP 応答がネットワーク上で送信されるたびにダイナミックに更新されます。一定期間使用されなかったエントリは、タイムアウトします。エントリが正しくない場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合など）、新しい情報で更新される前にこのエントリがタイムアウトする必要があります。

トランスペアレント モードの場合、管理トラフィックなどの ASA との間のトラフィックに、ASA は ARP テーブルのダイナミック ARP エントリのみを使用します。

ARP タイムアウトなどの ARP 動作を設定することもできます。

手順

ステップ 1 スタティック ARP エントリを追加します。

arp *interface_name ip_address mac_address* [**alias**]

例：

```
ciscoasa(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

この例では、外部インターフェイスで、IP アドレスが 10.1.1.1、MAC アドレスが 0009.7cbe.2100 のルータからの ARP 応答が許可されます。

このマッピングでプロキシ ARP を有効にするには、ルーテッド モードで**alias**を指定します。ASA は、指定された IP アドレスの ARP 要求を受信すると、ASA MAC アドレスで応答します。このキーワードは、ARP を実行しないデバイスがある場合などに役立ちます。トランスペアレント ファイアウォール モードでは、このキーワードは無視されます。ASA はプロキシ ARP を実行しません。

ステップ 2 ダイナミック ARP エントリの ARP タイムアウトを設定します。

arp timeout *seconds*

例：

```
ciscoasa(config)# arp timeout 5000
```

このフィールドでは、ASA が ARP テーブルを再構築するまでの時間を、60 ～ 4294967 秒の範囲で設定します。デフォルトは14400秒です。ARPテーブルを再構築すると、自動的に新しいホスト情報が更新され、古いホスト情報が削除されます。ホスト情報は頻繁に変更されるため、タイムアウトを短くすることが必要になる場合があります。

ステップ 3 非接続サブネットを許可する

arp permit-nonconnected

ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。ARPキャッシュをイネーブルにして、間接接続されたサブネットを含めることもできます。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASA に対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。

次の機能を使用する場合は、この機能を使用する必要がある可能性があります。

- セカンデリ サブネット。
- トラフィック転送の隣接ルートのプロキシ ARP。

ステップ 4 ARP レート制限を設定して 1 秒あたりの ARP パケット数を制御する

arp rate-limit *seconds*

例：

```
ciscoasa(config)# arp rate-limit 1000
```

10 ～ 32768 の範囲で値を入力します。デフォルト値は ASA モデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。

ARP インスペクションの有効化

この項では、ブリッジ グループ用に ARP インスペクションをイネーブルにする方法について説明します。

手順

ARP インスペクションをイネーブルにします。

arp-inspection *interface_name* **enable** [**flood** | **no-flood**]

例：

```
ciscoasa(config)# arp-inspection outside enable no-flood
```

flood キーワードは、一致しない ARP パケットをすべてのインターフェイスに転送し、**no-flood** は、一致しないパケットをドロップします。

デフォルト設定では、一致しないパケットはフラッドします。スタティック エントリにある ARP だけが ASA を通過するように制限するには、このコマンドを **no-flood** に設定します。

トランスペアレントモードのブリッジグループにおける MAC アドレス テーブルの

ここでは、ブリッジグループの MAC アドレステーブルをカスタマイズする方法について説明します。

ブリッジ グループのスタティック MAC アドレスの追加

通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティック エントリと同じ MAC アドレスを持つクライアントが、そのスタティック エントリに一致しないインターフェイスにトラフィックを送信しようとした場合、ASA はトラフィックをドロップし、システム メッセージを生成します。スタティック ARP エントリを追加するときに（スタティック ARP エントリの追加と、他の ARP パラメータのカスタマイズ（1112 ページ）を参照）、スタティック MAC アドレス エントリは MAC アドレス テーブルに自動的に追加されます。

MAC アドレス テーブルにスタティック MAC アドレスを追加するには、次の手順を実行します。

手順

スタティック MAC アドレス エントリを追加します。

mac-address-table static *interface_name mac_address*

例：

```
ciscoasa(config)# mac-address-table static inside 0009.7cbe.2100
```

interface_name は、発信元インターフェイスです。

MAC アドレス タイムアウトを設定する

ダイナミック MAC アドレス テーブルのデフォルトのタイムアウト値は 5 分ですが、タイムアウトは変更できます。タイムアウトを変更するには、次の手順を実行します。

手順

MAC アドレス エントリのタイムアウトを設定します。

mac-address-table aging-time *timeout_value*

例：

```
ciscoasa(config)# mac-address-table aging-time 10
```

timeout_value（分）は、5 ～ 720（12 時間）です。5 分がデフォルトです。

MAC アドレスラーニングの設定

デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできますが、この場合、MAC アドレスをテーブルにスタティックに追加しないと、トラフィックが ASA を通過できなくなります。ルーテッドモードでは、すべてのインターフェイスで非 IP パケットのフラッディングを有効にできます。

MAC アドレスラーニングを設定にするには、次の手順を実行します。

手順

ステップ 1 MAC アドレス ラーニングをディセーブルにします。

mac-learn *interface_name* **disable**

例：

```
ciscoasa(config)# mac-learn inside disable
```

このコマンドの **no** 形式を使用すると、MAC アドレス ラーニングが再度イネーブルになります。

clear configure mac-learn コマンドは、すべてのインターフェイスで MAC アドレス ラーニングを再度イネーブルにします。

ステップ 2 （ルーテッドモードのみ）非 IP パケットのフラッディングを有効にします。

mac-learn flood

例：

```
ciscoasa(config)# mac-learn flood
```

ARP インスペクションと MAC アドレス テーブルのモニタリング

- **show arp-inspection**

  ARP インスペクションをモニターします。すべてのインターフェイスについて、ARP インスペクションの現在の設定を表示します。

- **show mac-address-table [*interface_name*]**

  MAC アドレス テーブルをモニターします。すべての MAC アドレス テーブル（両方のインターフェイスのスタティック エントリとダイナミック エントリ）を表示できます。または、あるインターフェイスの MAC アドレス テーブルを表示できます。

  すべてのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table
interface        mac address           type         Time Left
------------------------------------------------------------------------
outside     0009.7cbe.2100       static    -
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

内部インターフェイスのテーブルを表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table inside
interface        mac address       type         Time Left
------------------------------------------------------------------------
inside     0010.7cbe.6101       static    -
inside     0009.7cbe.5101       dynamic    10
```

スタティックおよびダイナミック ブリッジ グループのエントリの合計数を表示する **show mac-address-table** コマンドの出力例を示します。

```
ciscoasa# show mac-address-table count
Static     mac-address bridges (curr/max): 0/16384
Dynamic    mac-address bridges (curr/max): 0/16384
```

ARP インスペクションと MAC アドレス テーブルの履歴

機能名	プラットフォーム リリース	機能情報
ARP インスペクション	7.0(1)	ARP インスペクションは、すべての ARP パケットの MACアドレス、IPアドレス、および送信元インターフェイスを、ARP テーブルのスタティック エントリと比較します。この機能は、トランスペアレント ファイアウォール モード、および 9.7(1) で始まるトランスペアレントモードとルーテッドモードのブリッジグループのインターフェイスで利用できます。 **arp**、**arp-inspection**、および **show arp-inspection** コマンドが導入されました。
MAC アドレス テーブル	7.0(1)	トランスペアレント モード、および 9.7(1) で始まるトランスペアレントモードとルーテッドモードのブリッジグループのインターフェイスの MAC アドレス テーブルをカスタマイズすることもできます。 **mac-address-table static**、**mac-address-table aging-time**、**mac-learn disable**、および **show mac-address-table** コマンドが導入されました。

機能名	プラットフォーム リリース	機能情報
間接接続されたサブネットのARPキャッシュの追加	8.4(5)/9.1(2)	ASA ARP キャッシュには、直接接続されたサブネットからのエントリだけがデフォルトで含まれています。また、ARPキャッシュに間接接続されたサブネットを含めることができるようになりました。セキュリティリスクを認識していない場合は、この機能をイネーブルにすることは推奨しません。この機能は、ASAに対するサービス拒否（DoS）攻撃を助長する場合があります。任意のインターフェイスのユーザが大量の ARP 応答を送信して、偽エントリで ASA ARP テーブルがあふれる可能性があります。 次の機能を使用する場合は、この機能を使用する必要がある可能性があります。 • セカンデリ サブネット。 • トラフィック転送の隣接ルートのプロキシ ARP。 **arp permit-nonconnected** コマンドが導入されました。
カスタマイズ可能な ARP レート制限	9.6(2)	1秒あたり許可されるARPパケットの最大数を設定できます。デフォルト値はASAモデルによって異なります。この値は ARP ストーム攻撃を防ぐためにカスタマイズできます。 次のコマンドを追加しました。**arp rate-limit**、**show arp rate-limit**

機能名	プラットフォーム リリース	機能情報
Integrated Routing and Bridging（IRB）	9.7(1)	Integrated Routing and Bridging（統合ルーティングおよびブリッジング）は、ブリッジグループとルーテッドインターフェイス間をルーティングする機能を提供します。ブリッジグループとは、ASA がルートの代わりにブリッジするインターフェイスのグループのことです。ASA は、ASA がファイアウォールとして機能し続ける点で本来のブリッジとは異なります。つまり、インターフェイス間のアクセス制御が実行され、通常のファイアウォール検査もすべて実行されます。以前は、トランスペアレント ファイアウォール モードでのみブリッジグループの設定が可能だったため、ブリッジグループ間でのルーティングはできませんでした。この機能を使用すると、ルーテッド ファイアウォール モードのブリッジ グループの設定と、ブリッジグループ間およびブリッジグループとルーテッドインターフェイス間のルーティングを実行できます。ブリッジ グループは、ブリッジ仮想インターフェイス（BVI）を使用して、ブリッジ グループのゲートウェイとして機能することによってルーティングに参加します。そのブリッジグループに指定する ASA 上に別のインターフェイスが存在する場合、Integrated Routing and Bridging（IRB）は外部レイヤ 2 スイッチの使用に代わる手段を提供します。ルーテッドモードでは、BVI は名前付きインターフェイスとなり、アクセス ルールや DHCP サーバーなどの一部の機能に、メンバー インターフェイスとは個別に参加できます。 トランスペアレント モードでサポートされるマルチ コンテキスト モードや ASA クラスタリングの各機能は、ルーテッドモードではサポートされません。マルチキャスト ルーティングとダイナミック ルーティングの機能も、BVI ではサポートされません。 次のコマンドが変更されました。**access-group**、**access-list ethertype**、**arp-inspection**、**dhcpd**、**mac-address-table static**、**mac-address-table aging-time**、**mac-learn**、**route**、**show arp-inspection**、**show bridge-group**、**show mac-address-table**、**show mac-learn**

第 V 部

IP ルーティング

- ルーティングの概要 （1123 ページ）
- スタティック ルートとデフォルト ルート （1139 ページ）
- ポリシーベースルーティング （1151 ページ）
- ルート マップ （1175 ページ）
- 双方向フォワーディング検出ルーティング （1183 ページ）
- BGP （1195 ページ）
- Open Shortest Path First（OSPF） （1241 ページ）
- IS-IS （1311 ページ）
- EIGRP （1367 ページ）
- マルチキャスト ルーティング （1401 ページ）

第 27 章

ルーティングの概要

この章では、ASA 内でのルーティングの動作について説明します。

- パスの決定 （1123 ページ）
- サポートされるルート タイプ （1124 ページ）
- ルーティングでサポートされるインターネット プロトコル （1126 ページ）
- ルーティングテーブル （1127 ページ）
- 管理トラフィック用ルーティングテーブル （1134 ページ）
- Equal-Cost Multipath（ECMP）ルーティング （1135 ページ）
- プロキシ ARP 要求のディセーブル化 （1136 ページ）
- ルーティング テーブルの表示 （1137 ページ）
- ルート概要の履歴 （1138 ページ）

パスの決定

ルーティング プロトコルでは、メトリックを使用して、パケットの移動に最適なパスを評価します。メトリックは、宛先への最適なパスを決定するためにルーティング アルゴリズムが使用する、パスの帯域幅などの測定基準です。パスの決定プロセスを支援するために、ルーティング アルゴリズムは、ルート情報が格納されるルーティング テーブルを初期化して保持します。ルート情報は、使用するルーティング アルゴリズムによって異なります。

ルーティング アルゴリズムにより、さまざまな情報がルーティング テーブルに入力されます。宛先またはネクスト ホップの関連付けにより、最終的な宛先に達するまで、「ネクスト ホップ」を表す特定のルータにパケットを送信することによって特定の宛先に最適に到達できることがルータに示されます。ルータは、着信パケットを受信すると宛先アドレスを確認し、このアドレスとネクスト ホップとを関連付けようとします。

ルーティング テーブルには、パスの妥当性に関するデータなど、他の情報を格納することもできます。ルータは、メトリックを比較して最適なルートを決定します。これらのメトリックは、使用しているルーティング アルゴリズムの設計によって異なります。

ルータは互いに通信し、さまざまなメッセージの送信によりそのルーティング テーブルを保持しています。ルーティング アップデート メッセージはそのようなメッセージの 1 つで、通常はルーティング テーブル全体か、その一部で構成されています。ルーティング アップデート

を他のすべてのルータから分析することで、ルータはネットワークトポロジの詳細な全体像を構築できます。ルータ間で送信されるメッセージのもう1つの例であるリンクステートアドバタイズメントは、他のルータに送信元のリンクのステートを通知します。リンク情報も、ネットワークの宛先に対する最適なルートをルータが決定できるように、ネットワークトポロジの全体像の構築に使用できます。

（注） 非対称ルーティングがサポートされるのは、マルチ コンテキスト モードでのアクティブ/アクティブ フェールオーバーに対してのみです。

サポートされるルート タイプ

ルータが使用できるルート タイプには、さまざまなものがあります。ASA では、次のルート タイプが使用されます。

- スタティックとダイナミックの比較
- シングルパスとマルチパスの比較
- フラットと階層型の比較
- リンクステートと距離ベクトル型の比較

スタティックとダイナミックの比較

スタティック ルーティング アルゴリズムは、実はネットワーク管理者が確立したテーブル マップです。このようなマッピングは、ネットワーク管理者が変更するまでは変化しません。スタティック ルートを使用するアルゴリズムは設計が容易であり、ネットワーク トラフィックが比較的予想可能で、ネットワーク設計が比較的単純な環境で正しく動作します。

スタティック ルーティング システムはネットワークの変更に対応できないため、一般に、変化を続ける大規模なネットワークには不向きであると考えられています。主なルーティング アルゴリズムのほとんどはダイナミック ルーティング アルゴリズムであり、受信したルーティング アップデート メッセージを分析することで、変化するネットワーク環境に適合します。メッセージがネットワークが変化したことを示している場合は、ルーティング ソフトウェアはルートを再計算し、新しいルーティング アップデート メッセージを送信します。これらのメッセージはネットワーク全体に送信されるため、ルータはそのアルゴリズムを再度実行し、それに従ってルーティング テーブルを変更します。

ダイナミック ルーティング アルゴリズムは、必要に応じてスタティック ルートで補足できます。たとえば、ラストリゾートルータ（ルーティングできないすべてのパケットが送信されるルータのデフォルトルート）を、ルーティングできないすべてのパケットのリポジトリとして機能するように指定し、すべてのメッセージを少なくとも何らかの方法で確実に処理することができます。

シングルパスとマルチパスの比較

一部の高度なルーティング プロトコルは、同じ宛先に対する複数のパスをサポートしています。シングルパス アルゴリズムとは異なり、これらのマルチパス アルゴリズムでは、複数の回線でトラフィックを多重化できます。マルチパス アルゴリズムの利点は、スループットと信頼性が大きく向上することであり、これは一般に「ロードシェアリング」と呼ばれています。

フラットと階層型の比較

ルーティング アルゴリズムには、フラットなスペースで動作するものと、ルーティング階層を使用するものがあります。フラット ルーティング システムでは、ルータは他のすべてのルータのピアになります。階層型ルーティング システムでは、一部のルータが実質的なルーティング バックボーンを形成します。バックボーン以外のルータからのパケットはバックボーン ルータに移動し、宛先の一般エリアに達するまでバックボーンを通じて送信されます。この時点で、パケットは、最後のバックボーン ルータから、1 つ以上のバックボーン以外のルータを通じて最終的な宛先に移動します。

多くの場合、ルーティング システムは、ドメイン、自律システム、またはエリアと呼ばれるノードの論理グループを指定します。階層型のシステムでは、ドメイン内の一部のルータは他のドメインのルータと通信できますが、他のルータはそのドメイン内のルータ以外とは通信できません。非常に大規模なネットワークでは、他の階層レベルが存在することがあり、最も高い階層レベルのルータがルーティング バックボーンを形成します。

階層型ルーティングの第一の利点は、ほとんどの企業の組織を模倣しているため、そのトラフィック パターンを適切にサポートするという点です。ほとんどのネットワーク通信は、小さい企業グループ（ドメイン）内で発生します。ドメイン内ルータは、そのドメイン内の他のルータだけを認識していれば済むため、そのルーティング アルゴリズムを簡素化できます。また、使用しているルーティング アルゴリズムに応じて、ルーティング アップデート トラフィックを減少させることができます。

リンクステートと距離ベクトル型の比較

リンクステート アルゴリズム（最短パス優先アルゴリズムとも呼ばれる）は、インターネットワークのすべてのノードにルーティング情報をフラッドします。ただし、各ルータは、それ自体のリンクのステートを記述するルーティング テーブルの一部だけを送信します。リンクステート アルゴリズムでは、各ルータはネットワークの全体像をそのルーティング テーブルに構築します。距離ベクトル型アルゴリズム（Bellman-Ford アルゴリズムとも呼ばれる）では、各ルータが、そのネイバーだけに対してそのルーティング テーブル全体または一部を送信するように要求されます。つまり、リンクステート アルゴリズムは小規模なアップデートを全体に送信しますが、距離ベクトル型アルゴリズムは、大規模なアップデートを隣接ルータだけに送信します。距離ベクトル型アルゴリズムは、そのネイバーだけを認識します。通常、リンクステート アルゴリズムは OSPF ルーティング プロトコルとともに使用されます。

ルーティングでサポートされるインターネットプロトコル

ASAは、ルーティングに対してさまざまなインターネットプロトコルをサポートしています。この項では、各プロトコルについて簡単に説明します。

- Enhanced Interior Gateway Routing Protocol（EIGRP）

  EIGRP は、IGRP ルータとの互換性とシームレスな相互運用性を提供するシスコ独自のプロトコルです。自動再配布メカニズムにより、IGRP ルートを Enhanced IGRP に、または Enhanced IGRP からインポートできるため、Enhanced IGRP を既存の IGRP ネットワークに徐々に追加できます。

- Open Shortest Path First（OSPF）

  OSPF は、インターネット プロトコル（IP）ネットワーク向けに、インターネット技術特別調査委員会（IETF）の Interior Gateway Protocol（IGP）作業部会によって開発されたルーティング プロトコルです。OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

- Routing Information Protocol（RIP）

  RIP は、ホップ カウントをメトリックとして使用するディスタンスベクトル プロトコルです。RIP は、グローバルなインターネットでトラフィックのルーティングに広く使用されている Interior Gateway Protocol（IGP）です。つまり、1 つの自律システム内部でルーティングを実行します。

- ボーダー ゲートウェイ プロトコル（BGP）

  BGP は自律システム間のルーティング プロトコルです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。カスタマーはISPに接続し、ISPはBGPを使用してカスタマーおよびISPルートを交換します。自律システム（AS）間で BGP を使用する場合、このプロトコルは外部 BGP（EBGP）と呼ばれます。サービスプロバイダーが BGP を使用して AS 内のルートを交換する場合、このプロトコルは内部 BGP（IBGP）と呼ばれます。

- Intermediate System to Intermediate System（IS-IS）

  IS-IS はリンクステート内部ゲートウェイ プロトコル（IGP）です。リンクステート プロトコルは、各参加ルータで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。

ルーティングテーブル

ASA はデータ トラフィック（デバイスを介して）および管理トラフィック（デバイスから）に別々のルーティングテーブルを使用します。ここでは、ルーティングテーブルの仕組みについて説明します。管理ルーティングテーブルの詳細については、管理トラフィック用ルーティングテーブル （1134 ページ）も参照してください。

ルーティング テーブルへの入力方法

ASAルーティングテーブルには、静的に定義されたルート、直接接続されているルート、およびダイナミック ルーティング プロトコルで検出されたルートを入力できます。ASA デバイスは、ルーティングテーブルに含まれるスタティックルートと接続されているルートに加えて、複数のルーティングプロトコルを実行できるため、同じルートが複数の方法で検出または入力される可能性があります。同じ宛先への 2 つのルートがルーティング テーブルに追加されると、ルーティング テーブルに残るルートは次のように決定されます。

- 2 つのルートのネットワーク プレフィックス長（ネットワーク マスク）が異なる場合は、どちらのルートも固有と見なされ、ルーティングテーブルに入力されます。入力された後は、パケット転送ロジックが 2 つのうちどちらを使用するかを決定します。

  たとえば、RIP プロセスと OSPF プロセスが次のルートを検出したとします。

  - RIP：192.168.32.0/24
  - OSPF：192.168.32.0/19

  OSPF ルートのアドミニストレーティブ ディスタンスの方が適切であるにもかかわらず、これらのルートのプレフィックス長（サブネットマスク）はそれぞれ異なるため、両方のルートがルーティング テーブルにインストールされます。これらは異なる宛先と見なされ、パケット転送ロジックが使用するルートを決定します。

- ASA デバイスが、（RIP などの）1 つのルーティングプロトコルから同じ宛先に複数のパスがあることを検知すると、（ルーティングプロトコルが判定した）メトリックがよい方のルートがルーティングテーブルに入力されます。

  メトリックは特定のルートに関連付けられた値で、ルートを最も優先されるものから順にランク付けします。メトリックスの判定に使用されるパラメータは、ルーティングプロトコルによって異なります。メトリックが最も小さいパスは最適パスとして選択され、ルーティングテーブルにインストールされます。同じ宛先への複数のパスのメトリックが等しい場合は、これらの等コスト パスに対してロード バランシングが行われます。

- ASA デバイスが、ある宛先へのルーティングプロトコルが複数あることを検知すると、ルートのアドミニストレーティブディスタンスが比較され、アドミニストレーティブディスタンスが最も小さいルートがルーティングテーブルに入力されます。

ルートのアドミニストレーティブ ディスタンス

ルーティング プロトコルによって検出されるルート、またはルーティング プロトコルに再配布されるルートのアドミニストレーティブ ディスタンスは変更できます。2 つの異なるルーティングプロトコルからの2つのルートのアドミニストレーティブディスタンスが同じ場合、デフォルトのアドミニストレーティブディスタンスが小さい方のルートがルーティングテーブルに入力されます。EIGRP ルートと OSPF ルートの場合、EIGRP ルートと OSPF ルートのアドミニストレーティブ ディスタンスが同じであれば、デフォルトで EIGRP ルートが選択されます。

アドミニストレーティブディスタンスは、2つの異なるルーティングプロトコルから同じ宛先に複数の異なるルートがある場合に、ASAが最適なパスの選択に使用するルートパラメータです。ルーティングプロトコルには、他のプロトコルと異なるアルゴリズムに基づいたメトリックがあるため、異なるルーティングプロトコルによって生成された同じ宛先への2つのルートのいずれが最適パスであるかは、必ずしも判別できません。

各ルーティング プロトコルには、アドミニストレーティブ ディスタンス値を使用して優先順位が付けられています。次の表に、ASAでサポートされているルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス値を示します。

表 *35*：サポートされるルーティングプロトコルのデフォルトのアドミニストレーティブディスタンス

ルートの送信元	デフォルトのアドミニストレーティブディスタンス
接続されているインターフェイス	0
VPN ルート	1
スタティック ルート	1
EIGRP集約ルート	5
外部 BGP	20
内部 EIGRP	90
OSPF	110
IS-IS	115
RIP	120
EIGRP 外部ルート	170
内部およびローカルBGP	200
不明	255

アドミニストレーティブ ディスタンス値が小さいほど、プロトコルの優先順位が高くなります。たとえば、ASAが OSPF ルーティング プロセス（デフォルトのアドミニストレーティブ

ディスタンスが 110）と RIP ルーティング プロセス（デフォルトのアドミニストレーティブ ディスタンスが 120）の両方から特定のネットワークへのルートを受信すると、OSPF ルーティング プロセスの方が優先度が高いため、ASAはOSPFルートを選択します。この場合、ルータは OSPF バージョンのルートをルーティング テーブルに追加します。

VPN アドバタイズされたルート（V-Route/RRI）は、デフォルトのアドミニストレーティブ ディスタンス 1 のスタティックルートと同等です。ただし、ネットワークマスク 255.255.255.255 の場合と同じように優先度が高くなります。

この例では、OSPF 導出ルートの送信元が（電源遮断などで）失われると、ASAは、OSPF 導出ルートが再度現れるまで、RIP 導出ルートを使用します。

アドミニストレーティブ ディスタンスはローカルの設定値です。たとえば、OSPF を通じて取得したルートのアドミニストレーティブディスタンスを変更する場合、その変更は、コマンドが入力された ASA のルーティング テーブルにだけ影響します。アドミニストレーティブ ディスタンスがルーティング アップデートでアドバタイズされることはありません。

アドミニストレーティブ ディスタンスは、ルーティング プロセスに影響を与えません。ルーティング プロセスは、ルーティング プロセスで検出されたか、またはルーティング プロセスに再配布されたルートだけをアドバタイズします。たとえば、RIPルーティングプロセスは、のルーティング テーブルで OSPF ルーティング プロセスによって検出されたルートが使用されていても、RIP ルートをアドバタイズします。

ダイナミック ルーロとフローティング スタティック ルートのバックアップ

ルートを最初にルーティングテーブルにインストールしようとしたとき、他のルートがインストールされてしまい、インストールできなかった場合に、そのルートはバックアップルートとして登録されます。ルーティングテーブルにインストールされたルートに障害が発生すると、ルーティング テーブル メンテナンス プロセスが、登録されたバックアップ ルートを持つ各ルーティングプロトコルプロセスを呼び出し、ルーティングテーブルにルートを再インストールするように要求します。障害が発生したルートに対して登録されたバックアップルートを持つプロトコルが複数ある場合、アドミニストレーティブディスタンスに基づいて優先順位の高いルートが選択されます。

このプロセスのため、ダイナミック ルーティング プロトコルによって検出されたルートに障害が発生したときにルーティング テーブルにインストールされるフローティング スタティック ルートを作成できます。フローティングスタティックルートとは、単に、ASAで動作しているダイナミックルーティングプロトコルよりも大きなアドミニストレーティブディスタンスが設定されているスタティックルートです。ダイナミック ルーティング プロセスで検出された対応するルートに障害が発生すると、このスタティック ルートがルーティング テーブルにインストールされます。

転送の決定方法

転送は次のように決定されます。

- 宛先が、ルーティング テーブル内のエントリと一致しない場合、パケットはデフォルト ルートに指定されているインターフェイスを通して転送されます。デフォルトルートが設定されていない場合、パケットは破棄されます。
- 宛先が、ルーティングテーブル内の1つのエントリと一致した場合、パケットはそのルートに関連付けられているインターフェイスを通して転送されます。
- 宛先がルーティングテーブル内の複数のエントリと一致した場合は、パケットが、ネットワーク プレフィックス長がより長いルートに関連付けられたインターフェイスから転送されます。

たとえば、192.168.32.1宛てのパケットが、ルーティングテーブルの次のルートでインターフェイスに到着するとします。

- 192.168.32.0/24 ゲートウェイ 10.1.1.2
- 192.168.32.0/19 ゲートウェイ 10.1.1.3

この場合、192.168.32.1 は 192.168.32.0/24 ネットワーク内にあるため、192.168.32.1 宛てのパケットは 10.1.1.2 宛てに送信されます。もうひとつのルートにもあてはまりますが、192.168.32.0/24 の方が長いプレフィックスを持つためです（24 ビットと 19 ビット）。パケットを転送する場合、プレフィックスが長い方が常に短いものより優先される。

（注） 既存の接続は、新しい同様の接続がルートの変更により異なる動作になる場合でも、引き続き確立されたインターフェイスを使用します。

ダイナミック ルーティングおよび フェールオーバー

アクティブなユニットでルーティング テーブルが変更されると、スタンバイ ユニットでダイナミック ルートが同期されます。これは、アクティブ ユニットのすべての追加、削除、または変更がただちにスタンバイ ユニットに伝播されることを意味します。スタンバイ ユニットがアクティブ/スタンバイの待受中 フェールオーバー ペアでアクティブになると、ルートはフェールオーバー バルク同期および連続複製プロセスの一部として同期されるため、そのユニットには以前のアクティブ ユニットと同じルーティング テーブルがすでに作成されています。

ダイナミック ルーティングおよびクラスタリング

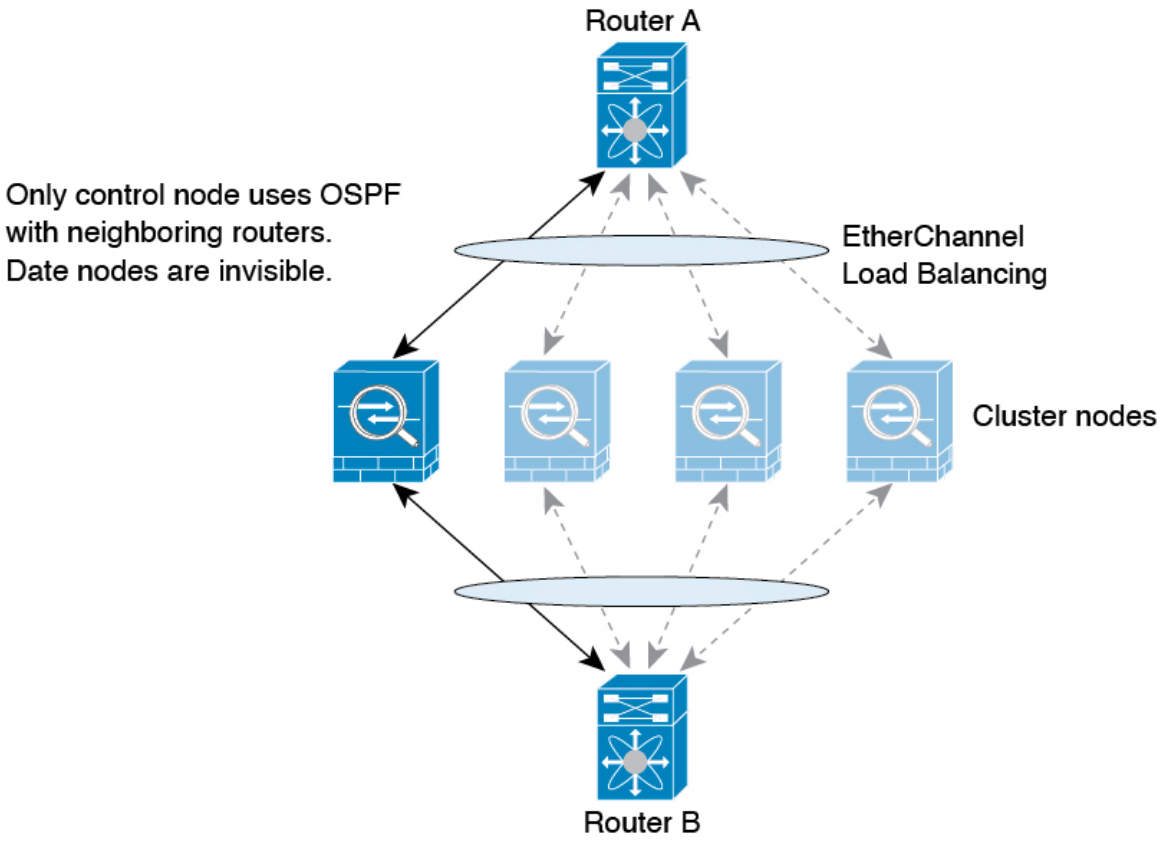
ここでは、クラスタリングでダイナミックルーティングを使用する方法について説明します。

スパンド EtherChannel モードでのダイナミック ルーティング

（注） IS-IS は、スパンド EtherChannel モードではサポートされていません。

ルーティングプロセスは制御ノード上だけで実行されます。ルートは制御ノードを介して学習され、データノードに複製されます。ルーティングパケットは、データノードに到着すると制御ノードにリダイレクトされます。

図 *77* : スパンド *EtherChannel* モードでのダイナミック ルーティング



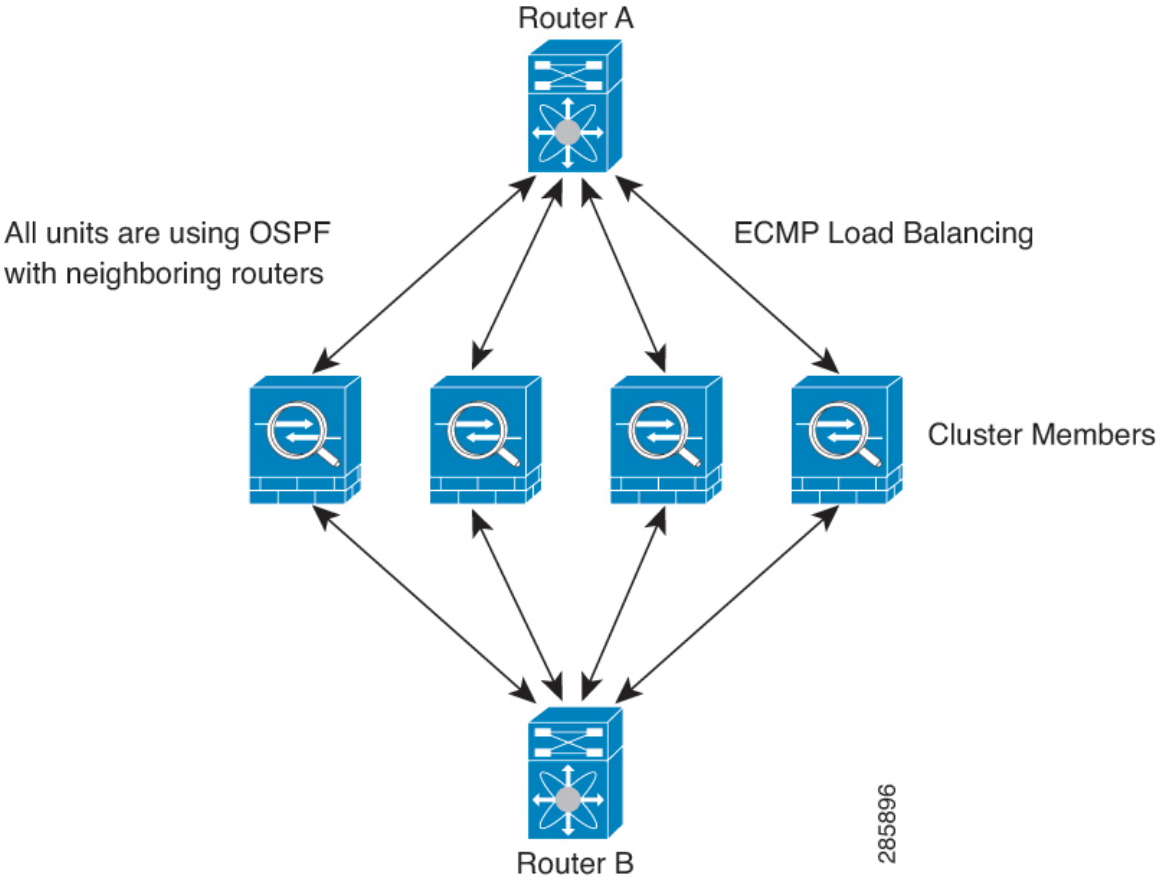
データノードが制御ノードからルートを学習すると、各ノードが個別に転送の判断を行います。

OSPF LSA データベースは、制御ノードからデータノードに同期されません。制御ノードのスイッチオーバーが発生した場合、ネイバールータが再起動を検出します。スイッチオーバーは透過的ではありません。OSPF プロセスが IP アドレスの 1 つをルータ ID として選択します。必須ではありませんが、スタティック ルータ ID を割り当てることができます。これで、同じルータ IDがクラスタ全体で使用されるようになります。割り込みを解決するには、OSPF ノンストップ フォワーディング機能を参照してください。

個別インターフェイス モードでのダイナミック ルーティング

個別インターフェイスモードでは、各ノードがスタンドアロンルータとしてルーティングプロトコルを実行します。ルートの学習は、各ノードが個別に行います。

図 *78 :* 個別インターフェイス モードでのダイナミック ルーティング



上の図では、ルータ A はルータ B への等コストパスが 4 本あることを学習します。パスはそれぞれ 1 つのノードを通過します。ECMP を使用して、4 パス間でトラフィックのロード バランシングを行います。各ノードは、外部ルータと通信するときに、それぞれ異なるルータ ID を選択します。

管理者は、各ノードに異なるルータ ID が設定されるように、ルータ ID のクラスタ プールを設定する必要があります。

EIGRP は、個別のインターフェイス モードのクラスタ ピアとのネイバー関係を形成しません。

（注） 冗長性の目的で、クラスタに同じルータへの複数の隣接関係がある場合、非対称ルーティングは許容できないトラフィック損失の原因となる可能性があります。非対称ルーティングを避けるためには、同じトラフィック ゾーンにこれらすべてのノードインターフェイスをまとめます。トラフィック ゾーンの設定 （995 ページ）を参照してください。

マルチ コンテキスト モードのダイナミック ルーティング

マルチ コンテキスト モードでは、各コンテキストで個別のルーティング テーブルおよびルーティング プロトコル データベースが維持されます。これにより、各コンテキストの OSPFv2 およびEIGRP を個別に設定することができます。EIGRP をあるコンテキストで設定し、OSPFv2 を同じまたは異なるコンテキストで設定できます。混合コンテキスト モードでは、ルーテッド モードのコンテキストの任意のダイナミック ルーティング プロトコルをイネーブルにできます。RIP および OSPFv3 は、マルチ コンテキスト モードではサポートされていません。

次の表に、EIGRP、OSPFv2、OSPFv2 および EIGRP プロセスへのルートの配布に使用されるルート マップ、およびマルチ コンテキスト モードで使用されている場合にエリアを出入りするルーティング アップデートをフィルタリングするためにOSPFv2 で使用されるプレフィックス リストの属性を示します。

EIGRP	OSPFv2	ルートマップとプレフィックスのリスト
コンテキストごとに1つのインスタンスがサポートされます。	コンテキストごとに2つのインスタンスがサポートされます。	該当なし
システム コンテキストでディセーブルになっています。		該当なし
2 つのコンテキストが同じまたは異なる自律システム番号を使用できます。	2 つのコンテキストが同じまたは異なるエリア ID を使用できます。	該当なし
2 つのコンテキストの共有インターフェイスでは、複数の EIGRP のインスタンスを実行できます。	2 つのコンテキストの共有インターフェイスでは、複数の OSPF のインスタンスを実行できます。	該当なし
共有インターフェイス間の EIGRP インスタンスの相互作用がサポートされます。	共有インターフェイス間の OSPFv2 インスタンスの相互作用がサポートされます。	該当なし
シングル モードで使用可能なすべての CLI はマルチ コンテキスト モードでも使用できます。		
各 CLI は使用されているコンテキストでだけ機能します。		

ルートのリソース管理

routes というリソース クラスは、コンテキストに存在できるルーティング テーブル エントリの最大数を指定します。これは、別のコンテキストの使用可能なルーティング テーブル エントリに影響を与える1つのコンテキストの問題を解決し、コンテキストあたりの最大ルート エントリのより詳細な制御を提供します。

明確なシステム制限がないため、このリソース制限には絶対値のみを指定できます。割合制限は使用できません。また、コンテキストあたりの上限および下限がないため、デフォルト クラ

スは変更されません。コンテキストのスタティックまたはダイナミック ルーティング プロトコル（接続、スタティック、OSPF、EIGRP、および RIP）のいずれかに新しいルートを追加し、そのコンテキストのリソース制限を超えた場合、ルートの追加は失敗し、syslog メッセージが生成されます。

管理トラフィック用ルーティングテーブル

標準的なセキュリティ対策として、多くの場合、（デバイスからの）管理トラフィックをデータトラフィックから分離する必要があります。この分離を実現するために、ASA デバイスは管理専用トラフィックとデータトラフィックに個別のルーティングテーブルを使用します。個別のルーティングテーブルを使用することで、データと管理用に別のデフォルトルートを作成できます。

各ルーティングテーブルのトラフィックのタイプ

デバイス間トラフィックでは、常にデータルーティングテーブルが使用されます。

デバイス発信トラフィックでは、タイプに応じて、デフォルトで管理専用ルーティングテーブルまたはデータルーティングテーブルが使用されます。デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

- 管理専用テーブルのデバイス発信トラフィックには、HTTP、SCP、TFTP、**copy** コマンド、スマートライセンス、Smart Call Home、**trustpoint**、**trustpool** などを使用してリモートファイルを開く機能が含まれています。
- データテーブルのデバイス発信トラフィックには、ping、DNS、DHCP などの他のすべての機能が含まれます。

管理専用ルーティングテーブルに含まれるインターフェイス

管理専用インターフェイスには、すべての管理 x/x インターフェイス、および管理専用として設定したすべてのインターフェイスが含まれています。

他のルーティングテーブルへのフォールバック

デフォルトのルーティングテーブルで一致が見つからなかった場合は、他のルーティングテーブルがチェックされます。

デフォルト以外のルーティングテーブルの使用

デフォルトのルーティングテーブルにないインターフェイスに移動するために、ボックス内のトラフィックを必要とするとき、場合によっては、他のテーブルへのフォールバックに頼るのではなく、インターフェイスを設定するときにそのインターフェイスを指定する必要があります。ASA は、指定されたインターフェイスのルートのみをチェックします。たとえば、管理専用インターフェイスから ping を送信する必要がある場合は、ping 機能でインターフェイスを指定します。他方、データルーティングテーブルにデフォルトルートがある場合は、デフォルトルートに一致し、管理ルーティングテーブルにフォールバックすることは決してありません。

ダイナミック ルーティング

管理専用ルーティングテーブルは、データ インターフェイス ルーティング テーブルから分離したダイナミックルーティングをサポートします。ダイナミック ルーティング プロセスは管理専用インターフェイスまたはデータ インターフェイスで実行されなければなりません。両方のタイプを混在させることはできません。分離した管理ルーティングテーブルが含まれていない以前のリリースからアップグレードする際、データインターフェイスと管理インターフェイスが混在し、同じダイナミック ルーティング プロセスを使用している場合、管理インターフェイスは破棄されます。

VPN 要件の管理アクセス機能

VPN を使用している際に ASA で参加したインターフェイス以外のインターフェイスに管理アクセスを許可する管理アクセス機能を設定した場合、分離した管理およびデータ ルーティング テーブルに関するルーティングの配慮のために、VPN 終端インターフェイスと管理アクセスインターフェイスは同じタイプである必要があります。両方とも管理専用インターフェイスまたは通常のデータ インターフェイスである必要があります。

管理インターフェイスの識別

management-only で設定されたインターフェイスは、管理インターフェイスと見なされます。

次の設定では、GigabitEthernet0/0 と Management0/0 の両インターフェイスは、管理インターフェイスと見なされます。

```
a/admin(config-if)# show running-config int g0/0
!
interface GigabitEthernet0/0
 management-only
 nameif inside
 security-level 100
 ip address 10.10.10.123 255.255.255.0
 ipv6 address 123::123/64
a/admin(config-if)# show running-config int m0/0
!
interface Management0/0
 management-only
 nameif mgmt
 security-level 0
 ip address 10.106.167.118 255.255.255.0
a/admin(config-if)#
```

Equal-Cost Multipath（ECMP）ルーティング

ASA は、等コスト マルチパス（ECMP）ルーティングをサポートしています。

インターフェイスごとに最大 8 つの等コストのスタティックルートまたはダイナミックルートを設定できます。たとえば、次のように異なるゲートウェイを指定する外部インターフェイスで複数のデフォルト ルートを設定できます。

```
route outside 0 0 10.1.1.2
route outside 0 0 10.1.1.3
route outside 0 0 10.1.1.4
```

この場合、トラフィックは10.1.1.2、10.1.1.3、および10.1.1.4間の外部インターフェイスでロードバランシングされます。トラフィックは、送信元 IP アドレスと宛先 IP アドレス、着信インターフェイス、プロトコル、送信元ポートと宛先ポートをハッシュするアルゴリズムに基づいて、指定したゲートウェイ間に分配されます。

トラフィックゾーンを使用した複数のインターフェイス間の ECMP

インターフェイスのグループを含むようにトラフィックゾーンを設定する場合、各ゾーン内の最大 8 つのインターフェイス間に最大 8 つの等コストの静的または動的ルートを設定できます。たとえば、次のようにゾーン内の3つのインターフェイ間に複数のデフォルトルートを設定できます。

```
route outside1 0 0 10.1.1.2
route outside2 0 0 10.2.1.2
route outside3 0 0 10.3.1.2
```

同様に、ダイナミック ルーティング プロトコルは、等コストルートを自動的に設定できます。ASA は、より堅牢なロード バランシング メカニズムを使用して、インターフェイス間のトラフィックのロードバランシングを行います。

ルートが紛失した場合、 デバイスはフローをシームレスに別のルートに移動させます。

プロキシ ARP 要求のディセーブル化

あるホストから同じイーサネット ネットワーク上の別のデバイスに IP トラフィックを送信する場合、そのホストは送信先のデバイスの MAC アドレスを知る必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは IP アドレスの所有者を尋ねる ARP 要求を送信します。その IP アドレスを所有するデバイスは、自分が所有者であることを自分の MAC アドレスで返答します。

プロキシ ARP は、デバイスが ARP 要求に対してその IP アドレスを所有しているかどうかに関係なく自分のMACアドレスで応答するときに使用されます。NATを設定し、ASAインターフェイスと同じネットワーク上のマッピング アドレスを指定する場合、ASA でプロキシ ARP が使用されます。トラフィックがホストに到達できる唯一の方法は、ASA でプロキシ ARP が使用されている場合、MAC アドレスが宛先マッピング アドレスに割り当てられていると主張することです。

まれに、NAT アドレスに対してプロキシ ARP をディセーブルにすることが必要になります。

既存のネットワークと重なる VPN クライアントアドレス プールがある場合、ASA はデフォルトで、すべてのインターフェイス上でプロキシ ARP 要求を送信します。同じレイヤ 2 ドメイン上にもう 1 つインターフェイスがあると、そのインターフェイスは ARP 要求を検出し、自分の MAC アドレスで応答します。その結果、内部ホストへの VPN クライアントのリターン トラフィックは、その誤ったインターフェイスに送信され、破棄されます。この場合、プロキシ ARP 要求をそれらが不要なインターフェイスでディセーブルにする必要があります。

手順

プロキシ ARP 要求をディセーブルにします。

sysopt noproxyarp *interface*

例：

```
ciscoasa(config)# sysopt noproxyarp exampleinterface
```

ルーティング テーブルの表示

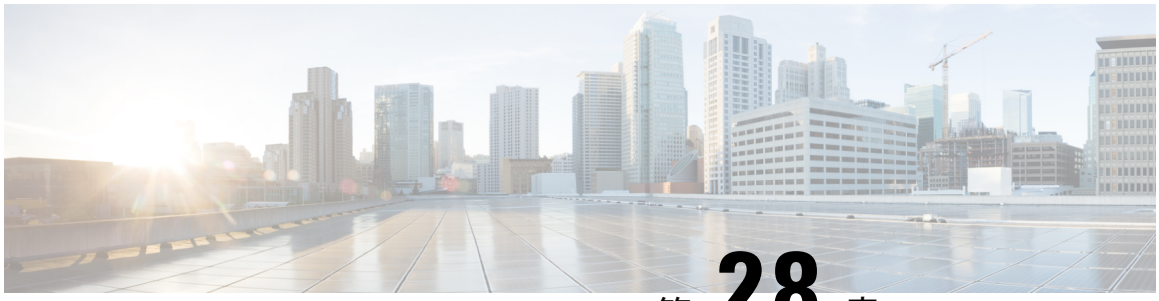
show route コマンドを使用してルーティング テーブル内のエントリを表示します。

```
ciscoasa# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

S    10.1.1.0 255.255.255.0 [3/0] via 10.86.194.1, outside
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

ルート概要の履歴

表 *36 :* ルート概要の履歴

機能名	プラットフォームリリース	機能情報
管理インターフェイス用のルーティングテーブル	9.5(1)	データ トラフィックから管理トラフィックを区別して分離するトラフィック専用のルーティング テーブルが追加されました。タそれぞれの専用ルーティング テーブルは IPv4 と Ipv6 の両方ASA の各コンテキストごとに作成されます。さらに、ASA の各トに対して、RIB と FIB の両方に 2 つの予備のルーティング テ加されます。 次のコマンドが導入されました。show route management-only、route management-only、show asp table route-management- only、management-only、clear ipv6 route management-only、copy interfactftp/ftp



第 28 章

スタティック ルートとデフォルト ルート

この章では、ASA でスタティック ルートとデフォルト ルートを設定する方法について説明します。

- スタティック ルートとデフォルト ルートについて （1139 ページ）
- スタティック ルートとデフォルト ルートのガイドライン （1142 ページ）
- デフォルト ルートおよびスタティック ルートの設定 （1143 ページ）
- スタティック ルートまたはデフォルト ルートのモニタリング （1148 ページ）
- スタティック ルートまたはデフォルト ルートの例 （1148 ページ）
- スタティック ルートおよびデフォルト ルートの履歴 （1149 ページ）

スタティック ルートとデフォルト ルートについて

接続されていないホストやネットワークにトラフィックをルーティングするには、スタティックルーティングまたはダイナミックルーティングを使用して、ホストまたはネットワークへのルートを定義する必要があります。通常は、少なくとも 1 つのスタティック ルート、つまり、他の方法でデフォルトのネットワーク ゲートウェイにルーティングされていない、すべてのトラフィック用のデフォルト ルート（通常、ネクスト ホップ ルータ）を設定する必要があります。

デフォルトルート

最も単純なオプションは、すべてのトラフィックをアップストリームルータに送信するようにデフォルトスタティックルートを設定して、トラフィックのルーティングをルータに任せることです。デフォルト ルートは、既知のルートもスタティック ルートも指定されていない IP パケットすべてを、ASAが送信するゲートウェイの IP アドレスを特定するルートです。デフォルト スタティック ルートとは、つまり宛先の IP アドレスとして 0.0.0.0/0（IPv4）または ::/0（IPv6）が指定されたスタティック ルートのことです。

デフォルト ルートを常に定義する必要があります。

ASAデバイスはデータトラフィックと管理トラフィックに個別のルーティングテーブルを使用するため、必要に応じて、データトラフィック用のデフォルトルートと管理トラフィック用の

別のデフォルトルートを設定できます。デバイス間トラフィックでは、タイプに応じてデフォルトで管理専用またはデータルーティングテーブルが使用されます。ただし、ルートが見つからない場合は、他のルーティングテーブルにフォールバックします。デフォルトルートは常にトラフィックに一致するため、他のルーティングテーブルへのフォールバックが妨げられます。この場合、インターフェイスがデフォルトのルーティングテーブルになければ、出力トラフィックに使用するインターフェイスを指定する必要があります。

スタティック ルート

次の場合は、スタティックルートを使用します。

- ネットワークでサポートされていないルータ検出プロトコルが使用されている。
- ネットワークが小規模でスタティック ルートを容易に管理できる。
- ルーティング プロトコルが関係するトラフィックまたは CPU のオーバーヘッドをなくす必要がある。
- デフォルトルートでは十分でない場合がある。デフォルトのゲートウェイでは宛先ネットワークに到達できない場合があるため、スタティックルートをさらに詳しく設定する必要があります。たとえば、デフォルトのゲートウェイが外部の場合、デフォルトルートは、ASA に直接接続されていない内部ネットワークにはまったくトラフィックを転送できません。
- ダイナミック ルーティング プロトコルをサポートしていない機能を使用している。

不要なトラフィックをドロップするための null0 インターフェイスへのルート

アクセスルールを使用すると、ヘッダーに含まれている情報に基づいてパケットをフィルタ処理することができます。null0 インターフェイスへのスタティック ルートは、アクセス ルールを補完するソリューションです。null0 ルートを使用して不要なトラフィックや望ましくないトラフィックを転送することで、トラフィックをドロップできます。

スタティック null0 ルートには、推奨パフォーマンス プロファイルが割り当てられます。また、スタティック null0 ルートを使用して、ルーティング ループを回避することもできます。BGP では、リモート トリガ型ブラック ホール ルーティングのためにスタティック null0 ルートを活用できます。

ルートのプライオリティ

- 特定の宛先が特定されたルートはデフォルト ルートより優先されます。
- 宛先が同じルートが複数存在する場合（スタティックまたはダイナミック）、ルートのアドミニストレーティブディスタンスによってプライオリティが決まります。スタティックルートは 1 に設定されるため、通常、それらが最もプライオリティの高いルートです。

- 宛先かつアドミニストレーティブ ディスタンスが同じスタティック ルートが複数存在する場合は、Equal-Cost Multipath（ECMP）ルーティング （1135 ページ）を参照してください。
- [トンネル化（Tunneled）] オプションを使用してトンネルから出力されるトラフィックの場合、このルートが他の設定済みルートまたは学習されたデフォルト ルートをすべてオーバーライドします。

トランスペアレント ファイアウォール モードおよびブリッジ グループのルート

ブリッジ グループ メンバー インターフェイスを通じて直接には接続されていないネットワークに向かう ASA で発信されるトラフィックの場合、ASA がどのブリッジ グループ メンバー インターフェイスからトラフィックを送信するかを認識するように、デフォルト ルートまたはスタティック ルートを設定する必要があります。ASA で発信されるトラフィックには、syslog サーバーまたは SNMP サーバーへの通信が含まれることもあります。1 つのデフォルト ルートで到達できないサーバーがある場合、スタティック ルートを設定する必要があります。トランスペアレント モードの場合、ゲートウェイ インターフェイスに BVI を指定できません。メンバー インターフェイスのみが使用できます。ルーテッド モードのブリッジ グループの場合、スタティック ルートに BVI を指定する必要があります。メンバー インターフェイスを指定することはできません。詳細については、MAC アドレスとルート ルックアップ （238 ページ）を参照してください。

スタティック ルート トラッキング

スタティック ルートの問題の 1 つは、ルートがアップ状態なのかダウン状態なのかを判定する固有のメカニズムがないことです。スタティック ルートは、ネクスト ホップ ゲートウェイが使用できなくなった場合でも、ルーティング テーブルに保持されています。スタティック ルートは、ASA 上の関連付けられたインターフェイスがダウンした場合に限りルーティング テーブルから削除されます。

スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。たとえば、ISP ゲートウェイへのデフォルト ルートを定義し、かつ、プライマリ ISP が使用できなくなった場合に備えて、セカンダリ ISP へのバックアップ デフォルト ルートを定義できます。

ASA では、ASA が ICMP エコー要求を使用してモニタする宛先ネットワーク上でモニタリング対象スタティック ルートを関連付けることでスタティック ルート トラッキングを実装します。指定された時間内にエコー応答がない場合は、そのホストはダウンしていると見なされ、関連付けられたルートはルーティング テーブルから削除されます。削除されたルートに代わって、メトリックが高い追跡対象外のバックアップ ルートが使用されます。

モニタリング対象の選択時には、その対象がICMPエコー要求に応答できることを確認してください。対象には任意のネットワーク オブジェクトを選択できますが、次のものを使用することを検討する必要があります。

- ISP ゲートウェイ アドレス（デュアル ISP サポート用）
- ネクストホップ ゲートウェイアドレス（ゲートウェイの使用可能状況に懸念がある場合）
- ASA が通信を行う必要のある対象ネットワーク上のサーバー（syslog サーバーなど）
- 宛先ネットワーク上の永続的なネットワーク オブジェクト

（注） 夜間にシャットダウンする PC は適しません。

スタティック ルート トラッキングは、スタティックに定義されたルートや、DHCP または PPPoEを通じて取得したデフォルトルートに対して設定することができます。設定済みのルート トラッキングでは、複数のインターフェイス上の PPPoE クライアントだけを有効化することができます。

スタティックルートとデフォルトルートのガイドライン

ファイアウォール モードとブリッジ グループ

- トランスペアレントモードでは、スタティック ルートはブリッジ グループ メンバー インターフェイスをゲートウェイとして使用する必要があります。BVIを指定することはできません。
- ルーテッドモードでは、BVIをゲートウェイとして指定する必要があります。メンバーインターフェイスは指定できません。
- スタティック ルート トラッキングは、ブリッジ グループ メンバー インターフェイスまたは BVI ではサポートされません。

サポートされるネットワークアドレス

- IPv6 では、スタティック ルート トラッキングはサポートされません。
- ASA はクラス E ルーティングをサポートしていないため、クラス E ネットワークはスタティックルートでルーティングできません。

クラスタリングとマルチコンテキストモード

- クラスタリングでは、スタティック ルート トラッキングはコントロールノードでのみサポートされます。
- スタティックルートトラッキングはマルチコンテキストモードではサポートされません。

ASP および RIB ルートエントリ

デバイスにインストールされているすべてのルートとその距離は、ASP ルーティングテーブルにキャプチャされます。これは、すべての静的および動的ルーティングプロトコルに共通です。最適な距離のルートのみが RIB テーブルにキャプチャされます。

デフォルト ルートおよびスタティック ルートの設定

少なくとも 1 つのデフォルト ルートを設定する必要があります。また、スタティック ルートの設定が必要になる場合があります。このセクションでは、デフォルト ルートの設定、スタティック ルートの設定、スタティック ルートの追跡を行います。

デフォルト ルートの設定

デフォルト ルートは、宛先 IP アドレスが 0.0.0.0/0 のスタティック ルートです。この手順に従って手動で設定するか、DHCP サーバーや他のルーティング プロトコルから取得するかに関わらず、デフォルト ルートは必ず設定する必要があります。

始める前に

[Tunneled] オプションについては、次のガイドラインを参照してください。

- トンネル ルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path** コマンド）を有効にしないでください。この設定を行うと、セッションでエラーが発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。この設定を行うと、セッションでエラーが発生します。
- これらのインスペクション エンジンはトンネル ルートを無視するため、トンネル ルートで VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンを使用しないでください。
- tunneled オプションで複数のデフォルト ルートを定義することはできません。
- トンネル トラフィックの ECMP はサポートされません。
- トンネルルートは、通過トラフィックの VPN 終端をサポートしないブリッジグループではサポートされません。

手順

デフォルト ルートを追加します。

IPv4：

route*if_name* **0.0.0.0 0.0.0.0** *gateway_ip* [**distance**] [**tunneled**]

IPv6：

ipv6 route *if_name* **::/0** *gateway_ip* [**distance**] [**tunneled**]

例：

```
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 192.168.2.4
ciscoasa(config)# route inside 0.0.0.0 0.0.0.0 10.1.2.3 tunneled
ciscoasa(config)# ipv6 route inside ::/0 3FFE:1100:0:CC00::1
```

if_name は、特定のトラフィックの送信を行うインターフェイスです。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。 ブリッジ グループでルーテッド モードを使用する場合は、BVI 名を指定します。

distance 引数は、ルートのアドミニストレーティブ ディスタンス（1 ～ 254）です。値を指定しない場合、デフォルトは**1**です。アドミニストレーティブディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブ ディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

（注）
through-the-box トラフィックの場合、異なるメトリックを持つ個別のインターフェイス上で 2 つのデフォルトルートが設定されていると、大きい方のメトリックを持つインターフェイスから ASA への接続の確立には失敗しますが、小さい方のメトリックを持つインターフェイスから ASA への接続は予期したとおりに成功します。from-the-box トラフィックの場合、異なるメトリックを持つ個別のインターフェイス上で 2 つのデフォルトルートが設定されていると、着信接続に使用されたインターフェイスによっては、両方のインターフェイスが from-the-box トラフィックに使用されることがあります。

VPN トラフィックに非 VPN トラフィックとは別のデフォルト ルートを使用する必要がある場合は、**tunneled** キーワードを使用して VPN トラフィック用の別個のデフォルト ルートを定義できます。その場合、たとえば VPN 接続からの着信トラフィックは内部ネットワークに転送する一方、内部ネットワークからのトラフィックは外部に転送するといった設定を簡単に行うことができます。tunneled オプションを使用してデフォルト ルートを作成すると、ASA に着信するトンネルからのすべてのトラフィックは、学習したルートまたはスタティック ルートを使用してルーティングできない場合、このルートに送信されます。このオプションは、ブリッジ グループではサポートされません。

ヒント
宛先ネットワーク アドレスおよびマスクとして、**0.0.0.0 0.0.0.0** の代わりに **0 0** と入力できます。たとえば、**routeoutside 0 0 192.168.2.4** のように入力します。

スタティック ルートの設定

スタティック ルートは、特定の宛先ネットワークのトラフィックの送信先を定義します。

手順

スタティック ルートを追加します。

IPv4：

route *if_name dest_ip mask gateway_ip* [**distance**]

IPv6：

ipv6 route *if_name dest_ipv6_prefix/prefix_length gateway_ip* [**distance**]

例：

```
ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1
ciscoasa(config)# ipv6 route outside 2001:DB8:1::0/32 2001:DB8:0:CC00::1
```

if_name は、特定のトラフィックの送信を行うインターフェイスです。不要なトラフィックをドロップするには、**null0** インターフェイスを入力します。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。 ブリッジ グループでルーテッド モードを使用する場合は、BVI 名を指定します。

dest_ip 引数と *mask* または *dest_ipv6_prefix/prefix_length* 引数は宛先ネットワークの IP アドレスであり、*gateway_ip* 引数はネクスト ホップ ルータのアドレスです。スタティック ルートに指定するアドレスは、ASA に到達して NAT を実行する前のパケットにあるアドレスです。

distance 引数は、ルートのアドミニストレーティブ ディスタンスです。値を指定しない場合、デフォルトは **1** です。アドミニストレーティブ ディスタンスは、複数のルーティング プロトコル間でルートを比較するのに使用されるパラメータです。スタティック ルートのデフォルトのアドミニストレーティブ ディスタンスは 1 で、ダイナミック ルーティング プロトコルで検出されるルートより優先されますが、直接には接続されていないルートです。OSPF で検出されるルートのデフォルトのアドミニストレーティブ ディスタンスは 110 です。スタティック ルートとダイナミック ルートのアドミニストレーティブディスタンスが同じ場合、スタティック ルートが優先されます。接続されているルートは常に、スタティック ルートおよびダイナミックに検出されたルートのどちらよりも優先されます。

例

次に、同じゲートウェイに移動する 3 つのネットワークと、別のゲートウェイに移動するもう 1 つのネットワークの例を示します。

```
route outside 10.10.10.0 255.255.255.0 192.168.1.1
route outside 10.10.20.0 255.255.255.0 192.168.1.1
```

```
route outside 10.10.30.0 255.255.255.0 192.168.1.1
route inside 10.10.40.0 255.255.255.0 10.1.1.1
```

スタティック ルート トラッキングの設定

スタティック ルート トラッキングを設定するには、次の手順を実行します。

手順

ステップ 1 ネットワークに到達するために使用されるインターフェイス（1 の外に）のスタティック ルートを構成します：

```
ciscoasa(config)# route outside1 172.29.139.134 255.255.255.255 10.0.0.1
```

ステップ 2 モニタリング プロセスを次のように定義します。

sla monitor sla_id

例：

```
ciscoasa(config)# sla monitor 5
ciscoasa(config-sla-monitor)#
```

ステップ 3 モニタリング プロトコル、追跡対象ネットワークのターゲット ホスト、ネットワークに到達するときに経由するネットワークを指定します。

type echo protocol ipicmpechotarget_ip **interface** if_name

例：

```
ciscoasa(config-sla-monitor)# type echo protocol ipicmpecho 172.29.139.134 interface
outside1
ciscoasa(config-sla-monitor-echo)#
```

target_ip 引数は、トラッキング プロセスによって使用可能かどうかをモニターされるネットワーク オブジェクトの IP アドレスです。このオブジェクトが使用可能な場合、トラッキング プロセス ルートがルーティング テーブルにインストールされます。このオブジェクトが使用できない場合、トラッキング プロセスがルートを削除し、代わりにバックアップ ルートが使用されます。

ステップ 4 （オプション）モニタリング オプションを設定します。**frequency**、**num-packets**、**request-data-size**、**threshold**、**timeout**、**tos** の各コマンドについては、コマンド リファレンスを参照してください。

ステップ 5 モニタリング プロセスのスケジュールを設定します。

sla monitor schedule sla_id [**life** {**forever** | seconds}] [**start-time** {hh:mm [:ss] [month day | day month] | **pending** | **now** | **after** hh:mm:ss}] [**ageout** seconds] [**recurring**]

例：

```
ciscoasa(config)# sla monitor schedule 5 life forever start-time now
```

通常、モニタリング スケジュールには **sla monitor schedule** *sla_id* **life forever start-time now** コマンドを使用し、モニタリング コンフィギュレーションでテスト頻度を決定できるようにします。

ただし、このモニタリング プロセスを将来開始するようにしたり、指定した時刻だけに実行されるようにスケジュールを設定したりできます。

ステップ 6 追跡するスタティック ルートを SLA モニタリング プロセスに関連付けます。

track track_id **rtr** sla_id **reachability**

例：

```
ciscoasa(config)# track 6 rtr 5 reachability
```

track_id 引数は、このコマンドで割り当てるトラッキング番号です。*sla_id* 引数は SLA プロセスの ID 番号です。

ステップ 7 次のルート タイプのいずれかを追跡します。

- スタティック ルート：

  route if_name dest_ip mask gateway_ip [distance] **track** track_id

  例：

  ```
  ciscoasa(config)# route outside 10.10.10.0 255.255.255.0 192.168.1.1 track 6
  ```

  tunneled オプションは使用できません。

- DHCP から取得したデフォルト ルート：

  ```
  interface interface_id
    dhcp client route track track_id
    ip address dhcp setroute
  ```

- PPPoE から取得したデフォルト ルート：

  ```
  interface interface_id
    pppoe client route track track_id
    ip address pppoe setroute
  ```

ステップ 8 追跡対象外のバックアップ ルートを作成します。

バックアップ ルートは、追跡されたルートと同じ宛先へのスタティック ルートですが、異なるインターフェイスまたはゲートウェイを経由します。このルートは、追跡されたルートより長いアドミニストレーティブ ディスタンス（メトリック）に割り当てる必要があります。

スタティック ルートまたはデフォルト ルートのモニタリング

- **show route**

  ルーティング テーブルを表示します。

スタティック ルートまたはデフォルト ルートの例

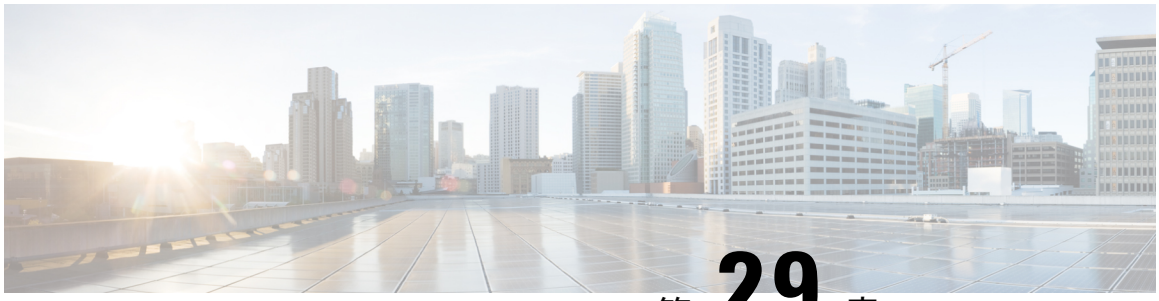
次の例は、スタティック ルートの作成方法を示します。スタティック ルートは、宛先が 10.1.1.0/24 のトラフィックすべてを内部インターフェイスに接続されているルータ（10.1.2.45）に送信します。また、dmz インターフェイスで 3 つの異なるゲートウェイにトラフィックを誘導する 3 つの等コスト スタティック ルートを定義し、トンネル トラフィックのデフォルト ルートと通常のトラフィックのデフォルト ルートを追加します。

```
route inside 10.1.1.0 255.255.255.0 10.1.2.45
route dmz 10.10.10.0 255.255.255.0 192.168.2.1
route dmz 10.10.10.0 255.255.255.0 192.168.2.2
route dmz 10.10.10.0 255.255.255.0 192.168.2.3
route outside 0 0 209.165.201.1
route inside 0 0 10.1.2.45 tunneled
```

スタティック ルートおよびデフォルト ルートの履歴

表 *37:* スタティック ルートおよびデフォルト ルートの機能履歴

機能名	プラットフォーム リリース	機能情報
スタティック ルート トラッキング	7.2(1)	スタティック ルート トラッキング機能には、スタティック ルートの使用可能状況を追跡し、プライマリ ルートがダウンした場合のバックアップ ルートをインストールするための方式が用意されています。 **clear configure sla**、**frequency, num-packets**、**request-data-size**、**show sla monitor**、**show running-config sla**、**sla monitor**、**sla monitor schedule, threshold**、**timeout**、**tos**、**track rtr** の各コマンドが導入されました。
スタティック null0 ルートによるトラフィックのドロップ	9.2(1)	トラフィックを null0 インターフェイスへ送信すると、指定したネットワーク宛のパケットはドロップします。この機能は、BGP の Remotely Triggered Black Hole (RTBH) の設定に役立ちます。 **route** コマンドが変更されました。



第 29 章

ポリシーベースルーティング

この章では、ポリシーベースルーティング（PBR）をサポートするように ASA を設定する方法について説明します。この項では、ポリシーベース ルーティング、PBR のガイドライン PBR の設定について説明します。

- ポリシーベース ルーティングについて （1151 ページ）
- ポリシーベース ルーティングのガイドライン （1154 ページ）
- パスモニタリング （1156 ページ）
- ポリシーベース ルーティングの設定 （1157 ページ）
- ポリシーベース ルーティングの例 （1162 ページ）
- ポリシーベース ルーティングの履歴 （1172 ページ）

ポリシーベース ルーティングについて

従来のルーティングは宛先ベースであり、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティング システムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベース ルーティング（PBR）では、宛先ネットワークではなく条件に基づいてルーティングを定義できます。PBR では、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル、またはこれらの組み合わせに基づいてトラフィックをルーティングできます。

ポリシーベース ルーティング：

- 区別したトラフィックに Quality of Service（QoS）を提供できます。
- 低帯域幅、低コストの永続パスと、高帯域幅、高コストのスイッチドパスに、インタラクティブ トラフィックとバッチ トラフィックを分散できます。
- インターネット サービス プロバイダーやその他の組織が、さまざまなユーザー セットから発信されるトラフィックを、適切に定義されたインターネット接続を経由してルーティングできます。

ポリシーベース ルーティングには、ネットワーク エッジでトラフィックを分類およびマークし、ネットワーク全体で PBR を使用してマークしたトラフィックを特定のパスに沿ってルーティングすることで、QoS を実装する機能があります。これにより、宛先が同じ場合でも、異

なる送信元から送信されるパケットを別のネットワークにルーティングすることができます。これは、複数のプライベート ネットワークを相互接続する場合に役立ちます。

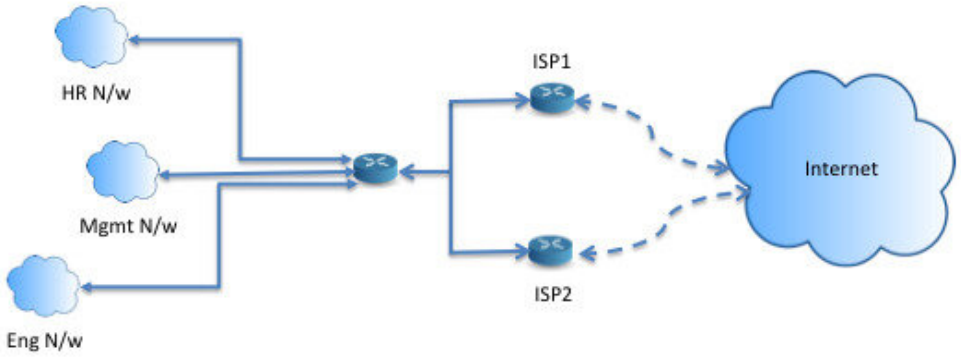
ポリシーベース ルーティングを使用する理由

ロケーション間に 2 つのリンクが導入されている企業を例に説明します。1 つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう 1 つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティング プロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅/遅延の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベース ルーティングの用途のいくつかを以下に示します。

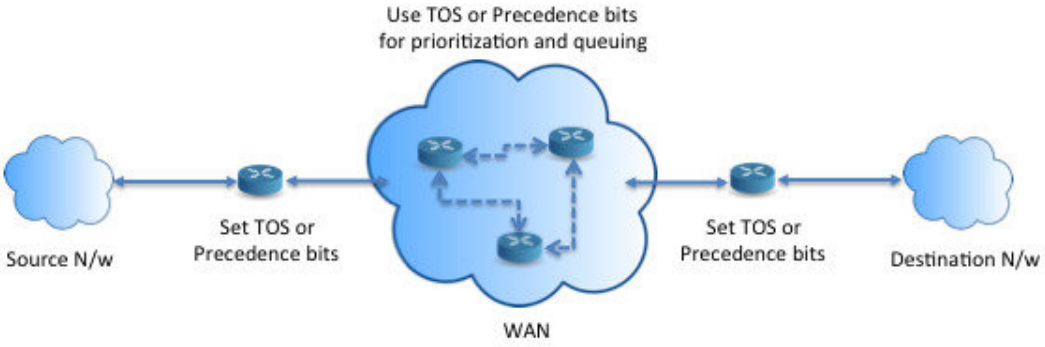
同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックは ISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベース ルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



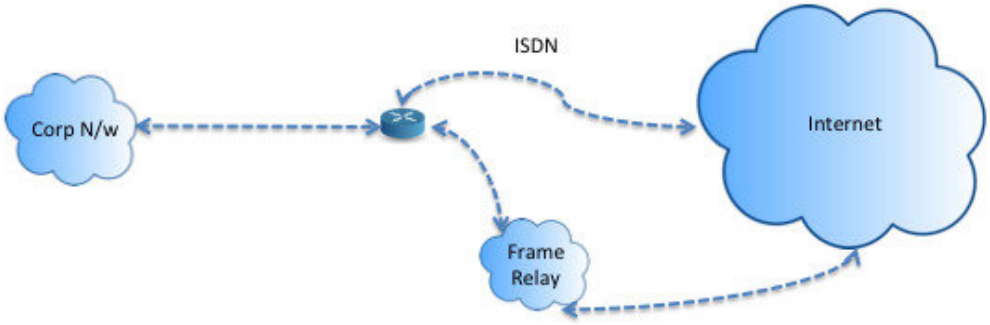
QoS

ネットワーク管理者は、ポリシーベース ルーティングでパケットにタグを付けることにより、ネットワーク トラフィックをネットワーク境界でさまざまなサービス クラスのために分類し、プライオリティ、カスタム、または重み付け均等化のキューイングを使用してそれらのサービス クラスをネットワークのコアに実装できます（下の図を参照）。この設定では、バックボーン ネットワークのコアの各 WAN インターフェイスでトラフィックを明示的に分類する必要がなくなるため、ネットワーク パフォーマンスが向上します。



コスト節約

組織は、特定のアクティビティに関連付けられている一括トラフィックを転送して、帯域幅が高い高コストリンクの使用を短時間にし、さらにここに示すようにトポロジを定義することで帯域幅が低い低コスト リンク上の基本的な接続を継続できます。



ロード シェアリング

ECMP ロード バランシングによって提供されるダイナミックなロード シェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR netto からのトラフィックと ISP2 を経由するエンジニアリング ネットワークからのトラフィックをロード シェアするようにポリシーベース ルーティングを設定できます。

PBR の実装

ASA は、ACL を使用してトラフィックを照合してから、トラフィックのルーティングアクションを実行します。具体的には、照合のために ACL を指定するルート マップを設定し、次にそのトラフィックに対して 1 つ以上のアクションを指定します。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルートマップを関連付けます。

（注） 設定に進む前に、特に NAT と VPN が使用されている場合に、非対称ルーティングによって引き起こされる予期しない動作を回避するために、各セッションの入力トラフィックと出力トラフィックが同じ ISP 側のインターフェイスを通過することを確認してください。

ポリシーベース ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フロー別のルーティング

ASA はフロー別にルーティングを実行するため、ポリシー ルーティングは最初のパケットに適用され、その結果決定したルーティングが、そのパケットに対して作成されたフローに格納されます。同一接続に属する後続のパケットはすべてこのフローと照合され、適切にルーティングされます。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベース ルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワード レグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用され、NAT が出力インターフェイスを選択している場合には PBR がトリガーされないことに注意してください。

初期トラフィックに適用されない PBR ポリシー

（注） 初期接続とは、送信元と宛先の間で必要になるハンドシェイクが完了していない状態を指します。

新しい内部インターフェイスが追加され、一意のアドレスプールを使用して新しい VPN ポリシーが作成されると、新しいクライアントプールの送信元に一致する外部インターフェイスに PBR が適用されます。そのため、PBR はクライアントからのトラフィックを新しいインターフェイスの次のホップに送信します。ただし、PBR は、クライアントへの新しい内部インターフェイスルートとの接続をまだ確立していないホストからのリターントラフィックには関与しません。したがって、有効なルートがないため、ホストから VPN クライアントへのリターントラフィック、具体的には VPN クライアントの応答はドロップされます。内部インターフェイスにおいて、よりメトリックの高い重み付けされたスタティックルートを設定する必要があります。

クラスタ

- クラスタリングがサポートされています。
- クラスタのシナリオでは、スタティック ルートまたはダイナミック ルートがない場合、ip-verify-reverse パスを有効にした非対称トラフィックはドロップされる可能性があります。したがって、ip-verify-reverse パスを無効にすることが推奨されます。

IPv6 のサポート

IPv6 はサポートされます。

パスモニタリングのガイドライン

インターフェイスでパスモニタリングを設定するうえでのガイドラインは、次のとおりです。

- インターフェイスにはインターフェイス名が必要です。
- 管理専用インターフェイスには、パスモニタリングを設定できません。パスモニタリングを設定するには、[このインターフェイスを管理専用にする（Dedicate this interface to management only）] チェックボックスをオフにする必要があります。
- パスモニタリングは、トランスペアレントまたはマルチコンテキスト システム モードのデバイスではサポートされません。
- 自動モニタリングタイプ（auto、auto4、および auto6）は、トンネルインターフェイスではサポートされません。
- パスモニタリングは、次のインターフェイスには設定できません。
  - BVI
  - ループバック
  - DVTI

その他のガイドライン

- ルート マップ関連の既存のすべての設定の制限事項が引き続き適用されます。
- ポリシーベースルーティングには、一致ポリシーリストを含むルートマップを使用しないでください。一致ポリシーリストは BGP にのみ使用されます。
- Unicast Reverse Path Forwarding（uRPF）は、インターフェイスで受信したパケットの送信元 IP アドレスを、PBR ルートマップではなく、ルーティングテーブルと照合して検証します。uRPF が有効になっている場合、PBR を介してインターフェイスで受信されたパケットは、特定のルートエントリがない場合と同じようにドロップされます。したがって、PBR を使用する場合は、uRPF を無効にしてください。

パスモニタリング

パスモニタリングをインターフェイスに設定すると、ラウンドトリップ時間（RTT）、ジッター、平均オピニオン評点（MOS）、インターフェイスごとのパケット損失などのメトリックが得られます。これらのメトリックは、PBR トラフィックをルーティングするための最適なパスを決定するために使用されます。

インターフェイスのメトリックは、インターフェイスのデフォルトゲートウェイまたは指定されたリモートピアへの ICMP プローブメッセージを使用して動的に収集されます。

デフォルトのモニタリングタイマー

メトリックの収集とモニタリングには、次のタイマーが使用されます。

- インターフェイスモニタの平均間隔は 30 秒です。この間隔は、プローブで平均する頻度を示します。
- インターフェイスモニタの更新間隔は 30 秒です。この間隔は、収集された値の平均が計算され、PBR が最適なルーティングパスを決定するために使用できるようになる頻度を示します。
- ICMP によるインターフェースモニタのプローブ間隔は 1 秒です。この間隔は、ICMP ping が送信される頻度を示します。
- HTTP によるアプリケーションモニタのプローブ間隔は 10 秒です。この間隔は、HTTP ping が送信される頻度を示します。パスモニタリングは、平均メトリックを計算するために HTTP ping の最新の 30 サンプルを使用します。

（注） これらのタイマーの間隔は設定または変更できません。

通常、PBR では、トラフィックは、出力インターフェイスに設定された優先順位値（インターフェイスコスト）に基づいて、出力インターフェイスを介して転送されます。Management Center のバージョン 7.2 以降では、PBR は IP ベースのパスモニタリングを使用して、出力インターフェイスのパフォーマンスメトリック（RTT、ジッター、パケット損失、MOS）を収集します。PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。

パスモニタリングは、ダイナミックメトリックを使用した場合のみ、RTT、ジッター、packet-lost、または MOS 変更がインターフェイスに設定されている場合にのみ機能します。パスモニタリングは、静的メトリック、つまりインターフェイスコスト（インターフェイスで設定されたコスト）では機能しません。

インターフェイスのパスモニタリングを有効にし、モニタリングタイプを設定する必要があります。[PBRポリシー（PBR policy）] ページでは、パスの決定に必要なメトリックを指定できます。ポリシーベース ルーティングの設定 （1157 ページ） を参照してください。

パスモニタリングの設定

ネットワーク サービス グループに基づいてポリシーベースルーティングを実行するようにパスモニタリングを設定できます。NSGなしでパスモニタリングを使用するには、**[インターフェイス（Interface）]>[編集（Edit）]**ページに移動して、パスモニタリングのタイプを指定できます。「ポリシーベースルーティングの設定」を参照してください。

手順

ステップ 1 ASDM で、**[設定（Configuration）]** > **[デバイスの設定（Device Setup）]** > **[インターフェイスの設定（Interface Settings）]** > **[パスモニタリング（Path Monitoring）]**の順に選択します。

ステップ 2 [インターフェイス（Interface）] ドロップダウンからインターフェイスを選択します。

ステップ 3 [利用可能なネットワークサービスグループ（Available Network Service Groups）] ボックスでネットワーク サービス グループ（NSG）を選択します。複数の NSG を選択するには、制御キーを使用して必要な NSG をクリックします。

ステップ 4 [追加（Add）] をクリックして、ネットワーク サービス グループを追加します。

ステップ 5 [適用（Apply）] をクリックします。

ステップ 6 設定を削除するには、[追加されたネットワークサービスグループ（Added Network Service Groups）] ボックスから NSG を選択し、[削除（Remove）]、[適用（Apply）] の順にクリックします。

ポリシーベース ルーティングの設定

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と permit 句または deny 句が付加されます。各ルート マップ文には、match コマンドと set コマンドが含まれています。match コマンドは、パケット データに適用される一致基準を示します。set コマンドは、パケットに対して実行されるアクションを示します。

- IPv4 と IPv6 の両方の match/set 句でルート マップを設定した場合、または IPv4 および IPv6 トラフィックを照合する統合 ACL を使用した場合、宛先 IP のバージョンに基づいた set アクションが適用されます。
- 複数のネクストホップまたはインターフェイスを set アクションとして設定すると、使用できる有効なオプションが見つかるまですべてのオプションが順に評価されます。設定された複数のオプション間のロード バランシングは実行されません。
- verify-availability オプションは、マルチ コンテキスト モードではサポートされません。

手順

ステップ 1 スタンドアロンまたは拡張アクセス リストを定義します。

access-list *name* **standard** {**permit** | **deny**} {**any4** | **host** *ip_address* | *ip_address mask*}

access-list *name* **extended** {**permit** | **deny**} *protocol source_and_destination_arguments*

例：

```
ciscoasa(config)# access-list testacl extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

標準 ACL を使用する場合、照合は宛先アドレスに対してのみ行われます。拡張 ACL を使用する場合、送信元、宛先、またはその両方に対して照合を行えます。

拡張 ACL では、IPv4、IPv6、アイデンティティ ファイアウォール、または Cisco TrustSec パラメータを指定できます。ネットワーク サービス オブジェクトを含めることもできます。完全な構文については、ASA コマンド リファレンスを参照してください。

ステップ 2 ルート マップ エントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map testmap permit 12
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序が ASA で使用されます。

ACL には、固有の permit および deny 文も含まれます。ルート マップと ACL が permit/permit で一致する場合、ポリシーベース ルーティング処理が続行されます。permit/deny で一致する場合、このルート マップでの処理が終了し、別のルート マップがチェックされます。それでも結果が permit/deny であれば、通常のルーティング テーブルが使用されます。deny/deny で一致する場合、ポリシーベース ルーティング処理が続行されます。

（注）
permit または deny アクションとシーケンス番号なしでルートマップを設定した場合、このマップはデフォルトでアクションが permit で、シーケンス番号が 10 であると見なされます。アクションとシーケンス番号を指定しない場合、ルートマップはデフォルト値で設定されている場合でも、不完全な CLI コマンドに関する警告メッセージが表示されます。

ステップ 3 アクセス リストを使用して適用される一致基準を定義します。

match ip address *access-list_name* [*access-list_name...*]

例：

```
ciscoasa(config-route-map)# match ip address testacl
```

（注）
アクセスリストに非アクティブなルールが含まれていないことを確認します。非アクティブなルールを持つ一致 ACL を PBR に設定することはできません。

ステップ 4 1 つ以上の set アクションを設定します。

- ネクストホップ アドレスを設定します。

  set {ip | ipv6} next-hop *ipv4_or_ipv6_address*

  複数のネクストホップ IP アドレスを設定できます。その場合、ルーティングできる有効なネクスト ホップ IP アドレスが見つかるまで、それらのアドレスが指定された順で評価されます。設定済みのネクストホップは、直接接続する必要があります。そうでなければ、set アクションが適用されません。

- デフォルトのネクストホップ アドレスを設定します。

  set {ip | ipv6} default next-hop *ipv4_or_ipv6_address*

  一致するトラフィックに対する通常のルート ルックアップが失敗すると、ASA はここで指定されたネクスト ホップ IP アドレスを使用してトラフィックを転送します。

- 再帰ネクスト ホップ IPv4 アドレスを設定します。

  set ip next-hop recursive *ip_address*

  set ip next-hop と **set ip default next-hop** はどちらも、ネクストホップが直接接続されたサブネット上に存在している必要があります。**set ip next-hop recursive** では、ネクストホップ アドレスが直接接続されている必要はありません。代わりにネクストホップ アドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティング パスに従って、そのルート エントリで使用されているネクストホップに転送されます。

- ルート マップの次の IPv4 ホップが使用できるかどうかを確認します。

  set ip next-hop verify-availability *next-hop-address sequence_number* **track** *object*

  ネクスト ホップの到達可能性を確認するには、SLA モニター追跡オブジェクトを設定できます。複数のネクストホップの可用性を確認するために、複数の **set ip next-hop verify-availability** コマンドを異なるシーケンス番号と異なるトラッキング オブジェクトで設定できます。

- パケットの出力インターフェイスを設定します。

  set interface *interface_name*

  または

  set interface null0

  このコマンドにより、一致するトラフィックを転送するために使用するインターフェイスが設定されます。複数のインターフェイスを設定できます。その場合、有効なインター

フェイスが見つかるまで、それらのインターフェイスが指定された順で評価されます。**null0** を指定すると、ルートマップと一致するすべてのトラフィックがドロップされます。指定されたインターフェイス（静的または動的のいずれか）経由でルーティングできる宛先のルートが存在している必要があります。

- インターフェイスのコストに基づいて出力インターフェイスを設定します。

  set adaptive-interface cost *interface_list*

  出力インターフェイスは、スペースで区切られたインターフェイスのリストから選択されます。インターフェイスのコストが同じである場合、アクティブ-アクティブ設定であり、出力インターフェイスでパケットがロードバランシング（ラウンドロビン）されます。コストが異なる場合、コストが最も低いインターフェイスが選択されます。インターフェイスは、アップしている場合にのみ考慮されます。次に例を示します。

  ```
  set adaptive-interface cost output1 output2
  ```

- デフォルトのインターフェイスを null0 に設定します。

  set default interface null0

  通常のルート ルックアップが失敗すると、ASA はトラフィックを null0 に転送し、トラフィックがドロップされます。

- IP ヘッダーに Don't Fragment（DF）ビット値を設定します。

  set ip df {0|1}

- パケットに Differentiated Services Code Point（DSCP）または IP プレシデンスの値を設定することによって、IP トラフィックを分類します。

  set {ip | ipv6} dscp *new_dscp*

（注）
複数の set アクションが設定されている場合、ASA は、これらを次の順序で評価します。 **set ip next-hop verify-availability; set ip next-hop**; **set ip next-hop recursive**; **set interface; set adaptive-interface cost**; **set ip default next-hop**; **set default interface**

ステップ 5 インターフェイスを設定して、インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
```

ステップ 6 ルートマップの基準として **set adaptive-interface cost** を使用する場合は、インターフェイスでコストを設定します。

policy-route cost *value*

値は 1 ー 65535 です。デフォルトは 0 です。この値は、コマンドの **no** バージョンを使用してリセットできます。値が小さいほど、プライオリティが高くなります。たとえば、1 は 2 よりも優先されます。

policy-route コストを設定し、ルートマップで **set adaptive-interface cost** コマンドを使用すると、出力トラフィックは、同じインターフェイスコストを持つ任意の選択されたインターフェイス間（アップしていると仮定）でラウンドロビン ロード バランシングされます。コストが異なる場合、コストの高いインターフェイスが、最もコストの低いインターフェイスへのバックアップとして使用されます。

たとえば、2 つの WAN リンクに同じコストを設定すると、これらのリンク間でトラフィックをロードバランシングして、パフォーマンスを向上させることができます。ただし、一方の WAN リンクの帯域幅が他方よりも高い場合は、高帯域幅リンクのコストを 1 に設定し、低帯域幅リンクを 2 に設定して、高帯域幅リンクがダウンしている場合にのみ低帯域幅リンクを使用します。

ステップ 7 インターフェイスのピアのモニタリングタイプを設定して、柔軟なメトリックを収集できます。

policy-route path-monitoring {**IPv4** | **IPv6** | **auto** | **auto4** | **auto6**}

それぞれの説明は次のとおりです。

- [自動（auto）]：自動 IPv4 と同じように、インターフェイスの IPv4 デフォルトゲートウェイ（存在する場合）に ICMP プローブを送信します。それ以外の場合は、自動 IPv6 と同じように、インターフェイスの IPv6 デフォルトゲートウェイに送信します。
- [ipv4]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。
- [ipv6]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。
- [auto4]：インターフェイスの IPv4 デフォルトゲートウェイに ICMP プローブを送信します。
- [auto6]：インターフェイスの IPv6 デフォルトゲートウェイに ICMP プローブを送信します。

例：

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost             set interface cost
  path-monitoring  Keyword for path monitoring
  route-map        Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config
```

```
ciscoasa(config-if)# policy-route path-monitoring auto
```

インターフェイスでパスモニタリング設定をクリアするには、**clear path-monitoring** コマンドを使用します。

例：

```
clear path-montoring outside1
```

ステップ 8 ポリシーベース ルーティングを through-the-box トラフィック用に設定します。

`policy-route route-map` *route_map_name*

例：

```
ciscoasa(config-if)# policy-route route-map testmap
```

既存のポリシーベース ルーティング マップを削除するには、単にこのコマンドの **no** 形式を入力します。

例：

```
ciscoasa(config-if)# no policy-route route-map testmap
```

ポリシーベース ルーティングの例

以下のセクションでは、ルートマップの設定、ポリシーベース ルーティング（PBR）の例と、PBR の具体的な動作例を示します。

ルート マップ コンフィギュレーションの例

次の例では、アクションとシーケンスが指定されないため、暗黙的に permit のアクションと 10 のシーケンス番号が想定されます。

```
ciscoasa(config)# route-map testmap
```

次の例では、match 基準が指定されないため、暗黙的に match は「any」と見なされます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

この例では、<acl> と一致するすべてのトラフィックが、ポリシー ルーティングされ、外部インターフェイス経由で転送されます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
ciscoasa(config-route-map)# set interface outside
```

次の例では、インターフェイスまたはネクストホップのアクションが設定されていないため、<acl>に一致するすべてのトラフィックのdf bitおよびdscpフィールドがコンフィギュレーションに従って変更され、通常のルーティングを使用して転送されます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

次の例では、<acl_1> に一致するすべてのトラフィックがネクストホップ 1.1.1.10 を使用して転送され、<acl_2> に一致するすべてのトラフィックがネクストホップ 2.1.1.10 を使用して転送され、残りのトラフィックはドロップされます。「match」基準がない場合、暗黙的にmatchは「any」と見なされます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

次の例では、ルートマップの評価は、（i）route-mapアクションpermitとaclアクションpermitがsetアクションを適用する、（ii）route-mapアクションdenyとaclアクションpermitが通常のルート ルックアップにスキップする、（iii）permit/denyのroute-mapアクションとaclアクションdenyが次のroute-mapエントリを続行するといったものになります。次のroute-mapエントリを使用できない場合は、通常のルート ルックアップにフォールバックします。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
ciscoasa(config-route-map)# set interface outside
```

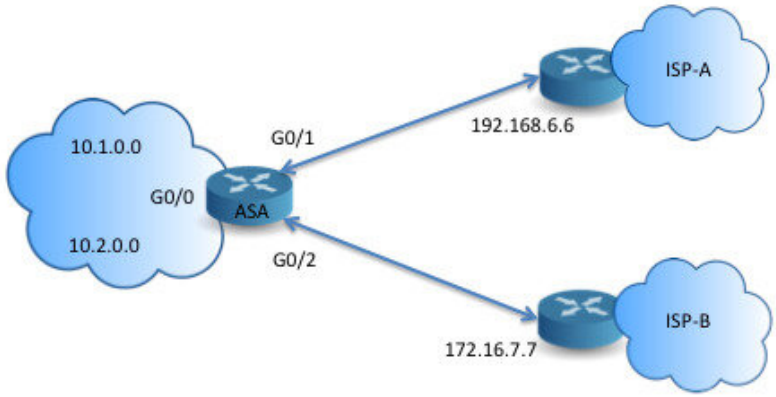
次の例では、複数のsetアクションを設定すると、それらのアクションが上記の順序で評価されます。setアクションのすべてのオプションが評価され、それらを適用できない場合にのみ、次のsetアクションが考慮されます。この順序設定により、すぐに使用可能な最短のネクストホップが最初に試行され、その後、次のすぐに使用可能な最短のネクストホップが試行される、といったようになります。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
```

```
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

PBR の設定例

ここでは、次のシナリオ用に PBR を設定するために必要な設定の完全なセットについて説明します。



まず、インターフェイスを設定する必要があります。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-1
ciscoasa(config-if)# ip address 192.168.6.5 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-2
ciscoasa(config-if)# ip address 172.16.7.6 255.255.255.0
```

次に、トラフィックを照合するためのアクセスリストを設定する必要があります。

```
ciscoasa(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
ciscoasa(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

必要な set アクションとともに、一致基準として上記のアクセスリストを指定することで、ルートマップを設定する必要があります。

```
ciscoasa(config)# route-map equal-access permit 10
```

```
ciscoasa(config-route-map)# match ip address acl-1
ciscoasa(config-route-map)# set ip next-hop 192.168.6.6

ciscoasa(config)# route-map equal-access permit 20
ciscoasa(config-route-map)# match ip address acl-2
ciscoasa(config-route-map)# set ip next-hop 172.16.7.7

ciscoasa(config)# route-map equal-access permit 30
ciscoasa(config-route-map)# set ip interface Null0
```

ここで、このルート マップをインターフェイスに接続する必要があります。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map equal-access
```

ポリシー ルーティング設定を表示するには：

```
ciscoasa(config)# show policy-route
Interface                  Route map
GigabitEthernet0/0   equal-access
```

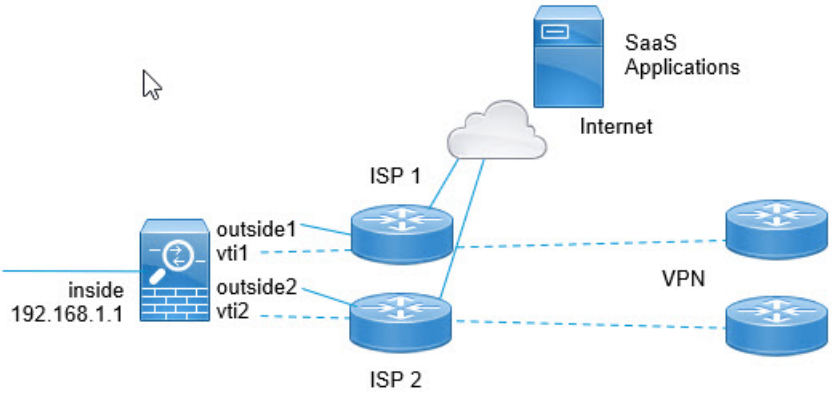
ソフトウェアデファインド WAN を使用したダイレクト インターネット アクセス

一般的な分散拠点ネットワークでは、サイト間 VPN を使用してブランチを企業のハブに接続します。すべての非ローカルトラフィックは、社内ネットワークに転送されます。社内ネットワークでは、必要に応じて内部サービスまたはインターネットに転送されます。

この設定により、企業のハブでボトルネックが発生します。一部のブランチトラフィックがGoogle検索やGmailなどのインターネットサービス向けである場合、インターネットに転送する前に企業ネットワークに転送する必要はありません。

ポリシーベースルーティングを使用すると、企業ネットワークのサービスを必要としないトラフィックに対して、ブランチから直接のインターネットアクセスを設定できます。したがって、インターネットへのトラフィックは企業のハブに送信されず、ハブは企業ネットワークの内部サービス宛てのトラフィックのみを処理する必要があります。この設定により、ネットワーク全体のパフォーマンスとスループットが向上します。

次に、2つの外部インターフェイスが異なるインターネット サービス プロバイダーに接続し、仮想トンネルインターフェイス（VTI）が企業ネットワークへのサイト間VPN接続を行う、次の設定の直接インターネットアクセスを設定する例を示します。この例では、選択した SaaS アプリケーション宛てのトラフィックをインターネットに転送し、企業ネットワークをバイパスする方法を示します。



始める前に

この例では、ブランチを企業ハブに接続するために、外部（WAN 側）インターフェイスで定義された仮想トンネルインターフェイス（VTI）を使用してサイト間 VPN がすでに定義されていて、正しく機能していることを前提としています。したがって、VTI インターフェイスにルーティングされるトラフィックは企業ネットワークに転送され、外部インターフェイスに直接ルーティングされるトラフィックはインターネットに転送されます。

また、DNS サーバ設定し、デバイスインターフェイスで DNS 解決を有効にしていることも前提としています。スヌーピングされるサーバを確認するには、**show dns trusted-source detail** コマンドを使用します。使用するサーバを制限する場合は、**no dns trusted-source** コマンドを使用して、選択したサーバのスヌーピングをオフにします。

手順

ステップ 1 ネットワーク サービス オブジェクトとグループを設定して、目的のトラフィックを定義します。

次の例では、Office365 と Webex を定義するオブジェクトを作成し、これらを含む SaaS_Applications オブジェクトグループを作成します。オブジェクトグループを作成する必要があります。アクセス コントロール エントリでオブジェクトを直接使用することはできません。

```
object network-service office365
    domain outlook.office365.com tcp eq 443
    domain onlineapps.live.com tcp eq 443
    domain skype.live.com tcp eq 443

object network-service webex
    domain webex.com tcp eq 443

object-group network-service SaaS_Applications
    network-service-member office365
    network-service-member webex
```

ステップ 2 目的のトラフィックと一致する拡張 ACL を作成します。

次の例では、内部ネットワークから SaaS アプリケーション オブジェクト グループへのトラフィックを照合します。

```
access-list DIA_traffic extended permit ip 192.168.1.0 255.255.255.0
object-group-network-service SaaS_Applications
```

ステップ 3 （任意）出力インターフェイスのコストを設定します。

output1 および output2 インターフェイスがすでに設定され、機能していると仮定すると、policy-route cost コマンドを追加するだけです。ラウンドロビン処理を使用して 2 つの出力 WAN リンク間でロードバランシングを行うようにシステムを設定する場合、この手順は任意です。ただし、アクティブ/バックアップ設定を作成する場合は、コストを設定する必要があります。この場合、ダウンしていない限り 1 つのリンクが使用されます。

次に、等コストのアクティブ/アクティブ設定の例を示します。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 1
```

次に、output1 が優先リンクで、output2 は output1 がダウンしている場合にのみ使用される例を示します。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

ステップ 4 拡張 ACL に一致するルートマップを作成し、それに応じてトラフィックを転送します。

次の例では、ACL を使用してトラフィックを照合し、適応インターフェイスのコストを使用してトラフィックを出力インターフェイスに転送します。

```
route-map mymap 10
  match ip address DIA_traffic
  set adaptive-interface cost outside1 outside2
```

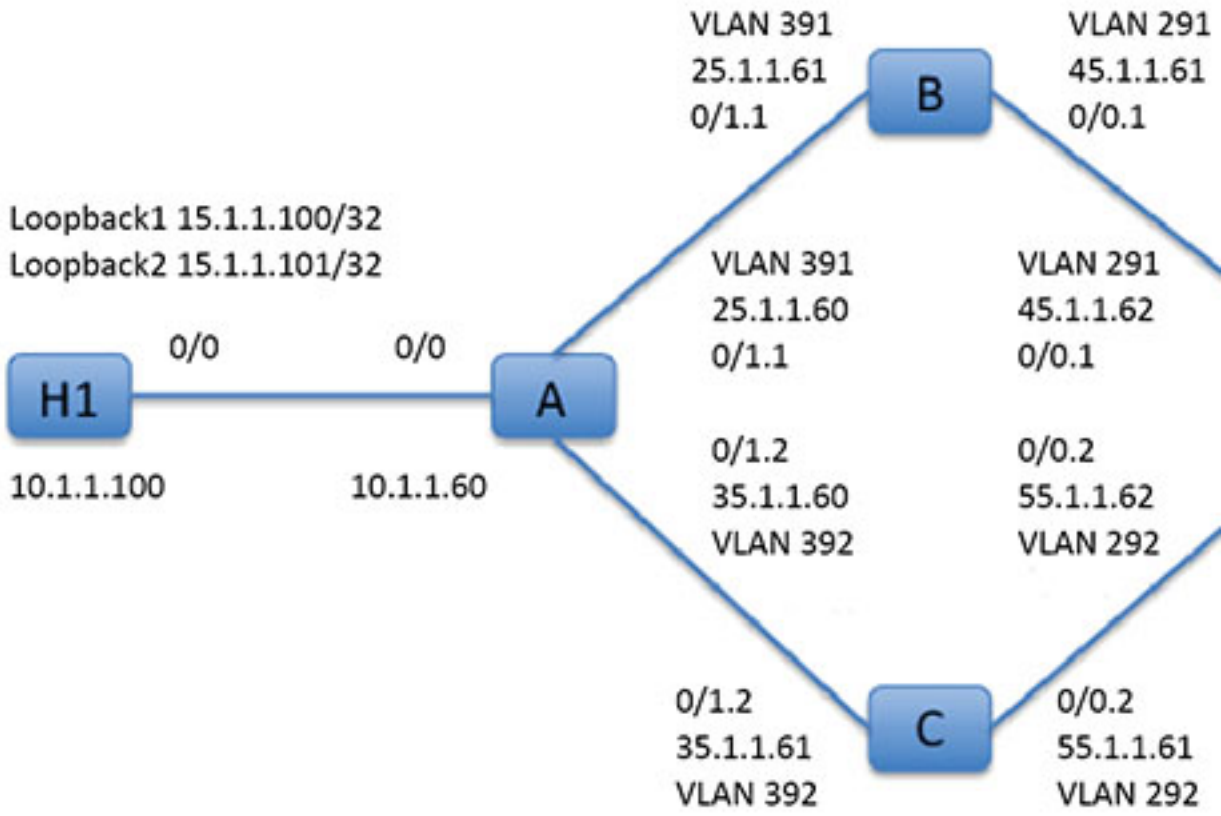
ステップ 5 SaaS トラフィックを外部インターフェイスに送信するために、入力インターフェイスでポリシーベースルーティングを設定します。

次の例では、ルートマップを内部インターフェイスに接続して、直接インターネットアクセスのポリシーベースルーティングを有効にします。

```
interface G1/0
  nameif inside
  policy-route route-map mymap
```

アクションでのポリシーベース ルーティング

このテスト設定を使用して、異なる一致基準および set アクションでポリシーベース ルーティングが設定され、それらがどのように評価および適用されるのかを確認します。



まず、セットアップに関係するすべてのデバイスの基本設定から始めます。ここで、A、B、C、および D は ASA デバイスを表し、H1 および H2 は IOS ルータを表します。

ASA-A：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
```

```
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0
```

```
ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1：

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255

ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.60
```

H2：

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

H1 から送信されるトラフィックをルーティングするように ASA-A で PBR を設定します。

ASA-A：

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap

ciscoasa(config-if)# debug policy-route
```

H1： ping 65.1.1.100 repeat 1 source loopback1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1
sub_proto 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

パケットは、ルートマップのネクストホップアドレスを使用して想定どおりに転送されます。

ネクストホップを設定した場合、入力ルートテーブルで検索して設定したネクストホップに接続されたルートを特定し、対応するインターフェイスを使用します。この例の入力ルートテーブルを次に示します（一致するルート エントリが強調表示されています）。

```
in   255.255.255.255 255.255.255.255 identity
in   10.1.1.60       255.255.255.255 identity
in   25.1.1.60       255.255.255.255 identity
in   35.1.1.60       255.255.255.255 identity
in   10.127.46.17    255.255.255.255 identity
in   10.1.1.0        255.255.255.0   inside
in   25.1.1.0        255.255.255.0   outside
in   35.1.1.0        255.255.255.0   dmz
```

次に、ASA-A の dmz インターフェイスからの H1 loopback2 から送信されるパケットをルーティングするように ASA-A を設定します。

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl_2
  set ip next-hop 35.1.1.61
!
```

H1：ping 65.1.1.100 repeat 1 source loopback2

デバッグを示します。

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6
sub_proto 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

さらに、入力ルート テーブルから選択されたルートのエントリをここに示します。

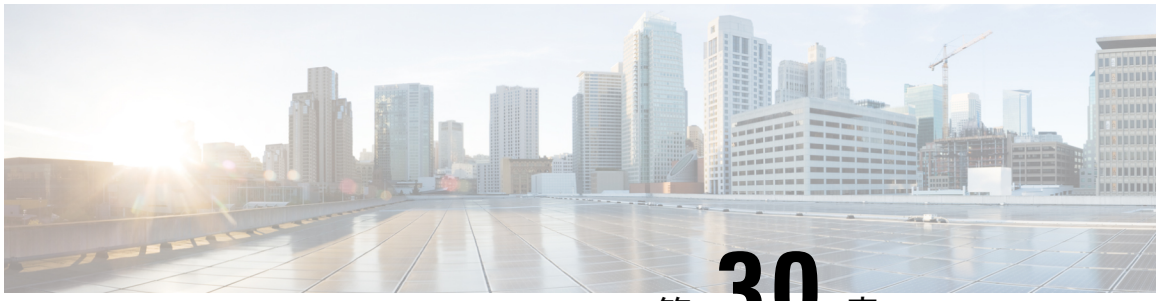
```
in   255.255.255.255 255.255.255.255 identity
 in   10.1.1.60       255.255.255.255 identity
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   10.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

ポリシーベース ルーティングの履歴

表 *38 :* ルート マップの履歴

機能名	プラットフォーム リリース	機能情報
HTTP クライアントによるパスモニタリング	9.20(1)	PBR は、特定の宛先 IP のメトリックではなく、アプリケーションドメインの HTTP クライアントを介したパスモニタリングによって収集されたパフォーマンスメトリック（RTT、ジッター、パケット損失、およびMOS）を使用できるようになりました。HTTP ベースのパスモニタリングは、ネットワーク サービス グループのオブジェクトを使用してインターフェイスで設定できます。
PBR のパスモニタリングメトリック。	9.18(1)	PBRはメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースをPBRに定期的に通知します。PBRは、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。 新規/変更されたコマンド：**clear path-monitoring**、**policy-route**、**show path-monitoring**
ポリシーベース ルーティング	9.4(1)	ポリシーベースルーティング（PBR）は、ACLを使用して指定されたQoSでトラフィックが特定のパスを経由するために使用するメカニズムです。ACLでは、パケットのレイヤ 3 および レイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックにQoSを提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチド パスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネットサービスプロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザーから送信されるトラフィックをルーティングできます。 **set ip next-hop verify-availability**、**set ip next-hop**、**set ip next-hop recursive**、**set interface**、**set ip default next-hop**、**set default interface**、**set ip df**、**set ip dscp**、**policy-route route-map**、**show policy-route**、**debug policy-route** の各コマンドが導入されました。

機能名	プラットフォーム リリース	機能情報
ポリシーベース ルーティングの IPv6 サポート	9.5(1)	ポリシーベース ルーティングで IPv6 アドレスがサポートされました。 次のコマンドが導入されました。**set ipv6 next-hop**、**set default ipv6-next hop**、**set ipv6 dscp**
ポリシーベース ルーティングの VXLAN サポート	9.5(1)	VNI インターフェイスでポリシーベース ルーティングを有効にできるようになりました。 変更されたコマンドはありません。
アイデンティティ ファイアウォールと Cisco TrustSec でのポリシーベース ルーティングのサポート	9.5(1)	アイデンティティ ファイアウォールと Cisco TrustSec を設定し、ポリシーベース ルーティングのルートマップでアイデンティティ ファイアウォールと Cisco TrustSec ACL を使用できるようになりました。 変更されたコマンドはありません。



第 30 章

ルート マップ

この章では、ASA のルートマップの設定方法とカスタマイズ方法について説明します。

- ルート マップについて （1175 ページ）
- ルート マップのガイドライン （1177 ページ）
- ルート マップの定義 （1177 ページ）
- ルート マップのカスタマイズ （1178 ページ）
- ルート マップの例 （1180 ページ）
- ルート マップの履歴 （1181 ページ）

ルート マップについて

ルート マップは、ルートを OSPF、RIP、EIGRP、または BGP ルーティング プロセスに再配布するときに使用します。また、OSPF ルーティング プロセスにデフォルト ルートを生成するときにも使用します。ルート マップは、指定されたルーティング プロトコルのどのルートを対象ルーティング プロセスに再配布できるのかを定義します。

ルート マップは、広く知られた ACL と共通の機能を数多く持っています。両方に共通する主な特性は次のとおりです。

- いずれも、それぞれが許可または拒否の結果を持つ個別のステートメントの順序シーケンスです。ACL またはルート マップの評価は、事前に定義された順序でのリストのスキャンと、一致する各ステートメントの基準の評価で構成されています。リストのスキャンは、ステートメントの一致が初めて見つかり、そのステートメントの一致に関連付けられたアクションが実行されると中断します。
- これらは汎用的なメカニズムです。基準照合と一致解釈は、適用方法とこれらを使用する機能によって決定します。同じルートマップであっても異なる機能に適用されると、解釈が異なる場合があります。

次のように、ルート マップと ACL には違いがいくつかあります。

- ルート マップは ACL よりも柔軟性が高く、ACL が確認できない基準に基づいてルートを確認できます。たとえば、ルート マップはルート タイプが内部であるかどうかを確認できます。

- 設計規則により、各 ACL は暗黙の deny ステートメントで終了します。照合中にルートマップの終わりに達した場合、そのルート マップの特定の適用によって結果が異なります。再配布に適用されるルート マップの動作は ACL と同じです。ルートがルートマップのどの句とも一致しない場合は、ルートマップの最後に deny ステートメントが含まれている場合と同様に、ルート再配布が拒否されます。

permit 句と deny 句

ルート マップでは permit 句と deny 句を使用できます。deny 句は、ルートの照合の再配布を拒否します。ルートマップでは、一致基準として ACL を使用できます。ACL には permit 句と deny 句もあるので、パケットが ACL と一致した場合に次のルールが適用されます。

- ACL の permit + ルート マップの permit：ルートは再配布されます。
- ACL の permit + ルート マップの deny：ルートは再配布されません。
- ACL の deny + ルート マップの permit または deny：ルート マップの句は一致せず、次のルート マップ句が評価されます。

match 句と set 句の値

各ルート マップ句には、次の 2 種類の値があります。

- match 値は、この句が適用されるルートを選択します。
- set 値は、ターゲット プロトコルに再配布される情報を変更します。

再配布される各ルートについて、ルータは最初にルートマップの句の一致基準を評価します。一致基準が満たされると、そのルートは、permit 句または deny 句に従って再配布または拒否され、そのルートの一部の属性が、set コマンドによって設定された値で変更されます。一致基準が満たされないと、この句はルートに適用されず、ソフトウェアはルートマップの次の句でルートを評価します。ルートマップのスキャンは、ルートと一致する句が見つかるまで、もしくはルートマップの最後に到達するまで続行します。

次のいずれかの条件が満たされる場合は、各句の match 値または set 値を省略したり、何回か繰り返したりできます。

- 複数の match エントリが句に含まれる場合に、特定のルートが句に一致するためには、そのルートですべての照合に成功しなければなりません（つまり、複数の match コマンドでは論理 AND アルゴリズムが適用される）。
- match エントリが 1 つのエントリの複数のオブジェクトを指している場合は、そのいずれかが一致していなければなりません（論理 OR アルゴリズムが適用される）。
- match エントリがない場合は、すべてのルートが句に一致します。
- ルート マップの permit 句に set エントリが存在しない場合、ルートは、その現在の属性を変更されずに再配布されます。

（注） ルート マップの deny 句では set エントリを設定しないでください。deny 句を指定するとルートの再配布が禁止され、情報が何も変更されないからです。

match エントリまたは set エントリがないルート マップ句はアクションを実行します。空の permit 句を使用すると、変更を加えずに残りのルートの再配布が可能になります。空の deny 句では、他のルートの再配布はできません。これは、ルートマップがすべてスキャンされたときに、明示的な一致が見つからなかったときのデフォルト アクションです。

ルート マップのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

その他のガイドライン

ルート マップは、ユーザー、ユーザー グループ、または完全修飾ドメイン名のオブジェクトを含む ACL をサポートしていません。

ルート マップの定義

ルート マップを定義する必要があるのは、指定したルーティング プロトコルからのどのルートを対象ルーティング プロセスに再配布できるのかを指定するときです。

手順

ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序がASAで使用されます。

ルート マップのカスタマイズ

ここでは、ルート マップをカスタマイズする方法について説明します。

特定の宛先アドレスに一致するルートの定義

手順

ステップ 1 ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* オプションを使用して指定できます。この引数で指定しなければ、ルート マップ エントリを追加した順序が ASA で使用されます。

ステップ 2 標準 ACL またはプレフィックス リストに一致する宛先ネットワークを持つ任意のルートを照合します。

match ip address {*acl_id* [*acl_id*] [...] | **prefix-list** *prefix_list_id* [*prefix_list_id*] [...]}

例：

```
ciscoasa(config-route-map)# match ip address acl1 acl2 acl3
```

複数の ACL またはプレフィックス リストを指定する場合、ルートは任意の ACL またはプレフィックス リストと一致します。

（注）
プレフィックス リストは、OSPF ではサポートされていません。

ステップ 3 指定したメトリックを持つ任意のルートを照合します。

match metric *metric_value*

例：

```
ciscoasa(config-route-map)# match metric 200
```

metric_value には、0 ～ 4294967295 の範囲が指定できます。

ステップ 4 標準 ACL と一致するネクスト ホップ ルータ アドレスを持つ任意のルートを照合します。

match ip next-hop *acl_id* [*acl_id*] [...]

例：

```
ciscoasa(config-route-map)# match ip next-hop acl2
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 5 指定されたネクスト ホップ インターフェイスを持つ任意のルートを照合します。

match interface *if_name*

例：

```
ciscoasa(config-route-map)# match interface if_name
```

2 つ以上のインターフェイスを指定する場合、ルートはいずれかのインターフェイスと一致します。

ステップ 6 標準の ACL と一致するルータによってアドバタイズされた任意のルートを照合します。

match ip route-source *acl_id* [*acl_id*] [...]

例：

```
ciscoasa(config-route-map)# match ip route-source acl_id [acl_id] [...]
```

複数の ACL を指定する場合、ルートは任意の ACL を照合できます。

ステップ 7 ルート タイプを照合します。

match route-type {**internal** | **external** [**type-1** | **type-2**]}

ルート アクションのメトリック値の設定

ルートが **match** コマンドで一致する場合は、次の **set** コマンドによって、ルートを再配布する前にルートで実行するアクションが決まります。

ルート アクションのメトリック値を設定するには、次の手順を実行します。

手順

ステップ 1 ルート マップのエントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map name {permit} [12]
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序が ASA で使用されます。

ステップ 2 ルート マップのメトリック値を設定します。

set metric *metric_value*

例：

```
ciscoasa(config-route-map)# set metric 200
```

metric_value の引数は、0～294967295 の範囲で指定できます。

ステップ 3 ルート マップのメトリック タイプを設定します。

set metric-type {**type-1** | **type-2**}

例：

```
ciscoasa(config-route-map)# set metric-type type-2
```

metric-type 引数には type-1 と type-2 があります。

ルート マップの例

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。

ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

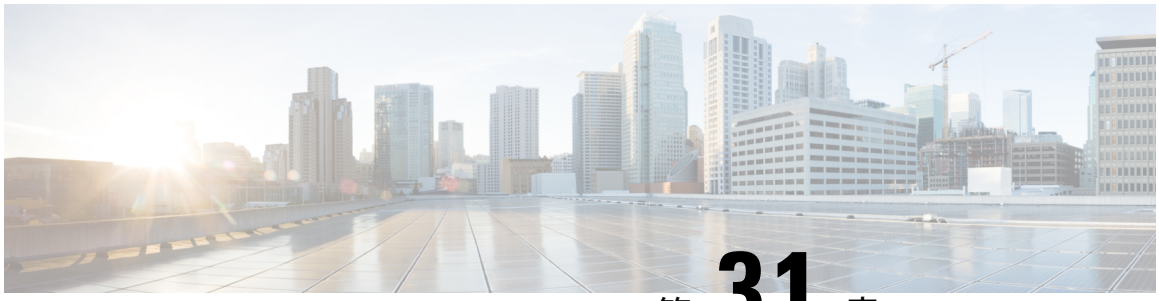
次に、メトリック値が設定された EIGRP プロセス 1 に 10.1.1.0 のスタティック ルートを再配布する例を示します。

```
ciscoasa(config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config-router)# redistribute static metric 250 250 1 1 1 route-map mymap2
```

ルート マップの履歴

表 *39 :* ルート マップの機能履歴

機能名	プラットフォーム リリース	機能情報
ルート マップ	7.0(1)	この機能が導入されました。 **route-map** コマンドが導入されました。
スタティックおよびダイナミック ルートマップのサポートの強化	8.0(2)	ダイナミックおよびスタティック ルートマップのサポートが強化されました。
ダイナミック ルーティング プロトコル（EIGRP、OSPF、RIP）のステートフル フェールオーバーと一般的なルーティング関連動作のデバッグのサポート	8.4(1)	**debug route**、および **show debug route** コマンドが導入されました。 **show route** コマンドが変更されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	ルート マップは、マルチ コンテキスト モードでサポートされます。
BGP のサポート	9.2(1)	この機能が導入されました。 **router bgp** コマンドが導入されました。
プレフィックス ルールの IPv6 サポート	9.3.2	この機能が導入されました。



第 31 章

双方向フォワーディング検出ルーティング

この章では、双方向フォワーディング検出（BFD）ルーティング プロトコルを使用するように ASA を設定する方法について説明します。

- BFD ルーティングについて （1183 ページ）
- BFD ルーティングのガイドライン （1188 ページ）
- BFD の設定 （1188 ページ）
- BFD のモニタリング （1193 ページ）
- BFD ルーティングの履歴 （1194 ページ）

BFD ルーティングについて

BFD はあらゆるメディア タイプ、カプセル化、トポロジ、およびルーティング プロトコルの高速転送パス障害検出回数を提供するように設計された検出プロトコルです。BFD は、2 つのシステム間の転送データ プロトコルすべてに加えて、ユニキャストのポイントツーポイント モードで動作します。パケットは、メディアやネットワークに対して適切なカプセル化プロトコルのペイロードで送信されます。

BFD は高速転送パス障害検出に加えて、ネットワーク管理者に一貫した障害検出方法を提供します。ネットワーク管理者は BFD を使用することで、さまざまなルーティング プロトコルの HELLO メカニズムにより、変動速度ではなく一定速度で転送パス障害を検出できるため、ネットワーク プロファイリングおよびプランニングが容易になります。また、再収束時間の整合性が保たれ、予測可能になります。

BFD 非同期モードおよびエコー機能

BFD は、エコー機能が有効であるかどうかに関わらず非同期モードで動作できます。

非同期モード

非同期モードでは、システムが相互に BFD 制御パケットを定期的に送信します。一方のシステムがこれらのパケットの多くを連続して受信しない場合、セッションはダウンしているものと宣言されます。純粋な非同期モード（エコー機能なし）では、エコー機能に必要な特定の検出時間を達成するのに必要なパケットの数が半分で済むため、便利です。

BFD エコー機能

BFD エコー機能は、フォワーディング エンジンから、直接接続シングル ホップ BFD ネイバーへエコー パケットを送信します。エコー パケットはフォワーディング エンジンによって送信され、検出を実行するために同じパスに沿って返信されます。もう一方の BFD セッションは、エコー パケットの実際のフォワーディングに参加しません。エコー機能およびフォワーディング エンジンが検出プロセスを処理するため、BFD ネイバー間で送信される BFD 制御パケットの数が減少します。また、フォワーディング エンジンがリモート ネイバー システムでフォワーディング パスをテストする際にリモート システムが関与しないため、パケット間の遅延のばらつきが改善します。この結果、障害検出にかかる時間が短くなります。

エコー機能が有効な場合、BFD はスロー タイマーを使用して、非同期セッションの時間を長くし、BFD ネイバー間で送信される BFD 制御パケットの数を減らすことができます。これにより、処理オーバーヘッドが削減し、同時に障害検出時間が短くなります。

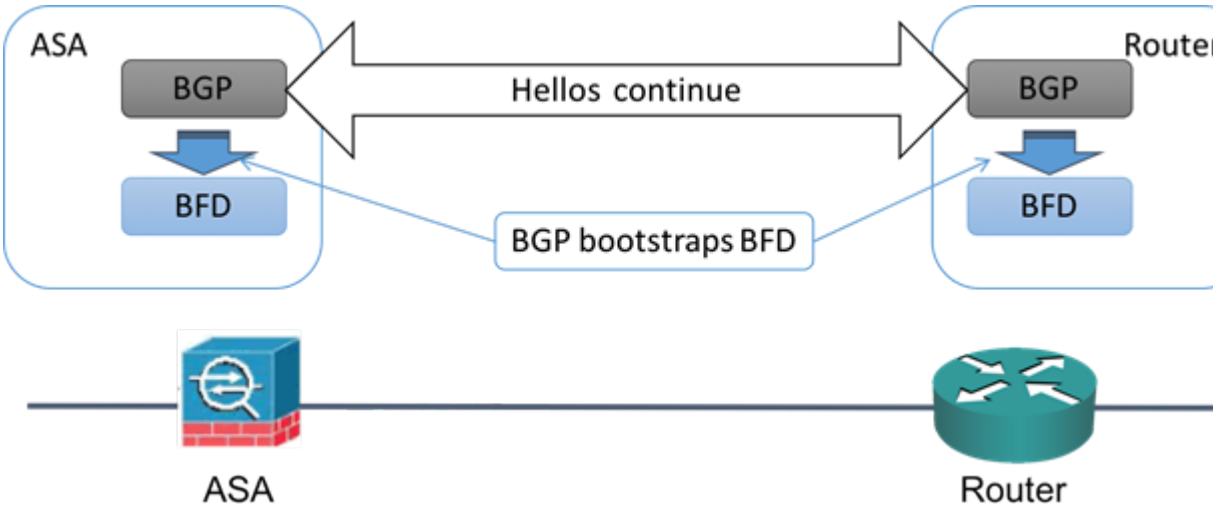
（注） IPv4 マルチホップまたは IPv6 シングルホップ BFD ネイバーでは、エコー機能はサポートされていません。

BFD はインターフェイス レベルとルーティング プロトコル レベルで有効にできます。両方のシステム（BFD ピア）で BFD を設定する必要があります。インターフェイスと、該当するルーティング プロトコルのルータ レベルで BFD を有効にすると、BFD セッションが作成され、BFD タイマーがネゴシエートされ、BFD ピアが BFD コントロール パケットをネゴシエートされたレベルで相互に送信し始めます。

BFD セッション確立

次の例は、ASA と Border Gateway Protocol（BGP）を実行する隣接ルータを示します。両方のデバイスが起動する時点では、デバイス間で BFD セッションは確立されていません。

図 *79 : BFD* セッションの確立



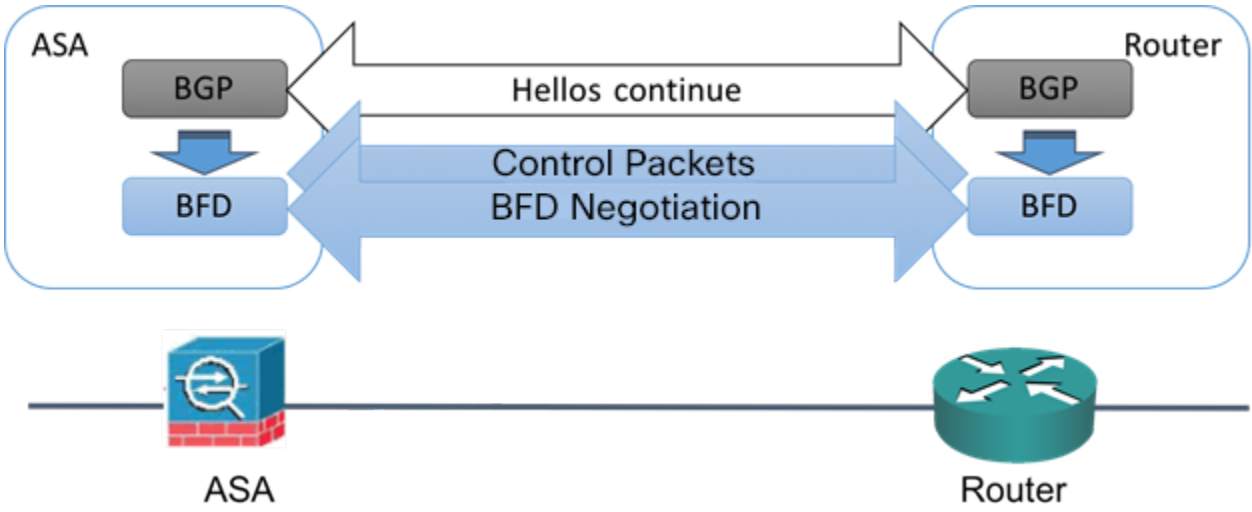
BGP は、BGP ネイバーの特定後に、そのネイバーの IP アドレスを使用して BFD プロセスをブートストラップします。BFD はそのピアを動的に検出しません。BFD は、設定されているルーティング プロトコルから、使用する IP アドレスと形成するピア関係を把握します。

ルータの BFD と ASA の BFD により BFD 制御パケットが形成され、BFD セッションが確立されるまで 1 秒間隔でこのパケットが相互に送信されます。両方のシステムの最初の制御パケットは非常によく似ています。たとえば、Vers、Diag、H、D、P、および F ビットはすべてゼロに設定され、State は Down に設定されます。[My Discriminator] フィールドには、送信デバイスで一意の値が設定されます。[Your Discriminator] フィールドにはゼロが設定されます。これは、BFD セッションがまだ確立されていないためです。TX タイマーと RX タイマーには、デバイスの設定で検出された値が設定されます。

リモート BFD デバイスは、セッション開始フェーズで BFD 制御パケットを受信すると、[My Discriminator] フィールドの値をデバイス自体の [Your Discriminator] フィールドに設定し、[Down] 状態から [Init] 状態、そして最終的には [Up] 状態に移行します。両方のシステムが、相互の制御パケットで各自の Discriminator を検出すると、セッションが正式に確立されます。

次の図は、確立された BFD 接続を示します。

図 *80 : BFD* セッションが確立されていない *BGP*



BFD タイマー ネゴシエーション

BFD デバイスは、BFD 制御パケットの送信速度を制御および同期するため、BFD タイマーをネゴシエートする必要があります。BFD タイマーをネゴシエートする前に、デバイスは以下の点を確認する必要があります。

- そのピア デバイスが、ローカル デイバスの提示されるタイマーを含むパケットを確認している。
- ピアで設定されている BFD 制御パケットの受信速度を上回る速度でデバイスが BFD 制御パケットを送信することがない。
- ローカル システムで設定されている BFD 制御パケットの受信速度を上回る速度でピアが BFD 制御パケットを送信することがない。

[Your Discriminator] フィールドと H ビットの設定は、初期タイマーの期間中にリモート デバイスがそのパケットを確認するローカルデバイスを交換できるようにするのに十分です。各システムは BFD 制御パケットを受信すると、Required Min RX Interval をシステム自体の Desired Min TX Interval と比較し、2 つの値のうち大きい方の値（低速な値）を、BDF パケットの転送速度として使用します。2 つのシステムのうち低速なシステムによって、転送速度が決定します。

これらのタイマーがネゴシエートされていない場合、セッション中の任意の時点で、セッションをリセットすることなく再ネゴシエートできます。タイマーを変更するデバイスは、F ビットがセットされている BFD 制御パケットをリモート システムから受信するまで、後続のすべての BFD 制御パケットの P ビットをセットします。このビット交換により、転送中に失われる可能性があるパケットが保護されます。

（注） リモート システムによって F ビットがセットされている場合、新たに提示されるタイマーをリモート システムが受け入れることを意味しているわけではありません。これは、タイマーが変更されたパケットをリモート システムが確認したことを意味します。

BFD 障害検出

BFD セッションとタイマーがネゴシエートすると、BFD のピアは、ネゴシエートされた間隔で BFD 制御パケットを相互に送信します。これらの制御パケットはハートビートの役割を果たします。これは、IGP Hello プロトコルとよく似ていますが、レートはさらに速くなっています。

設定されている検出間隔（必要な最小 RX 間隔）内の BFD 制御パケットを各 BFD ピアが受信する限り、BFD セッションは有効であり、BFD と関連付けられたルーティング プロトコルは隣接関係を維持します。BFD ピアがこの間隔内に制御パケットを受信しない場合、その BFD セッションに参加しているクライアントに障害発生を通知します。ルーティング プロトコルにより、その情報に対する適切な応答が決定されます。標準的な応答は、ルーティング プロトコル ピア セッションを終了し、再コンバージェンスの後、障害の発生したピアをバイパスすることです。

BFD セッション中に BFD ピアが正常に BFD 制御パケットを受信するたびに、このセッションの検出タイマーがゼロにリセットされます。したがって、障害検出は、受信側が最後にパケットを送信した時点ではなく、パケット受信に依存しています。

BFD 導入シナリオ

具体的なシナリオで BFD がどのように動作するかについて、以下に説明します。

フェールオーバー

フェールオーバー シナリオでは、アクティブ ユニットとネイバー ユニット間で BFD セッションが確立、維持されます。スタンバイ ユニットはネイバーとの BFD セッションを維持しません。フェールオーバーが発生すると、新しいアクティブ ユニットがネイバーとのセッション確立を開始する必要があります。これは、アクティブ ユニットとスタンバイ ユニットの間ではセッション情報が同期されないためです。

グレースフル リスタート/NSF シナリオでは、クライアント（BGP IPv4/IPv6）がそのネイバーに対してイベントを通知します。ネイバーはこの情報を受信すると、フェールオーバーが完了するまで RIB テーブルを維持します。フェールオーバー中に、デバイスで BFD と BGP セッションがダウンします。フェールオーバーが完了し、BGP セッションがアップになると、ネイバー間で新しい BFD セッションが確立されます。

スパンド EtherChannel および L2 クラスタ

スパンド EtherChannel クラスタ シナリオでは、プライマリ ユニットとそのネイバー間で BFD セッションが確立、維持されます。従属ユニットはネイバーとの間の BFD セッションを維持しません。スイッチでのロードバランシングが原因で BFD パケットが従属ユニッ

トにルーティングされる場合、従属ユニットはこのパケットをクラスタ リンク経由でプライマリ ユニットに転送する必要があります。クラスタ スイッチオーバーが発生すると、新しいプライマリユニットがネイバーとのセッション確立を開始します。これは、プライマリ ユニットと従属ユニットの間でセッション情報が同期されていないためです。

個別インターフェイス モードと L3 クラスタ

個別インターフェイスモードクラスタのシナリオでは、個々のユニットが各自のネイバーとの BFD セッションを維持します。

BFD ルーティングのガイドライン

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでサポートされます。スタンドアロン、フェールオーバー、およびクラスタ モードをサポートします。BFD は、フェールオーバーおよびクラスタ インターフェイスではサポートされません。クラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。BFD は、トランスペアレント モードではサポートされません。

IPv6 のガイドライン

エコー モードは IPv6 ではサポートされません。

その他のガイドライン

OSPFv2、OSPFv3、BGP IPv4、および BGP IPv6 プロトコルがサポートされています。

IS-ISおよび EiGRP プロトコルはサポートされていません。

スタティック ルートの BFD はサポートされません。

転送およびトンネルでの BFD はサポートされません。

（注） 最適なルーティングを行うため、NSF の BGP グレースフル リスタートがデバイスで設定されている場合は、BFD を設定しないでください。

BFD の設定

ここでは、システムで BGP ルーティング プロセスを有効にして設定する方法について説明します。

手順

ステップ 1 BFD テンプレートの作成 （1189 ページ）。
ステップ 2 BFD インターフェイスの設定 （1191 ページ）。
ステップ 3 BFD マップの設定 （1192 ページ）。

BFD テンプレートの作成

このセクションでは、BFD テンプレートを作成して BFD コンフィギュレーション モードを開始するために必要な手順を説明します。

BFD テンプレートは、一連の BFD 間隔値を指定します。BFD テンプレートで指定された BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。また、シングルホップ セッションとマルチホップ セッションの認証も設定できます。エコーをイネーブルにできるのは、シングルホップのみです。

手順

ステップ 1 BFD を ASA 上のルーティング プロトコルとしてイネーブルにするために、BFD テンプレート（シングルホップまたはマルチホップ）を作成します。

bfd-template [single-hop | multi-hop] *template-name*

例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)#
```

- **single-hop**：シングルホップ BFD テンプレートを指定します。
- **multi-hop**：マルチホップ BFD テンプレートを指定します。
- *template-name*：テンプレート名を指定します。テンプレート名にスペースを含めることはできません。

bfd-template コマンドを使用して、BFD テンプレートを作成し、BFD コンフィギュレーション モードを開始できます。

ステップ 2 （オプション）シングルホップ BFD テンプレートでエコーを設定します。

bfd-template single-hop *template_name*

例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
```

```
ciscoasa (config-bfd)# echo
```

エコーモードをイネーブルにできるのは、シングルホップテンプレートのみです。BFDエコーは、IPv6 BFD セッションではサポートされません。

ステップ 3 BFD テンプレートで間隔を設定します。

interval [**both** *milliseconds* | **microseconds {both | min-tx}** *microseconds* | **min-tx** *milliseconds*

例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# interval both 50
```

- **both**：最小送受信間隔機能。
- *milliseconds*：間隔（ミリ秒数）を指定します。指定できる範囲は 50 ～ 999 です。
- **microseconds**：**both** および **min-tx** の BFD 間隔をミリ秒で指定します。
- *microseconds*：指定できる範囲は 50,000 ～ 999,000 です。
- **min-tx**：最小送信間隔機能。

BFD テンプレートの一部として指定される BFD 間隔値は、1 つのインターフェイスに限定されるものではありません。インターフェイスごとに個別の BFD テンプレートを適用できます。BFD インターフェイスの設定 （1191 ページ）を参照してください。

ステップ 4 BFD テンプレートで認証を設定します。

authentication {md5 | meticulous-mds | meticulous-sha-1 | sha-1} [0|8] *word* **key-id** *id*

例：

```
ciscoasa(config)# bfd-template single-hop TEMPLATE1
ciscoasa(config-bfd)# authentication sha-1 0 cisco key-id 10
```

- **authentication**：認証タイプを指定します。
- **md5**：Message Digest 5（MD5）認証。
- **meticulous-md5**：Meticulous キー MD5 認証。
- **meticulous-sha-1**：Meticulous キー SHA-1 認証。
- **sha-1**：キー SHA-1 認証。
- **0|8**：0 は、暗号化されていないパスワードが後に続くことを示します。8：暗号化されたパスワードが後に続くことを示します。
- *word*：BFD パスワード（キー）。最大 29 文字からなる 1 桁のパスワード/キーです。最初の数字の後にスペースが続くパスワードはサポートされていません。たとえば、「0 pass」と「1」は無効です。

- **key-id**：認証キー ID。
- *id*：キー文字列に一致する共有キー ID。範囲は 0 ～ 255 文字です。

認証は、シングルホップ テンプレートとマルチホップ テンプレートに設定できます。セキュリティを強化するために認証を設定することをお勧めします。BFD の送信元と宛先のペアごとに認証を設定し、両方のデバイスで認証パラメータが一致する必要があります。

BFD インターフェイスの設定

BFD テンプレートをインターフェイスにバインドすることで、基準 BFD セッション パラメータの設定およびエコーモードのイネーブル化をインターフェイスごとに行うことができるようになります。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#
```

ステップ 2 BFD テンプレートをインターフェイスに適用します。

bfd template *template-name*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# bfd template TEMPLATE1
```

bfd-template コマンドを使用してテンプレートを作成していない場合でも、インターフェイスでテンプレート名を設定できますが、そのテンプレートを定義するまでテンプレートは無効と見なされます。テンプレート名を再設定する必要はありません。名前は自動的に有効になります。

ステップ 3 BFD セッション パラメータを設定します。

bfd interval *milliseconds* **min_rx** *milliseconds* **multiplier** *multiplier-value*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-router)# bfd interval 200 min_rx 200 multiplier 3
```

- **interval** *milliseconds*：BFD 制御パケットが BFD ピアに送信される速度を指定します。有効値は 50 ～ 999 ミリ秒です。
- **min_rx** *milliseconds*：BFD 制御パケットが BFD ピアから受信されるときに期待される速度を指定します。有効値は 50 ～ 999 ミリ秒です。
- **multiplier** *multiplier-value*：BFD ピアから連続して紛失してよい BFD 制御パケットの数を指定します。この数に達すると、BFD はそのピアが利用不可になっていることを宣言し、レイヤ 3 BFD ピアに障害が伝えられます。指定できる範囲は 3 ～ 50 です。

ステップ 4 インターフェイスで BFD エコー モードをイネーブルにします。

bfd echo

例：

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(if)# bfd echo
```

エコー モードはデフォルトでイネーブルになっていますが、BFD IPv6 セッションではサポートされていません。エコーモードを有効にすると、最小エコー送信レベルと必要最短送信間隔の値が **bfd interval***milliseconds* **min_rx** *milliseconds* 設定から取得されます。

（注）
BFD エコー モードを使用するには、**no ip redirects** コマンドを使用して ICMP リダイレクト メッセージを無効にする必要があります。これにより、CPU 使用率が高くなることを回避できます。

BFD マップの設定

マルチホップ テンプレートに関連付けることができる宛先が含まれている BFD マップを作成できます。マルチホップ BFD テンプレートがすでに設定されている必要があります。

手順

ステップ 1 マルチホップ BFD テンプレートを作成します。手順については、BFD テンプレートの作成（1189 ページ）を参照してください。

ステップ 2 BFD マルチホップ テンプレートを宛先のマップに関連付けます。

bfd map {ipv4 | ipv6} *destination/cdir source/cdire template-name*

例：

```
ciscoasa(config)# bfd map ipv4 10.11.11.0/24 10.36.42.5/32 MULTI-TEMPLATE1
ciscoasa(config-bfd)#
```

- **ipv4** ：IPv4 アドレスを設定します。
- **ipv6** ：IPv6 アドレスを設定します。
- *destination/cdir*：宛先プレフィックス/長さを指定します。形式は A.B.C.D/<0-32> です。
- *source/cdir*：送信元プレフィックス/長さを指定します。形式は X:X:X;X::X/<0-128> です。
- *template-name*：この BFD マップに関連付けられているマルチホップ テンプレートの名前を指定します。

ステップ 3 （オプション）BFD スロー タイマー値を設定します。

bfd slow-timers [*milliseconds*]

例：

```
ciscoasa(config)# bfd slow-timers 14000
ciscoasa(config-bfd)#
```

milliseconds：（オプション）BFD スロー タイマーの値。指定できる範囲は 1000 ～ 30000 です。デフォルトは 1000 です。

BFD のモニタリング

次のコマンドを使用して、BFD ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。

さまざまな BFD ルーティング統計情報をモニターまたは無効にするには、次のいずれかのコマンドを入力します。

- **show bfd neighbors**

  既存の BFD 隣接関係の詳細なリストを表示します。

- **show bfd summary**

  BFD、BFD クライアント、または BFD セッションの概要情報を表示します。

- **show bfd drops**

  BFD でドロップされたパケットの数を表示します。

- **show bfd map**

  設定済みの BFD マップを表示します。

- **show running-config bfd**

  BFD マップおよびその他の BFD に関するコンフィギュレーションを表示します。

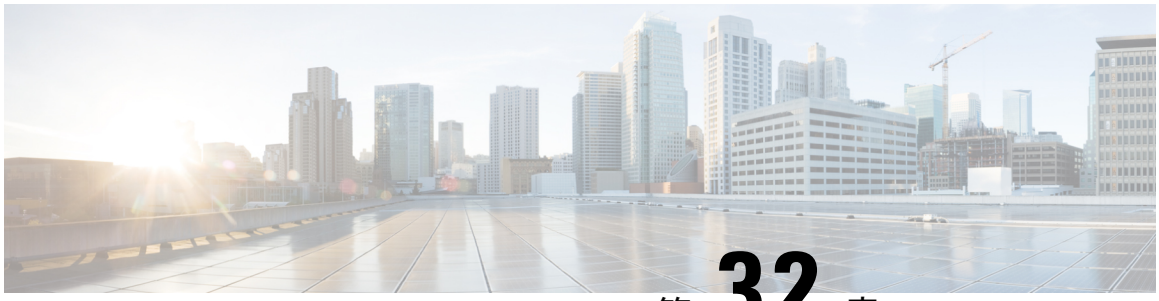
- **show running-config bfd-template**

  BFD テンプレートに関するコンフィギュレーションを表示します。

BFD ルーティングの履歴

表 *40 : BFD* ルーティングの機能履歴

機能名	プラットフォーム リリース	機能情報
BFD ルーティング サポート	9.6(2)	ASAは、BFD ルーティング プロトコルをサポートするようになりました。BFDテンプレート、インターフェイスおよびマッピングの設定が新たにサポートされました。BFD を使用するための BGP ルーティング プロトコルのサポートも追加されました。 次のコマンドが追加されました。 **bfd echo**、**bfd interval**、**bfd map**、**bfd slow-timers**、**bfd-template**、**clear bfd counters**、**clear conf bfd**、**neighbor fall-over bfd**、**show bfd drops**、**show bfd map**、**show bfd neighbors**、**show bfd summary**、**show running-config bfd**



第 32 章

BGP

この章では、Border Gateway Protocol（BGP）を使用してデータのルーティング、認証の実行、ルーティング情報の再配布を行うように ASA を設定する方法について説明します。

- BGPについて （1195 ページ）
- BGP のガイドライン （1199 ページ）
- BGP の設定 （1200 ページ）
- BGP のモニタリング （1234 ページ）
- BGP の例 （1236 ページ）
- BGP の履歴 （1239 ページ）

BGPについて

BGP は相互および内部の自律システムのルーティングプロトコルです。自律システムとは、共通の管理下にあり、共通のルーティングポリシーを使用するネットワークまたはネットワークのグループです。BGP は、インターネットのルーティング情報を交換するために、インターネット サービス プロバイダー（ISP）間で使用されるプロトコルです。

BGP を使用する状況

通常、大学や企業などの顧客ネットワークではネットワーク内でルーティング情報を交換するために OSPF などの Interior Gateway Protocol（IGP）を採用しています。カスタマーはISPに接続し、ISPはBGPを使用してカスタマーおよびISPルートを交換します。自律システム（AS）間でBGPを使用する場合、このプロトコルは外部BGP（EBGP）と呼ばれます。サービスプロバイダーがBGPを使用してAS内のルートを交換する場合、このプロトコルは内部BGP（IBGP）と呼ばれます。

BGPは、IPv6ネットワーク上でIPv6プレフィックスのルーティング情報を伝送するためにも使用することができます。

（注） BGPv6 デバイスがクラスタに参加すると、ロギング レベル 7 が有効の場合、ソフト トレースバックを生成します。

ルーティング テーブルの変更

BGP ネイバーは、ネイバー間で最初に TCP 接続を確立する際に、完全なルーティング情報を交換します。ルーティングテーブルで変更が検出された場合、BGPルータはネイバーに対し、変更されたルートのみを送信します。BGP ルータは、定期的にルーティング アップデートを送信しません。また BGP ルーティング アップデートは、宛先ネットワークに対する最適パスのアドバタイズのみを行います。

（注） AS ループの検出は、完全な AS パス（AS_PATH 属性で指定される）をスキャンし、ローカル システムの AS 番号が AS パスに現れないことを確認することによって実行されます。デフォルトでは、EBGP は学習したルートを同じピアにアドバタイズすることで、ループチェックを実行するときにデバイスで追加の CPU サイクルが発生することを防ぐとともに、既存の発信更新タスクの遅延を防ぎます。

BGPにより学習されたルートには、特定の宛先に対して複数のパスが存在する場合、宛先に対する最適なルートを決定するために使用されるプロパティが設定されています。次のプロパティはBGP属性と呼ばれ、ルート選択プロセスで使用されます。

- Weight: これはシスコ定義の属性で、ルータに対してローカルです。Weight属性は、隣接ルータにアドバタイズされません。ルータが同じ宛先への複数のルートがあることを学習すると、[重み（Weight）] 属性値が最も大きいルートが優先されます。
- Local preference: Local preference属性は、ローカルASからの出口点を選択するために使用されます。Weight属性とは異なり、Local preference属性は、ローカルAS全体に伝搬されます。ASからの出口点が複数ある場合は、Local preference属性が最も高い出口点が特定のルートの出口点として使用されます。
- Multi-exit discriminator: メトリック属性であるMulti-exit discriminator (MED)は、メトリックをアドバタイズしているASへの優先ルートに関して、外部ASへの提案として使用されます。これが提案と呼ばれるのは、MEDを受信している外部ASがルート選択の際に他のBGP属性も使用している可能性があるためです。MEDメトリックが小さい方のルートが優先されます。
- Origin: Origin属性は、BGPが特定のルートについてどのように学習したかを示します。Origin属性は、次の3つの値のいずれかに設定することができ、ルート選択に使用されます。
  - IGP: ルートは発信側ASの内部にあります。この値は、ネットワークルータコンフィギュレーションコマンドを使用してBGPにルートを挿入する場合に設定されます。
  - EGP: ルートはExterior Border Gateway Protocol (EBGP)を使用して学習されます。
  - Incomplete: ルートの送信元が不明であるか、他の方法で学習されています。IncompleteのOriginは、ルートがBGPに再配布されるときに発生します。

- AS_path：ルートアドバタイズメントが自律システムを通過すると、ルートアドバタイズメントが通過した AS 番号が AS 番号の順序付きリストに追加されます。AS_path リストが最も短いルートのみ、IP ルーティングテーブルにインストールされます。
- Next hop: EBGPのnext-hop属性は、アドバタイジングルータに到達するために使用されるIPアドレスです。EBGP ピアの場合、ネクストホップアドレスは、ピア間の接続の IP アドレスです。IBGP の場合、EBGP のネクストホップアドレスがローカル AS に伝送されます。ただし、ネクストホップが eBGP ピアのピアリングアドレスと同じサブネットにある場合、ネクストホップは変更されません。この動作は、サードパーティのネクストホップと呼ばれます。

  VPN でアドバタイズされたルートを iBGP ピアに再配布する場合は、**next-hop-self** コマンドを使用して、ルートが正しいネクストホップ IP で再配布されるようにします。
- Community: Community属性は、ルーティングの決定(承認、優先順位、再配布など)を適用できる接続先をグループ化する方法、つまりコミュニティを提供します。ルートマップは、Community 属性を設定するために使用されます。事前定義済みのCommunity属性は次のとおりです。
  - no-export: EBGPピアにアドバタイズしません。
  - no-advertise: どのピアにもこのルートをアドバイタイズしません。
  - internet：インターネット コミュニティにこのルートをアドバタイズします。ネットワーク内のすべてのルートがこのコミュニティに属します。

BGP パスの選択

BGPは、異なる送信元から同じルートに対する複数のアドバタイズメントを受信する場合があります。BGP はベストパスとして 1 つのパスだけを選択します。ベストパスを選択すると、BGPは選択したパスをIPルーティングテーブルに格納し、そのネイバーにパスを伝達します。BGP は、次に示す順序で次の条件を使用して、宛先のパスを選択します。

- パスで指定されているネクストホップが到達不能な場合、更新はドロップされます。
- 重みが最大のパスが優先されます。
- 重みが同じ場合、ローカルプリファレンスが最大のパスが優先されます。
- ローカルプリファレンスが同じ場合、このルータで動作している BGP により発信されたパスが優先されます。
- ルートが発信されていない場合、AS_pathが最短のルートが優先されます。
- すべてのパスの AS_path の長さが同じ場合、Origin タイプが最下位のパス（IGP は EGP よりも低く、EGP は Incomplete よりも低い）が優先されます。
- Origin コードが同じ場合、最も小さい MED 属性を持つパスが優先されます。
- パスの MED が同じ場合、内部パスより外部パスが優先されます。

- それでもパスが同じ場合、最も近い IGP ネイバーを経由するパスが優先されます。
- BGPマルチパス （1198ページ） 用のルーティングテーブルに複数のパスをインストールする必要があるか判断します。
- 両方のパスが外部のときは、先に受信したパス(最も古いパス)が優先されます。
- BGPルータIDで指定された、IPアドレスが最も小さいパスが優先されます。
- 発信元 ID またはルータ ID が複数のパスで同じ場合は、最小のクラスタ リスト長を持つパスが優先されます。
- 最も小さいネイバー アドレスから発信されたパスが優先されます。

BGP マルチパス

BGP マルチパスでは、同じ宛先プレフィックスへの複数の等コスト BGP パスの IP ルーティングテーブルへのインストールが許可されます。その場合、宛先プレフィックスへのトラフィックは、インストールされたすべてのパス間で共有されます。

これらのパスは、ロードシェアリング用にベストパスとともにテーブルにインストールされます。BGPマルチパスはベストパスの選択には影響しません。たとえば、ルータではアルゴリズムに従って、ベストパスとしてパスの 1 つが引き続き指定され、そのベストパスが BGP ピアにアドバタイズされます。

マルチパスの候補になるためには、同じ宛先へのパスに、最適パスの特性に等しいこれらの特性が備わっている必要があります。

- 重量
- ローカル プリファレンス
- AS-PATH length
- オリジン コード
- Multi Exit識別子(MED)
- 次のいずれか。
  - ネイバー AS または sub-AS（BGP マルチパス機能が追加される前）
  - AS-PATH（BGP マルチパス機能が追加された後）

一部の BGP マルチパス機能により、マルチパス候補に関する追加要件が加わりました。

- パスは、外部またはコンフェデレーション外部の近接ルータ（eBGP）から学習されます。
- BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

内部 BGP（iBGP）マルチパスの候補には次の追加要件があります。

- パスは、内部の近接ルータ（iBGP）から学習されます。

- ルータが不等コスト iBGP マルチパスで設定されない限り、BGP ネクストホップへの IGP メトリックは、最適パスの IGP メトリックと等しくなる必要があります。

BGP は、マルチパス候補から最近受信した最大 *n* 個のパスを IP ルーティングテーブルに挿入します。ここで、*n* は、BGP マルチパスを設定するときに指定した、ルーティングテーブルにインストールするルートの数です。マルチパスがディセーブルになっている場合のデフォルト値は 1 です。

不等コスト ロード バランシングでは、BGP リンク帯域幅も使用できます。

（注） 内部ピアへの転送前に、eBGP マルチパスで選択されたベストパスに対し、同等の next-hop-self が実行されます。

BGP のガイドライン

コンテキスト モードのガイドライン

- シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。
- すべてのコンテキストでサポートされる自律システム（AS）番号は 1 つだけです。

ファイアウォール モードのガイドライン

トランスペアレント ファイアウォール モードはサポートされません。BGP は、ルーテッドモードでのみサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- システムは、PPPoE 経由で受信した IP アドレスのルートエントリを CP ルートテーブルに追加しません。BGP は常に CP ルートテーブルを調べて TCP セッションを開始するため、BGP は TCP セッションを形成しません。

  つまり、PPPoE 経由の BGP はサポートされません。

- 管理専用または BVI インターフェイスでは、BGP はサポートされません
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- PATH MTU（PMTU）を使用した BGP は、特に ECMP ルーティングで MTU ディスカバリが失敗した場合に、隣接関係（アジャセンシー）フラップを引き起こす可能性がありま

す。したがって、何らかの理由で MTU ディスカバリが失敗した場合にパケットドロップが発生する可能性があるため、BGP、PMTU、および ECMP の使用時には注意が必要です。

- メンバーユニットの BGP テーブルは、制御ユニットテーブルと同期されません。ルーティングテーブルだけが、制御ユニットのルーティングテーブルと同期されます。

BGP の設定

ここでは、システムで BGP プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 BGP の有効化 （1200 ページ）。
ステップ 2 BGP ルーティング プロセスの最適なパスの定義 （1202 ページ）。
ステップ 3 ポリシー リストの設定 （1203 ページ）。
ステップ 4 AS パス フィルタの設定 （1204 ページ）。
ステップ 5 コミュニティ ルールの設定 （1205 ページ）。
ステップ 6 IPv4 アドレス ファミリの設定 （1206 ページ）。
ステップ 7 IPv6 アドレス ファミリの設定 （1221 ページ）。

BGP の有効化

ここでは、BGP の有効化、BGP ルーティング プロセスの確立、一般的な BGP パラメータの設定に必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

autonomous-num の有効値は 1 ～ 4294967295 および 1.0 ～ XX.YY です。

ステップ 2 指定値を超えている AS パス セグメントを含むルートを破棄します。

bgp maxas-limit number

例：

```
ciscoasa(config-router)# bgp maxas-limit 15
```

number 引数には、自律システム セグメントの最大許容数を指定します。有効値は 1 ～ 254 です。

ステップ 3 BGP ネイバーのリセットをログに記録します。

bgp log-neighbor-changes

ステップ 4 BGP で各 BGP セッションの最適な TCP パス MTU を自動検出できるようにします。

bgp transport path-mtu-discovery

ステップ 5 BGP が、ピアに到達するために使用されているリンクがダウンした場合に、ホールドダウン タイマーが期限切れになるのを待たずに、直接隣接するいずれかのピアの外部 BGP セッションを終了できるようにします。

bgp fast-external-fallover

ステップ 6 BGP ルーティング プロセスで、自律システム（AS）番号を着信ルートの AS_path 属性の 1 つ目の AS パス セグメントとしてリストしていない外部 BGP（eBGP）ピアから受信したアップデートを破棄できるようにします。

bgp enforce-first-as

ステップ 7 デフォルトの表示を変更し、BGP 4 バイト自律システム番号の正規表現一致形式を、asplain（10 進数の値）からドット付き表記にします。

bgp asnotation dot

ステップ 8 BGP ネットワーク タイマーを調整します。

timers bgp keepalive holdtime [min-holdtime]

例：

```
ciscoasa(config-router)# timers bgp 80 120
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルト値は 60 秒です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- （オプション）min-holdtime：ネイバーからキープアライブ メッセージを受信できない状態が継続して、ネイバーがデッドであると ASA が宣言するまでの時間（秒）。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 9 BGP グレースフル リスタート機能をイネーブルにします。

bgp graceful-restart [restart-time seconds|stalepath-time seconds][all]

例：

```
ciscoasa(config-router)# bgp graceful-restart restart-time 200
```

- restart-time：リスタートイベントが発生した後、グレースフル リスタート対応ネイバーが通常の動作に戻るまで ASA が待機する最大時間（秒）。デフォルトは 120 秒です。有効な値は 1 ～ 3600 秒です。
- stalepath-time：リスタートしているピアの古いパスを ASA が保持する最大時間（秒）。すべての古いパスは、このタイマーが期限切れになった後に削除されます。デフォルト値は 360 秒です。有効な値は 1 ～ 3600 秒です。

BGP ルーティング プロセスの最適なパスの定義

ここでは、BGP の最適なパスを設定するために必要な手順について説明します。最適なパスの詳細については、BGP パスの選択 （1197 ページ）を参照してください。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 デフォルトの Local preference 値を変更します。

bgp default local-preference number

例：

```
ciscoasa(config-router)# bgp default local-preference 500
```

number 引数は、0 ～ 4294967295 の値です。値が大きいほど、優先度が高いことを示します。

デフォルト値は 100 です。

ステップ 3 さまざまな自律システムのネイバーから学習したパス間での Multi-exit discriminator（MED）比較をイネーブルにします。

bgp always-compare-med

ステップ 4 最適なパスの選択プロセス中に外部 BGP（eBGP）ピアから受信した類似ルートを比較し、最適なパスをルータ ID が最も小さいルートに切り替えます。

bgp bestpath compare-routerid

ステップ 5 隣接 AS からアドバタイズされた最適な MED パスを選択します。

bgp deterministic-med

ステップ 6 MED 属性が欠落しているパスを最も優先度の低いパスとして設定します。

bgp bestpath med missing-as-worst

ポリシー リストの設定

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理されます。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。ここでは、ポリシー リストを設定するために必要な手順について説明します。

手順

ステップ 1 BGP ポリシーリストを作成します。

policy-list *policy_list_name* {**permit** | **deny**}

permit キーワードを指定すると、条件が一致した場合にアクセスが許可されます。

deny キーワードを指定すると、条件が一致した場合にアクセスが拒否されます。

例：

```
ciscoasa(config)# policy-list Example-policy-list1 permit
```

ステップ 2 指定したいずれかのインターフェイスの外部にネクスト ホップを持つルートを配布します。

match interface [*interface_name* [*interface_name*] […]]

例：

```
ciscoasa(config-policy-list)# match interface outside
```

ステップ 3 宛先アドレス、ネクスト ホップ ルータ アドレス、ルータ/アクセス サーバ ソースのいずれかまたはすべてを一致させてルートを再配布します。

match ip {**address** | **next-hop** | **route-source**}

ステップ 4 BGP 自律システム パスを一致させます。

match as-path

ステップ 5 BGP コミュニティを一致させます。

match community {*community-list_name* | **exact-match**}

- *community-list_name* ：1 つ以上のコミュニティ リスト。
- **exact-match**：完全一致が必要であることを示します。指定されたすべてのコミュニティのみが存在する必要があります。

例：

```
ciscoasa(config-policy-list)# match community ExampleCommunity1
```

ステップ 6 指定したメトリックを持つルートを再配布します。

match metric *metric* [*metric* […]]

ステップ 7 指定されたタグと一致するルーティング テーブルのルートを再配布します。

match tag *tag* [*tag* […]]

AS パス フィルタの設定

AS パス フィルタで、アクセス リストを使用してルーティング アップデート メッセージをフィルタリングし、アップデート メッセージ内の個々のプレフィックスを確認できます。アップデート メッセージ内のプレフィックスがフィルタ基準に一致すると、フィルタ エントリで実行するように設定されているアクションに応じて、個々のプレフィックスは除外されるか受け入れられます。ここでは、AS パス フィルタを設定するために必要な手順について説明します。

（注） AS パス アクセス リストは、通常のファイアウォール ACL とは異なります。

手順

グローバル コンフィギュレーション モードで正規表現を使用して自律システム パス フィルタを設定します。

as-path access-list acl-number {permit|deny} regexp

例：

```
ciscoasa(config)# as-path access-list 35 permit testaspath
```

- *acl-number*：AS パス アクセスリストの番号。有効な値は、1 ～ 500 です。
- regexp：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。

コミュニティ ルールの設定

コミュニティは、共通するいくつかの属性を共有する宛先のグループです。コミュニティ リストを使用すると、ルート マップの match 句で使用されるコミュニティ グループを作成できます。アクセス リストと同様に、一連のコミュニティ リストを作成できます。ステートメントは一致が見つかるまでチェックされ、1 つのステートメントが満たされると、テストは終了します。ここでは、コミュニティ ルールを設定するために必要な手順について説明します。

手順

BGP コミュニティ リストを作成または設定して、そのリストへのアクセスを制御します。

community-list {standard| community list-name {deny|permit} [community-number] [AA:NN] [internet] [no-advertise][no-export]}| {expanded|expanded list-name {deny| permit}regexp}

例：

```
ciscoasa(config)# community-list standard excomm1 permit 100 internet no-advertise
no-export
```

- standard：1 ～ 99 の数字を使用して標準のコミュニティ リストを設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- （オプション）community-number：1 ～ 4294967200 の 32 ビットの数値で表わされたコミュニティ。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
- AA:NN：4 バイトの新コミュニティ形式で入力された自律システム番号およびネットワーク番号。この値は、コロンで区切られた 2 バイトの数 2 つで設定されます。2 バイトの数ごとに 1 ～ 65535 の数を入力できます。1 つのコミュニティ、または複数のコミュニティをそれぞれスペースで区切って入力できます。
- （オプション）internet：インターネット コミュニティを指定します。このコミュニティのルートは、すべてのピア（内部および外部）にアドバタイズされます。
- （オプション）no-advertise：no-advertise コミュニティを指定します。このコミュニティのあるルートはピア（内部または外部）にはアドバタイズされません。

- （オプション）no-export：no-export コミュニティを指定します。このコミュニティのあるルートは、同じ自律システム内のピアへのみ、または連合内の他のサブ自律システムへのみアドバタイズされます。これらのルートは外部ピアにはアドバタイズされません。
- （オプション）expanded：100 ～ 500 の拡張コミュニティ リスト番号を設定し、1 つ以上の許可または拒否コミュニティ グループを識別します。
- regexp：AS パス フィルタを定義する正規表現。自律システム番号は 1 ～ 65535 の範囲で表します。

（注）
正規表現を使用できるのは拡張コミュニティ リストだけです。

IPv4 アドレス ファミリの設定

BGP の IPv4 設定は、BGP 設定セットアップ内の IPv4 ファミリ オプションから指定できます。IPv4 ファミリ セクションには、一般設定、集約アドレスの設定、フィルタリング設定、ネイバー 設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv4 ファミリに固有のパラメータをカスタマイズすることができます。

IPv4 ファミリの一般設定

ここでは、一般的な IPv4 の設定に必要な手順を説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 （オプション）ローカル BGP ルーティング プロセスの固定ルータ ID を設定します。

bgp router-id A.B.C.D

例：

```
ciscoasa(config-router-af)# bgp router-id 10.86.118.3
```

引数 A.B.C.D には、ルータ ID を IP アドレス形式で指定します。ルータ ID を指定しない場合、自動的に割り当てられます。

ステップ 4 （オプション）個別インターフェイス（L3）モードで IP アドレスのクラスタ プールを設定します。

bgp router-id cluster-pool

例：

```
ciscoasa(config-router-af)# bgp router-id cp
```

（注）
L3 クラスタでは、BGP ネイバーをクラスタ プールの IP アドレスの 1 つとして定義できません。

ステップ 5 BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp external-distance internal-distance local-distance

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance：外部 BGP ルートのアドミニストレーティブ ディスタンス。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。
- internal-distance：内部 BGP ルートのアドミニストレーティブ ディスタンス。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。
- local-distance：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 6 BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

table-map {WORD|route-map_name}

例：

```
ciscoasa(config-router-af)# table-map example1
```

引数 route-map_name には route-map コマンドのルート マップ名を指定します。

ステップ 7 BGP ルーティング プロセスを設定し、デフォルト ルート（ネットワーク 0.0.0.0）を配布します。

default-information originate

ステップ 8 ネットワーク レベルのルートへのサブネット ルートの自動集約を設定します。

auto-summary

ステップ 9 ルーティング情報ベース（RIB）にインストールされていないルートのアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 10 BGP と Interior Gateway Protocol（IGP）システム間で同期します。

同期

ステップ 11 OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 12 ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time scanner-interval

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

引数 scanner-interval には BGP ルーティング情報のスキャン間隔を指定します。有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 13 BGP ネクスト ホップ アドレス トラッキングを設定します。

bgp nexthop trigger {delay seconds|enable}

例：

```
ciscoasa(config-router-af)# bgp nexthop trigger delay 15
```

- trigger：BGP ネクスト ホップ アドレス トレッキングの使用を指定します。ネクスト ホップ トラッキングの遅延を変更するには、このキーワードを delay キーワードとともに使用します。ネクスト ホップ アドレス トラッキングを有効にするには、このキーワードを enable キーワードとともに使用します。
- delay：ルーティング テーブルにインストールされている更新済みのネクスト ホップ ルートのチェック間の遅延間隔を変更します。
- seconds：遅延を秒数で指定します。指定できる値の範囲は 0 ～ 100 です。デフォルトは 5 です。
- enable：BGP ネクスト ホップ アドレス トラッキングをすぐに有効化します。

ステップ 14 ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {number_of_paths|ibgp number_of_paths}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

（注）
ibgp キーワードを使用しない場合、number_of_paths 引数は、並列 EBGP ルートの最大数を制御します。

number_of_paths 引数には、ルーティング テーブルにインストールするルートの数を指定します。有効な値は、1 ～ 8 です。

IPv4 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP データベースで集約エントリを作成します。

aggregate-address address mask [as-set][summary-only][suppress-map map-name][advertise-map map-name][attribute-map map-name]

例：

```
ciscoasa(config-router-af) aggregate-address 10.86.118.0 255.255.255.0 as-set summary-only
 suppress-map example1 advertise-map example1 attribute-map example1
```

- address：集約アドレス。
- mask：集約マスク。
- map-name：ルート マップ。
- （オプション）as-set：自律システムの設定パス情報を生成します。
- （オプション）summary-only：アップデートから固有性の強いルートをすべてフィルタリングします。
- （オプション）Suppress-map map-name：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）Advertise-map map-name：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）Attribute-map map-name：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

IPv4 ファミリのフィルタリング設定

ここでは、着信 BGP アップデートで受信したルートまたはネットワークをフィルタリングするために必要な手順について説明します。

手順

ステップ 1 BGPP ルーティング プロセスを有効にし、ルータ コンフィギュレーション モードを開始します。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [**unicast**]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 着信 BGP アップデートで受信したルータまたはネットワーク、あるいは発信 BGP アップデートでアドバタイズされたルータまたはネットワークをフィルタリングします。

distribute-list *acl-number* {**in** | **out**} [*protocol process-number* | **connected** | **static**]

引数 *acl-number* には、IP アクセス リストの番号を指定します。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。

キーワード **in** はフィルタを着信 BGP アップデートに適用する必要があることを指定し、**out** はフィルタを発信 BGP アップデートに適用する必要があることを指定します。

アウトバウンド フィルタの場合、必要に応じて、配布リストに適用するプロトコル（**bgp**、**eigrp**、**ospf**、または **rip**）をプロセス番号付き（RIP を除く）で指定できます。ピアおよびネットワークが **connected** または **static** ルート経由で学習されたかどうかでフィルタすることもできます。

例：

```
ciscoasa(config-router-af)# distribute-list ExampleAcl in bgp 2
```

IPv4 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 エントリを BGP ネイバー テーブルに追加します。

neighbor ip-address remote-as autonomous-number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remote-as 3
```

ステップ 4 （オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor ip-address shutdown

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 shutdown 3
```

ステップ 5 BGP ネイバーと情報を交換します。

neighbor ip-address activate

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 activate
```

ステップ 6 BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

neighbor ip-address ha-mode graceful-restart [disable]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ha-mode graceful-restart
```

（オプション）disable キーワードを指定すると、ネイバーの BGP グレースフル リスタート機能が無効化されます。

ステップ 7 アクセス リストで指定された BGP ネイバー情報を配布します。

neighbor {ip-address} distribute-list {access-list-name}{in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 distribute-list ExampleAcl in
```

- access-list-number：標準アクセス リストまたは拡張アクセス リストの番号。標準アクセス リストの番号の範囲は 1 ～ 99 です。拡張アクセス リストの番号の範囲は 100 ～ 199 です。
- expanded-list-number：拡張アクセス リストの番号。拡張アクセス リストの範囲は 1300 ～ 2699 です。
- access-list-name：標準アクセス リストまたは拡張アクセス リストの名前。
- prefix-list-name：BGP プレフィックス リストの名前。
- in：アクセス リストはそのネイバーへの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 8 着信ルートまたは発信ルートにルート マップを適用します。

neighbor {ip-address} route-map map-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 route-map example1 in
```

キーワード in を指定すると、ルート マップは着信ルートに適用されます。

キーワード out を指定すると、ルート マップは発信ルートに適用されます。

ステップ 9 プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {ip-address} prefix-list prefix-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 prefix-list NewPrefixList in
```

キーワード in は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード out は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 10 フィルタ リストを設定します。

neighbor {ip-address} filter-list access-list-number {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 filter-list 5 in
```

- access-list-name：自律システム パスのアクセス リストの番号を指定します。ip as-path access-list コマンドを使用して、このアクセス リストを定義します。
- in：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 11 ネイバーから受信できるプレフィックスの数を制御します。

neighbor {ip-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 maximum-prefix 7 75 restart 12
```

- maximum：このネイバーからの許可される最大プレフィックス数。
- （オプション）threshold：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は 1 ～ 100 です。デフォルト値は 75（%）です。
- （オプション）restart interval：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。

- （オプション）warning-only：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 12 BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

neighbor {ip-address} default-originate [route-map map-name]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 default-originate route-map example1
```

引数 map-name は、ルートマップの名前です。ルート マップでは、条件に応じてルート 0.0.0.0 を挿入できます。

ステップ 13 BGP ルーティング アップデートの最小送信間隔を設定します。

neighbor {ip-address} advertisement-interval seconds

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 advertisement-interval 15
```

引数 seconds は時間（秒）です。0 ～ 600 の範囲の値を指定できます。

ステップ 14 設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {ip-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

例：

```
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name：exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップの名前。
- exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される exist-map の名前。
- non-exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される non-exist-map の名前。
- （オプション）check all paths：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックを有効化します。

ステップ 15 プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {ip-address} remove-private-as

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 remove-private-as
```

ステップ 16 特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {ip-address} timers keepalive holdtime min holdtime

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 timers 15 20 12
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効値は、0 ～ 65535 です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- min holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）。

（注）
ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 17 2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {ip-address} password string

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 password test
```

引数 string は大文字と小文字を区別するパスワードで、service password-encryption コマンドが有効化されている場合は最大 25 文字、service password-encryption コマンドが有効化されていない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注）
パスワードの最初の文字を数字にする場合、数字の直後にスペースを入れないでください。つまり、数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 18 BGP ネイバーに送信する Community 属性を指定します。

neighbor {ip-address} send-community

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 send-community
```

ステップ 19 ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

neighbor {ip-address}next-hop-self

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 next-hop-self
```

ステップ 20 直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {ip-address} ebgp-multihop [ttl]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ebgp-multihop 5
```

引数 ttl には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 21 ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。

neighbor {ip-address} disable-connected-check

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 disable-connected-check
```

ステップ 22 BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor ip-addressttl-security hops hop-count

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 hop-count は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効値は 1 ～ 254 です。

ステップ 23 ネイバー接続に重みを割り当てます。

neighbor {ip-address} weight number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 weight 30
```

引数 number は、ネイバー接続に割り当てる重みです。有効値は、0 ～ 65535 です。

ステップ 24 特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {ip-address} version number

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 version 4
```

引数 number には、BGP バージョン番号を指定します。バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

ステップ 25 BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {ip-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 transport path-mtu-discovery
```

- connection-mode：接続のタイプ（active または passive）。
- path-mtu-discovery：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリを有効にします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）disable：TCP パス MTU ディスカバリを無効にします。

ステップ 26 External Border Gateway Protocol（eBGP）ネイバーから受信したルートの AS_path 属性をカスタマイズします。

neighbor {ip-address} local-as [autonomous-system-number[no-prepend]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）autonomous-system-number：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）no-prepend：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

ステップ 27 BGP ネイバーシップの送信元としてインターフェイスを更新する場合：

neighbor *ip_address* **update-source** *interface_name*

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 update-source loop1
```

引数 *interface_name* は、BGP ネイバーが BGP ルーティングの送信元として使用するインターフェイスの名前です。

（注）
BGP ネイバーシップの送信元としてループバック インターフェイスを更新すると、ループバック インターフェイスの IP アドレスがネットワーク全体にアドバタイズされます。ループバック インターフェイスは eBGP ピアとして機能し、ルーティングに参加します。ループバック

インターフェイスは有効にすると安定し、管理上のシャットダウンまで使用可能な状態になるため、ループバック インターフェイスの IP アドレスで常に ASA に到達できます。

IPv4 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。

network {network-number [mask network-mask]}[route-map map-tag]

例：

```
ciscoasa(config-router-af)# network 10.86.118.13 mask 255.255.255.255 route-map example1
```

（注）
ネットワークプレフィックスをアドバタイズするには、デバイスへのルートがルーティングテーブルに存在する必要があります。

- network-number：BGP がアドバタイズするネットワーク。
- （オプション）network-mask：マスク アドレスを持つネットワーク マスクまたはサブネットワーク マスク。

- （オプション）map-tag：設定されているルートマップの ID。ルートマップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

IPv4 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 別のルーティング ドメインから BGP 自律システムにルートを再配布します。

redistribute protocol [process-id] [metric] [route-map [map-tag]]

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol：ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または Static のいずれかを指定できます。
- （オプション）process-id：特定のルーティング プロセスの名前。
- （オプション）metric：再配布されるルートのメトリック。
- （オプション）map-tag：設定されているルート マップの ID。

（注）
ルートマップは、再配布されるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークが再配布されます。

IPv4 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv4 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv4 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv4[unicast]
```

キーワード unicast では、IPv4 ユニキャスト アドレス プレフィックスを指定します。これは、指定されていない場合でもデフォルト値になります。

ステップ 3 BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map inject-map exist-map exist-map [copy-attributes]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
- exist-map：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。

- （オプション）copy-attributes：集約ルートの属性を継承するよう注入されたルートを設定します。

IPv6 アドレス ファミリの設定

BGP の IPv6 設定は、BGP 設定セットアップ内の IPv6 ファミリ オプションから指定できます。IPv6 ファミリ セクションには、一般設定、集約アドレスの設定、ネイバー設定のサブセクションが含まれます。これらの各サブセクションを使用して、IPv6 ファミリに固有のパラメータをカスタマイズすることができます。

ここでは、BGP IPv6 ファミリの設定をカスタマイズする方法について説明します。

IPv6 ファミリの一般設定

ここでは、一般的な IPv6 の設定に必要な手順を説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 BGP ルートのアドミニストレーティブ ディスタンスを設定します。

distance bgp external-distance internal-distance local-distance

例：

```
ciscoasa(config-router-af)# distance bgp 80 180 180
```

- external-distance：外部 BGP ルートのアドミニストレーティブ ディスタンス。外部自律システムから学習されたルートは、外部ルートです。この引数の値の範囲は 1 ～ 255 です。
- internal-distance：内部 BGP ルートのアドミニストレーティブ ディスタンス。ローカル自律システムのピアから学習されたルートは、内部ルートです。この引数の値の範囲は 1 ～ 255 です。

- local-distance：ローカル BGP ルートのアドミニストレーティブ ディスタンス。ローカル ルートは、別のプロセスから再配布されているルータまたはネットワークの、多くの場合バック ドアとして、ネットワーク ルータ コンフィギュレーション コマンドによりリストされるネットワークです。この引数の値の範囲は 1 ～ 255 です。

ステップ 4 （オプション）デフォルト ルート（ネットワーク 0.0.0.0）を配布するように BGP ルーティング プロセスを設定します。

default-information originate

ステップ 5 （オプション）ルーティング情報ベース（RIB）にインストールされていないルートのアドバタイズメントを抑制します。

bgp suppress-inactive

ステップ 6 BGP と Interior Gateway Protocol（IGP）システム間で同期します。

同期

ステップ 7 OSPF などの IGP への iBGP の再配布を設定します。

bgp redistribute-internal

ステップ 8 ネクスト ホップの検証用に BGP ルータのスキャン間隔を設定します。

bgp scan-time scanner-interval

例：

```
ciscoasa(config-router-af)# bgp scan-time 15
```

scanner-interval 引数の有効な値は 5 ～ 60 秒です。デフォルトは 60 秒です。

ステップ 9 ルーティング テーブルにインストールできる並列 iBGP ルートの最大数を制御します。

maximum-paths {number_of_paths|ibgp number_of_paths}

例：

```
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

number_of_paths 引数の有効な値は 1 ～ 8 です。

ibgp キーワードを使用しない場合、number_of_paths 引数は、並列 EBGP ルートの最大数を制御します。

IPv6 ファミリ集約アドレスの設定

ここでは、特定のルートの 1 つのルートへの集約を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 unicast

ステップ 3 BGP データベースで集約エントリを作成します。

aggregate-address ipv6-address/cidr [as-set][summary-only][suppress-map map-name][advertise-map ipv6-map-name][attribute-map map-name]

例：

```
ciscoasa(config-router-af) aggregate-address 2000::1/8 summary-only
```

- address：集約 IPv6 アドレス。
- （オプション）as-set：自律システムの設定パス情報を生成します。
- （オプション）summary-only：アップデートから固有性の強いルートをすべてフィルタリングします。
- （オプション）suppress-map map-name：抑制するルートを選択するために使用するルートマップの名前を指定します。
- （オプション）advertise-map map-name：AS_SET 発信コミュニティを作成するためのルートを選択するために使用するルート マップの名前を指定します。
- （オプション）attribute-map map-name：集約ルートの属性を設定するために使用するルート マップの名前を指定します。

ステップ 4 BGP ルートが集約される間隔を設定します。

bgp aggregate-timer seconds

例：

```
ciscoasa(config-router-af)bgp aggregate-timer 20
```

IPv6 ファミリの BGP ネイバーの設定

ここでは、BGP ネイバーおよびネイバー設定を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ルータをルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 エントリを BGP ネイバー テーブルに追加します。

neighbor ipv6-address remote-as autonomous-number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 remote-as 3
```

引数 ipv6-address には、指定したネットワークに到達するために使用できるネクスト ホップの IPv6 アドレスを指定します。ネクスト ホップの IPv6 アドレスは直接接続しないようにする必要があります。直接接続されたネクスト ホップの IPv6 アドレスを検出するために再帰が実行されるためです。インターフェイス タイプおよびインターフェイス番号を指定すると、パケットの出力先のネクスト ホップの IPv6 アドレスを指定できます（オプション）。リンクローカルアドレスをネクストホップとして使用する場合は、インターフェイス タイプおよびインターフェイス番号を指定する必要があります（また、リンクローカル ネクスト ホップが隣接デバイスである必要があります）。

（注）
この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。

ステップ 4 （オプション）ネイバーまたはピア グループをディセーブルにします。

neighbor ipv6-address shutdown

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 shutdown 3
```

ステップ 5 BGP ネイバーと情報を交換します。

neighbor ipv6-address activate

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 activate
```

ステップ 6 BGP ネイバーの Border Gateway Protocol（BGP）グレースフル リスタート機能をイネーブルまたはディセーブルにします。

neighbor {ip-address} ha-mode graceful-restart [disable]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1/8 ha-mode graceful-restart
```

（オプション）disable キーワードを指定すると、ネイバーの BGP グレースフル リスタート機能が無効化されます。

ステップ 7 着信ルートまたは発信ルートにルート マップを適用します。

neighbor {ipv6-address} route-map map-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 route-map example1 in
```

キーワード in を指定すると、ルート マップは着信ルートに適用されます。

キーワード out を指定すると、ルート マップは発信ルートに適用されます。

ステップ 8 プレフィックス リストで指定された BGP ネイバー情報を配布します。

neighbor {ipv6-address} prefix-list prefix-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 prefix-list NewPrefixList in
```

キーワード in は、プレフィックス リストがそのネイバーからの着信アドバタイズメントに適用されることを意味します。

キーワード out は、プレフィックス リストがそのネイバーへの発信アドバタイズメントに適用されることを意味します。

ステップ 9 フィルタ リストを設定します。

neighbor {ipv6-address} filter-list access-list-name {in|out}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 filter-list 5 in
```

- access-list-name：自律システム パスのアクセス リストの番号を指定します。ip as-path access-list コマンドを使用して、このアクセス リストを定義します。
- in：アクセス リストはそのネイバーからの着信アドバタイズメントに適用されます。
- out：アクセス リストはそのネイバーへの発信アドバタイズメントに適用されます。

ステップ 10 ネイバーから受信できるプレフィックスの数を制御します。

neighbor {ipv6-address} maximum-prefix maximum [threshold][restart restart interval][warning-only]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 maximum-prefix 7 75 restart 12
```

- maximum：このネイバーからの許可される最大プレフィックス数。
- （オプション）threshold：最大数の何パーセントになったらルータが警告メッセージの生成を開始するかを指定する整数。指定できる範囲は1～100です。デフォルト値は75（%）です。
- （オプション）restart interval：BGP ネイバーが再起動するまでの時間を指定する整数値（分）。
- （オプション）warning-only：プレフィックスの最大数を超えた場合に、ピアリングを終了する代わりに、ルータでログ メッセージを生成できます。

ステップ 11 BGP スピーカー（ローカル ルータ）にネイバーへのデフォルト ルート 0.0.0.0 の送信を許可して、このルートがデフォルト ルートとして使用されるようにします。

neighbor {ipv6-address} default-originate [route-map map-name]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 default-originate route-map example1
```

引数 map-name はルート マップの名前です。ルート マップにより、ルート 0.0.0.0 が条件に応じて注入されます。

ステップ 12 BGP ルーティング アップデートの最小送信間隔を設定します。

neighbor {ipv6-address} advertisement-interval seconds

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertisement-interval 15
```

引数 seconds は時間（秒）です。0 ～ 600 の範囲の値を指定できます。

ステップ 13 プライベート自律システム番号を発信ルーティング アップデートから削除します。

neighbor {ipv6-address} remove-private-as

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 remove-private-as
```

ステップ 14 設定されているルート マップと一致する BGP テーブル内のルートをアドバタイズします。

neighbor {ipv6-address} advertise-map map-name {exist-map map-name |non-exist-map map-name}[check-all-paths]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 advertise-map MAP1 exist-map MAP2
```

- advertise-map map name：exist-map または non-exist-map の条件に一致した場合にアドバタイズされるルート マップの名前。
- exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される exist-map の名前。
- non-exist-map map name：advertise-map のルートがアドバタイズされるかどうかを判断するために BGP テーブル内のルートと比較される non-exist-map の名前。
- （オプション）check all paths：BGP テーブル内のプレフィックスを持つ exist-map によるすべてのパスのチェックを有効化します。

ステップ 15 特定の BGP ピアまたは BGP ピア グループのタイマーを設定します。

neighbor {ipv6-address} timers keepalive holdtime min holdtime

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 timers 15 20 12
```

- keepalive：ASA がキープアライブ メッセージをピアに送信する頻度（秒）。デフォルトは 60 秒です。有効値は、0 ～ 65535 です。
- holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの時間（秒）。デフォルト値は 180 秒です。
- min holdtime：キープアライブ メッセージを受信できない状態が継続して、ピアがデッドであると ASA が宣言するまでの最小時間（秒）。

  （注）
  ホールドタイムが 20 秒未満の場合、ピアフラッピングの可能性が高くなります。

ステップ 16 2 つの BGP ピア間の TCP 接続で Message Digest 5（MD5）認証をイネーブルにします。

neighbor {ipv6-address} password string

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 password test
```

引数 string は大文字と小文字を区別するパスワードで、service password-encryption コマンドが有効化されている場合は最大25 文字、service password-encryption コマンドが有効化されていない場合は最大 81 文字を指定できます。この文字列には、スペースも含め、あらゆる英数字を使用できます。

（注）
パスワードの最初の文字を数字にする場合、数字の直後にスペースを入れないでください。つまり、数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。

ステップ 17 BGP ネイバーに送信する Community 属性を指定します。

neighbor {ipv6-address} send-community [standard]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 send-community
```

（オプション）standard キーワード：標準コミュニティのみ送信されます。

ステップ 18 ルータを BGP スピーキング ネイバーまたはピア グループのネクスト ホップとして設定します。

neighbor {ipv6-address}next-hop-self

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 next-hop-self
```

ステップ 19 直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor {ipv6-address} ebgp-multihop [ttl]

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 ebgp-multihop 5
```

引数 ttl には、1 ～ 255 ホップの範囲の存続可能時間を指定します。

ステップ 20 ループバック インターフェイスを使用するシングル ホップ ピアと eBGP ピアリング セッションを確立するための接続確認をディセーブルにします。

neighbor {ipv6-address} disable-connected-check

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 disable-connected-check
```

ステップ 21 BGP ピアリング セッションを保護し、2 つの外部 BGP （eBGP）ピアを区切るホップの最大数を設定します。

neighbor {ipv6-address} ttl-security hops hop-count

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 ttl-security hops 15
```

引数 hop-count は、eBGP ピアを区切るホップの数です。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。有効値は 1 ～ 254 です。

ステップ 22 ネイバー接続に重みを割り当てます。

neighbor {ipv6-address} weight number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 weight 30
```

引数 number は、ネイバー接続に割り当てる重みです。有効値は、0 ～ 65535 です。

ステップ 23 特定の BGP バージョンだけを受け入れるように ASA を設定します。

neighbor {ipv6-address} version number

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 version 4
```

引数 number には、BGP バージョン番号を指定します。デフォルトはバージョン 4 です。現在は、BGP バージョン 4 のみがサポートされます。

ステップ 24 BGP セッションの TCP トランスポート セッション オプションをイネーブルにします。

neighbor {ipv6-address} transport {connection-mode{active|passive}| path-mtu-discovery[disable]}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 transport connection-mode active
```

- connection-mode：接続のタイプ（active または passive）。
- path-mtu-discovery：TCP トランスポート パスの最大伝送ユニット（MTU）ディスカバリを有効にします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
- （オプション）disable：TCP パス MTU ディスカバリを無効にします。

ステップ 25 External Border Gateway Protocol（eBGP）ネイバーから受信したルートの AS_path 属性をカスタマイズします。

neighbor {ipv6-address} local-as [autonomous-system-number[no-prepend]]

例：

```
ciscoasa(config-router-af)# neighbor 10.86.118.12 local-as 5 no-prepend replace-as
```

- （オプション）autonomous-system-number：AS_path 属性の前に追加する自律システムの番号。この引数の値の範囲は、1 ～ 4294967295 または 1.0 ～ XX.YY の有効な任意の自律システム番号です。
- （オプション）no-prepend：eBGP ネイバーから受信したルートの前にローカル自律システム番号を追加しません。

注意
BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。このコマンドは、自律システムの移行のためだけに設定する必要があり、遷移が完了した後設定解除する必要があります。この手順は、経験豊富なネットワーク オペレータだけが行うべきものです。不適切な設定によってルーティング ループが作成される可能性があります。

ステップ 26 BGP ネイバーシップの送信元としてインターフェイスを更新する場合：

neighbor {ipv6-address} update-source {interface name}

例：

```
ciscoasa(config-router-af)# neighbor 2000::1 update-source loop1
```

引数 interface name は、BGP ネイバーが BGP ルーティングの送信元として使用するインターフェイスの名前を指定します。

（注）
BGP ネイバーシップの送信元としてループバック インターフェイスを更新すると、ループバック インターフェイスの IP アドレスがネットワーク全体にアドバタイズされます。ループバック インターフェイスは eBGP ピアとして機能し、ルーティングに参加します。ループバック インターフェイスは有効にすると安定し、管理上のシャットダウンまで使用可能な状態になるため、ループバック インターフェイスの IP アドレスで常に ASA に到達できます。

IPv6 ネットワークの設定

ここでは、BGP ルーティング プロセスによってアドバタイズされるネットワークを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp *autonomous-num*

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

ステップ 3 BGP ルーティング プロセスによってアドバタイズされるネットワークを指定します。

network {*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] | *ipv6_prefix*/*prefix_length*} [**route-map** *route_map_name*]

例：

```
ciscoasa(config-router-af)# network 2001:1/64 route-map test_route_map
ciscoasa(config-router-af)# network outside-prefix 1::/64
ciscoasa(config-router-af)# network outside-prefix 2::/64
```

- *prefix_delegation_name*：DHCPv6 プレフィクス委任クライアント（**ipv6 dhcp client pd**）を有効にすると、プレフィックスをアドバタイズできます。プレフィックスをサブネット化するには、*subnet_prefix*/*prefix_length* を指定します。
- *ipv6 network*/*prefix_length*：BGP がアドバタイズするネットワーク。
- （オプション）**route-map** *name*：設定されているルート マップの ID。ルート マップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。

IPv6 再配布の設定

ここでは、別のルーティング ドメインから BGP にルートを再配布する条件を定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6[unicast]
```

ステップ 3 別のルーティング ドメインから BGP 自律システムにルートを再配布します。

```
redistribute protocol [process-id][autonomous-num][metric metric value][match{internal|
 external1|external2|NSSA external 1|NSSA external 2}][route-map [map-tag]][subnets]
```

例：

```
ciscoasa(config-router-af)# redistribute ospf 2 route-map example1 match external
```

- protocol：ルートの再配布元となるソース プロトコル。Connected、EIGRP、OSPF、RIP または Static のいずれかを指定できます。
- （オプション）process-id：OSPF プロトコルの場合は、ルートの再配布元となる適切な OSPF プロセス ID です。この値により、ルーティング プロセスを識別します。この値は 0 以外の 10 進数で指定します。

  （注）
  この値は、その他のプロトコルでは自動入力されます。

- （オプション）metric metric value：同じルータ上で 1 つの OSPF プロセスから別の OSPF プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPF プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。デフォルト値は 0 です
- （オプション）match internal | external1 | external2 | NSSA external 1 | NSSA external 2：OSPF ルートが他のルーティング ドメインに再配布される条件を表します。次のいずれかを指定できます。
  - internal：特定の自律システムの内部にあるルート。
  - external 1：自律システムの外部だが、BGP に OSPF タイプ 1 外部ルートとしてインポートされるルート。
  - external 2：自律システムの外部だが、BGP に OSPF タイプ 2 外部ルートとしてインポートされるルート。
  - NSSA external 1：自律システムの外部だが、BGP に OSPF NSSA タイプ 1 外部ルートとしてインポートされるルート。
  - NSSA external 2：自律システムの外部だが、BGP に OSPF NSSA タイプ 2 外部ルートとしてインポートされるルート。
- （オプション）map-tag：設定されているルート マップの ID。

（注）

ルートマップは、再配布されるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークが再配布されます。

IPv6 ルート注入の設定

ここでは、条件に応じて BGP ルーティング テーブルに注入されるルートを定義するために必要な手順について説明します。

手順

ステップ 1 BGP ルーティング プロセスをイネーブルにし、ASA をルータ コンフィギュレーション モードにします。

router bgp autonomous-num

例：

```
ciscoasa(config)# router bgp 2
```

ステップ 2 アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6 [unicast]
```

ステップ 3 BGP ルーティング テーブルに固有性の強いルートを注入するよう条件付きルート注入を設定します。

bgp inject-map inject-map exist-map exist-map [copy-attributes]

例：

```
ciscoasa(config-router-af)# bgp inject-map example1 exist-map example2 copy-attributes
```

- inject-map：ローカル BGP ルーティング テーブルに注入するプレフィックスを指定するルート マップの名前。
- exist-map：BGP スピーカーが追跡するプレフィックスを含むルート マップの名前。
- （オプション）copy-attributes：集約ルートの属性を継承するよう注入されたルートを設定します。

BGP のモニタリング

次のコマンドを使用して、BGP ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな BGP ルーティング統計情報をモニターするには、次のコマンドの 1 つを入力します。

- **show bgp** [ip-address [mask [longer-prefixes [injected] | shorter-prefixes [length]]]| prefix-list name | route-map name]

  BGP ルーティング テーブル内のエントリを表示します。

- **show bgp** cidr-only

  ナチュラル ネットワーク マスク以外を使用するルート（つまり、クラスレス ドメイン間ルーティング（CIDR））を表示します。

- **show bgp community community-number [exact-match][no-advertise][no-export]**

  指定された BGP コミュニティに属するルートを表示します。

- **show bgp community-list community-list-name [exact-match]**

  BGP コミュニティ リストによって許可されたルートを表示します。

- **show bgp filter-list** *access-list-number*

  指定されたフィルタ リストと一致するルートを表示します。

- **show bgp injected-paths**

  BGP ルーティング テーブルに注入されたすべてのパスを表示します。

- **show bgp ipv4 unicast**

  ユニキャスト セッションの IPv4 BGP ルーティング テーブルのエントリを表示します。

- show bgp ipv6 unicast

  IPv6 の Border Gateway Protocol（BGP）ルーティング テーブルのエントリを表示します。

- show bgp ipv6 community

  指定された IPv6 Border Gateway Protocol（BGP）コミュニティに属するルートを表示します。

- show bgp ipv6 community-list

  IPv6 Border Gateway Protocol（BGP）コミュニティ リストによって許可されたルートを表示します。

- show bgp ipv6 filter-list

  指定された IPv6 フィルタ リストと一致するルートを表示します。

- show bgp ipv6 inconsistent-as

  整合性のない発信自律システムを使用している IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 neighbors

  ネイバーへの IPv6 Border Gateway Protocol（BGP）接続に関する情報を表示します。

- show bgp ipv6 paths

  データベース内のすべての IPv6 Border Gateway Protocol（BGP）パスを表示します。

- show bgp ipv6 prefix-list

  プレフィックス リストに一致するルートを表示します。

- show bgp ipv6 quote-regexp

  自律システム パスの正規表現と一致する IPv6 Border Gateway Protocol（BGP）ルートを引用符で囲まれた文字列として表示します。

- show bgp ipv6 regexp

  自律システム パスの正規表現と一致する IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 route-map

  ルーティング テーブルにインストールできなかった IPv6 Border Gateway Protocol（BGP）ルートを表示します。

- show bgp ipv6 summary

  すべての IPv6 Border Gateway Protocol（BGP）接続のステータスを表示します。

- show bgp neighbors ip_address

  ネイバーに対する BGP 接続と TCP 接続に関する情報を表示します。

- show bgp paths [LINE]

  データベース内のすべての BGP パスを表示します。

- show bgp pending-prefixes

  削除が保留されているプレフィックスを表示します。

- show bgp prefix-list prefix_list_name [WORD]

  指定のプレフィックス リストに一致するルートを表示します。

- show bgp regexp regexp

  自律システム パスの正規表現と一致するルートを表示します。

- show bgp replication [index-group | ip-address]

  BGP アップデート グループのアップデートのレプリケーション統計情報を表示します。

- show bgp rib-failure

ルーティング情報ベース（RIB）テーブルにインストールできなかったBGPルートを表示します。

- show bgp route-map map-name

  指定されたルート マップに基づいて、BGP ルーティング テーブルのエントリを表示します。

- show bgp summary

  すべての BGP 接続のステータスを表示します。

- show bgp system-config

  マルチ コンテキスト モードでシステム コンテキスト固有の BGP 設定を表示します。

  このコマンドは、マルチ コンテキスト モードのすべてのユーザー コンテキストで使用できます。

- show bgp update-group

  BGP アップデート グループに関する情報を表示します。

（注） BGP ログ メッセージを無効にするには、ルータ コンフィギュレーション モードで **no bgp log-neighbor-changes** コマンドを入力します。これにより、ネイバー変更メッセージのロギングが無効になります。BGP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。デフォルトでは、ネイバー変更はログに記録されます。

BGP の例

次の例に、さまざまなオプションのプロセスを使用して BGPv4 をイネーブルにし、設定する方法を示します。

1. ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap2 permit 10
```

2. 指定されたアクセス リストのいずれかによって渡されるルートアドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

3. ポリシー ルーティング用のルートマップのmatch節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ip next-hop peer address
```

4. グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

5. アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 remote-as 65
```

7. 着信ルートまたは発信ルートにルート マップを適用します。

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 route-map mymap2 in
```

8. BGP スピーキングネイバーの送信元としてインターフェイスを更新する場合：

```
ciscoasa(config-router-af)# neighbor 10.108.0.0 update-source loop1
```

次の例に、さまざまなオプションのプロセスを使用して BGPv6 を有効にし、設定する方法を示します。

1. ルーティング プロトコル間のルートの再配布に対する条件を定義します。または、ポリシー ルーティングをイネーブルにします。

```
ciscoasa(config)# route-map mymap1 permit 10
```

2. 指定されたアクセス リストのいずれかによって渡されるルート アドレスまたは一致パケットを持つルートを再配布します。

```
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

3. ポリシー ルーティング用のルート マップの match 節を通過したパケットの送出先を指定します。

```
ciscoasa(config-route-map)# set ipv6 next-hop peer address
```

4. グローバル コンフィギュレーション モードで BGP ルーティング プロセスをイネーブルにします。

```
ciscoasa(config)# router bgp 2
```

5. アドレス ファミリ コンフィギュレーション モードでローカル Border Gateway Protocol（BGP）ルーティング プロセスの固定ルータ ID を設定します。

```
ciscoasa(config)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 19.168.254.254
```

6. アドレス ファミリ コンフィギュレーション モードを開始し、標準 IPv6 アドレス プレフィックスを使用するルーティング セッションを設定します。

```
address-family ipv6 [unicast]
```

7. エントリを BGP ネイバー テーブルに追加します。

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 remote-as 64600
```

8. 着信ルートまたは発信ルートにルート マップを適用します。

```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 route-map mymap1 in
```

9. BGP スピーキング ネイバーの送信元としてインターフェイスを更新する場合：

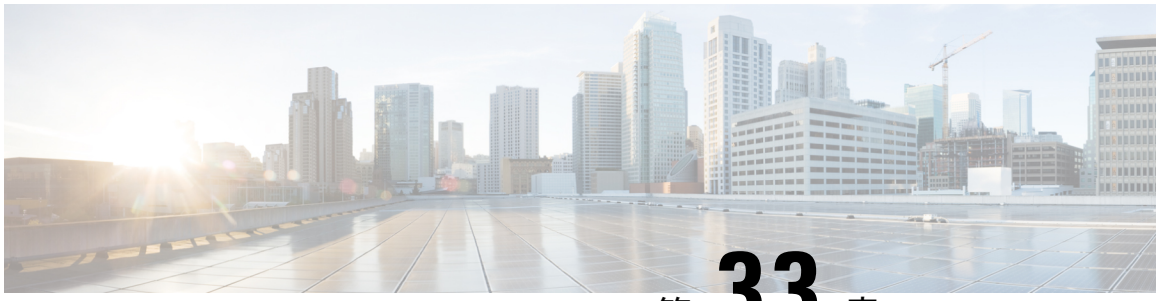
```
ciscoasa(config-router-af)# neighbor 2001:DB8:0:CC00::1 update-source loop1
```

BGP の履歴

表 *41 : BGP* の各機能の履歴

機能名	プラットフォーム リリース	機能情報
BGP のサポート	9.2(1)	Border Gateway Protocol を使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。 次のコマンドが導入されました。**router bgp**、**bgp maxas-limitbgp maxas-limit**、**bgp log-neighbor-changes**、**bgp transport path-mtu-discovery**、**bgp fast-external-fallover**、**bgp enforce-first-as**、**bgp asnotation dot**、**timers bgp**、**bgp default local-preference**、**bgp always-compare-med**、**bgp bestpath compare-routerid**、**bgp deterministic-med**、**bgp bestpath med missing-as-worst**、**policy-list**、**match as-path**、**match community**、**match metric**、**match tag**、**as-path access-list**、**community-list**、**address-family ipv4**、**bgp router-id**、**distance bgp**、**table-map**、**bgp suppress-inactive**、**bgp redistribute-internal**、**bgp scan-time**、**bgp nexthop**、**aggregate-address**、**neighbor**、**bgp inject-map**、**show bgp**、**show bgp cidr-only**、**show bgp all community**、**show bgp all neighbors**、**show bgp community**、**show bgp community-list**、**show bgp filter-list**、**show bgp injected-paths**、**show bgp ipv4 unicast**、**show bgp neighbors**、**show bgp paths**、**show bgp pending-prefixes**、**show bgp prefix-list**、**show bgp regexp**、**show bgp replication**、**show bgp rib-failure**、 **show bgp route-map**、**show bgp summary**、**show bgp system-config**、**show bgp update-group**、**clear route network**、**maximum-path**、 **network**。 次のコマンドが変更されました。**show route**、**show route summary**、**show running-config router**、**clear config router**、**clear route all**、**timers lsa arrival**、**timers pacing**、**timers throttle**、**redistribute bgp**。
ASA クラスタリングに対する BGP のサポート	9.3(1)	L2 および L3 クラスタリングのサポートが追加されました。 次のコマンドが導入されました。bgp router-id clusterpool

機能名	プラットフォーム リリース	機能情報
ノンストップ フォワーディングに対する BGP のサポート	9.3(1)	ノンストップ フォワーディングのサポートが追加されました。 次のコマンドが導入されました。bgp graceful-restart、neighbor ha-mode graceful-restart
アドバタイズされたマップに対する BGP のサポート	9.3(1)	アドバタイズされたマップに対する BGPv4 のサポートが追加されました。 次のコマンドが導入されました。neighbor advertise-map
IPv6 に対する BGP のサポート	9.3(2)	IPv6 のサポートが追加されました。 次のコマンドが導入されました。address-family ipv6、ipv6 prefix-list、ipv6 prefix-list description、ipv6 prefix-list sequence-number、match ipv6 next-hop、match ipv6 route-source、match ipv6- address prefix-list、set ipv6-address prefix -list、set ipv6 next-hop、set ipv6 next-hop peer-address 次のコマンドが変更されました。bgp router-id
委任プレフィックスの IPv6 ネットワーク アドバタイズメント	9.6(2)	ASA は DHCPv6 プレフィックスの委任クライアントをサポートするようになりました。ASA は DHCPv6 サーバーから委任プレフィックスを取得します。ASA は、これらのプレフィックスを使用して他の ASA インターフェイスのアドレスを設定し、ステートレス アドレス自動設定（SLAAC）クライアントが同じネットワーク上で IPv6 アドレスを自動設定できるようにします。これらのプレフィックスをアドバタイズするように BGP ルータを設定できます。 次のコマンドが変更されました。**network**
BGP トラフィックのループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、BGP トラフィックに使用できるようになりました。 新規/変更されたコマンド：**interface loopback**、**neighbor update-source**
IPv6 のグレースフル リスタート	9.19(1)	IPv6 アドレス ファミリのグレースフル リスタート サポートを追加しました。



第 33 章

Open Shortest Path First（OSPF）

この章では、Open Shortest Path First（OSPF）ルーティング プロトコルを使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように ASA を設定する方法について説明します。

- OSPF について （1241 ページ）
- OSPF のガイドライン （1245 ページ）
- OSPFv2 の設定 （1249 ページ）
- OSPFv2 ルータ ID の設定 （1253 ページ）
- OSPF fast hello パケットの設定 （1254 ページ）
- OSPFv2 のカスタマイズ （1255 ページ）
- OSPFv3 の設定 （1272 ページ）
- グレースフル リスタートの設定 （1295 ページ）
- OSPFv2 の例 （1301 ページ）
- OSPFv3 の例 （1302 ページ）
- OSPF のモニタリング （1303 ページ）
- OSPF の履歴 （1308 ページ）

OSPF について

OSPF は、パスの選択にディスタンス ベクターではなくリンク ステートを使用する Interior Gateway Routing Protocol です。OSPF は、ルーティング テーブル更新ではなく、リンクステート アドバタイズメントを伝達します。ルーティング テーブル全体ではなく LSA だけが交換されるため、OSPF ネットワークは RIP ネットワークよりも迅速に収束します。

OSPF は、リンクステート アルゴリズムを使用して、すべての既知の宛先までの最短パスを構築および計算します。OSPF エリア内の各ルータには、ルータが使用可能なインターフェイスと到達可能なネイバーそれぞれのリストである同一のリンクステート データベースが置かれています。

RIP と比べ OSPF には次の利点があります。

- OSPF では、リンクステート データベースの更新が RIP ほど頻繁に送信されません。また、ステート情報がタイムアウトすると、リンクステート データベースは徐々にではなく、すぐに更新されます。
- ルーティングはコスト、つまり特定のインターフェイスを介してパケットを送信するために必要なオーバーヘッドに基づいて決定されます。ASA は、インターフェイスのコストをリンク帯域幅に基づいて計算し、接続先までのホップ数は使用しません。コストを設定して優先パスを指定することができます。

最短パスを優先するアルゴリズムの欠点は、CPU サイクルとメモリが大量に必要になることです。

ASA は、OSPF プロトコルのプロセスを 2 つ同時に異なるインターフェイス セット上で実行できます。同じ IP アドレスを使用する複数のインターフェイス（NAT ではこのようなインターフェイスが共存可能ですが、OSPF ではアドレスは重複できません）がある場合に、2 つのプロセスを実行できます。あるいは、一方のプロセスを内部で実行しながら別のプロセスを外部で実行し、ルートのサブセットをこの 2 つのプロセス間で再配布することもできます。同様に、プライベート アドレスをパブリック アドレスから分離する必要がある場合もあります。

OSPF ルーティング プロセスには、別の OSPF ルーティング プロセスや RIP ルーティング プロセスから、または OSPF 対応インターフェイスに設定されているスタティック ルートおよび接続ルートから、ルートを再配布できます。

ASA では、次の OSPF の機能がサポートされています。

- エリア内ルート、エリア間ルート、および外部ルート（タイプ I とタイプ II）。
- 仮想リンク。
- LSA フラッディング。
- OSPF パケットの認証（パスワード認証と MD5 認証の両方）。
- ASA の代表ルータまたはバックアップ代表ルータとしての設定。ASA は、ABR として設定することもできます。
- スタブ エリアと Not-So-Stubby Area。
- エリア境界ルータのタイプ 3 LSA フィルタリング。

OSPF は、MD5 およびクリア テキスト ネイバー認証をサポートします。OSPF と他のプロトコル（RIP など）の間のルート再配布にあたっては、攻撃者によるルーティング情報の悪用の可能性があるため、できる限りすべてのルーティング プロトコルで認証を行う必要があります。

NAT を使用していて、OSPF がパブリック エリアおよびプライベート エリアで動作している場合、またアドレス フィルタリングが必要な場合は、2 つの OSPF プロセス（1 つはパブリック エリア用、1 つはプライベート エリア用）を実行する必要があります。

複数のエリアにインターフェイスを持つルータは、エリア境界ルータ（ABR）と呼ばれます。ゲートウェイとして動作し、OSPF を使用しているルータと他のルーティング プロトコルを使用しているルータの間でトラフィックを再配布するルータは、自律システム境界ルータ（ASBR）と呼ばれます。

ABR は LSA を使用して、使用可能なルートに関する情報を他の OSPF ルータに送信します。ABR タイプ 3 LSA フィルタリングを使用して、ABR として機能する ASA により、プライベートエリアとパブリック エリアを分けることができます。タイプ 3 LSA（エリア間ルート）は、プライベート ネットワークをアドバタイズしなくても NAT と OSPF を一緒に使用できるように、1 つのエリアから他のエリアにフィルタリングできます。

（注） フィルタリングできるのはタイプ 3 LSA のみです。プライベート ネットワーク内の ASBR として設定されている ASA は、プライベート ネットワークを記述するタイプ 5 LSA を送信しますが、これは AS 全体（パブリック エリアも含む）にフラッディングされます。

NAT が採用されているが、OSPF がパブリック エリアだけで実行されている場合は、パブリック ネットワークへのルートを、デフォルトまたはタイプ 5 AS 外部 LSA としてプライベート ネットワーク内で再配布できます。ただし、ASA により保護されているプライベート ネットワークにはスタティック ルートを設定する必要があります。また、同一の ASA インターフェイス上で、パブリック ネットワークとプライベート ネットワークを混在させることはできません。

ASA では、2 つの OSPF ルーティング プロセス（1 つの RIP ルーティング プロセスと 1 つの EIGRP ルーティング プロセス）を同時に実行できます。

fast hello パケットに対する OSPF のサポート

fast hello パケットに対する OSPF のサポートには、1 秒未満のインターバルで hello パケットの送信を設定する方法が用意されています。このような設定により、Open Shortest Path First（OSPF）ネットワークでのコンバージェンスがより迅速になります。

Fast Hello パケットに対する OSPF サポートの前提条件

OSPF がネットワークですでに設定されているか、Fast Hello パケット機能向けの OSPF のサポートと同時に設定される必要があります。

fast hello パケットに対する OSPF のサポートについて

次に、fast hello パケットに関する OSPF のサポートと、OSPF fast hello パケットの利点について説明します。

OSPF Hello インターバルと dead 間隔

OSPF hello パケットとは、OSPF プロセスがネイバーとの接続を維持するために OSPF ネイバーに送信するパケットです。hello パケットは、設定可能なインターバル（秒単位）で送信されます。デフォルトのインターバルは、イーサネット リンクの場合 10 秒、ブロードキャスト以外のリンクの場合 30 秒です。hello パケットには、dead 間隔中に受信したすべてのネイバーのリストが含まれます。dead 間隔も設定可能なインターバル（秒単位）で送信されます。デフォルトは Hello インターバルの値の 4 倍です。Hello インターバルの値は、ネットワーク内ですべて

同一にする必要があります。dead 間隔の値も、ネットワーク内ですべて同一にする必要があります。

この 2 つのインターバルは、リンクが動作していることを示すことにより、接続を維持するために連携して機能します。ルータが dead 間隔内にネイバーから hello パケットを受信しない場合、ルータはこのネイバーがダウンしていると判定します。

OSPF fast hello パケット

OSPF fast hello パケットとは、1 秒よりも短い間隔で送信される hello パケットのことです。fast hello パケットを理解するには、OSPF hello パケット インターバルと dead 間隔との関係についてあらかじめ理解しておく必要があります。OSPF Hello インターバルと dead 間隔 （1243 ページ）を参照してください。

OSPF fast hello パケットは、ospf dead-interval コマンドで設定されます。dead 間隔は 1 秒に設定され、hello-multiplier の値は、その 1 秒間に送信する hello パケット数に設定されるため、1 秒未満の「fast」hello パケットになります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる Hello インターバルは 0 に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

OSPF Fast Hello パケットの利点

OSPF Fast Hello パケット機能を利用すると、ネットワークがこの機能を使用しない場合よりも、コンバージェンス時間が短くなります。この機能によって、失われたネイバーを 1 秒以内に検出できるようになります。この機能は、ネイバーの損失がオープン システム相互接続（OSI）物理層またはデータリンク層で検出されないことがあっても、特に LAN セグメントで有効です。

OSPFv2 および OSPFv3 間の実装の差異

OSPFv3 には、OSPFv2 との後方互換性はありません。OSPF を使用して、IPv4 および IPv6 トラフィックの両方をルーティングするには、OSPFv2 および OSPFv3 の両方を同時に実行する必要があります。これらは互いに共存しますが、相互に連携していません。

OSPFv3 では、次の追加機能が提供されます。

- リンクごとのプロトコル処理。
- アドレッシング セマンティックの削除。
- フラッディング スコープの追加。
- リンクごとの複数インスタンスのサポート。
- ネイバー探索およびその他の機能に対する IPv6 リンクローカル アドレスの使用。

- プレフィックスおよびプレフィックス長として表される LSA。
- 2 つの LSA タイプの追加。
- 未知の LSA タイプの処理。
- RFC-4552 で指定されている OSPFv3 ルーティング プロトコル トラフィックの IPsec ESP 標準を使用する認証サポート。

OSPF のガイドライン

コンテキスト モードのガイドライン

OSPFv2 は、シングル コンテキスト モードとマルチ コンテキスト モードをサポートしています。

- デフォルトでは、共有インターフェイス間でのマルチキャスト トラフィックのコンテキスト間交換がサポートされていないため、OSPFv2 インスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、OSPFv2 プロセスの OSPFv2 プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの OSPFv2 ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 OSPFv2 がサポートされています。

（ポイントツーポイント トポロジの場合） マルチ コンテキスト モードでは、スタティック OSPFv2 ネイバーを設定して、ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズできます。OSPF 隣接関係を正常に形成するには、共有インターフェイスの OSPF を削除して再設定するときに、次の順序でコマンドを実行します。

- `no router <ospf name>` を使用して OSPF 設定を削除します。その後、 `no ospf network point-to-point non-broadcast` を使用して、インターフェイスの OSPF ポイントツーポイント 非ブロードキャスト設定を削除します。
- 共有インターフェイスで OSPF を再設定する場合は、 `router <ospf name>` を使用して OSPF ルータを設定します。次に `ospf network point-to-point non-broadcast` でインターフェイスを設定します。

OSPFv3 は、シングル モードのみをサポートしています。

キー チェーン認証のガイドライン

OSPFv2 は、単一モードと複数モードの両方で、物理モードでも、仮想モードでも、キーチェーンの認証をサポートしています。ただし、複数モードでキーチェーンが設定できるのはコンテキスト モードのみです。

- 循環キーは OSPFv2 プロトコルにのみ適用されます。キー チェーンを使用した OSPF エリア認証はサポートされていません。

- OSPFv2 内に時間範囲がない既存の MD5 認証も、新しい循環キーとともにサポートされています。
- プラットフォームは SHA1 と MD5 の暗号化アルゴリズムをサポートしていますが、認証には MD5 暗号化アルゴリズムのみが使用されます。

ファイアウォール モードのガイドライン

OSPF は、ルーテッド ファイアウォール モードのみをサポートしています。OSPF は、トランスペアレント ファイアウォール モードをサポートしません。

フェールオーバー ガイドライン

OSPFv2 および OSPFv3 は、ステートフル フェールオーバー をサポートしています。

IPv6 のガイドライン

- OSPFv2 は IPv6 をサポートしません。
- OSPFv3 は IPv6 をサポートしています。
- OSPFv3 は、IPv6 を使用して認証を行います。
- ASA は、OSPFv3 ルートが最適なルートの場合、IPv6 RIB にこのルートをインストールします。
- OSPFv3 パケットは、**capture** コマンドの IPv6 ACL を使用してフィルタリングで除外できます。

OSPFv3 Hello パケットと GRE

通常、OSPF トラフィックは GRE トンネルを通過しません。IPv6 の OSPFv3 が GRE 内でカプセル化されている場合、マルチキャスト宛先などのセキュリティチェックで IPv6 ヘッダー検証が失敗します。このパケットは、宛先が IPv6 マルチキャストであるため、暗黙的なセキュリティチェックの検証でドロップされます。

GRE トラフィックをバイパスするプレフィルタルールを定義できます。ただし、プレフィルタルールでは、内部パケットはインスペクションエンジンによって問い合わせられません。

クラスタリングのガイドライン

- OSPFv3 暗号化はサポートされていません。クラスタリング環境で OSPFv3 暗号化を設定しようとすると、エラー メッセージが表示されます。
- スパンド インターフェイス モードでは、ダイナミック ルーティングは管理専用インターフェイスではサポートされません。
- 個別インターフェイスモードで、OSPFv2 または OSPFv3 ネイバーとして制御ユニットおよびデータユニットが確立されていることを確認します。

- 個別インターフェイスモードでは、OSPFv2 との隣接関係は、制御ユニットの共有インターフェイスの 2 つのコンテキスト間でのみ確立できます。スタティック ネイバーの設定は、ポイントツーポイン リンクでのみサポートされます。したがって、インターフェイスで許可されるのは 1 つのネイバー ステートメントだけです。
- クラスタで制御ロールの変更が発生した場合、次の挙動が発生します。
  - スパンド インターフェイス モードでは、ルータプロセスは制御ユニットでのみアクティブになり、データユニットでは停止状態になります。コンフィギュレーションが制御ユニットと同期されているため、各クラスタユニットには同じルータ ID があります。その結果、隣接ルータはロール変更時のクラスタのルータ ID の変更を認識しません。
  - 個別インターフェイス モードでは、ルータ プロセスはすべての個別のクラスタ ユニットでアクティブになります。各クラスタ ユニットは設定されたクラスタ プールから独自の個別のルータ ID を選択します。クラスタで制御ロールが変更されても、ルーティングトポロジは変更されません。

マルチプロトコル ラベル スイッチング（MPLS）と OSPF のガイドライン

MPLS 設定ルータから送信されるリンク ステート（LS）アップデート パケットに、Opaque Type-10 リンクステート アドバタイズメント（LSA）が含まれており、この LSA に MPLS ヘッダーが含まれている場合、認証は失敗し、アプライアンスはアップデート パケットを確認せずにサイレントにドロップします。ピア ルータは確認応答を受信していないため、最終的にネイバー関係を終了します。

ネイバー関係の安定を維持するため、ASA の Opaque 機能を無効にします。

```
router ospf process_ID_number
no nsf ietf helper
no capability opaque
```

（注） Firepower 4100/9300 モデルでは、複数の受信キュー間のロードバランシング不足のため、MPLS を使用した際に遅延が大きくなる可能性があります。

双方向フォワーディング検出（BFD）および OSPF に関する注意事項

- OSPFv2 および OSPFv3 インターフェイス（物理インターフェイス、サブインターフェイス、およびポートチャネル）で BFD を有効にできます。
- BFD は、VTI トンネル、DVTI トンネル、ループバック、スイッチポート、VNI、VTEP、および IRB インターフェイスではサポートされません。

ルートの再配布のガイドライン

- IPv4 プレフィックス リストを使用した OSPFv2 でのルートマップの再配布はサポートされています。ただし、IPv6 プレフィックス リストを使用した OSPFv3 でのルートマップ

の再配布はサポートされていません。再配布には、OSPF のルートマップでアクセス リストを使用します。

- OSPF が、EIGRP ネットワークの一部であるデバイスで設定されている場合、またはその逆の場合は、ルートにタグを付けるように OSPF ルータが設定されていることを確認します（EIGRP はルートタグをまだサポートしていません）。

  OSPF を EIGRP に再配布し、EIGRP を OSPF に再配布する場合は、いずれかのリンクまたはインターフェイスで障害が発生したときや、ルート発信元がダウンしたときにも、ルーティングループが発生します。あるドメインから同じドメインに再度ルートを再配布することを避けるため、ルータは、再配布する際にドメインに属しているルートにタグ付けすることができます。そして、そのタグに基づいて、リモートルータでそれらのルートをフィルタ処理できます。それらのルートはルーティングテーブルにインストールされないため、再度同じドメインに再配布されることはありません。

その他のガイドライン

- OSPFv2 および OSPFv3 は 1 つのインターフェイス上での複数インスタンスをサポートしています。
- OSPFv3 は、非クラスタ環境での ESP ヘッダーを介した暗号化をサポートしています。
- OSPFv3 は非ペイロード暗号化をサポートします。
- OSPFv2 は RFC 4811、4812 および 3623 でそれぞれ定義されている、Cisco NSF グレースフル リスタートおよびIETF NSF グレースフル リスタート メカニズムをサポートします。
- OSPFv3 は RFC 5187 で定義されているグレースフル リスタート メカニズムをサポートします。
- 配布可能なエリア内（タイプ 1）ルートの数は限られています。これらのルートでは、1 つのタイプ 1 LSA にすべてのプレフィックスが含まれています。システムではパケット サイズが 35 KB に制限されているため、3000 ルートの場合、パケットがこの制限を超過します。2900 本のタイプ 1 ルートが、サポートされる最大数であると考えてください。
- ルートアップデートがリンク上の最小 MTU より大きい場合に、ルートアップデートがドロップされることによる隣接フラップを回避するには、リンクの両側のインターフェイスで同じ MTU を設定する必要があります。
- ASA Virtual は、Azure クラウドルーティングの特性により、EIGRP や OSPF などのダイナミックな内部ルーティングプロトコルを使用できません。有効なルーティング テーブルは、仮想クライアントにスタティック/ダイナミック ルートが設定されているかどうかに関係なく、ネクスト ホップを決定します。

  現在、有効なルーティングテーブルまたはシステム ルーティング テーブルはどちらも表示できません。
- パケット サイズが 8190 を超えた場合、OSPFv3 は LS アップデートをドロップします。その結果、隣接関係は終了します。そのため、「ospfv3 mtu-ignore」コマンドを使用してスイッチを設定し、ネイバーシップの終了を回避します。

OSPFv2 の設定

ここでは、ASA で OSPFv2 プロセスを有効化する方法について説明します。

OSPFv2 をイネーブルにした後、ルート マップを定義する必要があります。詳細については、ルートマップの定義（1177 ページ）を参照してください。その後、デフォルトルートを生成します。詳細については、スタティック ルートの設定（1145 ページ）を参照してください。

OSPFv2 プロセスのルート マップを定義した後で、ニーズに合わせてカスタマイズできます。ASA 上で OSPFv2 プロセスをカスタマイズする方法については、OSPFv2 のカスタマイズ（1255 ページ）を参照してください。

OSPFv2 をイネーブルにするには、OSPFv2 ルーティング プロセスを作成し、このルーティング プロセスに関連付ける IP アドレスの範囲を指定し、さらにその IP アドレスの範囲にエリア ID を割り当てる必要があります。

最大 2 つの OSPFv2 プロセス インスタンスをイネーブルにできます。各 OSPFv2 プロセスには、独自のエリアとネットワークが関連付けられます。

OSPFv2 をイネーブルにするには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ASA 上で OSPF プロセスが 1 つしか有効化されていないと、そのプロセスがデフォルトで選択されます。既存のエリアを編集する場合、OSPF プロセス ID を変更できません。

ステップ 2 OSPF を実行する IP アドレスを定義し、そのインターフェイスのエリア ID を定義します。

network *ip_address mask* **area** *area_id*

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

新しいエリアを追加する場合、そのエリア ID を入力します。このエリア ID には、10 進数か IP アドレスを指定できます。有効な 10 進値の範囲は、0 ～ 4294967295 です。既存のエリアを編集する場合、エリア ID は変更できません。

ステップ 3 すべての OSPFv2 インターフェイスで BFD を有効にするには、次の手順を実行します。

bfd all-interfaces

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# bfd all-interfaces
```

ステップ 4 OSPFv2 をサポートしている特定のインターフェイスで BFD を有効にするには、次の手順を実行します。

bfd interface *interface*

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# bfd interface inside
```

認証用のキー チェーンの設定

デバイスのデータ セキュリティと保護を向上させるため、循環キーを有効にして IGP ピアを認証することができます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

この項では、OSPF ピア認証用のキーチェーンを作成する方法について説明します。キーチェーンオブジェクトを設定した後、それを使用して、インターフェイスおよび仮想リンクの OSPFv2 認証を定義することができます。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキー チェーン）とキー ID を使用します。インターフェイスの認証を定義する方法についてはOSPFv2 インターフェイス パラメータの設定（1259 ページ）を参照してください。。

キー チェーンを設定するには、次のステップを実行します。

手順

ステップ 1 名前を使用してキー チェーンを設定します。

key chain*key-chain-name*

例：

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

これで、キー チェーンの関連パラメータの定義に進むことができます。

ステップ 2 キー チェーンの識別子を設定します。

key*key-id*

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

例：

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

ステップ 3 キー チェーンのキーまたはパスワードを設定します。

key-string [**0** | **8**] *key-string-text*

- 例に示すように、暗号化されていないパスワードが続くことを示すために **0** を使用します。
- 暗号化されたパスワードが続くことを示すには **8** を使用します。
- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

例：

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

ステップ 4 キー チェーンの暗号化アルゴリズムを設定します。

cryptographic-algorithm*md5*

暗号化認証アルゴリズムを指定する必要があります。プラットフォームは SHA1 と MD5 をサポートしていますが、キー チェーン管理でサポートしているのは MD5 のみです。

例：

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

ステップ 5 （オプション）キー チェーンのライフタイムを次のように設定します。

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

別のデバイスとのキー交換時にキーを受け入れるか、または送信するための時間間隔をデバイスに指定できます。終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無限です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、終了ライフタイムよりも前である必要があります。

例：

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

デバイスのスタートアップキー チェーン設定を表示するには、 **show key chain** コマンドを使用します。**show run key chain** コマンドを実行して、デバイスで現在実行されているキー チェーンの設定を表示します。

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#


ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
```

```
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

次のタスク

これで、設定したキーチェーンを適用してインターフェイスのOSPFv2認証を定義できるようになりました。

- OSPFv2 インターフェイス パラメータの設定 （1259 ページ）

OSPFv2 ルータ ID の設定

OSPF ルータ ID は、OSPF データベース内の特定のデバイスを識別するために使用されます。OSPF システム内の 2 台のルータが同じルータ ID を持つことはできません。

ルータ ID が OSPF ルーティングプロセスで手動で設定されていない場合、ルータはアクティブインターフェイスの最も高い IP アドレスから決定されたルータ ID を自動的に設定します。ルータ ID を設定すると、ルータに障害が発生するか、または OSPF プロセスがクリアされ、ネイバー関係が再確立されるまで、ネイバーは自動的に更新されません。

OSPF ルータ ID の手動設定

ここでは、ASA の OSPFv2 プロセスで router-id を手動で設定する方法について説明します。

手順

ステップ 1 固定ルータ ID を使用するには、**router-id** コマンドを使用します。

router-id *ip-address*

例：

```
ciscoasa(config-router)# router-id 193.168.3.3
```

ステップ 2 以前の OSPF ルータ ID の動作に戻すには、**no router-id** コマンドを使用します。

no router-id *ip-address*

例：

```
ciscoasa(config-router)# no router-id 193.168.3.3
```

移行中のルータ ID の挙動

ある ASA、たとえば ASA 1 から別の ASA、たとえば ASA 2 に OSPF 設定を移行すると、次のルータ ID 選択動作が見られます。

1. すべてのインターフェイスがシャットダウン モードの場合、ASA 2 は OSPF router-id に IP アドレスを使用しません。すべてのインターフェイスが「admin down」ステートまたはシャットダウン モードの場合に考えられる router-id の設定は次のとおりです。
   - ASA 2 に以前設定された router-id がない場合は、次のメッセージが表示されます。

     ```
     %OSPF: Router process 1 is not running, please configure a router-id
     ```

     最初のインターフェイスが起動すると、ASA 2 はこのインターフェイスの IP アドレスをルータ ID として取得します。
   - ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときにすべてのインターフェイスが「admin down」ステートになっていた場合、ASA 2 は古いルータ ID を使用します。ASA 2 は、「clear ospf process」コマンドが発行されるまで、起動されたインターフェイスの IP アドレスが変更されても、古いルータ ID を使用します。
2. ASA 2 に router-id が以前設定されていて、「no router-id」コマンドが発行されたときに少なくとも 1 つのインターフェイスが「admin down」ステートまたはシャットダウン モードになっていない場合、ASA 2 は新しいルータ ID を使用します。インターフェイスが「down/down」ステートの場合でも、ASA 2 はインターフェイスの IP アドレスから新しいルータ ID を使用します。

OSPF fast hello パケットの設定

ここでは、OSPF fast hello パケットを設定する方法について説明します。

手順

ステップ 1 インターフェイスを設定します。

interface *port-channel number*

例：

```
ciscoasa(config)# interface port-channel 10
```

number 引数は、ポートチャネル インターフェイスの番号を示します。

ステップ 2 少なくとも 1 個の hello パケットの受信が必要なインターバルを設定します。受信されなければ、ネイバーがダウンしていると判断されます。

ospf dead-interval minimal hello-multiplier *no.of times*

例：

```
ciscoasa(config-if)# ospf dead-interval minimal hell0-multiplier 5
ciscoasa
```

no.of times 引数は、毎秒送信される hello パケットの数を示します。有効な値は、3 ～ 20 です。

ここでは、minimal キーワードおよび hello-multiplier キーワードと値を指定することにより、fast hello パケットに対する OSPF のサポートがイネーブルになっています。multiplier キーワードが 5 に設定されているため、hello パケットが毎秒 5 回送信されます。

OSPFv2 のカスタマイズ

ここでは、OSPFv2 プロセスをカスタマイズする方法について説明します。

OSPFv2 へのルートの再配布

ASA は、OSPFv2 ルーティング プロセス間のルート再配布を制御できます。

（注） 指定されたルーティング プロトコルから、ターゲット ルーティング プロセスに再配布できるルートを定義することでルートを再配布する場合は、デフォルト ルートを最初に生成する必要があります。スタティック ルートの設定（1145 ページ）を参照し、その後にルート マップの定義 （1177 ページ）に従ってルート マップを定義します。

スタティック ルート、接続されているルート、RIP ルート、または OSPFv2 ルートを OSPFv2 プロセスに再配布するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 接続済みルートを OSPF ルーティング プロセスに再配布します。

redistribute connected [[**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute connected 5 type-1 route-map-practice
```

ステップ 3 スタティック ルートを OSPF ルーティング プロセスに再配布します。

redistribute static [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute static subnets
```

このコマンドは、すべてのスタティック ルートを OSPF に渡します。選択的スタティック ルートを再配布するには、スタティック ルートを含むアクセスリストを作成してから、ルートマップに含めてください：

例：

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

ルート マップを作成した後、次のように redistribute コマンドに含めます：

例：

```
ciscoasa(config)#router ospf 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

ステップ 4 ルートを OSPF ルーティング プロセスから別の OSPF ルーティング プロセスに再配布します。

redistribute ospf pid [**match {internal** | **external** [**1** | **2]** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

このコマンドの **match** オプションを使用して、ルート プロパティを照合および設定したり、ルート マップを使用したりできます。**subnets** オプションは、**route-map** コマンドで使用する場合と同じではありません。ルート マップと **redistribute** コマンドの **match** オプションの両方を使用する場合、これらは一致している必要があります。

この例では、ルートをメトリック 1 に照合することによる、OSPF プロセス 1 から OSPF プロセス 2 へのルートの再配布を示しています。ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

ステップ 5 ルートを RIP ルーティング プロセスから OSPF ルーティング プロセスに再配布します。

redistribute rip [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute rip 5
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

ステップ 6 ルートを EIGRP ルーティング プロセスから OSPF ルーティング プロセスに再配布します。

redistribute eigrp as-num [**metric** *metric-value*] [**metric-type** {**type-1** | **type-2**}] [**tag** *tag_value*] [**subnets**] [**route-map** *map_name*]

例：

```
ciscoasa(config)# redistribute eigrp 2
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

OSPFv2 にルートを再配布する場合のルート集約の設定

他のプロトコルからのルートを OSPF に再配布する場合、各ルートは外部 LSA で個別にアドバタイズされます。その一方で、指定したネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのルートをアドバタイズするように ASA を設定することができます。この設定によって OSPF リンクステート データベースのサイズが小さくなります。

指定した IP アドレス マスク ペアと一致するルートは抑制できます。ルート マップで再配布を制御するために、タグ値を一致値として使用できます。

ルート サマリー アドレスの追加

ネットワーク アドレスとマスクに含まれる再配布ルートすべてに対して 1 つのサマリー ルートをアドバタイズするようにソフトウェアを設定するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 サマリー アドレスを設定します。

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

例：

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

この例のサマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンクステート アドバタイズメントでは、アドレス 10.1.0.0 だけがアドバタイズされます。

OSPFv2 エリア間のルート集約の設定

ルート集約は、アドバタイズされるアドレスを統合することです。この機能を実行すると、1 つのサマリー ルートがエリア境界ルータを通して他のエリアにアドバタイズされます。OSPF のエリア境界ルータは、ネットワークをある 1 つのエリアから別のエリアへとアドバタイズしていきます。あるエリアにおいて連続する複数のネットワーク番号が割り当てられている場合、指定された範囲に含まれるエリア内の個別のネットワークをすべて含むサマリー ルートをアドバタイズするようにエリア境界ルータを設定することができます。

ルート集約のアドレス範囲を定義するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成して、この OSPF プロセスのルータ コンフィギュレーション モードを開始します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 アドレス範囲を設定します。

area *area-id* range *ip-address mask* [**advertise** | **not-advertise**]

例：

```
ciscoasa(config-rtr)# area 17 range 12.1.0.0 255.255.0.0
```

この例では、アドレス範囲は OSPF エリア間で設定されます。

OSPFv2 インターフェイス パラメータの設定

必要に応じて一部のインターフェイス固有の OSPFv2 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、**ospf hello-interval**、**ospf dead-interval**、**ospf authentication-key** の各インターフェイス パラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

OSPFv2 インターフェイス パラメータを設定するには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf*process-id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子で、任意の正の整数を使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPF を実行する IP アドレスを定義し、そのインターフェイスのエリア ID を定義します。

network*ip-address mask***area***area-id*

例：

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

ステップ 3 インターフェイス コンフィギュレーション モードを開始します。

interface *interface-name*

例：

```
ciscoasa(config)# interface my_interface
```

ステップ 4 このインターフェイスで BFD をイネーブルにするには、次の手順を実行します。

ospf bfd

例：

```
ciscoasa(config-interface)# ospf bfd
```

ステップ 5 インターフェイスの認証タイプを指定します。

ospf authentication [**key-chain** *key-chain-name* | **message-digest** | **null**]

設定されているキー チェーン名を入力します。キー チェーンの設定については、次を参照してください。 認証用のキー チェーンの設定 （1250 ページ）

例：

```
ciscoasa(config-interface)# ospf authentication message-digest
```

ステップ 6 OSPF 簡易パスワード認証を使用しているネットワーク セグメント上で近接する OSPF ルータが使用するパスワードを割り当てます。

ospf authentication-key*key*

例：

```
ciscoasa(config-interface)# ospf authentication-key cisco
```

key 引数には、最大 8 バイトの連続する文字列が指定できます。

このコマンドで作成するパスワードはキーとして使用され、このキーは ASA のソフトウェアによるルーティング プロトコル パケットの発信時に OSPF ヘッダーに直接挿入されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

ステップ 7 OSPF インターフェイスでパケットを送信するコストを明示的に指定します。

ospf cost*cost*

例：

```
ciscoasa(config-interface)# ospf cost 20
```

cost は、1 ～ 65535 の整数です。

この例では、cost は 20 に設定されています。

ステップ 8 デバイスが hello パケットを受信していないためネイバー OSPF ルータがダウンしていることを宣言するまでデバイスが待機する秒数を設定します。

ospf dead-interval*seconds*

例：

```
ciscoasa(config-interface)# ospf dead-interval 40
```

この値はネットワーク上のすべてのノードで同じにする必要があります。

ステップ 9 ASA が OSPF インターフェイスから hello パケットを送信する時間間隔を指定します。

ospf hello-interval*seconds*

例：

```
ciscoasa(config-interface)# ospf hello-interval 10
```

この値はネットワーク上のすべてのノードで同じにする必要があります。

ステップ 10 OSPF Message Digest 5（MD5）認証を有効にします。

ospf message-digest-key*key-id***md5***key*

例：

```
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
```

次の引数を設定できます。

key-id：1 ～ 255 の範囲の識別子。

key：最大 16 バイトの英数字パスワード

通常は、インターフェイスあたり 1 つのキーを使用して、パケット送信時に認証情報を生成するとともに着信パケットを認証します。隣接ルータの同一キー識別子は、キー値を同一にする必要があります。

1 インターフェイスで 2 つ以上のキーを保持しないことをお勧めします。新しいキーを追加したらその都度古いキーを削除して、ローカル システムが古いキー情報を持つ悪意のあるシステムと通信を続けることのないようにしてください。古いキーを削除すると、ロールオーバー中のオーバーヘッドを減らすことにもなります。

ステップ 11 ネットワークに対して、OSPF で指定されたルータを判別するときに役立つプライオリティを設定します。

ospf priority *number-value*

例：

```
ciscoasa(config-interface)# ospf priority 20
```

number_value 引数の範囲は 0 ～ 255 です。

マルチコンテキストモードでは、共有インターフェイスに0を指定して、デバイスが指定ルータにならないようにします。OSPFv2 インスタンスは、共有インターフェイス間で相互に隣接関係を形成できません。

ステップ 12 OSPF インターフェイスに属する隣接ルータに LSA を再送信する間隔を秒単位で指定します。

ospf retransmit-interval *number-value*

例：

```
ciscoasa(config-interface)# ospf retransmit-interval seconds
```

seconds の値は、接続されているネットワーク上の任意の 2 ルータ間で予想されるラウンドトリップ遅延よりも長い秒数でなければなりません。範囲は1～8192秒です。デフォルト値は5秒です。

ステップ 13 OSPFインターフェイスでリンクステートアップデートパケットを送信するために必要な予想時間を秒単位で設定します。

ospf transmit-delay*seconds*

例：

```
ciscoasa(config-interface)# ospf transmit-delay 5
```

seconds の値は、1 ～ 8192 秒です。デフォルト値は 1 秒です。

ステップ 14 1 秒間に送信される hello パケットの数を設定します。

ospf dead-interval minimal hello-interval multiplier整数

例：

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 6
```

有効な値は 3 ～ 20 の整数です。

ステップ 15 インターフェイスをポイントツーポイントの非ブロードキャストネットワークとして指定します。

ospf network point-to-point non-broadcast

例：

```
ciscoasa(config-interface)# ospf network point-to-point non-broadcast
```

インターフェイスをポイントツーポイントの非ブロードキャストとして指定するには、手動で OSPF ネイバーを定義する必要があります。ダイナミック ネイバー探索はできません。詳細に

ついては、「スタティック OSPFv2 ネイバーの定義（1267 ページ）」を参照してください。さらに、そのインターフェイスに定義できる OSPF ネイバーは 1 つだけです。

OSPFv2 エリア パラメータの設定

複数の OSPF エリア パラメータを設定できます。これらのエリア パラメータ（後述のタスク リストに表示）には、認証の設定、スタブ エリアの定義、デフォルト サマリー ルートへの特定のコストの割り当てがあります。認証では、エリアへの不正アクセスに対してパスワード ベースで保護します。

スタブ エリアは、外部ルートの情報が送信されないエリアです。その代わりに、ABR で生成されるデフォルトの外部ルートがあり、このルートは自律システムの外部の宛先としてスタブ エリアに送信されます。OSPF スタブ エリアのサポートを活用するには、デフォルトのルーティングをスタブ エリアで使用する必要があります。スタブ エリアに送信される LSA の数をさらに減らすには、ABR で実行する **area stub** コマンドの **no-summary** キーワードを使用して、スタブ エリアにサマリー リンク アドバタイズメント（LSA タイプ 3）が送信されないようにします。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPF エリアの認証を有効にします。

area *area-id* authentication

例：

```
ciscoasa(config-rtr)# area 0 authentication
```

ステップ 3 OSPF エリアの MD5 認証を有効にします。

area *area-id* authentication message-digest

例：

```
ciscoasa(config-rtr)# area 0 authentication message-digest
```

OSPFv2 フィルタ ルールの設定

OSPF アップデートで受信または送信されるルートまたはネットワークをフィルタリングするには、次の手順を実行します。

手順

ステップ 1 OSPF ルーティング プロセスを有効にし、ルータ コンフィギュレーション モードを開始します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

ステップ 2 着信 OSPF アップデートで受信したルートまたはネットワーク、あるいは発信 OSPF アップデートでアドバタイズされたルートまたはネットワークをフィルタリングします。

distribute-list *acl-number* **in** [**interface** *ifname*]

distribute-list *acl-number* **out** [*protocol process-number* | **connected** | **static**]

引数 *acl-number* には、IP アクセス リストの番号を指定します。アクセス リストは、ルーティング アップデートで受信されるネットワークと抑制されるネットワークを定義します。

着信アップデートにフィルタを適用するには、**in** を指定します。オプションで、インターフェイスを指定して、そのインターフェイスが受信するアップデートにフィルタを制限することができます。

発信アップデートにフィルタを適用するには、**out** を指定します。必要に応じて、配布リストに適用するプロトコル（**bgp**、**eigrp**、**ospf**、または **rip**）をプロセス番号付き（RIP を除く）で指定できます。ピアおよびネットワークが **connected** または **static** ルート経由で学習されたかどうかでフィルタすることもできます。

例：

```
ciscoasa(config-rtr)# distribute-list ExampleAcl in interface inside
```

OSPFv2 NSSA の設定

NSSA の OSPFv2 への実装は、OSPFv2 のスタブ エリアに似ています。NSSA は、タイプ 5 の外部 LSA をコアからエリアにフラッディングすることはありませんが、自律システムの外部ルートをある限られた方法でエリア内にインポートできます。

NSSA は、再配布によって、タイプ 7 の自律システムの外部ルートを NSSA エリア内部にインポートします。これらのタイプ 7 の LSA は、NSSA の ABR によってタイプ 5 の LSA に変換され、ルーティング ドメイン全体にフラッディングされます。変換中は集約とフィルタリングがサポートされます。

OSPFv2 を使用する中央サイトから異なるルーティング プロトコルを使用するリモート サイトに接続しなければならない ISP またはネットワーク管理者は、NSSA を使用することによって管理を簡略化できます。

NSSA が実装される前は、企業サイトの境界ルータとリモート ルータ間の接続では、OSPFv2 スタブ エリアとしては実行されませんでした。これは、リモート サイト向けのルートは、スタブ エリアに再配布することができず、2 種類のルーティング プロトコルを維持する必要があったためです。RIP のようなシンプルなプロトコルを実行して再配布を処理する方法が一般的でした。NSSA が実装されたことで、企業ルータとリモート ルータ間のエリアを NSSA として定義することにより、NSSA で OSPFv2 を拡張してリモート接続をカバーできます。

この機能を使用する前に、次のガイドラインを参考にしてください。

- 外部の宛先に到達するために使用可能なタイプ 7 のデフォルト ルートを設定できます。設定すると、NSSA または NSSA エリア境界ルータまでのタイプ 7 のデフォルトがルータによって生成されます。
- 同じエリア内のすべてのルータは、エリアが NSSA であることを認識する必要があります。そうでない場合、ルータは互いに通信できません。

手順

ステップ 1 OSPF ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 NSSA エリアを定義します。

area *area-id* nssa [**no-redistribution**] [**default-information-originate**]

例：

```
ciscoasa(config-rtr)# area 0 nssa
```

ステップ 3 サマリー アドレスを設定します。これは、ルーティング テーブルのサイズを小さくするために役立ちます。

summary-address *ip_address mask* [**not-advertise**] [tag *tag*]

例：

```
ciscoasa(config-rtr)# summary-address 10.1.0.0 255.255.0.0
```

OSPF でこのコマンドを使用すると、このアドレスでカバーされる再配布ルートすべての集約として、1 つの外部ルートが OSPF ASBR からアドバタイズされます。

この例のサマリー アドレスの 10.1.0.0 には、10.1.1.0、10.1.2.0、10.1.3.0 などのアドレスが含まれます。外部のリンクステート アドバタイズメントでは、アドレス 10.1.0.0 だけがアドバタイズされます。

（注）
OSPF は summary-address 0.0.0.0 0.0.0.0 をサポートしません。

クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）

個別インターフェイス クラスタリングを使用する場合は、ルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てることができます。

OSPFv2 および OSPFv3 の個別インターフェイス クラスタリングのルータ ID のクラスタ プールの IPv4 アドレスの範囲を割り当てるには、次のコマンドを入力します。

手順

個別インターフェイス クラスタリングのルータ ID のクラスタ プールを指定します。

router-id cluster-pool hostname | A.B.C.D ip_pool

例：

```
hostname(config)# ip local pool rpool 1.1.1.1-1.1.1.4
hostname(config)# router ospf 1
hostname(config-rtr)# router-id cluster-pool rpool
hostname(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
hostname(config-rtr)# log-adj-changes
```

cluster-pool キーワードは、個別インターフェイス クラスタリングが設定されている場合に、IP アドレス プールのコンフィギュレーションをイネーブルにします。**hostname** | **A.B.C.D.** キー

ワードは、この OSPF プロセスの OSPF ルータ ID を指定します。*ip_pool* 引数には、IP アドレス プールの名前を指定します。

（注）
クラスタリングを使用している場合は、ルータ ID の IP アドレス プールを指定する必要はありません。IP アドレス プールを設定しない場合、ASA は自動的に生成されたルータ ID を使用します。

スタティック OSPFv2 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv2 ルートをアドバタイズするには、スタティック OSPFv2 ネイバーを定義する必要があります。この機能により、OSPFv2 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv2 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定（1145 ページ）を参照してください。

手順

ステップ 1 OSPFv2 ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv2 ネイバーフッドを定義します。

neighbor *addr* [**interface** if_name]

例：

```
ciscoasa(config-rtr)# neighbor 255.255.0.0 [interface my_interface]
```

addr 引数には OSPFv2 ネイバーの IP アドレスを指定します。*if_name* 引数は、ネイバーとの通信に使用するインターフェイスです。OSPFv2 ネイバーが直接接続されているインターフェイスのいずれとも同じネットワーク上にない場合、interface を指定する必要があります。

ルート計算タイマーの設定

OSPFv2 によるトポロジ変更受信と最短パス優先（SPF）計算開始との間の遅延時間が設定できます。最初に SPF を計算してから次に計算するまでの保持時間も設定できます。

手順

ステップ 1 OSPFv2 ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ルート計算時間を設定します。

timers throttle spf *spf-start spf-hold spf-maximum*

例：

```
ciscoasa(config-router)# timers throttle spf 500 500 600
```

spf-start 引数は、OSPF によるトポロジ変更受信と SPF 計算開始との間の遅延時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

spf-hold 引数は、2 回の連続する SPF 計算間の最小時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

spf-maximum 引数は、2 回の連続する SPF 計算間の最大時間（ミリ秒）です。0 ～ 600000 の整数に設定できます。

ネイバーの起動と停止のロギング

デフォルトでは、OSPFv2 ネイバーがアップ状態またはダウン状態になったときに、syslog メッセージが生成されます。

アップ状態またはダウン状態になった OSPFv2 ネイバーについて、**debug ospf adjacency** コマンドを実行せずに確認する必要がある場合に、**log-adj-changes** コマンドを設定します。**log-adj-changes** コマンドでは、少ない出力によってピアの関係が高いレベルで表示されます。それぞれの状態変化メッセージを確認するには、**log-adj-changes detail** コマンドを設定します。

手順

ステップ 1 OSPFv2 ルーティング プロセスを作成します。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数が使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 アップ状態またはダウン状態になったネイバーに対するロギングを設定します。

log-adj-changes [**detail**]

認証用のキー チェーンの設定

デバイスのデータ セキュリティと保護を向上させるため、循環キーを有効にして IGP ピアを認証することができます。循環キーは、悪意のあるユーザーがルーティング プロトコル認証に使用されているキーを推測できないようにし、ネットワークによる誤ったルートのアドバタイズやトラフィックのリダイレクトを防ぎます。頻繁にキーを変更することで、推測されるリスクを最終的に軽減します。キー チェーンを提供するルーティング プロトコルの認証を設定する場合は、キー チェーン内でキーを設定してライフタイムを重複させます。こうすることによって、キーで保護された通信がアクティブなキーがないことよって損失することを防ぐために役立ちます。キーのライフタイムが切れ、アクティブなキーがなくなると、OSPF は最後に有効だったキーを使用してピアとの隣接関係を維持します。

この項では、OSPF ピア認証用のキーチェーンを作成する方法について説明します。キーチェーンオブジェクトを設定した後、それを使用して、インターフェイスおよび仮想リンクの OSPFv2 認証を定義することができます。隣接関係を正常に確立するには、ピアに対して同じ認証タイプ（MD5 またはキーチェーン）とキー ID を使用します。インターフェイスの認証を定義する方法についてはOSPFv2 インターフェイス パラメータの設定（1259 ページ）を参照してください。。

キー チェーンを設定するには、次のステップを実行します。

手順

ステップ 1 名前を使用してキー チェーンを設定します。

key chain*key-chain-name*

例：

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)#
```

これで、キー チェーンの関連パラメータの定義に進むことができます。

ステップ 2 キー チェーンの識別子を設定します。

key*key-id*

キー ID の値には 0 ～ 255 を使用できます。無効なキーを通知する場合にのみ、値 0 を使用します。

例：

```
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)#
```

ステップ 3 キー チェーンのキーまたはパスワードを設定します。

key-string [**0** | **8**] *key-string-text*

- 例に示すように、暗号化されていないパスワードが続くことを示すために **0** を使用します。
- 暗号化されたパスワードが続くことを示すには **8** を使用します。
- パスワードの最大長は 80 文字です。
- パスワードは 10 文字以上必要です。また、数字の後に空白を含む文字列は使用できません。たとえば、「0 pass」や「1」は無効です。

例：

```
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)#
```

ステップ 4 キー チェーンの暗号化アルゴリズムを設定します。

cryptographic-algorithm*md5*

暗号化認証アルゴリズムを指定する必要があります。プラットフォームは SHA1 と MD5 をサポートしていますが、キー チェーン管理でサポートしているのは MD5 のみです。

例：

```
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)#
```

ステップ 5 （オプション）キー チェーンのライフタイムを次のように設定します。

accept-lifetime [**local** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

send-lifetime [**ocal** | *start-time*] [**duration** *duration value* | **infinite** | *end-time*]

別のデバイスとのキー交換時にキーを受け入れるか、または送信するための時間間隔をデバイスに指定できます。終了時刻は、期間、受け入れ/送信ライフタイムが終了する絶対時間、または無限です。

次に、開始と終了の値についての検証ルールを示します。

- 終了ライフタイムを指定した場合、開始ライフタイムを null にできません。
- 受け入れまたは送信のライフタイムの開始ライフタイムは、終了ライフタイムよりも前である必要があります。

例：

```
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite
ciscoasa(config-keychain-key)#
```

デバイスのスタートアップキー チェーン設定を表示するには、**show key chain** コマンドを使用します。**show run key chain** コマンドを実行して、デバイスで現在実行されているキー チェーンの設定を表示します。

```
ciscoasa# show key chain
Key-chain CHAIN2:
    key 1 -- text "KEY1CHAIN2"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
  * key 2 -- text "(unset)"
        accept lifetime (11:00:12 UTC Sep 1 2018) - (11:12:12 UTC Sep 1 2018)
        send lifetime (always valid) - (always valid) [valid now]
Key-chain CHAIN1:
    key 1 -- text "CHAIN1KEY1STRING"
        accept lifetime (11:22:33 UTC Sep 1 2018) - (-1 seconds)
        send lifetime (always valid) - (always valid) [valid now]
ciscoasa#


ciscoasa# sh run key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# sh run key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

次のタスク

これで、設定したキーチェーンを適用してインターフェイスのOSPFv2認証を定義できるようになりました。

- OSPFv2 インターフェイス パラメータの設定 （1259 ページ）

OSPFv3 の設定

ここでは、OSPFv3 ルーティング プロセスの設定に関連するタスクについて説明します。

OSPFv3 の有効化

OSPFv3 をイネーブルにするには、OSPFv3 ルーティング プロセスを作成し、OSPFv3 用のエリアを作成して、OSPFv3 のインターフェイスをイネーブルにする必要があります。その後、ターゲットの OSPFv3 ルーティング プロセスにルートを再配布する必要があります。

手順

ステップ 1 OSPFv3 ルーティング プロセスを作成します。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 引数は、このルーティング プロセス内部で使用されるタグです。任意の正の整数が使用できます。このタグは内部専用のため、他のどのデバイス上のタグとも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 インターフェイスをイネーブルにします。

interface *interface_name*

例：

```
ciscoasa(config)# interface Gigabitethernet0/0
```

ステップ 3 特定のプロセス ID を持つ OSPFv3 ルーティング プロセスおよび指定したエリア ID を持つ OSPFv3 のエリアを作成します。

ipv6 ospf *process-id* **area** *area_id*

例：

```
ciscoasa(config)# ipv6 ospf 200 area 100
```

OSPFv3 インターフェイス パラメータの設定

必要に応じて特定のインターフェイス固有の OSPFv3 パラメータを変更できます。これらのパラメータを必ずしも変更する必要はありませんが、hello interval と dead interval というインターフェイスパラメータは、接続されているネットワーク内のすべてのルータで一致している必要があります。これらのパラメータを設定する場合は、ネットワーク上のすべてのルータで、コンフィギュレーションの値が矛盾していないことを確認してください。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 10
```

process-id 引数は、このルーティング プロセス内部で使用されるタグです。任意の正の整数が使用できます。このタグは内部専用のため、他のどのデバイス上のタグとも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 このインターフェイスで BFD をイネーブルにするには、次の手順を実行します。

ipv6 ospf bfd

例：

```
ciscoasa(config-if)# ipv6 ospf bfd
```

ステップ 3 OSPFv3 エリアを作成します。

ipv6 ospf **area** [*area-num*] [**instance**]

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
```

```
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

area-num 引数は、認証がイネーブルになるエリアであり、10 進数値または IP アドレスを指定できます。**instance** キーワードは、インターフェイスに割り当てられるエリア インスタンス ID を指定します。インターフェイスは、OSPFv3 エリアを 1 つだけ保有できます。複数のインターフェイスで同じエリアを使用でき、各インターフェイスは異なるエリア インスタンス ID を使用できます。

ステップ 4 インターフェイス上でパケットを送信するコストを指定します。

ipv6 ospf cost *interface-cost*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
```

interface-cost 引数は、リンクステート メトリックとして表される符号なし整数値を指定します。値の範囲は、1 ～ 65535 です。デフォルトのコストは帯域幅に基づきます。

ステップ 5 OSPFv3 インターフェイスへの発信 LSA をフィルタリングします。

ipv6 ospf database-filter all out

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf database-filter all out
```

デフォルトでは、すべての発信 LSA がインターフェイスにフラッディングされます。

ステップ 6 秒単位で設定する期間内に hello パケットが確認されないと、当該ルータがダウンしていることがネイバーによって示されます。

ipv6 ospf dead-interval *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf dead-interval 60
```

この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 倍です。

ステップ 7 インターフェイスに暗号化タイプを指定します。

ipv6 ospf encryption {**ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [[*key-encryption-type*] *key* | **null**}

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf encryption ipsec spi 1001 esp null sha1 123456789A123456789B123456789C123456789D
```

ipsec キーワードは、IP セキュリティ プロトコルを指定します。**spi** *spi* キーワード引数のペアは、セキュリティ ポリシー インデックスを指定します。値の範囲は 256 ～ 42949667295 である必要があり、10 進数で入力する必要があります。

esp キーワードは、カプセル化セキュリティ ペイロードを指定します。*encryption-algorithm* 引数は、ESP で使用される暗号化アルゴリズムを指定します。有効な値は次のとおりです。

- aes-cdc：AES-CDC 暗号化をイネーブルにします。
- 3des：トリプル DES 暗号化をイネーブルにします。
- des：DES 暗号化をイネーブルにします。
- null：暗号化なしの ESP を指定します。

key-encryption-type 引数に、次の 2 つのうちいずれかの値を指定します。

- 0：キーは暗号化されません。

• 7：キーは暗号化されます。

key 引数は、メッセージ ダイジェストの計算で使用される番号を指定します。この番号の長さは 32 桁の 16 進数（16 バイト）です。キーのサイズは、使用される暗号化アルゴリズムによって異なります。AES-CDC など、一部のアルゴリズムでは、キーのサイズを選択することができます。*authentication-algorithm* 引数は、使用される次のいずれかの暗号化認証アルゴリズムを指定します。

• md5：Message Digest 5（MD5）をイネーブルにします。

• sha1：SHA-1 をイネーブルにします。

null キーワードはエリアの暗号化より優先されます。

インターフェイスで OSPFv3 暗号化が有効化されており、ネイバーが異なるエリア（たとえば、エリア 0）にあり、ASA がそのエリアとの隣接関係を形成する場合は、ASA のエリアを変更する必要があります。ASA のエリアを 0 に変更すると、OSPFv3 の隣接関係が確立される前に 2 分の遅延が発生します。

ステップ 8 インターフェイスに LSA のフラッディング削減を指定します。

ipv6 ospf flood-reduction

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

ステップ 9 インターフェイス上で送信される hello パケット間の間隔（秒数）を指定します。

ipv6 ospf hello-interval *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf hello-interval 15
```

この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。

ステップ 10 DBD パケットを受信した場合の OSPF MTU 不一致検出をディセーブルにします。

ipv6 ospf mtu-ignore

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf mtu-ignore
```

OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。

ステップ 11 ネットワーク タイプに依存するデフォルト以外のタイプに OSPF ネットワーク タイプを設定します。

ipv6 ospf network {**broadcast** | **point-to-point non-broadcast**}

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf network point-to-point non-broadcast
```

point-to-point non-broadcast キーワードは、ネットワーク タイプをポイントツーポイント、非ブロードキャストに設定します。**broadcast** キーワードは、ネットワーク タイプをブロードキャストに設定します。

ステップ 12 ルータ プライオリティを設定します。これは、ネットワークにおける指定ルータの特定に役立ちます。

ipv6 ospf priority *number-value*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
```

```
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf priority 4
```

有効値の範囲は 0 ～ 255 です。

ステップ 13 非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

ステップ 14 インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。

ipv6 ospf retransmit-interval *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-interval 8
```

接続ネットワーク上の任意の2台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。

ステップ 15 インターフェイス上でリンクステート更新パケットを送信する時間を秒単位で設定します。

ipv6 ospf transmit-delay *seconds*

例：

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 10.20.200.30 255.255.255.0 standby 10.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf retransmit-delay 3
```

有効な値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

OSPFv3 ルータ パラメータの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 10
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 エリア パラメータを設定します。

area

例：

```
ciscoasa(config-rtr)# area 10
```

サポートされているパラメータには、0 ～ 4294967295 の 10 進数値のエリア ID、**A.B.C.D** の IP アドレス形式のエリア ID などがあります。

ステップ 3 コマンドをデフォルト値に設定します。

デフォルト

例：

```
ciscoasa(config-rtr)# default originate
```

originate パラメータはデフォルト ルートを配布します。

ステップ 4 デフォルト情報の配布を制御します。

default-information

ステップ 5 ルート タイプに基づいて、OSPFv3 ルート アドミニストレーティブ ディスタンスを定義します。

distance

例：

```
ciscoasa(config-rtr)# distance 200
```

サポートされるパラメータには、1～254 の値のアドミニストレーティブディスタンス、OSPFv3 ディスタンスの **ospf** などがあります。

ステップ 6 ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合に、**lsa** パラメータが指定されている syslog メッセージの送信を抑止します。

ignore

例：

```
ciscoasa(config-rtr)# ignore lsa
```

ステップ 7 OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

log-adjacency-changes

例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail パラメータによって、すべての状態変更がログに記録されます。

ステップ 8 インターフェイスでのルーティング アップデートの送受信を抑止します。

passive-interface [*interface_name*]

例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 引数は、OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。

ステップ 9 あるルーティング ドメインから別のルーティング ドメインへのルートの再配布を設定します。

redistribute {**connected** | **ospf** | **static**}

それぞれの説明は次のとおりです。

- **connected**：接続ルートを指定します。
- **ospf**：OSPFv3 ルートを指定します。
- **static**：スタティック ルートを指定します。

例：

```
ciscoasa(config-rtr)# redistribute ospf
```

ステップ 10 指定したプロセスの固定ルータ ID を作成します。

router-id {*A.B.C.D* | **cluster-pool** | **static**}

それぞれの説明は次のとおりです。

A.B.C.D：IP アドレス形式の OSPF ルータ ID を指定します。

cluster-pool：個別インターフェイス クラスタリングが設定されている場合に、IP アドレス プールを設定します。クラスタリングで使用される IP アドレス プールの詳細については、クラスタリングの IP アドレス プールの設定（OSPFv2 および OSPFv3）（1266 ページ）を参照してください。

例：

```
ciscoasa(config-rtr)# router-id 10.1.1.1
```

ステップ 11 0 ～ 128 の有効な値で IPv6 アドレス サマリーを設定します。

summary-prefix *X:X:X:X::X/*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-router)# router-id 192.168.3.3
ciscoasa(config-router)# summary-prefix FECO::/24
ciscoasa(config-router)# redistribute static
```

X:X:X:X::X/ パラメータは、IPv6 プレフィックスを指定します。

ステップ 12 ルーティング タイマーを調整します。

timers

ルーティング タイマー パラメータは次のとおりです。

- **lsa**：OSPFv3 LSA タイマーを指定します。
- **nsf**：OSPFv3 NSF 待機タイマーを指定します。

- **pacing**：OSPFv3 ペーシング タイマーを指定します。
- **throttle**：OSPFv3 スロットル タイマーを指定します。

例：

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)# timers throttle spf 6000 12000 14000
```

OSPFv3 エリア パラメータの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。

この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 NSSA エリアまたはスタブ エリアのサマリー デフォルト コストを設定します。

area *area-id* **default-cost** *cost*

例：

```
ciscoasa(config-rtr)# area 1 default-cost nssa
```

ステップ 3 アドレスおよび境界ルータ専用のマスクと一致するルートを集約します。

area *area-id* **range** *ipv6-prefix*/ *prefix-length* [**advertise** | **not advertise**] [**cost** *cost*]

例：

```
ciscoasa(config-rtr)# area 1 range FE01:1::1/64
```

- *area-id* 引数は、ルートが集約されているエリアを識別します。値には、10 進数または IPv6 プレフィックスを指定できます。

- *ipv6-prefix* 引数は、IPv6 プレフィックスを指定します。*prefix-length* 引数は、プレフィックス長を指定します。
- **advertise** キーワードは、アドレス範囲ステータスをアドバタイズに設定し、Type 3 サマリー LSA を生成します。
- **not-advertise** キーワードはアドレス範囲ステータスを DoNotAdvertise に設定します。
- Type 3 サマリー LSA は抑制され、コンポーネント ネットワークは他のネットワークから隠された状態のままです。
- **cost** *cost* キーワード引数のペアは、宛先への最短パスを決定するために OSPF SPF 計算で使用されるサマリー ルートのメトリックまたはコストを指定します。
- 有効値の範囲は 0 ～ 16777215 です。

ステップ 4 NSSA エリアを指定します。

area *area-id* **nssa**

例：

```
ciscoasa(config-rtr)# area 1 nssa
```

ステップ 5 スタブ エリアを指定します。

area *area-id* **stub**

例：

```
ciscoasa(config-rtr)# area 1 stub
```

ステップ 6 仮想リンクとそのパラメータを定義します。

area *area-id* **virtual-link** *router-id* [**hello-interval** *seconds*] [**retransmit-interval** *seconds*] [**transmit-delay** *seconds*] [**dead-interval** *seconds*] [**ttl-security hops** *hop-count*]

例：

```
ciscoasa(config-rtr)# area 1 virtual-link 192.168.255.1 hello-interval 5
```

- *area-id* 引数は、ルートが集約されているエリアを識別します。**virtual link** キーワードは、仮想リンク ネイバーの作成を指定します。
- *router-id* 引数は、仮想リンク ネイバーに関連付けられたルータ ID を指定します。
- ルータ ID を表示するには、**show ospf** コマンドまたは **show ipv6 ospf** コマンドを入力します。デフォルト値はありません。
- **hello-interval** キーワードは、インターフェイス上で送信される hello パケット間の時間を秒単位で指定します。hello 間隔は、hello パケットでアドバタイズされる符号なし整数です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サー

バーで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。デフォルトは 10 です。

- **retransmit-interval** *seconds* キーワード引数のペアは、インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。再送信間隔は、接続されているネットワーク上の任意の 2 台のルータ間の予想されるラウンドトリップ遅延です。この値は、予想されるラウンドトリップ遅延より大きくなり、1 ～ 8192 の範囲で指定できます。デフォルトは 5 分です。
- **transmit-delay** *seconds* キーワード引数のペアは、インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を秒単位で設定します。ゼロよりも大きい整数値を指定します。アップデート パケット内の LSA 自体の経過時間は、転送前にこの値の分だけ増分されます。値の範囲は 1 ～ 8192 です。デフォルトは 1 です。
- **dead-interval seconds** キーワード引数のペアは、ルータがダウンしていることをネイバーが示す前に hello パケットを非表示にする時間を秒単位で指定します。Dead 間隔は符号なし整数です。デフォルトは hello 間隔の 4 倍または 40 秒です。この値は、共通のネットワークに接続されているすべてのルータおよびアクセス サーバーで同じであることが必要です。有効値の範囲は 1 ～ 8192 です。
- **ttl-security hops** キーワードは仮想リンクの存続可能時間（TTL）セキュリティを設定します。*hop-count* 引数の値は 1 ～ 254 の範囲で指定できます。

OSPFv3 受動インターフェイスの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process_id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 インターフェイスでのルーティング アップデートの送受信を抑止します。

passive-interface [*interface_name*]

例：

```
ciscoasa(config-rtr)# passive-interface inside
```

interface_name 引数は、OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。*no interface_name* 引数を指定すると、OSPFv3 プロセス *process_id* のすべてのインターフェイスがパッシブとなります。

OSPFv3 アドミニストレーティブ ディスタンスの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process_id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 ルートのアドミニストレーティブ ディスタンスを設定します。

distance [**ospf** {**external** | **inter-area** | **intra-area**}] *distance*

例：

```
ciscoasa(config-rtr)# distance ospf external 200
```

ospf キーワードは、OSPFv3 ルートを指定します。**external** キーワードは、OSPFv3 の外部タイプ 5 およびタイプ 7 ルートを指定します。**inter-area** キーワードは、OSPVv3 のエリア間ルートを指定します。**intra-area** キーワードは、OSPFv3 のエリア内ルートを指定します。*distance* 引数は、10 ～ 254 の整数であるアドミニストレーティブ ディスタンスを指定します。

OSPFv3 タイマーの設定

OSPFv3 の LSA 到着タイマー、LSA ペーシング タイマー、およびスロットリング タイマーを設定できます。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ASAが OSPF ネイバーから同一の LSA を受け入れる最小間隔を設定します。

timers lsa arrival *milliseconds*

例：

```
ciscoasa(config-rtr)# timers lsa arrival 2000
```

milliseconds 引数は、ネイバーから到着する同じ LSA の受け入れの間で経過する最小遅延をミリ秒単位で指定します。有効な範囲は 0 ～ 6,000,000 ミリ秒です。デフォルトは 1000 ミリ秒です。

ステップ 3 LSA フラッド パケット ペーシングを設定します。

timers pacing flood *milliseconds*

例：

```
ciscoasa(config-rtr)# timers lsa flood 20
```

milliseconds 引数は、フラッディング キュー内の LSA が更新と更新の間にペーシングされる時間（ミリ秒）を指定します。設定できる範囲は 5 ～ 100 ミリ秒です。デフォルト値は、33 ミリ秒です。

ステップ 4 OSPFv3 LSA を収集してグループ化し、リフレッシュ、チェックサム、またはエージングを行う間隔を変更します。

timers pacing lsa-group *seconds*

例：

```
ciscoasa(config-rtr)# timers pacing lsa-group 300
```

seconds 引数は、LSA がグループ化、リフレッシュ、チェックサム計算、またはエージングされる間隔を秒単位で指定します。有効な範囲は 10 ～ 1800 秒です。デフォルト値は 240 秒です。

ステップ 5 LSA 再送信パケット ペーシングを設定します。

timers pacing retransmission *milliseconds*

例：

```
ciscoasa(config-rtr)# timers pacing retransmission 100
```

milliseconds 引数は、再送信キュー内の LSA がペーシングされる時間（ミリ秒）を指定します。設定できる範囲は 5 ～ 200 ミリ秒です。デフォルト値は 66 ミリ秒です。

ステップ 6 OSPFv3 LSA スロットリングを設定します。

timers throttle lsa *milliseconds1 milliseconds2 milliseconds3*

例：

```
ciscoasa(config-rtr)# timers throttle lsa 500 6000 8000
```

- *milliseconds1* 引数は、LSA の最初のオカレンスを生成する遅延をミリ秒単位で指定します。*milliseconds2* 引数は、同じ LSA を送信する最大遅延をミリ秒単位で指定します。*milliseconds3* 引数は、同じ LSA を送信する最小遅延をミリ秒単位で指定します。
- LSA スロットリングでは、最小時間または最大時間が最初のオカレンスの値よりも小さい場合、OSPFv3 が自動的に最初のオカレンス値に修正します。同様に、指定された最遅延が最小遅延よりも小さい場合、OSPFv3 が自動的に最小遅延値に修正します。
- *milliseconds1* の場合、デフォルト値は 0 ミリ秒です。
- *milliseconds2* および *milliseconds3* の場合、デフォルト値は 5000 ミリ秒です。

ステップ 7 OSPFv3 SPF スロットリングを設定します。

timers throttle spf *milliseconds1 milliseconds2 milliseconds3*

例：

```
ciscoasa(config-rtr)# timers throttle spf 5000 12000 16000
```

- *milliseconds1* 引数は、SPF 計算の変更を受信する遅延をミリ秒単位で指定します。*milliseconds2* 引数は、最初と 2 番目の SPF 計算の間の遅延をミリ秒単位で指定します。*milliseconds3* 引数は、SPF 計算の最大待機時間をミリ秒単位で指定します。
- SPF スロットリングでは、*milliseconds2* または *milliseconds3* が *milliseconds1* よりも小さい場合、OSPFv3 が自動的に *milliseconds1* の値に修正します。同様に、*milliseconds3* が *milliseconds2* より小さい場合、OSPFv3 が自動的に *milliseconds2* の値に修正します。
- *milliseconds1* の場合、SPF スロットリングのデフォルト値は 5000 ミリ秒です。

- *milliseconds2* および *milliseconds3* の場合、SPF スロットリングのデフォルト値は 10000 ミリ秒です。

スタティック OSPFv3 ネイバーの定義

ポイントツーポイントの非ブロードキャスト ネットワークを介して OSPFv3 ルートをアドバタイズするには、スタティック OSPF ネイバーを定義する必要があります。この機能により、OSPFv3 アドバタイズメントを GRE トンネルにカプセル化しなくても、既存の VPN 接続でブロードキャストすることができます。

開始する前に、OSPFv3 ネイバーに対するスタティック ルートを作成する必要があります。スタティック ルートの作成方法の詳細については、スタティック ルートの設定（1145ページ）を参照してください。

手順

ステップ 1 OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始します。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter all out**]

例：

```
ciscoasa(config-if)# interface ethernet0/0 ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

OSPFv3 デフォルト パラメータのリセット

OSPFv3 パラメータをデフォルト値に戻すには、次の手順を実行します。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 オプションのパラメータをデフォルト値に戻します。

default [**area** | **auto-cost** | **default-information** | **default-metric** | **discard-route** | **discard-route** | **distance** | **distribute-list** | **ignore** | **log-adjacency-changes** | **maximum-paths** | **passive-interface** | **redistribute** | **router-id** | **summary-prefix** | **timers**]

例：

```
ciscoasa(config-rtr)# default metric 5
```

- **area** キーワードは、OSPFv3 エリア パラメータを指定します。**auto-cost** キーワードは、帯域幅に従って OSPFv3 インターフェイス コストを指定します。
- **default-information** キーワードはデフォルト情報を配布します。**default-metric** キーワードは、再配布ルートのメトリックを指定します。
- **discard-route** キーワードは、廃棄ルートのインストールをイネーブルまたはディセーブルにします。**distance** キーワードはアドミニストレーティブ ディスタンスを指定します。
- **distribute-list** キーワードは、ルーティング アップデートのネットワークをフィルタリングします。
- **Ignore** キーワードは、特定のイベントを無視します。**log-adjacency-changes** キーワードは、隣接状態の変更をログに記録します。
- **maximum-paths** キーワードは、複数のパスを介して複数のパケットを転送します。
- **passive-interface** キーワードは、インターフェイス上のルーティング アップデートを抑止します。
- **redistribute** キーワードは、別のルーティング プロトコルからの IPv6 プレフィックスを再配布します。
- **router-id** キーワードは、指定されたルーティング プロセスのルータ ID を指定します。
- **summary-prefix** キーワードは、IPv6 サマリー プレフィックスを指定します。

- **timers** キーワードは、OSPFv3 タイマーを指定します。

Syslog メッセージの送信

OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。

log-adjacency-changes [**detail**]

例：

```
ciscoasa(config-rtr)# log-adjacency-changes detail
```

detail キーワードは、OSPFv3 ネイバーが起動または停止したときだけではなく、各状態の syslog メッセージを送信します。

Syslog メッセージの抑止

ルータがサポートされていない LSA タイプ 6 Multicast OSPF（MOSPF）パケットを受信した場合の syslog メッセージの送信を抑止するには、次の手順を実行します。

手順

ステップ 1 OSPFv2 のルーティング プロセスをイネーブルにします。

router ospf *process_id*

例：

```
ciscoasa(config-if)# router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ルータが、サポートされていない LSA タイプ 6 MOSPF パケットを受信した場合の syslog メッセージの送信を抑止します。

ignore lsa mospf

例：

```
ciscoasa(config-rtr)# ignore lsa mospf
```

集約ルート コストの計算

手順

RFC 1583 に従ってサマリー ルート コストの計算に使用される方式に復元します。

compatible rfc1583

例：

```
ciscoasa (config-rtr)# compatible rfc1583
```

OSPFv3 ルーティング ドメインへのデフォルトの外部ルートの生成

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 OSPFv3 ルーティング ドメインへのデフォルトの外部ルートを生成します。

default-information originate [**always**] **metric** *metric-value* [**metric-type** *type-value*] [**route-map** *map-name*]

例：

```
ciscoasa(config-rtr)# default-information originate always metric 3 metric-type 2
```

- **always** キーワードは、デフォルト ルートがあるかどうかにかかわらず、デフォルト ルートをアドバタイズします。
- **metric** *metric-value* キーワード引数のペアは、デフォルト ルートの生成に使用するメトリックを指定します。
- **default-metric** コマンドを使用して値を指定しない場合、デフォルト値は 10 です。有効なメトリック値の範囲は、0 ～ 16777214 です。
- **metric-type** *type-value* キーワード引数のペアは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプを指定します。有効な値は次のいずれかになります。
  - 1：タイプ 1 外部ルート
  - 2：タイプ 2 外部ルート

  デフォルトはタイプ 2 外部ルートです。
- **route-map** *map-name* キーワード引数のペアは、ルート マップが一致している場合にデフォルト ルートを生成するルーティング プロセスを指定します。

IPv6 サマリー プレフィックスの設定

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 IPv6 サマリー プレフィックスを設定します。

summary-prefix *prefix* [**not-advertise | tag** *tag-value*]

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
ciscoasa(config-rtr)# router-id 192.168.3.3
ciscoasa(config-rtr)# summary-prefix FECO::/24
ciscoasa(config-rtr)# redistribute static
```

prefix 引数は、宛先の IPv6 ルート プレフィックスです。**not-advertise** キーワードは、指定したプレフィックスとマスク ペアと一致するルートを抑止します。このキーワードは OSPFv3 だけに適用されます。**tag** *tag-value* キーワード引数のペアは、ルート マップで再配布を制御するために一致値として使用できるタグ値を指定します。このキーワードは OSPFv3 だけに適用されます。

IPv6 ルートの再配布

手順

ステップ 1 OSPFv3 のルーティング プロセスをイネーブルにします。

ipv6 router ospf *process-id*

例：

```
ciscoasa(config-if)# ipv6 router ospf 1
```

process-id 引数は、このルーティング プロセス内部で使用される識別子です。ローカルに割り当てられ、1 ～ 65535 の任意の正の整数を指定できます。この ID は内部管理専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 ある OSPFv3 プロセスから別の OSPFv3 プロセスに IPv6 ルートを再配布します。

redistribute *source-protocol* [*process-id*] [**include-connected** {[**level-1** | **level-2**}] [*as-number*] [**metric** [*metric-value* | **transparent**}] **[metric-type** *type-value*] [**match** {**external** [**1**|**2**] | **internal** | **nssa-external** [**1**|**2**]}] [**tag** *tag-value*] [**route-map** *map-tag*]

例：

```
ciscoasa(config-rtr)# redistribute connected 5 type-1
```

- *source-protocol* 引数は、ルートの再配布元となるソース プロトコルを指定します。これは、スタティック、接続済み、または OSPFv3 にすることができます。
- *process-id* 引数は、OSPFv3 ルーティング プロセスがイネーブルになったときに管理目的で割り当てられる番号です。
- **include-connected** キーワードは、ソース プロトコルから学習したルートと、ソース プロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲットプロトコルが再配布できるようにします。
- **level-1** キーワードは、Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
- **level-1-2** キーワードは、IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに再配布されることを指定します。
- **level-2** キーワードは、IS-IS 用に、レベル 2 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
- **metric** *metric-value* キーワード引数のペアでは、ある OSPFv3 プロセスのルートを同じルータ上の別の OSPFv3 プロセスに再配布する場合、メトリック値を指定しないと、メトリックは 1 つのプロセスから他のプロセスへ存続します。他のプロセスを OSPFv3 プロセスに再配布するときに、メトリック値を指定しない場合、デフォルトのメトリックは 20 です。
- **metric transparent** キーワードにより、RIP は RIP メトリックとして再配布ルートのルーティング テーブル メトリックを使用します。
- **metric-type** *type-value* キーワード引数のペアは、OSPFv3 ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられる外部リンク タイプを指定します。有効な値は、タイプ 1 外部ルートの場合は 1、タイプ 2 外部ルートの場合は 2 です。**metric-type** キーワードに値が指定されていない場合、ASA は、タイプ 2 外部ルートを受け入れます。IS-IS の場合、リンク タイプは、63 未満の IS-IS メトリックの場合は内部、64 を超えて 128 未満の IS-IS メトリックの場合は外部となります。デフォルトは、内部です。
- **match** キーワードは、他のルーティング ドメインにルートを再配布し、次のいずれかのオプションとともに使用されます。自律システムの外部であり、タイプ 1 またはタイプ 2 の外部ルートとして OSPFv3 にインポートされるルートの場合は **external** [**1**|**2**]、特定の自律システムの内部にあるルートの場合は **internal**、自律システムの外部であり、タイプ 1 またはタイプ 2 の外部ルートとして IPv6 の NSSA で OSPFv3 にインポートされるルートの場合は **nssa-external** [**1**|**2**]。
- **tag** *tag-value* キーワード引数のペアは、ASBR 間で情報を通信するために使用できる、各外部ルートに付加される 32 ビットの 10 進数値を指定します。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用されます。その他のプロトコルについては、ゼロが使用されます。有効値の範囲は、0 ～ 4294967295 です。

- **route-map** キーワードは、送信元ルーティング プロトコルから現在のルーティング プロトコルへのルートのインポートのフィルタリングをチェックするルート マップを指定します。このキーワードを指定しない場合、すべてのルートが再配布されます。このキーワードを指定し、ルート マップ タグが表示されていない場合、ルートはインポートされません。*map-tag* 引数は、設定されたルート マップを識別します。

グレースフル リスタートの設定

ASA では、既知の障害状況が発生することがあります。これにより、スイッチング プラットフォーム全体でパケット転送に影響を与えることがあってはなりません。Non-Stop Forwarding（NSF）機能では、ルーティング プロトコル情報を復元している間に、既知のルートへのデータ転送が続行されます。

ハイアベイラビリティモードでは、アクティブユニットが非アクティブになり、スタンバイユニットが新しいアクティブになると、OSPF プロセスが再起動します。同様に、クラスタモードでは、制御ユニットが非アクティブになり、データユニットが新しい制御ユニットとして選択されると、OSPF プロセスが再起動します。このような OSPF 移行プロセスでは、かなりの遅延が発生します。OSPF プロセスの状態変更時のトラフィック損失を回避するように NSF を設定できます。また NSF 機能は、スケジュール済みヒットレス ソフトウェア アップグレードがあるときに便利です。

グレースフル リスタートは、OSPFv2 と OSPFv3 の両方でサポートされています。NSF Cisco（RFC 4811 および RFC 4812）または NSF IETF（RFC 3623）のいずれかを使用して、OSPFv2 上でグレースフル リスタートを設定できます。graceful-restart（RFC 5187）を使用して、OSPFv3 上でグレースフル リスタートを設定できます。

NSF グレースフル リスタート機能の設定には、機能の設定と NSF 対応または NSF 認識としてのデバイスの設定という 2 つのステップが伴います。NSF 対応デバイスは、ネイバーに対して独自のリスタート アクティビティを示すことができ、NSF 認識デバイスはネイバーのリスタートをサポートすることができます。

デバイスは、いくつかの条件に応じて、NSF 対応または NSF 認識として設定できます。

- デバイスは、現在のデバイスのモードに関係なく、NSF 認識デバイスとして設定できます。
- デバイスを NSF 対応として設定するには、デバイスはフェールオーバーまたはスパンド EtherChannel（L2）クラスタ モードのいずれかである必要があります。
- デバイスを NSF 認識または NSF 対応にするには、必要に応じて opaque リンク ステート アドバタイズメント（LSA）/リンク ローカル シグナリング（LLS）ブロックの機能を使って設定する必要があります。

（注） OSPFv2 用に fast hello が設定されている場合、アクティブ ユニットのリロードが発生し、スタンバイ ユニットがアクティブになっても、グレースフル リスタートは発生しません。これは、ロール変更にかかる時間は、設定されているデッド インターバルよりも大きいためです。

機能の設定

Cisco NSF グレースフル リスタート メカニズムは、リスタート アクティビティを示すために、Hello パケットで RS ビットが設定された LLS ブロックを送信するため、LLS 機能に依存しています。IETF NSF メカニズムは、リスタート アクティビティを示すために、タイプ 9 の opaque LSA を送信するため、opaque LSA 機能に依存しています。機能を設定するには、次のコマンドを入力します。

手順

ステップ 1 OSPF ルーティング プロセスを作成し、再配布する OSPF プロセスのルータ コンフィギュレーション モードに入ります。

router ospf *process_id*

例：

```
ciscoasa(config)# router ospf 2
```

process_id 引数は、このルーティング プロセス内部で使用される識別子です。任意の正の整数を使用できます。この ID は内部専用のため、他のどのデバイス上の ID とも照合する必要はありません。最大 2 つのプロセスが使用できます。

ステップ 2 LLS データ ブロックまたは opaque LSA の使用をイネーブルにして、NSF をイネーブルにします。

capability {lls|opaque}

lls キーワードは、Cisco NSF グレースフル リスタート メカニズムに対して、LLS 機能をイネーブルにするために使用されます。

opaque キーワードは、IETF NSF グレースフル リスタート メカニズムに対して、opaque LSA 機能をイネーブルにするために使用されます。

OSPFv2 のグレースフル リスタートの設定

OSPFv2、Cisco NSF および IETF NSF には、2 つのグレースフル リスタート メカニズムがあります。OSPF インスタンスに対しては、これらのグレースフル リスタート メカニズムのうち一

度に設定できるのは 1 つだけです。NSF 認識デバイスは、Cisco NSF ヘルパーと IETF NSF ヘルパーの両方として設定できますが、NSF 対応デバイスはOSPF インスタンスに対して、Cisco NSF または IETF NSF モードのいずれかとして設定できます。

OSPFv2 の Cisco NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の Cisco NSF グレースフル リスタートを設定します。

手順

ステップ 1 NSF 対応デバイスで Cisco NSF をイネーブルにします。

nsf cisco [enforce global]

例：

```
ciscoasa(config-router)# nsf cisco
```

enforce global キーワードは、非 NSF 認識ネイバー デバイスが検出されると、NSF リスタートをキャンセルします。

ステップ 2 NSF 認識デバイスで、Cisco NSF ヘルパー モードをイネーブルにします。

capability {lls|opaque}

例：

```
ciscoasa(config-router)# capability lls
```

このコマンドは、デフォルトでイネーブルになっています。このコマンドの no 形式を使用すると、ディセーブルになります。

OSPFv2 の IETF NSF グレースフル リスタートの設定

NSF 対応または NSF 認識デバイスに対して、OSPFv2 の IETF NSF グレースフル リスタートを設定します。

手順

ステップ 1 NSF 対応デバイスで IETF NSF を有効にします。

nsf ietf [restart-interval *seconds***]**

例：

```
ciscoasa(config-router)# nsf ietf restart-interval 80
```

グレースフルリスタートの間隔を秒単位で指定できます。有効な値は1～1800秒です。デフォルト値は 120 秒です。

隣接関係（アジャセンシー）が有効になるまでにかかる時間よりも再起動間隔が小さい値に設定されている場合、グレースフル リスタートは終了することがあります。たとえば、30 秒以下の再起動間隔はサポートされていません。

ステップ 2 NSF 認識デバイスで、IETF NSF ヘルパー モードをイネーブルにします。

nsf ietf helper [strict-lsa-checking]

例：

```
ciscoasa(config-router)# nsf ietf helper
```

strict-LSA-checking キーワードは、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更されたLSAがあると検出された場合、ヘルパールータはルータの再起動プロセスを終了させることを示します。

このコマンドは、デフォルトでイネーブルになっています。このコマンドの no 形式を使用すると、ディセーブルになります。

OSPFv3 のグレースフル リスタートの設定

OSPFv3 の NSF グレースフル リスタート機能を設定するには、2 つのステップを伴います。NSF 対応としてのデバイスの設定と、NSF 認識としてのデバイスの設定です。

手順

ステップ 1 明示的な IPv6 アドレスが設定されていないインターフェイスにおける IPv6 処理をイネーブルにします。

interface physical_interface ipv6 enable

例：

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

physical_interface 引数は、OSPFv3 NSF に参加するインターフェイスを識別します。

ステップ 2 NSF 対応デバイスで OSPFv3 のグレースフル リスタートをイネーブルにします。

graceful-restart [restart interval seconds]

例：

```
ciscoasa(config-router)# graceful-restart restart interval 80
```

restart interval seconds は、グレースフル リスタート間隔の長さを秒単位で指定します。有効な値は 1 ～ 1800 秒です。デフォルト値は 120 秒です。

隣接関係（アジャセンシー）が有効になるまでにかかる時間よりもリスタート間隔が小さい値に設定されている場合、グレースフル リスタートは終了することがあります。たとえば 30 秒以下の再起動間隔は、サポートされていません。

ステップ 3 NSF 認識デバイスで OSPFv3 のグレースフル リスタートをイネーブルにします。

graceful-restart helper [strict-lsa-checking]

例：

```
ciscoasa(config-router)# graceful-restart helper strict-lsa-checking
```

strict-LSA-checking キーワードは、再起動ルータにフラッディングされる可能性がある LSA への変更があることが検出された場合、またはグレースフル リスタート プロセスが開始されたときに再起動ルータの再送リスト内に変更された LSA があると検出された場合、ヘルパー ルータはルータの再起動プロセスを終了させることを示します。

グレースフル リスタート ヘルパー モードは、デフォルトでイネーブルになっています。

OSPF のグレースフル リスタート待機タイマーの設定

OSPF ルータでは、すべてのネイバーがパケットに含まれているかが不明な場合は、Hello パケットにアタッチされている EO-TLV に RS ビットを設定することが予期されます。ただし、隣接関係（アジャセンシー）を維持するにはルータの再起動が必要です。ただし、RS ビット値は RouterDeadInterval 秒より長くすることはできません。そのため、Hello パケットの RS ビットを RouterDeadInterval 秒未満に設定するための **timers nsf wait** コマンドが導入されました。NSF 待機タイマーのデフォルト値は 20 秒です。

始める前に

- OSPF の Cisco NSF 待機時間を設定するには、デバイスが NSF 認識または NSF 対応である必要があります。

手順

ステップ 1 OSPF ルータ コンフィギュレーション モードを開始します。

例：

```
ciscoasa(config)# router ospf
```

ステップ 2 タイマーを入力し、NSF を指定します。

例：

```
ciscoasa(config-router)# timers?
router mode commands/options:
  lsa       OSPF LSA timers
  nsf       OSPF NSF timer
  pacing    OSPF pacing timers
  throttle  OSPF throttle timers
ciscoasa(config-router)# timers nsf ?
```

ステップ 3 グレースフルリスタート待機間隔を入力します。この値は、1 ～ 65535 の範囲で指定できます。

例：

```
ciscoasa(config-router)# timers nsf wait 200
```

グレースフルリスタート待機間隔を使用することで、待機間隔がルータの dead 間隔よりも長くならないようにできます。

OSPFv2 設定の削除

OSPFv2 設定を削除します。

手順

イネーブルにした OSPFv2 設定全体を削除します。

clear configure router ospf *pid*

例：

```
ciscoasa(config)# clear configure router ospf 1000
```

設定をクリアした後、**router ospf** コマンドを使用して OSPF を再設定する必要があります。

OSPFv3 設定の削除

OSPFv3 設定を削除します。

手順

イネーブルにした OSPFv3 設定全体を削除します。

clear configure ipv6 router ospf *process-id*

例：

```
ciscoasa(config)# clear configure ipv6 router ospf 1000
```

設定をクリアした後、**ipv6 router ospf** コマンドを使用して OSPFv3 を再設定する必要があります。

OSPFv2 の例

次の例に、さまざまなオプションのプロセスを使用して OSPFv2 をイネーブルにし、設定する方法を示します。

1. OSPFv2 をイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
```

2. （オプション）1 つの OSPFv2 プロセスから別の OSPFv2 プロセスにルートを再配布するには、次のコマンドを入力します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 1
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
ciscoasa(config-route-map)# router ospf 2
ciscoasa(config-rtr)# redistribute ospf 1 route-map 1-to-2
```

3. （オプション）OSPFv2 インターフェイス パラメータを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-rtr)# network 10.0.0.0 255.0.0.0 area 0
ciscoasa(config-rtr)# interface inside
ciscoasa(config-interface)# ospf cost 20
ciscoasa(config-interface)# ospf retransmit-interval 15
ciscoasa(config-interface)# ospf transmit-delay 10
ciscoasa(config-interface)# ospf priority 20
ciscoasa(config-interface)# ospf hello-interval 10
ciscoasa(config-interface)# ospf dead-interval 40
ciscoasa(config-interface)# ospf authentication-key cisco
ciscoasa(config-interface)# ospf message-digest-key 1 md5 cisco
ciscoasa(config-interface)# ospf authentication message-digest
```

4. （オプション）OSPFv2 エリア パラメータを設定するには、次のコマンドを入力します。

```
ciscoasa(config)# router ospf 2
```

```
ciscoasa(config-rtr)# area 0 authentication
ciscoasa(config-rtr)# area 0 authentication message-digest
ciscoasa(config-rtr)# area 17 stub
ciscoasa(config-rtr)# area 17 default-cost 20
```

5. （オプション）ルート計算タイマーを設定し、ログにネイバーのアップおよびダウンのメッセージを表示するには、次のコマンドを入力します。

```
ciscoasa(config-rtr)# timers spf 10 120
ciscoasa(config-rtr)# log-adj-changes [detail]
```

6. （オプション）現在の OSPFv2 の設定を表示するには、**show ospf** コマンドを入力します。

次に、 **show ospf** コマンドの出力例を示します。

```
ciscoasa(config)# show ospf

Routing Process "ospf 2" with ID 10.1.89.2 and Domain ID 0.0.0.2
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
Number of external LSA 5. Checksum Sum 0x 26da6
Number of opaque AS LSA 0. Checksum Sum 0x     0
Number of DCbitless external and opaque AS LSA 0
Number of DoNotAge external and opaque AS LSA 0
Number of areas in this router is 1. 1 normal 0 stub 0 nssa
External flood list length 0
    Area BACKBONE(0)
        Number of interfaces in this area is 1
        Area has no authentication
        SPF algorithm executed 2 times
        Area ranges are
        Number of LSA 5. Checksum Sum 0x 209a3
        Number of opaque link LSA 0. Checksum Sum 0x     0
        Number of DCbitless LSA 0
        Number of indication LSA 0
        Number of DoNotAge LSA 0
        Flood list length 0
```

7. OSPFv2 設定をクリアするには、次のコマンドを入力します。

```
ciscoasa(config)# clear configure router ospf pid
```

OSPFv3 の例

次に、インターフェイス レベルで OSPFv3 をイネーブルにして設定する例を示します。

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf 1 area 1
```

次に、**show running-config ipv6** コマンドの出力例を示します。

```
ciscoasa (config)# show running-config ipv6
ipv6 router ospf 1
 log-adjacency-changes
```

次に、**show running-config interface** コマンドの出力例を示します。

```
ciscoasa (config-if)# show running-config interface GigabitEthernet3/1
interface GigabitEthernet3/1
 nameif fda
 security-level 100
 ip address 1.1.11.1 255.255.255.0 standby 1.1.11.2
 ipv6 address 9098::10/64 standby 9098::11
 ipv6 enable
 ipv6 ospf 1 area 1
```

次に、OSPFv3 専用インターフェイスを設定する例を示します。

```
ciscoasa (config)# interface GigabitEthernet3/1
ciscoasa (config-if)# nameif fda
ciscoasa (config-if)# security-level 100
ciscoasa (config-if)# ip address 10.1.11.1 255.255.255.0 standby 10.1.11.2
ciscoasa (config-if)# ipv6 address 9098::10/64 standby 9098::11
ciscoasa (config-if)# ipv6 enable
ciscoasa (config-if)# ipv6 ospf cost 900
ciscoasa (config-if)# ipv6 ospf hello-interval 20
ciscoasa (config-if)# ipv6 ospf network broadcast
ciscoasa (config-if)# ipv6 ospf database-filter all out
ciscoasa (config-if)# ipv6 ospf flood-reduction
ciscoasa (config-if)# ipv6 ospf mtu-ignore
ciscoasa (config-if)# ipv6 ospf 1 area 1 instance 100
ciscoasa (config-if)# ipv6 ospf encryption ipsec spi 890 esp null md5
123456789012345678901234567890 12

ciscoasa (config)# ipv6 router ospf 1
ciscoasa (config)# area 1 nssa
ciscoasa (config)# distance ospf intra-area 190 inter-area 100 external 100
ciscoasa (config)# timers lsa arrival 900
ciscoasa (config)# timers pacing flood 100
ciscoasa (config)# timers throttle lsa 900 900 900
ciscoasa (config)# passive-interface fda
ciscoasa (config)# log-adjacency-changes
ciscoasa (config)# redistribute connected metric 100 metric-type 1 tag 700
```

OSPFv3 仮想リンクを設定する方法の例については、次の URL を参照してください:

http://www.cisco.com/en/US/tech/tk365/technologies_configuration_example09186a0080b8fd06.shtml

OSPF のモニタリング

IP ルーティング テーブルの内容、キャッシュの内容、およびデータベースの内容など、特定の統計情報を表示できます。提供される情報は、リソースの使用状況を判定してネットワークの問題を解決するために使用することもできます。また、ノードの到達可能性情報を表示し

て、デバイス パケットがネットワークを通過するときにとるルーティング パスを見つけることもできます。

さまざまなOSPFv2ルーティング統計情報をモニターまたは表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show ospf [*process-id* [*area-id*]]	OSPFv2 ルーティング プロセスに関する一般情報を表示します。
show ospf border-routers	ABR および ASBR までの内部 OSPFv2 ルーティング テーブル エントリを表示します。
show ospf [*process-id* [*area-id*]] database	特定のルータの OSPFv2 データベースに関係する情報のリストを表示します。

コマンド	目的
show ospf flood-list *if-name*	（OSPFv2 パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。 OSPFv2 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。 • 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。 • フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。 ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv2 アップデートおよび再送信パケットの送信の効率をよくすることです。 この機能を設定するタスクはありません。自動的に行われます。
show ospf interface [*if_name*]	OSPFv2-related インターフェイスの情報を表示します。
show ospf neighbor [*interface-name*] [*neighbor-id*] [**detail**]	OSPFv2 ネイバー情報をインターフェイスごとに表示します。
show ospf request-list *neighbor if_name*	ルータで要求されるすべての LSA のリストを表示します。
show ospf retransmission-list *neighbor if_name*	再送信を待機しているすべての LSA のリストを表示します。

コマンド	目的
show ospf [*process-id*] summary-address	OSPFv2 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ospf [*process-id*] **traffic**	特定の OSPFv2 インスタンスで送信または受信されたパケットのさまざまなタイプのリストを表示します。
show ospf [*process-id*] virtual-links	OSPFv2-related 仮想リンク情報を表示します。
show route cluster	クラスタリングの追加 OSPFv2 ルートの同期情報を表示します。

さまざまな OSPFv3 ルーティング統計情報をモニターまたは表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show ipv6 ospf [*process-id* [*area-id*]]	OSPFv3 ルーティング プロセスに関する一般的な情報を表示します。
show ipv6 ospf [*process-id*] **border-routers**	ABR および ASBR までの内部 OSPFv3 ルーティング テーブル エントリを表示します。
show ipv6 ospf [*process-id* [*area-id*]] database [**external** | **inter-area prefix** | **inter-area-router** | **network** | **nssa-external** | **router** | **area** | **as** | **ref-lsa** | [*destination-router-id*] [**prefix** *ipv6-prefix*] [*link-state-id*]] [**link** [**interface** *interface-name*] [**adv-router** *router-id*] | **self-originate**] [**internal**] [**database-summary**]	特定のルータの OSPFv3 データベースに関する情報のリストを表示します。
show ipv6 ospf [*process-id* [*area-id*]] **events**	OSPFv3 イベント情報を表示します。

コマンド	目的
show ipv6 ospf [*process-id*] [*area-id*] flood-list *interface-type interface-number*	（OSPFv3 パケット ペーシングの観察のため）インターフェイスへのフラッディングを待機している LSA のリストを表示します。 OSPFv3 アップデート パケットは、自動的にペーシングされるため、各パケットの送信間隔が 33 ミリ秒未満になることはありません。ペーシングを行わないと、リンクが低速の状態でアップデート パケットの一部が失われたり、ネイバーがアップデートを十分すばやく受信できなくなったり、あるいは、ルータがバッファ スペースを使い切ってしまったりすることがあります。たとえば、ペーシングを行わないと、次のいずれかのトポロジが存在する場合にパケットがドロップされる可能性があります。 • 高速ルータがポイントツーポイント リンクを介して低速のルータと接続している。 • フラッディング中に、複数のネイバーから 1 つのルータに同時にアップデートが送信される。 ペーシングは、再送信間でも、送信効率を高めて再送信パケットの損失を最小にするために利用されます。インターフェイスからの送信を待機している LSA を表示することもできます。ペーシングの利点は、OSPFv3 アップデートおよび再送信パケットの送信の効率をよくすることです。 この機能を設定するタスクはありません。自動的に行われます。
show ipv6 ospf [*process-id*] [*area-id*] **interface** [*type number*] [**brief**]	OSPFv3 関連のインターフェイス情報を表示します。
show ipv6 ospf neighbor [*process-id*] [*area-id*] [*interface-type interface-number*] [*neighbor-id*] [**detail**]	OSPFv3 ネイバー情報をインターフェイスごとに表示します。
show ipv6 ospf [*process-id*] [*area-id*] **request-list** [*neighbor*] [*interface*] [*interface-neighbor*]	ルータで要求されるすべての LSA のリストを表示します。
show ipv6 ospf [*process-id*] [*area-id*] retransmission-list [*neighbor*] [*interface*] [*interface-neighbor*]	再送信を待機しているすべての LSA のリストを表示します。

コマンド	目的
show ipv6 ospf statistic [*process-id*] [**detail**]	さまざまな OSPFv3 統計情報を表示します。
show ipv6 ospf [*process-id*] summary-prefix	OSPFv3 プロセスで設定されているサマリー アドレスのすべての再配布情報のリストを表示します。
show ipv6 ospf [*process-id*] **timers** [**lsa-group** | **rate-limit**]	OSPFv3 タイマー情報を表示します。
show ipv6 ospf [*process-id*] **traffic** [*interface_name*]	OSPFv3 トラフィック関連の統計情報を表示します。
show ipv6 ospf virtual-links	OSPFv3-related 仮想リンク情報を表示します。
show ipv6 route cluster [**failover**] [**cluster**] [**interface**] [**ospf**] [**summary**]	クラスタ内の IPv6 ルーティング テーブルのシーケンス番号、IPv6 再コンバージェンス タイマーのステータス、および IPv6 ルーティング エントリのシーケンス番号を表示します。

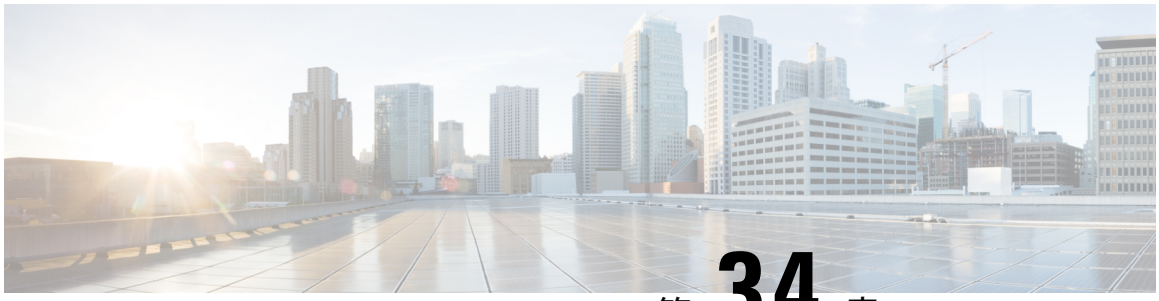
OSPF の履歴

表 *42 : OSPF* の機能履歴

機能名	プラットフォーム リリース	機能情報
OSPF サポート	7.0(1)	Open Shortest Path First（OSPF）ルーティング プロトコルを使用した、データのルーティング、認証、およびルーティング情報の再配布とモニタについて、サポートが追加されました。 **route ospf** コマンドが導入されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	OSPFv2 ルーティングは、マルチ コンテキスト モードでサポートされます。
クラスタ	9.0(1)	OSPFv2 および OSPFv3 の場合、バルク同期、ルートの同期およびスパンド EtherChannel ロードバランシングは、クラスタリング環境でサポートされます。 **show route cluster**、**show ipv6 route cluster**、**debug route cluster**、**router-id cluster-pool** の各コマンドが導入または変更されました。

機能名	プラットフォームリリース	機能情報
IPv6 の OSPFv3 サポート	9.0(1)	OSPFv3 ルーティングが IPv6 に対してサポートされます。 **ipv6 ospf**、**ipv6 ospf area**、**ipv6 ospf cost**、**ipv6 ospf database-filter all out**、**ipv6 ospf dead-interval**、**ipv6 ospf encryption**、**ipv6 ospf hello-interval**、**ipv6 ospf mtu-ignore**、**ipv6 ospf neighbor**、**ipv6 ospf network**、**ipv6 ospf flood-reduction**、**ipv6 ospf priority**、**ipv6 ospf retransmit-interval**、**ipv6 ospf transmit-delay**、**ipv6 router ospf**、**ipv6 router ospf area**、**ipv6 router ospf default**、**ipv6 router ospf default-information**、**ipv6 router ospf distance**、**ipv6 router ospf exit**、**ipv6 router ospf ignore**、**ipv6 router ospf log-adjacency-changes**、**ipv6 router ospf no**、**ipv6 router ospf passive-interface**、**ipv6 router ospf redistribute**、**ipv6 router ospf router-id**、**ipv6 router ospf summary-prefix**、**ipv6 router ospf timers**、**area encryption**、**area range**、**area stub**、**area nssa**、**area virtual-link**、**default**、**default-information originate**、**distance**、**ignore lsa mospf**、**log-adjacency-changes**、**redistribute**、**router-id**、**summary-prefix**、**timers lsa arrival**、**timers pacing flood**、**timers pacing lsa-group**、**timers pacing retransmission**、**timers throttle**、**show ipv6 ospf**、**show ipv6 ospf border-routers**、**show ipv6 ospf database**、**show ipv6 ospf events**、**show ipv6 ospf flood-list**、**show ipv6 ospf graceful-restart**、**show ipv6 ospf interface**、**show ipv6 ospf neighbor**、**show ipv6 ospf request-list**、**show ipv6 ospf retransmission-list**、**show ipv6 ospf statistic**、**show ipv6 ospf summary-prefix**、**show ipv6 ospf timers**、**show ipv6 ospf traffic**、**show ipv6 ospf virtual-links**、**show ospf**、**show running-config ipv6 router**、**clear ipv6 ospf**、**clear configure ipv6 router**、**debug ospfv3**、**ipv6 ospf neighbor** の各コマンドが導入または変更されました。
Fast Hello に対する OSPF サポート	9.2(1)	OSPF は、Fast Hello パケット機能をサポートしているため、OSPF ネットワークでのコンバージェンスが高速なコンフィギュレーションになります。 次のコマンドが変更されました。**ospf dead-interval**
タイマー	9.2(1)	新しい OSPF タイマーを追加し、古いタイマーを廃止しました。 次のコマンドが導入されました。timers lsa arrival、timers pacing、timers throttle 次のコマンドが削除されました。Timers spf、timers lsa-grouping-pacing
アクセス リストを使用したルート フィルタリング	9.2(1)	ACL を使用したルート フィルタリングがサポートされるようになりました。 次のコマンドが導入されました。distribute-list
OSPF モニタリングの強化	9.2(1)	OSPF モニタリングの詳細情報が追加されました。 次のコマンドが変更されました。show ospf events、show ospf rib、show ospf statistics、show ospf border-routers [detail]、show ospf interface brief

機能名	プラットフォームリリース	機能情報
OSPF 再配布 BGP	9.2(1)	OSPF 再配布機能が追加されました。 次のコマンドが追加されました。redistribute bgp
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.3(1)	NSF に対する OSPFv2 および OSPFv3 のサポートが追加されました。 次のコマンドが追加されました。capability、nsf cisco、nsf cisco helper、nsf ietf、nsf ietf helper、nsf ietf helper strict-lsa-checking、graceful-restart、graceful-restart helper、graceful-restart helper strict-lsa-checking
ノンストップ フォワーディング（NSF）に対する OSPF のサポート	9.13(1)	NSF 待機タイマーが追加されました。 NSF 再起動間隔のタイマーを設定するための新しいコマンドが追加されました。このコマンドが導入され、待機間隔がルータの dead 間隔よりも長くならないようになりました。 次のコマンドが導入されました。 **timers nsf wait <seconds>**



第 34 章

IS-IS

この章では、Intermediate System to Intermediate System（IS-IS）ルーティング プロトコルについて説明します。

- IS-IS について （1311 ページ）
- IS-IS の前提条件 （1318 ページ）
- IS-IS のガイドライン （1319 ページ）
- IS-IS の設定 （1319 ページ）
- IS-IS の監視 （1354 ページ）
- IS-IS の履歴 （1357 ページ）
- IS-IS の例 （1357 ページ）

IS-IS について

IS-IS ルーティング プロトコルはリンクステート内部ゲートウェイ プロトコル（IGP）です。リンクステートプロトコルは、各参加デバイスで完全なネットワーク接続マップを構築するために必要な情報の伝播によって特徴付けられます。このマップは、その後、宛先への最短パスを計算するために使用されます。IS-IS の実装は、IPv4 と IPv6 をサポートします。

ルーティング ドメインを 1 つ以上のサブドメインに分割することができます。各サブドメインはエリアと呼ばれ、エリアアドレスが割り当てられます。エリア内のルーティングは、レベル 1 ルーティングと呼ばれます。レベル 1 エリア間のルーティングは、レベル 2 ルーティングと呼ばれます。ルータは、中継システム（IS）と呼ばれます。IS はレベル 1 とレベル 2、またはその両方で稼働できます。レベル 1 で稼働している IS は、同じエリア内にある他のレベル 1 の IS とルーティング情報を交換します。レベル 2 で稼働している IS は、他のレベル 2 のルータとルーティング情報を交換します。この場合はルータが同じレベル 1 エリアにあるかどうかは関係しません。レベル 2 にあるルータと、これらとインターコネクトしているリンクは、レベル 2 サブドメインを形成します。ルーティングが正しく機能するためには、これらをパーティション化してはなりません。

NET について

IS は ネットワーク エンティティ タイトル（NET）と呼ばれるアドレスで識別されます。NET はネットワーク サービス アクセスポイント（NSAP）のアドレスで、これにより IS で動作する IS-IS ルーティング プロトコルのインスタンスを識別できます。NET は、長さが 8 ～ 20 オクテットで、次の 3 つの部分にわかれています。

- エリア アドレス：このフィールドは 1 ～ 13 オクテット長で、アドレスの上位のオクテットで構成されます。

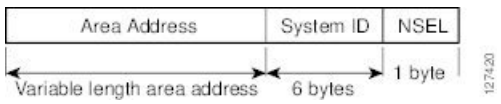
（注） IS-IS インスタンスに複数のエリア アドレスを割り当てることができます。その場合、すべてのエリアアドレスが同義と見なされます。複数の同義エリアアドレスは、ドメインでエリアをマージまたは分割するときに役立ちます。マージまたは分割が完了した後は、複数のエリア アドレスを IS-IS インスタンスに割り当てる必要はありません。

- システム ID：このフィールドは 6 オクテット長で、エリア アドレスの直後に続きます。IS がレベル 1 で動作する場合、システム ID は、同じエリア内のすべてのレベル 1 デバイス間で一意である必要があります。IS がレベル 2 で動作する場合、システム ID は、ドメイン内のすべてのデバイス間で一意である必要があります。

（注） 1 つの IS インスタンスに 1 つのシステム ID を割り当てます。

- NSEL：この N セレクタ フィールドは 1 オクテット長で、システム ID の直後に続きます。このフィールドは 00 に設定する必要があります。

図 *81 : NET* の形式



IS-IS ダイナミック ホスト名

IS-IS ルーティング ドメインでは、各 ASA はシステム ID により表されます。システム ID は、IS-IS ASA ごと構成されている NET の一部です。たとえば、NET 49.0001.0023.0003.000a.00 が設定されている ASA のシステム ID が 0023.0003.000a であるとします。ネットワーク管理者にとって、ASA でのメンテナンスやトラブルシューティングの間、ASA 名とシステム ID の対応を覚えているのは難しいことです。

show isis hostname コマンドを入力すると、システム ID に対する ASA 名のマッピング テーブルに含まれるエントリが表示されます。

ダイナミック ホスト名メカニズムはリンクステートプロトコル（LSP）フラッディングを使用して、ネットワーク全体に ASA 名に対するシステム ID のマッピング情報を配布します。ネットワーク上の ASA はすべて、このシステム ID に対する ASA 名のマッピング情報をルーティング テーブルにインストールしようと試みます。

ネットワーク上で、ダイナミック名のタイプ、長さ、値（TLV）をアドバタイズしている ASA が突然、アドバタイズメントを停止した場合、最後に受信されたマッピング情報が最大 1 時間、ダイナミック ホスト マッピング テーブルに残るため、ネットワークに問題が発生している間、ネットワーク管理者はマッピング テーブル内のエントリを表示できます。

IS-IS での PDU のタイプ

IS では、プロトコル データ ユニット（PDU）を使用してルーティング情報をピアと交換します。PDU の中間システム相互間 Hello PDU（IIH）、リンク状態 PDU（LSP）、およびシーケンス番号 PDU（SNP）タイプが使用されます。

IIH

IIH は、IS-IS プロトコルが有効になっている回線の IS ネイバー間で交換されます。IIH には、送信者のシステム ID、割り当てられたエリア アドレス、送信 IS に認識されているその回線上のネイバーのアイデンティティが含まれます。追加のオプションの情報が含まれる場合もあります。

IIH には、次の 2 種類があります。

- レベル 1 LAN IIH：これらは、マルチアクセス回線において、送信 IS がその回線でレベル 1 デバイスとして動作する場合に送信されます。
- レベル 2 LAN IIH：これらは、マルチアクセス回線において、送信 IS がその回線でレベル 2 デバイスとして動作する場合に送信されます。

LSP

IS では LSP を生成して、そのネイバーや IS に直接接続されている接続先をアドバタイズします。LSP は、以下のものによって一意に識別できます。

- LSP を生成した IS のシステム ID。
- Pseudonode ID：この値は LSP が pseudonode LSP の場合を除き、常に 0 です
- LSP 番号（0 ～ 255）
- 32 ビットのシーケンス番号

LSP の新しいバージョンが生成されるたびに、シーケンス番号が増加します。

レベル 1 の LSP は、レベル 1 をサポートしている ISで生成されます。レベル 1 の LSP はレベル 1 のエリア全体にフラッディングされます。エリア内のすべてのレベル 1 の IS で生成されたレベル 1 の LSP のセットは、レベル 1 LSP データベース（LSPDB）となります。エリア内のすべてのレベル 1 の IS は同一のレベル 1 の LSPDB を持ちます。したがって、そのエリアの同一のネットワーク接続マップを持つことになります。

レベル 2 の LSP は、レベル 2 をサポートしている ISで生成されます。レベル 2 の LSP は、レベル 2 のサブドメイン全体にフラッディングされます。ドメイン内のすべてのレベル 2 の IS で生成されたレベル 2 の LSP のセットは、レベル 2 LSP データベース（LSPDB）となります。すべてのレベル 2 の IS は同一のレベル 2 の LSPDB を持ちます。したがって、そのレベル 2 のサブドメインの同一の接続マップを持つことになります。

SNP

SNP には、1 つ以上の LSP のサマリー説明が含まれます。レベル 1 とレベル 2 の両方について、次の 2 つのタイプの SNP があります。

- Complete Sequence Number PDU（CSNP）は、特定のレベルに関して IS が持つ LSPDB のサマリを送信するために使用されます。
- Partial Sequence Number PDU（PSNP）は、IS がそのデータベースに持つか取得する必要がある特定のレベルに関する LSP のサブセットのサマリを送信するために使用されます。

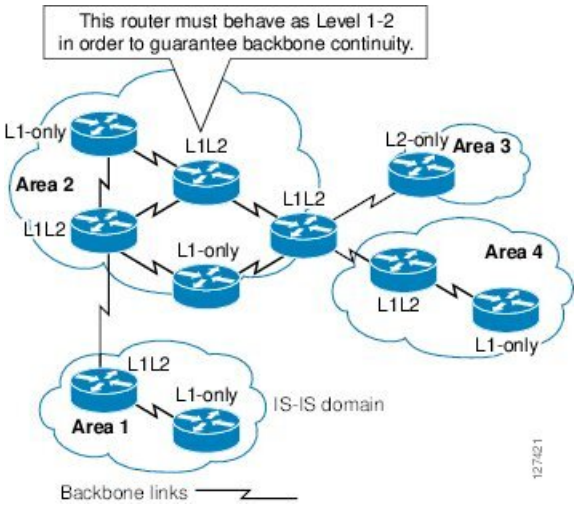
マルチアクセス回線での IS-IS の動作

マルチアクセス回線では複数の IS がサポートされます。つまり、回線で 2 つ以上の IS が動作します。マルチアクセス回線で必要な前提条件は、マルチキャスト アドレスまたはブロードキャストアドレスを使用して複数のシステムのアドレスを指定できることです。マルチアクセス回線でレベル 1 をサポートする IS は、レベル 1 の LAN IIH を回線上に送信します。マルチアクセス回線でレベル 2 をサポートする IS は、レベル 2 の LAN IIH を回線上に送信します。IS は、回線上でネイバー IS とレベルごとに別々の隣接関係（アジャセンシー）を形成します。

IS は回線上でレベル 1 をサポートする他の IS とレベル 1 の隣接関係（アジャセンシー）を形成し、同じエリアアドレスを持ちます。同一マルチアクセス回線上で、レベル 1 をサポートするエリア アドレスの整合性のないセットを持つ 2 つの IS は、サポートされていません。IS は回線上でレベル 2 をサポートする他の IS とレベル 2 の隣接関係（アジャセンシー）を形成します。

以下の図の IS-IS のネットワーク トポロジ内のデバイスは、ネットワークのバックボーンに従って、レベル 1、レベル 2、またはレベル 1 と 2 のルーティングを実行します。

図 *82 : IS-IS* ネットワーク トポロジにおけるレベル *1*、レベル *2*、レベル *1-2* デバイス



IS-IS での代表 IS の選択

各 IS が LSP 内のマルチアクセス回線上のすべての隣接関係をアドバタイズする場合、必要なアドバタイズメントの総数は N 2 になります。ここで、N は回線の特定のレベルで動作している IS の数です。この拡張性の問題を解消するため、IS-IS ではマルチアクセス回線を表す擬似ノードを定義します。特定のレベルで動作するすべての IS が、その回線の代表中継システム（DIS）として機能するように IS のいずれかを選定します。DIS は、回線でアクティブな各レベルごとに選定されます。

DIS は擬似ノード LSP を発行する責任を担います。擬似ノード LSP には、その回線で動作するすべての IS のネイバー アドバタイズメントが含まれます。その回線で動作するすべての IS（DIS を含む）が非擬似ノード LSP 内の擬似ノードにネイバーアドバタイズメントを提供し、マルチアクセス回線上のネイバーはアドバタイズしません。このように、必要なアドバタイズメントの総数は、N（回線で動作する IS の数）に応じて変わります。

擬似ノード LSP は次の ID によって一意に分類されます。

- LSP を生成した DIS のシステム ID
- Pseudonode ID（常にゼロ以外）
- LSP 番号（0 ～ 255）
- 32 ビットのシーケンス番号

ゼロ以外の擬似ノード ID は、擬似ノード LSP と擬似ノード以外の LSP を区別するもので、このレベルでも DIS である場合に、他の LAN 回線の間で一意になるように、DIS によって選択されます。

また、DIS は回線上に定期的な CSNP を送信する責任も担っています。これは、DIS 上の LSPDB の現在のコンテンツに関する完全な要約説明を提供します。回線上の他の IS が次のアクティ

ビティを実行できます。これにより、マルチアクセス回線上のすべての IS の LSPDB が効率的かつ確実に同期されます。

- DIS によって送信された CSNP に存在しない LSP、またはその CSNP に記述された LSP より新しい LSP をフラッディングします。
- ローカル データベースに存在しない DIS によって送信された CSNP セットに記述されている LSP、または CSNP セットに記述されている LSP より古い LSP の PSNP を送信することで、LSP を要求します。

IS-IS LSPDB の同期

IS-IS を適切に動作させるには、各 IS 上の LSPDB を同期するため信頼性の高い効率的なプロセスが必要です。IS-IS では、このプロセスは更新プロセスと呼ばれます。更新プロセスは、各サポート レベルで独立して動作します。ローカルに生成される LSP は常に新しい LSP です。回線上のネイバーから受信した LSP は、他の IS によって生成されているか、またはローカル IS によって生成された LSP のコピーであることがあります。受信した LSP はローカル LSPDB の現在のコンテンツに比べ、古い、同じ、または新しい場合があります。

新しい LSP の処理

ローカル LSPDB に追加された新しい LSP は、LSPDB の同じ LSP の古いコピーを置き換えます。新しい LSP は、新しい LSP を受信した回線を除き、IS が現在、新しい LSP に関連付けられているレベルでアップ状態の隣接関係（アジャセンシー）を持つすべての回線に送信されるようにマークされます。

マルチアクセス回線では、IS は新しい LSP を 1 回フラッディングします。IS は、マルチアクセス回線用に DIS によって定期的に送信される一連の CNSP を調べます。ローカル LSPDB に CSNP セットに記述されている LSP より新しい LSP が 1 つ以上含まれている場合は（これには CSNP セットに存在しない LSP も含まれる）、それらの LSP がマルチアクセス回線経由で再度フラッディングされます。ローカル LSPDB に CSNP セットに記述された LSP より古い LSP が 1 つ以上含まれる場合は（これには、ローカル LSPDB に存在しない CSNP セットに記述された LSP も含まれる）、更新が必要な LSP の記述とともに PSNP がマルチアクセス回線上に送信されます。マルチアクセス回線の DIS は、要求された LSP を送信することで応答します。

古い LSP の処理

IS でローカルの LSPDB のコピーよりも古い LSP を受信する場合があります。また IS でローカルの LSPDB のコピーよりも古い LSP について説明する SNP（全体または一部）を LSPDB 受信する場合もあります。いずれの場合も、IS によってローカル データベースでその LSP がマークされ、古い LSP が含まれている古い LSP または SNP が受信された回線にフラッディングされます。実行されるアクションは、前述の新しい LSP がローカルデータベースに追加された後のアクションと同じです。

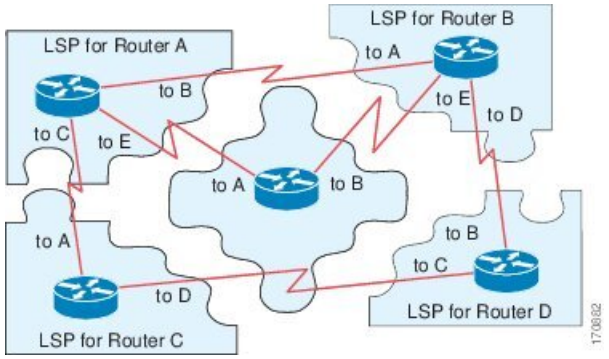
経過期間が同じ LSP の処理

更新プロセスの分散型の特性のため、IS がローカル LSPDB の現在のコンテンツと同じ LSP のコピーを受信する可能性があります。マルチアクセス回線では、経過期間が同じ

LSP の受信は無視されます。回線の DIS によって設定された CSNP が定期的に送信され、LSP を受信した送信者への明示的な確認応答の役割を果たします。

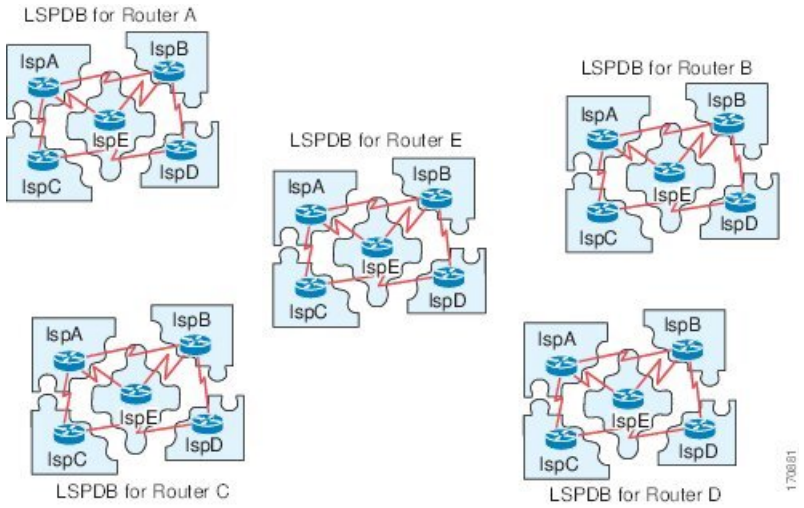
次の図は、LSP を使用してネットワーク マップを作成する方法を示しています。ネットワーク トポロジをジグソー パズルとして想像してください。各 LSP（IS を表す）はジグソー パズルの 1 つのピースに相当します。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

図 *83 : IS-IS* ネットワーク マップ



次の図は、ネイバー デバイス間で隣接関係（アジャセンシー）が形成された後に、IS-IS ネットワーク内の各デバイスが完全に更新されたリンクステートデバイスを備えていることを示しています。エリア内のすべてのレベル 1 デバイスまたはレベル 2 サブドメイン内のすべてのレベル 2 デバイスに適用されます。

図 *84 : LSPDB* が同期された *IS-IS* デバイス



IS-IS 最短パスの計算

LSPDB のコンテンツが変更されると、各 IS は独立して最短パスの計算を再実行します。アルゴリズムは、有向グラフに沿って最短パスを見つけるためのよく知られたダイクストラ アルゴリズムに基づいています。有向グラフでは、各 IS がグラフの頂点で、IS 間のリンクが非負の

重みを持つエッジとなります。2つのIS間のリンクをグラフの一部として見なす前に、双方向接続チェックが実行されます。これによって、たとえば、1つのISがすでにネットワーク内で動作していないが、動作を停止する前に、生成したLSPセットを消去しなかった場合などに、LSPDB 内で古い情報が使用されるのを防ぎます。

SPFの出力は、一連のタプル（宛先、ネクストホップ）です。宛先は、プロトコルによって異なります。複数のネクスト ホップが同じ宛先に関連付けられている場合は、複数の等コストパスがサポートされます。

IS によってサポートされているレベルごとに、独立した SPF が実行されます。同じ宛先がレベル 1 パスとレベル 2 パスの両方によって到達可能な場合は、レベル 1 パスが優先されます。

他のエリアに 1 つ以上のレベル 2 ネイバーを持つことを示しているレベル 2 IS は、デフォルトルートとも呼ばれる、ラストリゾートのパスとして同じエリア内のレベル1デバイスによって使用される場合があります。レベル 2 IS は、レベル 1 LSP 0 に ATT（Attached）bit を設定することで、他のエリアへのアタッチメントを示します。

（注） IS は、各レベルで最大 256 の LSP を生成できます。LSP は、0 ～ 255 の番号によって識別されます。LSP 0 は、他のエリアへのアタッチメントを示すための ATT ビットの設定の意味を含め、特別なプロパティを備えています。番号 1 ~ 255 の LSP に ATT ビットが設定されている場合は、それに意味はありません。

IS-IS シャットダウン プロトコル

IS-IS をシャットダウンする（管理上のダウン状態にする）ことで、設定パラメータを失うことなく IS-IS プロトコル設定に変更を加えることができます。グローバル IS-IS プロセス レベルまたはインターフェイス レベルで IS-IS をシャットダウンできます。プロトコルがオフになっているときにデバイスが再起動すると、プロトコルは、通常、ディセーブル状態でアップします。プロトコルが管理上のダウン状態に設定されている場合、ネットワーク管理者は、プロトコル設定を失うことなく IS-IS プロトコルを管理上オフにし、中間状態（多くの場合、望ましくない状態）を経てプロトコルの動作を遷移させることなくプロトコル設定に一連の変更を加え、適切なタイミングでプロトコルを再度イネーブルにすることができます。

IS-IS の前提条件

IS-IS を設定する前に、次の前提条件を満たしている必要があります。

- IPv4 および IPv6 を理解していること。
- IS-IS を設定する前にネットワーク設計およびそれを経由するトラフィックのフロー方法を理解していること。
- エリアを定義し、デバイスのアドレッシング計画を準備し（NET の定義を含む）、IS-IS を実行するインターフェイスを決定していること。

- デバイスを設定する前に、隣接関係テーブルに表示されるネイバーを示す隣接関係のマトリックスを準備しておくこと。これにより検証が容易になります。

IS-IS のガイドライン

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

クラスタのガイドライン

個々のインターフェイス モードでのみサポート：スパンド EtherChannel モードはサポートされません。

その他のガイドライン

双方向転送で、IS-IS はサポートされていません。

IS-IS の設定

ここでは、システムで IS-IS プロセスをイネーブルにして設定する方法について説明します。

手順

ステップ 1 IS-IS ルーティングのグローバルな有効化 （1320 ページ）。
ステップ 2 IS-IS 認証の有効化 （1324 ページ）。
ステップ 3 IS-IS LSP の設定 （1329 ページ）
ステップ 4 IS-IS サマリー アドレスの設定 （1333 ページ）。
ステップ 5 IS-IS パッシブ インターフェイスの設定 （1334 ページ）。
ステップ 6 IS-IS インターフェイスの設定 （1335 ページ）。
ステップ 7 IS-IS インターフェイス hello パディングの設定 （1340 ページ）
ステップ 8 IS-IS IPv4 アドレス ファミリの設定 （1343 ページ）。
ステップ 9 IS-IS IPv6 アドレス ファミリの設定 （1349 ページ）。

IS-IS ルーティングのグローバルな有効化

IS-IS 設定は 2 段階で行われます。最初に、グローバル コンフィギュレーション モードで IS-IS プロセスを設定し、次にルータ コンフィギュレーション モードで NET および IS-IS のルーティング レベルを指定します。このほかにも、ルータ コンフィギュレーション モードで設定できる一般的なパラメータがあります。そのほうが、インターフェイスごとに設定するよりも、ネットワークにとって合理的です。この項では、それらのコマンドについて説明します。

次に、インターフェイス コンフィギュレーション モードで、インターフェイスごとに IS-IS プロトコルを有効にします。こうすることで、インターフェイスがダイナミック ルーティングに参加し、ネイバーデバイスとの隣接関係（アジャセンシー）を確立できるようになります。隣接関係（アジャセンシー）を確立し、ダイナミック ルーティングを可能にするには、その前に、1 つ以上のインターフェイスでルーティングを有効にしておく必要があります。インターフェイスでの IS-IS の設定手順については、IS-IS インターフェイスの設定 （1335 ページ）を参照してください。

この手順では、ルータ コンフィギュレーション モードで、ASA で IP ルーティング プロトコルとして IS-IS を有効にし、その他の一般オプションを有効にする方法について説明します。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ASA でルーティング プロトコルとして IS-IS を有効にします。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 ルーティング プロセスの NET を指定します。

net *network-entity-title*

例：

```
ciscoasa(config-router)# net 49.1234.aaaa.bbbb.cccc.00
```

NET によって IS-IS のデバイスが特定されます。NET の詳細については、NET について （1312 ページ）を参照してください。

ステップ 3 （オプション）IS-IS ルーティング プロセスのルーティング レベルを割り当てます。

is-type [level-1 | level-2-only | level-1-2]

例：

```
ciscoasa(config-router)# is-type level-1
```

- （任意）**level-1**：エリア内ルーティングを示します。ASA は、エリア内の宛先のみを学習します。
- （任意）**level-2-only**：エリア間ルーティングを示します。ASA はバックボーンの一部であり、自分のエリア内にあるレベル 1 ルータとは通信しません。
- （任意）**level-1-2**：ASA は、レベル 1 およびレベル 2 両方のルーティングを実行します。このルータは、ルーティング プロセスのインスタンスを 2 つ実行します。このルータは、エリア内（レベル 1 ルーティング）の宛先について 1 つの LSDB を持っており、SPF の計算を実行してエリア トポロジを検出します。また、他のすべてのバックボーン（レベル 2）ルータの LSP による別の LSDB も備え、別の SPF 計算を実行してバックボーンのトポロジと他のすべてのエリアの存在を検出します。

従来の IS-IS コンフィギュレーションでは、ASA はレベル 1（エリア内）およびレベル 2（エリア間）ルータとしてだけ機能します。マルチエリア IS-IS コンフィギュレーションでは、設定された IS-IS ルーティング プロセスの最初のインスタンスは、デフォルトでレベル 1-2（エリア内およびエリア間）ルータです。設定されている IS-IS プロセスの残りのインスタンスはデフォルトでレベル 1 ルータになります。

（注）
IS-IS ルーティング プロセスのタイプを設定することを水晶します。

ステップ 4 ASA で IS-IS ダイナミック ホスト名機能を有効にします。

hostname dynamic

このコマンドは、デフォルトでイネーブルになっています。IS-IS のダイナミック ホスト名の詳細については、IS-IS ダイナミック ホスト名 （1312 ページ）を参照してください。

ステップ 5 ASA のすべてのインターフェイスで hello パディングを設定します。

hello padding multi-point

このコマンドは、デフォルトでイネーブルになっています。これは、IS-IS hello をフル MTU サイズに設定します。これにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。

hello パディングを無効にして（IS-IS ルーティング プロセスに対し、ルータ上のすべてのインターフェイスに **no hello padding multi-point** を指定）、両方のインターフェイスの MTU が同じである場合や、トランスレーショナルブリッジングの場合に、ネットワーク帯域幅が浪費されないようにすることができます。hello パディングが無効になっても、ASA は、MTU 不一致検出の利点を維持するため、最初の 5 回の IS-IS hello をフル サイズの MTU にパディングして送信します。

ルータ レベルで hello パディングがオフになっていることを確認するには、特権 EXEC モードで **show clns interface** コマンドを入力します。詳細は、IS-IS の監視 （1354 ページ）を参照してください。

ステップ 6 （オプション）NLSP IS-IS 隣接関係（アジャセンシー）の状態が変更（アップまたはダウン）されたときに、ASA がログ メッセージを生成できるようにします。

log-adjacency-changes [all]

このコマンドは、デフォルトでディセーブルになっています。隣接関係（アジャセンシー）の変更をロギングすると、大規模なネットワークをモニタリングする際に役立ちます。メッセージは次の形式になります。

例：

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

all：（オプション）non_IIH イベントによって生成される変更を含みます。

ステップ 7 （オプション）IS-IS プロトコルを無効にして、IS-IS プロトコルがどのインターフェイスでも隣接関係（アジャセンシー）を確立できないようにし、LSP データベースをクリアします。

protocol shutdown

このコマンドにより、既存の IS-IS 設定パラメータを削除することなく、特定のルーティング インスタンスの IS-IS プロトコルを無効にすることができます。このコマンドを入力した場合、IS-IS プロトコルは引き続きルータ上で動作し、ユーザーは現在の IS-IS 設定を使用できますが、IS-IS はいずれのインターフェイスでも隣接関係を確立せず、IS-IS LSP データベースをクリアします。特定のインターフェイスについて IS-IS を無効にするには、**isis protocol shutdown** コマンドを使用します。手順については、IS-IS インターフェイスの設定 （1335 ページ）を参照してください。

ステップ 8 （オプション）IS-IS IP プレフィックスにハイ プライオリティを割り当てます。

route priority high tag *tag-value*

例：

```
ciscoasa(config-router)# route priority high tag 100
```

tag *tag-value*：特定のルート タグが先頭に付加された IS-IS IP にハイ プライオリティを割り当てます。指定できる範囲は 1 ～ 4294967295 です。

グローバル ルーティング テーブルでより高速な処理とインストールを行うために、このコマンドを使用して、より高いプライオリティの IS-IS IP プレフィックスにタグ付けすると、より速くコンバージェンスを達成できます。たとえば、VoIP トラフィックが、その他のタイプのパケットよりも速く更新されるようにするために、VoIP ゲートウェイ アドレスが最初に処理されるようにすることができます。

ステップ 9 （オプション）すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。

metric *default-value* **[level-1 | level-2]**

例：

```
ciscoasa(config-router)# metric 55 level-1
```

- *default-value*：リンクに割り当てられ、宛先へのリンクを介したパス コストを計算するために使用されるメトリック値。指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。

すべての IS-IS インターフェイスに対してデフォルトのメトリックを変更する必要がある場合は、**metric** コマンドを使用することをお勧めします。こうすることで、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

ステップ 10 （オプション）新しいスタイル、長さ、値オブジェクト（TLV）を生成し、それらのオブジェクトのみを受け入れるように ASA を設定します。

metric-style narrow | transition | wide [level-1 | level-2 | level-1-2]

例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**：旧スタイルの TLV とナロー メトリックを使用します。
- **transition**：旧スタイルおよび新スタイルの TLV の両方を受け入れるように ASA に指示します。
- **wide**：新スタイルの TLV を使用してワイド メトリックを伝送します。
- （任意）**level-1**：ルーティング レベル 1 でこのコマンドをイネーブルにします。
- （任意）**level-2**：ルーティング レベル 2 でこのコマンドをイネーブルにします。
- （任意）**level-1-2**：ルーティング レベル 2 でこのコマンドをイネーブルにします。

このコマンドを使用すると、ASA が新スタイルの TLV のみを生成して受け入れるようになります。こうすることで、旧スタイルと新スタイル両方の TLV を生成した場合よりも、ASA によるメモリおよびその他のリソースの使用量が減少します。

ステップ 11 （オプション）すべてのインターフェイス上で指定した ASA のプライオリティを設定します。

priority *number-value*

例：

```
ciscoasa(config-router)# priority 80
```

number-value：ASA のプライオリティ。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。

ステップ 12 （オプション）IS-IS エリアの追加のマニュアル アドレスを設定します。

max-area-addresses *number*

例：

```
ciscoasa(config-router)# max-area-addresses 3
```

number：追加するマニュアル アドレスの数。範囲は 3 ～ 254 です。デフォルト値はありません。

このコマンドにより、追加マニュアル アドレスを設定することでIS-IS エリアのサイズを最大化できるようになります。各マニュアルアドレスを作成するには、追加するアドレスの数を指定し、NET アドレスを割り当てます。NET の詳細については、NET について （1312 ページ）を参照してください。

ステップ 13 IS-IS のマルチパス ロード シェアリングを設定します。

maximum-paths *number-of-paths*

例：

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths：ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。デフォルトは 1 です。

maximum-path コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチロード シェアリングを設定するために使用されます。

IS-IS 認証の有効化

IS-IS ルート認証により、未承認の送信元から不正なルーティング メッセージまたは誤ったルーティング メッセージを受信することが防止されます。各 IS-IS エリアまたはドメインにパスワードを設定することで、不正なルータが誤ったルーティング情報をリンクステート データベースに挿入することを阻止できます。あるいは IS-IS 認証タイプ（IS-IS MD5 認証または拡張クリアテキスト認証）を設定できます。インターフェイスごとに認証を設定することもできます。IS-IS メッセージ認証対象として設定されたインターフェイス上にあるすべての IS-IS ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

エリアとドメインの詳細については、IS-IS について （1311 ページ）を参照してください。

始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化（1320 ページ）を参照してください。

手順

ステップ 1 IS-IS ルータ コンフィギュレーション モードを開始し、IS-IS エリア認証パスワードを設定します。

area-password *password* [**authenticate snp {validate | send-only}**]

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)# area-password track authenticate snp validate
```

- *password*：割り当てるパスワード。
- （オプション）**authenticate snp**：これを指定すると、システムはパスワードを SNP に挿入するようになります。
- **validate**：これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
- **send-only**：これを指定すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。

あるエリアに存在するすべての ASA でこのコマンドを使用することで、不正ルータがリンクステートデータベースへ誤ったルーティング情報を挿入することを阻止できます。ただし、このパスワードはプレーン テキストとしてやり取りされるため、この機能により提供されるセキュリティは限定されています。

パスワードはレベル 1（ステーション ルータ レベル）PDU LSP、CSNP、および PSNP に挿入されます。**authenticate snp** キーワードを **validate** キーワードまたは **send-only** キーワードのいずれかと共に指定しない場合、IS-IS プロトコルはパスワードを SNP に挿入しません。

ステップ 2 IS-IS ルータ コンフィギュレーション モードを開始し、IS-IS ドメイン認証パスワードを設定します。

domain-password *password* [**authenticate snp {validate | send-only}**]

例：

```
ciscoasa(config-router)# domain-password users2j45 authenticate snp validate
```

- *password*：割り当てるパスワード。

- （オプション）**authenticate snp**：これを指定すると、システムはパスワードをシーケンス番号 PDU（SNP）に挿入するようになります。
- **validate**：これを指定すると、システムはパスワードを SNP に挿入し、受け取ったパスワードを SNP で確認するようになります。
- **send-only**：これを指定すると、システムは SNP へのパスワードの挿入だけは行うようになりますが、SNP での受け取ったパスワードの確認は行われません。このキーワードは、ソフトウェアのアップグレード中、移行をスムーズに行うために使用します。

このパスワードはプレーンテキストとしてやり取りされるため、この機能により提供されるセキュリティは限定されています。

パスワードはレベル 2（エリア ルータ レベル）PDU LSP、CSNP、および PSNP に挿入されます。**authenticate snp** キーワードを **validate** キーワードまたは **send-only** キーワードのいずれかと共に指定しない場合、IS-IS プロトコルはパスワードを SNP に挿入しません。

ステップ 3 送信される IS-IS パケットに対してのみ認証が実行される（受信パケットに対しては実行されない）ように、IS-IS インスタンスをグローバルまたはインターフェイスごとに設定します。

ルータ モード：**authentication send-only [level-1 | level-2]**

例：

```
ciscoasa(config-router)# authentication send-only level-1
```

インターフェイス モード：**isis authentication send-only [level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis authentication send-only level-1
```

- （オプション）**level-1**：認証は受信ではなく、送信されるレベル 1 パケットだけに実行されます。
- （オプション）**level-2**：認証は受信ではなく、送信されるレベル 2 パケットだけに実行されます。

このコマンドは、認証モードおよび認証キー チェーンを設定する前に使用します。これにより、認証の実装がスムーズに進むようになります。レベル 1 またはレベル 2 を指定しない場合は、send-only が両方のレベルに適用されます。

（注）
送信されるパケットだけに認証が挿入され、受信されるパケットではチェックされない場合、各 ASA で、キーの設定に費やせる時間が長くなります。このコマンドを使用して、通信を必要とする ASA をすべて設定した後で、ASA ごとに、認証モードとキー チェーンをイネーブルにします。

ステップ 4 IS-IS インスタンスに対する IS-IS パケットで使用される認証モードのタイプをグローバルまたはインターフェイスごとに指定します。

ルータ モード：**authentication mode {md5 | text} [level-1 | level-2]**

例：

```
ciscoasa(config-router)# authentication mode md5 level-1
```

インターフェイス モード：**isis authentication mode {md5 | text} [level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)#  isis authentication mode md5 level-1
```

- **md5**：Message Digest 5 認証を有効にします。
- **text**：クリア テキスト認証を使用します。
- （オプション）**level-1**：レベル 1 パケットについてだけ、指定された認証を有効にします。
- （オプション）**level-2**：レベル 2 パケットについてだけ、指定された認証を有効にします。

area-password または **domain-password** を使用してクリア テキスト認証が設定されている場合、これらのどちらのコマンドよりも isis authentication mode が優先されます。**isis authentication mode** を設定した場合、**area-password** または **domain-password** を設定しようとしても許可されません。レベル 1 またはレベル 2 を指定しない場合、このモードは両方のレベルに適用されます。

ステップ 5 IS-IS の認証をグローバルまたはインターフェイスごとに有効にします。

ルータ モード：**authentication key [0 | 8]** パスワード **[level-1 | level-2]**

例：

```
ciscoasa(config-router)# authentication key 0 site1 level-1
```

インターフェイス モード：**isis authentication key [0 | 8]** パスワード **[level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# router isis
ciscoasa(config-if)# isis authentication key 0 second level-1
```

- **0**：暗号化されていないパスワードが続くことを指定します。
- **8**：暗号化されたパスワードが後に続くことを指定します。
- *password*：認証を有効にし、キーを指定します。

- （オプション）**level-1**：レベル 1 パケットについてだけ認証をイネーブルにします。
- （オプション）**level-2**：レベル 2 パケットについてだけ認証をイネーブルにします。

key コマンドで設定されたパスワードが存在しない場合、キー認証は行われません。キー認証は、クリアテキスト認証またはMD5認証に適用できます。モードを設定するには、ステップ 4 を参照してください。IS-IS に一度に適用できる認証キーは 1 つだけです。別のキーを設定すると、1 番めのキーは上書きされます。レベル 1 またはレベル 2 を指定しない場合、パスワードは両方のレベルに適用されます。

ステップ 6 インターフェイスの認証パスワードを設定します。

isis password *password* **[level-1 | level-2]**

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis password analyst level-1
```

- *password*：インターフェイスに割り当てられる認証パスワード。
- （オプション）**level-1**：レベル 1 での認証パスワードを個別に設定します。レベル 1 ルーティングでは、ASA はステーション ルータとしてだけ動作します。
- （オプション）**level-2**：レベル 2 での認証パスワードを個別に設定します。レベル 2 ルーティングでは、ASA はエリア ルータとしてだけ動作します。

このコマンドにより、不正ルータによるこの ASA との隣接の形成を阻止し、ネットワークを不正侵入から保護することができます。パスワードはプレーンテキストとしてやり取りされるため、これにより提供されるセキュリティは限定されています。**level-1** キーワードと **level-2** キーワードを使用して、異なるルーティング レベルに対して異なるパスワードを割り当てることができます。

例

次の例は、レベル 1 パケットに対して MD5 認証を実行し、site1 という名前のキーチェーンに属している任意のキーを送信する IS-IS インスタンスを示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0101.0101.0101.00
ciscoasa(config-router)# is-type level-1
ciscoasa(config-router)# authentication send-only level-1
ciscoasa(config-router)# authentication mode md5 level-1
ciscoasa(config-router)# authentication key 0 site1 level-1
```

IS-IS LSP の設定

IS では LSP を生成して、そのネイバーや IS に直接接続されている接続先をアドバタイズします。LSP の詳細については、IS-IS での PDU のタイプ （1313 ページ）を参照してください。

高速コンバージェンス設定となるように LSP を設定するには、次のコマンドを使用します。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 内部チェックサム エラーのある IS-IS LSP を受信した場合に、LSP をパージするのではなく無視するように ASA を設定します。

ignore-lsp-errors

例：

```
ciscoas(config-router)# ignore-lsp-errors
```

IS-IS では、データリンク チェックサムが不正な LSP を受信側がパージすることになっています。これにより、パケットの発信側は LSP を再生成します。正しいデータリンク チェックサムを持つ LSP をまだ送信している間にデータ破損を引き起こすリンクがネットワークにあった場合、大量のパケットをパージして再生成する連続サイクルが発生し、ネットワークの機能が停止してしまう可能性があります。LSP をパージするのではなく無視するには、このコマンドを使用します。デフォルトではイネーブルになっています。

ステップ 3 パッシブ インターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS を設定します。

advertise passive-only

このコマンドは、LSP アドバタイズメントから、接続されているネットワークの IP プレフィックスを除外します。これにより、ルータ非擬似ノード LSP でアドバタイズされるプレフィックスが少なくなるため、IS-IS のコンバージェンス時間が短縮されます。

ステップ 4 IS-IS LSP がフルになるように設定します。

fast-flood *lsp-number*

例：

```
ciscoasa(config-router)# fast-flood 7
```

（オプション）*lsp-number*：ここで指定した数の LSP があふれると、SPF が開始されます。

このコマンドでは、指定した数の LSP が ASA から送信されます。LSP は、SPF の実行前に SPF を呼び出します。LSP フラッディング プロセスを高速化すると、全体的なコンバージェンス時間が短縮されます。指定できる範囲は 1 ～ 15 です。デフォルトは 5 分です。

（注）
ルータが SPF 計算を実行する前に、LSP の高速フラッディングを有効にすることをお勧めします。

ステップ 5 IS-IS LSP の MTU サイズを設定します。

lsp-mtu *bytes*

例：

```
ciscoasa(config-router)# lsp-mtu 1300
```

bytes：最大パケット サイズ（バイト単位）。バイト数は、ネットワーク内の任意のリンクの最小 MTU 以下の値に設定する必要があります。指定できる範囲は 128 ～ 4352 です。

ステップ 6 LSP が ASA のデータベースで更新されずに保持される最大時間を設定します。

max-lsp-lifetime *seconds*

例：

```
ciscoasa(config-router)# max-lsp-lifetime 2400
```

seconds：LSP のライフタイム（秒数）。指定できる範囲は 1 ～ 65,535 です。デフォルトは 1200 です。

更新 LSP の着信前にライフタイムを超えると、LSP がデータベースからドロップされます。

ステップ 7 SPF 計算の IS-IS スロットリングをカスタマイズします。

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。

- *spf-max-wait*：2 つの連続した SPF 計算の間の最大間隔を指定します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。
- （オプション）*spf-initial-wait*：トポロジが変更されてから最初の SPF 計算までの初期の待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された SPF 最大待機間隔に達するまでそれが行われます。
- （オプション）*spf-second-wait*：最初と 2 番目の SPF 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

SPF 計算が実行されるのは、トポロジが変更されたときだけです。このコマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。

（注）
SPF 計算は、プロセッサに高い負荷を与えます。したがって、特にエリアが大きくてトポロジが頻繁に変更される場合は、これを実行する頻度を制限すると役に立つことがあります。SPF 間隔を大きくすると、ASA のプロセッサ負荷が軽減されますが、コンバージェンス速度が低下する可能性があります。

ステップ 8 LSP 生成の IS-IS スロットリングをカスタマイズします。

lsp-gen-interval [level-1 | level-2] *lsp-max-wait [lsp-intial-wait lsp-second wait]*

例：

```
ciscoasa(config-router)#  lsp-gen-interval level-1 2 50 100
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *lsp-max-wait*：2 つの LSP が連続して生成される最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*lsp-initial-wait*：最初の LSP を生成する前の初期待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルト値は 50 ミリ秒です。

  毎回の間隔はその前の間隔の 2 倍の長さになり、指定された LSP 最大待機間隔に達するまでそれが行われます。
- （オプション）*spf-second-wait*：最初と 2 番目の LSP 生成の間の間隔を指定します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  このコマンドは、生成された LSP 間の遅延を制御します。

ステップ 9 LSP の更新間隔を設定します。

lsp-refresh-interval *seconds*

例：

```
ciscoasa(config-router)# lsp-refresh-interval 1080
```

（オプション）*seconds*：LSP が更新される頻度。指定できる範囲は 1 ～ 65535 秒です。デフォルト値は 900 秒（15 分）です。

リフレッシュ間隔によって、ソフトウェアが定期的に LSP で発信元のルート トポロジ情報を送信するレートが決定されます。これは、データベース情報が古くなるのを避けるために実行されます。

（注）
LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。**lsp-refresh-interval** コマンドに対して設定される値は、**max-lsp-lifetime** コマンドに対して設定される値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 間隔と比べて LSP ライフタイムを大幅に少なく設定する場合、ソフトウェアが LSP リフレッシュ間隔を減らして、LSP がタイムアウトしないようにします。

ステップ 10 PRC の IS-IS スロットリングをカスタマイズします。

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait*：2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*prc-initial-wait*：トポロジ変更後の最初の PRC 待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された PRC 最大待機間隔に達するまでそれが行われます。
- （オプション）*prc-second-wait*：最初と 2 番目の PRC 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  PRC は SPF 計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジは変更されていないが、特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートを RIB に再インストールしようとしたりすることが必要な場合に可能です。

ステップ 11 PDU がいっぱいになったらルートを抑制するように設定します。

lsp-full suppress {external [interlevel] | interlevel [external] | none}

例：

```
ciscoasa(config-router)# lsp-full suppress interlevel external
```

- **external** この ASA 上にある再配布済みルートを抑制します。

- **interlevel**他のレベルからのルートを抑制します。たとえば、レベル 2 の LSP がフルになると、レベル 1 からのルートが抑制されます。
- **none**ルートを抑制しません。

IS-IS への再配布ルート数に制限のない（つまり **redistribute maximum-prefix** コマンドが設定されていない）ネットワークでは、LSP がフルとなり、ルートが廃棄される可能性があります。**lsp-full suppress** コマンドを使用することにより、LSP がフルになった場合にどのルートを抑制するかを事前に定義してください。

IS-IS サマリー アドレスの設定

複数のアドレス グループを特定のレベルに集約できます。他のルーティング プロトコルから学習したルートも集約できます。サマリーのアドバタイズに使用されるメトリックは、具体的なルートすべての中で最小のメトリックです。これにより、ルーティング テーブルのサイズを削減することができます。

ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。

手順

ステップ 1 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 IS-IS の集約アドレスを作成します。

summary-address *address mask* **[level-1 | level-1-2 | level-2] tag** *tag-number* **metric** *metric-value*

例：

```
ciscoasa(config-router)# summary-address 10.1.0.0 255.255.0.0 tag 100 metric 110
```

- *address*：IP アドレスの範囲を表すために指定するサマリー アドレス。
- *mask*：集約ルートに使用される IP サブネット マスク。
- （任意）**level-1**：設定済みのアドレスとマスク値を使用して、レベル 1 に再配布されたルートのみが集約されます。

- （任意）**level-1-2**：ルートをレベル 1 およびレベル 2 に再配布するとき、およびレベル 2 IS-IS がレベル 1 ルートをエリアで到達可能なものとしてアドバタイズしたときに集約ルートが適用されます。
- （任意）**level-2**：設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートはレベル 2 バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートも集約されます。
- （任意）**tag** *tag-number*：集約ルートにタグを付けるために使用される番号を指定します。指定できる範囲は 1 ～ 4294967295 です。
- （任意）**metric** *metric-value*：集約ルートに適用されるメトリック値を指定します。**metric** キーワードはリンクに割り当てられ、宛先へのリンクを介したパスコストを計算するために使用されます。このメトリックは、レベル 1 またはレベル 2 ルーティングに対してだけ設定できます。指定できる範囲は 1 ～ 4294967295 です。デフォルト値は 10 です。

インターフェイスのメトリック値を検証するため、**show clns interface** コマンドを入力します。詳細については、IS-IS の監視 （1354 ページ） を参照してください。

IS-IS パッシブ インターフェイスの設定

トポロジ データベースにインターフェイス アドレスが含まれている間は、インターフェイス上で IS-IS hello パケットおよびルーティング アップデートを無効にできます。これらのインターフェイスは、IS-IS ネイバー隣接関係を形成しません。

IS-IS ルーティングに参加させたくないが、アドバタイズしたいネットワークに接続しているインターフェイスがある場合、インターフェイスが IS-IS を使用しないようにするため、（**passive-interface** コマンドを使用して）パッシブ インターフェイスを設定します。さらに、ASA がアップデートのために使用する IS-IS のバージョンを指定することもできます。パッシブ ルーティングは、IS-IS ルーティング情報のアドバタイズメントの制御に有効であり、インターフェイスでの IS-IS ルーティング アップデートの送受信を無効にします。

手順

ステップ 1 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

ステップ 2 ASA でパッシブ インターフェイスを設定します。

passive-interface *interface-name*

例：

```
ciscoasa(config-router)# passive-interface inside
```

- **default**：すべてのインターフェイス上でルーティング アップデートを抑止します。
- **management**：管理 0/1 インターフェイスでアップデートを抑止します。
- **management2**：管理 0/2 インターフェイスでアップデートを抑止します。
- **inside**：内部インターフェイスでアップデートを抑止します。

このコマンドは、インターフェイスが IS-IS ネイバー隣接関係を形成しないが、IS-IS データベースにインターフェイス アドレスを追加するように設定します。

ステップ 3 パッシブ インターフェイスをアドバタイズするように ASA を設定します。

advertise passive-only

例：

```
ciscoasa(config-router)# advertise passive-only
```

このコマンドは、パッシブ インターフェイスに属するプレフィックスだけをアドバタイズするように IS-IS を設定します。これにより、接続されているネットワークの IP プレフィックスが LSP アドバタイズメントから除外され、IS-IS コンバージェンス時間が短縮されます。

IS-IS インターフェイスの設定

この手順では、IS-IS ルーティングのための個々の ASA インターフェイスを変更する方法について説明します。以下を変更できます。

- 一般設定（IS-IS の有効化、インターフェイス上での IS-IS シャットダウン プロトコル、優先度、タグ、隣接関係（アジャセンシー）フィルタの有効化など）。
- 認証キーとモード（インターフェイス上に認証を設定する手順については、IS-IS 認証の有効化 （1324 ページ）を参照してください）。
- hello パディング値（インターフェイスの hello パディングを設定する手順については、IS-IS インターフェイス hello パディングの設定 （1340 ページ）を参照してください）。
- LSP の設定。
- IS-iS メトリックの計算で使用されるインターフェイス遅延メトリック。

始める前に

IS-IS ルーティング プロセスを役立てるには、予め NET を割り当てる必要があります。また、いくつかのインターフェイスについて IS-IS を有効にする必要もあります。レベル 2（エリア

間）ルーティングを実行するために設定できるプロセスは 1 つだけです。レベル 2 ルーティングが任意のプロセス上に設定されている場合、追加のプロセスは、すべて自動的にレベル 1 に設定されます。このプロセスは、同時にエリア内（レベル 1）ルーティングを実行するように設定できます。1 つのインターフェイスが複数のエリアに属することはできません。ただし、関連するルーティング プロセスがレベル 1 ルーティングおよびレベル 2 ルーティングの両方を実行している場合は例外です。手順については、IS-IS ルーティングのグローバルな有効化（1320 ページ）を参照してください。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

ステップ 2 IS-IS 隣接の確立をフィルタリングします。

isis adjacency-filter *name* **[match-all]**

例：

```
ciscoasa(config-if)# isis adjacency-filter ourfriends match-all
```

- *name*：適用するフィルタ セットまたは表現の名前。
- （オプション）**match-all**：隣接関係（アジャセンシー）を受け入れるには、すべての NSAP アドレスがフィルタと一致する必要があります。指定しない場合（デフォルト）、受け入れる隣接関係（アジャセンシー）に関するフィルタに一致する必要があるのは 1 つのアドレスだけです。

着信 IS-IS hello パケットから、hello に含まれる各エリア アドレスと システム ID を組み合わせて NSAP アドレスを作成することにより、フィルタリングが実行されます。その後、これらの各 NSAP アドレスがフィルタを通過します。すべてのアドレスが適合することを要求する **match-all** キーワードが指定されていない場合は、いずれかの NSAP が一致するとフィルタに適合したと見なされます。**match-all** キーワードの機能は、特定のアドレスがない場合にのみ隣接関係（アジャセンシー）を受け入れるといったネガティブテストを実行するときに便利です。

ステップ 3 IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。

isis advertise prefix

例：

```
ciscoasa(config-if)# isis advertise prefix
```

このコマンドはデフォルトでイネーブルになります。そのため、接続されたルートは、配布を目的としていない場合でも配布されます。接続されたルートの不要な再配布を停止し、IS-IS コンバージェンス時間を改善するには、**no isis advertise prefix** コマンドを使用します。これにより、接続されているネットワークの IP プレフィックスが LSP アドバタイズメントから除外され、IS-IS コンバージェンス時間が短縮されます。

（注）
IS-IS インターフェイスごとにこのコマンドの **no** 形式を設定すると、ルータの非擬似ノード LSP でアドバタイズされるプレフィックスの数が少なくなるため、IS-IS コンバージェンス時間の短縮という課題を小規模に解決することができます。**isis advertise prefix** コマンドの代替手段としては、**advertise passive-only** コマンドがあります。これは、IS-IS インスタンスごとに設定されるため、スケーラブルなソリューションです。

ステップ 4 IS-IS インターフェイスで IPv6 を有効化します。

ipv6 router isis

例：

```
ciscoasa(config-if)# ipv6 router isis
```

ステップ 5 連続する IS-IS LSP 送信間の遅延時間をインターフェイスごとに設定します。

isis lsp-interval *milliseconds*

例：

```
ciscoasa(config-if)# isis lsp-interval 100
```

milliseconds：連続する LSP 間の遅延時間。指定できる範囲は 1 ～ 4294967298 です。デフォルトは 33 ミリ秒です。

多数の IS-IS ネイバーやインターフェイスが存在するトポロジでは、LSP 送信および受信を原因とする CPU 負荷が、ASA の障害となる可能性があります。このコマンドにより、LSP の送信率（および、暗黙のうちにその他のシステムの受信率）が低下します。

ステップ 6 IS-IS メトリックの値を設定します。

isis metric {*metric-value* | **maximum**} [**level-1** | **level-2**]

例：

```
ciscoasa(config-if)# isis metric 15 level-1
```

- *metric-value*：リンクに指定されたメトリック。このメトリックは、リンクを通じてネットワーク内の他の各ルータから他の宛先へのコスト計算に使用されます。レベル 1 またはレベル 2 のルーティングに対してこのメトリックを設定できます。範囲は 1 ～ 63 です。デフォルト値は 10 です。

- **maximum**：SPF の計算からリンクまたは隣接関係（アジャセンシー）を除外します。
- （任意）**level-1**：このメトリックがレベル 1（エリア内）ルーティングの SPF 計算だけで使用されることを表します。オプション キーワードが指定されていない場合、このメトリックはルーティングレベル 1 およびレベル 2 でイネーブルになります。
- （任意）**level-2**：このメトリックがレベル 2（エリア間）ルーティングの SPF 計算だけで使用されることを表します。オプション キーワードが指定されていない場合、このメトリックはルーティングレベル 1 およびレベル 2 でイネーブルになります。

ステップ 7 インターフェイス上の指定 ASA のプライオリティを設定します。

isis priority *number-value* **[level-1 | level-2]**

例：

```
ciscoasa(config-if)# isis priority 80 level-1
```

- *number-value*：ASA の優先順位を設定します。指定できる範囲は 0 ～ 127 です。デフォルトは 64 です。
- （任意）**level-1**：レベル 1 専用の優先順位を設定します。
- （任意）**level-2**：レベル 2 専用の優先順位を設定します。

プライオリティは、LAN 上のどの ASA が指定ルータまたは DIS であるかを決定するために使用されます。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つ ASA が DIS になります。

（注）
IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高いルータがオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

ステップ 8 指定されたインターフェイスで隣接関係（アジャセンシー）を形成できないようにして、インターフェイスの IP アドレスを ASA によって生成された LSP に配置するように IS-IS プロトコルをディセーブルにします。

isis protocol shutdown

例：

```
ciscoasa(config-if)# isis protocol shutdown
```

このコマンドを使用すると、コンフィギュレーションパラメータを削除せずに、指定されたインターフェイスの IS-IS プロトコルをディセーブルにできます。IS-IS プロトコルは、このコマンドを設定したインターフェイスの隣接関係（アジャセンシー）を形成しません。ルータが生成した LSP にインターフェイスの IP アドレスが設定されます。IS-IS がインターフェイスの隣接関係（アジャセンシー）を形成しないようにし、IS-IS LSP データベースをクリアするには、

protocol shutdown コマンドを使用します。手順については、IS-IS ルーティングのグローバルな有効化 （1320 ページ）を参照してください。

ステップ 9 各 IS-IS LSP の再伝送間の時間を設定します。

isis retransmit-interval *seconds*

例：

```
ciscoasa(config-if)#  isis retransmit-interval 60
```

（オプション）*seconds*：各 LSP の再送信の間隔。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな数値にする必要があります。指定できる範囲は 0 ～ 65535 です。デフォルトは 5 秒です。

seconds 引数は控えめな値にする必要があります。値が大きすぎると、不要な再送信が発生します。このコマンドは、LAN（マルチポイント）インターフェイスに影響を与えません。

ステップ 10 各 IS-IS LSP の再伝送間の時間を設定します。

isis retransmit-throttle-interval *milliseconds*

例：

```
ciscoasa(config-if)#  isis retransmit-throttle-interval 300
```

（オプション）*milliseconds*：インターフェイスにおける LSP 再送信間の最小遅延。指定できる範囲は 0 ～ 65535 です。

このコマンドは、LSP 再送信トラフィックの制御方法と同様に、多くの LSP およびインターフェイスを持つ大規模なネットワークで役立つ場合があります。このコマンドは、インターフェイスで LSP を再送信できるレートを制御します。

このコマンドは、LSP がインターフェイス上で送信されるレート（**isis lsp-interval** コマンドで制御）および単一 LSP の再送信間隔（**isis retransmit-interval** コマンドで制御）とは異なります。これらのコマンドを組み合わせて使用することにより、1 つの ASA からのそのネイバーへのルーティング トラフィックで発生する負荷を制御できます。

ステップ 11 この IP プレフィックスが IS-IS LSP に設定されている場合に、インターフェイスに設定された IP アドレスにタグを設定します。

isis tag *tag-number*

例：

```
ciscoasa(config-if)# isis tag 100
```

tag-number：IS-IS ルートでタグとして機能する番号。指定できる範囲は 1 ～ 4294967295 です。

タグが使用されないかぎり、タグ付けされたルートではいかなるアクション（ルートの再配布やルートの集約のためのアクションなど）も発生しません。このコマンドを設定すると、タグがパケット内の新規の情報であるため、ASA は新しい LSP をトリガーします。

例

次に、2 つのインターフェイスに異なるタグ値をタグ付けする例を示します。デフォルトでは、これらの 2 つの IP アドレスは IS-IS レベル 1 およびレベル 2 のデータベースに設定されています。ただし、**redistribute** コマンドを使用してルートマップをタグ 110 に一致させると、IP アドレス 172.16. 0.0 だけがレベル 2 データベースに設定されます。

```
ciscoasa (config)# interface GigabitEthernet1/0
ciscoasa (config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 120
ciscoasa (config)# interface GigabitEthernet1/1
ciscoasa (config-if)# ip address 172.16.0.0
ciscoasa (config-if)# isis
ciscoasa (config-if)# isis tag 110
ciscoasa (config-router)# route-map match-tag permit 10
ciscoasa (config-router)# match tag 110
ciscoasa (config)# router isis
ciscoasa (config-router)# net 49.0001.0001.0001.0001.00
ciscoasa (config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
```

IS-IS インターフェイス hello パディングの設定

helloパケットは、ネイバーの検出と維持に使用されます。インターフェイス レベルで次の hello パディング パラメータを設定できます。IS-IS 全体で hello パディングを有効/無効にする場合は、IS-IS ルーティングのグローバルな有効化 （1320 ページ）を参照してください。

手順

ステップ 1 インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis
```

ステップ 2 インターフェイス コンフィギュレーション モードを開始し、ASA のすべてのインターフェイスに対して、IS-IS hello プロトコル データ ユニット（PDU）のパディングを設定します。

isis hello padding

例：

```
ciscoasa(config-if)# isis hello padding
```

hello がフル MTU に埋め込まれます。これにより、大きなフレームに関連した送信問題によるエラーや隣接インターフェイスの MTU 不一致によるエラーの検出が可能になります。IS-IS hello パディングは、デフォルトで有効になっています。

（注）
両方のインターフェイスの MTU が同じである場合やトランスレーショナル ブリッジングの場合には、ネットワーク帯域幅の無駄を省くため、hello パディングをディセーブルにできます。hello パディングがディセーブルになっても、ASA は、MTU 不一致検出の利点を維持するため、最初の 5 回の IS-IS hello をフルサイズの MTU に埋め込みます。

ステップ 3 IS-IS によって送信される連続した hello パケット間の時間を指定します。

isis hello-interval {*seconds* | **minimal**} **[level-1 | level-2]**

例：

```
ciscoasa(config-if)# isis hello-interval 5 level-1
```

- *seconds*：hello パケットの送信間隔。デフォルトでは、送信される hello パケットで、hello インターバル（seconds）の 3 倍の値が保持時間としてアドバタイズされます**isis hello-multiplier** コマンドを設定することにより、この乗数（3）を変更できます。hello インターバルが狭まると、トポロジ変更の検出も速くなりますが、ルーティング トラフィック量は増大します。指定できる範囲は 0 ～ 65535 です。デフォルトは 10 です。
- **minimal**：結果として得られるホールド タイムが 1 秒になるように、**isis hello-multiplier** コマンドで指定された hello 乗数に基づいて hello 間隔を計算することをシステムに指示します。
- （オプション）**level-1**：レベル 1 での hello 間隔を個別に設定します。X.25、Switched Multimegabit Data Service（SMDS）、フレーム リレー マルチアクセス ネットワークでは、これを使用します。
- （オプション）**level-2**：レベル 2 での hello 間隔を個別に設定します。X.25、SMDS、フレーム リレー マルチアクセス ネットワークでは、これを使用します。

（注）
hello 間隔を長くすると帯域幅と CPU 使用率を節約できますが、トラフィック エンジニアリング（TE）トンネルを使用する大規模構成などの一部の状況では、短い hello 間隔が推奨されます。TE トンネルが IS-IS を内部ゲートウェイ プロトコル（IGP）として使用する場合、IP ルーティング プロセスがネットワークの入力点のルータ（ヘッドエンド）で再起動されると、すべての TE トンネルがデフォルトの hello 間隔で再シグナル化されます。再シグナル化を回避するには、hello 間隔を短くします。multiplier{1} command.hello 間隔をさらに短く設定するには、**isis hello-multiplier** コマンドを使用して、IS-IS の hello 間隔を手動で増やす必要があります。

ステップ 4 ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接関係（アジャセンシー）がダウンしていると宣言します。

isis hello-multiplier *multiplier* **[level-1 | level-2]**

例：

```
ciscoasa(config-if)# isis hello-multiplier 10 level-1
```

- *multipler*：IS-IS hello パケットのアドバタイズされる保持時間は、hello 間隔に hello 乗数を掛けた値に設定されます。ネイバーは、アドバタイズされた保持時間中に IS-IS hello パケットをまったく受信しなかった場合、この ASA への隣接関係（アジャセンシー）がダウンしていると宣言します。保持時間（つまり、hello 乗数と hello 間隔）はインターフェイス単位で設定できます。また、1 つのエリア内のルータごとに別々の保持時間を設定できます。指定できる範囲は 3 ～ 1000 です。デフォルトは 3 です。
- （オプション）**level-1**：レベル 1 隣接での hello 乗数を個別に設定します。
- （オプション）**level-2**：レベル 2 隣接での hello 乗数を個別に設定します。

hello パケットが頻繁に失われ、IS-IS 隣接が不必要に失敗する場合は、このコマンドを使用します。

（注）
hello 乗数を小さくすると、コンバージェンスが高速になりますが、ルーティングが不安定になる可能性があります。必要に応じて、ネットワークの安定性を高めるために hello 乗数の値を変更してください。hello 乗数をデフォルトの 3 未満の値に設定しないでください。

ステップ 5 IS-IS に使用される隣接関係（アジャセンシー）のタイプを設定します。

isis circuit-type [level-1 | level-1-2 | level-2-only]

例：

```
ciscoasa(config-if)# isis circuit-type level-2-only
```

- （オプション）**level-1**：レベル 1 の隣接関係に対してのみ ASA を設定します。
- （オプション）**level-1-2**：レベル 1 およびレベル 2 の隣接関係に対して ASA を設定します。
- （オプション）**level-2**：レベル 2 の隣接関係に対してのみ ASA を設定します。

通常、このコマンドを設定する必要はありません。ASA でレベルを設定するのが適切な方法です。手順については、IS-IS ルーティングのグローバルな有効化（1320 ページ）を参照してください。エリア（レベル1 ～ 2 ルータ）間にある ASA でのみ、一部のインターフェイスをレベル 2 として設定する必要があります。これにより、未使用の レベル1 hello パケットを送信することで帯域幅を節約できます。

ステップ 6 ブロードキャストインターフェイス上で定期的にCSNPパケットが送信される間隔を設定します。

isis csnp-interval *seconds* **[level-1 | level-1-2 | level-2]**

例：

```
ciscoasa(config-if)#  isis csnp-interval 30 level-1
```

- *seconds*：マルチアクセス ネットワークでの CSNP の転送間隔。この間隔は指定 ASA だけに適用されます。指定できる範囲は 0 ～ 65,535 です。デフォルトは 10 秒です。
- （オプション）**level-1**：レベル 1 での CSNP の転送間隔を個別に設定します。
- （オプション）**level-2**：レベル 2 での CSNP の転送間隔を個別に設定します。

このコマンドのデフォルト値を変更する必要はほとんどありません。

このコマンドは、指定したインターフェイスのDRに対してのみ適用されます。DRだけがデータベースの同期を維持するためにCSNPパケットを送信します。レベル 1 とレベル 2 で個別に CSNP 間隔を設定できます。

IS-IS IPv4 アドレス ファミリの設定

ルータからは、他の任意のルーティングプロトコル、スタティック設定、または接続されたインターフェイスから学習した外部プレフィックスまたはルートを再配布できます。再配布されたルートはレベル 1 ルータまたはレベル 2 ルータで許可されます。

隣接関係（アジャセンシー）、最短パス優先（SPF）を設定し、IPv4 アドレスに対し、別のルーティング ドメインからISIS（再配布）にルートを再配布するための条件を定義できます。

始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化（1320 ページ）を参照してください。

手順

ステップ 1 IPv4 アドレス ファミリを設定するには、ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
ciscoasa(config)# router isis
```

```
cisco(config-router)#
```

ステップ 2 隣接関係（アジャセンシー）チェックを実行して、IS-IS プロトコル サポートを確認します。

adjacency-check

例：

```
cisco(config-router)# adjacency-check
```

ステップ 3 IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。

distance *weight*

weight：IS-IS ルートに割り当てられるアドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。

例：

```
ciscoasa(config-router)# distance 20
```

このコマンドは、IS-IS ルートが RIB に挿入されるときに適用されるディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性に影響を与えます。

（注）
通常は、アドミニストレーティブディスタンスの値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

ステップ 4 IS-IS のマルチパス ロード シェアリングを設定します。

maximum-paths *number-of-paths*

例：

```
ciscoasa(config-router)# maximum-paths 8
```

number-of-paths：ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。デフォルトは 1 です。

maximum-path コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチロード シェアリングを設定するために使用されます。

ステップ 5 IS-IS ルーティング ドメインへのデフォルト ルートを生成します。

default-information originate [**route-map** *map-name*]

例：

```
ciscoasa(config-router)# default-information originate route-map RMAP
```

（任意）**route-map** *map-name*：ルーティング プロセスは、ルート マップが満たされている場合にデフォルト ルートを生成します。

このコマンドを使用して設定された ASA がルーティング テーブルに 0.0.0.0 へのルートを持っている場合、IS-IS は LSP で 0.0.0.0 に対するアドバタイズメントを発信します。ルート マップが存在しない場合、デフォルトではレベル 2 LSP だけでアドバタイズされます。レベル 1 ルーティングでデフォルト ルートを発見するメカニズムには、最も近いレベル 1 またはレベル 2 ルータを探すというものがあります。最も近いレベル 1 またはレベル 2 ルータは、レベル 1 LSP で ATT を調べることにより検出できます。**match ip address** *standard-access-list* コマンドを使用することで、ASA が 0/0 をアドバタイズする前に存在している必要がある 1 つ以上の IP ルートを指定できます。

ステップ 6 IS-IS メトリックをレベル 1 およびレベル 2 に対しグローバルに設定します。

metric *default-value* **[level-1 | level-2]**

例：

```
ciscoasa(config-router)# metric 55 level-1
ciscoasa(config-router)# metric 45 level-2
```

- *default-value*：リンクに割り当てられ、宛先へのリンクを介したパス コストを計算するために使用されるメトリック値。指定できる範囲は 1 ～ 63 です。デフォルトは 10 です。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。

ステップ 7 メトリック スタイルおよび適用するレベルを指定します。

metric-style [narrow | transition | wide] [level-1 | level-2 | level-1-2]

例：

```
ciscoasa(config-router)# metric-style wide level-1
```

- **narrow**：旧スタイルの TLV とナロー メトリックを使用するように ASA に指示します。
- **transition**：移行時に旧スタイルおよび新スタイルの TLV の両方を受け入れるように ASA に指示します。
- **wide**：新スタイルの TLV を使用してワイド メトリックを伝送するように ASA に指示します。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-1-2**：レベル 1 とレベル 2 の IPv4 または IPv6 メトリックを設定します。

ステップ 8 レベル 1 - レベル 2 ルータがその接続ビットを設定する必要がある場合の制約を指定します。

set-attached-bit route-map *map-tag*

例：

```
ciscoasa(config-router)# set-attached-bit route-map check-for-L2_backbone_connectivity
```

route-map *map-tag*：設定したルート マップの識別情報。指定されたルート マップが一致した場合、ルータはその接続ビットを引き続き設定します。このコマンドは、デフォルトでディセーブルになっています。

ISO 10589 に指定されているように、現在の IS-IS 実装で、レベル 1 - レベル 2 ルータは、自ドメイン内の他のエリアを認識する際や、他のドメインを認識する際に、レベル 1 LSP 接続ビットを設定します。ただし、ネットワーク トポロジの中には、別のエリアにある隣接レベル 1 - レベル 2 ルータとレベル 2 バックボーンとの接続が失われている可能性のあるものもあります。レベル 1 ルータは、エリアやドメイン外の宛先へのトラフィックを、レベル 2 バックボーンとの接続がない可能性のあるレベル 1 - レベル 2 ルータへ送信できます。

このコマンドによって、レベル 1 - レベル 2 ルータの接続ビット設定に対し、より詳細な制御が可能になります。ルート マップは、1 つ以上の CLNS ルートを指定できます。少なくとも 1 つの match address route map 句がレベル 2 CLNS ルーティング テーブル内のルートと一致し、接続ビットを設定するためのその他すべての要件が合致する場合、レベル 1 - レベル 2 ルータはレベル 1 LSP に接続ビットを設定し続けます。要件に合致しない場合や、match address route map 句がレベル 2 CLNS ルーティング テーブル内のルートと一致しない場合、接続ビットは設定されません。

ステップ 9 SPF 計算の中間ホップとして使用しないように、ASA が他のルータに通知するように ASA を設定します。

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

例：

```
ciscoasa(config-router)# set-overload-bit on-startup wait-for-bgp suppress interlevel
external
```

- （任意）**on-startup**：システム起動時の過負荷ビットを設定します。過負荷ビットは、後続の指定引数またはキーワードに応じて、設定された秒数、または BGP が収束するまで設定されたままになります。
- （オプション）*seconds*：システム起動時に過負荷ビットが設定され、設定された状態が続く秒数。指定できる範囲は 5 ～ 86400 です。
- （任意）**wait-for-bgp**：**on-startup** キーワードが設定されている場合、過負荷ビットがシステム起動時に設定され、BGP が収束するまで設定されたままになります。
- （任意）**suppress**：後続キーワードによって指定されるプレフィックスのタイプが抑制されます。
- （任意）**interlevel**：**suppress** キーワードが設定されている場合、別の IS-IS レベルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。
- （任意）**external**：**suppress** キーワードが設定されている場合、他のプロトコルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。

このコマンドは、ASA に対して、非疑似 LSP に過負荷ビット（「hippity bit」とも呼ばれる）を強制的に設定させます。通常、過負荷ビットの設定は、ASA で問題が発生した場合にのみ許可されます。たとえば、ASA でメモリ不足が発生した場合、リンクステート データベースが不完全であり、その結果不完全または不正確なルーティング テーブルが生成されている可能性があります。LSP に過負荷ビットを設定することにより、ルータが問題から復旧するまで、他のルータがその SPF 計算で信頼できないルータを無視することができます。その結果、このルータを通過するパスは、IS-IS エリア内の他のルータから見えなくなります。ただし、IP および CLNS プレフィックスはこのルータに直接接続されます。

ステップ 10 PRC の IS-IS スロットリングをカスタマイズします。

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

例：

```
ciscoasa(config-router)#  prc-interval 5 10 20
```

- *prc-max-wait*：2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*prc-initial-wait*：トポロジ変更後の最初の PRC 待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された PRC 最大待機間隔に達するまでそれが行われます。
- （オプション）*prc-second-wait*：最初と 2 番目の PRC 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  PRC は SPF 計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジは変更されていないが、特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートを RIB に再インストールしようとしたりすることが必要な場合に可能です。

ステップ 11 SPF 計算の IS-IS スロットリングをカスタマイズします。

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

例：

```
ciscoasa(config-router)#  spf-interval level-1 5 10 20
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *spf-max-wait*：2 つの連続 SPF 計算間の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。

- （オプション）*spf-initial-wait*：トポロジが変更されてから、最初の SPF 計算までの初期の待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された SPF 最大待機間隔に達するまでそれが行われます。

- （オプション）*spf-second-wait*：最初と 2 番目の SPF 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

SPF 計算が実行されるのは、トポロジが変更されたときだけです。このコマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。

（注）
SPF 計算は、プロセッサに高い負荷を与えます。したがって、特にエリアが大きくてトポロジが頻繁に変更される場合は、これを実行する頻度を制限すると役に立つことがあります。SPF 間隔を大きくすると、ASA のプロセッサ負荷が軽減されますが、コンバージェンス速度が低下する可能性があります。

ステップ 12 SFP 計算中は外部メトリックを使用するように IS-IS を設定します。

use external-metrics

ステップ 13 BGP、接続、IS-IS、OSPF、またはスタティック ルート再配布を設定します。

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

例：

```
ciscoasa(config-router)# redistribute bgp level-1 metric-type internal metric 6
```

（注）
メトリックに一致するルートマップを使用したスタティックルートの再配布はサポートされていません。

metric *number*：メトリックの値。指定できる範囲は 1 ～ 4294967295 です。

接続ビットの設定

次の例では、ルータが L2 CLNS ルーティング テーブル内の 49.00aa と一致する際に接続ビットが設定されたままになります。

```
ciscoasa(config)# router isis
 ciscoasa(config-router)# clns filter-set L2_backbone_connectivity permit 49.00aa
 ciscoasa(config-router)# route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# match clns address L2_backbone_connectivity
ciscoasa(config)# router isis
 ciscoasa(config-router)#set-attached-bit route-map check-for-L2_backbone_connectivity
 ciscoasa(config-router)# end
 ciscoasa# show clns route 49.00aa
```

```
Known via "isis", distance 110, metric 30, Dynamic Entry
Routing Descriptor Blocks:
 via tr2, Serial0
   isis, route metric is 30, route version is 58
```

IS-IS IPv6 アドレス ファミリの設定

隣接関係（アジャセンシー）、SPF を設定し、IPv6 アドレスに対し、別のルーティング ドメインから IS-IS（再配布）にルートを再配布するための条件を定義できます。

始める前に

IS-IS のルート認証を有効にするには、予め IS-IS を有効にしてエリアを設定しておく必要があります。手順については、IS-IS ルーティングのグローバルな有効化（1320 ページ）を参照してください。

手順

ステップ 1 ルータ コンフィギュレーション モードを開始します。

router isis

例：

```
cisco(config-router)#
```

ステップ 2 メトリック スタイルを以下の範囲で指定します。

metric-style wide [transition] [level-1 | level-2 | level-1-2]

例：

```
ciscoas(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

- （任意）**transition**：旧スタイルおよび新スタイルの TLV の両方を受け入れるようにルータに指示します。
- （任意）**level-1**：レベル 1 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-2**：レベル 2 IPv4 または IPv6 メトリックを設定します。
- （任意）**level-1-2**：レベル 1 とレベル 2 の IPv4 または IPv6 メトリックを設定します。

すべての IS-IS インターフェイスに対してデフォルトのメトリックを変更する必要がある場合は、**metric** コマンドを使用することをお勧めします。こうすることで、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルトメトリック 10

に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

ステップ 3 標準 IPv4 または IPv6 アドレス プレフィックスを使用する IS-IS ルーティング セッションを設定するために、アドレス ファミリ コンフィギュレーション モードを開始します。

address-family ipv6 [unicast]

例：

```
ciscoasa(config-router)# address-family ipv6 unicast
cisco(config-router-af)#
```

ステップ 4 隣接関係（アジャセンシー）チェックを実行して、IS-IS プロトコル サポートを確認します。

adjacency-check

例：

```
cisco(config-router-af)# adjacency-check
```

ステップ 5 IS-IS のマルチパス ロード シェアリングを設定します。

maximum-paths *number-of-paths*

例：

```
ciscoasa(config-router-af)# maximum-paths 8
```

number-of-paths：ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。デフォルトは 1 です。

maximum-path コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチロード シェアリングを設定するために使用されます。

ステップ 6 IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。

distance *weight*

weight：IS-IS ルートに割り当てられるアドミニストレーティブ ディスタンス。指定できる範囲は 1 ～ 255 です。デフォルトは 115 です。

例：

```
ciscoasa(config-router-af)# distance 20
```

このコマンドは、IS-IS ルートが RIB に挿入されるときに適用されるディスタンスを設定し、他のプロトコルによって検出された同じ宛先アドレスへのルートよりもこれらのルートが優先される可能性に影響を与えます。

（注）

通常は、アドミニストレーティブディスタンスの値が大きいほど、信頼性の格付けが下がります。255 のアドミニストレーティブディスタンスは、ルーティング情報源がまったく信頼できないため、無視すべきであることを意味します。重み値は主観的に選択します。重み値を選択するための定量的方法はありません。

ステップ 7 IS-IS ルーティング ドメインへのデフォルト ルートを生成します。

default-information originate [**route-map** *map-name*]

例：

```
ciscoasa(config-router-af)# default-information originate route-map TEST7
```

（任意）**route-map** *map-name*：ルーティング プロセスは、ルート マップが満たされている場合にデフォルト ルートを生成します。

このコマンドを使用して設定された ASA がルーティング テーブルに 0.0.0.0 へのルートを持っている場合、IS-IS は LSP で 0.0.0.0 に対するアドバタイズメントを発信します。ルート マップが存在しない場合、デフォルトではレベル 2 LSP だけでアドバタイズされます。レベル 1 ルーティングでデフォルト ルートを発見するメカニズムには、最も近いレベル 1 またはレベル 2 ルータを探すというものがあります。最も近いレベル 1 またはレベル 2 ルータは、レベル 1 LSP で ATT を調べることにより検出できます。**match ip address** *standard-access-list* コマンドを使用することで、ASA が 0/0 をアドバタイズする前に存在している必要がある 1 つ以上の IP ルートを指定できます。

ステップ 8 SPF 計算の中間ホップとして使用しないように、ASA が他のルータに通知するように ASA を設定します。

set-overload-bit [on-startup {*seconds* | **wait-for bgp**}] [**suppress [[interlevel] [external**]]]

例：

```
ciscoasa(config-router-af)# set-overload-bit on-startup wait-for-bgp suppress interlevel
 external
```

- （任意）**on-startup**：システム起動時の過負荷ビットを設定します。過負荷ビットは、後続の指定引数またはキーワードに応じて、設定された秒数、または BGP が収束するまで設定されたままになります。
- （オプション）*seconds*：システム起動時に過負荷ビットが設定され、設定された状態が続く秒数。指定できる範囲は 5 ～ 86400 です。
- （任意）**wait-for-bgp**：**on-startup** キーワードが設定されている場合、過負荷ビットがシステム起動時に設定され、BGP が収束するまで設定されたままになります。
- （任意）**suppress**：後続キーワードによって指定されるプレフィックスのタイプが抑制されます。
- （任意）**interlevel**：**suppress** キーワードが設定されている場合、別の IS-IS レベルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。

- （任意）**external**：**suppress** キーワードが設定されている場合、他のプロトコルから学習された IP プレフィックスがアドバタイズされるのを防ぎます。

このコマンドは、ASA に対して、非疑似 LSP に過負荷ビット（「hippity bit」とも呼ばれる）を強制的に設定させます。通常、過負荷ビットの設定は、ASA で問題が発生した場合にのみ許可されます。たとえば、ASA でメモリ不足が発生した場合、リンクステート データベースが不完全であり、その結果不完全または不正確なルーティング テーブルが生成されている可能性があります。LSP に過負荷ビットを設定することにより、ルータが問題から復旧するまで、他のルータがその SPF 計算で信頼できないルータを無視することができます。その結果、このルータを通過するパスは、IS-IS エリア内の他のルータから見えなくなります。ただし、IP および CLNS プレフィックスはこのルータに直接接続されます。

ステップ 9 PRC の IS-IS スロットリングをカスタマイズします。

prc-interval *prc-max-wait [prc-intial-wait prc-second wait]*

例：

```
ciscoasa(config-router-af)#  prc-interval 5 10 20
```

- *prc-max-wait*：2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 5 秒です。
- （オプション）*prc-initial-wait*：トポロジ変更後の最初の PRC 待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された PRC 最大待機間隔に達するまでそれが行われます。
- （オプション）*prc-second-wait*：最初と 2 番目の PRC 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5000 ミリ秒（5 秒）、

  PRC は SPF 計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジは変更されていないが、特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートを RIB に再インストールしようとしたりすることが必要な場合に可能です。

ステップ 10 SPF 計算の IS-IS スロットリングをカスタマイズします。

spf-interval [level-1 | level-2] *spf-max-wait [spf-intial-wait spf-second wait]*

例：

```
ciscoasa(config-router-af)#  spf-interval level-1 5 10 20
```

- （任意） **level-1**：レベル 1 エリアにのみ間隔を適用します。
- （任意）**level-2**：レベル 2 エリアにのみ間隔を適用します。
- *spf-max-wait*：2 つの連続 SPF 計算間の最大間隔を示します。範囲は、1 ～ 120 秒です。デフォルトは 10 秒です。

- （オプション）*spf-initial-wait*：トポロジが変更されてから、最初の SPF 計算までの初期の待機時間を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

  その後の待機間隔はそれぞれ、その前の間隔の 2 倍の長さになり、指定された SPF 最大待機間隔に達するまでそれが行われます。

- （オプション）*spf-second-wait*：最初と 2 番目の SPF 計算間の間隔を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 5500 ミリ秒（5.5 秒）、

SPF 計算が実行されるのは、トポロジが変更されたときだけです。このコマンドは、ソフトウェアが SPF 計算を実行する頻度を制御します。

（注）
SPF 計算は、プロセッサに高い負荷を与えます。したがって、特にエリアが大きくてトポロジが頻繁に変更される場合は、これを実行する頻度を制限すると役に立つことがあります。SPF 間隔を大きくすると、ASA のプロセッサ負荷が軽減されますが、コンバージェンス速度が低下する可能性があります。

ステップ 11 BGP、接続、IS-IS、OSPF、またはスタティック ルート再配布を設定します。

redistribute bgp | connected | isis | ospf | static | level-1 | level-2 | level 1-2 metric-type internal | external metric *number*

例：

```
ciscoasa(config-router-af)# redistribute static level-1 metric-type internal metric 6
```

metric *number*：メトリックの値。指定できる範囲は 1 ～ 4294967295 です。

ステップ 12 特にレベル 1 からレベル 2 またはレベル 2 からレベル 1 へ IS-IS ルートを再配布します。

redistribute isis {level-1 | level-2} into {level-2 | level-1} [[distribute-list *list-number* **| [route-map** *map-tag***]]**

例：

```
ciscoasa(config-router-af)# redistribute isis level-1 into level-2
distribute-list 100
```

- **level-1 | level-2**：IS-IS ルートを再配布するレベル元とレベル先。
- **into**：ルートが再配布されるレベル元と、ルートを再配布するレベル先を区別するキーワード。
- （任意）**distribute-list** *list-number*：IS-IS 再配布を制御する配布リスト番号。配布リストまたはルート マップのいずれかを指定できますが、両方を指定できません。
- （任意）**route-map** *map-tag*：IS-IS 再配布を制御するルート マップ名。配布リストまたはルート マップのいずれかを指定できますが、両方を指定できません。

（注）

redistribute isis コマンドを機能させるためには、**metric-style wide** コマンドを指定する必要があります。この手順のステップ 1 を参照してください。

IS-IS では、すべてのエリアがスタブ エリアで、バックボーン（レベル 2）からエリア（レベル 1）へルーティング情報がリークしません。レベル 1 だけのルートは、そのエリア内にある最も近いレベル 1 - レベル 2 ルータへのデフォルト ルートを使用します。このコマンドにより、レベル 2 IP ルートをレベル 1 エリアに再配布することができます。この再配布により、レベル 1 だけのルータが IP プレフィックスのエリア外への最良パスを選択することができるようになります。これは IP のみの機能であり、CLNS ルーティングはまだスタブ ルーティングです。

（注）
制御と安定性を増すために、配布リストまたはルートマップを設定して、どのレベル 2 IP ルートをレベル 1 に再配布できるのかを制御できます。これを使用すると、大規模な IS-IS-IP ネットワークは、スケーラビリティを向上させるためにエリアを使用できます。

ステップ 13 IS-IS IPv6 ルートの集約プレフィックスを作成します。

summary-prefix *ipv6-prefix* **[level-1 | level-1-2 | level-2]**

例：

```
cisco(config-router-af)# summary-prefix 2001::/96 level-1
```

- *ipv6 address*：X.X.X.X.::X/0-128 形式の IPv6 プレフィックス。
- （任意）**level-1**：設定済みのアドレスとマスク値を使用して、レベル 1 に再配布されたルートのみが集約されます。
- （任意）**level-1-2**：ルートをレベル 1 およびレベル 2 IS-IS に再配布するとき、およびレベル 2 IS-IS がレベル 1 のルートをエリア内で到達可能なものとしてアドバタイズするときに、サマリー ルートが適用されます。
- （任意）**level-2**：設定済みアドレスとマスク値を使用して、レベル 1 ルーティングが学習したルートはレベル 2 バックボーンに集約されます。レベル 2 の IS-IS に再配布されたルートも集約されます。

IS-IS の監視

次のコマンドを使用して、IS-IS ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。

IS-IS データベースのモニタリング

IS-IS データベースをモニタリングするには、次のコマンドを使用します。

- **show isis database [level-1 | l1] [level-2 | l2] [detail]** ：レベル 1、レベル 2、および各 LSP の詳細な内容について、IS-IS リンクステート データベースを表示します。

- **show isis database verbose** ：IS-IS データベースに関する詳細情報（LSP のシーケンス番号、チェックサム、保留時間など）を表示します。

IS-IS マッピング テーブル エントリのモニタリング

IS-IS ホスト名をモニタリングするには、次のコマンドを使用します。

show isis hostname：IS-IS ルータの、ルータ名とシステム ID のマッピング テーブル エントリを表示します。

IS-IS IPv4 のモニタリング

IS-IS IPv4 をモニタリングするには、次のコマンドを使用します。

- **show isis ip rib**：IS-IS ルーティング プロセスの、IPv4 アドレス ファミリ固有の RIB を表示します。
- **show isis ip spf-log**：IS-IS ルーティング プロセスの、IPv4 アドレス ファミリ固有の SPF ログを表示します。
- **show isis ip topology**：IS-IS ルーティング プロセスの、IPv4 アドレス ファミリ固有のトポロジを表示します。
- **show isis ip redistribution** [**level-1** | **level-2**] [*network-prefix*]：IS-IS によって学習され、インストールされた IPv6 ルートを表示します。
- **show isis ip unicast**：IPv4 アドレス ファミリ固有の RIB、SPF ログ、および IS へのパスを表示します。

IS-IS IPv6 のモニタリング

IS-IS IPv6 をモニタリングするには、次のコマンドを使用します。

- **show isis ipv6 rib**：IS-IS ルーティング プロセスの、IPv6 アドレス ファミリ固有の RIB を表示します。
- **show isis ipv6 spf-log**：IS-IS ルーティング プロセスの、IPv6 アドレス ファミリ固有の SPF ログを表示します。
- **show isis ipv6 topology**：IS-IS ルーティング プロセスの、IPv6 アドレス ファミリ固有のトポロジを表示します。
- **show isis ipv6 redistribution** [**level-1** | **level-2**] [*network-prefix*]：IS-IS によって学習され、インストールされた IPv6 ルートを表示します。
- **show isis ipv6 unicast**：IPv6 アドレス ファミリ固有の RIB、SPF ログ、および IS へのパスを表示します。

IS-IS ログのモニタリング

IS-IS ログをモニタリングするには、次のコマンドを使用します。

- **show isis lsp-log**：新しい LSP をトリガーしたインターフェイスのレベル 1 およびレベル 2 の IS-IS LSP ログを表示します。

- **show isis spf-log**：ASA が SPF 計算を実行した頻度と、実行理由を表示します。

IS-IS プロトコルのモニタリング

IS-IS プロトコルをモニタリングするには、次のコマンドを使用します。

show clns protocol ：ASA での各 IS-IS ルーティング プロセスのプロトコル情報を表示します。

IS-IS ネイバーおよびルートのモニタリング

IS-IS ネイバーをモニタリングするには、次のコマンドを使用します。

- **show isis topology** ：すべてのエリア内の接続されたルータすべてのリストを表示します。このコマンドは、すべてのエリア内のすべてのルータの存在と接続を確認します。
- **show isis neighbors [detail]** ：IS-IS 隣接関係（アジャセンシー）情報を表示します。
- **show clns neighbors** [*process-tag*] [*interface-name*] [**detail**]：エンド システム（ES）、中継システム（IS）およびマルチトポロジ IS-IS（M-ISIS）ネイバーを表示します。このコマンドは、IPv6 のマルチトポロジ IS-IS を介して学習された隣接関係（アジャセンシー）を表示します。
- **show clns is-neighbors** *[interface-name]* **[detail]** ：IS-IS デバイス隣接関係の IS-IS 情報を表示します。

IS-IS RIB のモニタリング

IS-IS RIB をモニタリングするには、次のコマンドを使用します。

- **show isis rib** [*ip-address* | *ip-address-mask*]：RIB に保存されている主要なネットワークの特定のルートのパス、またはすべてのルートのパスを表示します。
- **show isis rib redistribution** [**level-1** | **level-2**] [*network-prefix*]：ローカル再配布キャッシュのプレフィックスを表示します。
- **show route isis** ルーティング テーブルの現在の状態を表示します。

IS-IS トラフィックのモニタリング

IS-IS トラフィックをモニタリングするには、次のコマンドを使用します。

show clns traffic [since {bootup | show}] ：ASA が認識した CLNS トラフィック統計情報を表示します。

IS-IS のデバッグ

IS-IS をデバッグするには、次のコマンドを使用します。

debug isis [adj-packets | authentication | checksum-errors | ip | ipv6 | local-updates | [rptpcp;-errors | rob | snp-packets | spf-events | spf-statistics | spf-triggers | update-packets]：IS-IS ルーティング プロトコルのさまざまな要素をデバッグします。

IS-IS の履歴

表 *43 : IS-IS* の機能の履歴

機能名	プラットフォーム リリース	機能情報
IS-IS ルーティング	9.6(1)	ASA で Intermediate System to Intermediate System（IS-IS）のルーティング プロトコルがサポートされました。IS-IS ルーティング プロトコルを使用した、データのルーティング、認証の実行、およびルーティング情報の再配布とモニターについて、サポートが追加されました。 次のコマンドが導入されました。 **advertise passive-only, area-password, authentication key, authentication mode, authentication send-only, clear, debug isis, distance, domain-password, fast-flood, hello padding, hostname dynamic, ignore-lsp-errors, isis adjacency-filter, isis advertise prefix, isis authentication key, isis authentication mode, isis authentication send-only, isis circuit-type, isis csnp-interval, isis hello-interval, isis hello-multiplier, isis hello padding, isis lsp-interval, isis metric, isis password, isis priority, isis protocol shutdown, isis retransmit-interval, isis retransmit-throttle-interval, isis tag, is-type, log-adjacency-changes, lsp-full suppress, lsp-gen-interval, lsp-refresh-interval, max-area-addresses, max-lsp-lifetime, maximum-paths, metric, metric-style, net, passive-interface, prc-interval, protocol shutdown, redistribute isis, route priority high, router isis, set-attached-bit, set-overload-bit, show clns, show isis, show route isis, spf-interval, summary-address**.

IS-IS の例

このセクションでは、IS-IS のさまざまな要素についてトポロジによる設定例を示します。

IS-IS ルーティングの設定

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   isis
```

IS-IS IPv6 ルーティングの設定

```
router isis
   net 49.1234.aaaa.bbbb.cccc.00

interface GigabitEthernet0/0
   ipv6 address 2001:192:16:32::1/64
   ipv6 router isis
```

同一エリア内でのダイナミック ルーティング

```
iRouter --------(inside G0/1) ASA (G0/0 outside)------------ oRouter

ASA Configuration
  interface GigabitEthernet0/0
   nameif outside
   security-level 0
   ip address 192.16.32.1 255.255.255.0
   ipv6 address 2001:192:16:32::1/64
   isis
   ipv6 router isis

  interface GigabitEthernet0/1
   nameif inside
   security-level 100
   ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
   ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
   isis
   ipv6 router isis

  router isis
   net 49.1234.2005.2005.2005.00
   is-type level-1
   metric-style wide

  interface GigabitEthernet0/0
   ip address 172.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:16:32::3/64
   ipv6 router isis
   isis priority 120

  interface GigabitEthernet0/1
   ip address 172.26.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:172:26:32::3/64
   ipv6 router isis

IOS Configuration
  iRouter
  router isis
   net 49.1234.2035.2035.2035.00
   is-type level-1
   metric-style wide

  oRouter
  interface GigabitEthernet0/0
   ip address 192.16.32.3 255.255.255.0
   ip router isis
   ipv6 address 2001:192:16:32::3/64
   ipv6 router isis

  oRouter
```

```
 interface GigabitEthernet0/1
  ip address 192.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:192:26:32::3/64
  ipv6 router isis

 oRouter
 router isis
  net 49.1234.2036.2036.2036.00
  is-type level-1
  metric-style wide
```

複数エリアでのダイナミック ルーティング

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis

 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis

 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 5
  exit-address-family
 !

IOS Configuration
 iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120


 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:26:32::3/64
  ipv6 router isis


 iRouter
 router isis
  net 49.1234.2035.2035.2035.00
```

```
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

重複するエリアでのダイナミック ルーティング

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration
interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis

interface GigabitEthernet0/0.301
 nameif outside
```

```
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis

router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family

IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis priority 120
 isis ipv6 metric 600


interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
 metric-style wide
 maximum-paths 6
!
 address-family ipv6
 summary-prefix 2001::/8 tag 301
 summary-prefix 6001::/16 level-1-2 tag 800
 redistribute static metric 800 level-1-2
exit-address-family


oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip pim sparse-dense-mode
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis
 isis tag 301
```

```
oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide

ASA Configuration
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 maximum-paths 5
!
 address-family ipv6 unicast
  redistribute static level-1-2
  maximum-paths 6
 exit-address-family
!
```

ルートの再配布

```
iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
  ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
  isis
  ipv6 router isis


 interface GigabitEthernet0/1.201
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
  ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
  isis
  ipv6 router isis


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  maximum-paths 5
 !
 address-family ipv6 unicast
  maximum-paths 6
 exit-address-family
!

IOS Configuration
iRouter
 interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
```

```
 isis priority 120


iRouter
interface GigabitEthernet0/1
 ip address 172.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis


oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis


oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

サマリー アドレス

```
iRouter ---------- ASA ------------ oRouter

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0
 ipv6 address 2001:172:16:32::1/64
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0
 ipv6 address 2001:192:16:32::1/64
 isis
 ipv6 router isis
```

```
router isis
 net 49.1234.2005.2005.2005.00
 authentication mode md5
 authentication key cisco#123 level-2
 metric-style wide
 summary-address 172.16.0.0 255.255.252.0
 redistribute static
 maximum-paths 5
address-family ipv6 unicast
 maximum-paths 6
exit-address-family
```

Passive Interfaces

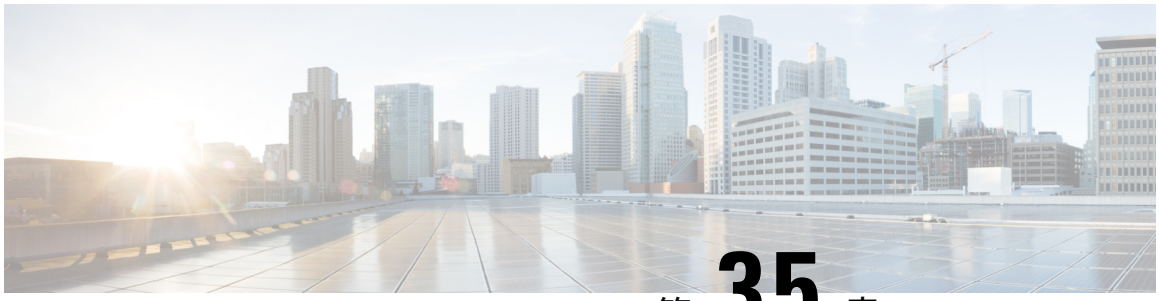
```
 iRouter ---------- ASA ------------ oRouter


 ASA Configuration
 interface GigabitEthernet0/0
  nameif outside
  security-level 80
  ip address 192.16.32.1 255.255.255.0
  ipv6 address 2001:192:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/1
  nameif inside
  security-level 100
  ip address 172.16.32.1 255.255.255.0
  ipv6 address 2001:172:16:32::1/64
  isis
  ipv6 router isis


 interface GigabitEthernet0/2
  nameif dmz
  security-level 0
  ip address 40.40.50.1 255.255.255.0
  ipv6 address 2040:95::1/64


 router isis
  net 49.1234.2005.2005.2005.00
  metric-style wide
  redistribute isis level-2 into level-1 route-map RMAP
  passive-interface default

IOS Configuration
 iRouter
  interface GigabitEthernet0/0
  ip address 172.16.32.3 255.255.255.0
  ip router isis
  ipv6 address 2001:172:16:32::3/64
  ipv6 router isis
  isis priority 120

 iRouter
 interface GigabitEthernet0/1
  ip address 172.26.32.3 255.255.255.0
```

```
 ip router isis
 ipv6 address 2001:172:26:32::3/64
 ipv6 router isis

iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 metric-style wide

oRouter
interface GigabitEthernet0/0
 ip address 192.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:16:32::3/64
 ipv6 router isis

oRouter
interface GigabitEthernet0/1
 ip address 192.26.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:192:26:32::3/64
 ipv6 router isis

oRouter
router isis
 net 49.1234.2036.2036.2036.00
 is-type level-1
 metric-style wide
```

認証

```
ASA ------------ Router

ASA Configuration

interface GigabitEthernet0/1
 nameif inside
 security-level 100
 ip address 172.16.32.1 255.255.255.0 standby 172.16.32.2
 ipv6 address 2001:172:16:32::1/64 standby 2001:172:16:32::2
 isis
 ipv6 router isis
 isis authentication key cisco#123 level-2
 isis authentication mode md5


interface GigabitEthernet0/0.301
 nameif outside
 security-level 80
 ip address 192.16.32.1 255.255.255.0 standby 192.16.32.2
 ipv6 address 2001:192:16:32::1/64 standby 2001:192:16:32::2
 isis
 ipv6 router isis


router isis
 net 49.1234.2005.2005.2005.00
 metric-style wide
 authentication mode md5
 authentication key cisco#123 level-2
```

```
IOS Configuration
iRouter
interface GigabitEthernet0/0
 ip address 172.16.32.3 255.255.255.0
 ip router isis
 ipv6 address 2001:172:16:32::3/64
 ipv6 enable
 ipv6 router isis
 isis authentication mode md5
 isis authentication key-chain KeyChain level-2
 isis priority 120
 isis ipv6 metric 600


iRouter
key chain KeyChain
 key 1
  key-string cisco#123


iRouter
router isis
 net 49.1234.2035.2035.2035.00
 net 49.2001.2035.2035.2035.00
 is-type level-2-only
 authentication mode md5
 authentication key-chain KeyChain level-2
```



第 35 章

EIGRP

この章では、Enhanced Interior Gateway Routing Protocol（EIGRP）を使用してデータをルーティングし、認証を実行し、ルーティング情報を再配布するように ASA を設定する方法について説明します。

- EIGRP について （1367 ページ）
- EIGRP のガイドライン （1369 ページ）
- EIGRP の設定 （1370 ページ）
- EIGRP のカスタマイズ （1373 ページ）
- EIGRPv6 プロセスの設定 （1390 ページ）
- EIGRP のモニタリング （1396 ページ）
- EIGRP の例 （1397 ページ）
- EIGRP の履歴 （1399 ページ）

EIGRP について

EIGRP は、シスコが開発した、IGRP の拡張バージョンです。IGRP や RIP と異なり、EIGRP が定期的にルート アップデートを送信することはありません。EIGRP アップデートは、ネットワーク トポロジが変更された場合にだけ送信されます。EIGRP を他のルーティング プロトコルと区別する主な機能には、迅速なコンバージェンス、可変長サブネット マスクのサポート、部分的アップデートのサポート、複数のネットワーク レイヤ プロトコルのサポートなどがあります。

EIGRP を実行するルータでは、すべてのネイバー ルーティング テーブルが格納されているため、代替ルートに迅速に適応できます。適切なルートが存在しない場合、EIGRP はそのネイバーにクエリーを送信して代替のルートを検出します。これらのクエリーは、代替ルートが検出されるまで伝搬します。EIGRP では可変長サブネット マスクがサポートされているため、ルートはネットワーク番号の境界で自動的に集約されます。さらに、任意のインターフェイスの任意のビット境界で集約を行うように EIGRP を設定することもできます。EIGRP は定期的なアップデートを行いません。その代わり、ルートのメトリックが変更されたときだけ、部分的なアップデートを送信します。部分的アップデートの伝搬では、境界が自動的に設定されるため、その情報を必要とするルータだけがアップデートされます。これらの 2 つの機能により、EIGRP の帯域幅消費量は IGRP に比べて大幅に減少します。

ネイバー探索は、ASA が直接接続されているネットワーク上にある他のルータをダイナミックに把握するために使用するプロセスです。EIGRP ルータは、マルチキャスト hello パケットを送信して、ネットワーク上に自分が存在していることを通知します。ASA は、新しいネイバーから hello パケットを受信すると、トポロジ テーブルに初期化ビットを設定してそのネイバーに送信します。ネイバーは、初期化ビットが設定されたトポロジアップデートを受信すると、自分のトポロジ テーブルを ASA に返送します。

hello パケットはマルチキャスト メッセージとして送信されます。hello メッセージへの応答は想定されていません。ただし、スタティックに定義されたネイバーの場合は例外です。**neighbor** コマンドを使用して（または ASDM で [Hello Interval] を設定して）ネイバーを設定すると、そのネイバーへ送信される hello メッセージはユニキャスト メッセージとして送信されます。ルーティング アップデートと確認応答が、ユニキャスト メッセージとして送信されます。

このネイバー関係が確立した後は、ネットワーク トポロジが変更された場合にだけ、ルーティング アップデートが交換されます。ネイバー関係は、hello パケットによって維持されます。ネイバーから受信した各 hello パケットには、保持時間が含まれています。ASA は、この時間内にそのネイバーから hello パケットを受信すると想定できます。ASA が保持時間内にそのネイバーからアドバタイズされた hello パケットを受信しない場合、ASA はそのネイバーを使用不能と見なします。

EIGRP プロトコルは、ネイバーの検出、ネイバーの回復、Reliable Transport Protocol（RTP）、およびルート計算に重要な DUAL を含む、4 の主要なアルゴリズム テクノロジーと 4 つの主要なテクノロジーを使用します。DUAL は、最小コストのルートだけでなく、宛先へのすべてのルートをトポロジ テーブルに保存します。最小コストのルートはルーティング テーブルに挿入されます。その他のルートは、トポロジテーブルに残ります。メインのルートに障害が発生したら、フィジブルサクセサから別のルートが選択されます。サクセサとは、宛先への最小コスト パスを持ち、パケット転送に使用される隣接ルータです。フィジビリティ計算によって、パスがルーティング ループを形成しないことが保証されます。

フィジブル サクセサがトポロジ テーブル内にない場合、必ずルート計算が発生します。ルートの再計算中、DUAL は EIGRP ネイバーにルートを求めるクエリーを送信して、次に EIGRP ネイバーがそのネイバーにクエリーを送信します。ルートのフィジブル サクセサがないルータは、到達不能メッセージを返します。

ルートの再計算中、DUAL は、ルートをアクティブとマークします。デフォルトでは、ASA は、ネイバーから応答が返ってくるのを 3 分間待ちます。ASA がネイバーから応答を受信しないと、そのルートは stuck-in-active とマークされます。トポロジ テーブル内のルートのうち、応答しないネイバーをフィジブル サクセサとして指しているものはすべて削除されます。

（注） EIGRP ネイバー関係では、GRE トンネルを使用しない IPsec トンネルの通過はサポートされていません。

EIGRPv6

EIGRP for IPv6 は、EIGRP IPv4 と同様に設定できます。EIGRPv6 は、IPv6 ピアとのみ通信し、IPv6 ルートのみをアドバタイズします。EIGRPv6 は、多くの点で EIGRPv4 に似ています。

- DUAL は、同じメトリックでルートの計算と選択に使用されます。
- 大規模なネットワークの実装に合わせて拡張できます。
- ネイバー、ルーティング、およびトポロジテーブルは維持されます。
- 等コストロードバランシングと不等コストロードバランシングの両方が提供されます。

ただし、EIGRPv6 は、次のような多くの点で EIGRPv4 とは異なります。

- network コマンドは IPv6 では使用されません。EIGRP はリンクを使用して設定されます。
- 設定時に各インターフェイスで EIGRPv6 を明示的に有効にする必要があります。

Null0 および EIGRP

デフォルトでは、EIGRP は Null0 ルートをサマリールートとしてピアにアドバタイズして、サマリーをアドバタイズしているルータがルートを持たないパケットを転送しないようにします。

たとえば、R1 と R2 の 2 つのルータについて考えてみます。R1 の 3 つのインターフェイスには、192.168.0.0/24、192.168.1.0/24、および 192.168.3.0/24 のネットワークがあります。R1 をサマリールート 192.168.0.0/22 で設定し、そのルートを R2 にアドバタイズします。R2 に 192.168.2.x の IP パケットがある場合、そのパケットは R1 に転送されます。R1 は、ルーティングテーブルに 192.168.2.x がないため、パケットをドロップします。ただし、R1 が ISP にも接続されており、ISP を指しているデフォルトルートがある場合、192.168.2.x パケットは ISP に転送されます。この転送アクションを防ぐために、EIGRP は、Null0 を指している、サマリールートに一致するエントリを生成します。したがって、192.168.2.x のパケットが受信されると、R1 はデフォルトルートを使用する代わりにパケットをドロップします。

EIGRP のガイドライン

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

クラスタのガイドライン

個別インターフェイス モードのクラスタの場合、EIGRP はルータ ID としてクラスタ プールを使用してクラスタのピアとの関係を形成できます。

IPv6 のガイドライン

IPv6 ルーティングをサポートします。

コンテキストのガイドライン

- デフォルトでは、共有インターフェイス間でのマルチキャストトラフィックのコンテキスト間交換がサポートされていないため、EIGRPインスタンスは共有インターフェイス間で相互に隣接関係を形成できません。ただし、EIGRP プロセスの EIGRP プロセス設定で静的ネイバー設定を使用すると、共有インターフェイスでの EIGRP ネイバーシップを形成できます。
- 個別のインターフェイスでのコンテキスト間 EIGRP がサポートされています。

再配布のガイドライン

EIGRP が、OSPF ネットワークの一部であるデバイスで設定されている場合、またはその逆の場合は、ルートにタグを付けるようにOSPFルータが設定されていることを確認します（EIGRP はルートタグをサポートしていません）。

EIGRP を OSPF に再配布し、OSPF を EIGRP に再配布する場合は、いずれかのリンクまたはインターフェイスで障害が発生したときや、ルート発信元がダウンしたときにも、ルーティングループが発生します。あるドメインから同じドメインに再度ルートを再配布することを避けるため、ルータは、再配布する際にドメインに属しているルートにタグ付けすることができます。そして、そのタグに基づいて、リモートルータでそれらのルートをフィルタ処理できます。それらのルートはルーティングテーブルにインストールされないため、再度同じドメインに再配布されることはありません。

その他のガイドライン

- 最大 1 つの EIGRP プロセスがサポートされます。
- 設定の変更が適用されるたびに、EIGRP隣接関係のフラップが発生し、特に配布リスト、オフセットリスト、および集約への変更のネイバーからの（送信または受信された）ルーティング情報が変更されます。ルータが同期されると、EIGRPはネイバー間の隣接関係を再確立します。隣接関係が壊れて再確立されると、ネイバー間で学習されたすべてのルートが消去され、新しい配布リストを使用して、ネイバー間の同期がすべて新しく実行されます。
- また、EIGRP ネイバーの最大数にも制限はありません。ただし、不要な EIGRP フラップを防ぐために、ユニットあたりの数を 500 に制限することを推奨します。

EIGRP の設定

この項では、システムでEIGRPプロセスをイネーブルにする方法について説明します。EIGRPをイネーブルにした後に、システムで EIGRP プロセスをカスタマイズする方法については、次の項を参照してください。

EIGRP のイネーブル化

ASA でイネーブルにすることができる EIGRP ルーティング プロセスは 1 つだけです。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

EIGRP IPv6 ルーティングプロセスをイネーブルにするには、次のコマンドを入力します。

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の **network** 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP のインターフェイスの設定（1374 ページ）を参照してください。

EIGRP スタブ ルーティングのイネーブル化

ASA を EIGRP スタブ ルータとしてイネーブル化し、設定することができます。スタブ ルーティングを使用すると、ASA で必要となるメモリおよび処理要件を減らすことができます。ASA をスタブ ルータとして設定すると、ローカル以外のトラフィックがすべて配布ルータに転送されるようになり、完全な EIGRP ルーティング テーブルを維持する必要がなくなります。一般に、配布ルータからスタブ ルートに送信する必要があるのは、デフォルト ルートだけです。

スタブ ルータから配布ルータには、指定されたルートだけが伝搬されます。スタブ ルータであるASAは、サマリー、接続されているルート、再配布されたスタティック ルート、外部ルート、および内部ルートに対するクエリーすべてに、応答として「inaccessible」というメッセージを返します。ASA がスタブとして設定されているときは、自身のスタブ ルータとしてのステータスを報告するために、特殊なピア情報パケットをすべての隣接ルータに送信します。スタブ ステータスの情報を伝えるパケットを受信したネイバーはすべて、スタブ ルータにルートのクエリーを送信しなくなり、スタブ ピアを持つルータはそのピアのクエリーを送信しなくなります。スタブルータが正しいアップデートをすべてのピアに送信するには、配布ルータが必要です。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の **network** 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、パッシブ インターフェイスの設定（1376ページ）の項を参照してください。

ステップ 3 スタブ ルーティング プロセスを設定します。

eigrp stub{**receive-only** |[**connected**] [**redistributed**] [**static**] [**summary**]}

例：

```
ciscoasa(config)# router eigrp 2
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# eigrp stub {receive-only | [connected] [redistributed] [static]
 [summary]}
```

スタブ ルーティング プロセスから配布ルータにアドバタイズされるネットワークを指定する必要があります。スタティック ルートおよび接続されているネットワークが、自動的にスタブ ルーティング プロセスに再配布されることはありません。

（注）
スタブ ルーティング プロセスでは、完全なトポロジ テーブルは維持されません。スタブ ルーティングには、ルーティングの決定を行うために、少なくとも配布ルータへのデフォルト ルートが必要です。

EIGRP のカスタマイズ

ここでは、EIGRP ルーティングをカスタマイズする方法について説明します。

EIGRP ルーティング プロセスのネットワークの定義

[Network] テーブルでは、EIGRP ルーティング プロセスで使用されるネットワークを指定できます。EIGRP ルーティングに参加するインターフェイスは、これらのネットワーク エントリで定義されるアドレスの範囲内に存在する必要があります。アドバタイズされる直接接続およびスタティックのネットワークも、これらのネットワーク エントリの範囲内である必要があります。

[Network] テーブルには、EIGRP ルーティング プロセス用に設定されているネットワークが表示されます。このテーブルの各行には、指定した EIGRP ルーティング プロセス用に設定されているネットワーク アドレスおよび関連するマスクが表示されます。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の **network** 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、パッシブインターフェイスの設定（1376ページ）を参照してください。

EIGRP のインターフェイスの設定

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、インターフェイスが接続されているネットワークが対象に含まれるように **network** コマンドを設定し、**passive-interface** コマンドを使用して、そのインターフェイスが EIGRP アップデートを送受信しないようにします。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

EIGRP IPv6 ルーティングプロセスをイネーブルにするには、次のコマンドを入力します。

ipv6 router eigrp as-num

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の network 文を設定できます。 ただし、**network** コマンドは EIGRP IPv6 では使用されません。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP ルーティング プロセスのネットワークの定義 （1373 ページ）を参照してください。

ステップ 3 候補となるデフォルト ルート情報の送受信を制御します。

no default-information {**in** | **out** | **WORD**}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

no default-information in コマンドを入力すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。

no default-information out コマンドを入力すると、アドバタイズされるルートのデフォルト ルート ビット設定がディセーブルになります。

詳細については、EIGRP でのデフォルト情報の設定 （1387 ページ）を参照してください。

ステップ 4 EIGRP パケットの MD5 認証をイネーブルにします。

authentication mode eigrp as-num **md5**

例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 引数は、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号です。EIGRP がイネーブルになっていないか、または誤った番号を入力した場合には、ASA が次のエラー メッセージを返します。

```
% Asystem(100) specified does not exist
```

詳細については、インターフェイスでの EIGRP 認証のイネーブル化 （1379 ページ）を参照してください。

ステップ 5 遅延値を設定します。

delay *value*

例：

```
ciscoasa(config-if)# delay 200
```

value 引数は 10 マイクロ秒単位で入力します。2000 マイクロ秒の遅延を設定するには、*value* に 200 を入力します。

インターフェイスに割り当てられている遅延値を表示するには、**show interface** コマンドを使用します。

詳細については、インターフェイス遅延値の変更 （1378 ページ）を参照してください。

ステップ 6 hello 間隔を変更します。

hello-interval eigrp as-num seconds

例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

詳細については、EIGRP Hello 間隔と保持時間のカスタマイズ （1385 ページ）を参照してください。

ステップ 7 保持時間を変更します。

hold-time eigrp as-num seconds

例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

詳細については、EIGRP Hello 間隔と保持時間のカスタマイズ （1385 ページ）を参照してください。

パッシブ インターフェイスの設定

1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRP の場合、受動インターフェイスではルーティング アップデートが送受信されません。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。このコマンドで、1 つ以上の **network** 文を設定できます。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP ルーティング プロセスのネットワークの定義（1373 ページ）を参照してください。

ステップ 3 インターフェイスが EIGRP ルーティング メッセージを送受信しないようにします。

passive-interface {**default** | if-name}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# passive-interface {default}
```

default キーワードを使用すると、すべてのインターフェイスで EIGRP ルーティング アップデートが無効になります。**nameif** コマンドで定義したインターフェイス名を指定すると、指定したインターフェイスで EIGRP ルーティング アップデートが無効になります。EIGRP ルータ コンフィギュレーション内で、複数の **passive-interface** コマンドを使用できます。

インターフェイスでのサマリー集約アドレスの設定

サマリーアドレスはインターフェイスごとに設定できます。ネットワーク番号の境界以外でサマリー アドレスを作成する場合、または自動ルート集約がディセーブルになった ASA でサマリー アドレスを使用する場合は、手動でサマリー アドレスを定義する必要があります。ルーティング テーブルに他にも個別のルートがある場合、EIGRP は、他の個別ルートすべての中で最小のメトリックと等しいメトリックで、サマリーアドレスをインターフェイスからアドバタイズします。

手順

ステップ 1 EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface inside
```

ステップ 2 サマリー アドレスを作成します。

summary-address eigrp *as-num address mask* [*distance*]

例：

```
ciscoasa(config-if)# summary-address eigrp 2 address mask [20]
```

EIGRP IPv6 のサマリーアドレスを作成します。

ipv6 summary-address eigrp *as-num address mask* [*distance*]

例：

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 summary-address eigrp 1 4001::1/64 ?
interface mode commands/options:
  <1-255>  Administrative distance
```

デフォルトでは、定義する EIGRP サマリー アドレスのアドミニストレーティブ ディスタンスは 5 になります。この値は、**summary-address** コマンドにオプションの引数 *distance* を指定して変更できます。

インターフェイス遅延値の変更

インターフェイス遅延値は、EIGRP ディスタンス計算で使用されます。この値は、インターフェイスごとに変更できます。

手順

ステップ 1 EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface inside
```

ステップ 2 遅延値を設定します。

delay *value*

例：

```
ciscoasa(config-if)# delay 200
```

value 引数は 10 マイクロ秒単位で入力します。2000 マイクロ秒の遅延を設定するには、*value* に 200 を入力します。

（注）
インターフェイスに割り当てられている遅延値を表示するには、**show interface** コマンドを使用します。

インターフェイスでの EIGRP 認証のイネーブル化

EIGRP ルート認証では、EIGRP ルーティング プロトコルからのルーティング アップデートに対する MD5 認証を提供します。MD5 キーを使用したダイジェストが各 EIGRP パケットに含まれており、承認されていない送信元からの不正なルーティング メッセージや虚偽のルーティング メッセージが取り込まれないように阻止します。

EIGRP ルート認証は、インターフェイスごとに設定します。EIGRP メッセージ認証対象として設定されたインターフェイス上にあるすべての EIGRP ネイバーには、隣接関係を確立できるように同じ認証モードとキーを設定する必要があります。

（注） EIGRP ルート認証をイネーブルにするには、事前に EIGRP をイネーブルにする必要があります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp *as-num*

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数は、EIGRP ルーティング プロセスの自律システム番号です。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network *ip-addr* [*mask*]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

- このコマンドで、1 つ以上の network 文を設定できます。
- 直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。
- アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP の設定 （1370 ページ）を参照してください。

ステップ 3 EIGRP メッセージ認証を設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface *phy_if*

例：

```
ciscoasa(config)# interface inside
```

ステップ 4 EIGRP パケットの MD5 認証をイネーブルにします。

authentication mode eigrp *as-num* md5

例：

```
ciscoasa(config)# authentication mode eigrp 2 md5
```

as-num 引数は、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号です。EIGRP がイネーブルになっていないか、または誤った番号を入力した場合には、ASA が次のエラー メッセージを返します。

```
% Asystem(100) specified does not exist
```

ステップ 5 MD5 アルゴリズムで使用するキーを設定します。

authentication key eigrp *as-num key* key-id *key-id*

例：

```
ciscoasa(config)# authentication key eigrp 2 cisco key-id 200
```

- as-num 引数は、ASA に設定されている EIGRP ルーティング プロセスの自律システム番号です。EIGRP がイネーブルになっていないか、または誤った番号を入力した場合には、ASA が次のエラー メッセージを返します。

```
% Asystem(100) specified does not exist%
```

- key 引数には、アルファベット、数字、特殊文字を含む最大 16 文字を含めることができます。key 引数では空白を使用できません。
- key-id 引数には、0 ～ 255 の範囲の数字を指定できます。

EIGRP ネイバーの定義

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

ステップ 3 スタティック ネイバーを定義します。

neighbor *ip-addr* **interface** *if_name*

例：

```
ciscoasa(config)# router eigrp 2
```

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

例：

EIGRP IPv6 の場合

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# neighbor 2001:DB8:0:ABCD::1 interface interface1
```

ip-addr 引数には、ネイバーの IP アドレスを指定します。

if-name 引数は、ネイバーを使用可能にしている **nameif** コマンドで指定したインターフェイスの名前です。1 つの EIGRP ルーティング プロセスに対して複数のネイバーを定義できます。

（注）
ネイバーシップ設定を有効にするには、EIGRP ルーティングに参加するインターフェイス ネットワークを設定する必要があります。

EIGRP へのルート再配布

RIP および OSPF で検出されたルートを、EIGRP ルーティング プロセスに再配布することができます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。接続されているルートが、EIGRP コンフィギュレーション内の **network** 文で指定された範囲に含まれている場合、再配布する必要はありません。

（注） RIP 限定：この手順を開始する前に、ルート マップを作成し、指定されたルーティング プロトコルのうち RIP ルーティング プロセスに再配布されるルートを詳細に定義する必要があります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 （オプション）EIGRP ルーティング プロセスに再配布するルートに適用するデフォルト メトリックを指定します。

default-metric bandwidth delay reliability loading mtu

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth delay reliability loading mtu
```

EIGRP ルータ コンフィギュレーション内にデフォルト メトリックを指定しない場合、各 **redistribute** コマンドにメトリック値を指定する必要があります。**redistribute** コマンドで EIGRP メトリックを指定し、EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれている場合、**redistribute** コマンドのメトリックが使用されます。

ステップ 3 接続済みルートを EIGRP ルーティング プロセスに再配布します。

redistribute connected [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router)# redistribute connected [metric bandwidth delay reliability
loading mtu] [route-map map_name]
```

EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれていない場合、**redistribute** コマンドに EIGRP メトリック値を指定する必要があります。

ステップ 4 スタティック ルートを EIGRP ルーティング プロセスに再配布します。

redistribute static [**route-map** map_name]

例：

```
ciscoasa(config-router)# redistribute static [route-map map_name]
```

このコマンドは、すべてのスタティック ルートを EIGRP に渡します。選択的スタティック ルートを再配布するには、スタティック ルートを含むアクセス リストを作成してから、ルート マップに含めてください。

例：

```
ciscoasa(config)# ip access-list extended R1_Loopback
ciscoasa(config-ext-nacl)#permit ip host 1.1.1.1 any
ciscoasa(config-ext-nacl)#exit

ciscoasa(config)#route-map Permit_to_Distribute
ciscoasa(config-route-map)#match ip address R1_Loopback
ciscoasa(config-route-map)#exit
```

ルート マップを作成した後、次のように redistribute コマンドに含めます。

例：

```
ciscoasa(config)#router eigrp 2
ciscoasa(config-router)#redistribute static subnets route-map Permit_to_Distribute
```

ステップ 5 ルートを OSPF ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。

redistribute ospf pid [**match** {**internal | external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router): redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}] [metric bandwidth delay reliability loading mtu] [route-map
map_name]
```

ステップ 6 ルートを RIP ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。

redistribute rip [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

例：

```
ciscoasa(config-router): redistribute rip [metric bandwidth delay
reliability load mtu] [route-map map_name]
```

EIGRP でのネットワークのフィルタリング

（注） この手順を開始する前に、標準の ACL を作成し、その中にアドバタイズするルートを定義する必要があります。つまり、標準の ACL を作成し、その中に送信または受信したアップデートからフィルタリングするルートを定義します。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

ciscoasa(config-router)# **network** ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の network 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP のインターフェイスの設定（1374 ページ）を参照してください。

ステップ 3 EIGRP ルーティング アップデートで送信するネットワークをフィルタリングします。

distribute-list acl **out** [**connected** | **ospf** | **rip** | **static** | **interface** if_name]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl out [connected]
```

インターフェイスを指定して、そのインターフェイスが送信するアップデートだけにフィルタを適用することができます。

EIGRP ルータ コンフィギュレーション内に、複数の **distribute-list** コマンドを入力できます。

ステップ 4 EIGRP ルーティング アップデートで受信するネットワークをフィルタリングします。

distribute-list acl **in** [**interface** if_name]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router): distribute-list acl in [interface interface1]
```

インターフェイスを指定して、そのインターフェイスが受信するアップデートだけにフィルタを適用することができます。

EIGRP Hello 間隔と保持時間のカスタマイズ

ASA は、ネイバーを検出する目的、およびネイバーが到達不能または動作不能になったことを把握する目的で、定期的に hello パケットを送信します。デフォルトでは、hello パケットは 5 秒間隔で送信されます。

hello パケットは、ASA の保持時間をアドバタイズします。保持時間によって、EIGRP ネイバーに、ASA を到達可能と見なす時間の長さを知らせます。アドバタイズされた保持時間内にネイ

バーが hello パケットを受信しなかった場合、ASA は到達不能と見なされます。デフォルトでは、アドバタイズされる保持時間は 15 秒です（hello 間隔の 3 倍）。

hello 間隔とアドバタイズされる保持時間のいずれも、インターフェイスごとに設定します。保持時間は hello 間隔の 3 倍以上に設定することをお勧めします。

手順

ステップ 1 hello 間隔またはアドバタイズされる保持時間を設定するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface inside
```

ステップ 2 hello 間隔を変更します。

hello-interval eigrp as-num seconds

例：

```
ciscoasa(config)# hello-interval eigrp 2 60
```

EIGRP IPv6 の hello 間隔を変更します。

ipv6 hello-interval eigrp as-num seconds

例：

```
ciscoasa(config)# ipv6 hello-interval eigrp 2 60
```

ステップ 3 保持時間を変更します。

hold-time eigrp as-num seconds

例：

```
ciscoasa(config)# hold-time eigrp 2 60
```

EIGRP IPv6 の保持時間を変更します。

ipv6 hold-time eigrp as-num seconds

例：

```
ciscoasa(config)# ipv6 hold-time eigrp 2 60
```

自動ルート集約の無効化

自動ルート集約は、デフォルトでイネーブルになっています。EIGRP ルーティング プロセスは、ネットワーク番号の境界で集約を行います。このことは、不連続ネットワークがある場合にルーティングの問題の原因となることがあります。

たとえば、ネットワーク 192.168.1.0、192.168.2.0、192.168.3.0 が接続されているルータがあり、それらのネットワークがすべて EIGRP に参加しているとすると、EIGRP ルーティング プロセスはそれらのルートに対しサマリー アドレス 192.168.0.0 を作成します。さらにネットワーク 192.168.10.0 と 192.168.11.0 が接続されているルータがこのネットワークに追加され、それらのネットワークが EIGRP に参加すると、これらもまた 192.168.0.0 として集約されます。トラフィックが誤った場所にルーティングされる可能性をなくすために、競合するサマリーアドレスを作成するルータでの自動ルート集約をディセーブルにする必要があります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 自動ルート集約をディセーブルにします。

no auto-summary

例：

```
ciscoasa(config-router)# no auto-summary
```

自動サマリー アドレスのアドミニストレーティブ ディスタンスは 5 です。

EIGRP でのデフォルト情報の設定

EIGRP アップデート内のデフォルト ルート情報の送受信を制御できます。デフォルトでは、デフォルト ルートが送信され、受け入れられます。デフォルト情報の受信を禁止するように ASA を設定すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。デフォルト情報の送信を禁止するように ASA を設定すると、アドバタイズされるルートのデフォルト ルート ビット設定が無効になります。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

router eigrp as-num

例：

```
ciscoasa(config)# router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 EIGRP ルーティングに参加するインターフェイスとネットワークを設定します。

network ip-addr [mask]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

このコマンドで、1 つ以上の network 文を設定できます。

直接接続されるネットワークとスタティック ネットワークが定義済みネットワークに含まれていれば、それらが ASA によってアドバタイズされます。さらに、定義されたネットワークに含まれる IP アドレスを持つインターフェイスだけが、EIGRP ルーティング プロセスに参加します。

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、EIGRP のインターフェイスの設定（1374 ページ）を参照してください。

ステップ 3 候補となるデフォルト ルート情報の送受信を制御します。

no default-information {**in** | **out** | **WORD**}

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

（注）
no default-information in コマンドを入力すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。**no default-information out** コマンドを入力すると、アドバタイズされるルートのデフォルト ルート ビット設定がディセーブルになります。

EIGRP スプリット ホライズンのディセーブル化

スプリット ホライズンは、EIGRP アップデート パケットとクエリー パケットの送信を制御します。スプリット ホライズンがインターフェイスでイネーブルになると、アップデート パケットとクエリー パケットは、このインターフェイスがネクスト ホップとなる宛先には送信されません。この方法でアップデート パケットとクエリー パケットを制御すると、ルーティング ループが発生する可能性が低くなります。

デフォルトでは、スプリット ホライズンはすべてのインターフェイスでイネーブルになっています。

スプリット ホライズンは、ルート情報が、その情報の発信元となるインターフェイスからルータによってアドバタイズされないようにします。通常、特にリンクが切断された場合には、この動作によって複数のルーティング デバイス間の通信が最適化されます。ただし、非ブロードキャスト ネットワークでは、この動作が望ましくない場合があります。このような場合は、EIGRP を設定したネットワークを含め、スプリット ホライズンをディセーブルにする必要が生じることもあります。

インターフェイスでのスプリット ホライズンをディセーブルにする場合、そのインターフェイス上のすべてのルータとアクセス サーバーに対してディセーブルにする必要があります。

EIGRP スプリット ホライズンをディセーブルにするには、次の手順を実行します。

手順

ステップ 1 EIGRP で使用される遅延値を変更するインターフェイスのインターフェイス コンフィギュレーション モードに入ります。

interface phy_if

例：

```
ciscoasa(config)# interface phy_if
```

ステップ 2 スプリット ホライズンをディセーブルにします。

no split-horizon eigrp *as-number*

例：

```
ciscoasa(config-if)# no split-horizon eigrp 2
```

EIGRP IPv6 のスプリットホライズンをディセーブルにします。

no ipv6 split-horizon eigrp *as-number*

例：

```
ciscoasa(config-if)# no ipv6 split-horizon eigrp 2
```

EIGRP プロセスの再始動

EIGRPプロセスを再始動したり、再配布またはカウンタをクリアしたりすることができます。

手順

EIGRP プロセスを再始動するか、再配布またはカウンタをクリアします。

clear eigrp pid {**1-65535** | **neighbors** | **topology** | **events)**}

例：

```
ciscoasa(config)# clear eigrp pid 10 neighbors
```

EIGRPv6 プロセスの設定

ここでは、システムで EIGRP IPv6 プロセスをイネーブルにして設定する方法について説明します。

EIGRPv6 の有効化

ASA で有効にできる EIGRPv6 ルーティングプロセスは 1 つだけです。

手順

IPv6 の EIGRP ルーティングプロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

ipv6 router eigrp *as-num*

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

EIGRPv6 のフィルタルール

（注） この手順を開始する前に、標準の ACL を作成し、その中にアドバタイズするルートを定義する必要があります。つまり、標準の ACL を作成し、その中に送信または受信したアップデートからフィルタリングするルートを定義します。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

ipv6 router eigrp as-num

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 インターフェイスからアドバタイズされる EIGRP for IPv6 ルーティングアップデートに、プレフィックスリストを適用します。

distribute-list prefix-list name **out interface** if_name

例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# distribute-list acl out interface interface2
```

EIGRP ルータ コンフィギュレーション内に、複数の **distribute-list** コマンドを入力できます。

ステップ 3 インターフェイス上で受信される EIGRP for IPv6 ルーティングアップデートに、プレフィックスリストを適用します。

distribute-list prefix-list name **in** [**interface** if_name]

例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# distribute-list acl in interface interface1
```

EIGRPv6 のインターフェイスの設定

アドバタイズするネットワークに接続されているインターフェイスを EIGRP ルーティングに参加させない場合は、インターフェイスが接続されているネットワークが対象に含まれるように ASA を設定し、**passive-interface** コマンドを使用してそのインターフェイスが EIGRP アップデートを送受信しないようにします。

手順

ステップ 1 EIGRP ルーティングプロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

ipv6 router eigrp as-num

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 候補となるデフォルト ルート情報の送受信を制御します。

no default-information {**in** | **out** | **WORD**}

例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# no default-information {in | out | WORD}
```

no default-information in コマンドを入力すると、候補のデフォルト ルート ビットが受信ルート上でブロックされます。

no default-information out コマンドを入力すると、アドバタイズされるルートのデフォルト ルート ビット設定がディセーブルになります。

詳細については、EIGRP でのデフォルト情報の設定 （1387 ページ）を参照してください。

ステップ 3 hello 間隔を変更します。

ipv6 hello-interval eigrp as-num seconds

例：

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hello-interval eigrp 2 60
```

詳細については、EIGRP Hello 間隔と保持時間のカスタマイズ （1385 ページ）を参照してください。

ステップ 4 保持時間を変更します。

ipv6 hold-time eigrp as-num seconds

例：

```
ciscoasa(config-if)# int gigabitEthernet 0/0
ciscoasa(config-if)# ipv6 hold-time eigrp 2 60
```

詳細については、EIGRP Hello 間隔と保持時間のカスタマイズ（1385 ページ）を参照してください。

EIGRPv6 のパッシブインターフェイスの設定

1 つ以上のインターフェイスを受動インターフェイスとして設定できます。EIGRPv6 の場合、受動インターフェイスではルーティングアップデートが送受信されません。

手順

ステップ 1 EIGRPv6 ルーティングプロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

ipv6 router eigrp as-num

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 インターフェイスが EIGRP ルーティング メッセージを送受信しないようにします。

passive-interface {**default** | if-name}

例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# passive-interface {default}
```

default キーワードを使用すると、すべてのインターフェイスで EIGRPv6 ルーティングアップデートが無効になります。**nameif** コマンドで定義したインターフェイス名を指定すると、指定したインターフェイスで EIGRP ルーティング アップデートが無効になります。EIGRPv6 ルータ コンフィギュレーションでは、複数の **passive-interface** コマンドを使用できます。

EIGRPv6 へのルートの再配布

OSPF、BGP、ISIS で検出されたルートを EIGRP IPv6 ルーティングプロセスに再配布できます。スタティック ルートおよび接続されているルートも、EIGRP ルーティング プロセスに再配布できます。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

ipv6 router eigrp as-num

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 （オプション）EIGRP ルーティング プロセスに再配布するルートに適用するデフォルト メトリックを指定します。

default-metric[bandwidth | delay | reliability | loading | mtu]

例：

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# default-metric bandwidth 10 delay 20
```

EIGRP ルータ コンフィギュレーション内にデフォルト メトリックを指定しない場合、各 **redistribute** コマンドにメトリック値を指定する必要があります。**redistribute** コマンドでEIGRP メトリックを指定し、EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれている場合、**redistribute** コマンドのメトリックが使用されます。

（注）
default-metric を指定すると、ASA の show run-config コマンドでは default-metric 設定は表示されません。

ステップ 3 接続済みルートを EIGRP ルーティング プロセスに再配布します。

redistribute connected [**metric** bandwidth | delay | reliability | loading | mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router)# redistribute connected [metric bandwidth 100] [route-map map_name]
```

EIGRP ルータ コンフィギュレーション内に **default-metric** コマンドが含まれていない場合、**redistribute** コマンドに EIGRP メトリック値を指定する必要があります。

ステップ 4 スタティック ルートを EIGRP ルーティング プロセスに再配布します。

redistribute static [**metric** bandwidth | delay | reliability | loading | mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router): redistribute static [route-map map_name]
```

ステップ 5 ルートを OSPF ルーティング プロセスから EIGRP ルーティング プロセスに再配布します。

redistribute ospf pid [**match** {**internal | external** [**1** | **2**] | **nssa-external** [**1** | **2**]}] [**metric** bandwidth delay reliability loading mtu] [**route-map** map_name]

例：

```
ciscoasa(config-router)# redistribute ospf pid [match {internal | external [1 | 2] |
nssa-external [1 | 2]}][route-map map_name]
```

ステップ 6 BGP ルーティングプロセスからのルートを EIGRP ルーティングプロセスに再配布します。

redistribute bgp [**metric** bandwidth delay reliability load mtu] [**route-map map_name**]

例：

```
ciscoasa(config-router)# redistribute bgp [route-map map_name]
```

ステップ 7 ISIS ルーティングプロセスからのルートを EIGRP ルーティングプロセスに再配布します。

redistribute isis [**level-1 | level-2 | level-1-2**][**include-connected | metric number | metric-type | tag | route-map map_name**]

例：

```
ciscoasa(config-router)# redistribute isis [level-1] [metric delay 20 [route-map map_name]]
```

EIGRPv6 ネイバーの定義

EIGRP hello パケットはマルチキャスト パケットとして送信されます。EIGRP ネイバーが、トンネルなど、非ブロードキャスト ネットワークを越えた場所にある場合、手動でネイバーを定義する必要があります。手動で EIGRP ネイバーを定義すると、hello パケットはユニキャスト メッセージとしてそのネイバーに送信されます。

手順

ステップ 1 EIGRP ルーティング プロセスを作成して、この EIGRP プロセスのルータ コンフィギュレーション モードを開始します。

ipv6 router eigrp as-num

例：

```
ciscoasa(config)# ipv6 router eigrp 2
```

as-num 引数には、EIGRP ルーティング プロセスの自律システム番号を指定します。

ステップ 2 スタティック ネイバーを定義します。

neighbor *ip-addr* **interface** *if_name*

例：

```
ciscoasa(config)# ipv6 router eigrp 2
ciscoasa(config-router)# neighbor 2001:DB8:0:ABCD::1 interface interface1
```

ip-addr 引数には、ネイバーの IP アドレスを指定します。

if-name 引数は、ネイバーを使用可能にしている **nameif** コマンドで指定したインターフェイスの名前です。1 つの EIGRP ルーティング プロセスに対して複数のネイバーを定義できます。

EIGRP のモニタリング

次のコマンドを使用して、EIGRP ルーティング プロセスをモニタできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。また、ネイバー変更メッセージとネイバー警告メッセージのロギングをディセーブルにできます。

さまざまな EIGRP ルーティング統計情報をモニターまたはディセーブル化するには、次のいずれかのコマンドを入力します。

- **router-id**

  EIGRP プロセスの router-id を表示します。

- **show eigrp** [*as-number*] **events** [{*start end*} | **type**]

  EIGRP イベント ログを表示します。

- **show eigrp** [*as-number*] **interfaces** [*if-name*] [**detail**]

  EIGRP ルーティングに参加するインターフェイスを表示します。

- **show eigrp** [as-number] **neighbors** [**detail** | **static**] [*if-name*]

  EIGRP ネイバー テーブルを表示します。

- **show eigrp** [*as-number*] **topology** [*ip-addr* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  EIGRP トポロジ テーブルを表示します。

- **show eigrp** [*as-number*] **traffic**

EIGRP トラフィックの統計情報を表示します。

- **show mfib cluster**

  転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

- **show route cluster**

  クラスタリングに関する追加ルートの同期の詳細を表示します。

- **no eigrp log-neighbor-changes**

  ネイバー変更メッセージのロギングをディセーブルにします。EIGRP ルーティング プロセスのルータ コンフィギュレーション モードでこのコマンドを入力します。

- **no eigrp log-neighbor-warnings**

  ネイバー警告メッセージのロギングをディセーブルにします。

- **show ipv6 eigrp** *as-number* **interface** *interface*

  EIGRP IPv6トポロジテーブルを表示します。

- **show ipv6 eigrp** [*as-number*] **traffic**

  EIGRP IPv6 トラフィックの統計情報を表示します。

- **show ipv6 eigrp** ［as-number］**neighbors**［*if-name*］

  EIGRP IPv6 ネイバーテーブルを表示します。

- **show ipv6 eigrp interfaces**［*if-name*］

  特定のインターフェイスに関するネイバー関連情報を表示します。

- **show ipv6 eigrp** [*as-number*] **topology** [*ipv6-address* [**mask**] | **active** | **all-links** | **pending** | **summary** | **zero-successors**]

  EIGRP IPv6トポロジテーブルを表示します。

- **show ipv6 eigrp** [*as-number*] **events** [{*start - end*} | **type**]

  EIGRP IPv6 イベントログを表示します。

- **show ipv6 eigrp timers**

  設定されている hello タイマーとホールドタイマーを表示します。

EIGRP の例

次の例に、さまざまなオプションのプロセスを使用して EIGRP をイネーブルにし、設定する方法を示します。

手順

ステップ 1 EIGRP をイネーブルにするには、次のコマンドを入力します。

```
ciscoasa(config)# router eigrp 2
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

ステップ 2 EIGRP ルーティング メッセージの送信または受信からインターフェイスを設定するには、次のコマンドを入力します。

```
ciscoasa(config-router)# passive-interface {default}
```

ステップ 3 EIGRP ネイバーを定義するには、次のコマンドを入力します。

```
ciscoasa(config-router)# neighbor 10.0.0.0 interface interface1
```

ステップ 4 EIGRPルーティングに参加するインターフェイスとネットワークを設定するには、次のコマンドを入力します。

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
```

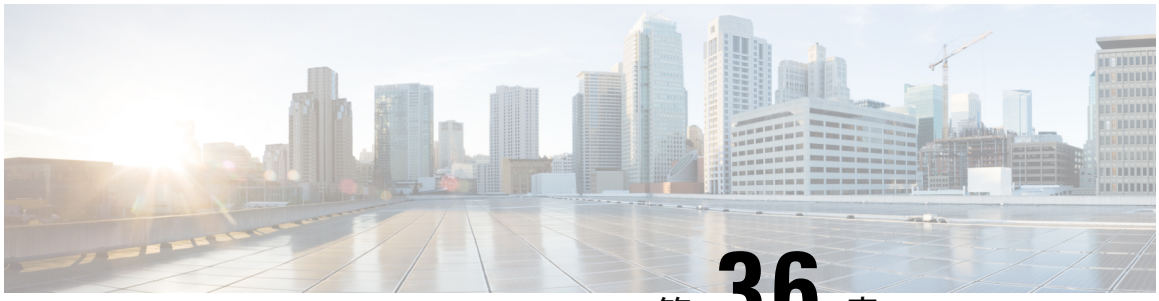
ステップ 5 EIGRPディスタンス計算で使用されるインターフェイス遅延値を変更するには、次のコマンドを入力します。

```
ciscoasa(config-router)# exit
ciscoasa(config)# interface phy_if
ciscoasa(config-if)# delay 200
```

EIGRP の履歴

表 *44 : EIGRP* の機能の履歴

機能名	プラットフォーム リリース	機能情報
EIGRP サポート	7.0(1)	Enhanced Interior Gateway Routing Protocol（EIGRP）を使用するデータのルーティング、認証の実行、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 **route eigrp** コマンドが導入されました。
マルチ コンテキスト モードのダイナミック ルーティング	9.0(1)	EIGRP ルーティングは、マルチ コンテキスト モードでサポートされます。
クラスタ	9.0(1)	EIGRP の場合、バルク同期、ルートの同期およびレイヤ 2 ロード バランシングは、クラスタリング環境でサポートされます。 **show route cluster**、**debug route cluster**、**show mfib cluster**、**debug mfib cluster** の各コマンドが導入または変更されました。
EIGRP Auto-Summary	9.2(1)	EIGRP の [Auto-Summary] フィールドはデフォルトでディセーブルになりました。
EIGRPv6 のサポート	9.20(1)	Enhanced Interior Gateway Routing Protocol（EIGRP）を使用するデータのルーティング、認証の実行、およびルーティング情報の再配布とモニタリングについて IPv6 のサポートが追加されました。 次のコマンドが導入されました。**ipv6 eigrp**、**ipv6 hello-interval eigrp**、**ipv6 hold-time eigrp**、**ipv6 split-horizon eigrp**、**show ipv6 eigrp interface** 、**show ipv6 eigrp traffic**、**show ipv6 eigrp neighbors** 、**show ipv6 eigrp interface**、**ipv6 summary-address eigrp**、**show ipv6 eigrp topology**、**show ipv6 eigrp events** 、**show ipv6 eigrp timers**、**clear ipv6 eigrp**、および **clear ipv6 router eigrp**。



第 36 章

マルチキャスト ルーティング

この章では、マルチキャスト ルーティング プロトコルを使用するように ASA を設定する方法について説明します。

- マルチキャスト ルーティングについて （1401 ページ）
- マルチキャスト ルーティングのガイドライン （1405 ページ）
- マルチキャスト ルーティングの有効化 （1406 ページ）
- マルチキャスト ルーティングのカスタマイズ （1406 ページ）
- PIM のモニタリング （1421 ページ）
- マルチキャスト ルーティングの例 （1421 ページ）
- マルチキャスト ルーティングの履歴 （1422 ページ）

マルチキャスト ルーティングについて

マルチキャストルーティングは、単一の情報ストリームを数千もの企業や家庭に同時に配信することでトラフィックを軽減する帯域幅節約型のテクノロジーです。マルチキャストルーティングを活用するアプリケーションには、ビデオ会議、企業通信、遠隔学習に加えて、ソフトウェア、株価、およびニュースの配信などがあります。

マルチキャスト ルーティング プロトコルでは、競合テクノロジーのネットワーク帯域幅の使用量を最小限に抑えながら、送信元や受信者の負荷を増加させずに発信元のトラフィックを複数の受信者に配信します。マルチキャスト パケットは、Protocol Independent Multicast（PIM）やサポートする他のマルチキャスト プロトコルを使用した ASA によりネットワークで複製されるため、複数の受信者にできる限り高い効率でデータを配信できます。

ASA は、スタブ マルチキャスト ルーティングと PIM マルチキャスト ルーティングの両方をサポートしています。ただし、1 つの ASA に両方を同時に設定することはできません。

（注） マルチキャスト ルーティングでは、UDP トランスポートおよび非 UDP トランスポートの両方がサポートされます。ただし、非 UDP トランスポートでは FastPath 最適化は行われません。

スタブ マルチキャスト ルーティング

スタブ マルチキャスト ルーティングは、ダイナミック ホスト登録の機能を提供して、マルチキャスト ルーティングを容易にします。スタブ マルチキャスト ルーティングを設定すると、ASA は IGMP のプロキシ エージェントとして動作します。ASA は、マルチキャスト ルーティングに全面的に参加するのではなく、IGMP メッセージをアップストリームのマルチキャスト ルータに転送し、そのルータがマルチキャスト データの送信をセットアップします。スタブ マルチキャスト ルーティングを設定する場合は、ASA を PIM スパース モードまたは双方向モード用に設定できません。IGMP スタブ マルチキャスト ルーティングに参加するインターフェイス上で PIM を有効にする必要があります。

ASA は、PIM-SM および双方向 PIM の両方をサポートしています。PIM-SM は、基盤となるユニキャスト ルーティング情報ベースまたは別のマルチキャスト対応ルーティング情報ベースを使用するマルチキャスト ルーティング プロトコルです。このプロトコルは、マルチキャスト グループあたり 1 つのランデブー ポイント（RP）をルートにした単方向の共有ツリーを構築し、オプションでマルチキャストの発信元ごとに最短パス ツリーを作成します。

PIM マルチキャスト ルーティング

双方向 PIM は PIM-SM の変形で、マルチキャストの発信元と受信者を接続する双方向の共有ツリーを構築します。双方向ツリーは、マルチキャスト トポロジの各リンクで動作する指定フォワーダ（DF）選択プロセスを使用して構築されます。DF に支援されたマルチキャスト データは発信元からランデブー ポイント（RP）に転送されます。この結果、マルチキャスト データは発信元固有の状態を必要とせず、共有ツリーをたどって受信者に送信されます。DF の選択は RP の検出中に行われ、これによってデフォルト ルートが RP に提供されます。

（注） ASAが PIM RP の場合は、ASAの変換されていない外部アドレスを RP アドレスとして使用してください。

PIM Source Specific Multicast のサポート

ASAは PIM Source Specific Multicast（SSM）の機能や関連設定をサポートしていません。ただし、ASAは最終ホップ ルータとして配置されていない限り、SSM 関連のパケットの通過を許可します。

SSMは、IPTVなどの1対多のアプリケーションのデータ送信メカニズムとして分類されます。SSM モデルは、（S、G）ペアで示される「チャネル」の概念を使用します。S は発信元アドレス、GはSSM宛先アドレスです。チャネルに登録するには、IGMPv3などのグループ管理プロトコルを使用して行います。SSMは、特定のマルチキャスト送信元について学習した後、受信側のクライアントを有効にします。これにより、共有ランデブー ポイント（RP）からではなく、直接送信元からマルチキャスト ストリームを受信できるようになります。アクセス制御メカニズムは SSM 内に導入され、現在のスパースまたはスパース - デンス モードの実装では提供されないセキュリティ拡張機能を提供します。

PIM-SSM は、RP または共有ツリーを使用しない点で PIM-SM とは異なります。代わりに、マルチキャスト グループの発信元アドレスの情報は、ローカル受信プロトコル（IGMPv3）経由で受信者から提供され、送信元固有のツリーを直接作成するために使用されます。

PIM ブートストラップ ルータ（BSR）

PIM ブートストラップ ルータ（BSR）は、RP 機能およびグループの RP 情報をリレーするために候補のルータを使用する動的ランデブーポイント（RP）セレクションモデルです。RP機能には RP の検出が含まれており、RP にデフォルト ルートを提供します。これは、一連のデバイスをBSR の選択プロセスに参加する候補の BSR（C-BSR）として設定し、その中から BSR を選択することで実現します。BSR が選択されると、候補のランデブー ポイント（C-RP）として設定されたデバイスは、選定された BSR にグループ マッピングの送信を開始します。次に、BSR はホップ単位で PIM ルータ間を移動する BSR メッセージ経由で、マルチキャスト ツリーに至る他のすべてのデバイスにグループ/RP マッピング情報を配布します。

この機能は、RP を動的に学習する方法を提供するため、RP が停止と起動を繰り返す複雑で大規模なネットワークには不可欠です。

PIM ブートストラップ ルータ（BSR）の用語

PIM BSR の設定では、次の用語がよく使用されます。

- ブートストラップ ルータ（BSR）：BSR はホップバイホップ ベースの PIM が設定された他のルータに、ランデブー ポイント（RP）情報をアドバタイズします。選択プロセスの後に、複数の候補 BSR の中から 1 つの BSR が選択されます。このブートストラップ ルータの主な目的は、すべての候補 RP（C-RP）通知を RP-set というデータベースに収集し、これをネットワーク内の他のすべてのルータに定期的に BSR メッセージとして送信することです（60 秒ごと）。
- ブートストラップ ルータ（BSR）メッセージ：BSR メッセージは、TTL が 1 に設定された All-PIM-Routers グループへのマルチキャストです。これらのメッセージを受信するすべての PIM ネイバーは、メッセージを受信したインターフェイスを除くすべてのインターフェイスからそのメッセージを再送信します（TTL は 1 に設定）。BSR メッセージには、現在アクティブな BSR の RP-set と IP アドレスが含まれています。この方法で、C-RP は C-RP メッセージのユニキャスト先を認識します。
- 候補ブートストラップ ルータ（C-BSR）：候補 BSR として設定されるデバイスは、BSR 選択メカニズムに参加します。最も優先順位の高い C-BSR が BSR として選択されます。C-BSR の最上位の IP アドレスはタイブレイカーとして使用されます。BSR の選択プロセスはプリエンプティブです。たとえば、より優先順位の高い C-BSR が新たに見つかると、新しい選択プロセスがトリガーされます。
- 候補ランデブーポイント（C-RP）：RP はマルチキャストデータの送信元と受信者が対面する場所として機能します。C-RP として設定されているデバイスは、マルチキャスト グループ マッピング情報を、ユニキャスト経由で直接、選択された BSR に定期的にアドバタイズします。これらのメッセージには、グループ範囲、C-RP アドレス、および保留時間が含まれています。現在の BSR の IP アドレスは、ネットワーク内のすべてのルータが

受信した定期的な BSR メッセージから学習されます。このようにして、BSR は現在動作中で到達可能な RP 候補について学習します。

（注） C-RP は BSR トラフィックの必須要件ですが、ASA は C-RP としては機能しません。ルータのみが C-RP として機能できます。したがって、BSR のテスト機能では、トポロジにルータを追加する必要があります。

- BSR 選択メカニズム：各 C-BSR は、BSR 優先順位フィールドを含むブートストラップ メッセージ（BSM）を生成します。ドメイン内のルータは、ドメイン全体に BSM をフラッディングします。自身より優先順位の高い C-BSR に関する情報を受け取った BSR は、一定期間、BSM の送信を抑止します。残った単一の C-BSR が選択された BSR となり、その BSM により、選択された BSR に関する通知がドメイン内の他のすべてのルータに対して送信されます。

マルチキャスト グループの概念

マルチキャストはグループの概念に基づくものです。受信者の任意のグループは、特定のデータ ストリームを受信することに関心があります。このグループには物理的または地理的な境界がなく、インターネット上のどの場所にホストを置くこともできます。特定のグループに流れるデータの受信に関心があるホストは、IGMP を使用してグループに加入する必要があります。ホストがデータ ストリームを受信するには、グループのメンバでなければなりません。

マルチキャスト アドレス

マルチキャストアドレスは、グループに加入し、このグループに送信されるトラフィックの受信を希望する IP ホストの任意のグループを指定します。

クラスタ

マルチキャスト ルーティングは、クラスタリングをサポートします。スパンド EtherChannel クラスタリングでは、ファーストパス転送が確立されるまでの間、制御ユニットがすべてのマルチキャスト ルーティング パケットとデータパケットを送信します。ファーストパス転送が確立されると、データユニットがマルチキャストデータ パケットを転送できます。すべてのデータ フローは、フルフローです。スタブ転送フローもサポートされます。スパンド EtherChannel クラスタリングでは 1 つのユニットだけがマルチキャストパケットを受信するため、制御ユニットへのリダイレクションは共通です。 個別インターフェイス クラスタリングでは、ユニットは個別に機能しません。すべてのデータとルーティングパケットは制御ユニットで処理され、転送されます。データユニットは、送信されたすべてのパケットをドロップします。

マルチキャスト ルーティングのガイドライン

コンテキスト モード

シングル コンテキスト モードでサポートされています。

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

IPv6

IPv6 はサポートされません。

マルチキャスト グループ

224.0.0.0 ー 224.0.0.255 のアドレス範囲は、ルーティングプロトコル、およびゲートウェイディスカバリやグループ メンバーシップ レポートなどのその他のトポロジディスカバリまたはメンテナンスプロトコルを使用するために予約されています。したがって、アドレス範囲224.0.0/24からのインターネット マルチキャスト ルーティングはサポートされません。予約されたアドレスのマルチキャストルーティングを有効にすると、IGMP グループは作成されません。

クラスタリング

IGMP および PIM のクラスタリングでは、この機能はプライマリ ユニットでのみサポートされます。

その他のガイドライン

- 224.1.2.3 などのマルチキャスト ホストへのトラフィックを許可するには、インバウンド インターフェイス上のアクセス制御ルールを設定する必要があります。ただし、ルールの宛先インターフェイスを指定したり、初期接続確認の間にマルチキャストの接続に適用したりすることはできません。
- PIM/IGMP マルチキャストルーティングは、トラフィックゾーン内のインターフェイスではサポートされません。
- ASA を同時にランデブーポイント（RP）とファーストホップルータになるように設定しないでください。
- HSRP スタンバイ IP アドレスは、PIM ネイバーシップに参加しません。したがって、RP ルータ IP が HSRP スタンバイ IP アドレスを介してルーティングされる場合、マルチキャストルーティングはASAで機能しません。マルチキャストトラフィックが正常に通過するようにするには、RP アドレスのルートが HSRP スタンバイ IP アドレスではないことを確認し、代わりに、ルートアドレスをインターフェイス IP アドレスに設定します。

マルチキャスト ルーティングの有効化

ASA でマルチキャストルーティングを有効にすると、デフォルトではすべてのデータインターフェイスで IGMP と PIM が有効になりますが、ほとんどのモデルの管理インターフェイスでは有効になりません（通過トラフィックを許可しないインターフェイスについては、管理スロット/ポートインターフェイス（826 ページ）を参照してください）。IGMP は、直接接続されているサブネット上にグループのメンバーが存在するかどうか学習するために使用されます。ホストは、IGMP レポートメッセージを送信することにより、マルチキャスト グループに参加します。PIM は、マルチキャスト データグラムを転送するための転送テーブルを維持するために使用されます。

管理インターフェイスでマルチキャストルーティングを有効にするには、管理インターフェイスでマルチキャスト境界を明示的に設定する必要があります。

（注） マルチキャストルーティングでは、UDP トランスポート レイヤだけがサポートされています。

以下の一覧に、特定のマルチキャストテーブルに追加されるエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

- MFIB：30,000
- IGMP グループ：30,000
- PIM ルート：72,000

手順

マルチキャスト ルーティングをイネーブルにします。

multicast-routing

例：

```
ciscoasa(config)# multicast-routing
```

マルチキャスト ルーティング テーブルのエントリの数は、ASA に搭載されている RAM の量によって制限されます。

マルチキャスト ルーティングのカスタマイズ

ここでは、マルチキャスト ルーティングをカスタマイズする方法について説明します。

スタブ マルチキャスト ルーティングの設定と IGMP メッセージの転送

（注） スタブ マルチキャスト ルーティングは、PIM スパース モードおよび双方向モードと同時にはサポートされません。

スタブ エリアへのゲートウェイとして動作している ASA は、PIM スパース モードまたは双方向モードに参加する必要はありません。その代わりに、そのセキュリティ アプライアンスを IGMP プロキシ エージェントとして設定すると、あるインターフェイスに接続されているホストから、別のインターフェイスのアップストリーム マルチキャスト ルータに IGMP メッセージを転送することができます。ASA を IGMP プロキシ エージェントとして設定するには、ホスト加入（join）メッセージおよびホスト脱退（leave）メッセージをスタブ エリアからアップストリーム インターフェイスに転送します。スタブ モードのマルチキャスト ルーティングに参加しているインターフェイスでも、PIM を有効にする必要があります。

手順

スタブ マルチキャスト ルーティングを設定し、IGMP メッセージを転送します。

igmp forward interface if_name

例：

```
ciscoasa(config-if)# igmp forward interface interface1
```

スタティック マルチキャスト ルートの設定

スタティック マルチキャスト ルートを設定すると、マルチキャスト トラフィックをユニキャスト トラフィックから分離できます。たとえば、送信元と宛先の間のパスでマルチキャスト ルーティングがサポートされていない場合は、その解決策として、2 つのマルチキャスト デバイスの間に GRE トンネルを設定し、マルチキャスト パケットをそのトンネル経由で送信します。

PIM を使用する場合、ASA は、ユニキャスト パケットを発信元に返送するときと同じインターフェイスでパケットを受信することを想定しています。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合などは、ユニキャスト パケットで 1 つのパスを使用し、マルチキャスト パケットで別の 1 つのパスを使用することもあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

手順

ステップ 1 スタティック マルチキャスト ルートを設定します。

mroute src_ip src_mask {input_if_name | *rpf_neighbor*} [distance]

例：

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
```

ステップ 2 スタブ エリアのスタティック マルチキャスト ルートを設定します。

mroute src_ip src_mask input_if_name [**dense** output_if_name] [distance]

例：

```
ciscoasa(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

dense*output_if_name* キーワードと引数のペアは、スタブ マルチキャスト ルーティングでのみサポートされています。

IGMP 機能の設定

IP ホストは、自身のグループ メンバーシップを直接接続されているマルチキャスト ルータに報告するために IGMP を使用します。IGMP は、マルチキャスト グループの個々のホストを特定の LAN にダイナミックに登録するために使用します。ホストは、そのローカル マルチキャスト ルータに IGMP メッセージを送信することで、グループ メンバーシップを識別します。IGMP では、ルータは IGMP メッセージをリッスンし、定期的にクエリを送信して、特定のサブネットでアクティブなグループと非アクティブなグループを検出します。

ここでは、インターフェイス単位で任意の IGMP 設定を行う方法について説明します。

インターフェイスでの IGMP の有効化

IGMP は、特定のインターフェイスでディセーブルにできます。この情報は、特定のインターフェイスにマルチキャスト ホストがないことがわかっていて、ASA からそのインターフェイスにホスト クエリー メッセージを発信しないようにする場合に有用です。

手順

インターフェイスで IGMP をディセーブルにします。

no igmp

例：

```
ciscoasa(config-if)# no igmp
```

インターフェイスで IGMP を再度イネーブルにするには、**igmp** コマンドを使用します。

（注）
インターフェイス コンフィギュレーションには、**no igmp** コマンドだけが表示されます。

IGMP グループ メンバーシップの設定

ASA をマルチキャスト グループのメンバとして設定できます。マルチキャスト グループに加入するように ASA を設定すると、アップストリーム ルータはそのグループのマルチキャスト ルーティング テーブル情報を維持して、このグループをアクティブにするパスを保持します。

（注） 特定のグループのマルチキャストパケットを特定のインターフェイスに転送する必要がある場合に、ASA がそのパケットをそのグループの一部として受け付けることがないようにする方法については、スタティック加入した IGMP グループの設定（1409 ページ）を参照してください。

手順

ASA をマルチキャスト グループのメンバとして設定します。

igmp join-group group-address

例：

```
ciscoasa(config-if)# igmp join-group mcast-group
```

group-address 引数はグループの IP アドレスです。

（注）
igmp join-group コマンドを使用すると、PIM は送信元またはランデブーポイント（RP）向けに参加要求を送信できます。ただし、このコマンドのファイアウォールは、コマンドが適用されるインターフェイス上の PIM 代表ルータ（DR）であることが条件です。

スタティック加入した IGMP グループの設定

設定によってはグループ メンバがグループ内で自分のメンバーシップを報告できない場合があります。また、ネットワーク セグメント上にグループのメンバが存在しないこともあります。しかし、それでも、そのグループのマルチキャスト トラフィックをそのネットワーク セグメ

ントに送信することが必要になる場合があります。そのようなグループのマルチキャスト トラフィックをそのセグメントに送信するには、スタティック加入したIGMP グループを設定します。

igmp static-group コマンドを入力します。ASA は、マルチキャスト パケットを受け入れる代わりに、指定されたインターフェイスに転送します。

手順

インターフェイスのマルチキャスト グループにスタティック加入するように、ASA を設定します。

igmp static-group

例：

```
ciscoasa(config-if)# igmp static-group group-address
```

group-address 引数はグループの IP アドレスです。

（注）
igmp static-group コマンドを使用すると、PIM は送信元またはランデブーポイント（RP）向けに参加要求を送信できます。ただし、このコマンドのファイアウォールは、コマンドが適用されるインターフェイス上の PIM 代表ルータ（DR）であることが条件です。

マルチキャスト グループへのアクセスの制御

アクセス コントロール リストを使用して、マルチキャスト グループへのアクセスを制御できます。

手順

ステップ 1 マルチキャスト トラフィックの標準 ACL を作成します。

access-list name **standard** [**permit | deny]** ip_addr mask

例：

```
ciscoasa(config)# access-list acl1 standard permit 192.52.662.25
```

1 つの ACL に複数のエントリを作成することができます。標準 ACL または拡張 ACL を使用できます。

ip_addr mask 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

ステップ 2 拡張 ACL を作成します。

access-list name **extended** [**permit | deny]** protocol src_ip_addr src_mask dst_ip_addr dst_mask

例：

```
ciscoasa(config)# access-list acl2 extended permit protocol
src_ip_addr src_mask dst_ip_addr dst_mask
```

dst_ip_addr 引数は、許可または拒否されるマルチキャスト グループの IP アドレスです。

ステップ 3 ACL をインターフェイスに適用します。

igmp access-group acl

例：

```
ciscoasa(config-if)# igmp access-group acl
```

acl 引数は、標準 IP ACL または拡張 IP ACL の名前です。

インターフェイスにおける IGMP 状態の数の制限

IGMP メンバーシップ報告の結果の IGMP 状態の数は、インターフェイスごとに制限することができます。設定された上限を超過したメンバーシップ報告は IGMP キャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

手順

インターフェイスにおける IGMP 状態の数を制限します。

igmp limit number

例：

```
ciscoasa(config-if)# igmp limit 50
```

有効値の範囲は 0 ～ 5000 で、デフォルト値は です。

この値を 0 に設定すると、学習したグループが追加されなくなりますが、（**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用して）手動で定義したメンバーシップは引き続き許可されます。このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。

（注） アクティブな結合があるインターフェイスでIGMP制限を変更した場合、新しい制限は既存のグループには適用されません。ASAでは、新しいグループがインターフェイスに追加されたときとIGMP joinタイマーが期限切れになったときにのみ制限を検証します。新しい制限をすぐに適用するには、インターフェイスでIGMPを無効にしてから再度有効にする必要があります。

マルチキャスト グループに対するクエリー メッセージの変更

ASAは、クエリー メッセージを送信して、インターフェイスに接続されているネットワークにメンバを持つマルチキャストグループを検出します。メンバーは、IGMP報告メッセージで応答して、特定のグループに対するマルチキャストパケットの受信を希望していることを示します。クエリ メッセージは、アドレスが224.0.0.1で存続可能時間値が1の全システム マルチキャスト グループ宛に送信されます。

これらのメッセージが定期的に送信されることにより、ASAに保存されているメンバーシップ情報はリフレッシュされます。ASAで、ローカルメンバがいなくなったマルチキャストグループがまだインターフェイスに接続されていることがわかると、そのグループへのマルチキャストパケットを接続されているネットワークに転送するのを停止し、そのパケットの送信元にプルーニング メッセージを戻します。

デフォルトでは、サブネット上のPIM代表ルータがクエリ メッセージの送信を担当します。このメッセージは、デフォルトでは125秒間に1回送信されます。

クエリ応答時間を変更する場合は、IGMPクエリでアドバタイズする最大クエリ応答所要時間はデフォルトで10秒になります。ASAがこの時間内にホストクエリーの応答を受信しなかった場合、グループを削除します。

（注） **igmp query-timeout** および **igmp query-interval** コマンドを実行するには、IGMP バージョン2が必要です。

クエリー間隔、クエリー応答時間、クエリータイムアウト値を変更するには、次の手順を実行します。

手順

ステップ1 クエリー間隔を秒単位で設定します。

igmp query-interval *seconds*

例：

```
ciscoasa(config-if)# igmp query-interval 30
```

有効値の範囲は 1～3600 で、デフォルト値は 125 です。

指定されたタイムアウト値（デフォルトは255秒）の間にインターフェイス上でクエリー メッセージが ASA によって検出されないと、ASA が指定ルータになり、クエリー メッセージの送信を開始します。

ステップ 2 クエリーのタイムアウト値を変更します。

igmp query-timeout *seconds*

例：

```
ciscoasa(config-if)# igmp query-timeout 30
```

有効値の範囲は 60～300 で、デフォルト値は 225 です。

ステップ 3 最大クエリー応答時間を変更します。

igmp query-max-response-time *seconds*

有効値の範囲は 1～25 で、デフォルト値は 10 です。

例：

```
ciscoasa(config-if)# igmp query-max-response-time 20
```

IGMP バージョンの変更

デフォルトでは、ASA は IGMP バージョン 2 を実行します。このバージョンでは **igmp query-timeout** コマンドや **igmp query-interval** コマンド などの、いくつかの追加機能を使用できます。

サブネットのマルチキャスト ルータはすべて、同じ IGMP バージョンをサポートしている必要があります。ASA は、バージョン 1 ルータを自動的に検出してバージョン 1 に切り替えることはありません。しかし、サブネットに IGMP のバージョン 1 のホストとバージョン 2 のホストが混在しても問題はありません。IGMP バージョン 2 を実行している ASA は、IGMP バージョン 1 のホストが存在しても正常に動作します。

手順

インターフェイスで実行する IGMP のバージョンを制御します。

igmp version {**1** | **2**}

例：

```
ciscoasa(config-if)# igmp version 2
```

PIM 機能の設定

ルータは PIM を使用して、マルチキャスト ダイアグラムを転送するために使われる転送テーブルを維持します。ASAでマルチキャスト ルーティングを有効にすると、PIM および IGMP がすべてのインターフェイスで自動的に有効になります。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

ここでは、任意の PIM 設定を行う方法について説明します。

インターフェイスでの PIM の有効化またはディセーブル化

PIM は、特定のインターフェイスでイネーブルまたはディセーブルにできます。

手順

ステップ 1 特定のインターフェイスで PIM をイネーブルにする、または再度イネーブルにします。

pim

例：

```
ciscoasa(config-if)# pim
```

ステップ 2 特定のインターフェイスで PIM をディセーブルにします。

no pim

例：

```
ciscoasa(config-if)# no pim
```

（注）
インターフェイス コンフィギュレーションには、**no pim** コマンドだけが表示されます。

スタティック ランデブー ポイント アドレスの設定

共通の PIM スパース モードまたは双方向ドメイン内のルータはすべて、PIM RP アドレスを認識している必要があります。このアドレスは、**pim rp-address** コマンドを使用してスタティックに設定されます。

（注） ASA は、Auto-RP をサポートしていません。RP アドレスを指定するには、**pim rp-address** コマンドを使用する必要があります。

複数のグループの RP として機能するように ASA を設定することができます。ACL に指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。ACL が指定されていない場合は、マルチキャスト グループ全体の範囲（224.0.0.0/4）にグループの RP が適用されます。

手順

特定のインターフェイスで PIM をイネーブルにする、または再度イネーブルにします。

pim rp-address ip_address [acl] [**bidir**]

ip_address 引数は、PIM RP となるように割り当てられたルータのユニキャスト IP アドレスです。

acl 引数は、RP とともに使用する必要があるマルチキャスト グループを定義している標準 ACL の名前または番号です。このコマンドではホスト ACL を使用しないでください。

bidir キーワードを除外すると、グループは PIM スパース モードで動作するようになります。

（注）
ASA は、実際の双方向構成にかかわらず、PIM の hello メッセージを使用して双方向の機能を常時アドバタイズします。

例：

```
ciscoasa(config)# pim rp-address 10.86.75.23 [acl1] [bidir]
```

指定ルータのプライオリティの設定

DR は、PIM 登録メッセージ、PIM 加入メッセージ、およびプルーニング メッセージの RP への送信を担当します。1 つのネットワーク セグメントに複数のマルチキャスト ルータがある場合は、DR プライオリティに基づいて DR が選択されます。複数のデバイスの DR プライオリティが等しい場合、最上位の IP アドレスを持つデバイスが DR になります。

デフォルトでは、ASA の DR プライオリティは 1 です。この値を変更できます。

手順

指定ルータのプライオリティを変更します。

pim dr-priority num

例：

```
ciscoasa(config-if)# pim dr-priority 500
```

num 引数は、1 ～ 4294967294 の任意の数字にできます。

PIM 登録メッセージの設定とフィルタリング

ASA が RP として動作しているときは、特定のマルチキャスト送信元を登録できないように制限することができます。このようにすると、未許可の送信元が RP に登録されるのを回避できます。[Request Filter] ペインでは、ASA で PIM 登録メッセージが受け入れられるマルチキャスト ソースを定義できます。

手順

PIM 登録メッセージをフィルタリングするように ASA を設定します。

pim accept-register {**list** acl | **route-map** map-name}

例：

```
ciscoasa(config)# pim accept-register {list acl1 | route-map map2}
```

この例では、ASA によって PIM 登録メッセージ *acl1* とルート マップ *map2* がフィルタリングされます。

PIM メッセージ間隔の設定

ルータ クエリー メッセージは、PIM DR の選択に使用されます。PIM DR は、ルータ クエリ メッセージを送信します。デフォルトでは、ルータ クエリ メッセージは 30 秒間隔で送信されます。さらに、60 秒ごとに、ASA は PIM 加入メッセージおよびプルーニング メッセージを送信します。

手順

ステップ 1 ルータ クエリー メッセージを送信します。

pim hello-interval seconds

例：

```
ciscoasa(config-if)# pim hello-interval 60
```

seconds 引数の有効な値は 1 ～ 3600 秒です。

ステップ 2 ASA が PIM 加入メッセージまたはプルーニング メッセージを送信する時間（秒）を変更します。

pim join-prune-interval seconds

例：

```
ciscoasa(config-if)# pim join-prune-interval 60
```

seconds 引数の有効な値は 10 ～ 600 秒です。

PIM ネイバーのフィルタリング

PIMネイバーにできるルータの定義が可能です。PIMネイバーにできるルータをフィルタリングすると、次の制御を行うことができます。

- 許可されていないルータが PIM ネイバーにならないようにする。
- 添付されたスタブ ルータが PIM に参加できないようにする。

手順

ステップ 1 標準 ACL を使用して、PIM に参加させるルータを定義します。

access-list pim_nbr deny *router-IP_addr PIM neighbor*

例：

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

この例では、次の ACL を **pim neighbor-filter** コマンドで使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

ステップ 2 隣接ルータをフィルタリングします。

pim neighbor-filter pim_nbr

例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim neighbor-filter pim_nbr
```

この例では、インターフェイス GigabitEthernet0/3 で 10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

双方向ネイバー フィルタの設定

ASA に PIM 双方向ネイバー フィルタが設定されている場合、[Bidirectional Neighbor Filter] ペインにそれらのフィルタが表示されます。PIM 双方向ネイバー フィルタは、DF 選定に参加できるネイバー デバイスを定義する ACL です。PIM 双方向ネイバー フィルタがインターフェイスに設定されていなければ、制限はありません。PIM 双方向ネイバー フィルタが設定されている場合は、ACL で許可されるネイバーだけが DF 選択プロセスに参加できます。

PIM 双方向ネイバー フィルタ設定が ASA に適用されると、実行コンフィギュレーションに *interface-name*_multicast という名前の ACL が表示されます。ここで、*interface-name* はマルチキャスト境界フィルタが適用されるインターフェイスの名前です。そのような名前の ACL がすでに存在していた場合は、名前に番号が追加されます（inside_multicast_1 など）。この ACL により、どのデバイスが ASA の PIM ネイバーになれるか定義されます。

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

PIM 双方向ネイバー フィルタを利用すると、スパース モード専用ネットワークから双方向ネットワークへの移行が可能になります。このフィルタで、DF 選定に参加するルータを指定する一方で、引き続きすべてのルータにスパース モード ドメインへの参加を許可できるからです。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

PIM 双方向ネイバー フィルタが有効な場合、その ACL によって許可されるルータは、双方向に対応しているとみなされます。したがって、次のことが当てはまります。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

手順

ステップ 1 標準 ACL を使用して、PIM に参加させるルータを定義します。

access-list pim_nbr deny *router-IP_addr PIM neighbor*

例：

```
ciscoasa(config)# access-list pim_nbr deny 10.1.1.1 255.255.255.255
```

この例では、次の ACL を **pim neighbor-filter** コマンドで使用すると、10.1.1.1 ルータを PIM ネイバーとして設定できなくなります。

ステップ 2 隣接ルータをフィルタリングします。

pim bidirectional-neighbor-filter pim_nbr

例：

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidirectional neighbor-filter pim_nbr
```

この例では、10.1.1.1 ルータが、インターフェイス GigabitEthernet0/3 上で PIM 双方向ネイバーとして設定できなくなります。

BSR 候補としての ASA の設定

ASA を BSR 候補として設定できます。

手順

ステップ 1 ルータがブートストラップルータ（BSR）として候補であることをアナウンスするよう設定します。

pim bsr-candidate *interface_name* [*hash_mask_length* [*priority*]]

例：

```
ciscoasa(config)# pim bsr-candidate inside 12 3
```

ステップ 2 （オプション）ASA を境界ブートストラップ ルータとして設定します。

interface *interface_name*

pim bsr-border

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# pim bsr-border
```

このコマンドがインターフェイスで設定されている場合、そのインターフェイスではブートストラップ ルータ（BSR）メッセージの送受信は行われません。

マルチキャスト境界の設定

アドレス スコーピングは、同じ IP アドレスを持つ RP が含まれるドメインが相互にデータを漏出させることのないように、ドメイン境界を定義します。スコーピングは、大きなドメイン内のサブネット境界や、ドメインとインターネットの間の境界で実行されます。

インターフェイスでマルチキャスト グループ アドレスの管理スコープ境界を設定できます。IANA では、239.0.0.0 ～ 239.255.255.255 のマルチキャスト アドレス範囲が管理スコープ アドレスとして指定されています。この範囲のアドレスは、さまざまな組織で管理されるドメイン内で再使用されます。このアドレスはグローバルではなく、ローカルで一意であるとみなされます。

影響を受けるアドレスの範囲は、標準 ACL で定義します。境界が設定されると、マルチキャスト データ パケットは境界を越えて出入りできなくなります。境界を定めることで、同じマルチキャスト グループ アドレスをさまざまな管理ドメイン内で使用できます。

filter-autorp キーワードを入力することにより、管理スコープ境界で Auto-RP 検出メッセージと通知メッセージを設定、検証、フィルタリングできます。境界の ACL で拒否された Auto-RP パケットからの Auto-RP グループ範囲通知は削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

手順

マルチキャスト境界を設定します。

multicast boundary acl [**filter-autorp**]

例：

```
ciscoasa(config-if)# multicast boundary acl1 [filter-autorp]
```

PIM のモニタリング

次のコマンドを使用して、PIM ルーティング プロセスをモニターできます。コマンド出力の例と説明については、コマンド リファレンスを参照してください。

さまざまな PIM ルーティング統計情報をモニターまたはディセーブル化するには、次のいずれかのコマンドを入力します。

- **show pim bsr-router**

  ブートストラップ ルータ情報を表示します。

- **show mroute**

  IP マルチキャスト ルーティング テーブルの内容を表示します。

- **show mfib summary**

  IPv4 PIM マルチキャスト転送情報ベースのエントリおよびインターフェイスの数に関する要約情報を表示します。

- **show mfib active**

  アクティブなマルチキャスト送信元がマルチキャスト グループに送信している速度を示す、マルチキャスト転送情報ベース（MFIB）からの情報を表示します。

- **show pim group-map**

  グループと PIM モードのマッピングを表示します。グループの RP を表示するには、グループ アドレスまたは名前を指定します。

- **show pim group-map rp-timers**

  各グループのタイマーの有効期限と稼働時間を PIM モード マッピング エントリに表示します。

- **show pim neighbor**

  PIM（Protocol Independent Multicast）ネイバーを表示します。

マルチキャスト ルーティングの例

次の例に、さまざまなオプションのプロセスを使用してマルチキャスト ルーティングをイネーブルにし、設定する方法を示します。

1. マルチキャスト ルーティングをイネーブルにします。

```
ciscoasa(config)# multicast-routing
```

2. スタティック マルチキャスト ルートを設定します。

```
ciscoasa(config)# mroute src_ip src_mask {input_if_name | rpf_neighbor} [distance]
ciscoasa(config)# exit
```

3. ASA をマルチキャスト グループのメンバとして設定します。

```
ciscoasa(config)# interface
ciscoasa(config-if)# igmp join-group group-address
```

マルチキャスト ルーティングの履歴

表 *45*：マルチキャスト ルーティングの機能履歴

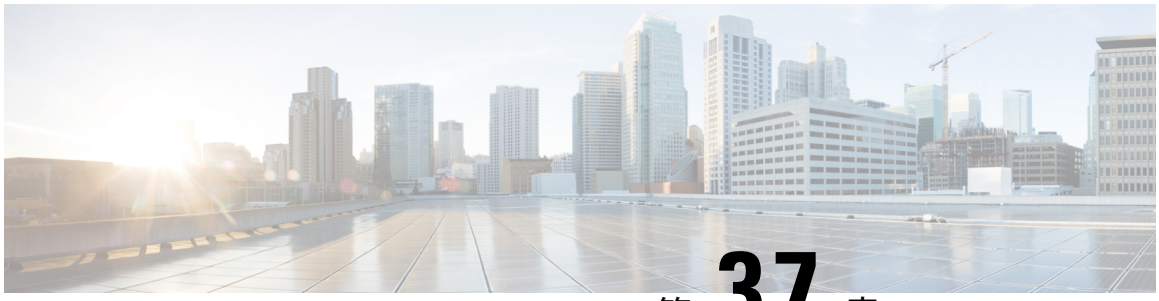
機能名	プラットフォーム リリース	機能情報
マルチキャスト ルーティング サポート	7.0(1)	マルチキャスト ルーティング プロトコルを使用した、データのマルチキャスト ルーティング データ、認証、およびルーティング情報の再配布とモニタリングのサポートが追加されました。 **multicast-routing** コマンドが導入されました。
クラスタリングのサポート	9.0(1)	クラスタリングのサポートが追加されました。 **debug mfib cluster**、**show mfib cluster** の各コマンドが導入されました。
Protocol Independent Multicast Source-Specific Multicast（PIM-SSM）パススルーのサポート	9.5(1)	ASA が最後のホップ ルータである場合を除いて、マルチキャスト ルーティングが有効になっているときに PIM-SSM パケットが通過できるようサポートを追加しました。これにより、さまざまな攻撃から保護すると同時に、マルチキャスト グループをより柔軟に選択できるようになりました。ホストは、明示的に要求された送信元からのトラフィックのみを受信します。 変更されたコマンドはありません。

機能名	プラットフォーム リリース	機能情報
Protocol Independent Multicast ブートストラップルータ（BSR）	9.5(2)	ランデブー ポイント（RP）機能の候補ルータを使用して、ランデブーポイント情報をグループに伝達するためのダイナミックランデブーポイント選択モデルがサポートされました。この機能は、ランデブーポイントを動的に学習する手段を提供します。これは、RP が停止と起動を繰り返す複雑で大規模なネットワークに不可欠です。 次のコマンドが導入されました。clear pim group-map、debug pim bsr、pim bsr-border、pim bsr-candidate、show pim bsr-router、show pim group-map rp-timers
igmp limit の緩和	9.15(1) *9.12(4)* でも同様	igmp limit が 500 から 5000 に増加しました。 新規/変更されたコマンド：**igmp limit**。

第 VI 部

AAA サーバーおよびローカル データベース

- AAA サーバーとローカル データベース （1427 ページ）
- AAA の RADIUS サーバー （1441 ページ）
- AAA 用の TACACS+ サーバー （1465 ページ）
- AAA の LDAP サーバー （1473 ページ）
- AAA の RSA SecurID サーバー （1487 ページ）



第 37 章

AAA サーバーとローカル データベース

この章では、認証、認可、アカウンティング（AAA は「トリプル A」と読む）について説明します。AAA は、コンピュータ リソースへのアクセスを制御するための一連のサービスで、サービスの課金に必要な情報を提供します。これらの処理は、効果的なネットワーク管理およびセキュリティにとって重要です。

この章では、AAA 機能用にローカル データベースを設定する方法について説明します。外部 AAA サーバーについては、ご使用のサーバー タイプに関する章を参照してください。

- AAA とローカル データベースについて （1427 ページ）
- ローカル データベースのガイドライン （1432 ページ）
- ローカル データベースへのユーザー アカウントの追加 （1432 ページ）
- ローカル データベースのモニタリング （1435 ページ）
- ローカル データベースの履歴 （1436 ページ）

AAA とローカル データベースについて

ここでは、AAA とローカル データベースについて説明します。

認証

認証はユーザーを特定する方法です。アクセスが許可されるには、ユーザーは通常、有効なユーザー名と有効なパスワードが必要です。AAA サーバは、ユーザのクレデンシャルとデータベースに保存されている他のユーザ クレデンシャルとを比較します。クレデンシャルが一致した場合は、ユーザはネットワークへのアクセスが許可されます。クレデンシャルが一致しない場合は、認証は失敗し、ネットワーク アクセスは拒否されます。

次の項目を認証するように ASA を設定できます。

- ASA へのすべての管理接続（この接続には、次のセッションが含まれます）
  - Telnet
  - SSH
  - シリアル コンソール

- ASDM（HTTPS を使用）
- VPN 管理アクセス

- **enable** コマンド
- ネットワーク アクセス層
- VPN アクセス

認証

許可はポリシーを適用するプロセスです。どのようなアクティビティ、リソース、サービスに対するアクセス許可をユーザーが持っているのかを判断します。ユーザーが認証されると、そのユーザーはさまざまなタイプのアクセスやアクティビティを認可される可能性があります。

次の項目を認可するように、ASA を設定できます。

- 管理コマンド
- ネットワーク アクセス層
- VPN アクセス

アカウンティング

アカウンティングは、アクセス時にユーザが消費したリソースを測定します。これには、システム時間またはセッション中にユーザが送受信したデータ量などが含まれます。アカウンティングは、許可制御、課金、トレンド分析、リソース使用率、キャパシティプランニングのアクティビティに使用されるセッションの統計情報と使用状況情報のログを通じて行われます。

認証、認可、アカウンティング間の相互作用

認証だけで使用することも、許可およびアカウンティングとともに使用することもできます。許可では必ず、ユーザの認証が最初に済んでいる必要があります。アカウンティングだけで使用することも、認証および認可とともに使用することもできます。

AAA サーバーおよびサーバーグループ

AAA サーバーは、アクセス制御に使用されるネットワーク サーバーです。認証は、ユーザーを識別します。認可は、認証されたユーザーがアクセスする可能性があるリソースとサービスを決定するポリシーを実装します。アカウンティングは、課金と分析に使用される時間とデータのリソースを追跡します。

外部 AAA サーバーを使用する場合は、まず外部サーバーで使用するプロトコルに応じた AAA サーバーグループを作成し、そのグループにサーバーを追加する必要があります。プロトコル

ごとに複数のグループを作成し、使用するすべてのプロトコルについてグループを分けることができます。各サーバー グループは、あるサーバーまたはサービスに固有です。

グループの作成方法の詳細については、次のトピックを参照してください。

- RADIUS サーバ グループの設定 （1455 ページ）
- TACACS+ サーバー グループの設定 （1468 ページ）
- LDAP サーバー グループの設定 （1480 ページ）
- RSA SecurID AAA サーバーグループの設定 （1488 ページ）

HTTP Form の使用の詳細については、 VPN 構成ガイドを参照してください。

（注） ASA 9.22.1 以降、Kerberos プロトコルはサポートされていません。AAA サービスに Kerberos を使用できなくなりました。下の 表 に記載されているその他のサポート対象サーバーを使用することをお勧めします。

次の表に、ローカルデータベースを含むサポートされるサーバーのタイプとその用途の概要を示します。

表 *46 : AAA* サーバーでサポートされるサービス

サーバータイプとサービス	認証	許可	アカウンティング
ローカル データベース			
管理者	はい	はい	非対応
VPN ユーザー	はい	非対応	非対応
ファイアウォールセッション（AAA ルール）	はい	はい	非対応
RADIUS			
管理者	はい	はい	はい
VPN ユーザー	はい	はい	はい
ファイアウォールセッション（AAA ルール）	はい	はい	はい
TACACS+			
管理者	はい	はい	はい
VPN ユーザー	はい	非対応	はい

サーバータイプとサービス	認証	許可	アカウンティング
ファイアウォールセッション（AAA ルール）	はい	はい	はい
LDAP			
管理者	はい	非対応	非対応
VPN ユーザー	はい	はい	非対応
ファイアウォールセッション（AAA ルール）	はい	非対応	非対応
SDI（RSA SecurID）			
管理者	はい	非対応	非対応
VPN ユーザー	はい	非対応	非対応
ファイアウォールセッション（AAA ルール）	はい	非対応	非対応
HTTP Form			
管理者	いいえ	非対応	非対応
VPN ユーザー	はい	非対応	非対応
ファイアウォールセッション（AAA ルール）	いいえ	非対応	非対応

注記

- RADIUS：管理者のアカウンティングには、コマンドアカウンティングは含まれません。
- RADIUS：ファイアウォールセッションの認可は、ユーザー固有のアクセスリストでだけサポートされます。このアクセスリストはRADIUS認証応答で受信または指定されます。
- TACACS+：管理者のアカウンティングには、コマンドアカウンティングが含まれます。
- HTTP Form：クライアントレスSSL VPNユーザーセッションの場合に限り、認証とSSO操作がサポートされます。

ローカル データベースについて

ASAは、ユーザープロファイルを取り込むことができるローカルデータベースを管理します。AAA サーバーの代わりにローカル データベースを使用して、ユーザー認証、認可、アカウンティングを提供することもできます。

次の機能にローカル データベースを使用できます。

- ASDM ユーザーごとのアクセス
- コンソール認証
- Telnet 認証および SSH 認証
- **enable** コマンド認証

  この設定は、CLI アクセスにだけ使用され、Cisco ASDM ログインには影響しません。
- コマンド許可

  ローカルデータベースを使用するコマンド許可を有効にすると、ASA では、ユーザー特権レベルを参照して使用可能なコマンドが特定されます。コマンド許可がディセーブルの場合は通常、特権レベルは参照されません。デフォルトでは、コマンドの特権レベルはすべて、0 または 15 のどちらかです。
- ネットワーク アクセス認証
- VPN クライアント認証

マルチ コンテキスト モードの場合、システム実行スペースでユーザー名を設定し、**login** コマンドを使用して CLI で個々にログインできます。ただし、システム実行スペースではローカル データベースを参照する AAA ルールは設定できません。

（注） ローカル データベースはネットワーク アクセス認可には使用できません。

フォールバック サポート

ローカル データベースは、複数の機能のフォールバック方式として動作できます。この動作は、ASA から誤ってロックアウトされないように設計されています。

ログインすると、コンフィギュレーション内で指定されている最初のサーバーから、応答があるまでグループ内のサーバーが順に 1 つずつアクセスされます。グループ内のすべてのサーバーが使用できない場合、ローカルデータベースがフォールバック方式（管理認証および許可限定）として設定されていると、ASA はローカルデータベースに接続しようとします。フォールバック方式として設定されていない場合、ASA は引き続き AAA サーバーにアクセスしようとします。

フォールバック サポートを必要とするユーザーについては、ローカル データベース内のユーザー名およびパスワードと、AAA サーバー上のユーザー名およびパスワードとを一致させることを推奨します。これにより、透過フォールバックがサポートされます。ユーザーは、AAA サーバーとローカルデータベースのどちらがサービスを提供しているかが判別できないので、ローカルデータベースのユーザー名およびパスワードとは異なるユーザー名およびパスワードを AAA サーバーで使用することは、指定するべきユーザー名とパスワードをユーザーが確信できないことを意味します。

ローカル データベースでサポートされているフォールバック機能は次のとおりです。

- コンソールおよびイネーブル パスワード認証：グループ内のサーバーがすべて使用できない場合、ASA ではローカル データベースを使用して管理アクセスを認証します。これには、イネーブル パスワード認証が含まれる場合があります。
- コマンド許可：グループ内の TACACS+ サーバーがすべて使用できない場合、特権レベルに基づいてコマンドを認可するためにローカル データベースが使用されます。
- VPN 認証および認可：VPN 認証および認可は、通常この VPN サービスをサポートしている AAA サーバーが使用できない場合、ASA へのリモート アクセスをイネーブルにするためにサポートされます。管理者である VPN クライアントが、ローカル データベースへのフォールバックを設定されたトンネル グループを指定する場合、AAA サーバー グループが使用できない場合でも、ローカルデータベースが必要な属性で設定されていれば、VPN トンネルが確立できます。

グループ内の複数のサーバーを使用したフォールバックの仕組み

サーバー グループ内に複数のサーバーを設定し、サーバー グループのローカル データベースへのフォールバックをイネーブルにしている場合、ASA からの認証要求に対してグループ内のどのサーバーからも応答がないと、フォールバックが発生します。次のシナリオで例証します。

サーバー 1、サーバー 2 の順で、LDAP サーバー グループに 2 台の Active Directory サーバーを設定します。リモート ユーザーがログインすると、ASA によってサーバー 1 に対する認証が試みられます。

サーバー 1 から認証エラー（「user not found」など）が返されると、ASA によるサーバー 2 に対する認証は試みられません。

タイムアウト期間内にサーバ 1 から応答がないと（または認証回数が、設定されている最大数を超えている場合）、ASA によってサーバ 2 に対する認証が試みられます。

グループ内のどちらのサーバーからも応答がなく、ASA にローカル データベースへのフォールバックが設定されている場合、ASA によってローカル データベースに対する認証が試みられます。

ローカル データベースのガイドライン

ローカル データベースを認証または認可に使用する場合、ASA からのロックアウトを必ず防止してください。

ローカル データベースへのユーザー アカウントの追加

ユーザーをローカル データベースに追加するには、次の手順を実行します。

手順

ステップ 1 ユーザー アカウントを作成します。

username *username* [**password** *password*] [**privilege** *priv_level*]

例：

```
ciscoasa(config)# username exampleuser1 password madmaxfuryroadrules privilege 1
```

username *username* キーワードは、3 ～ 64 文字の文字列で、スペースと疑問符を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）で構成されます。**password** *password* キーワードは、8 ～ 127 文字の文字列で、以下を除く任意の ASCII 印刷可能文字（文字コード 32 ～ 126）を組み合わせることができます。

- スペースは使用できません。
- 疑問符は使用できません。
- 3 文字以上連続した、順番に並んだ ASCII 文字または繰り返される ASCII 文字は使用できません。たとえば、次のパスワードは拒否されます。
  - **abc**user1
  - user**543**
  - user**aaaa**
  - user2**666**

SSH 公開キー認証を使用している場合など、パスワードを指定せずにユーザー名を作成することもできます。**privilege** *priv_level* キーワードでは、0 ～ 15 の範囲で特権レベルを設定します。デフォルトは 2 です。この特権レベルは、コマンド認可で使用されます。

注意
コマンド認可（**aaa authorization console LOCAL** コマンド）を使用していない場合、デフォルトのレベル 2 を使用して特権 EXEC モードにアクセスできます。特権 EXEC モードへのアクセスを制限する場合、特権レベルを 0 または 1 に設定するか、**service-type** コマンドを使用します。

使用頻度の低いこれらのオプションは上記の構文には示されていません。**nopassword** キーワードを使用すると、任意のパスワードを受け入れるユーザーアカウントが作成されます。このオプションは安全ではないため推奨されません。

encrypted キーワード（9.6 以前の場合は 32 文字以内のパスワード用）または **pbkdf2** キーワード（9.6 以降では 32 文字を超えるパスワード用、9.7 以降では長さを問わずすべてのパスワード用） は、（MD5 ベースのハッシュまたは PBKDF2（Password-Based Key Derivation Function 2）ハッシュを使用して）パスワードが暗号化されていることを示します。新しいパスワードを入力しない限り、既存のパスワードは MD5 ベースのハッシュを使用し続けることに注意し

てください。**username** コマンドのパスワードを定義すると、ASA はセキュリティを維持するために、そのパスワードを設定に保存するときに暗号化します。**show running-config** コマンドを入力すると、**username** コマンドでは実際のパスワードは示されません。暗号化されたパスワードとそれに続けて **encrypted** または **pbkdf2** キーワードが示されます。たとえば、パスワードに「test」と入力すると、**show running-config** コマンドの出力には次のように表示されます。

```
username user1 password DLaUiAX3l78qgoB5c7iVNw== encrypted
```

実際に CLI で **encrypted** または **pbkdf2** キーワードを入力するのは、同じパスワードを使用して、ある設定ファイルを他の ASA で使用するためにカット アンド ペーストする場合だけです。

ステップ 2 （オプション）ユーザ名属性を設定します。

username *username* **attributes**

例：

```
ciscoasa(config)# username exampleuser1 attributes
```

username 引数は、最初の手順で作成したユーザー名です。

デフォルトでは、このコマンドで追加した VPN ユーザーには属性またはグループ ポリシーが関連付けられません。**username attributes** コマンドを使用して、すべての値を明示的に設定する必要があります。詳細については、VPN 構成ガイドを参照してください。

ステップ 3 （オプション）管理認可を設定している場合は、**aaa authorization exec** コマンドを使用して、ユーザー レベルを設定します。

service-type {**admin** | **nas-prompt** | **remote-access**}

例：

```
ciscoasa(config-username)# service-type admin
```

admin キーワードは、**aaa authentication console LOCAL** コマンドによって指定されたサービスへのフル アクセスを許可します。デフォルトは **admin** キーワードです。

nas-prompt キーワードは、**aaa authentication** {**telnet** | **ssh** | **serial**} **console** コマンドを設定している場合は CLI へのアクセスを許可しますが、**aaa authentication http console** コマンドを設定している場合は ASDM へのコンフィギュレーション アクセスを拒否します。ASDM モニタリング アクセスは許可します。**aaa authentication enable console** コマンドを使用して認証を有効にしている場合、ユーザーは、**enable** コマンド（または **login** コマンド）を使用して特権 EXEC モードにアクセスできません。

remote-access キーワードは管理アクセスを拒否します。**aaa authentication console** コマンドで指定されたサービスは使用できません（**serial** キーワードを除きます。シリアル アクセスは許可されます）。

ステップ 4 （任意） ユーザ単位の ASA への SSH 接続の公開キー認証については、公開キー アクセス用の SSH の設定 （1501 ページ） を参照してください。

ステップ 5 （任意） VPN 認証にこのユーザー名を使用している場合、そのユーザーに多くの VPN 属性を設定できます。詳細については、VPN 構成ガイドを参照してください。

例

次の例では、admin ユーザ アカウントに対して特権レベル 15 を割り当てます。

```
ciscoasa(config)# username admin password farscape1 privilege 15
```

次の例では、管理認可を有効にし、パスワードを指定してユーザー アカウントを作成し、ユーザー名コンフィギュレーション モードを開始して、**nas-prompt** の **service-type** を指定します。

```
ciscoasa(config)# aaa authorization exec authentication-server
ciscoasa(config)# username user1 password gOrgeOus
ciscoasa(config)# username user1 attributes
ciscoasa(config-username)# service-type nas-prompt
```

ローカル データベースのモニタリング

ローカル データベースのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたデータベースの統計情報を表示します。AAA サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを使用します。

- **show running-config aaa-server**

  このコマンドは、AAA サーバーの実行コンフィギュレーションを表示します。AAA サーバー コンフィギュレーションをクリアするには、**clear configure aaa-server** コマンドを使用します。

ローカル データベースの履歴

表 *47:* ローカル データベースの履歴

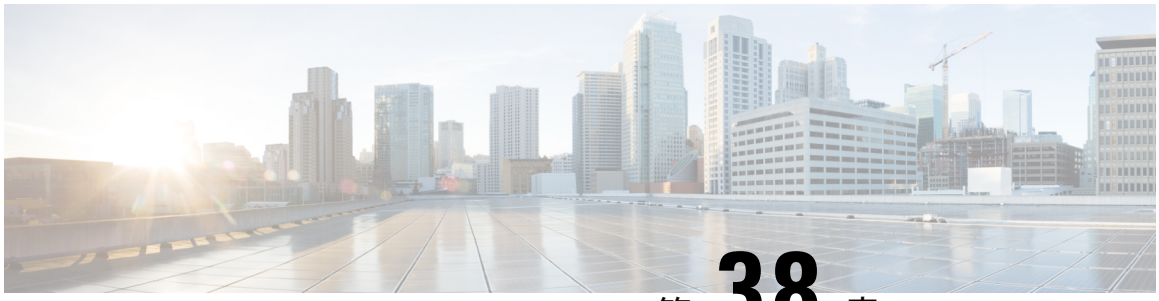
機能名	プラットフォーム リリース	説明
AAA のローカル データベース設定	7.0(1)	AAA 用にローカル データベースを設定する方法について説明します。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**aaa authentication** {**telnet | ssh | serial**} **console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**show running-config aaa-server**、**show aaa-server**、**clear configure aaa-server**、**clear aaa-server statistics**。
SSH 公開キー認証のサポート	9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザー単位で有効にできるようになりました。公開キー ファイル（PKF）でフォーマットされたキーまたはBase64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次のコマンドが導入されました。**ssh authenticaion**。 *8.4(4.1)* でも使用可能。*PKF* キー形式は *9.1(2)* でのみサポートされます。
ローカルの **username** および **enable** パスワードでより長いパスワード（127 文字まで）がサポートされます。	9.6(1)	127 文字までのローカル **username** および **enable** パスワードを作成できます（以前の制限は 32 文字でした）。32 文字以上のパスワードを作成すると、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。これよりも短いパスワードは引き続き MD5 ベースのハッシュを使用します。 次のコマンドを変更しました。**enable**、**username**

機能名	プラットフォーム リリース	説明
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカル ユーザー データベース（(**aaa authentication ssh console LOCAL**)）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（(**ssh authentication**)）を有効にすることができました。この設定は修正されたため、AAA SSH 認証を明示的に有効にする必要があります。ユーザーが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザー名を作成できるようになりました。 次のコマンドが変更されました。**ssh authentication**、**username**
すべてのローカル **username** および **enable** パスワードに対する PBKDF2 ハッシュ	9.7(1)	長さ制限内のすべてのローカル **username** および **enable** パスワードは、PBKDF2（パスワードベース キー派生関数 2）のハッシュを使用して設定に保存されます。以前は、32 文字以下のパスワードが MD5 ベースのハッシュ メソッドを使用していました。既存のパスワードでは、ユーザーが新しいパスワードを入力しない限り、MD5 ベースのハッシュが引き続き使用されます。ダウングレードのガイドラインについては、『一般操作構成ガイド』の「ソフトウェアおよびコンフィギュレーション」の章を参照してください。 次のコマンドを変更しました。**enable**、**username**

機能名	プラットフォーム リリース	説明
SSH 公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザー データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザーに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更されたコマンドはありません。

より強力なローカルユーザーと有効なパスワード要件	9.17(1)	ローカルユーザーと有効なパスワードについて、次のパスワード要件が追加されました。
		
		• パスワードの長さ：8 文字以上。以前は、最小値が 3 文字でした。
		
		• 繰り返し文字と連続文字：3 つ以上の連続した ASCII 文字または繰り返しの ASCII 文字は許可されません。たとえば、次のパスワードは拒否されます。
		
		  • **abc**user1
		
		  • user**543**
		
		  • user**aaaa**
		
		  • user2**666**
		
		新規/変更されたコマンド：**enable password**、**username**

機能名	プラットフォーム リリース	説明
ローカルユーザーのロックアウトの変更	9.17(1)	設定可能な回数のログイン試行に失敗すると、ASA はローカルユーザーをロックアウトする場合があります。この機能は、特権レベル 15 のユーザーには適用されませんでした。また、管理者がアカウントのロックを解除するまで、ユーザーは無期限にロックアウトされます。管理者がその前に **clear aaa local user lockout** コマンドを使用しない限り、ユーザーは 10 分後にロック解除されるようになりました。特権レベル 15 のユーザーも、ロックアウト設定が適用されるようになりました。 新規/変更されたコマンド：**aaa local authentication attempts max-fail** 、**show aaa local user**
SSH および Telnet パスワード変更プロンプト	9.17(1)	ローカルユーザーが SSH または Telnet を使用して ASA に初めてログインすると、パスワードを変更するように求められます。また、管理者がパスワードを変更した後、最初のログインに対してもプロンプトが表示されます。ただし、ASA がリロードすると、最初のログインであっても、ユーザーにプロンプトは表示されません。 新規/変更されたコマンド： **show aaa local user**



第 38 章

AAA の RADIUS サーバー

この章では、AAA 用に RADIUS サーバーを設定する方法について説明します。

- AAA 用の RADIUS サーバーについて （1441 ページ）
- AAA の RADIUS サーバーのガイドライン （1454 ページ）
- AAA 用の RADIUS サーバーの設定 （1455 ページ）
- AAA 用の RADIUS サーバーのモニタリング （1462 ページ）
- AAA 用の RADIUS サーバーの履歴 （1463 ページ）

AAA 用の RADIUS サーバーについて

ASA は AAA について、次の RFC 準拠 RADIUS サーバーをサポートします。

- Cisco Secure ACS 3.2、4.0、4.1、4.2、および 5.x
- Cisco Identity Services Engine（ISE）
- RSA 認証マネージャ 5.2、6.1 および 7.x の RSA Radius
- Microsoft

サポートされている認証方式

ASA は、RADIUS サーバーでの次の認証方式をサポートします。

- PAP：すべての接続タイプの場合。
- CHAP および MS-CHAPv1：L2TP-over-IPsec 接続の場合。
- MS-CHAPv2：L2TP-over-IPsec 接続の場合。また、パスワード管理機能がイネーブルで、通常の IPsec リモート アクセス接続の場合。MS-CHAPv2 は、クライアントレス接続でも使用できます。
- 認証プロキシ モード：RADIUS から Active Directory、RADIUS から RSA/SDI、Radius からトークン サーバー、RSA/SDI から RADIUS の各接続。

（注） MS-CHAPv2 を、ASA と RADIUS サーバーの間の VPN 接続で使用されるプロトコルとしてイネーブルにするには、トンネル グループ一般属性でパスワード管理をイネーブルにする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバーへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネル グループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバが MS-CHAPv2 以外の認証要求を送信するように設定できます。

VPN 接続のユーザー認証

ASA は、RADIUS サーバーを使用して、ダイナミック ACL またはユーザーごとの ACL 名を使用する VPN リモート アクセスおよびファイアウォール カットスルー プロキシ セッションのユーザー許可を実行できます。ダイナミック ACL を実装するには、これをサポートするように RADIUS サーバーを設定する必要があります。ユーザーを認証する場合、RADIUS サーバーによってダウンロード可能 ACL、または ACL 名が ASA に送信されます。所定のサービスへのアクセスが ACL によって許可または拒否されます。認証セッションの有効期限が切れると、ASA は ACL を削除します。

ACL に加えて、ASA は、VPN リモート アクセスおよびファイアウォール カットスルー プロキシセッションの認証およびアクセス許可の設定を行うための多くの属性をサポートしています。

RADIUS 属性のサポートされるセット

ASA は次の RADIUS 属性のセットをサポートしています。

- RFC 2138 および 2865 に定義されている認証属性
- RFC 2139 および 2866 に定義されているアカウンティング属性
- RFC 2868 および 6929 に定義されているトンネルプロトコルサポート用の RADIUS 属性
- Cisco IOS ベンダー固有属性（VSA）は、RADIUS ベンダー ID 9 で識別されます。
- RADIUS ベンダー ID 3076 によって識別される Cisco VPN 関連 VSA
- RFC 2548 に定義されている Microsoft VSA

サポートされる RADIUS 認証属性

認可では、権限または属性を使用するプロセスを参照します。認証サーバーとして定義されているRADIUSサーバーは、権限または属性が設定されている場合はこれらを使用します。これらの属性のベンダー ID は 3076 です。

次の表に、ユーザー認可に使用可能な、サポートされているRADIUS属性の一覧を示します。

（注） RADIUS 属性名には、cVPN3000 プレフィックスは含まれていません。Cisco Secure ACS 4.x は、この新しい名前をサポートしますが、4.0 以前の ACS の属性名にはまだ cVPN3000 プレフィックスが含まれています。ASA は、属性名ではなく数値の属性 ID に基づいて RADIUS 属性を使用します。

次の表に示した属性はすべてダウンストリーム属性であり、RADIUS サーバーから ASA に送信されます。ただし、属性番号 146、150、151、および 152 を除きます。これらの属性番号はアップストリーム属性であり、ASA から RADIUS サーバーに送信されます。RADIUS 属性 146 および 150 は、認証および認可の要求の場合に ASA から RADIUS サーバーに送信されます。前述の 4 つの属性はすべて、アカウンティング開始、中間アップデート、および終了の要求の場合に ASA から RADIUS サーバーに送信されます。アップストリーム RADIUS 属性 146、150、151、152 は、バージョン 8.4(3) で導入されました。

表 *48 :* サポートされる *RADIUS* 認証属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Access-Hours	Y	1	String	シングル	時間範囲の名前（Business-hours など）
Access-List-Inbound	Y	86	文字列	シングル	ACL ID
Access-List-Outbound	Y	87	文字列	シングル	ACL ID
Address-Pools	Y	217	文字列	シングル	IP ローカル プールの名前
Allow-Network-Extension-Mode	Y	64	ブール	シングル	0 = 無効1 = 有効
Authenticated-User-Idle-Timeout	Y	50	整数	シングル	1 ～ 35791394 分
Authorization-DN-Field	Y	67	文字列	シングル	有効な値：UID、OU、O、CN、L、SP、T、N、GN、SN、I、GENQ、DNQ、SE use-entire-name
Authorization-Required		66	整数	シングル	0 = いいえ 1 = はい
Authorization-Type	対応	65	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Banner1	Y	15	文字列	シングル	Cisco VPN リモートアクセスセッション（I IKEv1、セキュアクライアント SSL-TLS/DTLS/IKEv2、およびクライアント SSL）に対して表示されるバナー文字列
Banner2	Y	36	文字列	シングル	Cisco VPN リモートアクセスセッション（I IKEv1、セキュアクライアント SSL-TLS/DTLS/IKEv2、およびクライアント SSL）に対して表示されるバナー文字列Ban 字列はBanner1 文字列に連結されます（設定 いる場合）。
Cisco-IP-Phone-Bypass	Y	51	整数	シングル	0 = 無効1 = 有効
Cisco-LEAP-Bypass	Y	75	整数	シングル	0 = 無効1 = 有効
Client Type	Y	150	整数	シングル	1 = Cisco VPN Client（IKEv1） 2 = セキュア アント SSL VPN 3 = Clientless SSL VPN 4 = Cut-Through-Proxy 5 = L2TP/IPsec SSL VPN 6 キュアクライアント IPsec VPN（IKEv2）
Client-Type-Version-Limiting	Y	77	文字列	シングル	IPsec VPN のバージョン番号を示す文字列
DHCP-Network-Scope	Y	61	文字列	シングル	IP アドレス
Extended-Authentication-On-Rekey	Y	122	整数	シングル	0 = 無効1 = 有効
Framed-Interface-Id	Y	96	文字列	シングル	割り当てられた IPv6 インターフェイス ID。 割り当てられた IPv6 アドレスを作成するた Framed-IPv6-Prefix と組み合わせます。例： Framed-Interface-ID=1:1:1:1 と Framed-IPv6-Prefix=2001:0db8::/64 を組み合わ と、IP アドレス 2001:0db8::1:1:1:1 が得られ

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Framed-IPv6-Prefix	Y	97	文字列	シングル	割り当てられた IPv6 プレフィックスと長 に割り当てられたIPv6アドレスを作成す Framed-Interface-Id と組み合わせます。例 フィックス 2001:0db8::/64 と Framed-Interface-Id=1:1:1:1 を組み合わせ ドレス 2001:0db8::1:1:1:1 が得られます。 を使用して、フレームインターフェイス せずに IP アドレスを割り当てることが これには、プレフィックス長/128 を使用 なIPv6アドレスを割り当てます（たとえ ム化された IPv6 プレフィックス = 2001: 1/128）。
Group-Policy	Y	25	文字列	シングル	リモート アクセス VPN セッションのグ リシーを設定します。バージョン 8.2.x 以 IETF-Radius-Class の代わりにこの属性を す。次のいずれかの形式を使用できます • グループポリシー名 • OU=グループポリシー名 • OU=グループポリシー名。
IE-Proxy-Bypass-Local		83	整数	シングル	0 = なし 1 = ローカル
IE-Proxy-Exception-List		82	文字列	シングル	改行（\n）区切りの DNS ドメインのリス
IE-Proxy-PAC-URL	Y	133	文字列	シングル	PAC アドレス文字列
IE-Proxy-Server		80	文字列	シングル	IP アドレス
IE-Proxy-Server-Policy		81	整数	シングル	1 = 変更なし 2 = プロキシなし 3 = 自動検 ンセントレータ設定を使用する
IKE-KeepAlive-Confidence-Interval	Y	68	整数	シングル	10 ～ 300 秒
IKE-Keepalive-Retry-Interval	Y	84	整数	シングル	2 ～ 10 秒
IKE-Keep-Alives	Y	41	ブール	シングル	0 = 無効1 = 有効
Intercept-DHCP-Configure-Msg	Y	62	ブール	シングル	0 = 無効1 = 有効
IPsec-Allow-Passwd-Store	Y	16	ブール	シングル	0 = 無効1 = 有効

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Authentication		13	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP（認可のみ）ドメイン 4 = SDI 5 = 内部 6 = RADIUS での認証 7 = Active Directory
IPsec-Auth-On-Rekey	Y	42	ブール	シングル	0 = 無効1 = 有効
IPsec-Backup-Server-List	Y	60	文字列	シングル	サーバー アドレス（スペース区切り）
IPsec-Backup-Servers	Y	59	文字列	シングル	1 = クライアントが設定したリストを使用すクライアント リストを無効化して消去するクアップ サーバー リストを使用する
IPsec-Client-Firewall-Filter-Name		57	文字列	シングル	クライアントにファイアウォール ポリシー配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	58	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	28	文字列	シングル	クライアントに送信するデフォルト ドメイ1 つだけ指定します（1 ～ 255 文字）。
IPsec-IKE-Peer-ID-Check	Y	40	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場チェックしない
IPsec-IP-Compression	Y	39	整数	シングル	0 = 無効1 = 有効
IPsec-Mode-Config	Y	31	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP	Y	34	ブール	シングル	0 = 無効1 = 有効
IPsec-Over-UDP-Port	Y	35	整数	シングル	4001 ～ 49151。デフォルトは 10000 です。
IPsec-Required-Client-Firewall-Capability	Y	56	整数	シングル	0 = なし 1 = リモート FW Are-You-There（A定義されているポリシー 2 = Policy pushed C サーバーからのポリシー
IPsec-Sec-Association		12	文字列	シングル	セキュリティ アソシエーションの名前
IPsec-Split-DNS-Names	Y	29	文字列	シングル	クライアントに送信するセカンダリ ドメイリストを指定します（1 ～ 255 文字）。
IPsec-Split-Tunneling-Policy	Y	55	整数	シングル	0 = スプリット トンネリングなし 1 = スプリンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	27	文字列	シングル	スプリット トンネルの包含リストを記述しトワークまたは ACL の名前を指定します。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IPsec-Tunnel-Type	Y	30	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス
IPsec-User-Group-Lock		33	ブール	シングル	0 = 無効1 = 有効
IPv6-Address-Pools	Y	218	文字列	シングル	IP ローカル プール IPv6 の名前
IPv6-VPN-Filter	Y	219	文字列	シングル	ACL 値
L2TP-Encryption		21	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 128 ビット 8 = ステートレスが必要 15 = 4 トで暗号化/ステートレスが必要
L2TP-MPPC-Compression		38	整数	シングル	0 = 無効1 = 有効
Member-Of	Y	145	文字列	シングル	カンマ区切りの文字列。例： `Engineering, Sales` ダイナミック アクセス ポリシーで使用 属性。グループ ポリシーは設定されませ
MS-Client-Subnet-Mask	Y	63	ブール	シングル	IP アドレス
NAC-Default-ACL		92	文字列		ACL
NAC-Enable		89	整数	シングル	0 = いいえ 1 = はい
NAC-Revalidation-Timer		91	整数	シングル	300 ～ 86400 秒
NAC-Settings	Y	141	文字列	シングル	NAC ポリシーの名前
NAC-Status-Query-Timer		90	整数	シングル	30 ～ 1800 秒
Perfect-Forward-Secrecy-Enable	Y	88	ブール	シングル	0 = いいえ 1 = はい
PPTP-Encryption		20	整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 128 ビット 8 = ステートレスが必要 15 = 4 トで暗号化/ステートレスが必要
PPTP-MPPC-Compression		37	整数	シングル	0 = 無効1 = 有効
Primary-DNS	Y	5	文字列	シングル	IP アドレス
Primary-WINS	Y	7	文字列	シングル	IP アドレス
Privilege-Level	Y	220	整数	シングル	0 ～ 15 の整数。

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Required-Client- Firewall-Vendor-Code	Y	45	整数	シングル	1 = Cisco Systems（Cisco Integrated Client を使 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = Cisco Systems（Cisco Intrusion Prevention Sec Agent を使用）
Required-Client-Firewall-Description	Y	47	文字列	シングル	文字列
Required-Client-Firewall-Product-Code	Y	46	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent ま Cisco Integrated Client（CIC） Zone Labs 製品： 1 = Zone Alarm 2 = Zone Al 3 = Zone Labs Integrity NetworkICE 製品： 1 = BlackIce Defender/Ag Sygate 製品： 1 = Personal Firewall 2 = Person Firewall Pro 3 = Security Agent
Required-Individual-User-Auth	Y	49	整数	シングル	0 = 無効1 = 有効
Require-HW-Client-Auth	Y	48	ブール	シングル	0 = 無効1 = 有効
Secondary-DNS	Y	6	文字列	シングル	IP アドレス
Secondary-WINS	Y	8	文字列	シングル	IP アドレス
SEP-Card-Assignment		9	整数	シングル	未使用
Session Subtype	Y	152	整数	シングル	0 = なし 1 =クライアントレス 2 =クライアン クライアントのみ Session Subtype が適用されるのは、Session （151）属性の値が 1、2、3、または 4 の場 です。
Session Type	Y	151	整数	シングル	0 = なし 1 = セキュアクライアント SSL VPN キュアクライアント IPSec VPN（IKEv2） 3 イアントレス SSL VPN 4 = クライントレス電 ルプロキシ 5 = Cisco VPN Client（IKEv1） 6 = LAN-LAN 7 = IKEv2 LAN-LAN 8 = VPN ロー ンシング
Simultaneous-Logins	Y	2	整数	シングル	0-2147483647
Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
Smart-Tunnel-Auto	Y	138	整数	シングル	0 = ディセーブル 1 = イネーブル 2 = 自動
Smart-Tunnel-Auto-Signon-Enable	Y	139	文字列	シングル	ドメイン名が付加された Smart Tunnel Au リストの名前
Strip-Realm	Y	135	ブール	シングル	0 = 無効1 = 有効
SVC-Ask	Y	131	文字列	シングル	0=ディセーブル 1=イネーブル 3=デフォ ビスをイネーブルにする 5 = デフォルト ントレスをイネーブルにする （2 と 4 は い）
SVC-Ask-Timeout	Y	132	整数	シングル	5 ～ 120 秒
SVC-DPD-Interval-Client	Y	108	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DPD-Interval-Gateway	Y	109	整数	シングル	0 = オフ 5 ～ 3600 秒
SVC-DTLS	Y	123	整数	シングル	0 = False 1 = True
SVC-Keepalive	Y	107	整数	シングル	0 = オフ 15 ～ 600 秒
SVC-Modules	Y	127	文字列	シングル	文字列（モジュールの名前）
SVC-MTU	Y	125	整数	シングル	MTU 値 256 ～ 1406 バイト
SVC-Profiles	Y	128	文字列	シングル	文字列（プロファイルの名前）
SVC-Rekey-Time	Y	110	整数	シングル	0 = ディセーブル 1 ～ 10080 分
Tunnel Group Name	Y	146	文字列	シングル	1 ～ 253 文字
Tunnel-Group-Lock	Y	85	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	Y	11	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = I 16 = WebVPN 32 = SVC 64 = IPsec (IKEv2 相互排他。0 ～ 11、16 ～ 27、32 ～ 43、 有効な値。
Use-Client-Address		17	ブール	シングル	0 = 無効1 = 有効
VLAN	Y	140	整数	シングル	0 ～ 4094
WebVPN-Access-List	Y	73	文字列	シングル	アクセス リスト名
WebVPN ACL	Y	73	文字列	シングル	デバイスの WebVPN ACL 名

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-ActiveX-Relay	Y	137	整数	シングル	0 = 無効 その他 = 有効
WebVPN-Apply-ACL	Y	102	整数	シングル	0 = 無効1 = 有効
WebVPN-Auto-HTTP-Signon	Y	124	文字列	シングル	予約済み
WebVPN-Citrix-Metaframe-Enable	Y	101	整数	シングル	0 = 無効1 = 有効
WebVPN-Content-Filter-Parameters	Y	69	整数	シングル	1 = Java ActiveX 2 = Java スクリプト 4 = イメ = イメージに含まれるクッキー
WebVPN-Customization	Y	113	文字列	シングル	カスタマイゼーションの名前
WebVPN-Default-Homepage	Y	76	文字列	シングル	URL（たとえば http://example-example.com）
WebVPN-Deny-Message	Y	116	文字列	シングル	有効な文字列（500 文字以内）
WebVPN-Download_Max-Size	Y	157	整数	シングル	0x7fffffff
WebVPN-File-Access-Enable	Y	94	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Browsing-Enable	Y	96	整数	シングル	0 = 無効1 = 有効
WebVPN-File-Server-Entry-Enable	Y	95	整数	シングル	0 = 無効1 = 有効
WebVPN-Group-based-HTTP/HTTPS-Proxy-Exception-List	Y	78	文字列	シングル	オプションのワイルドカード（*）を使用し マ区切りの DNS/IP（たとえば、*.cisco.com 192.168.1.*、wwwin.cisco.com）
WebVPN-Hidden-Shares	Y	126	整数	シングル	0 = なし 1 = 表示される
WebVPN-Home-Page-Use-Smart-Tunnel	Y	228	ブール	シングル	クライアントレス ホームページをスマート ル経由で表示する場合にイネーブルにしま
WebVPN-HTML-Filter	Y	69	Bitmap	シングル	1 = Java ActiveX 2 = スクリプト 4 = イメージ キー
WebVPN-HTTP-Compression	Y	120	整数	シングル	0 = オフ 1 = デフレート圧縮
WebVPN-HTTP-Proxy-IP-Address	Y	74	文字列	シングル	http= または https= プレフィックス付きの、 区切りの DNS/IP:ポート（例：http=10.10.10. https=11.11.11.11:443）
WebVPN-Idle-Timeout-Alert-Interval	Y	148	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN-Keepalive-Ignore	Y	121	整数	シングル	0 ～ 900

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Macro-Substitution	Y	223	文字列	シングル	無制限。
WebVPN-Macro-Substitution	Y	224	文字列	シングル	無制限。
WebVPN-Port-Forwarding-Enable	Y	97	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	Y	98	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-HTTP-Proxy	Y	99	整数	シングル	0 = 無効1 = 有効
WebVPN-Port-Forwarding-List	Y	72	文字列	シングル	ポート転送リスト名
WebVPN-Port-Forwarding-Name	Y	79	文字列	シングル	名前の文字列（例、「Corporate-Apps」） このテキストでクライアントレス ポータ ページのデフォルト文字列「Application 置き換えられます。
WebVPN-Post-Max-Size	Y	159	整数	シングル	0x7fffffff
WebVPN-Session-Timeout-Alert-Interval	Y	149	整数	シングル	0 ～ 30。0 = ディセーブル。
WebVPN Smart-Card-Removal-Disconnect	Y	225	ブール	シングル	0 = 無効1 = 有効
WebVPN-Smart-Tunnel	Y	136	文字列	シングル	スマート トンネルの名前
WebVPN-Smart-Tunnel-Auto-Sign-On	Y	139	文字列	シングル	ドメイン名が付加されたスマート トンネ インオン リストの名前
WebVPN-Smart-Tunnel-Auto-Start	Y	138	整数	シングル	0 = 無効1 = 有効2 = 自動スタート
WebVPN-Smart-Tunnel-Tunnel-Policy	Y	227	文字列	シングル	「e ネットワーク名」、「i ネットワーク 「a」のいずれか。ここで、ネットワーク マート トンネル ネットワークのリストの す。e はトンネルが除外されることを示 ンネルが指定されることを示し、a はすべ ネルを示します。
WebVPN-SSL-VPN-Client-Enable	Y	103	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Keep- Installation	Y	105	整数	シングル	0 = 無効1 = 有効
WebVPN-SSL-VPN-Client-Required	Y	104	整数	シングル	0 = 無効1 = 有効
WebVPN-SSO-Server-Name	Y	114	文字列	シングル	有効な文字列
WebVPN-Storage-Key	Y	162	文字列	シングル	

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
WebVPN-Storage-Objects	Y	161	文字列	シングル	
WebVPN-SVC-Keepalive-Frequency	Y	107	整数	シングル	15 ～ 600 秒、0=オフ
WebVPN-SVC-Client-DPD-Frequency	Y	108	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-DTLS-Enable	Y	123	整数	シングル	0 = 無効1 = 有効
WebVPN-SVC-DTLS-MTU	Y	125	整数	シングル	MTU 値は 256 ～ 1406 バイトです。
WebVPN-SVC-Gateway-DPD-Frequency	Y	109	整数	シングル	5 ～ 3600 秒、0=オフ
WebVPN-SVC-Rekey-Time	Y	110	整数	シングル	4 ～ 10080 分、0=オフ
WebVPN-SVC-Rekey-Method	Y	111	整数	シングル	0（オフ）、1（SSL）、2（新しいトンネル
WebVPN-SVC-Compression	Y	112	整数	シングル	0（オフ）、1（デフォルトの圧縮）
WebVPN-UNIX-Group-ID (GID)	Y	222	整数	シングル	UNIX での有効なグループ ID
WebVPN-UNIX-User-ID (UIDs)	Y	221	整数	シングル	UNIX での有効なユーザー ID
WebVPN-Upload-Max-Size	Y	158	整数	シングル	0x7fffffff
WebVPN-URL-Entry-Enable	Y	93	整数	シングル	0 = 無効1 = 有効
WebVPN-URL-List	Y	71	文字列	シングル	URL リスト名
WebVPN-User-Storage	Y	160	文字列	シングル	
WebVPN-VDI	Y	163	文字列	シングル	設定のリスト

サポートされる IETF RADIUS 認証属性

次の表に、サポートされる IETF RADIUS 属性の一覧を示します。

表 *49 :* サポートされる *IETF RADIUS* 属性

属性名	ASA	属性番号	構文/タイプ	シングルまたはマルチ値	説明または値
IETF-Radius-Class	Y	25		シングル	バージョン 8.2.x 以降では、Group-Policy 属性（VSA 3076、#25）を使用することをお勧めします。 • グループポリシー名 • OU=グループポリシー名 • OU=グループ ポリシー名
IETF-Radius-Filter-Id	Y	11	文字列	シングル	フル トンネルの IPsec クライアントと SSL VPN クライアントのみに適用される、ASA で定義された ACL 名。
IETF-Radius-Framed-IP-Address	Y	n/a	文字列	シングル	IP アドレス
IETF-Radius-Framed-IP-Netmask	Y	n/a	文字列	シングル	IP アドレス マスク
IETF-Radius-Idle-Timeout	Y	28	整数	シングル	Seconds
IETF-Radius-Service-Type	Y	6	整数	シングル	秒。使用可能なサービス タイプの値： • .Administrative：ユーザーは configure プロンプトへのアクセスを許可されています。 • .NAS-Prompt：ユーザーは exec プロンプトのアクセスを許可されています。 • .remote-access：ユーザーはネットワーク アクセスを許可されています。
IETF-Radius-Session-Timeout	Y	27	整数	シングル	Seconds

RADIUS アカウンティング切断の理由コード

これらのコードは、パケットを送信するときに ASA が切断された場合に返されます。

切断の理由コード
ACCT_DISC_USER_REQ = 1
ACCT_DISC_LOST_CARRIER = 2
ACCT_DISC_LOST_SERVICE = 3

切断の理由コード
ACCT_DISC_IDLE_TIMEOUT = 4
ACCT_DISC_SESS_TIMEOUT = 5
ACCT_DISC_ADMIN_RESET = 6
ACCT_DISC_ADMIN_REBOOT = 7
ACCT_DISC_PORT_ERROR = 8
ACCT_DISC_NAS_ERROR = 9
ACCT_DISC_NAS_REQUEST = 10
ACCT_DISC_NAS_REBOOT = 11
ACCT_DISC_PORT_UNNEEDED = 12
ACCT_DISC_PORT_PREEMPTED = 13
ACCT_DISC_PORT_SUSPENDED = 14
ACCT_DISC_SERV_UNAVAIL = 15
ACCT_DISC_CALLBACK = 16
ACCT_DISC_USER_ERROR = 17
ACCT_DISC_HOST_REQUEST = 18
ACCT_DISC_ADMIN_SHUTDOWN = 19
ACCT_DISC_SA_EXPIRED = 21
ACCT_DISC_MAX_REASONS = 22

AAA の RADIUS サーバーのガイドライン

ここでは、AAA 用の RADIUS サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

- シングルモードで最大 200 個のサーバーグループ、またはマルチモードでコンテキストごとに 4 つのサーバーグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。
- RADIUS ペイロードの最大長は 4,096 バイトです。

AAA 用の RADIUS サーバーの設定

ここでは、AAA 用に RADIUS サーバーを設定する方法について説明します。

手順

ステップ 1 ASA の属性を RADIUS サーバーにロードします。属性をロードするために使用する方法は、使用している RADIUS サーバーのタイプによって異なります。

- Cisco ACS を使用している場合：サーバーには、これらの属性がすでに統合されています。したがって、この手順をスキップできます。
- 他のベンダーの RADIUS サーバー（たとえば Microsoft Internet Authentication Service）の場合：ASA の各属性を手動で定義する必要があります。属性を定義するには、属性名または番号、タイプ、値、ベンダー コード（3076）を使用します。

ステップ 2 RADIUS サーバ グループの設定 （1455 ページ）。

ステップ 3 グループへの RADIUS サーバーの追加 （1459 ページ）。

RADIUS サーバ グループの設定

認証、許可、またはアカウンティングに外部 RADIUS サーバーを使用する場合は、まず AAA プロトコルあたり少なくとも 1 つの RADIUS サーバー グループを作成して、各グループに 1 つ以上のサーバーを追加する必要があります。

手順

ステップ 1 RADIUS AAA サーバー グループを作成します。

aaa-server *group_name* **protocol radius**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

ステップ 2 （任意）次のサーバーを試す前にグループ内の RADIUS サーバーでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

範囲は、1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバーにアクセスしようとします。

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

ステップ 3 （任意）グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

それぞれの説明は次のとおりです。

- **depletion** [**deadtime** *minutes*] は、グループ内のすべてのサーバーが非アクティブになった後でのみ、障害が発生したサーバーを再アクティブ化します。これがデフォルトの再アクティブ化モードです。グループ内の最後のサーバーがディセーブルになってから、その後すべてのサーバーを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定できます。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。
- **timed** 30 秒のダウン時間の後、障害が発生したサーバーを再アクティブ化します。

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

ステップ 4 （任意）グループ内のすべてのサーバーにアカウンティング メッセージを送信します。

accounting-mode simultaneous

アクティブ サーバーだけ送信メッセージをデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

ステップ 5 （任意）RADIUS 中間アカウンティング アップデート メッセージの定期的な生成をイネーブルにします。

interim-accounting-update [**periodic** [*hours*]]

ISE は、ASA などの NAS デバイスから受信するアカウンティング レコードに基づいて、アクティブセッションのディレクトリを保持します。ただし、セッションがアクティブであるという通知（アカウンティング メッセージまたはポスチャ トランザクション）を 5 日間受信しなかった場合、ISE はデータベースからそのセッションのレコードを削除します。存続時間の長い VPN 接続が削除されないようにするには、すべてのアクティブ セッションについて ISE に定期的に中間アカウンティング更新メッセージを送信するように、グループを設定します。

- **periodic**[*hours*] は、対象のサーバー グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 時間です。
- （パラメータなし）。**periodic** キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。

例：

```
hostname(config-aaa-server-group)# interim-accounting-update periodic 12
```

ステップ 6 （任意）AAA サーバー グループの RADIUS の動的認可（ISE 許可変更、CoA）サービスをイネーブルにします。

dynamic-authorization [**port** *number*]

ポートの指定は任意です。デフォルトは 1700 です。指定できる範囲は 1024 ～ 65535 です。

VPN トンネルでサーバー グループを使用すると、対応する RADIUS サーバー グループが CoA 通知用に登録され、ASA は ISE からの CoA ポリシー更新用ポートをリッスンします。このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ動的認可をイネーブルにします。

例：

```
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

ステップ 7 （任意）認証に ISE を使用しない場合は、RADIUS サーバー グループに対し認可専用モードを有効にします。（このサーバー グループを ISE と併せてリモート アクセス VPN で使用する場合にのみ認可専用モードをイネーブルにします）。

authorize-only

これは、サーバー グループを認可に使用するときに、RADIUS アクセス要求メッセージが、AAA サーバー用に設定されているパスワード方式に反して、「認可専用」要求として構築されることを示しています。**radius-common-pw** コマンドを使用して RADIUS サーバーの共通パスワードを設定すると、そのパスワードは無視されます。

たとえば、認証にこのサーバー グループではなく証明書を使用する場合には、認可専用モードを使用します。VPN トンネルでの認可とアカウンティングにこのサーバー グループを使用する可能性があるからです。

例：

```
ciscoasa(config-aaa-server-group)# authorize-only
```

ステップ 8 （任意）ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL を結合します。

merge-dacl {**before-avpair** | **after-avpair**}

例：

```
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

このオプションは、VPN 接続にのみ適用されます。VPN ユーザーの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL と結合されません。AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

before-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの前に配置されるように指定します。

after-avpair オプションは、ダウンロード可能 ACL エントリが Cisco-AV-Pair エントリの後に配置されるように指定します。

例

次に、単一サーバーで 1 つの RADIUS グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthOutbound protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthOutbound (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key RadUauthKey
ciscoasa(config-aaa-server-host)# exit
```

次の例は、ISE サーバ グループに、動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
```

```
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。サーバー グループは認証用に使用されないため、authorize-only コマンドをサーバー グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

グループへの RADIUS サーバーの追加

RADIUS サーバーをグループに追加するには、次の手順を実行します。

手順

ステップ 1 RADIUS サーバーと、そのサーバーが属する AAA サーバー グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

ステップ 2 RADIUS サーバーからダウンロード可能な ACL で受信したネットマスクを ASA が処理する方法を指定します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

例：

```
ciscoasa(config-aaa-server-host)# acl-netmask-convert standard
```

auto-detect キーワードは、使用されているネットマスク表現のタイプの判別を ASA が試みる必要があることを指定します。ASA によってワイルドカード ネットマスク表現が検出された場合は、標準ネットマスク表現に変換されます。

standard キーワードは、RADIUS サーバーから受信したダウンロード可能 ACL には、標準ネットマスク表現のみが含まれていると ASA が見なすように指定します。ワイルドカード ネットマスク表現からの変換は実行されません。

wildcard キーワードは、RADIUS サーバーから受信したダウンロード可能 ACL には、ワイルドカード ネットマスク表現のみが含まれていると ASA が見なし、ACL をダウンロードしたときにそれらすべてを標準ネットマスク表現に変換するように指定します。

ステップ 3 ASA を介して RADIUS 認可サーバーにアクセスするすべてのユーザーが使用する共通パスワードを指定します。

radius-common-pw *string*

例：

```
ciscoasa(config-aaa-server-host)# radius-common-pw examplepassword123abc
```

string 引数は、大文字と小文字が区別される最大 127 文字の英数字キーワードです。RADIUS サーバーとのすべての認可トランザクションで共通パスワードとして使用されます。

ステップ 4 RADIUS サーバーへの MS-CHAPv2 認証要求をイネーブルにします。

mschapv2-capable

例：

```
ciscoasa(config-aaa-server-host)# mschapv2-capable
```

ステップ 5 サーバーへの接続試行のタイムアウト値を指定します。

timeout *seconds*

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the interval defined on the **retry-interval** command）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバー グループ内の max-failed-attempts コマンドで指定された制限に達すると、AAA サーバーは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバーへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 6 前のコマンドで指定した特定の AAA サーバーに対して、再試行間隔を設定します。

retry-interval *seconds*

例：

```
ciscoasa(config-aaa-server-host)# retry-interval 8
```

seconds 引数に要求の再試行間隔（1 ～ 10 秒）を指定します。これは、接続要求を再試行するまでに ASA が待機する時間です。

（注）
RADIUS プロトコルの場合、サーバが ICMP ポートに到達不能メッセージで応答すると、再試行間隔設定は無視され、AAA サーバは直ちに失敗状態に移動します。これが AAA グループ内の唯一のサーバである場合は、そのサーバが再度アクティブになり、別の要求が送信されます。これは意図された動作です。

ステップ 7 グループ内のすべてのサーバーにアカウンティング メッセージを送信します。

accounting-mode simultaneous

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバーにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

ステップ 8 認証ポートをポート番号 1645 に指定するか、またはユーザー認証に使用するサーバー ポートを指定します。

authentication-port *port*

例：

```
ciscoasa(config-aaa-server-host)# authentication-port 1646
```

ステップ 9 アカウンティング ポートをポート番号 1646 に指定するか、またはこのホストのアカウンティングに使用するサーバー ポートを指定します。

accounting-port *port*

例：

```
ciscoasa(config-aaa-server-host)# accounting-port 1646
```

ステップ 10 ASA に対する RADIUS サーバーの認証に使用されるサーバー秘密値を指定します。設定したサーバー秘密キーは、RADIUS サーバーで設定されたサーバー秘密キーと一致する必要があります。サーバー秘密キーの値が不明の場合は、RADIUS サーバーの管理者に問い合わせてください。最大長は、64 文字です。

key

例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

設定したサーバー秘密キーは、RADIUS サーバーで設定されたサーバー秘密キーと一致する必要があります。サーバー秘密キーの値が不明の場合は、RADIUS サーバーの管理者に問い合わせてください。最大長は、64 文字です。

ステップ 11 Message-Authenticator 属性が RADIUS 要求および応答内に存在する必要があることを指定します。

message-authenticator-required

Message-Authenticator 属性は、Blast- RADIUS 攻撃を防ぐために使用されます。メッセージ オーセンティケータをサポートするように RADIUS サーバーをアップグレードした場合は、このオプションを有効にして、Blast- RADIUS 攻撃を防御できます。有効にする場合、すべての要求と応答にメッセージ オーセンティケータが含まれている必要があります。含まれていない場合、認証は失敗します。

例：

```
ciscoasa(config-aaa-host)# message-authenticator-required
```

例

次に、既存の RADIUS サーバー グループに RADIUS サーバーを追加する例を示します。

```
ciscoasa(config)# aaa-server svrgrp1 protocol radius
ciscoasa(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
ciscoasa(config-aaa-server-host)# acl-netmask-convert wildcard
ciscoasa(config-aaa-server-host)# radius-common-pw myexaplepasswordabc123
ciscoasa(config-aaa-server-host)# mschapv2-capable
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry-interval 7
ciscoasa(config-aaa-server-host)# accounting-mode simultaneous
ciscoasa(config-aaa-server-host)# authentication-port 1650
ciscoasa(config-aaa-server-host)# authorization-port 1645
ciscoasa(config-aaa-server-host)# key mysecretkeyexampleiceage2
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

AAA 用の RADIUS サーバーのモニタリング

AAA 用の RADIUS サーバーのステータスのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定されたRADIUSサーバーの統計情報を表示します。**clear aaa-server statistics** コマンドを使用して、カウンタをゼロにリセットできます。

- **show running-config aaa-server**

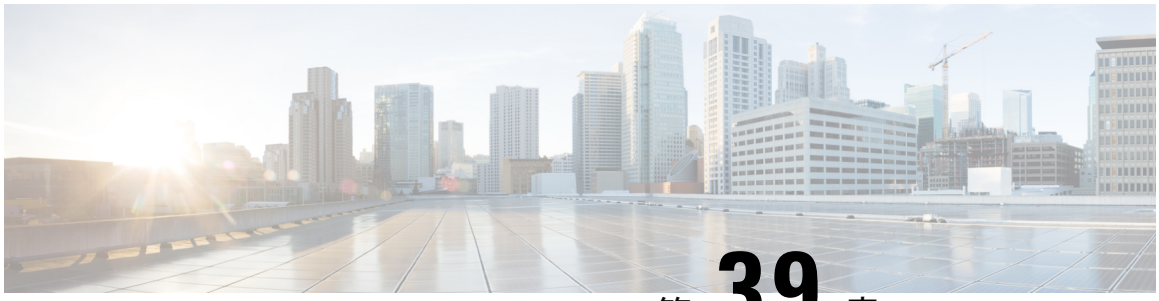
  このコマンドは、RADIUS サーバーの実行コンフィギュレーションを表示します。

AAA 用の RADIUS サーバーの履歴

表 *50 : AAA* 用の *RADIUS* サーバーの履歴

機能名	プラットフォーム リリース	説明
AAA の RADIUS サーバー	7.0(1)	AAA 用の RADIUS サーバーを設定する方法について説明します。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**show aaa-server**、**show running-config aaa-server**、**clear aaa-server statistics**、**authentication-port**、**accounting-port**、**retry-interval**、**acl-netmask-convert**、**clear configure aaa-server**、**merge-dacl**、**radius-common-pw**、**key**。
ASA からの RADIUS アクセス要求パケットおよびアカウンティング要求パケットでの主なベンダー固有属性（VSA）の送信	8.4(3)	4 つの新しい VSA：Tunnel Group Name（146）および Client Type（150）は、ASA からの RADIUS アクセス要求パケットで送信されます。Session Type（151）および Session Subtype（152）は、ASA からの RADIUS アカウンティング要求パケットで送信されます。4 つのすべての属性が、すべてのアカウンティング要求パケット タイプ（開始、中間アップデート、および終了）に送信されます。RADIUS サーバー（ACS や ISE など）は、認可属性やポリシー属性を強制適用したり、アカウンティングや課金のためにそれらの属性を使用したりできます。

機能名	プラットフォーム リリース	説明
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングル コンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに8台のサーバーを設定できます（以前の制限はグループごとに4台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host**
RADIUS Message-Authenticator 属性のサポート。	9.23(1)	Message-Authenticator 属性は、Blast- RADIUS 攻撃を防ぐために使用されます。メッセージ オーセンティケータをサポートするように RADIUS サーバーをアップグレードした場合は、このオプションを有効にして、Blast- RADIUS 攻撃を防御できます。有効にする場合、すべての要求と応答にメッセージ オーセンティケータが含まれている必要があります。含まれていない場合、認証は失敗します。 **message-authenticator-required** コマンドが追加されました。



第 39 章

AAA 用の TACACS+ サーバー

この章では、AAA で使われる TACACS+ サーバーの設定方法について説明します。

- AAA 用の TACACS+ サーバーについて （1465 ページ）
- AAA 用の TACACS+ サーバーのガイドライン （1467 ページ）
- TACACS+ サーバーの設定 （1467 ページ）
- AAA 用の TACACS+ サーバーのモニタリング （1471 ページ）
- AAA 用の TACACS+ サーバーの履歴 （1471 ページ）

AAA 用の TACACS+ サーバーについて

ASA は、ASCII、PAP、CHAP、MS-CHAPv1 の各プロトコルで TACACS+ サーバー認証をサポートします。

TACACS+ 属性

ASA は、TACACS+ 属性をサポートします。TACACS+ 属性は、認証、許可、アカウンティングの機能を分離します。プロトコルでは、必須とオプションの 2 種類の属性をサポートします。サーバーとクライアントの両方で必須属性を解釈できる必要があり、また、必須属性はユーザーに適用する必要があります。オプションの属性は、解釈または使用できることも、できないこともあります。

（注） TACACS+ 属性を使用するには、NAS 上で AAA サービスがイネーブルになっていることを確認してください。

次の表に、カットスループロキシ接続に対してサポートされる TACACS+ 許可応答属性の一覧を示します。

表 *51 :* サポートされる *TACACS+* 許可応答属性

属性	説明
acl	接続に適用する、ローカルで設定済みの ACL を識別します。
idletime	認証済みユーザー セッションが終了する前に許可される非アクティブ時間（分）を示します。
timeout	認証済みユーザーセッションが終了する前に認証クレデンシャルがアクティブな状態でいる絶対時間（分）を指定します。

次の表に、サポートされる TACACS+ アカウンティング属性の一覧を示します。

。

表 *52 :* サポートされる *TACACS+* アカウンティング属性

属性	説明
bytes_in	この接続中に転送される入力バイト数を指定します（ストップ レコードのみ）。
bytes_out	この接続中に転送される出力バイト数を指定します（ストップ レコードのみ）。
cmd	実行するコマンドを定義します（コマンド アカウンティングのみ）。
disc-cause	切断理由を特定する数字コードを示します（ストップ レコードのみ）。
elapsed_time	接続の経過時間（秒）を定義します（ストップ レコードのみ）。
foreign_ip	トンネル接続のクライアントの IP アドレスを指定します。最下位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
local_ip	トンネル接続したクライアントの IP アドレスを指定します。最上位のセキュリティ インターフェイスでカットスルー プロキシ接続のアドレスを定義します。
NAS port	接続のセッション ID が含まれます。
packs_in	この接続中に転送される入力パケット数を指定します。
packs_out	この接続中に転送される出力パケット数を指定します。
priv-level	コマンド アカウンティング要求の場合はユーザーの権限レベル、それ以外の場合は 1 に設定されます。
rem_iddr	クライアントの IP アドレスを示します。

属性	説明
service	使用するサービスを指定します。コマンド アカウンティングの場合にのみ、常に「shell」に設定されます。
task_id	アカウンティング トランザクションに固有のタスク ID を指定します。
username	ユーザーの名前を示します。

AAA 用の TACACS+ サーバーのガイドライン

ここでは、AAA 用の TACACS+ サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバーは、IPv4 または IPv6 アドレスを使用できます。

その他のガイドライン

- シングルモードで最大200個のサーバーグループ、またはマルチモードでコンテキストごとに 4 つのサーバーグループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。
- ASA アプライアンスモードで実行されている FPR1000、FPR2100、または FPR3100 シリーズの場合は、次のユーザー名規則に従う必要があります。
  - Linux に対して有効である必要があります。
  - 小文字のみを使用してください。
  - 英数字、ピリオド（.）、ハイフン（-）を含めることができます。
  - アット マーク（@）やスラッシュ（/）など、その他の特殊文字を含めることはできません。

TACACS+ サーバーの設定

ここでは、TACACS+ サーバーを設定する方法について説明します。

手順

ステップ 1 TACACS+ サーバー グループの設定 （1468 ページ）。
ステップ 2 グループへの TACACS+ サーバーの追加 （1470 ページ）。

TACACS+ サーバー グループの設定

認証、許可、アカウンティングに TACACS+ サーバーを使用する場合は、まず TACACS+ サーバー グループを少なくとも 1 つ作成し、各グループに 1 台以上のサーバーを追加する必要があります。TACACS+ サーバー グループは名前で識別されます。

TACACS+ サーバー グループを追加するには、次の手順を実行します。

手順

ステップ 1 サーバー グループ名とプロトコルを指定します。

aaa-server *server_tag* **protocol tacacs+**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol tacacs+
```

aaa-server protocol コマンドを入力すると、aaa-server グループ コンフィギュレーション モードが開始します。

ステップ 2 次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASAは引き続きグループ内のサーバーにアクセスしようとします。

ステップ 3 グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバーが非アクティブになって初めて、障害の発生したサーバーが再度アクティブ化されます。

deadtime *minutes* キーワードと引数のペアは、グループ内の最後のサーバーをディセーブルにしてから次にすべてのサーバーを再度イネーブルにするまでの経過時間を、0～1440分の範囲で指定します。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。

timed キーワードを指定すると、30秒のダウン時間の後、障害が発生したサーバーが再度アクティブ化されます。

ステップ 4 グループ内のすべてのサーバーにアカウンティング メッセージを送信します。

accounting-mode simultaneous

例：

```
ciscoasa(config-aaa-server-group)# accounting-mode simultaneous
```

アクティブ サーバーにのみメッセージを送信するデフォルトに戻すには、**accounting-mode single** コマンドを入力します。

例

次の例では、1 台のプライマリ サーバーと 1 台のバックアップ サーバーで構成された 1 つの TACACS+ グループを追加する例を示します。

```
ciscoasa(config)# aaa-server AuthInbound protocol tacacs+
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.1
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# aaa-server AuthInbound (inside) host 10.1.1.2
ciscoasa(config-aaa-server-host)# key TACPlusUauthKey2
ciscoasa(config-aaa-server-host)# exit
```

グループへの TACACS+ サーバーの追加

TACACS+ サーバーをグループに追加するには、次の手順を実行します。

手順

ステップ 1 TACACS+ サーバーと、そのサーバーが属するサーバー グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

サーバーは、IPv4 アドレスか IPv6 アドレスのどちらかを使用できます。

ステップ 2 サーバーへの接続試行のタイムアウト値を指定します。

timeout *seconds*

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the interval defined on the **retry-interval** command）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の max-failed-attempts コマンドで指定された制限に達すると、AAA サーバーは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバーへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 3 ポート番号 49、または ASA によって TACACS+ サーバーとの通信に使用される TCP ポート番号を指定します。

server-port *port_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 49
```

ステップ 4 TACACS+ サーバに対する NAS の認証に使用されるサーバ秘密値を指定します。

key

例：

```
ciscoasa(config-aaa-host)# key myexamplekey1
```

この値は大文字と小文字が区別される、最大127文字の英数字から成るキーワードで、TACACS+サーバー上のキーと同じ値です。127 を超える文字は無視されます。このキーはクライアントとサーバー間でデータを暗号化するために使われ、クライアントとサーバー両方のシステムで同じである必要があります。このキーにスペースを含めることはできませんが、他の特殊文字は使用できます。

AAA 用の TACACS+ サーバーのモニタリング

AAA 用の TACACS+ サーバーのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定された TACACS+ サーバーの統計情報を表示します。TACACS+ サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを入力します。

- **show running-config aaa-server**

  このコマンドは、TACACS+ サーバーの実行コンフィギュレーションを表示します。TACACS+ サーバー コンフィギュレーションをクリアするには、**clear configure aaa-server** コマンドを入力します。

AAA 用の TACACS+ サーバーの履歴

表 *53 : AAA* 用の *TACACS+* サーバーの履歴

機能名	プラットフォーム リリース	説明
TACACS+ サーバ	7.0(1)	AAA に TACACS+ サーバーを設定する方法について説明します。 次のコマンドを導入しました。 **aaa-server protocol**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**aaa authorization exec authentication-server**、**server-port**、**key**、**clear aaa-server statistics**、**clear configure aaa-server**、**show aaa-server**、**show running-config aaa-server**、**username**、**service-type**、**timeout**.
AAA 向けの IPv6 アドレス TACACS+ サーバー	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。

機能名	プラットフォーム リリース	説明
グループごとのAAAサーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200個のAAAサーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに4台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host**

第 40 章

AAA の LDAP サーバー

この章では、AAA で使用される LDAP サーバーの設定方法について説明します。

- LDAP および ASA について （1473 ページ）
- AAA の LDAP サーバーのガイドライン （1477 ページ）
- AAA の LDAP サーバーの設定 （1478 ページ）
- AAA の LDAP サーバーのモニタリング （1484 ページ）
- AAA の LDAP サーバーの履歴 （1485 ページ）

LDAP および ASA について

ASA はほとんどの LDAPv3 ディレクトリサーバーと互換性があり、それには次のものが含まれます。

- Sun Microsystems JAVA System Directory Server（現在は Oracle Directory Server Enterprise Edition の一部、旧名 Sun ONE Directory Server）
- Microsoft Active Directory
- Novell
- OpenLDAP

デフォルトでは、ASA によって Microsoft Active Directory、Sun LDAP、Novell、OpenLDAP、または汎用 LDAPv3 ディレクトリ サーバーに接続しているかどうかが自動検出されます。ただし、LDAP サーバー タイプの自動検出による決定が失敗した場合は、手動で設定できます。

LDAP での認証方法

認証中、ASA は、ユーザーの LDAP サーバーへのクライアント プロキシとして機能し、プレーン テキストまたは Simple Authentication and Security Layer（SASL）プロトコルのいずれかを使って LDAP サーバーに対する認証を行います。デフォルトで、ASA は、通常はユーザー名とパスワードである認証パラメータを LDAP サーバーにプレーン テキストで渡します。

ASA は、Digest-MD5 SASL メカニズムのみをサポートします。このメカニズムを使用して、ASA は、ユーザー名とパスワードから計算した MD5 値を使用して LDAP サーバーに応答します。

ユーザー LDAP 認証が成功すると、LDAP サーバーは認証されたユーザーの属性を返します。VPN 認証の場合、通常これらの属性には、VPN セッションに適用される認可データが含まれます。この場合、LDAP の使用により、認証と許可を 1 ステップで実行できます。

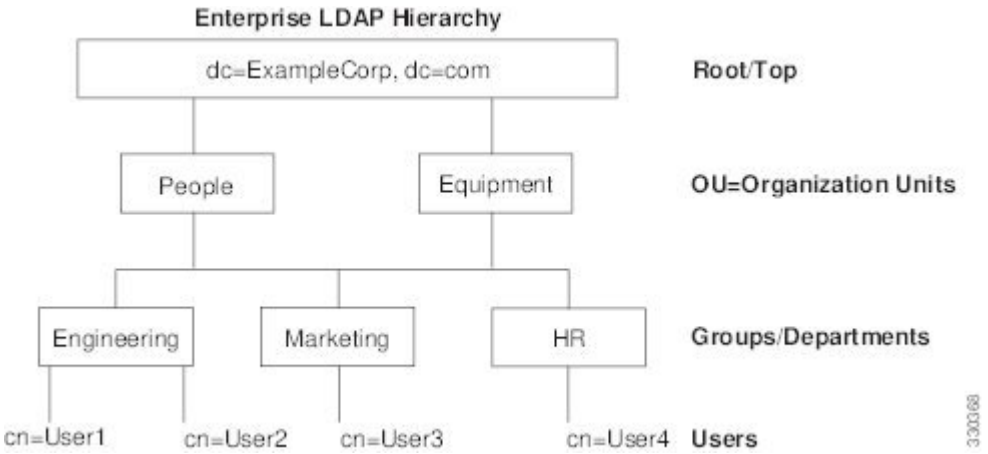
（注） LDAP プロトコルの詳細については、RFC 1777、2251、および 2849 を参照してください。

LDAP 階層

LDAP コンフィギュレーションは、組織の論理階層が反映されたものにする必要があります。たとえば、Example Corporation という企業の従業員 Employee1 を例に考えてみます。Employee1 は Engineering グループに従事しています。この企業の LDAP 階層は 1 つ以上のレベルを持つことができます。たとえば、シングルレベル階層をセットアップします。この中で、Employee1 は Example Corporation のメンバーであると見なされます。あるいは、マルチレベル階層をセットアップします。この中で、Employee1 は Engineering 部門のメンバーであると見なされ、この部門は People という名称の組織ユニットのメンバーであり、この組織ユニットは Example Corporation のメンバーです。マルチレベル階層の例については、次の図を参照してください。

マルチレベル階層の方が詳細ですが、検索結果が速く返されるのはシングルレベル階層の方です。

図 *85 :* マルチレベルの *LDAP* 階層



LDAP 階層の検索

ASA は、LDAP 階層内での検索を調整できます。ASA に次の 3 種類のフィールドを設定すると、LDAP 階層での検索開始場所とその範囲、および検索する情報のタイプを定義できます。これらのフィールドは、ユーザーの権限が含まれている部分だけを検索するように階層の検索を限定します。

- LDAP Base DN では、サーバーが ASA から認可要求を受信したときに LDAP 階層内のどの場所からユーザー情報の検索を開始するかを定義します。
- Search Scope では、LDAP 階層の検索範囲を定義します。この指定では、LDAP Base DN よりもかなり下位のレベルまで検索します。サーバーによる検索を直下の 1 レベルだけにするか、サブツリー全体を検索するかを選択できます。シングルレベルの検索の方が高速ですが、サブツリー検索の方が広範囲に検索できます。
- Naming Attribute では、LDAP サーバーのエントリを一意に識別する RDN を定義します。一般的な名前属性には、cn（一般名）、sAMAccountName、および userPrincipalName を含めることができます。

次の図に、Example Corporation の LDAP 階層の例を示します。この階層が指定されると、複数の方法で検索を定義できます。次の表に、2つの検索コンフィギュレーションの例を示します。

最初のコンフィギュレーションの例では、Employee1 が IPSec トンネルを確立するときに LDAP 認可が必要であるため、ASA から LDAP サーバーに検索要求が送信され、この中で Employee1 を Engineering グループの中で検索することが指定されます。この検索は短時間でできます。

2 番目のコンフィギュレーションの例では、ASA から送信される検索要求の中で、Employee1 を Example Corporation 全体の中で検索することが指定されています。この検索には時間がかかります。

表 *54 :* 検索コンフィギュレーションの例

番号	LDAP Base DN	検索範囲	名前属性	結果
1	group= Engineering,ou=People,dc=ExampleCorporation, dc=com	1 レベル	cn=Employee1	検索が高速
2	dc=ExampleCorporation,dc=com	サブツリー	cn=Employee1	検索に時間がかかる

LDAP サーバーへのバインド

ASA は、ログイン DN とログイン パスワードを使用して、LDAP サーバーとの信頼（バインド）を築きます。Microsoft Active Directory の読み取り専用操作（認証、許可、グループ検索など）を行うとき、ASA では特権の低いログイン DN でバインドできます。たとえば、Login DN には、AD の「Member Of」の指定が Domain Users の一部であるユーザを指定することができます。VPN のパスワード管理操作では、Login DN にはより高い特権が必要となり、AD の Account Operators グループの一部を指定する必要があります。

次に、Login DN の例を示します。

```
cn=Binduser1,ou=Admins,ou=Users,dc=company_A,dc=com
```

ASA は次の認証方式をサポートしています。

- 暗号化されていないパスワードを使用したポート 389 での簡易 LDAP 認証
- ポート 636 でのセキュアな LDAP（LDAP-S）
- Simple Authentication and Security Layer（SASL）MD5

ASA は匿名認証をサポートしていません。

（注） LDAP クライアントとしての ASA は、匿名のバインドや要求の送信をサポートしていません。

LDAP 属性マップ

ASA では、次の目的での認証のために LDAP ディレクトリを使用できます。

- VPN リモート アクセス ユーザー
- ファイアウォール ネットワークのアクセス/カットスルー プロキシ セッション
- ACL、ブックマーク リスト、DNS または WINS 設定、セッション タイマーなどのポリシーの権限（または許可属性と呼ばれる）の設定
- ローカル グループ ポリシーのキー属性の設定

ASA は、LDAP 属性マップを使用して、ネイティブ LDAP ユーザー属性を ASA 属性に変換します。それらの属性マップを LDAP サーバーにバインドしたり、削除したりすることができます。また、属性マップを表示または消去することもできます。

LDAP 属性マップは複数値属性をサポートしません。たとえば、あるユーザーが複数の AD グループのメンバで、LDAP 属性マップが複数のグループと一致する場合、選択される値は一致するエントリのアルファベット順に基づくものです。

属性マッピング機能を適切に使用するには、LDAP 属性の名前と値およびユーザー定義の属性の名前と値を理解する必要があります。

頻繁にマッピングされる LDAP 属性の名前と、一般にマッピングされるユーザー定義の属性のタイプは次のとおりです。

- IETF-Radius-Class（ASA バージョン 8.2 以降における Group_Policy）：ディレクトリ部門またはユーザー グループ（たとえば、Microsoft Active Directory memberOf）属性値に基づいてグループ ポリシーを設定します。ASDM バージョン 6.2/ASA バージョン 8.2 以降では、IETF-Radius-Class 属性の代わりに group-policy 属性が使用されます。
- IETF-Radius-Filter-Id：VPN クライアント、IPSec、SSL に対するアクセス コントロール リスト（ACL）に適用されます。
- IETF-Radius-Framed-IP-Address：VPN リモート アクセス クライアント、IPSec、および SSL にスタティック IP アドレスを割り当てます。
- Banner1：VPN リモート アクセス ユーザーのログイン時にテキスト バナーを表示します。

- Tunneling-Protocols：アクセス タイプに基づいて、VPN リモート アクセス セッションを許可または拒否します。

（注） 1 つの LDAP 属性マップに、1 つ以上の属性を含めることができます。特定の LADP サーバーからは、1 つの LDAP 属性のみをマップすることができます。

AAA の LDAP サーバーのガイドライン

この項では、AAA の LDAP サーバーを設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

IPv6

AAA サーバーは、IPv4 または IPv6 アドレスを使用できます。

その他のガイドライン

- Sun ディレクトリ サーバーにアクセスするために ASA に設定されている DN が、サーバーのデフォルト パスワード ポリシーにアクセスできる必要があります。DN として、ディレクトリ管理者、またはディレクトリ管理者権限を持つユーザーを使用することを推奨します。または、デフォルト パスワード ポリシーに ACL を設定できます。
- Microsoft Active Directory および Sun サーバーでのパスワード管理をイネーブルにするために LDAP over SSL を設定する必要があります。
- ASA は、Novell、OpenLDAP およびその他の LDAPv3 ディレクトリ サーバーによるパスワード管理をサポートしません。
- バージョン 7.1（x）以降、ASA はネイティブ LDAP スキーマを使用して認証および認可を行うため、Cisco スキーマは必要なくなりました。
- シングル モードで最大 200 個のサーバー グループ、またはマルチ モードでコンテキストごとに 4 つのサーバー グループを持つことができます。
- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。
- ユーザーがログインすると、コンフィギュレーション内で指定されている最初のサーバーから順に、サーバーが応答するまで LDAP サーバーが 1 つずつアクセスされます。グループ内のすべてのサーバーが使用できない場合、ASA は、ローカル データベースがフォールバック方式として設定されていると、ローカルデータベースに接続しようとします（管理認証および認可限定）。フォールバック メソッドとして設定されていない場合、ASA は LDAP サーバーに引き続きアクセスしようとします。

AAA の LDAP サーバーの設定

この項では、AAA に LDAP サーバーを設定する方法について説明します。

手順

ステップ 1 LDAP 属性マップを設定します。LDAP 属性マップの設定 （1478 ページ）を参照してください。

ステップ 2 LDAP サーバー グループを追加します。LDAP サーバー グループの設定 （1480 ページ）を参照してください。

ステップ 3 （オプション）認証メカニズムとは別の異なる、LDAP サーバーからの許可を設定します。「VPN の LDAP 認証の設定 （1483 ページ）」を参照してください。

LDAP 属性マップの設定

LDAP 属性マップを設定するには、次の手順を実行します。

手順

ステップ 1 空の LDAP 属性マップ テーブルを作成します。

ldap-attribute-map *map-name*

例：

```
ciscoasa(config)# ldap-attribute-map att_map_1
```

ステップ 2 ユーザー定義の属性名 department を、シスコの属性にマッピングします。

map-name *user-attribute-name Cisco-attribute-name*

例：

```
ciscoasa(config-ldap-attribute-map)# map-name department IETF-Radius-Class
```

ステップ 3 ユーザー定義のマップ値である department をユーザー定義の属性値とシスコの属性値にマッピングします。

map-value *user-attribute-name Cisco-attribute-name*

例：

```
ciscoasa(config-ldap-attribute-map)# map-value department Engineering group1
```

ステップ 4 サーバーと、そのサーバーが属する AAA サーバー グループを識別します。

aaa-server *server_group* [*interface_name*] **host** *server_ip*

例：

```
ciscoasa(config)# aaa-server ldap_dir_1 host 10.1.1.4
```

ステップ 5 属性マップを LDAP サーバーにバインドします。

ldap-attribute-map *map-name*

例：

```
ciscoasa(config-aaa-server-host)# ldap-attribute-map att_map_1
```

例

次の例は、accessType という名前のLDAP 属性に基づいて管理セッションを ASA に制限する方法を示しています。accessType 属性には、以下の値のいずれかが含まれる可能性があります。

- [VPN]
- admin
- helpdesk

次の例では、各値が、ASA でサポートされる有効な IETF-Radius-Service-Type 属性のいずれかにマッピングされる方法を示します。有効なタイプには、remote-access（Service-Type 5）発信、admin（Service-Type 6）管理、および nas-prompt（Service-Type 7）NAS プロンプトがあります。

```
ciscoasa(config)# ldap attribute-map MGMT
ciscoasa(config-ldap-attribute-map)# map-name accessType IETF-Radius-Service-Type
ciscoasa(config-ldap-attribute-map)# map-value accessType VPN 5
ciscoasa(config-ldap-attribute-map)# map-value accessType admin 6
ciscoasa(config-ldap-attribute-map)# map-value accessType helpdesk 7

ciscoasa(config-ldap-attribute-map)# aaa-server LDAP protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server LDAP (inside) host 10.1.254.91
ciscoasa(config-aaa-server-host)# ldap-base-dn CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)# ldap-login-password test
ciscoasa(config-aaa-server-host)# ldap-login-dn CN=Administrator,CN=Users,DC=cisco,DC=local
ciscoasa(config-aaa-server-host)# server-type auto-detect
ciscoasa(config-aaa-server-host)# ldap-attribute-map MGMT
```

次の例では、シスコの LDAP 属性名の全リストを表示します。

```
ciscoasa(config)# ldap attribute-map att_map_1
```

```
ciscoasa(config-ldap-attribute-map)# map-name att_map_1?

ldap mode commands/options:
cisco-attribute-names:
  Access-Hours
  Allow-Network-Extension-Mode
  Auth-Service-Type
  Authenticated-User-Idle-Timeout
  Authorization-Required
  Authorization-Type
 :
 :
  X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

LDAP サーバー グループの設定

LDAP サーバー グループを作成して設定し、LDAP サーバーをそのグループに追加するには、次の手順を実行します。

始める前に

LDAP サーバーを LDAP サーバー グループに追加する前に、属性マップを追加する必要があります。

手順

ステップ 1 サーバー グループ名とプロトコルを指定します。

aaa-server *server_tag* **protocol ldap**

例：

```
ciscoasa(config)# aaa-server servergroup1 protocol ldap
ciscoasa(config-aaa-server-group)#
```

aaa-server protocol コマンドを入力する場合は、コンフィギュレーション モードを開始します。

ステップ 2 次のサーバーを試す前にグループ内の LDAP サーバーでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASA は引き続きグループ内のサーバーにアクセスしようとします。

ステップ 3 グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバーが非アクティブになった後に、障害の発生したサーバーが再度アクティブ化されます。

deadtime *minutes* キーワード引数のペアには、グループ内の最後のサーバーをディセーブルにしてから、次にすべてのサーバーを再度イネーブルにするまでの経過時間を分単位で 0 ～ 1440 から指定します。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。

timed キーワードは、30 秒間のダウンタイムの後に障害が発生したサーバーを再度アクティブ化します。

ステップ 4 LDAP サーバーと、そのサーバーが属する AAA サーバー グループを識別します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config)# aaa-server servergroup1 outside host 10.10.1.1
```

(*interface_name***)** を指定していない場合、ASA はデフォルトで**内部**インターフェイスを使用します。

aaa-server host コマンドを入力すると、aaa-server ホスト コンフィギュレーション モードが開始します。必要に応じて、ホスト コンフィギュレーション モード コマンドを使用して、さらに AAA サーバーを設定します。

LDAP サーバーで使用できるコマンドと、新しい LDAP サーバー定義にそのコマンドのデフォルト値があるかどうかを、次の表に示します。デフォルト値が指定されていない場合（「—」で表示）、コマンドを使用して値を指定します。

表 *55 :* ホスト モード コマンドとデフォルト値

コマンド	デフォルト値	説明
ldap-attribute-map	—	—
ldap-base-dn	—	—
ldap-login-dn	—	—
ldap-login-password	—	—
ldap-naming-attribute	—	—
ldap-over-ssl	636	設定されていない場合は、ASA では LDAP 要求に sAMAccountName を使用します。SASL とプレーンテキストのどちらを使用する場合でも、ASA と LDAP サーバーの間での通信のセキュリティは SSL で確保されます。SASL を設定しない場合、SSL で LDAP 通信を保護することを強くお勧めします。 **reference-identity** サブモードコマンドを使用して、ASA が LDAPS（SSL）サーバー ID を検証するために使用する参照 ID 名を設定できます。設定すると、ASA は **crypto ca reference-identity** <*name*> で設定された一致基準を使用して aaa-ldap サーバーを検証します。証明書のサブジェクト名または SAN に一致するものが見つからない場合、または reference-identity で指定されたホストが解決されない場合、接続は終了します。
ldap-scope	—	—
sasl-mechanism	—	—
server-port	389	—
server-type	自動検出	自動検出により LDAP サーバのタイプが特定できなくても、そのサーバが、Microsoft Active Directory、Sun LDAP ディレクトリ サーバ、それ以外の LDAP サーバのいずれであるかがわかっている場合は、そのサーバ タイプを手動で設定できます。
ssl-client-certificate	—	ASA がクライアント証明書として LDAP サーバーに提示する証明書。この証明書は、クライアント証明書を LDAP サーバーで検証するように設定する場合に必要です。また、**ldap-over-ssl** を有効にする必要があります。証明書を設定しないと、ASA は LDAP サーバーから要求されたときに証明書を提示しません。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。
timeout	10 秒	—

例

次の例では、watchdogs という名前の LDAP サーバー グループを設定し、そのグループに LDAP サーバーを追加する方法を示します。この例では、この例ではリトライ インターバルや LDAP サーバーがリスンするポートを定義しないため、ASA はこの 2 つのサーバー固有パラメータにデフォルト値を使用します。

```
ciscoasa(config)# aaa-server watchdogs protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

VPN の LDAP 認証の設定

VPN アクセスのための LDAP ユーザー認証が成功すると、ASA は、LDAP 属性を返す LDAP サーバーのクエリーを実行します。通常これらの属性には、VPN セッションに適用される認可データが含まれます。このように LDAP を使用すると、1 つのステップで認証および認可を完了できます。

ただし、場合によっては、認可メカニズムとは別の異なる認可を LDAP ディレクトリ サーバーから取得する必要があります。たとえば、認証に SDI または証明書サーバーを使用している場合、認可情報は返されません。この場合、ユーザー認可では、認証の成功後に LDAP ディレクトリのクエリーを実行するため、認証と認可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザー許可を設定するには、次の手順を実行します。

手順

ステップ 1 remotegrp という名前の IPsec リモート アクセス トンネル グループを作成します。

tunnel-group *groupname*

例：

```
ciscoasa(config)# tunnel-group remotegrp
```

ステップ 2 サーバー グループとトンネル グループを関連付けます。

tunnel-group *groupname* **general-attributes**

例：

```
ciscoasa(config)# tunnel-group remotegrp general-attributes
```

ステップ 3 以前作成した認証のための AAA サーバー グループに新しいトンネル グループを割り当てます。

authorization-server-group *group-tag*

例：

```
ciscoasa(config-general)# authorization-server-group ldap_dir_1
```

例

特定の要件で使用できる許可関連のコマンドとオプションは他にもありますが、次の例では、LDAP でのユーザー許可をイネーブルにするコマンドを示します。この例では、remote-1 という名前の IPsec リモート アクセス トンネル グループを作成し、すでに作成してある許可用の ldap_dir_1 AAA サーバー グループにその新しいトンネル グループを割り当てています。

```
ciscoasa(config)# tunnel-group remote-1 type ipsec-ra
ciscoasa(config)# tunnel-group remote-1 general-attributes
ciscoasa(config-general)# authorization-server-group ldap_dir_1
ciscoasa(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ検索の開始点、ディレクトリ検索の範囲など、追加の LDAP 許可パラメータを設定できます。

```
ciscoasa(config)# aaa-server ldap_dir_1 protocol ldap
ciscoasa(config-aaa-server-group)# aaa-server ldap_dir_1 host 10.1.1.4
ciscoasa(config-aaa-server-host)# ldap-login-dn obscurepassword
ciscoasa(config-aaa-server-host)# ldap-base-dn starthere
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa(config-aaa-server-host)#
```

AAA の LDAP サーバーのモニタリング

AAA の LDAP サーバーのモニタリングについては、次のコマンドを参照してください。

- **show aaa-server**

  このコマンドは、設定された AAA サーバーの統計情報を表示します。AAA サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを使用します。

- **show running-config aaa-server**

  このコマンドは、AAA サーバーの実行コンフィギュレーションを表示します。AAA サーバー コンフィギュレーションをクリアするには、**clear configure aaa-server** コマンドを使用します。

AAA の LDAP サーバーの履歴

表 *56 : AAA* サーバーの履歴

機能名	プラットフォーム リリース	説明
AAA の LDAP サーバー	7.0(1)	LDAP サーバーの AAA のサポートと LDAP サーバーの設定方法について説明します。 次のコマンドを導入しました。 **username**、**aaa authorization exec authentication-server**、**aaa authentication console LOCAL**、**aaa authorization exec LOCAL**、**service-type**、**ldap attribute-map**、**aaa-server protocol**、**aaa authentication telnet | ssh | serial**} **console LOCAL**、**aaa authentication http console LOCAL**、**aaa authentication enable console LOCAL**、**max-failed-attempts**、**reactivation-mode**、**accounting-mode simultaneous**、**aaa-server host**、**authorization-server-group**、**tunnel-group**、**tunnel-group general-attributes**、**map-name**、**map-value**、**ldap-attribute-map**。
AAA 向けの IPv6 アドレス LDAP サーバー	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバー グループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host**

機能名	プラットフォーム リリース	説明
相互l LDAPS 認証。	9.18(1)	ASA が認証のために証明書を要求したときに LDAP サーバーに提示するように ASA のクライアント証明書を設定できます。この機能は、LDAP over SSL を使用する場合に適用されます。LDAP サーバーがピア証明書を要求するように設定されている場合、セキュア LDAP セッションが完了せず、認証/許可要求が失敗します。 **ssl-client-certificate** コマンドが追加されました。

第 41 章

AAA の RSA SecurID サーバー

ここでは、AAA で使用する RSA SecurID サーバーの設定方法について説明します。RSA SecureID サーバーは、通信に SDI プロトコルを使用することから、SDI サーバーとも呼ばれます。管理接続、ネットワークアクセス、および VPN ユーザーアクセスの認証に RSA SecurID サーバーを使用できます。

- RSA SecurID サーバーについて （1487 ページ）
- AAA の RSA SecurID サーバーのガイドライン （1487 ページ）
- AAA の RSA SecurID サーバーの設定 （1488 ページ）
- AAA の RSA SecurID サーバーのモニタリング （1491 ページ）
- AAA の RSA SecurID サーバーの履歴 （1492 ページ）

RSA SecurID サーバーについて

RSA SecurID サーバは、認証に直接使用することも、認証の第 2 要素として間接的に使用することもできます。後者の場合は、SecurID サーバーと RADIUS サーバーの間で SecurID サーバーとの関係を設定し、RADIUS サーバーを使用するように ASA を設定します。

一方、SecurID サーバーに対して直接認証する場合は、SDI プロトコルの AAA サーバーグループを作成します。これは、それらのサーバーとの通信に使用されるプロトコルです。

SDI を使用する場合は、AAA サーバーグループを作成するときにプライマリ SecurID サーバーを指定するだけで済みます。ASA からサーバーに最初に接続したときに、すべての SecurID サーバーのレプリカをリストした sdiconf.rec ファイルを取得します。以降にプライマリサーバが応答しない場合、それらのレプリカが認証に使用されます。

さらに、ASA を認証エージェントとして RSA Authentication Manager に登録する必要があります。ASA を登録していないと認証の試行は失敗します。

AAA の RSA SecurID サーバーのガイドライン

- シングルモードで最大 200 個のサーバーグループ、またはマルチモードでコンテキストごとに 8 つのサーバーグループを持つことができます。

- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。ユーザーがログインすると、コンフィギュレーション内で指定されている最初のサーバーから順に、サーバーが応答するまでこれらのサーバーが 1 つずつアクセスされます。

AAA の RSA SecurID サーバーの設定

ここでは、RSA SecurID サーバーグループの設定方法について説明します。管理アクセスや VPN を設定するときに、これらのグループを使用できます。

RSA SecurID AAA サーバーグループの設定

認証に RSA SecurID サーバーとの直接通信を使用する場合は、最初に少なくとも 1 つの SDI サーバーグループを作成し、各グループに 1 つ以上のサーバーを追加する必要があります。RADIUS サーバーとプロキシ関係が確立された SecurID サーバーを使用する場合は、ASA で SDI AAA サーバーグループを設定する必要はありません。

手順

ステップ 1 SDI AAA サーバーグループを作成し、AAA サーバーグループ コンフィギュレーション モードを開始します。

aaa-server *server_group_name* **protocol sdi**

例：

```
ciscoasa(config)# aaa-server watchdog protocol sdi
```

ステップ 2 （オプション）次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASAは引き続きグループ内のサーバーにアクセスしようとします。

ステップ 3 （任意）グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバーが非アクティブになって初めて、障害の発生したサーバーが再度アクティブ化されます。これは、デフォルトのモードです。

deadtime *minutes* キーワードと引数のペアは、グループ内の最後のサーバーをディセーブルにしてから次にすべてのサーバーを再度イネーブルにするまでの経過時間を、0～1440分の範囲で指定します。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。デフォルトは 10 分です。

timed キーワードを指定すると、30秒のダウン時間の後、障害が発生したサーバーが再度アクティブ化されます。

SDI サーバーグループへの RSA SecurID サーバーの追加

SDI サーバーグループを使用する前に、少なくとも 1 つの RSA SecurID サーバーをグループに追加する必要があります。

SDI サーバーグループのサーバーは、ASA との通信に認証およびサーバー管理プロトコル（ACE）を使用します。

手順

ステップ 1 RSA SecurID サーバーを SDI サーバーグループに追加します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

インターフェイスを指定しない場合、ASAではデフォルトで**内部**インターフェイスを使用します。

IPv4 または IPv6 アドレスを使用できます。

ステップ 2 サーバーへの接続試行のタイムアウト値を指定します。

timeout *seconds*

Specify the timeout interval（1-300 seconds）for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts（based on the interval defined on the **retry-interval** command）until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の **max-failed-attempts** コマンドで指定された制限に達すると、AAA サーバーは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバーへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 3 再試行間隔を指定します。システムはこの時間待機してから接続要求を再試行します。

retry-interval *seconds*

1 ー 10 秒を指定できます。デフォルトは 10 です。

例：

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

ステップ 4 デフォルトの RSA SecurID ポート（TCP/5500）と異なる場合はサーバーポートを指定します。ASA は、このポートで RSA SecurID サーバーに接続します。

server-port *port_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

SDI ノードシークレットファイルのインポート

RSA Authentication Manager（SecurID）サーバーによって生成されたノードシークレットファイルを手動でインポートできます。

手順

ステップ 1 RSA Authentication Manager サーバーからノードシークレットファイルをエクスポートします。詳細については、RSA Authentication Manager のドキュメントを参照してください。

ステップ 2 解凍したバージョンのノードシークレットファイルを ASA からアクセスできるサーバーに配置するか、ASA 自体にコピーします。

サーバーは、FTP、HTTP、HTTPS、SCP、SMB、TFTP のいずれかの転送プロトコルをサポートしている必要があります。

ステップ 3 ノードシークレットファイルをインポートします。

aaa sdi import-node-secret *filepath rsa_server_address password*

値は次のとおりです。

- *filepath* は、RSA Authentication Manager からエクスポートして解凍されたノードシークレットファイルへの完全なパスです。ローカルシステムのファイルは、disk0:、disk1:、または flash: としてアドレス指定できます。リモートサーバーのファイルの場合は、ftp:// などの標準の URL 表記を使用します。
- *rsa_server_address* は、ノードシークレットが属する RSA Authentication Manager サーバーの IP アドレスまたは完全修飾ホスト名です。
- *password* は、エクスポート時にファイルを保護するために使用されるパスワードです。

例：

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

AAA の RSA SecurID サーバーのモニタリング

次のコマンドを使用して、RSA SecurID 関連情報をモニターおよびクリアできます。

- **show aaa-server**

  AAA サーバーの統計情報を表示します。サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを使用します。

- **show running-config aaa-server**

  システムに設定されている AAA サーバーを表示します。AAA サーバー コンフィギュレーションを削除するには、**clear configure aaa-server** コマンドを使用します。

- **show aaa sdi node-secrets**

  インポートされたノードシークレットファイルがある RSA SecurID サーバーを表示します。ノードシークレットファイルを削除するには、**clear aaa sdi node-secret** コマンドを使用します。

AAA の RSA SecurID サーバーの履歴

機能名	プラットフォーム リリース	説明
SecurID サーバー	7.2(1)	AAA の SecurID サーバーの管理認証でのサポート。以前のリリースでは、SecurID は VPN 認証でサポートされていました。
AAA の IPv6 アドレス	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバーグループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングル コンテキスト モードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、次のコマンドが変更されました。**aaa-server**、**aaa-server host**
SDI AAA サーバーグループで使用するノードシークレットファイルの RSA Authentication Manager からの手動インポート。	9.15(1)	SDI AAA サーバーグループで使用するために RSA Authentication Manager からエクスポートしたノードシークレットファイルをインポートできます。 次のコマンドが追加されました。**aaa sdi import-node-secret**、**clear aaa sdi node-secret**、**show aaa sdi node-secrets**。

第 VII 部

システム管理

- 管理アクセス （1495 ページ）
- ソフトウェアおよびコンフィギュレーション （1553 ページ）
- システム イベントに対する応答の自動化 （1603 ページ）
- テストとトラブルシューティング （1617 ページ）

第 42 章

管理アクセス

この章では、Telnet、SSH、およびHTTPS（ASDMを使用）経由でシステム管理のためにASAにアクセスする方法、ユーザーを認証および許可する方法、およびログインバナーを作成する方法について説明します。

- 管理リモート アクセスの設定 （1495 ページ）
- システム管理者用 AAA の設定 （1516 ページ）
- デバイス アクセスのモニタリング （1540 ページ）
- 管理アクセスの履歴 （1542 ページ）

管理リモート アクセスの設定

ここでは、ASDM 用の ASA アクセス、Telnet または SSH、およびログイン バナーなどのその他のパラメータの設定方法について説明します。

SSH アクセスの設定

SSH ガイドライン

- また、ASA インターフェイスに SSH アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、SSH アクセスを設定する必要があるだけです。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの SSH アクセスはサポートされません。たとえば、SSH ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。7
- ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 SSH 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。ただし、設定コマンドは変更されるリソースをロックする可能性があるため、すべての変更が正しく適用されるように、一度に 1 つの SSH セッションで変更を行う必要があります。
- SSH では次の機能はサポートされていません。

- EDDSA キーペア
- FIPS モードの RSA キーペア

- ASA **copy** コマンドを使用して SCP サーバーとの間でファイルをコピーするには、次の手順を実行する必要があります。
  - 25 **ssh** コマンドを使用して、ASA で SCP サーバーサブネット/ホストの SSH アクセスを有効にします。
  - **crypto key generate**コマンドを使用して、キーペアを生成します（物理 ASA の場合のみ）。
- SSH デフォルトユーザー名はサポートされなくなりました。**pix** または **asa** ユーザー名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンドを使用して AAA 認証を設定してから、**username** コマンドを入力してローカル ユーザーを定義します。ローカル データベースの代わりにAAAサーバーを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。
- SSH バージョン 2 のみがサポートされます。

ASA への SSH アクセスを設定するには、SSH サーバをイネーブルにして、許可する IP アドレスを指定します。ユーザーを認証するために、次の方法を使用できます。

- ローカル データベースまたは AAA サーバーのいずれかを使用するユーザー名とパスワード。
- ローカル データベースを使用したユーザー名と公開キー。

SSH サーバーを有効化

SSH サーバーをイネーブルにし、接続を許可する IP アドレスを指定します。その他の SSH サーバー設定を行うこともできます。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

手順

ステップ 1 ASA がアドレスまたはサブネットごとに接続を受け入れる IP アドレスと、SSH を使用可能なインターフェイスを特定します。

ssh *source_IP_address mask source_interface*

- *source_interface*：名前付きインターフェイスを指定します。ブリッジ グループの場合、ブリッジ グループ メンバ インターフェイスを指定します。

Telnet と異なり、SSH は最も低いセキュリティ レベルのインターフェイスで実行できます。

例：

```
ciscoasa(config)# ssh 192.168.3.0 255.255.255.0 inside
```

ステップ 2 （任意） ASA がセッションを切断するまでに SSH がアイドル状態を維持する時間の長さを設定します。

ssh timeout *minutes*

例：

```
ciscoasa(config)# ssh timeout 30
```

タイムアウトは 1 ～ 60 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

ステップ 3 （任意） セキュアコピー（SCP）サーバーをイネーブルにできます。

ssh scopy enable

SCP サーバーにはディレクトリサポートがありません。ディレクトリ サポートがないため、ASA の内部ファイルへのリモート クライアント アクセスは制限されます。

SCP サーバーでは、バナーまたはワイルドカードがサポートされていません。

ステップ 4 （任意） SSH 暗号の暗号化アルゴリズムを設定します。

ssh cipher encryption {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_encryption_ciphers*}

例：

```
ciscoasa(config)# ssh cipher encryption custom 3des-cbc:aes128-cbc:aes192-cbc
```

デフォルトは **medium** です。暗号方式は、リストされた順に使用されます。事前定義されたリストでは、暗号方式が最も高いの順で、最も低いセキュリティに割り当てられています。

- **all** キーワードは、すべての暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes192-ctr aes256-ctr ）を使用することを指定します
- カスタム暗号ストリングを設定する場合は、**custom** キーワードを使用し、各暗号ストリングをコロンで区切って入力します。
- FIPS 対応の暗号方式（aes128-cbc aes256-cbc）のみを使用する場合は、**fips** キーワードを使用します。

- **high** キーワードは、強度が高の暗号方式のみ：aes256-cbc aes128-gcm@openssh.com chacha20-poly1305@openssh.com aes256-ctr
- 強度が低、中、高の暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、**low** キーワードを使用します。
- 強度が中および高の暗号方式（3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr）を使用する場合は、**medium** キーワードを使用します（デフォルト）。

ステップ 5 （任意） SSH 暗号の整合性アルゴリズムを設定します。

ssh cipher integrity {**all** | **fips** | **high** | **low** | **medium** | **custom** *colon-delimited_list_of_integrity_ciphers*}

例：

```
ciscoasa(config)# ssh cipher integrity custom hmac-sha1-96:hmac-md5
```

デフォルトは **high** です。

- すべての暗号方式（hmac-sha1 hmac-sha1-96（非推奨）hmac-md5（非推奨）hmac-md5-96（非推奨）hmac-sha2-256）を使用する場合は、**all** キーワードを使用します。
- カスタム暗号ストリングを設定する場合は、**custom** キーワードを使用し、各暗号ストリングをコロンで区切って入力します。
- FIPS 対応の暗号方式（hmac-sha1 hmac-sha2-256）のみを使用する場合は、**fips** キーワードを使用します。
- 強度が高の暗号方式のみ（hmac-sha2-256）を使用する場合は、**high** キーワードを使用します（デフォルト）。
- 強度が低、中、高の暗号方式（hmac-sha1 hmac-sha1-96 hmac-md5 hmac-md5-96 hmac-sha2-256）を使用する場合は、**low** キーワードを使用します。
- 強度が中および高の暗号方式（hmac-sha1 hmac-sha1-96（非推奨）hmac-sha2-256）を使用する場合は、**medium** キーワードを使用します。

ステップ 6 （任意）（管理コンテキストのみ）Diffie-Hellman（DH）キー交換モードを設定します。

ssh key-exchange group {**curve25519-sha256** | **dh-group14-sha1** | **dh-group14-sha256** | **ecdh-sha2-nistp256**}

例：

```
ciscoasa(config)# ssh key-exchange group dh-group14-sha1
```

デフォルトは **dh-group14-sha256**

DH キー交換では、いずれの当事者も単独では決定できない共有秘密を使用します。キー交換を署名およびホストキーと組み合わせることで、ホスト認証が実現します。このキー交換方式により、明示的なサーバ認証が可能となります。DH キー交換の使用方法の詳細については、

RFC 4253 を参照してください。キー交換は管理コンテキストでのみ設定できます。この値はすべてのコンテキストで使用されます。

例

次に、ASA への SCP セッションの例を示します。外部ホストのクライアントから、SCP ファイル転送を実行します。たとえば、Linux では次のコマンドを入力します。

scp -v -pw *password* [*path*/]*source_filename*
username@asa_address:{**disk0**|**disk1**}:/[*path*/]*dest_filename*

-v は冗長を表します。**-pw** が指定されていない場合は、パスワードの入力を求めるプロンプトが表示されます。

パスワード アクセス用の SSH の設定

ユーザー名とパスワードを使用して SSH 認証を構成します。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

手順

ステップ 1 SSH に必要なキーペアを生成します（物理 ASA の場合のみ）。

ASA 仮想 の場合、キーペアは導入後に自動的に作成されます。

a) キーペアを生成します。
crypto key generate {**ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

例：

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **ecdsa elliptic-curve** *size*：ビット単位のサイズは 256、384、または 521 です。
- **rsa modulus** *size*：ビット単位のサイズは 2048、3072、または 4096 です。

指定するキーのサイズが大きいほど、キーペアの生成にかかる時間は長くなります。SSH は ECDSA、RSA の順にキーを試みます。**show crypto key mypubkey** {**ecdsa** | **rsa**} コマンドを使用してキーを表示します。SSH によって使用されるキーは <Default-*type*-Key> と呼ばれます。

b) （任意） デフォルトのキー順序（ECDSA、RSA）を使用しない場合は、使用するキーペアを指定します。

ssh key-exchange hostkey {**rsa** | **ecdsa**}

RSA を選択した場合、2048 以上のキーサイズを使用する必要があります。アップグレードの互換性のために、これより小さいキーは、デフォルトのキー順序を使用する場合にのみサポートされます。

例：

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

ステップ 2 キーを永続的なフラッシュメモリに保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 3 SSH アクセスに使用できるローカル データベースまたは AAA サーバーでユーザーを作成します。ローカルユーザー名を追加するには、次のコマンドを参照してください（推奨）。

username *name* **password** *password* **privilege** *level*

同じローカル ユーザーに対して、公開キー認証またはパスワード認証を使用できます。AAA サーバを使用した公開キー認証はサポートされていません。

例：

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

デフォルトの特権レベルは 2 です。0 ～ 15 の範囲でレベルを入力します。15 を指定すると、すべての特権を使用できます。

ステップ 4 SSH アクセスのローカルまたは AAA サーバー認証をイネーブルにします。

aaa authentication ssh console {**LOCAL** | *server_group* [**LOCAL**]}

このコマンドは、**ssh authentication** コマンドセットでのユーザー名のローカル公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。このコマンドは、ユーザー名とパスワードにのみ影響します。ローカルユーザーが公開キー認証またはパスワードを使用できるようにするには、パスワードアクセスを有効にするため、このコマンドで明示的にローカル認証を設定する必要があります。

例：

```
ciscoasa(config)# aaa authentication ssh console LOCAL
```

公開キー アクセス用の SSH の設定

パブリック キーを使用した SSH 公開キー認証の設定

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

手順

ステップ 1 SSH に必要なキーペアを生成します（物理 ASA の場合のみ）。

ASA 仮想 の場合、キーペアは導入後に自動的に作成されます。

a) キーペアを生成します。

crypto key generate {**ecdsa elliptic-curve** *size* |**rsa modulus** *size*}

例：

```
ciscoasa(config)# crypto key generate ecdsa elliptic-curve 521
```

- **ecdsa elliptic-curve** *size*：ビット単位のサイズは 256、384、または 521 です。
- **rsa modulus** *size*：ビット単位のサイズは 2048、3072、または 4096 です。

指定するキーのサイズが大きいほど、キーペアの生成にかかる時間は長くなります。SSH は ECDSA、RSA の順にキーを試みます。**show crypto key mypubkey** {**ecdsa** | **rsa**} コマンドを使用してキーを表示します。SSH によって使用されるキーは <Default-*type*-Key> と呼ばれます。

b) （任意） デフォルトのキー順序（ECDSA、RSA）を使用しない場合は、使用するキーペアを指定します。

ssh key-exchange hostkey {**rsa** | **ecdsa**}

RSA を選択した場合、2048 以上のキーサイズを使用する必要があります。アップグレードの互換性のために、これより小さいキーは、デフォルトのキー順序を使用する場合にのみサポートされます。

例：

```
ciscoasa(config)# ssh key-exchange hostkey ecdsa
```

ステップ 2 キーを永続的なフラッシュメモリに保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ステップ 3 SSH アクセスに使用できるユーザーをローカル データベースに作成します。

username *name* [**password** *password*] **privilege** *level*

例：

```
ciscoasa(config)# username admin password Far$cape1999 privilege 15
```

デフォルトの特権レベルは 2 です。0 ～ 15 の範囲でレベルを入力します。15 を指定すると、すべての特権を使用できます。ユーザーにパスワード認証ではなく公開キー認証（**ssh authentication**）を強制する場合は、パスワードなしでユーザーを作成することを推奨します。**username** コマンドで公開キー認証およびパスワードの両方を設定した場合、ユーザーはいずれの方法でもログインできます（パスワードアクセス用の SSH の設定 （1499 ページ）この手順で AAA 認証を明示的に設定した場合）。**注**：ユーザー名とパスワードを作成しなければならないという事態を回避するため、**username** コマンド **nopassword** オプション**nopassword** オプションでは、任意のパスワードを入力できますが、パスワードなしは不可能です。パスワード アクセス用の SSH の設定 （1499 ページ）

ステップ 4 パスワード認証ではなく公開キー認証のみ、またはこれら両方の認証をユーザーに許可し、ASA で公開キーを入力します。

username *name* **attributes**

ssh authentication {**pkf** | **publickey** *key*}

例：

```
ciscoasa(config)# username admin attributes
ciscoasa(config-username)# ssh authentication pkf

Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "256-bit ED25519, converted by dean@dwinchester-mac from "
AAAAC3NzaC1lZDI1NTE5AAAAIDmIeTNfEOnuH0094p1MKX80fW2O216g4trnf7gwWe5Q
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
```

ローカル **username** の場合、パスワード認証ではなく公開キー認証のみ、またはこれら両方の認証を有効にできます。ssh-rsa、or ecdsa-sha2-nistp raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、公開キー/秘密キーのペアを生成できます。ASA で公開キーを入力します。その後、SSH クライアントは秘密キー（およびキー ペアを作成するために使用したパスフレーズ）を使用して ASA に接続します。

pkf キーの場合、PKF でフォーマットされたキーを最大 4096 ビット貼り付けるよう求められます。Base64 形式では大きすぎてインラインで貼り付けることができないキーにはこのフォーマットを使用します。たとえば、ssh keygen を使って 4096 ビットのキーを生成してから PKF に変換し、そのキーに対して **pkf** キーワードが求められるようにすることができます。**注**：フェールオーバーで **pkf** オプションを使用することはできますが、PKF キーは、スタンバイ

システムに自動的に複製されません。PKF キーを同期するには、**write standby** コマンドを入力する必要があります。

publickey キーの場合、これは Base64 でエンコードされた公開キーのことです。ssh-rsa、ecdsa-sha2-nistp raw キー（証明書なし）を生成可能な任意の SSH キー生成ソフトウェア（ssh keygen など）を使用して、キーを生成できます。

例

次に、PKF 形式のキーを使用して認証する例を示します。

```
ciscoasa(config)# crypto key generate rsa modulus 4096
ciscoasa(config)# write memory
ciscoasa(config)# username exampleuser1 password examplepassword1 privilege 15
ciscoasa(config)# username exampleuser1 attributes
ciscoasa(config-username)# ssh authentication pkf
Enter an SSH public key formatted file.
End with the word "quit" on a line by itself:
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by xxx@xxx from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnFaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77II==
---- END SSH2 PUBLIC KEY ----
quit
INFO: Import of an SSH public key formatted file SUCCEEDED.
ciscoasa(config)#
```

次の例では、Linux または Macintosh システムの SSH の共有キーを生成して、ASA にインポートします。

1. コンピュータで 4096 ビットの RSA 公開キーおよび秘密キーを生成します。

```
jcrichton-mac:~ john$ ssh-keygen -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/Users/john/.ssh/id_rsa):
/Users/john/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase): pa$$phrase
Enter same passphrase again: pa$$phrase
Your identification has been saved in /Users/john/.ssh/id_rsa.
Your public key has been saved in /Users/john/.ssh/id_rsa.pub.
The key fingerprint is:
c0:0a:a2:3c:99:fc:00:62:f1:ee:fa:f8:ef:70:c1:f9 john@jcrichton-mac
The key's randomart image is:
+--[ RSA 4096]----+
| .               |
```

```
|  o  .           |
|+...  o          |
|B.+.....         |
|.B ..+  S        |
|  =   o          |
|   + . E         |
|  o o            |
| ooooo           |
+-----------------+
```

2. PKF 形式にキーを変換します。

```
jcrichton-mac:~ john$ cd .ssh
jcrichton-mac:.ssh john$ ssh-keygen -e -f id_rsa.pub
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "4096-bit RSA, converted by john@jcrichton-mac from OpenSSH"
AAAAB3NzaC1yc2EAAAADAQABAAACAQDNUvkgza37lB/Q/fljpLAv1BbyAd5PJCJXh/U4LO
hleR/qgIROjpnDaS7Az8/+sjHmq0qXC5TXkzWihvRZbhefyPhPHCi0hIt4oUF2ZbXESA/8
jUT4ehXIUE7FrChffBBtbD4d9FkV8A2gwZCDJBxEM26ocbZCSTx9QC//wt6E/zRcdoqiJG
p4ECEdDaM+56l+yf73NUigO7wYkqcrzjmI1rZRDLVcqtj8Q9qD3MqsV+PkJGSGiqZwnyIl
QbfYxXHU9wLdWxhUbA/xOjJuZ15TQMa7KLs2u+RtrpQgeTGTffIh6O+xKh93gwTgzaZTK4
CQ1kuMrRdNRzza0byLeYPtSlv6Lv6F6dGtwlqrX5a+w/tV/aw9WUg/rapekKloz3tsPTDe
p866AFzU+Z7pVR1389iNuNJHQS7IUA2m0cciIuCM2we/tVqMPYJl+xgKAkuHDkBlMS4i8b
Wzyd+4EUMDGGZVeO+corKTLWFO1wIUieRkrUaCzjComGYZdzrQT2mXBcSKQNWlSCBpCHsk
/r5uTGnKpCNWfL7vd/sRCHyHKsxjsXR15C/5zgHmCTAaGOuIq0Rjo34+61+70PCtYXebxM
Wwm19e3eH2PudZd+rj1dedfr2/IrislEBRJWGLoR/N+xsvwVVM1Qqw1uL4r99CbZF9NghY
NRxCQOY/7K77IQ==
---- END SSH2 PUBLIC KEY ----
jcrichton-mac:.ssh john$
```

3. キーをクリップボードにコピーします。

4. ASDM で、**[構成（Configuration）] > [デバイス管理（Device Management）] > [ユーザ/AAA（Users/AAA）] > [ユーザアカウント（User Accounts）]** の順に選択し、ユーザ名を選択してから [編集（Edit）] をクリックします。[Public Key Using PKF] をクリックして、ウィンドウにキーを貼り付けます。

5. ユーザが ASA に SSH できることを確認します。パスワードには、キーペアの作成時に指定した SSH キーパスワードを入力します。

```
jcrichton-mac:.ssh john$ ssh test@10.86.118.5
The authenticity of host '10.86.118.5 (10.86.118.5)' can't be established.
RSA key fingerprint is 39:ca:ed:a8:75:5b:cc:8e:e2:1d:96:2b:93:b5:69:94.
Are you sure you want to continue connecting (yes/no)? yes
```

次のダイアログボックスが、パスフレーズを入力するために表示されます。

一方、端末セッションでは、以下が表示されます。

```
Warning: Permanently added '10.86.118.5' (RSA) to the list of known hosts.
Identity added: /Users/john/.ssh/id_rsa (/Users/john/.ssh/id_rsa)
Type help or '?' for a list of available commands.
asa>
```

Telnet アクセスの設定

Telnet を使用して ASA にアクセス可能なクライアント IP アドレスを指定するには、次の手順を実行します。次のガイドラインを参照してください。

- また、ASA インターフェイスに Telnet アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、Telnet アクセスを設定する必要があるだけです。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの Telnet アクセスはサポートされません。たとえば、Telnet ホストが外部インターフェイスにある場合、外部インターフェイスへの直接 Telnet 接続のみ開始できます。このルールの例外は、VPN 接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定（1510 ページ）を参照してください。
- VPN トンネル内で Telnet を使用する場合を除き、最も低いセキュリティ インターフェイスに対して Telnet は使用できません。
- ASA は、コンテキスト/単一のモードあたり最大 5 つの同時 Telnet 接続と、すべてのコンテキストにまたがり分散された最大 100 の接続を許容します。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

- Telnet を使用して ASA CLI にアクセスするには、**password** コマンドで設定したログインパスワードを入力します。Telnet を使用する前に手動でパスワードを設定する必要があります。

手順

ステップ 1 ASA が指定したインターフェイスのアドレスまたはサブネットごとに接続を受け入れる IP アドレスを特定します。

telnet *source_IP_address mask source_interface*

- *source_interface*：名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジグループメンバインターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定（1510ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

インターフェイスが 1 つしかない場合は、インターフェイスのセキュリティ レベルが 100 である限り、そのインターフェイスにアクセスするように Telnet を設定することができます。

例：

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

ステップ 2 ASA がセッションを切断するまで Telnet セッションがアイドル状態を維持する時間の長さを設定します。

telnet timeout *minutes*

例：

```
ciscoasa(config)#  telnet timeout 30
```

タイムアウトは 1 ～ 1440 分に設定します。デフォルトは 5 分です。デフォルトの期間では一般に短すぎるので、実働前のテストとトラブルシューティングがすべて完了するまでは、長めに設定しておいてください。

例

次の例は、アドレスが 192.168.1.2 の内部インターフェイスのホストで ASA にアクセスする方法を示しています。

```
ciscoasa(config)# telnet 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0 のネットワーク上のすべてのユーザーが内部インターフェイス上の ASA にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# telnet 192.168.3.0. 255.255.255.255 inside
```

ASDM、その他のクライアントの HTTPS アクセスの設定

ASDM または CSM などの他の HTTPS クライアントを使用するには、HTTPS サーバーを有効にし、ASA への HTTPS 接続を許可する必要があります。HTTPS アクセスは工場出荷時のデフォルト設定の一部として有効化されています。HTTPSアクセスを設定するには、次のステップを実行します。次のガイドラインを参照してください。

- また、ASA インターフェイスに HTTPS アクセスの目的でアクセスするために、ホスト IP アドレスを許可するアクセス ルールは必要ありません。このセクションの手順に従って、HTTPSアクセスを設定する必要があるだけです。ただし、HTTP リダイレクトを設定して HTTP 接続を HTTPS に自動的にリダイレクトするには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。
- ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスはサポートされません。たとえば、管理ホストが外部インターフェイスにある場合、外部インターフェイスへの直接管理接続のみ開始できます。このルールの例外は、VPN接続を介した場合のみです。VPN トンネルを介した管理アクセスの設定（1510ページ）を参照してください。
- シングル コンテキスト モードでは、最大 5 の ASDM 同時セッションを構成できます。マルチ コンテキスト モードでは、コンテキストごとに最大 5 つの同時 ASDM セッションを使用でき、全コンテキスト間で最大 200 の ASDM インスタンスの使用が可能です。

  ASDMセッションでは、2つのHTTPS接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、マルチ コンテキスト モード システムの ASDM セッションの制限が 200 の場合、HTTPS セッション数は 400 に制限されます。
- ASA では、シングルコンテキストモードまたはコンテキストごとに最大 6 つの非 ASDM HTTPS 同時セッション（使用可能な場合）を許可し、すべてのコンテキスト間で最大または 100 の HTTPS セッションを許可します。
- 同じインターフェイス上で SSL（[webvpn] > [インターフェイスの有効化（enable interface）]）と HTTPS アクセスの両方を有効にした場合、**https://***ip_address* から セキュア クライアント にアクセスでき、**https://***ip_address*/**admin** から ASDM にアクセスできます。どちらもポート 443 を使用します。**aaa authentication http console** も有効にする場合は、ASDM アクセス用に別のポートを指定する必要があります。

始める前に

- マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システムからコンテキスト コンフィギュレーションに変更するには、**changeto context** *name* を入力します。

手順

ステップ 1 ASA が指定したインターフェイスのアドレスまたはサブネットごとに HTTPS 接続を受け入れる IP アドレスを特定します。

http *source_IP_address mask source_interface*

- *source_interface*：名前付きインターフェイスを指定します。ブリッジグループの場合、ブリッジグループメンバインターフェイスを指定します。VPN 管理アクセスのみ（VPN トンネルを介した管理アクセスの設定（1510ページ）を参照してください）の場合、名前付き BVI インターフェイスを指定します。

例：

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

ステップ 2 HTTPS サーバーをイネーブルにします。

http server enable [*port*]

例：

```
ciscoasa(config)# http server enable 444
```

デフォルトでは、port は 443 です。ポート番号を変更する場合は、必ず ASDM アクセス URL に変更したポート番号を含めてください。たとえば、ポート番号を 444 に変更する場合は、次の URL を入力します。

https://10.1.1.1:444

ステップ 3 非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。

http server basic-auth-client *user_agent*

- *user_agent*：HTTP 要求の HTTP ヘッダーにあるクライアントの User-Agent 文字列を指定します。完全な文字列または部分文字列を指定できます。部分文字列については、User-Agent 文字列の先頭と一致している必要があります。セキュリティを強化するために完全な文字列をお勧めします。文字列では大文字と小文字が区別されることに注意してください。

  たとえば、 **curl** は次の User-Agent 文字列と一致します。

  curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

  curl は、次の User-Agent 文字列とは一致しません。

  abcd curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1 Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2

CURL は、次の User-Agent 文字列とは一致しません。

```
curl/7.19.7 (x86_64-redhat-linux-gnu) libcurl/7.19.7 NSS/3.19.1
Basic ECC zlib/1.2.3 libidn/1.18 libssh2/1.4.2
```

個別のコマンドを使用して、各クライアント文字列を入力します。多くの専門クライアント（python ライブラリ、curl、wget など）は、クロスサイト要求の偽造（CSRF）トークンベースの認証をサポートしていないため、これらのクライアントが ASA 基本認証方式を使用することを明確に許可する必要があります。セキュリティ上の理由から、必要なクライアントのみを許可する必要があります。

例：

```
ciscoasa(config)# http server basic-auth-client curl
```

ステップ 4 （任意） 接続とセッションのタイムアウトを設定します。

http server idle-timeout*minutes*

http server session-timeout*minutes*

http connection idle-timeout*seconds*

- **http server idle-timeout** *minutes*：ASDM 接続のアイドルタイムアウトを 1 ～ 1440 分の範囲で設定します。デフォルトは 20 分です。ASA は、設定した期間アイドル状態の ASDM 接続を切断します。
- **http server session-timeout** *minutes*：ASDM セッションのセッションタイムアウトを 1 ～ 1440 分の範囲で設定します。このタイムアウトはデフォルトで無効になっています。ASA は、設定した期間を超えた ASDM 接続を切断します。
- **http connection idle-timeout** *seconds*：ASDM、WebVPN、および他のクライアントを含むすべての HTTPS 接続のアイドルタイムアウトを 10 ～ 86400 秒の範囲で設定します。このタイムアウトはデフォルトで無効になっています。ASA は、設定した期間アイドル状態の接続を切断します。**http server idle-timeout** コマンドと **http connection idle-timeout** コマンドの両方を設定した場合は、**http connection idle-timeout** コマンドが優先されます。

例：

```
ciscoasa(config)# http server idle-timeout 30
ciscoasa(config)# http server session-timeout 120
```

例

次の例は、HTTPS サーバーを有効化し、アドレスが 192.168.1.2 の内部インターフェイス上のホストで ASDM にアクセスする方法を示しています。

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

```
ciscoasa(config)# http 192.168.1.2 255.255.255.255 inside
```

次の例は、192.168.3.0/24 のネットワーク上のすべてのユーザーが内部インターフェイス上の ASDM にアクセスできるようにする方法を示しています。

```
ciscoasa(config)# http 192.168.3.0 255.255.255.0 inside
```

ASDM アクセスまたはクライアントレス SSL VPN のための HTTP リダイレクトの設定

ASDM またはクライアントレス SSL VPN を使用して ASA に接続するには、HTTPS を使用する必要があります。利便性のために、HTTP 管理接続を HTTPS にリダイレクトすることができます。たとえば、HTTP をリダイレクトすることによって、**http://10.1.8.4/admin/** または **https://10.1.8.4/admin/** と入力し、ASDM 起動ページで HTTPS アドレスにアクセスできます。

IPv4 と IPv6 の両方のトラフィックをリダイレクトできます。

始める前に

通常、ホスト IP アドレスを許可するアクセス ルールは必要ありません。ただし、HTTP リダイレクトのためには、HTTP を許可するアクセス ルールを有効化する必要があります。そうしないと、インターフェイスが HTTP ポートをリッスンできません。

手順

Enable HTTP redirect:

http redirect *interface_name* [*port*]

例：

```
ciscoasa(config)# http redirect outside 88
```

port は、インターフェイスが HTTP 接続のリダイレクトに使用するポートを指定します。デフォルトは 80 です。

VPN トンネルを介した管理アクセスの設定

あるインターフェイスで VPN トンネルが終端している場合、別のインターフェイスにアクセスして ASA を管理するには、そのインターフェイスを管理アクセス インターフェイスとして指定する必要があります。たとえば、外部インターフェイスから ASA に入る場合は、この機能を使用して、ASDM、SSH、または Telnet 経由で内部インターフェイスに接続するか、外部インターフェイスから入るときに内部インターフェイスに ping を実行できます。

（注） CiscoSSH スタックを使用する場合（これがデフォルトです）、この機能は SSH ではサポートされません。

（注） この機能は SNMP ではサポートされません。VPN 経由の SNMP の場合、ループバック インターフェイスで SNMP を有効にすることをお勧めします。ループバック インターフェイスで SNMP を使用するために、管理アクセス機能を有効にする必要はありません。ループバックは SSH でも機能します。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの VPN アクセスはサポートされません。たとえば、VPN アクセスが外部インターフェイスにある場合、外部インターフェイスへの直接接続のみ開始できます。複数のアドレスを覚える必要がないように、ASA の直接アクセス可能インターフェイスの VPN を有効にし、名前解決を使用してください。

管理アクセスは、IPsec クライアント、IPsec サイト間、Easy VPN、セキュアクライアント SSL VPN の VPN トンネルタイプ経由で行えます。

始める前に

- この機能は管理専用インターフェイスではサポートされません。
- 管理アクセス インターフェイスを使用し、アイデンティティ NAT を構成する場合、ルート ルックアップ オプションを使用して NAT を構成する必要があります。詳細については、ASA ファイアウォール CLI 構成ガイドの適切なリリースの「*NAT* の例と参照」のセクションの「NAT および VPN 管理アクセス」の項を参照してください。

手順

別のインターフェイスから ASA に入るときにアクセスする管理インターフェイスの名前を指定します。

management-access *management_interface*

Easy VPN およびサイト間トンネルでは、名前付き BVI を指定できます（ルーテッド モード）。

例：

```
ciscoasa(config)# management-access inside
```

コンソール タイムアウトの変更

コンソール タイムアウトでは、接続を特権 EXEC モードまたはコンフィギュレーション モードにしておくことができる時間を設定します。タイムアウトに達すると、セッションはユーザー EXEC モードになります。デフォルトでは、セッションはタイムアウトしません。この設定は、コンソール ポートへの接続を保持できる時間には影響しません。接続がタイムアウトすることはありません。

手順

特権セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。

console timeout *number*

例：

```
ciscoasa(config)# console timeout 0
```

デフォルトのタイムアウトは 0 であり、セッションがタイムアウトしないことを示します。

CLI プロンプトのカスタマイズ

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

デフォルトでは、プロンプトに ASA のホスト名が表示されます。マルチ コンテキスト モードでは、プロンプトにコンテキスト名も表示されます。CLI プロンプトには、次の項目を表示できます。

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
コンテキスト	（マルチ モードのみ）現在のコンテキストの名前を表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。

state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、state キーワードに対して次の値が表示されます。 • [act]：フェールオーバーが有効であり、装置ではトラフィックをアクティブに通過させています。 • [stby]：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailover]：フェールオーバーは無効であり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーは無効であり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタリングの場合、制御とデータの値が表示されます。

手順

次のコマンドを入力して、CLI プロンプトをカスタマイズします。

prompt {[**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]}

例：

```
ciscoasa(config)# prompt hostname context slot state priority
ciscoasa/admin/pri/act(config)#
```

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。要素はスラッシュ（/）で区切ります。

ログイン バナーの設定

ユーザーが ASA に接続するとき、ログインする前、または特権 EXEC モードに入る前に表示されるメッセージを設定できます。

始める前に

- セキュリティの観点から、バナーで不正アクセスを防止することが重要です。「ウェルカム」や「お願いします」などの表現は侵入者を招き入れているような印象を与えるので使用しないでください。以下のバナーでは、不正アクセスに対して正しい表現を設定しています。

```
You have logged in to a secure device.
If you are not authorized to access this device,
log out immediately or risk possible criminal consequences.
```

- バナーが追加された後、次の場合に ASA に対する Telnet または SSH セッションが終了する可能性があります。
  - バナー メッセージを処理するためのシステム メモリが不足している場合。
  - バナー メッセージの表示を試みたときに、TCP 書き込みエラーが発生した場合。
- バナー メッセージのガイドラインについては、RFC 2196 を参照してください。

手順

ユーザーが最初に接続したとき（「今日のお知らせ」（motd））、ユーザーがログインしたとき（login）、ユーザーが特権EXECモードにアクセスしたとき（exec）のいずれかに表示するバナーを追加します。

banner {**exec** | **login** | **motd**} *text*

例：

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).
```

ユーザーが ASA に接続すると、まず「今日のお知らせ」バナーが表示され、その後にログイン バナーとプロンプトが表示されます。ユーザーが ASA に正常にログインすると、exec バナーが表示されます。

複数の行を追加する場合は、各行の前に **banner** コマンドを追加します。

バナー テキストに関する注意事項：

- スペースは使用できますが、CLI を使用してタブを入力することはできません。
- バナーの長さの制限は、RAM およびフラッシュ メモリに関するもの以外はありません。
- ASA のホスト名またはドメイン名は、**$(hostname)** 文字列と **$(domain)** 文字列を組み込むことによって動的に追加できます。
- システム コンフィギュレーションでバナーを設定する場合は、コンテキスト コンフィギュレーションで **$(system)** 文字列を使用することによって、コンテキスト内でそのバナー テキストを使用できます。

例

以下に、「今日のお知らせ」バナーを追加する例を示します。

```
ciscoasa(config)# banner motd Only authorized access is allowed to $(hostname).

ciscoasa(config)# banner motd Contact me at admin@example.com for any issues.
```

管理セッション クォータの設定

ASA で許可する ASDM、SSH、および Telnet の同時最大セッション数を設定できます。この最大値に達すると、それ以降のセッションは許可されず、syslog メッセージが生成されます。システム ロックアウトを回避するために、管理セッション割り当て量のメカニズムではコンソール セッションをブロックできません。

（注） マルチコンテキストモードではASDMセッションの数を設定することはできず、最大セッション数は 5 で固定されています。

（注） また、最大管理セッション（SSHなど）のコンテキストあたりのリソース制限を設定した場合は、小さい方の値が使用されます。

始める前に

マルチ コンテキスト モードでは、コンテキスト実行スペースで次の手順を実行します。システム コンフィギュレーションからコンテキスト コンフィギュレーションに切り替えるには、**changeto context** *name* コマンドを入力します。

手順

ステップ 1 次のコマンドを入力します。

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

- **ssh**：1 ～ 5 の SSH セッションの最大数を設定します。デフォルトは 5 分です。
- **telnet**：1 ～ 5 の Telnet セッションの最大数を設定します。デフォルトは 5 分です。
- **http**：1 ～ 5 の HTTPS（ASDM）セッションの最大数を設定します。デフォルトは 5 分です。
- **user**：1～5のユーザーごとのセッションの最大数を設定します。デフォルトは5分です。
- *number*：のセッションの数を設定します。その他のキーワードを指定せずに入力すると、この引数では 1 ～ 15 のセッションの集約数が設定されます。デフォルトは 15 です。

例：

```
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

ステップ 2 使用中の現在のセッションを表示します。

show quota management-session[**ssh** |**telnet** |**http** |**user**]

例：

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                  Username
1                             SSH                        cisco
2                             TELNET                     cisco
1                             SSH                        cisco1
```

システム管理者用 AAA の設定

この項では、システム管理者の認証、管理許可、コマンド許可を設定する方法について説明します。

管理認証の設定

CLI および ASDM アクセスの認証を設定します。

管理認証について

ASA へのログイン方法は、認証を有効にしているかどうかによって異なります。

SSH 認証の概要

認証ありまたは認証なしでの SSH アクセスについては、次の動作を参照してください。

- 認証なし：SSH は認証なしでは使用できません。
- 認証あり：SSH 認証を有効にした場合は、AAA サーバーまたはローカルユーザーデータベースに定義されているユーザー名とパスワードを入力します。公開キーの認証では、ASA はローカル データベースのみをサポートします。 SSH 公開キー認証を設定した場合、ASA ではローカル データベースを暗黙的に使用します。ログインにユーザー名とパスワードを使用する場合に必要なのは、SSH認証を明示的に設定することのみです。ユーザー EXEC モードにアクセスします。

Telnet 認証の概要

認証の有無にかかわらず、Telnet アクセスについては、次の動作を参照してください。

- 認証なし：Telnet の認証を有効にしていない場合は、ユーザー名を入力しません。ログイン パスワード（**password** コマンドで設定）を入力します。デフォルトのパスワードはありません。したがって、ASA へ Telnet 接続するには、パスワードを設定する必要があります。ユーザー EXEC モードにアクセスします。
- 認証あり：Telnet認証を有効にした場合は、AAA サーバーまたはローカルユーザーデータベースに定義されているユーザー名とパスワードを入力します。ユーザーEXECモードにアクセスします。

ASDM 認証の概要

認証ありまたは認証なしでのASDMアクセスに関しては、次の動作を参照してください。AAA認証の有無にかかわらず、証明書認証を設定することも可能です。

- 認証なし：デフォルトでは、ブランクのユーザー名と **enable password** コマンドによって設定されたイネーブル パスワード（デフォルトではブランク）を使用して ASDM にログインできます。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。ホスト名、ドメイン名、およびイネーブル パスワードと Telnet パスワードの設定 （1005 ページ）を参照してください。CLI で **enable** コマンドを最初に入力したときに、パスワードを変更するように求められます。ASDMにログインしたときには、この動作は適用されません。ログイン画面で（ユーザー名をブランクのままにしないで）ユーザー名とパスワードを入力した場合は、ASDM によってローカル データベースで一致がチェックされることに注意してください。
- 証明書認証（シングル、ルーテッドモードのみ）：ユーザーに有効な証明書を要求できます。証明書のユーザー名とパスワードを入力すると、ASA が PKI トラストポイントに対して証明書を検証します。
- AAA 認証：ASDM（HTTPS）認証を有効にした場合は、AAA サーバーまたはローカル ユーザーデータベースに定義されているユーザー名とパスワードを入力します。これで、ブランクのユーザー名とイネーブル パスワードで ASDM を使用できなくなりました。
- AAA 認証と証明書認証の併用（シングル、ルーテッド モードのみ）：ASDM（HTTPS）認証を有効にした場合は、AAA サーバーまたはローカル ユーザー データベースに定義されているユーザー名とパスワードを入力します。証明書認証用のユーザー名とパスワードが異なる場合は、これらも入力するように求められます。ユーザー名を証明書から取得してあらかじめ入力しておくよう選択できます。

シリアル認証の概要

認証ありまたは認証なしでのシリアル コンソール ポートへのアクセスに関しては、次の動作を参照してください。

- 認証なし：シリアルアクセスの認証を有効にしていない場合は、ユーザー名、パスワードを入力しません。ユーザー EXEC モードにアクセスします。
- 認証あり：シリアルアクセスの認証を有効にした場合は、AAA サーバーまたはローカル ユーザーデータベースで定義されているユーザー名とパスワードを入力します。ユーザー EXEC モードにアクセスします。

enable 認証の概要

ログイン後に特権EXECモードに入るには、**enable**コマンドを入力します。このコマンドの動作は、認証がイネーブルかどうかによって異なります。

- 認証なし：enable 認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。デフォルトは空白です。**enable**コマンドを最初に入力したときに、それを変更するように求められます。ただし、enable 認証を使用しない場合、**enable** コマンドを入力した後は、特定のユーザーとしてログインしていません。これにより、コマンド認可などユーザーベースの各機能が影響を受けることがあります。ユーザー名を維持するには、enable 認証を使用してください。
- 認証あり：enable 認証を設定した場合は、ASA はプロンプトにより AAA サーバーまたはローカルユーザーデータベースで定義されているユーザー名とパスワードを要求します。この機能は、ユーザーが入力できるコマンドを判別するためにユーザー名が重要な役割を果たすコマンド許可を実行する場合に特に役立ちます。

ローカル データベースを使用する enable 認証の場合は、**enable** コマンドの代わりに **login** コマンドを使用できます。**login** コマンドによりユーザー名が維持されますが、認証をオンにするための設定は必要ありません。

⚠

注意 CLIにアクセスできるユーザや特権EXECモードを開始できないようにするユーザをローカルデータベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザは、CLI で自分のパスワードを使用して特権EXECモード（およびすべてのコマンド）にアクセスできます。あるいは、認証処理でローカルデータベースではなく AAA サーバーを使用してログイン コマンドを回避するか、またはすべてのローカル ユーザーをレベル 1 に設定することにより、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザーを制御できます。

ホスト オペレーティング システムから ASA へのセッション

一部のプラットフォームでは、ASAの実行を別のアプリケーションとしてサポートしています（例：Firepower 4100/9300 の ASA）。ホスト オペレーティング システムから ASA へのセッションの場合、接続のタイプに応じてシリアルおよび Telnet 認証を設定できます。

マルチ コンテキスト モードでは、システム コンフィギュレーションで AAA コマンドを設定できません。ただし、Telnet またはシリアル認証を管理コンテキストで設定した場合、認証はこれらのセッションにも適用されます。この場合、管理コンテキストの AAA サーバーまたはローカル ユーザー データベースが使用されます。

CLIおよびASDM アクセス認証の設定

始める前に

- Telnet、SSH、または HTTP アクセスを設定します。

- 外部認証の場合は、AAA サーバー グループを設定します。ローカル認証の場合は、ローカル データベースにユーザーを追加します。
- HTTP 管理認証では、AAA サーバー グループの SDI プロトコルをサポートしていません。
- この機能は、**ssh authentication** コマンドによるローカル ユーザー名に関する SSH 公開キー認証には影響しません。ASA では、公開キー認証に対し、ローカル データベースを暗黙的に使用します。この機能は、ユーザー名とパスワードにのみ影響します。ローカル ユーザーが公開キー認証またはパスワードを使用できるようにするには、この手順を使用してローカル認証を明示的に設定し、パスワード アクセスを許可する必要があります。

手順

管理アクセス用のユーザーを認証します。

aaa authentication {**telnet** | **ssh** | **http** | **serial**} **console** {**LOCAL** | *server_group* [**LOCAL**]}

例：

```
ciscoasa(config)# aaa authentication ssh console radius_1 LOCAL
ciscoasa(config)# aaa authentication http console radius_1 LOCAL
ciscoasa(config)# aaa authentication serial console LOCAL
```

telnet キーワードは Telnet アクセスを制御します。**ssh** キーワードは SSH アクセスを制御します（パスワードのみ。公開キー認証では暗黙のうちにローカルデータベースが使用されます）。**http** キーワードは ASDM アクセスを制御します。**serial** キーワードはコンソール ポート アクセスを制御します。

認証に AAA サーバー グループを使用する場合は、AAA サーバーが使用できないときにローカルデータベースをフォールバック方式として使用するように ASA を設定できます。サーバー グループ名を指定し、その後に **LOCAL**（大文字と小文字の区別あり）を追加します。ローカル データベースでは AAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASA のプロンプトでは、どの方式が使用されているかが示されないためです。**LOCAL** だけを入力して、ローカルデータベースを認証の主要方式として（フォールバックなしで）使用することもできます。

enable コマンド認証の設定（特権 EXEC モード）

ユーザーが **enable** コマンドを入力する際に、そのユーザーを認証できます。

始める前に

enable 認証の概要 （1518 ページ）を参照してください。

手順

ユーザーを認証するための次のオプションのいずれかを選択します。

- AAA サーバーまたはLOCALデータベースを使用してユーザーを認証するには、次のコマンドを入力します。

  aaa authentication enable console {**LOCAL** | *server_group* [**LOCAL**]}

  例：

  ```
  ciscoasa(config)# aaa authentication enable console LOCAL
  ```

  ユーザー名とパスワードの入力を求めるプロンプトがユーザーに対して表示されます。

  認証に AAA サーバー グループを使用する場合は、AAA サーバーが使用できないときにローカルデータベースをフォールバック方式として使用するようにASAを設定できます。サーバー グループ名を指定し、その後に**LOCAL**（大文字と小文字の区別あり）を追加します。ローカル データベースではAAA サーバーと同じユーザー名およびパスワードを使用することを推奨します。これは、ASAのプロンプトでは、どの方式が使用されているかが示されないためです。

  LOCALだけを入力して、ローカルデータベースを認証の主要方式として（フォールバックなしで）使用することもできます。

- ローカル データベースからユーザーとしてログインするには、次のコマンドを入力します。

  login

  例：

  ```
  ciscoasa# login
  ```

  ASA により、ユーザー名とパスワードの入力を求めるプロンプトが表示されます。パスワードを入力すると、ASA により、ユーザーはローカル データベースで指定されている特権レベルに置かれます。

  ユーザーは独自のユーザー名とパスワードでログインして特権EXECモードにアクセスすることができるので、システム イネーブル パスワードを全員に提供する必要がなくなります。ユーザがログイン時に特権EXECモード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを2（デフォルト）～15に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。

ASDM 証明書認証の設定

AAA 認証の有無にかかわらず証明書認証を必須にできます。ASA は証明書を PKI トラストポイントに照合して検証します。

始める前に

この機能は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 証明書認証をイネーブルにします。

http authentication-certificate *interface_name*[**match** *certificate_map_name*]

例：

```
ciscoasa(config)# crypto ca certificate map map1 10
ciscoasa(config-ca-cert-map)# subject-name emailAddress www.example.com
ciscoasa(config)# http authentication-certificate outside match map1
```

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

証明書が証明書マップと一致することを要件にするには、**match** キーワードとマップ名を指定します。**crypto ca certificate map** コマンドを使用して、マップを設定します。

ステップ 2 （任意） ASDM で証明書からユーザー名を抽出する際に使用する属性を設定します。

http username-from-certificate{*primary-attr* [*secondary-attr*] | **use-entire-name** | **use-script**} [**pre-fill-username**]

例：

```
ciscoasa(config)# http username-from-certificate CN pre-fill-username
```

デフォルトでは、ASDM は CN OU 属性を使用します。

- *primary-attr* 引数は、ユーザ名の抽出に使用する属性を指定します。*secondary-attr* 引数は、オプションで、ユーザー名を抽出するためにプライマリ属性と一緒に使用する追加の属性を指定します。次の属性を使用できます。
  - C：国
  - CN：共通名
  - DNQ：DN 修飾子
  - emailAddress：電子メールアドレス
  - GENQ：世代修飾子
  - GN：名

- I：イニシャル
- L：局所性
- N：名前
- O：組織
- OU：組織単位
- SER：シリアル番号
- SN：姓
- SP：都道府県
- T：役職
- UID：ユーザー ID
- UPN：ユーザー プリンシパル名

- **use-entire-name** キーワードでは DN 名全体を使用します。
- **use-script** キーワードでは ASDM によって生成された Lua スクリプトを使用します。
- **pre-fill-username** キーワードでは、認証を求めるプロンプトにユーザー名が事前入力されています。そのユーザー名が最初に入力したものと異なる場合、最初のユーザー名が事前入力された新しいダイアログボックスが表示されます。そこに、認証用のパスワードを入力できます。

管理許可による CLI および ASDM アクセスの制限

ASA ではユーザーの認証時に管理アクセス ユーザーとリモート アクセス ユーザーを区別できるようになっています。ユーザー ロールを区別することで、リモート アクセス VPN ユーザーやネットワーク アクセス ユーザーが ASA に管理接続を確立するのを防ぐことができます。

始める前に

RADIUS または LDAP（マッピング済み）ユーザー

ユーザーが LDAP 経由で認証されると、ネイティブ LDAP 属性とその値が Cisco ASA 属性にマッピングされ、特定の許可機能が提供されます。Cisco VSA CVPN3000-Privilege-Level の値を 0 ～ 15 の範囲で設定した後、ldap map-attributes**ldap map-attributes** コマンドを使用して、LDAP 属性を Cisco VAS CVPN3000-Privilege-Level にマッピングします。

RADIUS IETF の **service-type** 属性が、RADIUS 認証および許可要求の結果として access-accept メッセージで送信される場合、この属性は認証されたユーザーにどのタイプのサービスを付与するかを指定するために使用されます。

RADIUS Cisco VSA **privilege-level** 属性（ベンダー ID 3076、サブ ID 220）が access-accept メッセージで送信される場合は、ユーザーの権限レベルを指定するために使用されます。

TACACS+ ユーザー

「service=shell」で許可が要求され、サーバーは PASS または FAIL で応答します。

ローカル ユーザー

指定したユーザー名に対する **service-type** コマンドを設定します。デフォルトでは、service-type は admin で、**aaa authentication console** コマンドで指定されたすべてのサービスに対してフルアクセスが許可されます。

管理許可の属性

管理許可の AAA サーバー タイプおよび有効な値については、次の表を参照してください。ASA ではこれらの値を使用して管理アクセス レベルを決定します。

管理レベル	**RADIUS/LDAP** の（マッピングされた）属性	**TACACS+** 属性	ローカル データベースの属性
[Full Access]： **aaa authentication console** コマンド	Service-Type 6（アドミニストレーティブ）、Privilege-Level 1	PASS、特権レベル 1	admin
[Partial Access]： **aaa authentication console** コマンドで設定すると、CLI または ASDM に対するアクセスが許可されます。ただし、**aaa authentication enable console** コマンドを使用して **enable** 認証を設定する場合、CLI y ユーザーは **enable** コマンドを使用して特権 EXEC モードにアクセスすることはできません。	Service-Type 7（NAS プロンプト）、Privilege-Level 2 以上 Framed (2) および Login (1) サービス タイプは同様に扱われます。	PASS、特権レベル 2 以上	nas-prompt
[No Access]：管理アクセスが拒否されます。ユーザーは **aaa authentication console** コマンドで指定されたいずれのサービスも使用できません（**serial** キーワードは除きます。つまり、シリアル アクセスは許可されます）。リモート アクセス（IPsec および SSL）ユーザーは、引き続き自身のリモートアクセスセッションを認証および終了できます。他のすべてのサービスタイプ（ボイス、ファクスなど）も同様に処理されます。	Service-Type 5（アウトバウンド）	FAIL	remote-access

その他のガイドライン

- シリアル コンソール アクセスは管理許可に含まれません。
- この機能を使用するには、管理アクセスにAAA認証も設定する必要があります。CLIおよびASDM アクセス認証の設定 （1518 ページ）を参照してください。
- 外部認証を使用する場合は、この機能をイネーブルにする前に、AAA サーバー グループを設定しておく必要があります。
- HTTP 許可は、シングル ルーテッド モードでのみサポートされます。

手順

ステップ 1 Telnet と SSH の管理許可をイネーブルにします。

aa authorization exec {**authentication-server** | **LOCAL**} [**auto-enable**]

auto-enable キーワードを使用して、十分な認証特権を持つ管理者が、ログインするときに特権 EXEC モードに自動的に入ることができます。

例：

```
ciscoasa(config)# aaa authentication ssh console RADIUS
ciscoasa(config)# aaa authorization exec authentication-server auto-enable
```

ステップ 2 HTTPS の管理許可をイネーブルにします（ASDM）。

aa authorization http console {**authentication-server** | **LOCAL**}

例：

```
ciscoasa(config)# aaa authentication http console RADIUS
ciscoasa(config)# aaa authorization http console authentication-server
```

ステップ 3

例

次の例は、LDAP 属性マップを定義する方法を示しています。この例では、セキュリティ ポリシーによって、LDAP によって認証されているユーザーが、ユーザー レコードのフィールドまたはパラメータの title と company を、IETF-RADIUS service-type と privilege-level にそれぞれマップすることを指定しています。

```
ciscoasa(config)# ldap attribute-map admin-control
ciscoasa(config-ldap-attribute-map)# map-name title IETF-RADIUS-Service-Type
ciscoasa(config-ldap-attribute-map)# map-name company
```

次の例では、LDAP 属性マップを LDAP AAA サーバーに適用します。

```
ciscoasa(config)# aaa-server ldap-server (dmz1) host 10.20.30.1
ciscoasa(config-aaa-server-host)# ldap attribute-map admin-control
```

コマンド認可の設定

コマンドへのアクセスを制御する場合、ASA ではコマンド許可を設定でき、ユーザーが使用できるコマンドを決定できます。デフォルトでは、ログインするとユーザー EXEC モードにアクセスでき、最低限のコマンドだけが提供されます。**enable** コマンド（または、ローカル データベースを使用するときは **login** コマンド）を入力すると、特権 EXEC モードおよびコンフィギュレーション コマンドを含む高度なコマンドにアクセスできます。

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル
- TACACS+ サーバー特権レベル

コマンド認可について

コマンド認可を有効にし、承認済みのユーザーにのみコマンド入力を許容することができます。

サポートされるコマンド認可方式

次の 2 つのコマンド許可方式のいずれかを使用できます。

- ローカル特権レベル：ASA でコマンド特権レベルを設定します。ローカル ユーザー、RADIUS ユーザー、または LDAP ユーザー（LDAP 属性を RADIUS 属性にマッピングする場合）を CLI アクセスについて認証する場合、ASA はそのユーザーをローカル データベース、RADIUS、または LDAP サーバーで定義されている特権レベルに所属させます。ユーザーは、割り当てられた特権レベル以下のコマンドにアクセスできます。すべてのユーザは、初めてログインするときに、ユーザ EXEC モード（レベル 0 または 1 のコマンド）にアクセスします。ユーザは、特権 EXEC モード（レベル 2 以上のコマンド）にアクセスするために再び **enable** コマンドで認証するか、**login** コマンドでログイン（ローカル データベースに限る）できます。

（注） ローカル データベース内にユーザーが存在しなくても、また CLI 認証や **enable** 認証がない場合でも、ローカル コマンド許可を使用できます。代わりに、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力すると、ASA によってレベル 15 に置かれます。次に、すべてのレベルのイネーブル パスワードを作成します。これにより、**enable** *n*（2 ～ 15）を入力したときに、ASA によってレベル *n* に置かれるようになります。これらのレベルは、ローカル コマンド許可を有効にするまで使用されません。

- TACACS+ サーバー特権レベル：TACACS+ サーバーで、ユーザーまたはグループが CLI アクセスについて認証した後で使用できるコマンドを設定します。CLI でユーザーが入力するすべてのコマンドは、TACACS+ サーバーで検証されます。

セキュリティ コンテキストとコマンド許可

AAA 設定はコンテキストごとに個別であり、コンテキスト間で共有されません。

コマンド許可を設定する場合は、各セキュリティ コンテキストを別々に設定する必要があります。この設定により、異なるセキュリティ コンテキストに対して異なるコマンド許可を実行できます。

セキュリティ コンテキストを切り替える場合、管理者は、ログイン時に指定したユーザ名で許可されるコマンドが新しいコンテキスト セッションでは異なる可能性があることや、新しいコンテキストではコマンド許可がまったく設定されていない可能性があることを念頭に置いてください。コマンド許可がセキュリティ コンテキストによって異なる場合があることを管理者が理解していないと、混乱が生じる可能性があります。

（注） システム実行スペースでは AAA コマンドがサポートされないため、システム実行スペースではコマンド許可を使用できません。

コマンド権限レベル

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のすべてのコマンドは特権レベル 15 に割り当てられます。

- **show checksum**
- **show curpriv**
- イネーブル化
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、configure コマンドも同じレベルに移動してください。このようにしないと、ユーザーはコンフィギュレーション モードに入ることができません。

ローカル コマンド許可の設定

ローカル コマンド許可を使用して、コマンドを 16 の特権レベル（0 ～ 15）の 1 つに割り当てることができます。デフォルトでは、各コマンドは特権レベル 0 または 15 に割り当てられます。各ユーザーを特定の特権レベルに定義でき、各ユーザーは割り当てられた特権レベル以下のコマンドを入力できます。ASA は、ローカル データベース、RADIUS サーバー、または LDAP サーバー（LDAP 属性を RADIUS 属性にマッピングする場合）に定義されているユーザー特権レベルをサポートしています。

手順

ステップ 1 特権レベルにコマンドを割り当てます。

privilege [**show** | **clear** | **cmd**] **level** *level* [**mode** {**enable** | **cmd**}] **command** コマンド

例：

```
ciscoasa(config)# privilege show level 5 command filter
```

再割り当てする各コマンドに対してこのコマンドを繰り返します。

このコマンドのオプションは、次のとおりです。

- **show**|**clear**|**cmd**：これらのオプション キーワードを使用すると、コマンドの show、clear、または configure 形式に対してだけ特権を設定できます。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。これらのキーワードのいずれかを使用しない場合は、コマンドのすべての形式が影響を受けます。
- **level** *level*：0 ～ 15 の重大度。
- **mode** {**enable**|**configure**}：ユーザー EXEC モードまたは特権 EXEC モードおよびコンフィギュレーション モードでコマンドを入力することができ、そのコマンドが各モードで異なるアクションを実行する場合は、それらのモードの特権レベルを個別に設定することができます。
  - **enable**：ユーザー EXEC モードと特権 EXEC モードの両方を指定します。
  - **configure**：**configure terminal** コマンドを使用してアクセスされるコンフィギュレーション モードを指定します。
- **command** *command*：設定しているコマンド。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、

aaa authentication コマンドと **aaa authorization** コマンドのレベルを個別に設定できません。

ステップ 2 （任意） コマンド認可のための AAA ユーザーを有効にします。このコマンドを入力しない場合、ASA は、ローカル データベース ユーザーの特権レベルだけをサポートし、他のタイプのユーザーをすべてデフォルトでレベル 15 に割り当てます。

aaa authorization exec authentication-server [auto-enable]

例：

```
ciscoasa(config)# aaa authorization exec authentication-server
```

さらに、このコマンドは管理認証を有効にします。管理許可による CLI および ASDM アクセスの制限 （1522 ページ）を参照してください。

ステップ 3 ローカルのコマンド特権レベルの使用を有効にします。

aaa authorization command LOCAL

例：

```
ciscoasa(config)# aaa authorization command LOCAL
```

コマンド特権レベルを設定する場合は、このコマンドでコマンド許可を設定しない限り、コマンド許可は実行されません。

例

filter コマンドの形式は次のとおりです。

- **filter**（**configure** オプションにより表されます）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。次は、各形式を個別に設定する方法の例です。

```
ciscoasa(config)# privilege show level 5 command filter
ciscoasa(config)# privilege clear level 10 command filter
ciscoasa(config)# privilege cmd level 10 command filter
```

また、次の例では、すべての filter コマンドを同じレベルに設定する例を示します。

```
ciscoasa(config)# privilege level 5 command filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザー EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
ciscoasa(config)# privilege cmd level 0 mode enable command enable
ciscoasa(config)# privilege cmd level 15 mode cmd command enable
ciscoasa(config)# privilege show level 15 mode cmd command enable
```

次の例では、**mode** キーワードを使用する追加コマンド（**configure** コマンド）を示します。

```
ciscoasa(config)# privilege show level 5 mode cmd command configure
ciscoasa(config)# privilege clear level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode cmd command configure
ciscoasa(config)# privilege cmd level 15 mode enable command configure
```

（注） この最後の行は、**configure terminal** コマンドに関する行です。

TACACS+ サーバーでのコマンドの設定

グループまたは個々のユーザーの共有プロファイル コンポーネントとしての Cisco Secure Access Control Server（ACS）TACACS+ サーバーでコマンドを設定できます。サードパーティの TACACS+ サーバーの場合は、コマンド許可サポートの詳細については、ご使用のサーバーのマニュアルを参照してください。

Cisco Secure ACS バージョン 3.1 でコマンドを設定する場合は、次のガイドラインを参照してください。

- ASA は、シェル コマンドとして許可するコマンドを送信し、TACACS+ サーバーでシェル コマンドとしてコマンドを設定します。

（注） Cisco Secure ACS には、「pix-shell」と呼ばれるコマンド タイプが含まれている場合があります。このタイプは ASA コマンド許可に使用しないでください。

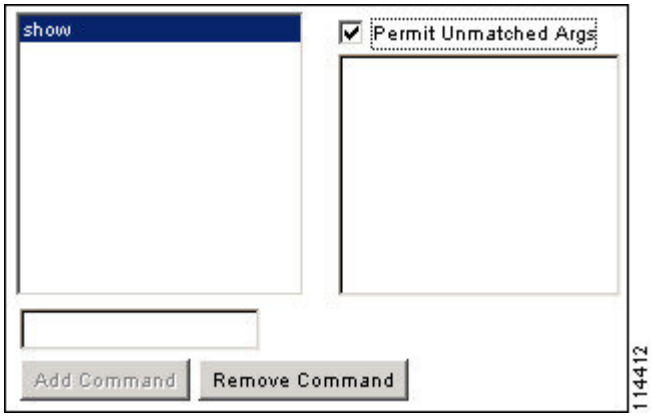
- コマンドの最初のワードは、メイン コマンドと見なされます。その他のワードはすべて引数と見なされます。これは、**permit** または **deny** の後に置く必要があります。

  たとえば、**show running-configuration aaa-server** コマンドを許可するには、コマンド フィールドに **show running-configuration** を追加し、引数フィールドに **permit aaa-server** を入力します。

- [Permit Unmatched Args] チェックボックスをオンにすると、明示的に拒否していないすべてのコマンド引数を許可できます。

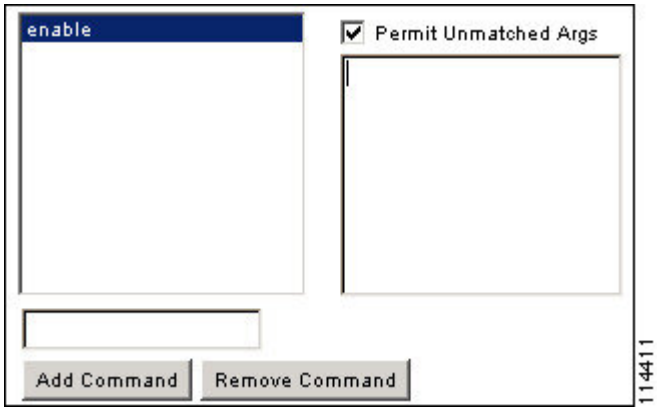
  たとえば、特定の **show** コマンドを設定するだけで、すべての **show** コマンドが許可されます。CLI の使用法を示す疑問符や省略形など、コマンドの変形をすべて予想する必要がなくなるので、この方法を使用することをお勧めします（次の図を参照）。

  図 ***86:*** 関連するすべてのコマンドの許可



- **enable** や **help** など、単一ワードのコマンドについては、そのコマンドに引数がない場合でも、一致しない引数を許可する必要があります（次の図を参照）。

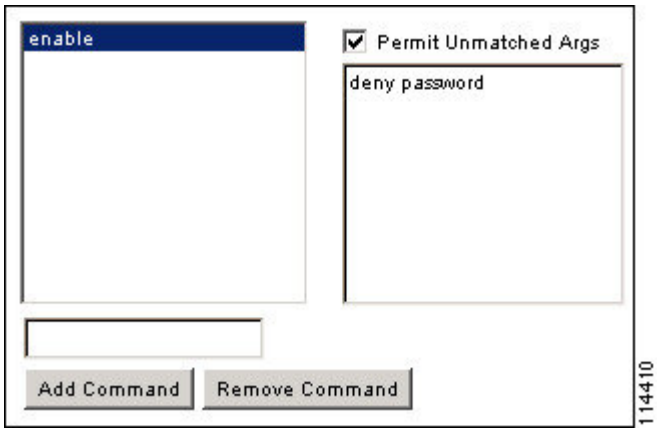
  図 ***87:*** 単一ワードのコマンドの許可



- 引数を拒否するには、その引数の前に **deny** を入力します。

  たとえば、**enable** コマンドを許可し、**enable password** コマンドを許可しない場合には、コマンドフィールドに **enable** を入力し、引数フィールドに **deny password** を入力します。**enable** だけが許可されるように、必ず、[Permit Unmatched Args] チェックボックスをオンにしてください（次の図を参照）。

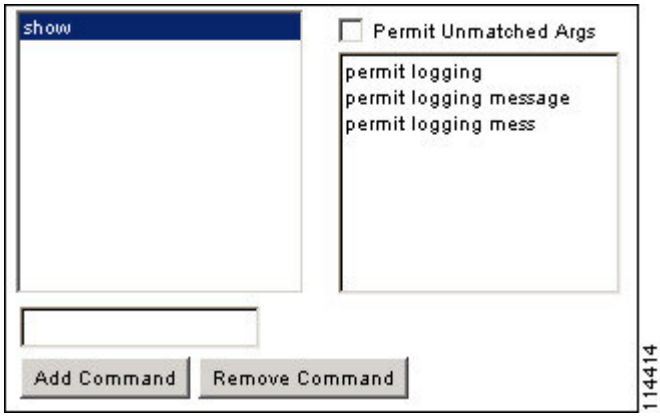
図 *88* : 引数の拒否



- コマンドラインでコマンドを省略形で入力した場合、ASA はプレフィックスとメイン コマンドを完全なテキストに展開しますが、その他の引数は入力したとおりに TACACS+ サーバーに送信します。

  たとえば、**sh log** と入力すると、ASA は完全なコマンド **show logging** を TACACS+ サーバーに送信します。一方、**sh log mess** と入力すると、ASA は展開されたコマンド **show logging message** ではなく、**show logging mess** を TACACS+ サーバーに送信します。省略形を予想して同じ引数の複数のスペルを設定できます（次の図を参照）。

図 *89* : 省略形の指定



- すべてのユーザーに対して次の基本コマンドを許可することをお勧めします。
  - **show checksum**
  - **show curpriv**
  - **イネーブル化**
  - **help**
  - **show history**
  - **login**

- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

TACACS+ コマンド許可の設定

TACACS+ コマンド認可をイネーブルにし、ユーザーが CLI でコマンドを入力すると、ASA はそのコマンドとユーザー名を TACACS+ サーバーに送信し、コマンドが認可されているかどうかを判別します。

TACACS+ コマンド許可をイネーブルにする前に、TACACS+ サーバーで定義されたユーザーとして ASA にログインしていること、および ASA の設定を続けるために必要なコマンド許可があることを確認してください。たとえば、すべてのコマンドが認可された管理ユーザーとしてログインする必要があります。このようにしないと、意図せずロックアウトされる可能性があります。

意図したとおりに機能することが確認できるまで、設定を保存しないでください。間違いによりロックアウトされた場合、通常はASAを再始動することによってアクセスを回復できます。

TACACS+ システムが完全に安定して信頼できることを確認します。必要な信頼性レベルについて、通常は、完全冗長 TACACS+ サーバー システムと ASA への完全冗長接続が必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続された 1 つのサーバとインターフェイス 2 に接続された別のサーバを含めます。TACACS+ サーバが使用できない場合にフォールバック方式としてローカル コマンド許可を設定することもできます。

TACACS+ サーバーを使用したコマンド許可を設定するには、次の手順を実行します。

手順

次のコマンドを入力します。

aaa authorization command *tacacs+_server_group* [**LOCAL**]

例：

```
ciscoasa(config)# aaa authorization command tacacs+_server_group [LOCAL]
```

TACACS+ サーバーを使用できない場合は、ローカル データベースをフォールバック方式として使用するように ASA を設定できます。フォールバックを有効にするには、サーバー グループ名の後ろに **LOCAL** を指定します（**LOCAL** は大文字と小文字を区別します）。ローカル データベースでは TACACS+ サーバーと同じユーザー名およびパスワードを使用することを推

奨します。これは、ASAのプロンプトでは、どの方式が使用されているかが示されないためです。必ずローカル データベースのユーザーとコマンド特権レベルを設定してください。

ローカル データベース ユーザーのパスワード ポリシーの設定

ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。

パスワード ポリシーはローカル データベースを使用する管理ユーザーに対してのみ適用されます。ローカルデータベースを使用するその他のタイプのトラフィック（VPNやAAAによるネットワーク アクセスなど）や、AAA サーバーによって認証されたユーザーには適用されません。

パスワードポリシーの設定後は、自分または別のユーザーのパスワードを変更すると、新しいパスワードに対してパスワードポリシーが適用されます。既存のパスワードについては、現行のポリシーが適用されます。新しいポリシーは、 **username** コマンドおよび **change-password** コマンドを使用したパスワードの変更に適用されます。

始める前に

- ローカルデータベースを使用してCLIまたはASDMアクセスのAAA認証を設定します。
- ローカル データベース内にユーザー名を指定します。

手順

ステップ 1 （オプション）リモート ユーザーのパスワードの有効期間を日数で設定します。

password-policy lifetime *days*

例：

```
ciscoasa(config)# password-policy lifetime 180
```

（注）
コンソール ポートを使用しているユーザーは、パスワードの有効期限が切れてもロックアウトされません。

有効な値は、0 ～ 65536 です。デフォルト値は 0 日です。この場合、パスワードは決して期限切れになりません。

パスワードの有効期限が切れる 7 日前に、警告メッセージが表示されます。パスワードの有効期限が切れると、リモート ユーザーのシステム アクセスは拒否されます。有効期限が切れた後アクセスするには、次のいずれかの手順を実行します。

- 他の管理者に **username** コマンドを使用してパスワードを変更してもらいます。
- 物理コンソール ポートにログインして、パスワードを変更します。

ステップ 2 （オプション）新しいパスワードと古いパスワードで違わなければならない最小文字数を設定します。

password-policy minimum-changes *value*

例：

```
ciscoasa(config)# password-policy minimum-changes 2
```

有効な値は、0 ～ 64 文字です。デフォルト値は 0 です

文字マッチングは位置に依存しません。したがって、新しいパスワードで使用される文字が、現在のパスワードのどこにも使用されていない場合に限り、パスワードが変更されたとみなされます。

ステップ 3 （オプション）パスワードの最小長を設定します。

password-policy minimum-length *value*

例：

```
ciscoasa(config)# password-policy minimum-length 8
```

有効な値は、3 ～ 64 文字です。推奨されるパスワードの最小長は 8 文字です。

ステップ 4 （オプション）パスワードに含める大文字の最小個数を設定します。

password-policy minimum-uppercase *value*

例：

```
ciscoasa(config)# password-policy  minimum-uppercase 3
```

有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 5 （オプション）パスワードに含める小文字の最小個数を設定します。

password-policy minimum-lowercase *value*

例：

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 6 （オプション）パスワードに含める数字の最小個数を設定します。

password-policy minimum-numeric *value*

例：

```
ciscoasa(config)# password-policy minimum-numeric 1
```

有効な値は、0 ～ 64 文字です。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 7 （オプション）パスワードに含める特殊文字の最小個数を設定します。

password-policy minimum-special *value*

例：

```
ciscoasa(config)# password-policy minimum-special 2
```

有効な値は、0 ～ 64 文字です。特殊文字には、!、@、#、$、%、^、&、*、(、および) が含まれます。デフォルト値は、最小個数がないことを意味する 0 です。

ステップ 8 パスワードを再利用を禁止します。

password-policy reuse-interval *value*

例：

```
ciscoasa(config)# password-policy reuse-interval 5
```

以前に使用された 2 ～ 7 個のパスワードと一致するパスワードの再利用を禁止することができます。以前のパスワードは、**password-history** コマンドを使用して、暗号化された形で各ユーザー名の設定に保存されます。このコマンドをユーザーが設定することはできません。

ステップ 9 ユーザー名と一致するパスワードを禁止します。

password-policy username-check

ステップ 10 （オプション）ユーザーが自分のパスワードの変更に **username** コマンドではなく **change-password** コマンドを使用する必要があるかを設定します。

password-policy authenticate enable

例：

```
ciscoasa(config)# password-policy authenticate enable
```

デフォルト設定はディセーブルです。どちらの方法でも、ユーザーはパスワードを変更することができます。

この機能を有効にして、**username** コマンドを使用してパスワードを変更しようとすると、次のエラー メッセージが表示されます。

```
ERROR: Changing your own password is prohibited
```

clear configure username コマンドを使用して自分のアカウントを削除することもできません。消去を試みた場合は、次のエラー メッセージが表示されます。

```
ERROR: You cannot delete all usernames because you are not allowed to delete yourself
```

パスワードの変更

パスワードポリシーでパスワードの有効期間を設定した場合、有効期間を過ぎるとパスワードを新しいパスワードに変更する必要があります。パスワードポリシー認証をイネーブルにした場合は、このパスワード変更のスキームが必須です。パスワードポリシー認証がイネーブルでない場合は、このメソッドを使用することも、直接ユーザーアカウントを変更することもできます。

username パスワードを変更するには、次の手順を実行します。

手順

次のコマンドを入力します。

change-password [**old-password** *old_password* [**new-password** *new_password*]]

例：

```
ciscoasa# change-password old-password j0hncr1chton new-password a3rynsun
```

コマンドに新旧のパスワードを入力していない場合は、ASA によって入力が求められます。

ログインの履歴を有効にして表示する

デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。

始める前に

- ログイン履歴はユニット（装置）ごとに保存されます。フェールオーバーおよびクラスタリング環境では、各ユニットが自身のログイン履歴のみを保持します。
- ログインの履歴データは、リロードされると保持されなくなります。
- 1 つ以上の CLI 管理方式（SSH、Telnet、シリアル コンソール）でローカル AAA 認証をイネーブルにした場合、AAA サーバのユーザ名またはローカル データベースのユーザ名にこの機能が適用されます。ASDM のログインは履歴に保存されません。

手順

ステップ 1 ログインの履歴の期間を次のように設定します。

aaa authentication login-history duration *days*

例：

```
ciscoasa(config)# aaa authentication login-history duration 365
```

days を 1 ～ 365 日に設定できます。デフォルトは 90 です。ログイン履歴を無効にするには、**no aaa authentication login-history** を入力します。

ユーザーがログインすると、以下の SSH の例のように、自身のログイン履歴が表示されます。

```
cugel@10.86.194.108's password:
The privilege level for user cugel is 15.  The privilege level at the previous login was
 2.
User cugel logged in to ciscoasa at 21:04:10 UTC Dec 14 2016
Last login: 21:01:44 UTC Dec 14 2016 from ciscoasa console
Successful logins over the last 90 days: 6
Authentication failures since the last login: 0
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 2 ログイン履歴を次のように表示します。

show aaa login-history [**user** *name*]

例：

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

管理アクセス アカウンティングの設定

CLI で **show** コマンド以外のコマンドを入力する場合、アカウンティング メッセージを TACACS+ アカウンティング サーバーに送信できます。ユーザーがログインするとき、ユーザーが **enable** コマンドを入力するとき、またはユーザーがコマンドを発行するときのアカウンティングを設定できます。

コマンド アカウンティングに使用できるサーバーは、TACACS+ だけです。

管理アクセスおよびイネーブル コマンド アカウンティングを設定するには、次の手順を実行します。

手順

ステップ 1 次のコマンドを入力します。

aaa accounting {**serial** | **telnet** | **ssh** | **enable**} **console** *server-tag*

例：

```
ciscoasa(config)# aaa accounting telnet console group_1
```

有効なサーバー グループ プロトコルは RADIUS と TACACS+ です。

ステップ 2 コマンドアカウンティングをイネーブルにします。TACACS+サーバーだけがコマンドアカウンティングをサポートします。

aaa accounting command [**privilege** *level*] *server-tag*

例：

```
ciscoasa(config)# aaa accounting command privilege 15 group_1
```

privilege *level* というキーワードと引数のペアは最小特権レベルであり、*server-tag* 引数は ASA がコマンドアカウンティング メッセージを送信する TACACS+サーバー グループの名前です。

ロックアウトからの回復

状況によっては、コマンド許可やCLI認証をオンにすると、ASA CLIからロックアウトされる場合があります。通常は、ASAを再起動することによってアクセスを回復できます。ただし、すでにコンフィギュレーションを保存した場合は、ロックアウトされたままになる可能性があります。

次の表に、一般的なロックアウト条件とその回復方法を示します。

表 *57 : CLI* 認証およびコマンド許可のロックアウト シナリオ

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル CLI 認証	ローカル データベースにユーザーが設定していない。	ローカル データベース内にユーザーが存在しない場合は、ログインできず、ユーザーの追加もできません。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザーを追加することができます。
TACACS+ コマンド許可 TACACS+ CLI 認証 RADIUS CLI 認証	サーバーがダウンしているか到達不能で、フォールバック方式を設定していない。	サーバーが到達不能である場合は、ログインもコマンドの入力もできません。	**1.** ログインし、パスワードと AAA コマンドをリセットします。 **2.** サーバーがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。	**1.** ASA でネットワーク コンフィギュレーションが正しくないためにサーバーが到達不能である場合は、スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてネットワークを再設定することができます。 **2.** サーバーがダウンしたときにロックアウトされないように、ローカル データベースをフォールバック方式として設定します。
TACACS+ コマンド許可	十分な特権のないユーザーまたは存在しないユーザーとしてログインした。	コマンド許可がイネーブルになりますが、ユーザーはこれ以上コマンドを入力できなくなります。	TACACS+ サーバーのユーザー アカウントを修正します。 TACACS+ サーバーへのアクセス権がなく、ASA をすぐに設定する必要がある場合は、メンテナンス パーティションにログインして、パスワードと **aaa** コマンドをリセットします。	スイッチから ASA へのセッションを接続します。システム実行スペースから、コンテキストに切り替えてコンフィギュレーションの変更を完了することができます。また、TACACS+ コンフィギュレーションを修正するまでコマンド許可をディセーブルにすることもできます。

機能	ロックアウト条件	説明	対応策：シングル モード	対応策：マルチ モード
ローカル コマンド許可	十分な特権のないユーザーとしてログインしている。	コマンド許可がイネーブルになりますが、ユーザーはこれ以上コマンドを入力できなくなります。	ログインし、パスワードと **aaa** コマンドをリセットします。	スイッチからASAへのセッションを接続します。システム実行スペースから、コンテキストに切り替えてユーザー レベルを変更することができます。

デバイス アクセスのモニタリング

デバイス アクセスのモニタリングについては、次のコマンドを参照してください。

- **show running-config all privilege all**

  このコマンドは、すべてのコマンドの特権レベルを表示します。

  show running-config all privilege all コマンドの場合、ASA は特権レベルに対する各 CLI コマンドの現在の割り当てを表示します。次に、このコマンドの出力例を示します。

```
ciscoasa(config)# show running-config all  privilege all
privilege show level 15 command aaa
privilege clear level 15 command aaa
privilege configure level 15 command aaa
privilege show level 15 command aaa-server
privilege clear level 15 command aaa-server
privilege configure level 15 command aaa-server
privilege show level 15 command access-group
privilege clear level 15 command access-group
privilege configure level 15 command access-group
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
privilege show level 15 command activation-key
privilege configure level 15 command activation-key
...
```

- **show running-config privilege level** *level*

  このコマンドは、特定の特権レベルのコマンドを示します。level 引数は、0 ～ 15 の範囲の整数になります。

  次の例は、特権レベル 10 に対するコマンド割り当てを示しています。

```
ciscoasa(config)# show running-config all privilege level 10
privilege show level 10 command aaa
```

- **show running-config privilege command** コマンド

  このコマンドは、特定のコマンドの特権レベルを表示します。

次の例は、**access-list** コマンドに対するコマンド割り当てを示しています。

```
ciscoasa(config)# show running-config all privilege command access-list
privilege show level 15 command access-list
privilege clear level 15 command access-list
privilege configure level 15 command access-list
```

- **show curpriv**

  このコマンドは、現在のログイン ユーザーを表示します。

  次に、**show curpriv** コマンドの出力例を示します。

```
ciscoasa# show curpriv
Username: admin
Current privilege level: 15
Current Mode/s: P_PRIV
```

  次の表で、**show curpriv** コマンドの出力について説明します。

  表 *58 : show curpriv* コマンド出力の説明

フィールド	説明
ユーザ名	[Username]。デフォルトユーザーとしてログインすると、名前は enable_1（ユーザー EXEC）または enable_15（特権 EXEC）になります。
Current privilege level	レベルの範囲は 0 ～ 15 です。ローカル コマンド許可を設定してコマンドを中間特権レベルに割り当てない限り、使用されるレベルはレベル 0 と 15 だけです。
Current Modes	使用可能なアクセス モードは次のとおりです。 • P_UNPR：ユーザー EXEC モード（レベル 0 と 1） • P_PRIV：特権 EXEC モード（レベル 2 ～ 15） • P_CONF：コンフィギュレーション モード

- **show quota management-session** [**ssh** | **telnet** | **http** | **username** *user*]

  このコマンドは、使用中の現在のセッションを表示します。

  次に、**show quota management-session** コマンドの出力例を示します。

```
ciscoasa(config)#show quota management-session

#Sessions               ConnectionType                 Username
1                             SSH                       cisco
2                             TELNET                    cisco
1                             SSH                       cisco1
```

- **show aaa login-history** [**user** *name*]

このコマンドは、ユーザーごとのログイン履歴を表示します。

次に、**show aaa login-history** コマンドの出力例を示します。

```
ciscoasa(config)# show aaa login-history
Login history for user:    turjan
Logins in last   1 days:   1
Last successful login:     16:44:32 UTC Jul 23 2018 from console
Failures since last login: 0
Last failed login:         None
Privilege level:                                    14
Privilege level changed from 11 to 14 at:           14:07:30 UTC Aug 21 2018
```

管理アクセスの履歴

表 *59* : 管理アクセスの履歴

機能名	プラットフォーム リリース	説明
ASA SSH スタックが廃止されました	9.23(1)	ASA SSH スタックを使用できなくなります。Cisco SSH スタックが唯一のスタックになりました。 新規/変更されたコマンド： **ssh stack ciscossh**
CiscoSSH スタックのデフォルト化	9.19(1)	Cisco SSH スタックがデフォルトで使用されるようになりました。 新規/変更されたコマンド： **ssh stack ciscossh**
SSH と Telnet のループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、次の機能に使用できるようになりました。 • SSH • Telnet 新規/変更されたコマンド：**interface loopback**、**ssh**、**telnet**

機能名	プラットフォーム リリース	説明
CiscoSSH スタック	9.17(1)	ASA は、SSH 接続に独自の SSH スタックを使用します。代わりに、OpenSSH に基づく CiscoSSH スタックを使用するように選択できるようになりました。デフォルトスタックは引き続き ASA スタックです。Cisco SSH は次をサポートします。 • FIPS の準拠性 • シスコおよびオープンソースコミュニティからの更新を含む定期的な更新 CiscoSSH スタックは次をサポートしないことに注意してください。 • VPN を介した別のインターフェイスへの SSH（管理アクセス） • EdDSA キーペア • FIPS モードの RSA キーペア これらの機能が必要な場合は、引き続き ASA SSH スタックを使用する必要があります。 CiscoSSH スタックでは、SCP 機能に若干の変更があります。ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、**ssh** コマンドを使用して、ASA で SCP サーバサブネット/ホストの SSH アクセスを有効にする必要があります。 新規/変更されたコマンド： **ssh stack ciscossh**
ローカルユーザーのロックアウトの変更	9.17(1)	設定可能な回数のログイン試行に失敗すると、ASA はローカルユーザーをロックアウトする場合があります。この機能は、特権レベル 15 のユーザーには適用されませんでした。また、管理者がアカウントのロックを解除するまで、ユーザーは無期限にロックアウトされます。管理者がその前に **clear aaa local user lockout** コマンドを使用しない限り、ユーザーは 10 分後にロック解除されるようになりました。特権レベル 15 のユーザーも、ロックアウト設定が適用されるようになりました。 新規/変更されたコマンド：**aaa local authentication attempts max-fail** 、**show aaa local user**

機能名	プラットフォーム リリース	説明
SSH および Telnet パスワード変更プロンプト	9.17(1)	ローカルユーザーが SSH または Telnet を使用して ASA に初めてログインすると、パスワードを変更するように求められます。また、管理者がパスワードを変更した後、最初のログインに対してもプロンプトが表示されます。ただし、ASA がリロードすると、最初のログインであっても、ユーザーにプロンプトは表示されません。 VPN などのローカル ユーザー データベースを使用するサービスは、SSH または Telnet ログイン中に変更された場合、新しいパスワードも使用する必要があることに注意してください。 新規/変更されたコマンド： **show aaa local user**
SSH セキュリティの改善	9.16(1)	SSH が次の SSH セキュリティの改善をサポートするようになりました。 • ホストキーの形式：**crypto key generate** {**eddsa** | **ecdsa**}。RSA に加えて、EdDSA および ECDSA ホストキーのサポートが追加されました。ASA は、存在する場合、EdDSA、ECDSA、RSA の順にキーの使用を試みます。**ssh key-exchange hostkey rsa** コマンドで RSA キーを使用するように ASA を明示的に設定する場合は、2048 ビット以上のキーを生成する必要があります。アップグレードの互換性のために、ASA はデフォルトのホストキー設定が使用されている場合にのみ、より小さい RSA ホストキーを使用します。RSA のサポートは今後のリリースで削除されます。 • キー交換アルゴリズム：**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**} • 暗号化アルゴリズム：**ssh cipher encryption chacha20-poly1305@openssh.com** • SSH バージョン 1 はサポートされなくなりました。**ssh version** コマンドは削除されました。 新規/変更されたコマンド：**crypto key generate eddsa**、**crypto key zeroize eddsa**、**show crypto key mypubkey**、**ssh cipher encryption chacha20-poly1305@openssh.com**、**ssh key-exchange group** {**ecdh-sha2-nistp256** | **curve25519-sha256**}、**ssh key-exchange hostkey**、**ssh version**

機能名	プラットフォーム リリース	説明
SNMP 向け管理アクセス	9.14(2)	サイト間 VPN 経由のセキュアな SNMP ポーリングを実現するための VPN 設定の一環として、VPN トンネル経由の管理アクセスを設定する際に、外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。
HTTPS アイドルタイムアウトの設定	9.14(1)	ASDM、WebVPN、および他のクライアントを含む、ASA へのすべての HTTPS 接続のアイドルタイムアウトを設定できるようになりました。これまでは、**http server idle-timeout** コマンドを使用して ASDM アイドルタイムアウトを設定することしかできませんでした。両方のタイムアウトを設定した場合は、新しいコマンドによる設定が優先されます。 新規/変更されたコマンド：**http connection idle-timeout**
事前定義されたリストに応じて最も高いセキュリティから最も低いセキュリティへという順序で SSH 暗号化の暗号を表示	9.13(1)	事前定義されたリストに応じて、SSH 暗号化の暗号が最も高いセキュリティから最も低いセキュリティへという順序（中または高）で表示されるようになりました。以前のリリースでは、最も低いものから最も高いものへの順序でリストされており、セキュリティが高い暗号よりも低い暗号が先に表示されていました。 新規/変更されたコマンド：**ssh cipher encryption**
SSH キー交換モードの設定は、管理コンテキストに限定されています。	9.12(2)	管理コンテキストでは SSH キー交換を設定する必要があります。この設定は、他のすべてのコンテキストによって継承されます。 新規/変更されたコマンド：**ssh key-exchange**
enable ログイン時のパスワードの変更が必須に	9.12(1)	デフォルトの **enable** のパスワードは空白です。ASA で特権 EXEC モードへのアクセスを試行する場合に、パスワードを 3 文字以上の値に変更することが必須となりました。空白のままにすることはできません。**no enable password** コマンドは現在サポートされていません。 CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザー）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブル パスワードを設定する必要があります。 このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザー名を使用せず **enable** パスワードを使用してログインすることができます。 新規/変更されたコマンド：**enable password**

機能名	プラットフォーム リリース	説明
管理セッションの設定可能な制限	9.12(1)	集約、ユーザー単位、およびプロトコル単位の管理セッションの最大数を設定できます。これまでは、セッションの集約数しか設定できませんでした。この機能がコンソール セッションに影響を与えることはありません。マルチ コンテキスト モードでは HTTPS セッションの数を設定することはできず、最大セッション数は 5 で固定されています。また、**quota management-session** コマンドはシステム コンフィギュレーションでは受け入れられず、代わりにコンテキスト コンフィギュレーションで使用できるようになっています。集約セッションの最大数が 15 になりました。0（無制限）または16以上に設定してアップグレードすると、値は 15 に変更されます。 新規/変更されたコマンド：**quota management-session**、**show quota management-session**
管理権限レベルの変更通知	9.12(1)	有効なアクセス（**aaa authentication enable console**）を認証するか、または特権 EXEC への直接アクセス（**aaa authorization exec auto-enable**）を許可すると、前回のログイン以降に割り当てられたアクセス レベルが変更された場合に ASA からユーザーへ通知されるようになりました。 新規/変更されたコマンド： **show aaa login-history**
SSH によるセキュリティの強化	9.12(1)	次の SSH セキュリティの改善を参照してください。 • Diffie-Hellman Group 14 SHA256 キー交換のサポート。この設定がデフォルトになりました。以前のデフォルトはGroup 1 SHA1 でした。 • HMAC-SHA256整合性暗号のサポート。デフォルトは、高セキュリティの暗号セット（hmac-sha2-256 のみ）になりました。以前のデフォルトは中程度のセットでした。 新規/変更されたコマンド：**ssh cipher integrity** 、**ssh key-exchange group dh-group14-sha256**
非ブラウザベースの HTTPS クライアントによる ASA へのアクセスの許可	9.12(1)	非ブラウザベースの HTTPS クライアントが ASA 上の HTTPS サービスにアクセスできるようにすることができます。デフォルトでは、ASDM、CSM、および REST API が許可されています。 新規/変更されたコマンド： **http server basic-auth-client**
RSA キー ペアは 3072 ビット キーをサポートしています	9.9(2)	モジュラス サイズを 3072 に設定できるようになりました。 新規または変更されたコマンド：**crypto key generate rsa modulus**

機能名	プラットフォーム リリース	説明
ブリッジ型仮想インターフェイス（BVI）の VPN 管理アクセス	9.9(2)	VPN の **management-access** がその BVI で有効になっている場合、**telnet**、**http**、**ssh** などの管理サービスを BVI で有効にできるようになりました。非 VPN 管理アクセスの場合は、ブリッジ グループ メンバ インターフェイスでこれらのサービスの設定を続行する必要があります。 新規または変更されたコマンド：**https**、**telnet**、**ssh**、**management-access**
SSH バージョン 1 の廃止	9.9(1)	SSH バージョン 1 は廃止され、今後のリリースで削除される予定です。デフォルト設定が SSH v1 と v2 の両方から SSH v2 のみに変更されました。 新規/変更されたコマンド： **ssh version**
SSH 公開キー認証を使用するユーザーの認証とパスワードを使用するユーザーの認証を区別します。	9.6(3)/9.8(1)	9.6(2) より前のリリースでは、ローカル ユーザー データベース（**ssh authentication**）を使用して AAA SSH 認証を明示的に有効にしなくても、SSH 公開キー認証（**aaa authentication ssh console LOCAL**）を有効にすることができました。9.6(2) では、ASA で AAA SSH 認証を明示的に有効にする必要がありました。このリリースでは、AAA SSH 認証を明示的に有効にする必要はありません。ユーザーに対して **ssh authentication** コマンドを設定すると、このタイプの認証を使用するユーザーのローカル認証がデフォルトで有効になります。さらに、明示的に AAA SSH 認証を設定すると、この設定はパスワード付きのユーザー名にのみ適用されます。また、任意の AAA サーバー タイプ（**aaa authentication ssh console radius_1** など）を使用できます。たとえば、一部のユーザーはローカル データベースを使用して公開キー認証を使用し、他のユーザーは RADIUS でパスワードを使用できます。 変更されたコマンドはありません。
ログイン履歴	9.8(1)	デフォルトでは、ログイン履歴は 90 日間保存されます。この機能を無効にするか、期間を最大 365 日まで変更できます。1 つ以上の管理メソッド（SSH、ASDM、Telnet など）でローカル AAA 認証を有効にしている場合、この機能はローカル データベースのユーザー名にのみ適用されます。 次のコマンドが導入されました。**aaa authentication login-history**、**show aaa login-history**

機能名	プラットフォーム リリース	説明
パスワードの再利用とユーザー名と一致するパスワードの使用を禁止するパスワード ポリシーの適用	9.8(1)	最大7世代にわたるパスワードの再利用と、ユーザー名と一致するパスワードの使用を禁止できるようになりました。 次のコマンドが導入されました。**password-history**、**password-policy reuse-interval**、**password-policy username-check**
ASDM に対する ASA SSL サーバー モード マッチング	9.6(2)	証明書マップと照合するために、証明書で認証を行うASDMユーザーに対して証明書を要求できるようになりました。 次のコマンドを変更しました。**http authentication-certificate match**
SSH 公開キー認証の改善	9.6(2)	以前のリリースでは、ローカル ユーザー データベース（(**aaa authentication ssh console LOCAL**)）を使用して AAA SSH 認証を有効にしなくても、SSH 公開キー認証（(**ssh authentication**)）を有効にすることができました。この設定は修正されたため、AAA SSH認証を明示的に有効にする必要があります。ユーザーが秘密キーの代わりにパスワードを使用できないよう、パスワード未定義のユーザー名を作成できるようになりました。 次のコマンドが変更されました。**ssh authentication**、**username**
ASDM 管理認証	9.4(1)	HTTP アクセスと Telnet および SSH アクセス別に管理認証を設定できるようになりました。 次のコマンドが導入されました。 **aaa authorization http console**
証明書コンフィギュレーションの ASDM ユーザー名	9.4(1)	ASDM の証明書認証（**http authentication-certificate**）を有効にすると、ASDM が証明書からユーザー名を抽出する方法を設定できます。また、ログイン プロンプトでユーザー名を事前に入力して表示できます。 次のコマンドが導入されました。**http username-from-certificate**
改善されたワンタイム パスワード認証	9.2(1)	十分な認可特権を持つ管理者は、認証クレデンシャルを一度入力すると特権 EXEC モードに移行できます。**auto-enable** オプションが **aaa authorization exec** コマンドに追加されました。 次のコマンドが変更されました。**aaa authorization exec**。
HTTP リダイレクトの IPv6 サポート	9.1(7)/9.6(1)	ASDM アクセスまたはクライアントレス SSL VPN 用の HTTPS に HTTP リダイレクトを有効にすると、IPv6 アドレスへ送信されるトラフィックもリダイレクトできるようになりました。 次のコマンドに機能が追加されました。**http redirect**

機能名	プラットフォーム リリース	説明
設定可能なSSH暗号機能と整合性アルゴリズム	9.1(7.4)、9.3(3)、9.6(1)	ユーザーはSSH暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対してHMACと暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASAは3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctrの順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbcなどの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc**を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**。
SSH の AES-CTR 暗号化	9.1(2)	ASA での SSH サーバの実装が、AES-CTR モードの暗号化をサポートするようになりました。
SSH キー再生成間隔の改善	9.1(2)	SSH 接続は、接続時間 60 分間またはデータ トラフィック 1 GB ごとに再生成されます。 次のコマンドが導入されました。**show ssh sessions detail**。
マルチ コンテキスト モードの ASASM において、スイッチからの Telnet 認証および仮想コンソール認証をサポートしました。	8.5(1)	マルチ コンテキスト モードのスイッチから ASASM への接続はシステム実行スペースに接続しますが、これらの接続を制御するために管理コンテキストでの認証を設定できます。
ローカルデータベースを使用する場合の管理者パスワードポリシーのサポート	8.4(4.1)、9.1(2)	ローカル データベースを使用して CLI または ASDM アクセスの認証を設定する場合は、指定期間を過ぎるとユーザーにパスワードの変更を要求し、パスワードの最短長と最低変更文字数などのパスワード標準に従うことを要求するパスワード ポリシーを設定できます。 次のコマンドが導入されました。**change-password**、**password-policy lifetime**、**password-policy minimum changes**、**password-policy minimum-length**、**password-policy minimum-lowercase**、**password-policy minimum-uppercase**、**password-policy minimum-numeric**、**password-policy minimum-special**、**password-policy authenticate enable**、**clear configure password-policy**、**show running-config password-policy**.

機能名	プラットフォーム リリース	説明
SSH 公開キー認証のサポート	8.4(4.1)、9.1(2)	ASA への SSH 接続の公開キー認証は、ユーザー単位で有効にできます。公開キー ファイル（PKF）でフォーマットされたキーまたは Base64 キーを指定できます。PKF キーは、4096 ビットまで使用できます。ASA がサポートする Base64 形式（最大 2048 ビット）では大きすぎるキーについては、PKF 形式を使用します。 次のコマンドが導入されました。**ssh authenticaion**。 *PKF* キー形式のサポートは *9.1(2)* 以降のみです。
SSH キー交換の Diffie-Hellman グループ 14 のサポート	8.4(4.1)、9.1(2)	SSH キー交換に Diffie-Hellman グループ 14 が追加されました。これまでは、グループ 1 だけがサポートされていました。 次のコマンドが導入されました。**ssh key-exchange**。
管理セッションの最大数のサポート	8.4(4.1)、9.1(2)	同時 ASDM、SSH、Telnet セッションの最大数を設定できます。 次のコマンドが導入されました。**quota management-session**、**show running-config quota management-session**、**show quota management-session**。
SSH セキュリティが向上し、SSH デフォルトユーザー名はサポートされなくなりました。	8.4(2)	8.4(2) 以降、pix または asa ユーザー名とログイン パスワードで SSH を使用して ASA に接続することができなくなりました。SSH を使用するには、**aaa authentication ssh console LOCAL** コマンド（CLI）または [Configuration] > [Device Management] > [Users/AAA] > [AAA Access] > [Authentication (ASDM)] を使用して AAA 認証を設定してから、ローカルユーザーを定義する必要があります。定義するには、**username** コマンド（CLI）を入力するか、[Configuration] > [Device Management] > [Users/AAA] > [User Accounts (ASDM)] を選択します。ローカル データベースの代わりに AAA サーバを認証に使用する場合、ローカル認証もバックアップの手段として設定しておくことをお勧めします。

機能名	プラットフォーム リリース	説明
管理アクセス	7.0(1)	この機能が導入されました。 次のコマンドを導入しました。 **show running-config all privilege all**、**show running-config privilege level**、**show running-config privilege command**、**telnet**、**telnet timeout**、**ssh**、**ssh timeout**、**http**、**http server enable**、**asdm image disk**、**banner**、**console timeout**、**icmp**、**ipv6 icmp**、**management access**、**aaa authentication console**、**aaa authentication enable console**、**aaa authentication telnet | ssh console**、**service-type**、**login**、**privilege**、**aaa authentication exec authentication-server**、**aaa authentication command LOCAL**、**aaa accounting serial | telnet | ssh | enable console**、**show curpriv**、**aaa accounting command privilege**。

第 43 章

ソフトウェアおよびコンフィギュレーション

この章では、ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

- ソフトウェアのアップグレード （1553 ページ）
- ROMMON を使用したイメージのロード（ISA 3000） （1553 ページ）
- ROMMON イメージのアップグレード（ISA 3000） （1555 ページ）
- ソフトウェアのダウングレード （1557 ページ）
- ファイルの管理 （1563 ページ）
- ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定 （1573 ページ）
- コンフィギュレーションまたはその他のファイルのバックアップと復元 （1577 ページ）
- Cisco Secure Firewall 3100/4200 での SSD のホットスワップ （1596 ページ）
- USB ポートの無効化 （1598 ページ）
- ソフトウェアとコンフィギュレーションの履歴 （1600 ページ）

ソフトウェアのアップグレード

完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON を使用したイメージのロード（ISA 3000）

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 ISA 3000 コンソールへのアクセス （13 ページ）に従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

（注）
ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、ASA 5516-X、および ISA 3000 プラットフォームで無視されるため、これらのプラットフォームで Management 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

ステップ 5 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6 TFTP サーバーに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
```

```
Updating NVRAM Parameters...
```

ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON イメージのアップグレード（ISA 3000）

ISA 3000 の ROMMON イメージをアップグレードするには、次の手順に従います。 ASA モデルの場合、システムの ROMMON バージョンは 1.1.8 以上である必要があります。最新バージョンへのアップグレードを推奨します。

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。

⚠

注意 ISA 3000 の ROMMON 1.0.5 へのアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカル サポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

始める前に

Cisco.com から新しい ROMMON イメージを取得して、サーバー上に置いて ASA にコピーします。ASA は、FTP サーバー、TFTP サーバー、SCP サーバー、HTTP（S）サーバー、および SMB サーバーをサポートしています。次の URL からイメージをダウンロードします。

- ISA 3000： https://software.cisco.com/download/home/286288493/type

手順

ステップ 1 ROMMON イメージを ASA フラッシュ メモリにコピーします。この手順では、FTP コピーを表示します。他のサーバータイプのシンタックスの場合は **copy ?** と入力します。

copy ftp://[*username*:*password*@]*server_ip*/**asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

ステップ 2 現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

ステップ 3 ROMMON イメージをアップグレードします。

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
```

```
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASA が ROMMON イメージをアップグレードして、その後オペレーティングシステムをリロードします。

ソフトウェアのダウングレード

多くの場合、ASA ソフトウェアをダウングレードし、以前のソフトウェアバージョンからバックアップ設定を復元することができます。ダウングレードの方法は、ASA プラットフォームによって異なります。

ダウングレードに関するガイドラインおよび制限事項

ダウングレードする前に、次のガイドラインを参照してください。

- **クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません**：ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
  - **クラスタリングを含む 9.9(1) より前のリリースへのダウングレード**：9.9(1) 以降では、バックアップの配布が改善されています。クラスタに 3 つ以上のユニットがある場合は、次の手順を実行する必要があります。
    1. クラスタからすべてのセカンダリ ユニットを削除します（クラスタはプライマリ ユニットのみで構成されます）。
    2. 1 つのセカンダリ ユニットをダウングレードし、クラスタに再参加させます。
    3. プライマリ ユニットでクラスタリングを無効にします。そのユニットをダウングレードし、クラスタに再参加させます。
    4. 残りのセカンダリ ユニットをダウングレードし、それらを一度に 1 つずつクラスタに再参加させます。
  - **クラスタサイトの冗長性を有効にする場合は、9.9(1) より前のリリースにダウングレードします**：ダウングレードする場合（または 9.9(1) より前のユニットをクラスタに追加する場合）は、サイトの冗長性を無効にする必要があります。そうしないと、古いバージョンを実行しているユニットにダミーの転送フローなどの副作用が発生します。

- **クラスタリングおよび暗号マップを使用する場合に 9.8(1) からダウングレードする**：暗号マップが設定されている場合に9.8(1)からダウングレードすると、ゼロ ダウンタイム ダウングレードはサポートされません。ダウングレード前に暗号マップ設定をクリアし、ダウングレード後に設定をもう一度適用する必要があります。
- **クラスタリングユニットのヘルスチェックを 0.3 ～ 0.7 秒に設定した状態で 9.8(1) からダウングレードする**：（**health-check holdtime** で）ホールド時間を 0.3 ～ 0.7 秒に設定した後で ASA ソフトウェアをダウングレードすると、新しい設定はサポートされないため、設定値はデフォルトの 3 秒に戻ります。
- **クラスタリング（CSCuv82933）を使用している場合に 9.5(2) 以降から 9.5(1) 以前にダウングレードする**：9.5(2)からダウングレードする場合、ゼロ ダウンタイム ダウングレードはサポートされません。ユニットがオンラインに戻ったときに新しいクラスタが形成されるように、すべてのユニットをほぼ同時にリロードする必要があります。ユニットが順番にリロードされるのを待つと、クラスタを形成できなくなります。
- **クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする**：ゼロ ダウンタイム ダウングレードはサポートされません。

- **9.22 以降からのダウングレードの問題**：usb-port disable コマンドを使用して USB ポートを無効にした後、以前のリリースにダウングレードすると、ポートは無効のままになり、再度有効にするには NVRAM（FXOS local-mgmt **erase secure all** コマンド）を消去する必要があります。
- **9.18 以降からのダウングレードの問題**：9.18 では動作が変更され、**access-group** コマンドがその **access-list** コマンドの前にリストされます。ダウングレードすると、**access-group** コマンドはまだ **access-list** コマンドをロードしていないため拒否されます。以前に **forward-reference enable** コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての **access-group** コマンドを手動でコピーし、ダウングレード後に再入力してください。
- **スマートライセンスの 9.10(1) からのダウングレード**：スマートエージェントの変更により、ダウングレードする場合、デバイスを Cisco Smart Software Manager に再登録する必要があります。新しいスマートエージェントは暗号化されたファイルを使用するので、古いスマートエージェントが必要とする暗号化されていないファイルを使用するために再登録する必要があります。
- **PBKDF2（パスワードベースのキー派生関数 2）ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする**：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。9.7(1) では、すべての新しいパスワードは、長さに関わらず PBKDF2 ハッシュを使用します（既存のパスワードは引き続き MD5 ハッシュを使用します）。ダウングレードすると、**enable** パスワードがデフォルト（空白）に戻ります。ユーザー名は正しく解析されず、**username** コマンドが削除されます。ローカルユーザーをもう一度作成する必要があります。

- **ASA 仮想 用のバージョン 9.5(2.200) からのダウングレード**：ASA 仮想 はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。
- **元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます**：このシナリオは、ダウングレード時に発生します。その場合、VPN接続を切断して再接続してください。
- **バージョン 9.23（1）から以前のバージョンへの柔軟な永続ライセンス予約を備えた ASA 仮想 のダウングレード**：バージョン 9.23（1）および柔軟な永続ライセンス予約で ASA 仮想 をダウングレードしないことをお勧めします。ライセンス登録状態は **[未登録（Unregistered）]**になります。

ダウングレード後に削除される互換性のない設定

以前のバージョンにダウングレードすると、それ以降のバージョンで導入されたコマンドは設定から削除されます。ダウングレードする前に、ターゲットバージョンに対して設定を自動的にチェックする方法はありません。新しいコマンドが ASA の新しい機能にいつ追加されたかをリリースごとに表示できます。

show startup-config errors コマンドを使用してダウングレードした後、拒否されたコマンドを表示できます。ラボデバイスでダウングレードを実行できる場合は、実稼働デバイスでダウングレードを実行する前にこのコマンドを使用して効果を事前に確認できます。

場合によっては、ASAはアップグレード時にコマンドを新しいフォームに自動的に移行するため、バージョンによっては新しいコマンドを手動で設定しなかった場合でも、設定の移行によってダウングレードが影響を受けることがあります。ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。ダウングレードに影響する可能性がある自動コマンド移行の詳細については、『ASAアップグレードガイド』の「バージョン固有のガイドラインと移行」を参照してください。

ダウングレードに関するガイドラインおよび制限事項（1557ページ）の既知のダウングレードの問題も参照してください。

たとえば、バージョン9.8(2) を実行している ASA には、次のコマンドが含まれています。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
```

9.0(4) にダウングレードすると、起動時に次のエラーが表示されます。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
```

```
                                    ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
                                          ^
ERROR: % Invalid input detected at '^' marker.
```

この例では、**access-list extended** コマンドでの **sctp** のサポートがバージョン 9.5(2) で、**username** コマンドでの **pbkdf2** のサポートがバージョン 9.6(1) で、**snmp-server user** コマンドでの **engineID** のサポートがバージョン9.5(3) で追加されました。

ASA アプライアンスのダウングレード

ASA のバージョンを古いバージョンに設定し、バックアップ設定をスタートアップ コンフィギュレーションに復元してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。この手順は、次のモデルに適用されます。

- Firepower 1000
- Cisco Secure Firewall 1200
- Firepower 2100
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 スタンドアロン、フェールオーバー、またはクラスタリング展開のために、『ASA Upgrade Guide』のアップグレード手順を使用して、ASA ソフトウェアの古いバージョンをロードします。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。**重要**：まだ ASAをリロードしないでください。

ステップ 2 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

ステップ 3 ASA をリロードします。

ASA CLI

reload

ASDM

[Tools] > **[System Reload]** を選択します。

Firepower 4100/9300 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。
- ASA の古いバージョンが、FXOS の現在のバージョンと互換性があることを確認します。互換性がない場合は、古い ASA 設定を復元する前に最初の手順として FXOS をダウングレードします。ダウングレードされた FXOS も、（ダウングレードする前に）ASA の現在のバージョンと互換性があることを確認してください。互換性を実現できない場合は、ダウングレードを実行しないことをお勧めします。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーまたはクラスタリングの場合は、アクティブ/制御ユニットでこの手順を実行します。この手順では、コマンドをスタンバイ/データユニットに複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Firewall Chassis マネージャ または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

ステップ 3 また、FXOS をダウングレードする場合は、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Firewall Chassis マネージャ または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って FXOS ソフトウェアの古いバージョンを最新のバージョンに設定します。

ISA 3000 のダウングレード

ダウングレードでは、ISA 3000 モデルで以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。
- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- 古いコンフィギュレーションのバックアップをスタートアップ コンフィギュレーションにコピーします（**copy** *old_config_ur* **startup-config**）。
- リロード（**reload**）。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。

手順

ソフトウェアをダウングレードし、古いコンフィギュレーションを復元します。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

例：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm オプションを指定すると、プロンプトが表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存された移行前の設定へのパスです。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

ファイルの管理

フラッシュ メモリ内のファイルの表示

フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を参照できます。

手順

ステップ 1 フラッシュ メモリ内のファイルを表示します。

dir [**disk***n***:**]

disk0: は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。

例：

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

ステップ 2 特定のファイルに関する追加情報を表示します。

show file information [path:/]*filename*

例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

示されているファイル サイズは例にすぎません。

デフォルト パスは、内部フラッシュ メモリのルート ディレクトリ（disk0:/）です。

フラッシュ メモリからのファイルの削除

不要になったファイルはフラッシュ メモリから削除できます。

手順

フラッシュ メモリからファイルを削除します。

delete disk*n***:** *filename*

disk0: は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。

パスを指定しないと、デフォルトにより、ファイルは現在の作業ディレクトリから削除されます。ファイルを削除するときは、ワイルドカードを使用できます。削除するファイル名を求めるプロンプトが表示されます。その後、削除を確認する必要があります。

フラッシュ ファイル システムの削除

フラッシュ ファイル システムを消去するには、次の手順を実行します。

手順

ステップ 1 ISA 3000 コンソールへのアクセス （13 ページ）の手順に従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 **erase** コマンドを入力します。これにより、すべてのファイルが上書きされてファイル システムが消去されます（非表示のシステム ファイルを含む）。

rommon #1> **erase** [**disk0:** | **disk***n***:** | **usb:**]

disk0: は内部メモリです。その他のドライブ番号は外部ストレージを表します。新しいモデルでは、外部 USB ドライブに **usb:** を使用しています。

ファイル アクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバーとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバーとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバーは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

FTP モードをパッシブに設定します。

ftp mode passive

例：

```
ciscoasa(config)# ftp mode passive
```

ASA セキュアコピークライアントの設定

ASA が SCP クライアントとして動作する場合は、**copy** コマンドを使用して SCP を設定できます。

SCP のパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。提示された暗号方式を変更するには、**ssh cipher encryption** コマンド。たとえば、**ssh cipher encryption custom aes128-cbc**

始める前に

- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。
- 特に指定されていないかぎり、マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- SCP サーバーの場合は、SSH アクセスの設定 （1495 ページ） に従って ASA で SSH を有効にします。

手順

ステップ 1 （オプション）ASA は接続先の各 SCP サーバーの SSH ホストキーを保存します。必要に応じて、手動でキーを管理できます。

ssh pubkey-chain [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

例：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

各サーバについて、SSH ホストの **key-string**（公開キー） または **key-hash**（ハッシュ値）を指定できます。

key_string はリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

key-hash {**md5** | **sha256**} *fingerprint* では、たとえば、**show** コマンドの出力からコピーしたキーなどの、すでにハッシュされているキー（MD5 または SHA-256 キーを使用）が入力されます。

ステップ 2 （任意） SSH ホスト キー チェックを有効または無効にします。マルチ コンテキスト モードでは、管理コンテキストでこのコマンドを入力します。

[**no**] **ssh stricthostkeycheck**

例：

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

例

次に、10.86.94.170 にあるサーバのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

次に、10.7.8.9 にあるサーバのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバー ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバーとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバーへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

configure net および **copy** コマンドで使用するために、TFTP サーバーのアドレスおよびファイル名を事前定義します。

tftp-server *interface_name server_ip filename*

例：

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
```

```
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

コマンドを入力するとファイル名を上書きできます。たとえば、**copy** コマンドを使用するときに事前定義された TFTP サーバーのアドレスを利用できますが、インタラクティブプロンプトでファイル名を入力することもできます。

copy コマンドに、**tftp://***url* ではなく **tftp:** を入力して tftp-server の値を使用します。

ASA へのファイルのコピー

このセクションでは、アプリケーションイメージ、ASDM ソフトウェア、設定ファイル、その他内部または外部のフラッシュメモリにダウンロードする必要があるファイルを TFTP、FTP、SMB、HTTP、HTTPS、または SCP サーバーまたは USB ドライブなどのデバイスからコピーする方法について説明します。。

ガイドライン

- **disk0:** は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。
- USB ドライブが EXT2/3/4 または VFAT/FAT32 としてフォーマットされていることを確認します。
- 文字の大文字と小文字が異なっていても、同じ名前の 2 つのファイルをフラッシュ メモリの同じディレクトリに保存できません。たとえば、config.cfg というファイルが存在する場所に Config.cfg というファイルをダウンロードしようとすると、次のエラー メッセージが表示されます。

  ```
  %Error opening disk0:/Config.cfg (File exists)
  ```

- マルチ コンテキスト モードの場合は、プライベート ストレージ（**storage-url private**）を設定しない限り、システム実行スペース内にいる必要があります。コンテキスト内では、実行コンフィギュレーションまたはスタートアップ コンフィギュレーション（スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー（1571 ページ） プライベート ストレージおよびがある場合は コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ（1588 ページ）を参照）、またはキャプチャをコピーすることもできます。 SCP は、 コンテキスト内ではサポートされません。

始める前に

- ASA **copy** コマンドを使用して SCP サーバーとの間でファイルをコピーするには、次の手順を実行する必要があります。
  - **ssh** コマンドを使用して、ASA で SCP サーバーサブネット/ホストの SSH アクセスを有効にします。
  - **crypto key generate** コマンドを使用してキーペアを生成します（物理 ASA の場合のみ）。

手順

次のサーバー タイプの 1 つを使用してファイルをコピーします。

- TFTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- FTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?

Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- HTTP（S） サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  例：

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SMB サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* **disk***n***:/**[*path/*]*dest_filename*

  例：

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SCP サーバーからコピーします。

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] **disk***n***:/**[*path/*]*dest_filename*

  例：

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?

Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
```

```
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

- USB または内蔵または外付けドライブからコピーします。

  copy [**/noconfirm**] **disk***n***:/**[*path*]*/src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy /noconfirm disk1:/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

スタートアップコンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー

テキスト ファイルは、TFTP、FTP、SMB、HTTP（S）、または SCP サーバーから、またはフラッシュ メモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードできます。

コンフィギュレーションを実行コンフィギュレーションにコピーするには、2つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが衝突する場合、またはコマンドが ASA の実行に影響を与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

（オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

マルチコンテキストモードのコンテキスト内で、プライベートストレージ（**storage-url private**）をイネーブルにする場合は、この手順を使用できます。プライベートストレージなしで、TFTP サーバーから実行コンテキスト コンフィギュレーションにダウンロードするには、 **configure net** コマンドを使用します。 SCP は コンテキスト内でサポートされません。

手順

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロードサーバーに対して次のコマンドのいずれかを入力します。

- TFTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **tftp://***server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- FTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- HTTP（S） サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**://**[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- SMB サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
  ```

- SCP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  例：

```
ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
```

;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

例

たとえば、TFTP サーバーからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバーからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバーからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、必要に応じて、隠しディレクトリではなく表示されるファイルシステム内のファイルを指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできないため、ASA イメージに対してこの手順を使用しないでください。ASA と FXOS は個別にアップグレードでき、FXOSディレクトリリストに別々に表示されます。ASAパッケージには必ず ASDM が含まれています。
- Firepower 1000Cisco Secure Firewall 1200/3100/4200：ASA、ASDM、および FXOS のイメージは 1 つのパッケージに一緒にバンドルされています。パッケージの更新は、次の手順を

使用してASAによって管理されます。これらのプラットフォームでは、ブートするイメージを識別するためにASAが使用されますが、基盤となるメカニズムはレガシーASAとは異なります。詳細については、以下のコマンドの説明を参照してください。

- モデルのASDM：ASDMはASAオペレーティングシステム内からアップグレードできるため、バンドルされたASDMイメージのみを使用する必要はありません。Firepower 4100/9300では、手動でアップロードするASDMイメージはFXOSイメージリストに表示されません。ASAからASDMイメージを管理する必要があります。

（注） ASAバンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内のASDMイメージがASA上の前のASDMバンドルイメージに置き換わります。ただし、アップロードした別のASDMイメージ（たとえば**asdm-782.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のあるASDMバージョンを実行していることを確認するには、バンドルをアップグレードする前にASDMをアップグレードするか、またはASAバンドルをアップグレードする直前に、バンドルされたASDMイメージ（**asdm.bin**）を使用するようにASAを再設定する必要があります。

- ASA仮想：初期導入時のASA仮想パッケージでは、ASAイメージが読み取り専用boot:/パーティションに配置されます。ASA仮想をアップグレードする際は、フラッシュメモリ内の別のイメージを指定します。後でコンフィギュレーションをクリアすると（**clear configure all**）、ASA仮想は元の展開のイメージをロードするようになることに注意してください。初期導入時のASA仮想パッケージには、フラッシュメモリに配置されるASDMイメージも含まれています。ASDMイメージを個別にアップグレードできます。
- **disk0:** は内部メモリです。その他のドライブ番号は、USBドライブ、SSD、SDカードなどの外部ストレージを表します。

次のデフォルト設定を参照してください。

- ASAイメージ：
  - Firepower 1000Cisco Secure Firewall 1200/3100/4200：以前実行していたブートイメージをブートします。
  - ISA 3000：内部フラッシュメモリ内で見つかった最初のアプリケーションイメージをブートします。
  - ASA仮想：最初に展開したときに作成された、読み取り専用のboot:/パーティションにあるイメージをブートします。
  - Firepower 4100/9300シャーシ：どのASAイメージをブートするかはFXOSシステムによって決定されます。この手順を使用してASAイメージを設定することはできません。

- すべての ASA 上の ASDM イメージ：内部フラッシュ メモリ内で見つかった（この場所にイメージがない場合は外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。
- スタートアップ コンフィギュレーション：デフォルトで、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順

ステップ 1 ASA ブート イメージの場所を設定します。

boot system *url*

例：

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

URL は次のようになります。

- **disk** *n***:/**[*path*/]*filename*
- **tftp://**[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*

  TFTP オプションは、すべてのモデルでサポートされるわけではありません。

Firepower 1000 Secure Firewall 1200/3100/4200：1 つの **boot system** コマンドのみ入力できます。新しいイメージにアップグレードする場合は、**no boot system** を入力して、以前に設定したイメージを削除する必要があります。設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。このコマンドを入力した後、ASA フラッシュメモリから元のイメージファイルを削除することもできます。すると、ASA はブート場所から正しく起動します。ただし、**boot system** コマンドはフラッシュメモリ内のイメージでのみ動作するため、フラッシュメモリで使用するイメージを保持することをお勧めします。他のモデルとは異なり、スタートアップコンフィギュレーション内のこのコマンドは、ブートイメージに影響しません（本質的に表面的なものです）。リロード時には、最後にロードされたブートイメージが常に実行されます。このコマンドを入力した後で設定を保存しない場合、リロードすると、新しいイメージが起動された場合でも、古いコマンドが設定に出現します。設定を保存することにより、設定の同期を維持する必要があります。Cisco ダウンロード サイトからロードできるのは、元のファイル名のイメージのみです。ファイル名を変更した場合はロードされません。また、Firewall Threat Defense イメージをロードして Firewall Threat Defense に再イメージ化できます。この場合は、すぐにリロードするように求められます。

ASA 仮想 および ISA 3000：最大 4 つの **boot system** コマンドエントリを入力して、ブートする複数のイメージを順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブートエントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。

（注）
ASA が連続ブートのサイクルから抜け出せない場合は、ASA を ROMMON モードにリブートします。ROMMON モードの詳細については、デバッグ メッセージの表示（1621 ページ）を参照してください。

例：

```
asa(config)# boot system disk0:/cisco-asa-fp2k.9.13.2.SPA
The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.13.2 will do the following:
   - upgrade to the new platform version 2.7.2
   - upgrade to the CSP ASA version 9.13.2
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
asa(config)#
```

ステップ 2 ブートする ASDM イメージを設定します。

asdm image disk*n*:/[*path*/]*filename*

例：

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

ブートするイメージを指定しない場合、インストールされているイメージが 1 つしかなくても、ASA によって **asdm image** コマンドが実行コンフィギュレーションに挿入されます。[自動更新（Auto Update）]（設定されている場合）の問題を避けるため、また起動時ごとのイメージ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。

ステップ 3 （オプション）スタートアップ コンフィギュレーションをデフォルトの隠しファイルではなく既知のファイルになるように設定します。

boot config disk*n*:/[*path*/]*filename*

この機能は、隠しディレクトリに収まらない大規模な設定を使用する場合に重要です。大規模な設定を保存する場合、次のエラーメッセージが表示されるときは、代わりにこのコマンドを使用して設定を新しいファイルに保存してください。

```
%Error writing. nvram:/startup-config (No space left on device:)
```

例：

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

コンフィギュレーションまたはその他のファイルのバックアップと復元

システム障害に備えて、コンフィギュレーション ファイルなどのシステム ファイルを定期的にバックアップすることを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zipバックアップ tar.gz ファイルへのバックアップおよび復元方法と、そのファイルのローカルコンピュータへの転送方法について説明します。

バックアップまた復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。

- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、マスターパスフレーズの設定（1015ページ）を参照して、バックアップを続行する前に、マスターパスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    セキュアクライアント（SVC）画像とプロファイル

    セキュアクライアント（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - Application Profile Custom Framework（APCF）
  - Bookmarks
  - カスタマイゼーション
  - ダイナミック アクセス ポリシー（DAP）
  - プラグイン

- 接続プロファイル用の事前入力スクリプト
- プロキシ自動設定
- 変換テーブル
- Web コンテンツ
- バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1 システムをバックアップします。

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

例：

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

interface *name* を指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

システム実行スペースからのマルチ コンテキスト モードで、**context** キーワードを入力して、指定したコンテキストをバックアップします。各コンテキストは個別にバックアップする必要があります。つまり、ファイルごとに **backup** コマンドを再入力する必要があります。

VPN 証明書および事前共有キーのバックアップ中、証明書を符号化するために、**passphrase** キーワードで指定された秘密キーが必要です。PKCS12 形式の証明書を符号化および復号化するために使用するパスフレーズを入力する必要があります。バックアップに含まれるのは証明書に関連する RSA キー ペアだけであり、スタンドアロン証明書は除外されます。

バックアップの **location** にはローカル ディスクまたはリモート URL を指定できます。location を指定しない場合は、次のデフォルト名が使用されます。

- シングル モード：disk0:*hostname*.backup.*timestamp*.tar.gz
- マルチ モード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

ステップ 2 プロンプトに従います。

例：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?
```

```
Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 バックアップ ファイルからシステムを復元します。

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

context キーワードを使用して複数のコンテキストを復元する場合、バック アップされた各コンテキスト ファイルは個別に復元する必要があります。つまり、**restore** コマンドをファイルごとに再入力する必要があります。

ステップ 2 プロンプトに従います。

例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
```

```
Cleaning up ... Done!
Restore finished!
```

自動バックアップおよび復元の設定（ISA 3000）

ISA 3000 では、**write memory** を使用して設定を保存するたびに、特定の場所への自動バックアップを設定できます。

自動復元では、完全な設定を SD フラッシュメモリカードにロードして、新しいデバイスを簡単に設定できます。工場出荷時のデフォルト設定では、自動復元が有効になっています。

自動バックアップの設定（ISA 3000）

ISA 3000 では、**write memory** を使用して設定を保存するたびに、特定の場所への自動バックアップを設定できます。

始める前に

この機能は、ISA 3000 のみで使用できます。

手順

ステップ 1 パッケージのバックアップ パラメータを設定します。

backup-package backup [**interface** *name*] **location** {**disk***n***:** | *url*} [**passphrase** *string*]

- **interface** *name*：オフデバイスストレージを指定した場合に、バックアップ URL に到達するためのインターフェイスを指定します。interface name を指定しない場合、ASA は管理専用のルーティングテーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。
- **location** {**disk***n***:** | *url*}：データのバックアップに使用するストレージメディアを指定します。URL またはローカルストレージを指定できます。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。自動復元のデフォルト設定では disk3 が使用されます。
- **passphrase** *string*：バックアップデータを保護するためのパスフレーズを設定します。自動復元のデフォルト設定では、パスフレーズとして「cisco」が使用されます。

これらの設定は、手動の **backup** コマンドでもデフォルトで使用されます。システムのバックアップ（1579 ページ）を参照してください。自動バックアップまたは復元を有効にしている場合に手動の**backup**コマンドを使用すると、指定した名前のバックアップファイルと、自動バックアップおよび復元で使用される「auto-backup-asa.tgz」という名前のファイルが保存されます。

例：

```
ciscoasa(config)# backup-package backup location disk3: passphrase cisco
```

ステップ 2 バックアップおよび復元の自動モードを有効にします。

backup-package backup auto

write memory を使用して設定を保存すると、設定は自動的にバックアップ場所とスタートアップ コンフィギュレーションに保存されます。バックアップファイルの名前は「auto-backup-asa.tgz」です。自動バックアップを無効にするには、このコマンドの **no** 形式を使用します。

例：

```
ciscoasa(config)# backup-package backup auto
```

自動復元の設定（ISA 3000）

自動復元モードは、ユーザの操作なしでデバイスのシステム設定を復元します。たとえば、保存したバックアップ設定を含む SD メモリカードを新しいデバイスに挿入し、デバイスの電源をオンにします。デバイスが起動すると、システム設定を復元する必要があるかどうかを判断するために SD カードがチェックされます。（復元は、バックアップファイルに別のデバイスの「フィンガープリント」がある場合にのみ開始されます。バックアップファイルのフィンガープリントは、バックアップまたは復元操作中に現在のデバイスに一致するように更新されます。そのため、デバイスがすでに復元を完了している場合、またはデバイスが独自のバックアップを作成している場合は、自動復元はスキップされます。）フィンガープリントに復元が必要であることが示されている場合、デバイスはシステム設定を置き換えます（startup-config、running-config、SSL VPN 設定など。バックアップの内容の詳細については、システムのバックアップ（1579 ページ）を参照してください）。デバイスの起動が完了すると、保存された設定が実行されます。

工場出荷時のデフォルト設定では自動復元が有効になっているため、デバイスの事前設定を実行しなくても、SD メモリカードにロードされた完全な設定で新しいデバイスを簡単に設定できます。

デバイスは、システム設定を復元する必要があるかどうかをブートプロセスの早い段階で決定する必要があるため、ROMMON 変数をチェックして、デバイスが自動復元モードかどうかを判断し、バックアップ設定の場所を取得します。次の ROMMON 変数が使用されます。

- **RESTORE_MODE =** {**auto** | **manual**}

  デフォルトは **auto** です。

- **RESTORE_LOCATION =** {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  デフォルトは **disk3:** です。

- **RESTORE_PASSPHRASE =** *key*

デフォルトは **cisco** です。

自動復元設定を変更するには、次の手順を実行します。

始める前に

- この機能は、ISA 3000 のみで使用できます。
- デフォルトの復元設定を使用する場合は、SD メモリカード（部品番号 SD-IE-1GB=）を取り付ける必要があります。
- 自動復元を有効にするためにデフォルト設定を復元する必要がある場合は、**configure factory default** コマンドを使用します。このコマンドは、トランスペアレント ファイアウォール モードでのみ使用できます。そのため、ルーテッド ファイアウォール モードの場合は、最初に **firewall transparent** コマンドを使用します。

手順

ステップ 1 パッケージの復元のパラメータを設定します。

backup-package restore location {**disk***n***:** | *url*} [**passphrase** *string*]

- **location disk***n***:**：データの復元に使用するストレージメディアを指定します。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。デフォルトは disk3 です。
- **passphrase** *string*：バックアップデータを読み取るパスフレーズを設定します。デフォルトは「cisco」です。

これらの設定は、手動の **restore** コマンドでもデフォルトで使用されます。システムのバックアップ （1579 ページ）を参照してください。

例：

```
ciscoasa(config)# backup-package restore location disk1: passphrase $upe3rnatural
```

ステップ 2 復元の自動モードを有効または無効にします。

[**no**] **backup-package restore auto**

復元されるファイルの名前は「auto-backup-asa.tgz」です。

例：

```
ciscoasa(config)# no backup-package restore auto
```

シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ

シングルコンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバーまたはローカル フラッシュ メモリにコピーできます。

始める前に

（オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

手順

次のサーバー タイプの 1 つを使用してコンフィギュレーションをバックアップします。

- TFTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **tftp://***server*[*/path*]*/dst_filename*

  例：

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- FTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- SMB サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

  ```
  ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
  ```

- SCP サーバーにコピーします。

copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

例：

```
ciscoasa# copy startup-config
scp://pilot:moya@10.86.94.170/new-startup.cfg
```

;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

- ローカル フラッシュ メモリにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  例：

```
ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
```

  宛先ディレクトリが存在することを確認してください。存在しない場合は、まず**mkdir** コマンドを使用してディレクトリを作成します。

フラッシュ メモリ内のコンテキスト コンフィギュレーションまたはその他のファイルのバック アップ

システム実行スペースで次のいずれかのコマンドを入力することによって、ローカル フラッシュ メモリにあるコンテキスト コンフィギュレーションまたは他のファイルをコピーします。

始める前に

（オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

手順

次のサーバー タイプの 1 つを使用してコンテキスト コンフィギュレーションバックアップをバックアップします。

- フラッシュから TFTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* **tftp://***server*[*/path*]*/dst_filename*

  例：

```
ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
```

- フラッシュから FTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  ftp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

```
ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
```

- フラッシュから SMB サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  smb://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

```
ciscoasa# copy /noconfirm copy disk0:/asdm.bin
smb://chiana:dargo@10.1.1.67/asdm.bin
```

- フラッシュから SCP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  例：

```
ciscoasa# copy disk0:/context1.cfg
scp://pilot:moya@10.86.94.170/context1.cfg
```

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

- フラッシュからローカル フラッシュ メモリにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  例：

```
ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
```

  宛先ディレクトリが存在することを確認してください。存在しない場合は、まず**mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチ コンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

手順

ステップ 1 （リモート サーバーの場合、admin コンテキストに接続された）スタートアップ構成サーバーに実行コンフィギュレーションをコピーします。スタートアップ コンフィギュレーションの場所は、コンテキスト内から **config-url** コマンドで指定します。

copy running-config startup-config

例：

```
ciscoasa/contexta# copy running-config startup-config
```

ステップ 2 コンテキスト ネットワークに接続された TFTP サーバーに実行構成をコピーします。

copy running-config {**ftp** | **tftp**}**:**//*url*/*dest_filename*

正確な URL オプションについては、 **copy** コマンドのヘルプを参照してください。

プライベート ストレージ（**storage-url private**）を有効にすると、他のサーバオプションも使用できます。 ただし、 コンテキスト内では SCP はサポートされません。

例：

```
ciscoasa/contexta# copy running-config tftp:/10.89.6.8/configs/1010-1.cfg
```

端末ディスプレイからのコンフィギュレーションのコピー

手順

ステップ 1 コンフィギュレーションを端末に表示します。

more system:running-config

ステップ 2 コマンドから出力をコピーして、コンフィギュレーションをテキスト ファイルに貼り付けます。

export および import コマンドを使用した追加ファイルのバックアップ

コンフィギュレーションに欠かせない追加ファイルは次のとおりです。

- **import webvpn** コマンドを使用してインポートするファイル。現在これらのファイルには、カスタマイゼーション、URL リスト、Web コンテンツ、プラグイン、および言語翻訳などがあります。
- DAP ポリシー（dap.xml）。
- CSD コンフィギュレーション（data.xml）。
- デジタル キーおよびデジタル証明書。
- ローカル CA ユーザー データベース ファイルと証明書ステータス ファイル。

CLI では、**export** コマンドと **import** コマンドを使用して、コンフィギュレーションの個々の要素をバックアップおよび復元できます。

これらのファイル（たとえば、**import webvpn** コマンドを使用してインポートしたこれらのファイルや証明書など）をバックアップするには、次の手順を実行します。

手順

ステップ 1 次のように、適用可能な **show** コマンドを実行します。

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

ステップ 2 バックアップするファイルに対して **export** コマンドを発行します（この例では rdp ファイルです）。

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

スクリプトを使用したファイルのバックアップおよび復元

スクリプトを使用して、ASA のコンフィギュレーション ファイルをバックアップおよび復元できます。これには、**import webvpn** CLI によってインポートする拡張機能のすべて、CSD コンフィギュレーションの XML ファイル、および DAP コンフィギュレーションの XML ファイルが含まれます。セキュリティ上の理由により、デジタル キーと証明書、またはローカル CA キーの自動バックアップを実行することはお勧めしません。

この項では、自動バックアップの手順について説明します。また、そのまま使用することも、環境要件に合わせて修正することもできるサンプル スクリプトを示します。サンプル スクリプトはLinuxシステムに固有のスクリプトです。Microsoft Windowsシステムで使用するには、サンプルのロジックを使用して修正する必要があります。

（注） 代わりに、**backup** コマンドと **restore** コマンドを使用することもできます。詳細については、完全なシステム バックアップまたは復元の実行 （1577 ページ）を参照してください。

バックアップおよび復元スクリプトを使用する前に

スクリプトを使用して ASA コンフィギュレーションをバックアップおよび復元するには、まず次の作業を実行します。

- Expect モジュールとともに Perl をインストールする。
- ASA に到達可能な SSH クライアントをインストールする。
- TFTP サーバーをインストールして、ASA からバックアップ サイトにファイルを送信する。

別の選択肢としては、市販のツールを使用します。このスクリプトのロジックをそれらのツールに取り入れることができます。

スクリプトを実行する

バックアップおよび復元のスクリプトを実行するには、次の手順を実行します。

手順

ステップ 1 システムの任意の場所に、スクリプトファイルをダウンロードまたはカットアンドペーストします。

ステップ 2 コマンド ラインで、**Perl***scriptname* と入力します。*scriptname* はスクリプト ファイルの名前です。

ステップ 3 Enter を押します。

ステップ 4 オプションごとに値を入力するように、プロンプトが表示されます。あるいは、**Perl***scriptname* コマンドを入力するときにオプションの値を入力してから、**Enter** を押すこともできます。どちらの方法でも、スクリプトによりオプションごとに値を入力するよう求められます。

ステップ 5 このスクリプトが実行され、発行されるコマンドが出力されます。この出力はCLIの記録となります。これらの CLI は後で行われる復元に使用できます。特に、ファイルを 1 つまたは 2 つだけ復元する場合に便利です。

サンプルスクリプト

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#      -r: Restore with an argument that specifies the file name. This file is produced
 during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
```

```
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
```

```
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
```

```
   $obj->send("dir sdesktop\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub webcontent {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn webcontent\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /No custom/;
     next unless (/^.+\s+.+$/);
     ($url, $type) = split(/\s+/,$_);
     $turl = $url;
     $turl =~ s/\//\+//;
     $turl =~ s/\+\//-/;
     $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}
```

```
sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }

  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
```

```
        $restore_file = $options{r};
    }
}
```

Cisco Secure Firewall 3100/4200 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

⚠

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
ciscoasa# show raid
Virtual Drive
```

```
ID:                           1
Size (MB):                    858306
Operability:                  operable
Presence:                     equipped
Lifecycle:                    available
Drive State:                  optimal
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     0
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                  nvme1n1
Disk State:                   in-sync
Disk Slot:                    2
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                           1
Size (MB):                    858306
Operability:                  degraded
Presence:                     equipped
Lifecycle:                    available
Drive State:                  degraded
Type:                         raid
Level:                        raid1
Max Disks:                    2
Meta Version:                 1.0
Array State:                  active
Sync Action:                  idle
Sync Completed:               unknown
Degraded:                     1
Sync Speed:                   none

RAID member Disk:
Device Name:                  nvme0n1
Disk State:                   in-sync
Disk Slot:                    1
Read Errors:                  0
Recovery Start:               none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。
b) SSD を RAID に追加します。

raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。

USB ポートの無効化

デフォルトでは、タイプ A USB ポートは有効になっています。セキュリティ上の理由から、USB ポートへのアクセスを無効にする必要がある場合があります。USB の無効化は、次のモデルでサポートされています。

- Firepower 1000 シリーズ
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200

ガイドライン

- USB ポートを有効または無効にするにはリロードが必要です。
- USB ポートが無効で、この機能をサポートしていないバージョンにダウングレードすると、ポートは無効のままになります。NVRAM を消去（FXOS local-mgmt **erase secure all** コマンド）せずに再度有効にすることはできません。
- ROMMON **factory-reset** または FXOS local-mgmt **erase secure** を実行すると、USB ポートが再度有効になります。
- アクティブユニットまたは制御ノードの USB ポートを無効または有効にし、高可用性またはクラスタリングを設定します。コマンドが他のノードに複製されます。ただし、変更を有効にするには、各ユニットをリロードする必要があります。

（注） この機能は、USB コンソールポート（存在する場合）には影響しません。

手順

ステップ 1 USB ポートを無効化します。

usb-port disable

write memory

reload

USB ポートを再度有効にするには、**no usb-port disable** と入力します。

例：

```
ciscoasa(config)# usb-port disable
Requesting USB disable. This may take 30 seconds to complete.
Please execute 'write memory' and reboot the system to apply
any operational state changes.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 19d02ee0 671dbe24 88193adb bccb8147

12382 bytes copied in 0.530 secs
[OK]

ciscoasa(config)# reload
Proceed with reload? [confirm]
```

ステップ 2 ポートステータスを表示します。

show usb-port

[管理ステータス（Admin State）] には、USB ポートの設定が表示されます。[動作ステータス（Oper State）] には、現在の動作が表示されます。たとえば、USB ポートを無効化してリロードしていない場合、[管理ステータス（Admin State）] には無効と表示され、[動作ステータス（Oper State）] は有効になります。

例：

```
ciscoasa(config)# show usb-port
USB Port info
---------------
Admin State: disabled
Oper State: disabled
```

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォーム リリース	機能情報
セキュアコピークライアントおよびサーバ	9.1(5)/9.2(1)	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP）クライアントおよびサーバをサポートするようになりました。 **ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash**、**ssh stricthostkeycheck** の各コマンドが導入されました。 **copy scp** コマンドが変更されました。
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)/9.5(3)/9.6(1)	ユーザーは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**

機能名	プラットフォーム リリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバー証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 設定を移行する場合は、次のように確認なしを明示的に設定します。 **auto-update server no-verification** **auto-update server** {**verify-certificate** | **no-verification**} コマンドが変更されました。
CLIを使用したシステムのバックアップと復元	9.3(2)	CLIを使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。 **backup** および **restore** の各コマンドが導入されました。
新しいASA 5506W-Xイメージの回復およびロード	9.4(1)	新しいASA 5506W-Xイメージのリカバリおよびロードがサポートされています。 **hw-module module wlan recover image** コマンドが導入されました。
ISA 3000 の自動バックアップと復元	9.7(1)	バックアップ コマンドと復元コマンドのプリセット パラメータを使用して、自動バックアップ機能や自動復元機能を有効にできます。これらの機能は、外部メディアからの初期設定、デバイス交換、作動可能状態へのロールバックなどで使用されます。 次のコマンドが導入されました。**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary**

機能名	プラットフォーム リリース	機能情報
SCP クライアントを使用する場合、CiscoSSH スタックには SSH アクセスが必要です	9.17(1)	CiscoSSH スタックを使用する場合、ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、**ssh** コマンドを使用して SCP サーバサブネット/ホストの SSH アクセスを ASA で有効にする必要があります。
Cisco Secure Firewall 3100 での SSD の RAID サポート	9.17(1)	SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新規/変更されたコマンド： **raid, show raid, show ssd**
USB ポートの無効化	9.22(1)	デフォルトでは、タイプ A USB ポートは有効になっており、無効にできません。次のモデルで、セキュリティ上の目的で USB ポートアクセスを無効にできるようになりました。 • Firepower 1000 • Cisco Secure Firewall 1200 • Cisco Secure Firewall 3100 • Cisco Secure Firewall 4200 この設定はファームウェアに保存され、リロードが必要です。USB ポートが無効で、この機能をサポートしていないバージョンにダウングレードすると、ポートは無効のままになります。NVRAM を消去せずに再度有効にすることはできません。 （注） この機能は、USB コンソールポート（存在する場合）には影響しません。 新規/変更されたコマンド：**usb-port disable**、**show usb-port**

第 44 章

システム イベントに対する応答の自動化

この章では、Embedded Event Manager（EEM）を設定する方法について説明します。

- EEM について （1603 ページ）
- EEM のガイドライン （1605 ページ）
- EEM の設定 （1605 ページ）
- EEM の例 （1613 ページ）
- EEM のモニタリング （1614 ページ）
- EEM の履歴 （1615 ページ）

EEM について

EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。

サポートされるイベント

EEM は次のイベントをサポートします。

- Syslog：ASA は、syslog メッセージの ID を使用して、イベント マネージャ アプレットをトリガーする syslog メッセージを識別します。複数の syslog イベントを設定できますが、単一のイベント マネージャ アプレット内で syslog メッセージの ID が重複することはできません。
- タイマー：タイマーを使用して、イベントをトリガーできます。各タイマーは、各イベント マネージャ アプレットに対して一度だけ設定できます。各イベント マネージャ アプレットには最大で 3 つのタイマーがあります。3 種類のタイマーは次のとおりです。
  - ウォッチドッグ（定期的）タイマーは、アプレットアクションの完了後に指定された期間が経過するとイベント マネージャ アプレットをトリガーし、自動的にリスタートします。

- カウントダウン（ワンショット）タイマーは、指定された期間が経過するとイベントマネージャアプレットを1回トリガーします。削除および再追加されない限りはリスタートしません。
- 絶対（1 日 1 回）タイマーは、イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートします。時刻の形式は hh:mm:ss です。

  各イベント マネージャ アプレットに対して、各タイプのタイマー イベントを 1 つだけ設定できます。

- なし：CLI または ASDM を使用してイベント マネージャ アプレットを手動で実行する場合、イベントはトリガーされません。
- クラッシュ：ASA がクラッシュした場合、クラッシュ イベントがトリガーされます。一部のシナリオでは、強制クラッシュがトリガーされます。

  ASA がブロックの枯渇時にリロードするように設定されていて、設定された期間に ASA がメモリ不足のままになっている場合、ASA は syslog を送信してトラブルシューティング データを収集します。ASA は強制的にクラッシュし、リロードプロセスをトリガーしてメモリブロックを解放します。HA 設定では、このような場合に、フェールオーバーがトリガーされます。クラスタ設定では、ノードはクラスタを離れます。

  output コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

イベント マネージャ アプレットのアクション

イベント マネージャ アプレットがトリガーされると、そのイベント マネージャ アプレットのアクションが実行されます。各アクションには、アクションの順序を指定するために使用される番号があります。このシーケンス番号は、イベント マネージャ アプレット内で一意である必要があります。イベント マネージャ アプレットには複数のアクションを設定できます。コマンドは典型的な CLI コマンドです（**show blocks** など）。

出力先

output コマンドを使用すると、アクションの出力を指定した場所に送信できます。一度にイネーブルにできる出力値は1つだけです。デフォルト値は **output none** です。この値は、**action** コマンドによるすべての出力を破棄します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。次の3つの場所のいずれかに **action** CLI コマンドの出力を送信できます。

- **なし**：デフォルトの設定です。出力を破棄します。
- **コンソール**：出力を ASA コンソールに送信します。
- **ファイル**：出力をファイルに送信します。次の 4 つのファイル オプションを使用できます。

- **一意のファイルを作成する**：イベントマネージャ アプレットが呼び出されるたびに、一意の名前を持つ新しいファイルを作成します。
- **ファイルを作成する/ファイルを上書きする**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルを上書きします。
- **ファイルを作成する/ファイルに付加する**：イベント マネージャ アプレットが呼び出されるたびに、指定されたファイルに付加します。ファイルがまだ存在しない場合は作成されます。
- **一連のファイルを作成する**：イベント マネージャ アプレットが呼び出されるたびにローテーションされる、一意の名前を持つ一連のファイルを作成します。

EEM のガイドライン

ここでは、EEM を設定する前に確認する必要のあるガイドラインおよび制限事項について説明します。

コンテキスト モードのガイドライン

マルチ コンテキスト モードではサポートされません。

その他のガイドライン

- 通常、クラッシュ時は、ASA の状態は不明です。こうした状況では、一部のコマンドの実行は安全ではない可能性があります。
- イベント マネージャ アプレットの名前にはスペースを含めることができません。
- None イベントおよび Crashinfo イベント パラメータは変更できません。
- syslog メッセージが EEM に送信されて処理されるため、パフォーマンスが影響を受ける可能性があります。
- 各イベント マネージャ アプレットのデフォルトの出力は **output none** です。この設定を変更するには、異なる出力値を入力する必要があります。
- 各イベント マネージャ アプレットに定義できる出力オプションは 1 つだけです。

EEM の設定

EEM の設定は、次のタスクで構成されています。

手順

ステップ 1 イベントマネージャアプレットの作成とイベントの設定（1606ページ）を使用して無効にすることができます。

ステップ 2 「アクションおよびアクションの出力先の設定 （1608 ページ）」を参照してください。

ステップ 3 「イベント マネージャ アプレットの実行 （1610 ページ）」を参照してください。

ステップ 4 「トラック メモリ割り当ておよびメモリ使用量 （1610 ページ）」を参照してください。

イベント マネージャ アプレットの作成とイベントの設定

イベントマネージャアプレットを作成してイベントを設定するには、次の手順を実行します。

手順

ステップ 1 イベント マネージャ アプレットを作成し、イベント マネージャ アプレットのコンフィギュレーション モードを開始します。

event manager applet *name*

例：

```
ciscoasa(config)# event manager applet exampleapplet1
```

name 引数には、最大 32 文字の英数字を指定できます。スペースは使用できません。

イベント マネージャ アプレットを削除するには、このコマンドを **no** 形式で入力します。

ステップ 2 イベント マネージャ アプレットの説明を入力します。

description *text*

例：

```
ciscoasa(config-applet)# description applet1example
```

text 引数は、最大 256 文字です。引用符内であれば、説明テキストにスペースを含めることができます。

ステップ 3 指定されたイベントを設定するには、次のコマンドのいずれかを入力します。設定されたイベントを削除するには、それぞれのコマンドを **no** 形式で入力します。

- syslog イベントを設定するには、イベント マネージャ アプレットをトリガーする単一の syslog メッセージまたは syslog メッセージの範囲を指定します。

  event syslog id *nnnnnn* [*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

例：

```
ciscoasa(config-applet)# event syslog id 106201
```

nnnnnn 引数には、syslog メッセージの ID を指定します。キーワードと引数のペアである **occurs** *n* は、イベント マネージャ アプレットを呼び出すために syslog メッセージが発生しなければならない回数を示しています。デフォルトの発生回数は 0 秒ごとに 1 回です。有効な値は、1 ～ 4294967295 です。キーワードと引数のペアである **period** *seconds* は、イベントが発生する際の許容時間（秒数）を示しています。また、イベント マネージャ アプレットが設定された期間に 1 回呼び出される際の最大の間隔を制限します。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

- イベントを設定された期間ごとに 1 回発生させ、自動的にリスタートするように設定します。

  event timer watchdog time *seconds*

  例：

  ```
  ciscoasa(config-applet)# event timer watchdog time 30
  ```

  秒数は、1 ～ 604800 の範囲で設定してください。

- イベントを 1 回発生させ、削除および再追加されない限りはリスタートしないように設定します。

  event timer countdown time *seconds*

  例：

  ```
  ciscoasa(config-applet)# event timer countdown time 60
  ```

  秒数は、1 ～ 604800 の範囲で設定してください。カウントダウン タイマー イベントを削除するには、このコマンドの **no** 形式を使用します。

  （注）
  スタートアップ コンフィギュレーションである場合、このタイマーはリブート時に再実行されます。

- イベントを 1 日 1 回指定された時刻に発生させ、自動的にリスタートするように設定します。

  event timer absolute time *hh:mm:ss*

  例：

  ```
  ciscoasa(config-applet)# event timer absolute time 10:30:20
  ```

  時刻の形式は hh:mm:ss です。時刻の範囲は 00:00:00（真夜中）から 23:59:59 です。

- ASA のクラッシュ時にクラッシュ イベントをトリガーします。

event crashinfo

例：

```
ciscoasa(config-applet)# event crashinfo
```

output コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルを対象とします。出力は **show tech** コマンドの前に生成されます。

アクションおよびアクションの出力先の設定

アクションおよびアクションの出力を送信する特定の宛先を設定するには、次の手順を実行します。

手順

ステップ 1 イベント マネージャ アプレットにアクションを設定します。

action *n* **cli command** *"command"*

例：

```
ciscoasa(config-applet)# action 1 cli command "show version"
```

n オプションはアクション ID です。有効な ID の範囲は、0 ～ 4294967295 です。*command* オプションの値は、引用符で囲む必要があります。引用符で囲んでいない場合、コマンドが 2 つ以上の単語で構成されているとエラーが発生します。このコマンドは、特権レベル 15（最高）を持つユーザとして、グローバル コンフィギュレーション モードで実行されます。ディセーブルになっているため、このコマンドは入力を受け付けない場合があります。コマンドで使用可能な場合は、**noconfirm** オプションを使用します。

ステップ 2 使用可能な出力先オプションを 1 つ選択します。出力先を削除するには、各コマンドの **no** 形式を使用します。

- **None** オプションは、**action** コマンドからのあらゆる出力を破棄します。これがデフォルト設定です。

  output none

  例：

  ```
  ciscoasa(config-applet)# output none
  ```

- **Console** オプションは、**action** コマンドの出力をコンソールに送信します。

  output console

例：

```
ciscoasa(config-applet)# output console
```

（注）
このコマンドを実行すると、パフォーマンスに影響を及ぼします。

- **New File** オプションは、呼び出された各イベント マネージャ アプレットの新しいファイルに **action** コマンドの出力を送信します。

  output file new

  例：

  ```
  ciscoasa(config-applet)# output file new
  ```

  ファイル名の形式は、eem-*applet-timestamp*.log です。ここで、*applet* はイベント マネージャ アプレットの名前、*timestamp* は日付のタイム スタンプ（形式は YYYYMMDD-hhmmss）を示しています。

- **New Set of Rotated Files** オプションは、ローテーションされる一連のファイルを作成します。新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。

  output file rotate *n*

  例：

  ```
  ciscoasa(config-applet)# output file rotate 50
  ```

  最も新しいファイルが 0 で示され、最も古いファイルが最大数（*n* -1）で示されます。*n* オプションはローテーションの値です。有効な値の範囲は 2 ～ 100 です。ファイル名の形式は、eem-*applet-x*.log です。ここで、*applet* はアプレットの名前、*x* はファイル番号を示しています。

- **Single Overwritten File** オプションは、**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。

  output file overwrite *filename*

  例：

  ```
  ciscoasa(config-applet)# output file overwrite examplefile1
  ```

  filename 引数は、（ASA に対して）ローカルのファイル名です。このコマンドは、FTP、TFTP、および SMB のターゲット ファイルを使用する場合もあります。

- **Single Appended File** オプションは、**action** コマンドの出力を単一のファイルに書き込みますが、このファイルは毎回上書きされます。

  output file append *filename*

例：

```
ciscoasa(config-applet)# output file append examplefile1
```

filename 引数は、（ASA に対して）ローカルのファイル名です。

イベント マネージャ アプレットの実行

イベント マネージャ アプレットを実行するには、次の手順を実行します。

手順

イベント マネージャ アプレットを実行します。

event manager run *applet*

例：

```
ciscoasa# event manager run exampleapplet1
```

event none コマンドで設定されていないイベントマネージャアプレットを実行すると、エラーが発生します。*applet*引数は、イベント マネージャ アプレットの名前です。

トラック メモリ割り当ておよびメモリ使用量

メモリ割り当てとメモリ使用量をログに記録するには、次の手順を実行します。

手順

ステップ 1 メモリ ロギングをイネーブルにします。

memory logging [1024-4194304] [**wrap**] [**size** [1-2147483647]] [**process** *process-name*] [**context** *context-name*]

例：

```
ciscoasa(config)# memory logging 202980
```

必要な唯一の引数は、メモリ ロギング バッファ内のエントリ数です。**wrap** オプションは、ラップ時にバッファを保存するようメモリ ロギング ユーティリティに指示します。保存できるのは一度だけです。

メモリ ロギング バッファが複数回ラップした場合は、上書きされます。バッファがラップすると、そのデータの保存をイネーブルにするトリガーがイベントマネージャに送信されます。**size** オプションは、特定のサイズをモニターします。**process** オプションは、特定のプロセスをモニタします。

（注）
Checkheaps プロセスは、非標準の方法でメモリ アロケータを使用するため、プロセスとして完全に無視されます。

context オプションは、指定した名前で特定の仮想コンテキストのメモリ ロギングを記録します。

メモリ ロギング パラメータを変更するには、それをディセーブルにしてから、再度イネーブルにします。

ステップ 2 メモリ ロギング結果を表示します。

```
show memory logging [brief | wrap]
show memory logging include [address] [caller] [operator] [size] [process] [time] [context]
```

例：

```
ciscoasa# show memory logging
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] time=[13:26:33.407] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:33.407] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x000000000013193e8
0x0000000000443455 0x0000000001318f5b
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:35.964] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:35.964] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[CMGR Server Process] time=[13:26:37.964] oper=[free]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000021246ef 0x0000000001827098
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:37.964] oper=[free]
addr=0x00007fff224b9460 size=40 @ 0x00000000021246ef 0x000000000182711b
```

```
0x000000000182c08d 0x000000000182c262 process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff2cd0aa00 size=16 @ 0x00000000016466ea 0x0000000002124542
0x000000000182774d 0x000000000182cc8a process=[CMGR Server Process]
time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000016466ea 0x0000000002124542
0x0000000000bfef9a 0x0000000000bff606 process=[CMGR Server Process]
time=[13:26:38.464] oper=[free]
addr=0x00007fff224bb9f0 size=512 @ 0x00000000021246ef 0x0000000000bff3d8
0x0000000000bff606 0x000000000182ccb0
process=[CMGR Server Process] time=[13:26:38.464] oper=[malloc]
addr=0x00007fff224b9460 size=40 @ 0x00000000016466ea 0x0000000002124542
0x0000000001834188 0x000000000182ce83
process=[ci/console] time=[13:26:38.557] oper=[malloc]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000016466ea 0x0000000002124542
0x000000000131911a 0x0000000000442bfd process=[ci/console] time=[13:26:38.557] oper=[free]
addr=0x00007fff2cd0a6c0 size=72 @ 0x00000000021246ef 0x00000000013193e8
0x0000000000443455 0x0000000001318f5b

ciscoasa# show memory logging include process operation size
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
process=[ci/console] oper=[malloc] size=72 process=[ci/console] oper=[free]
size=72 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[CMGR Server Process] oper=[free] size=16 process=[CMGR Server Process]
oper=[free] size=40 process=[CMGR Server Process] oper=[malloc] size=16
process=[CMGR Server Process] oper=[malloc] size=512 process=[CMGR Server Process]
oper=[free] size=512 process=[CMGR Server Process] oper=[malloc] size=40
process=[ci/console] oper=[malloc] size=72 process=[ci/console]
oper=[free] size=72 ciscoasa# show memory logging brief
Number of free                          6
Number of calloc                        0
Number of malloc                        8
Number of realloc-new                   0
Number of realloc-free                  0
Number of realloc-null                  0
Number of realloc-same                  0
Number of calloc-fail                   0
Number of malloc-fail                   0
Number of realloc-fail                  0
Total operations 14
Buffer size: 50 (3688 x2 bytes)
```

どのオプションも指定しない場合、**show memory logging** は統計情報を表示し、記録された処理を表示します。**brief** オプションは、統計情報だけを表示します。**wrap** オプションは、重複したデータが表示または保存されないように、ラップ時点でバッファを表示してから、そのデータを消去します。**include** オプションは、指定されたフィールドのみを出力に含めます。任意の順序でフィールドを指定できますが、必ず次の順序で表示されます。

1. プロセス
2. 時刻
3. コンテキスト（シングル モード以外）
4. 処理（free/malloc/など）
5. アドレス
6. サイズ
7. 発信者

出力形式は、次のとおりです。

process=[XXX] time=[XXX] context=[XXX] oper=[XXX] address=0xXXXXXXXX size=XX @ XXXXXXXX XXXXXXXX XXXXXXXX XXXXXXXX

最大4つの発信者アドレスが表示されます。例に示すように、処理の種類（番号）が出力に列挙されます。

ステップ3 メモリ ロギング ラップ イベントに応答します。

event memory-logging-wrap

例：

```
ciscoasa(config)# event manager applet memlog
ciscoasa(config)# event memory-logging-wrap
ciscoasa(config)# action 0 cli command "show memory logging wrap"
ciscoasa(config)# output file append disk0:/memlog.log
```

この例では、すべてのメモリ割り当てを記録するアプレットを示します。メモリ ロギングに対してラップがイネーブルになっている場合は、メモリ ロガーが、設定されたアプレットをトリガーするイベントをイベント マネージャに送信します。

EEM の例

次に、ブロックの漏えい情報を1時間ごとに記録し、その出力をローテーションされる一連のログ ファイルに書き込み、1 日分のログを保持するイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet blockcheck
ciscoasa(config-applet)# description “Log block usage”
ciscoasa(config-applet)# event timer watchdog time 3600
ciscoasa(config-applet)# output rotate 24
ciscoasa(config-applet)# action 1 cli command “show blocks old”
```

次に、毎日午前 1 時に ASA をリブートし、必要に応じて設定を保存するイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet dailyreboot
ciscoasa(config-applet)# description "Reboot every night"
ciscoasa(config-applet)# event timer absolute time 1:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "reload save-config noconfirm"
```

次に、午前 0 時から午前 3 時の間に特定のインターフェイスをディセーブルにするイベント マネージャ アプレットの例を示します。

```
ciscoasa(config)# event manager applet disableintf
ciscoasa(config-applet)# description "Disable the interface at midnight"
ciscoasa(config-applet)# event timer absolute time 0:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"

ciscoasa(config)# event manager applet enableintf
ciscoasa(config-applet)# description "Enable the interface at 3am"
ciscoasa(config-applet)# event timer absolute time 3:00:00
ciscoasa(config-applet)# output none
ciscoasa(config-applet)# action 1 cli command "interface GigabitEthernet 0/0"
ciscoasa(config-applet)# action 2 cli command "no shutdown"
ciscoasa(config-applet)# action 3 cli command "write memory"
```

EEM のモニタリング

EEM をモニターするには、次のコマンドを参照してください。

- **clear configure event manager**

  このコマンドは、イベント マネージャの実行コンフィギュレーションを削除します。

- **clear configure event manager applet** *appletname*

  このコマンドは、コンフィギュレーションから指定のイベント マネージャ アプレットを削除します。

- **show counters protocol eem**

  このコマンドは、イベント マネージャのカウンタを表示します。

- **show event manager**

  このコマンドは、ヒット カウントやイベント マネージャ アプレットが最後に呼び出されたのはいつかなど、設定されたイベント マネージャ アプレットに関する情報を表示します。

- **show memory logging**、**show memory logging include**

これらのコマンドは、メモリ割り当てとメモリ使用量に関する統計情報を表示します。

- **show running-config event manager**

  このコマンドは、イベント マネージャの実行コンフィギュレーションを表示します。

EEM の履歴

表 *60 : EEM* の履歴

機能名	プラットフォーム リリース	説明
Embedded Event Manager（EEM）	9.2(1)	EEM サービスを利用することで、問題をデバッグし、トラブルシューティングに対して汎用ロギングを提供できます。EEM サービスには 2 つのコンポーネント、つまり EEM が応答またはリッスンするイベント、およびアクションと EEM が応答するイベントを定義するイベント マネージャ アプレットがあります。さまざまなイベントに応答し、さまざまなアクションを実行するために、複数のイベント マネージャ アプレットを設定できます。 **event manager applet**、**description**、**event syslog id**、**event none**、**event timer** {**watchdog time** *seconds* | **countdown time** *seconds* | **absolute time** *hh:mm:ss*}、**event crashinfo**、**action cli command**、**output** {**none** | **console** | **file** {**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*}}、**show running-config event manager**、**event manager run**、**show event manager**、**show counters protocol eem**、**clear configure event manager**、**debug event manager**、**debug menu eem** の各コマンドが導入または変更されました。
EEM のメモリ トラッキング	9.4(1)	メモリ割り当てとメモリ使用量をログに記録し、メモリ ロギング ラップ イベントに応答する新しいデバッグ機能が追加されました。 **memory logging**、**show memory logging**、**show memory logging include**、**event memory-logging-wrap** の各コマンドが導入または変更されました。

第 45 章

テストとトラブルシューティング

この章では、ASA のトラブルシューティング方法と基本接続のテスト方法について説明します。

- イネーブル パスワードと Telnet パスワードの回復 （1617 ページ）
- デバッグ メッセージの表示 （1621 ページ）
- パケット キャプチャ （1622 ページ）
- クラッシュ ダンプの表示 （1629 ページ）
- コア ダンプの表示 （1629 ページ）
- CPU 使用率とレポート （1629 ページ）
- 設定のテスト （1635 ページ）
- 接続のモニタリング （1649 ページ）
- テストおよびトラブルシューティングの履歴 （1650 ページ）

イネーブル パスワードと Telnet パスワードの回復

ASA 仮想 および ISA 3000 モデルでは、イネーブルパスワードまたは Telnet パスワードを忘れた場合に回復できます。CLI を使用してタスクを実行する必要があります。

（注） その他のプラットフォームでは、パスワードを忘れた場合に回復することはできません。工場出荷時のデフォルト設定に戻すことは可能で、パスワードをデフォルトにリセットできます。Firepower 4100/9300 の場合は、『FXOS configuration guide』を参照してください。他のモデルについては、『FXOS トラブルシューティング ガイド』を参照してください。

ISA 3000 でのパスワードの回復

ISA 3000 のパスワードの回復には、次の手順を実行します。

手順

ステップ 1 ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップ後、ROMMONモードに入るようにプロンプトが表示されたら、**Escape**キーを押します。

ステップ 4 コンフィギュレーション レジスタ値をアップデートするには、次のコマンドを入力します。

```
rommon #1> confreg 0x41

You must reset or power cycle for new config to take effect
```

ASAで現在のコンフィギュレーション レジスタ値と構成オプションのリストが表示されます。後で回復できるように、現在のコンフィギュレーションのレジスタ値を記録します。

```
Configuration Register: 0x00000041

Configuration Summary
 [ 0 ] password recovery
 [ 1 ] display break prompt
 [ 2 ] ignore system configuration
 [ 3 ] auto-boot image in disks
 [ 4 ] console baud: 9600
 boot: ..... auto-boot index 1 image in disks
```

ステップ 5 次のコマンドを入力して、ASA をリロードします。

```
rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.

Loading disk0:/asa932-226-k8.bin... Booting...Loading...
```

ASAは、スタートアップ コンフィギュレーションの代わりにデフォルト コンフィギュレーションをロードします。

ステップ 6 次のコマンドを入力して、特権 EXEC モードにアクセスします。

```
ciscoasa# enable
```

ステップ 7 パスワードの入力を求められたら、**Enter** キーを押します。

パスワードは空白です。

ステップ 8 次のコマンドを入力して、スタートアップ コンフィギュレーションをロードします。

```
ciscoasa# copy startup-config running-config
```

ステップ 9 次のコマンドを入力して、グローバル コンフィギュレーション モードにアクセスします。

```
ciscoasa# configure terminal
```

ステップ 10 次のコマンドを入力して、デフォルト コンフィギュレーションで必要に応じてパスワードを変更します。

```
ciscoasa(config)# password password
ciscoasa(config)# enable password password
ciscoasa(config)# username name password password
```

ステップ 11 次のコマンドを入力して、デフォルト コンフィギュレーションをロードします。

```
ciscoasa(config)# no config-register
```

デフォルト コンフィギュレーションのレジスタ値は 0x1 です。コンフィギュレーション レジスタの詳細については、コマンド リファレンスを参照してください。

ステップ 12 次のコマンドを入力して、新しいパスワードをスタートアップ コンフィギュレーションに保存します。

```
ciscoasa(config)# copy running-config startup-config
```

ASA 仮想 のパスワードまたはイメージの回復

ASA 仮想 のパスワードまたはイメージを回復するには、次の手順を実行します。

手順

ステップ 1 実行コンフィギュレーションを ASA 仮想 のバックアップ ファイルにコピーします。

copy running-config *filename*

例：

```
ciscoasa# copy running-config backup.cfg
```

ステップ 2 ASA 仮想 を再起動します。

reload

ステップ 3 [GNU GRUB] メニューから、下矢印を押し、**コンフィギュレーションをロードしない**オプションで <**filename**> を選択し、Enter キーを押します。ファイル名は、ASA 仮想 のデフォルトのブート イメージのファイル名です。デフォルトのブート イメージは、**fallback** コマンドによっ

て自動的にブートされることはありません。その後、選択したブート イメージをロードします。

```
GNU GRUB version 2.0(12)4
bootflash:/asa100123-20-smp-k8.bin
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

例：

```
GNU GRUB version 2.0(12)4
bootflash: /asa100123-20-smp-k8.bin with no configuration load
```

ステップ 4 実行コンフィギュレーションにバックアップ コンフィギュレーション ファイルをコピーします。

copy *filename* **running-config**

例：

```
ciscoasa (config)# copy backup.cfg running-config
```

ステップ 5 パスワードのリセット。

enable password *password*

例：

```
ciscoasa(config)# enable password cisco123
```

ステップ 6 新しい設定を保存します。

write memory

例：

```
ciscoasa(config)# write memory
```

ISA 3000 ハードウェアのパスワード回復の無効化

（注） ASA 仮想、Cisco Secure Firewall モデルでパスワード回復をディセーブルにすることはできません。

権限のないユーザーがパスワード回復メカニズムを使用して ASA を危険にさらすことがないように、パスワード回復をディセーブルにするには、次の手順を実行します。

始める前に

ASA で、**no service password-recovery** コマンドを使用すると ROMMON モードに入って、コンフィギュレーションの変更を防ぐことができます。ROMMON モードに入ると、ASA では、すべてのフラッシュ ファイル システムの消去を求めるプロンプトが表示されます。最初に消去を実行しないと、ROMMON モードを開始できません。フラッシュ ファイル システムを消去しない場合、ASA はリロードされます。パスワード回復は ROMMON モードの使用と既存のコンフィギュレーションの保持に依存しているので、この消去によって、パスワードの回復ができなくなります。ただし、パスワードを回復できなくすることで、不正なユーザーがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態に回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

service password-recovery コマンドは、コンフィギュレーション ファイルに通知用としてのみ表示されます。CLI プロンプトに対してコマンドを入力すると、設定は NVRAM に保存されます。設定を変更する唯一の方法は、CLI プロンプトでコマンドを入力することです。このコマンドの異なるバージョンで新規コンフィギュレーションをロードしても、設定は変更されません。（パスワード回復の準備段階で）スタートアップ時にスタートアップ コンフィギュレーションを無視するよう ASA が設定されている場合にパスワード回復をディセーブルにすると、通常どおりスタートアップ コンフィギュレーションをロードするように ASA の設定が変更されます。フェールオーバーを使用し、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置が設定されている場合は、**no service password- recovery** コマンドでスタンバイ装置に複製したときに、コンフィギュレーション レジスタに同じ変更が加えられます。

手順

パスワード回復をディセーブルにします。

no service password-recovery

例：

```
ciscoasa (config)# no service password-recovery
```

デバッグ メッセージの表示

デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。デバッグをこのような時間帯に行うと、**debug** コマンド処理のオーバーヘッドの増加によりシステムの使用に影響が及ぶ可能性が少な

くなります。デバッグ メッセージを有効にするには、コマンド リファレンスの **debug** コマンドを参照してください。

パケット キャプチャ

パケットキャプチャは、接続の問題のトラブルシューティングまたは不審なアクティビティのモニタリングを行うときに役立つことがあります。パケット キャプチャ サービスを使用する場合は、Cisco TAC に連絡することをお勧めします。

パケット キャプチャのガイドライン

コンテキスト モード

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
- 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
- キャプチャを指定したインターフェイスに着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN 上の他のコンテキストへのトラフィックも含まれます。したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブキャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

その他のガイドライン

- ASA が不正な形式の TCP ヘッダーを持つパケットを受信し、ASP が *invalid-tcp-hdr-length* であるというドロップ理由でそのパケットをドロップする場合、そのパケットを受信したインターフェイス上の **show capture** コマンド出力は、そのパケットを表示しません。
- IP トラフィックだけをキャプチャできます。ARP などの非 IP パケットはキャプチャできません。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。

- パケットキャプチャには、システムを変更する、またはインスペクションのために接続に挿入されるパケット、NAT、TCPの正規化、パケットの内容を調整するその他の機能が含まれます。
- データパスに挿入された仮想パケットの寿命のトレースは、データパスでの物理パケットの処理を正確に反映していません。この違いは、ソフトウェアバージョン、構成、および挿入された仮想パケットのタイプによって異なります。違いが生じる原因となる可能性がある構成の設定を次に示します。
  - 同じホストに対して 2 つ以上の NAT ステートメントが存在する。
  - 接続の順方向と逆方向のフローでプロトコルが異なる（順方向のフローが UDP または TCP で、逆方向のフローが ICMP である場合など）。
  - ICMP エラーインスペクションが有効になっている。

パケットのキャプチャ

パケットをキャプチャするには、次の手順を実行します。

手順

ステップ 1 パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**file-size**] [**headers-only**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

例：

```
ciscoasa# capture captest interface inside
```

キャプチャするすべてのパケットのインターフェイスを設定する必要があります。複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ *capture_name* を使用します。

type asp-dropキーワードは、高速セキュリティ パスでドロップされるパケットをキャプチャします。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。マルチ コンテキスト モードでは、このオプションがシステム実行スペースで発行されると、すべてのドロップされたデータ パケットがキャプチャされます。このオプションがコンテキストで発行されたときは、ドロップされたデータ パケットのうち、そのコンテキストに属するインターフェイスから入ったものだけがキャプチャされます。

type raw-data キーワードは、着信パケットと発信パケットをキャプチャします。この設定は、デフォルトです。

inline-tag *tag* のキーワードと引数のペアは、特定の SGT 値のタグを指定します。指定しない場合は、任意の SGT 値を持つタグ付きパケットをキャプチャします。

buffer キーワードは、パケットを保存するために使用するバッファ サイズを定義します。このバイト バッファがいっぱいになると、パケット キャプチャは停止します。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。**circular-buffer** キーワードを指定すると、バッファがいっぱいになったときに、バッファが先頭から順に上書きされます。

ethernet-type キーワードは、キャプチャするイーサネットタイプを設定します。サポートされるイーサネット タイプには、8021Q、ARP、IP、IP6、LACP、PPPOED、PPPOES、RARP、および VLAN などがあります。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、照合には内部イーサネット タイプが使用されます。IP はデフォルトのイーサネットタイプです。

interface キーワードは、パケット キャプチャを使用するインターフェイスの名前を設定します。

データプレーン上のパケットをキャプチャするには、**asa_dataplane** キーワードを使用します。

キャプチャファイルのサイズを設定するには、**file-size** キーワードを使用します。ファイルサイズは 32 ー 10000 MB です。

データを含まないパケットの L2、L3、および L4 ヘッダーだけをキャプチャする場合は、**headers-only** コマンドを使用します。

match キーワードは、一致するプロトコルおよび送信元と宛先 IP アドレス、およびオプションのポートをキャプチャします。このキーワードは、1つのコマンドで3回まで使用できます。**any**キーワードは、IPv4 トラフィックだけをキャプチャします。**any4** および **any6** キーワードを使用して、一致する IPv4 および IPv6 ネットワーク トラフィックを個別にキャプチャできます。operator には次のいずれかを指定できます。

- lt：より小さい
- gt：より大きい
- eq：等しい

real-time キーワードを指定すると、キャプチャしたパケットがリアルタイムで連続して表示されます。

reinject-hide キーワードを指定すると、再注入されたパケットはキャプチャされません。これは、クラスタリング環境にのみ適用されます。

（注）
ACL の最適化が設定されている場合、**access-list** コマンドはキャプチャでは使用できません。**access-group** コマンドのみ使用できます。この場合、**access-list** コマンドを使用しようとするとエラーが表示されます。

ステップ 2 クラスタ制御リンク トラフィックをキャプチャします。

capture*capture_name*{ **type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**cp-cluster**] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* { **host** *source-ip* | *source-ip mask* | **any** | **any4**|**any6**} [*operator src_port*] { **host** *dest_ip* |*dest_ip mask* | **any** | **any4**|**any6**} [*operator dest_port*]]

例：

```
ciscoasa# capture ccl type lacp interface GigabitEthernet0/0
ciscoasa# capture ccl interface cluster match udp any eq 49495 any
ciscoasa# capture ccl interface cluster match udp any any eq 49495
```

次の2つの方法でクラスタ制御リンクのトラフィックをキャプチャできます。クラスタ制御リンクのすべてのトラフィックをキャプチャするには、インターフェイス名に **cluster** キーワードを使用します。cLACP パケットのみをキャプチャするには **type lacp** を指定し、インターフェイス名ではなく物理インターフェイス ID を指定します。クラスタ制御リンク上のパケットには、コントロール プレーン パケットとデータ プレーン パケットの 2 種類があり、どちらも、転送されたデータ トラフィックとクラスタ LU メッセージが含まれています。IP アドレス ヘッダーの TTL フィールドは、この 2 種類のパケットを区別できるように符号化されます。転送されたデータ パケットがキャプチャされるときは、デバッグのためにクラスタリング トレーラもキャプチャ ファイルに出力されます。

キーワード **cp-cluster** はクラスタ制御リンク（およびデータ プレーン パケットなし）でコントロール プレーン パケットのみをキャプチャできるようになりました。このオプションは、マルチ コンテキスト モードのシステムで、ACL を使用してトラフィックを照合できない場合に役立ちます。

ステップ 3 クラスタ全体のパケットをキャプチャします。

cluster exec capture *capture_name arguments*

ステップ 4 スイッチの出力トラフィック パケットをキャプチャします（Cisco Secure Firewall 4200 モデル デバイスでのみサポートされています）。

capture *capture_name* **switch interface** *interface_name* **direction egress**

（注）
both 引数を使用して、スイッチの出力トラフィックと入力トラフィックの両方のキャプチャを作成します。

ステップ 5 パケット キャプチャを停止します。

no capture *capture_name*

リアルタイム パケット キャプチャを終了するには、**Ctrl + c** を入力します。キャプチャを完全に削除するには、このコマンドの **no** 形式を使用します。リアルタイム オプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにのみ適用されます。

ステップ 6 バッファからパケットを削除せずに手動でパケット キャプチャを停止する場合：

capture *name* **stop**

ステップ 7 再度キャプチャを開始する場合：

no capture *name***stop**

ステップ 8 クラスタ ユニットで永続的なパケット トレースをキャプチャします。

cluster exec *capture_test* **persist**

ステップ 9 永続的なパケット トレースをクリアします。

cluster exec *clear* **packet-trace**

ステップ 10 復号化された IPsec パケットをキャプチャします。

cluster exec *capture_test* **include-decrypted**

ステップ 11 キャプチャをクリアします。

clear capture *capture_name*

例

コントロール プレーン パケット

コントロールプレーンと通信するすべてのパケットはTTLが255に設定されており、ポート番号49495がクラスタリング コントロール プレーン リッスン ポートに使用されます。次の例では、クラスタリング環境の LACP キャプチャを作成する方法を示します。

```
ciscoasa# capture lacp type lacp interface GigabitEthernet0/0
```

次の例では、クラスタリング リンクでの制御パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa# capture cp interface cluster match udp any eq 49495 any
ciscoasa# capture cp interface cluster match udp any any eq 49495
```

データ プレーン パケット

データ パケットには、1 つのユニットから別のユニット（その接続の所有者）に転送されるパケットと、クラスタ LU メッセージが含まれます。通常のクラスタ LU 更新メッセージは、TTL が 254 に設定されており、TTL が 253 に設定された特別な LU パケットがあります。この特別な LU パケットは TCP のみで、ディレクタが新しいフローの所有者を選択した場合にのみ発生します。ディレクタはCLU_FULLアップデート パケットとともに要求パケットを送り返します。LU パケットには、元のパケットの L3/L4 ヘッダーが書き込まれます。これにより、受信者側で潜在的な競合状態が発生するのを回避できます。転送されるデータ パケットは、TTL が 4 未満に設定されます。次の例では、クラスタ制御リンクでデータ パス パケットのキャプチャを作成する

方法を示します。クラスタ間データプレーンの「flow logical update」メッセージをすべてキャプチャするには、ポート 4193 を使用します。

```
ciscoasa# access-list cc1 extended permit udp any any eq 4193
ciscoasa# access-list cc1 extended permit udp any eq 4193 any
ciscoasa# capture dp interface cluster access-list cc1
```

パケット キャプチャの表示

CLI でパケット キャプチャをブラウザ上に表示したり、任意のサーバーにキャプチャをダウンロードしたりすることができます。

手順

ステップ 1 CLI でキャプチャを表示するには：

[**cluster exec**] **show capture** [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

例：

```
ciscoasa# show capture capin

 8 packets captured

 1: 03:24:35.526812       192.168.10.10 > 203.0.113.3: icmp: echo request
 2: 03:24:35.527224       203.0.113.3 > 192.168.10.10: icmp: echo reply
 3: 03:24:35.528247       192.168.10.10 > 203.0.113.3: icmp: echo request
 4: 03:24:35.528582       203.0.113.3 > 192.168.10.10: icmp: echo reply
 5: 03:24:35.529345       192.168.10.10 > 203.0.113.3: icmp: echo request
 6: 03:24:35.529681       203.0.113.3 > 192.168.10.10: icmp: echo reply
 7: 03:24:57.440162       192.168.10.10 > 203.0.113.3: icmp: echo request
 8: 03:24:57.440757       203.0.113.3 > 192.168.10.10: icmp: echo reply
```

access-list キーワードは、特定のアクセス リスト ID の IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。

cluster exec キーワードを使用すると、あるユニットで **show capture** コマンドを発行し、他のすべてのユニットでそのコマンドを同時に実行できます。

count キーワードは、指定したデータのパケット数を表示します。

decode キーワードは、**isakmp** タイプのキャプチャがインターフェイスに適用される場合に役立ちます。当該のインターフェイスを通過する ISAKMP データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報とともに表示されます。パケットのデコード出力は、パケットのプロトコルによって異なります。通常、このコマンドは、ICMP、UDP、および TCP プロトコルの IP デコードをサポートします。バージョン 9.10(1) から、このコマンドは GRE および IPinIP の IP デコードもサポートします。

detail キーワードは、各パケットの追加のプロトコル情報を表示します。

dump キーワードは、データ リンク経由で転送されたパケットの 16 進ダンプを表示します。

packet-number キーワードは、指定したパケット番号で表示を開始します。

ステップ 2 ブラウザでパケット キャプチャを表示するには：

https://*ip_of_asa*/**admin/capture/***capture_name*/**pcap**

pcap キーワードを省略すると、**show capture** *capture_name* コマンド出力に相当する内容のみが表示されます。

マルチ コンテキスト モードでは、システム実行スペースでのみ **copy capture** コマンドを使用できます。

ステップ 3 パケット キャプチャをサーバーにコピーします。この例では FTP を示します。

[**cluster exec**] **copy /pcap capture:**[*context-name*/]*capture_name* **ftp://***username***:***password***@***server_ip***/***path*

pcap キーワードを省略すると、**show capture** *capture_name* コマンド出力に相当する内容のみが表示されます。

（注）
パケットキャプチャをディスクにコピーする場合は、キャプチャファイル名が 63 文字以下であることを確認してください。ファイル名が 63 文字を超える場合、パケットキャプチャは成功しますが、ディスクへのキャプチャのコピーは失敗します。

例

次の例は、asp-drop タイプのキャプチャを示します。

```
ciscoasa# capture asp-drop type asp-drop acl-drop
ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown

ciscoasa# show capture asp-drop

 2 packets captured

 1: 04:12:10.428093       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2: 04:12:12.427330       192.168.10.10.34327 > 10.94.0.51.15868: S
    2669456341:2669456341(0) win 4128 <mss 536> Drop-reason: (acl-drop)
    Flow is denied by configured rule
 2 packets shown
```

次の例は、ethernet タイプのキャプチャを示します。

```
ciscoasa# capture arp ethernet-type arp interface inside
ciscoasa# show cap arp

22 packets captured

   1: 05:32:52.119485       arp who-has 10.10.3.13 tell 10.10.3.12
   2: 05:32:52.481862       arp who-has 192.168.10.123 tell 192.168.100.100
   3: 05:32:52.481878       arp who-has 192.168.10.50 tell 192.168.100.10
   4: 05:32:53.409723       arp who-has 10.106.44.135 tell 10.106.44.244
   5: 05:32:53.772085       arp who-has 10.106.44.108 tell 10.106.44.248
   6: 05:32:54.782429       arp who-has 10.106.44.135 tell 10.106.44.244
   7: 05:32:54.784695       arp who-has 10.106.44.1 tell 11.11.11.112:
```

クラッシュ ダンプの表示

ASA か ASA 仮想 がクラッシュした場合に、クラッシュダンプ情報を表示できます。クラッシュ ダンプの内容を調べる必要がある場合は、Cisco TAC に連絡することを推奨します。コマンド リファレンスで **show crashdump** コマンドを参照してください。

コア ダンプの表示

コア ダンプは、プログラムが異常終了（クラッシュ）したときの、実行中のプログラムのスナップショットです。コア ダンプは、エラーを診断またはデバッグするため、および障害を後からオフサイトで分析できるよう、クラッシュを保存するために使用されます。ASA か ASA 仮想 でのアプリケーションまたはシステムクラッシュをトラブルシューティングするために、コアダンプ機能を有効にするよう Cisco TAC から要請される場合があります。コマンドリファレンスで **coredump** コマンドを参照してください。

CPU 使用率とレポート

CPU使用率レポートには、指定された時間内に使用されたCPUの割合の要約が表示されます。通常、コアはピーク時以外には合計 CPU 容量の約 30 ～ 40% で動作し、ピーク時は約 60 ～ 70% の容量で動作します。

の vCPU 使用率ASA 仮想

CPU 使用率の統計を表示するには、ASA 仮想 で **show cpu usage** コマンドを使用します。ASA 仮想 の vCPU 使用率では、データ パス、制御ポイント、および外部プロセスで使用されている vCPU の量を表示します。

（VMware、Azure、OCI などの）クラウド サービス プロバイダーによって報告される vCPU 使用率には、示されている ASA 仮想 使用率に加えて、以下が含まれます。

- ASA 仮想 のアイドル時間
- ASA VM に使用された %SYS オーバーヘッド
- vSwitch、vNIC および pNIC の間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASA 仮想 のレポート：40%
- DP：35%
- 外部プロセス：5%
- vSphere のレポート：95%
- ASA（ASA 仮想 レポートとして）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

ASA 仮想 のためのオーバーヘッドとして、ESXi サーバが追加のコンピューティング リソースを使用する場合があるため、使用率は 100% を超えることがあります。

VMware の CPU 使用率のレポート

vSphere で [VM Performance] タブをクリックし、[Advanced] をクリックすると [Chart Options] ドロップダウンリストが表示されます。ここには VM の各ステート（%USER、%IDLE、%SYS など）の vCPU 使用率が表示されます。この情報は、VMware の観点から CPU リソースが使用されている場所を理解するのに役立ちます。

ESXi サーバーのシェル（ホストへの接続に SSH を使用してシェルにアクセスします）では、esxtop を使用できます。Esxtop は Linux の **top** コマンドに似た操作性と外観を持ち、次の内容を含む vSphere のパフォーマンスに関する VM のステート情報を提供します。

- vCPU、メモリ、ネットワーク使用率の詳細
- 各 VM のステートごとの vCPU 使用率
- メモリ（実行中に「M」と入力）とネットワーク（実行中に「N」と入力）に加えて、統計情報と RX ドロップ数

ASA 仮想 と vCenter のグラフ

ASA 仮想 と vCenter の CPU 使用率の数値には違いがあります。

- vCenter のグラフの数値は常に ASA 仮想 の数値よりも大きくなります。
- vCenter ではこの値は %CPU usage と呼ばれ、ASA 仮想 ではこの値は %CPU utilization と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

vCenter は CPU % usage を次のように計算します。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

使用率を MHz で比較すると、vCenter と ASA 仮想 両方の数値は一致します。vCenter グラフから、MHz % CPU 使用率は 60/(2499 x 1 vCPU) = 2.4 と求められます。

Amazon CloudWatch CPU 使用率レポート

メトリックエクスプローラを表示して、タグとプロパティでリソースをモニターできます。特定のインスタンスの CPU 使用率の統計を表示するには、次の手順を実行します。

手順

ステップ 1 [CloudWatch] コンソールを開き、ナビゲーションペインで [メトリクス（Metrics）] を選択します。

ステップ 2 **EC2** メトリクスの名前空間を選択し、[インスタンスごとのメトリクス（Per-instance Metrics）] ディメンションを選択します。

ステップ 3 検索フィールドに **CPUUtilization** と入力して Enter を押します。必要なインスタンスの行を選択し、そのインスタンスの **CPUUtilization** メトリックのグラフを表示します。

詳細については、Amazon CloudWatch のドキュメントを参照してください。

ASA 仮想 と Amazon CloudWatch のグラフ

Amazon CloudWatch のグラフの数値は、CPU 使用率の計算方法が ASA 仮想 と CloudWatch で異なるため、数値よりも大きくなっています。

ASA 仮想 がポーリングモードで実行されている場合、各 CPU は、省電力モードやその他のアイドル状態に入る代わりに、軽量コマンドのループを実行します。これにより、インテルの電源状態によってオンオフを切り替えたりクロックを調整したりするのではなく、各コアが常にアクティブに保たれてパフォーマンスが向上します。

ASA 仮想 内では、このアクティビティはアイドリング動作であると認識され、CPU 使用率が正しく計算されます。ただし、Amazon CloudWatch では、すべての CPU サイクルに実行する命令があるため、アイドル状態の動作は通常の CPU アクティビティのように見えます。これにより、CloudWatch では高い CPU 使用率（85 ～ 90%）が表示されます。

Azure の CPU 使用率レポート

Azure Monitor から VM Insights を使用して、監視対象の VM すべての CPU 使用率を表示するには、次の手順を実行します。

手順

ステップ 1 Azure ポータルに移動し、[監視（Monitor）] を選択してから [ソリューション（Solutions）] セクションで [仮想マシン（Virtual Machines）] を選択します。

ステップ 2 [パフォーマンス（Performance）] タブを選択して [CPU使用率（CPU Utilization %）] グラフを表示します。このグラフには、平均プロセッサ使用率が最も高い上位5つのマシンが表示されます。

特定の Azure VM から直接 CPU 使用率グラフを表示するには、次の手順を実行します。

手順

ステップ 1 Azure ポータルに移動し、[仮想マシン（Virtual Machines）] を選択します。

ステップ 2 VM のリストから VM を選択します。

ステップ 3 [モニタリング（Monitoring）] セクションで、[Insights] を選択します。

ステップ 4 **[パフォーマンス（Performance）]** タブを選択します。

詳細については、「How to chart performance with VM insights」[英語] を参照してください。

ASA 仮想 と Azure のグラフ

ASA 仮想 と Azure の CPU 使用率の数値には違いがあります。Azure は、使用可能な CPU の合計に対する割合として指定される、アクティブに使用されている仮想 CUP の量として CPU 使用率を計算するため、Azure のグラフの数値は常に ASA 仮想 の数値より高くなります。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率/仮想 CPU の数 X コア周波数」として計算されます。

Azure は、ゲスト OS によって要求される CPU の量にもレート制限を適用します。ASA 仮想 が 40% の CPU 使用率を報告し、ハイパーバイザが 90% の CPU 使用率を報告しているシナリオについて考えてみましょう。ここで ASA 仮想 がさらなる処理能力を求めた場合、CPU 使用率が 80% を超え、ハイパーバイザが 95% を超える CPU 使用率を報告する可能性があります。これにより、ASA 仮想 がポーリングモードで軽量コマンドのループを実行しているだけでアイドリング動作を示していたとしても、ハイパーバイザは ASA 仮想 CPU をスロットリングすることになります。

Hyper-V CPU 使用率レポート

使用可能なクラウドサーバーの CPU、RAM、およびディスク容量の構成情報の表示に加えて、ディスク、I/O、およびネットワーク情報も表示できます。この情報を使用して、ニーズに適したクラウドサーバーを決定してください。コマンドライン nova クライアントまたは **Cloud Control Panel** インターフェイスを使用して、使用可能なサーバーを表示できます。

コマンドラインで、次のコマンドを実行します。

```
nova flavor-list
```

使用可能なすべてのサーバー構成が表示されます。リストには、次の情報が含まれています。

- ID：サーバー構成 ID
- 名前：RAM サイズとパフォーマンスタイプでラベル付けされた構成名
- Memory_MB：構成の RAM の量
- ディスク：GB 単位のディスクサイズ（汎用クラウドサーバーの場合、システムディスクのサイズ）
- エフェメラル：データディスクのサイズ

- スワップ：スワップ領域のサイズ
- VCPU：構成に関連付けられた仮想 CPU の数
- RXTX_Factor：サーバーに接続された PublicNet ポート、ServiceNet ポート、および分離されたネットワーク（クラウドネットワーク）に割り当てられる帯域幅の量（Mbps 単位）
- Is_Public：未使用

ASA Virtual と Hyper-V のグラフ

ASA Virtual と Hyper-V の CPU 使用率の数値には違いがあります。

- Hyper-V のグラフの数値は ASA Virtual の数値よりも常に大きくなります。
- Hyper-V ではこの値は %CPU usage と呼ばれ、ASA Virtual ではこの値は %CPU utilization と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

Hyper-V では %CPU usage は次のように計算されます。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

（注） 正確な CPU 使用率を得るには、ASA Virtual レポートを調べることをお勧めします。

OCI CPU 使用率レポート

コンピューティング インスタンス メトリック **oci_computeagent** を使用して、OCI の CPU 使用率を表示できます。CpuUtilization メトリックは、CPU からのアクティビティレベルを表示し、

合計時間に対する割合として表されます。単一のコンピューティングインスタンスのメトリックグラフを表示するには、次の手順を実行します。

手順

ステップ 1 ナビゲーションメニューを開き、[コンピューティング（Compute）] の下の [インスタンス（Instances）] をクリックします。

ステップ 2 インスタンスをクリックし、[リソース（Resources）]の下の [メトリック（Metrics）] をクリックします。

ステップ 3 メトリック名前空間リストで [oci_computeagent] を選択します。

詳細については、コンピューティング インスタンス メトリックを参照してください。

ASA 仮想 と OCI のグラフ

OCI は、使用可能な CPU の合計に対する割合として指定される、アクティブに使用されている仮想 CUP の量として CPU 使用率を計算するため、OCI のグラフの数値は常に ASA 仮想 の数値より高くなります。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率/仮想 CPU の数 X コア周波数」として計算されます。

設定のテスト

ここでは、シングル モード ASA または各セキュリティ コンテキストの接続性のテスト方法、ASA インターフェイスを ping する方法、およびあるインターフェイス上のホストから他のインターフェイス上のホストに ping できるようにする方法について説明します。

基本接続のテスト：アドレス向けの ping の実行

ping は、特定のアドレスが使用可能で、応答するかどうかを確認するための単純なコマンドです。次のトピックでは、このコマンドの詳細とそれを使って実行可能なテストについて説明します。

ping で実行可能なテスト

デバイスを ping すると、そのデバイスにパケットが送信され、デバイスが応答を返します。このプロセスを使用して、ネットワーク デバイスは、相互に検出、識別、およびテストすることができます。

ping を使用して、次のテストを実行できます。

- 2 つのインターフェイスのループバック テスト：同じ ASA で一方のインターフェイスからもう一方のインターフェイスに ping を外部ループバック テストとして起動すると、双方のインターフェイスの基本的な「アップ」ステータスおよび動作を検証できます。
- ASA の ping：別の ASA のインターフェイスを ping し、そのインターフェイスがアップしていて応答することを確認できます。
- ASA 経由の ping：ASA の反対側のデバイスを ping することによって、中間 ASA 経由で ping することができます。パケットは、それぞれの方向に移動するときに、2 つの中間 ASA のインターフェイスを通過します。このアクションは、中間ユニットのインターフェイス、動作、および応答時間の基本テストになります。
- ネットワーク デバイスの疑わしい動作をテストするための ping：ASA インターフェイスから、正常に機能していないと思われるネットワーク デバイスに ping することができます。インターフェイスが正しく設定されているにもかかわらずエコーが受信されない場合は、デバイスに問題があると考えられます。
- 中間通信をテストするための ping：ASA インターフェイスから、正常に機能することがわかっているネットワーク デバイスに ping することができます。エコーを受信した場合、中間にあるデバイスがすべて正常に動作し、物理的に正しく接続されていることが確認されたことになります。

ICMP ping と TCP ping の選択

ASA には、ICMP エコー要求パケットを送信して、エコー応答パケットを受信する従来の ping が付属しています。これは、標準ツールで、すべての仲介ネットワーク デバイスで ICMP トラフィックが許可される場合にうまく機能します。ICMP ping を使用して、IPv4/IPv6 アドレスまたはホスト名を ping することができます。

ただし、ICMP を禁止しているネットワークもあります。ご使用のネットワークがこれに該当する場合は、代わりに、TCP ping を使用してネットワーク接続をテストできます。TCP ping では、ping から TCP SYN パケットが送信され、応答で SYN-ACK が受信された段階でその ping が成功したと見なされます。また、TCP ping では、IPv4 アドレスまたはホスト名は ping できますが、IPv6 アドレスは ping できません。

正常な ICMP または TCP ping とは、使用されているアドレスが有効で特定のタイプのトラフィックに応答することを意味しているにすぎません。これは基本接続が機能していることを意味します。デバイス上で動作する他のポリシーで、特定のタイプのトラフィックがデバイスを通過できないようにすることができます。

ICMP の有効化

デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへの ping を実行できます。リターン トラフィックを通過させるように ICMP インスペクションをイネーブルにすることだけが必要です。セキュリティの低いインターフェイスから高いインターフェイスに ping するには、トラフィックを許可する ACL を適用する必要があります。

ASA インターフェイスを ping する場合は、そのインターフェイスに適用された ICMP ルールによって、エコー要求パケットとエコー応答パケットが許可される必要があります。ICMP ルールは省略可能です。このルールを設定しなかった場合は、インターフェイスへのすべての ICMP トラフィックが許可されます。

この手順では、ASA インターフェイスの ICMP ping をイネーブルにするため、または、ASA 経由の ping 用に構成する必要のある ICMP コンフィギュレーションのすべてについて説明します。

手順

ステップ 1 ICMP ルールでエコー要求/エコー応答が許可されることを確認します。

ICMP ルールは、省略可能で、インターフェイスに直接送信される ICMP パケットに適用されます。ICMP ルールを適用しなかった場合は、すべての ICMP アクセスが許可されます。この場合は、アクションが不要です。

ただし、ICMP ルールを実装する場合は、少なくとも以下の「inside」をご使用のデバイスのインターフェイス名に置き換えたものが各インターフェイスに含まれていることを確認します。

```
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo inside
ciscoasa(config)# icmp permit 0.0.0.0 0.0.0.0 echo-reply inside
```

ステップ 2 アクセス ルールで ICMP が許可されることを確認します。

ASA 経由でホストを ping する場合は、アクセス ルールで ICMP トラフィックの送受信が許可される必要があります。アクセス ルールは、少なくとも、エコー要求/エコー応答 ICMP パケットを許可する必要があります。これらのルールはグローバル ルールとして追加することができます。

アクセス ルールがインターフェイスに適用されている、または、グローバルに適用されている場合は、次のようなルールを関連 ACL に追加するだけです。

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any
anyecho-reply
```

または、すべての ICMP を許可するだけです。

```
ciscoasa(config)# access-list outside_access_in extendedpermit icmp any any
```

アクセスルールを使用しない場合は、必要な他のタイプのトラフィックも許可する必要があります。これは、インターフェイスにアクセス ルールを適用すると、暗黙の deny が追加されるため、他のすべてのトラフィックが破棄されるためです。ACL をインターフェイスに適用する、または、グローバルに適用するには、**access-group** コマンドを使用します。

単にテスト目的でルールを追加する場合は、**access-list** コマンドの **no** 形式を使用して ACL からルールを削除できます。ACL 全体をテストするだけの場合は、**no access-group** コマンドを使用してインターフェイスから ACL を削除します。

ステップ 3 ICMP インスペクションをイネーブルにします。

インターフェイスの ping とは対照的に、ASA 経由で ping する場合は、ICMP インスペクションが必要です。インスペクションを使用すれば、リターン トラフィック（つまり、エコー応答パケット）を ping を開始したホストに返すことができるうえ、パケットあたり 1 つの応答の存在が保証されるため、特定のタイプの攻撃を防止することができます。

ICMPインスペクションは、デフォルトのグローバルインスペクション ポリシーでイネーブルにできます。

```
ciscoasa(config)# policy-map  global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect icmp
```

ホストの ping

デバイスを ping するには、**ping 10.1.1.1** や **ping www.example.com** のように IP アドレスやホスト名と一緒に **ping** を入力します。TCP ping の場合は、**ping tcp www.example.com 80** のように **tcp** キーワードと宛先ポートを含めます。通常は、実行する必要のあるテストの範囲にします。

成功した ping の出力例：

```
Sending 5, 100-byte ICMP Echos to out-pc, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

ping が失敗した場合は、失敗した試行が？で示され、成功率が 100% 未満になります（すべて失敗した場合は 0% になります）。

```
Sending 5, 100-byte ICMP Echos to 10.132.80.101, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ただし、pingの一部の側面を制御するパラメータを追加することもできます。以下に基本オプションを示します。

- ICMP ping。

  ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes*] [**validate**]

  それぞれの説明は次のとおりです。

  - *if_name* は、ping の送信元 IP アドレスを指定します。ただし、出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。
  - *host* は、ping するホストの IPv4 アドレス、IPv6 アドレス、またはホスト名です。
  - **repeat** *count* は、送信するパケット数です。デフォルトは 5 分です。
  - **timeout** *seconds* は、応答がなかった場合にタイムアウトするパケットごとの秒数です。デフォルトは 2 です。
  - **data** *pattern* は、送信するパケットに使用される 16 進数のパターンです。デフォルトは 0xabcd です。
  - **size** *bytes* は、送信するパケットの長さです。デフォルト値は 100 バイトです。
  - **validate** は、応答データを検証する必要があることを示します。

- TCP ping。

  ping tcp [*if_name*] *host* [*port*] [**repeat** *count*] [**timeout** *seconds*] [**source** *host* [*ports*]

  それぞれの説明は次のとおりです。

  - *if_name* は、ping の送信元 IP アドレスを指定します。ただし、出力インターフェイスは、データルーティングテーブルを使用したルートルックアップによって決定されます。
  - *host* は、ping する宛先の IPv4 アドレスまたはホスト名です。TCP ping は IPv6 アドレスと一緒に使用できません。
  - *port* は、ping するホストの TCP ポートです。
  - **repeat** と **timeout** は、上記と同じ意味です。
  - **source** *host port* は、ping 用の送信元 IP アドレスおよびポートを示します。ランダムポートを取得するには、ポート 0 を使用します。

- インタラクティブ ping。

  ping

  パラメータを指定せずに ping を入力した場合は、インターフェイス、宛先、およびキーワードとして使用できない拡張パラメータを含むその他のパラメータが要求されます。ping パケットを細かく制御する必要がある場合は、この方式を使用します。

ASA 接続の体系的なテスト

ASA 接続のさらに体系的なテストを実行する場合は、次の一般的な手順を使用できます。

始める前に

手順で説明したsyslogメッセージを確認する場合は、ロギングをイネーブルにします（**logging enable** コマンドまたは ASDM の [Configuration] > [Device Management] > [Logging] > [Logging Setup]）。

また、必須ではありませんが、ICMPデバッグをイネーブルにして、外部デバイスからASAインターフェイスを ping したときのメッセージを ASA コンソールに表示することもできます（ASA を通過する ping に関するデバッグ メッセージは表示されません）。ping メッセージとデバッグ メッセージをイネーブルにするのはトラブルシューティング中だけにすることをお勧めします。これらのメッセージはパフォーマンスに影響する可能性があります。次に、ICMP デバッグをイネーブルにして、Telnet または SSH セッションに送信する syslog メッセージを設定し、それらをセッションに送信して、ロギングをイネーブルにする例を示します。または、**logging monitor debug** コマンドの代わりに、**logging buffer debug** コマンドを使用してログ メッセージをバッファに送信し、後で **show logging** コマンドを使用してそれらを表示することもできます。

```
ciscoasa(config)# debug icmp trace
ciscoasa(config)# logging monitor debug
ciscoasa(config)# terminal monitor
ciscoasa(config)# logging enable
```

この設定では、外部ホスト（209.165.201.2）から ASA の外部インターフェイス（209.165.201.1）への ping が成功すると、次のように表示されます。

```
ciscoasa(config)# debug icmp trace
Inbound ICMP echo reply (len 32 id 1 seq 256) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 512) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 512) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 768) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 768) 209.165.201.1 > 209.165.201.2
Outbound ICMP echo request (len 32 id 1 seq 1024) 209.165.201.2 > 209.165.201.1
Inbound ICMP echo reply (len 32 id 1 seq 1024) 209.165.201.1 > 209.165.201.2
```

この出力では、ICMP パケット長（32 バイト）、ICMP パケット識別子（1）、および ICMP シーケンス番号（ICMP シーケンス番号は 0 から始まり、要求が送信されるたびに増分されます）が示されています。

テストが終了したら、デバッグをディセーブルにします。この設定をそのままにしておくと、パフォーマンスとセキュリティのリスクが高まります。テストのためだけにロギングをイネーブルにした場合は、それもディセーブルにできます。

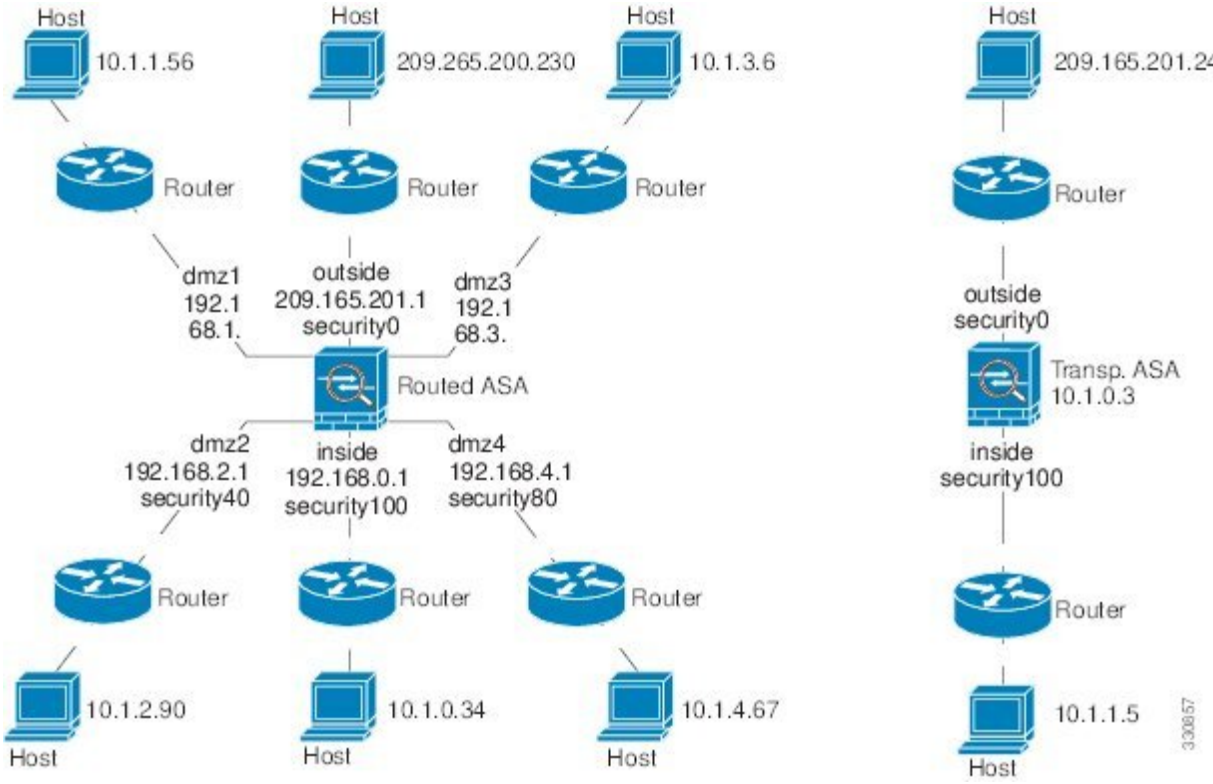
```
ciscoasa(config)# no debug icmp trace
ciscoasa(config)# no logging monitor debug
```

```
ciscoasa(config)# no terminal monitor
ciscoasa(config)# no logging enable
```

手順

ステップ 1 インターフェイス名、セキュリティ レベル、および IP アドレスを示すシングル モードの ASA またはセキュリティ コンテキストの図を作成します。図には、直接接続されたすべてのルータ、および ASA を ping するルータの反対側にあるホストも含める必要があります。

図 *90*：インターフェイス、ルータ、およびホストを含むネットワーク図



ステップ 2 直接接続されたルータから各 ASA インターフェイスを ping します。トランスペアレント モードでは、BVI IP アドレスを ping します。このテストでは、ASA インターフェイスがアクティブであること、およびインターフェイス コンフィギュレーションが正しいことを確認します。

ASA インターフェイスがアクティブではない場合、インターフェイス コンフィギュレーションが正しくない場合、または ASA とルータの間でスイッチがダウンしている場合、ping は失敗する可能性があります（次の図を参照）。この場合は、パケットが ASA に到達しないので、デバッグ メッセージや syslog メッセージは表示されません。

図 *91 : ASA* インターフェイスでの *ping* の失敗

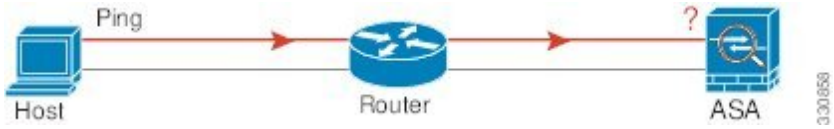
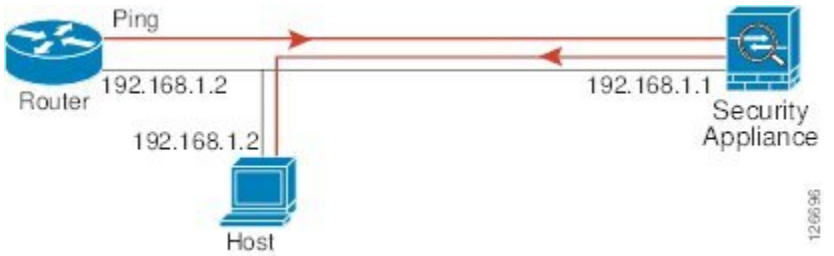


図 *92 : IP* アドレッシングの問題による *ping* の失敗



ping 応答がルータに戻されない場合は、スイッチ ループまたは冗長 IP アドレスが存在する可能性があります（次の図を参照）。

ステップ 3 リモート ホストから各 ASA インターフェイスを ping します。トランスペアレント モードでは、BVI IP アドレスを ping します。このテストでは、直接接続されたルータがホストと ASA の間でパケットをルーティングできるかどうか、および ASA がパケットを正確にルーティングしてホストに戻せるかどうかを確認します。

中間ルータを通ってホストに戻るルートが ASA にない場合、ping は失敗する可能性があります（次の図を参照）。この場合は、デバッグ メッセージは ping が成功したことを示しますが、ルーティングの失敗を示す syslog メッセージ 110001 が表示されます。

図 *93 : ASA* の戻りルート未設定による *ping* の失敗

ステップ 4 ASA インターフェイスから既知のネットワーク デバイスへの ping は正しく機能しています。

- ping を受信しない場合は、送信ハードウェアまたはインターフェイスのコンフィギュレーションに問題がある可能性があります。
- ASA のインターフェイスが正しく設定されているにもかかわらず、「既知の正常な」デバイスからエコー応答を受信しない場合は、インターフェイス ハードウェアの受信機能に問題があると考えられます。「既知の正常な」受信機能を持つ別のインターフェイスで、同じ「既知の正常な」デバイスに対して ping を送信してエコーを受信できる場合、最初のインターフェイスのハードウェアの受信機能に問題があると確認されたことになります。

ステップ 5 ホストまたはルータから発信元インターフェイスを介して別のインターフェイス上の別のホストまたはルータに ping します。確認が必要なすべてのインターフェイス ペアに対して、このステップを繰り返します。NAT を使用する場合は、このテストを行うと NAT が正しく動作していることがわかります。

ping が成功すると、ルーテッド モードのアドレス変換（305009 または 305011）と ICMP 接続が確立されたこと（302020）を確認する syslog メッセージが表示されます。**show xlate** コマンドまたは **show conns** コマンドを入力してこの情報を表示することもできます。

NAT が正しく設定されていないことが原因で、ping に失敗することもあります。この場合、NAT が失敗したことを示す syslog メッセージが表示されます（305005 または 305006）。ping が外部ホストから内部ホストへ送信され、スタティック変換が存在しない場合は、メッセージ 106010 が表示されます。

図 *94 : ASA* のアドレス変換の問題による *ping* の失敗

ホストまでのルートの追跡

IP アドレスへのトラフィックの送信で問題が発生している場合は、ホストまでのルートを追跡することによってネットワーク パスに問題がないかどうかを確認できます。

手順

ステップ 1 トレース ルート上の ASA の表示 （1643 ページ）を使用して無効にすることができます。

ステップ 2 「パケット ルートの決定 （1645 ページ）」を参照してください。

トレース ルート上の ASA の表示

デフォルトで、ASA はトレース ルート上にホップとして表示されません。これを表示するには、ASA を通過するパケットの存続可能時間を減らして、ICMP 到達不能メッセージのレート制限を増やす必要があります。

手順

ステップ 1 L3/L4 クラスマップを作成して、接続の設定をカスタマイズするトラフィックを識別します。

class-map *name*

match *parameter*

例：

```
ciscoasa(config)# class-map CONNS
ciscoasa(config-cmap)# match any
```

照合文の詳細については、ファイアウォール設定ガイドのサービス ポリシーに関する章を参照してください。

ステップ 2 クラスマップ トラフィックで実行するアクションを設定するポリシーマップを追加または編集して、クラス マップを指定します。

policy-map *name* **class** *name*

例：

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class CONNS
```

デフォルト設定では、global_policyポリシーマップはすべてのインターフェイスにグローバルに割り当てられます。global_policy を編集する場合は、ポリシー名として global_policy を入力します。クラス マップの場合、この手順ですでに作成したクラスを指定します。

ステップ 3 クラスと一致するパケットの存続可能時間（TTL）を減らします。

set connection decrement-ttl

ステップ 4 既存のサービス ポリシー（global_policy という名前のデフォルト グローバル ポリシーなど）を編集している場合は、このステップを省略できます。それ以外の場合は、1 つまたは複数のインターフェイスでポリシー マップをアクティブにします。

service-policy *policymap_name* {**global** | **interface** *interface_name* }

例：

```
ciscoasa(config)# service-policy global_policy global
```

global キーワードはポリシー マップをすべてのインターフェイスに適用し、**interface** はポリシーを 1 つのインターフェイスに適用します。グローバル ポリシーは 1 つしか適用できません。インターフェイスでは、そのインターフェイスへサービス ポリシーを適用することで、グローバル ポリシーを上書きできます。各インターフェイスには、ポリシー マップを 1 つだけ適用できます。

ステップ 5 トレース ルートの出力に ASA が表示されるように、ICMP 到達不能メッセージのレート制限を増やします。

icmp unreachable rate-limit *rate* **burst-size** *size*

例：

```
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 1
```

レート制限は 1 ～ 100 の範囲で設定できます。デフォルトは 1 です。バースト サイズは動作には影響しませんが、1 ～ 10 の範囲で設定する必要があります。

例

次の例では、すべてのトラフィックの TTL をグローバルに減らして、ICMP 到達不能制限を 50 に増やします。

```
ciscoasa(config)# class-map global-policy
ciscoasa(config-cmap)# match any
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class global-policy
ciscoasa(config-pmap-c)# set connection decrement-ttl
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 6
```

パケット ルートの決定

traceroute を使用すれば、パケットが宛先に到着するまでのルートを特定できます。traceroute は、無効なポート上の宛先に UDP パケットまたは ICMPv6 エコーを送信することで機能します。ポートが有効でないため、宛先への途中にあるルータは ICMP または ICMPv6 Time Exceeded Message で応答し、そのエラーを ASA に報告します。

traceroute は送信された各プローブの結果を表示します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、出力記号の説明を示します。

出力記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
U	宛先へのルートが存在しません。
nn msec	各ノードに対する、指定した数のプローブのラウンドトリップ時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。ICMPv6 では、アドレスは対象外です。
!H	ICMP ホストに到達できません。
!P	ICMP に到達できません。ICMPv6 では、ポートが到達不能です。
!A	ICMP が管理的に禁止されています。
?	ICMP の原因不明のエラーが発生しました。

手順

宛先までのルートを追跡します。

traceroute [*destination_ip* | *hostname*} [**source** {*source_ip* | *source-interface*}] [**numeric**] [**timeout** *timeout_value*] [**probe** *probe_num*] [**ttl** *min_ttl max_ttl*] [**port** *port_value*] [**use-icmp**]

例：

```
ciscoasa# traceroute 209.165.200.225

Type escape sequence to abort.
Tracing the route to 209.165.200.225

1 10.83.194.1 0 msec 10 msec 0 msec
2 10.83.193.65 0 msec 0 msec 0 msec
3 10.88.193.101 0 msec 10 msec 0 msec
4 10.88.193.97 0 msec 0 msec 10 msec
5 10.88.239.9 0 msec 10 msec 0 msec
6 10.88.238.65 10 msec 10 msec 0 msec
7 172.16.7.221 70 msec 70 msec 80 msec
8 209.165.200.225 70 msec 70 msec 70 msec

ciscoasa# traceroute 2002::130

Type escape sequence to abort.
Tracing the route to 2002::130

 1  5000::2 0 msec 0 msec 0 msec
 2  2002::130 10 msec 0 msec 0 msec
```

通常は、宛先 IP アドレスまたはホスト名を含める（**traceroute www.example.com** など）だけです。ただし、必要に応じて、トレースの特性を調整できます。

- **source** {*source_ip*|*source-interface*}：トレースの送信元として使用するインターフェイスを指定します。インターフェイスは、名前または IP アドレスで指定できます。IPv6 では、送信元インターフェイスを指定できません。送信元 IP アドレスだけを指定できます。IPv6 アドレスは、ASA インターフェイスで IPv6 を有効にしている場合にのみ有効です。トランスペアレント モードでは、管理アドレスを使用する必要があります。
- **numeric**：IP アドレスのみをトレース ルートに表示するように指示します。このキーワードを指定しなかった場合は、DNS が設定されていれば、トレース ルートでアドレスの DNS 参照が実行され、DNS 名が追加されます。
- **timeout** *timeout_value*：タイムアウトするまで応答を待機する時間。デフォルトは 3 秒です。
- **probe** *probe_num*：各 TTL レベルで送信するプローブの数。デフォルトは 3 です。
- **ttl** *min_ttl* max_ttl：プローブの最小および最大存続可能時間。デフォルトの最小値は 1 ですが、この値を増やして、既知のホップの表示を抑制することができます。デフォルトの最大値は 30 です。トレースルートは、パケットが宛先に到達するか、または最大値に達すると終了します。

- **port** *port_value*：使用する UDP ポート。デフォルトは 33434 です。
- **use-icmp**：プローブの UDP パケットの代わりに ICMP パケットを送信します。

パケット トレーサを使用したポリシー設定のテスト

送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによってポリシー設定をテストできます。トレースは、ポリシー参照を実行してアクセスルールや NAT などをテストし、パケットを許可するか、拒否するかを確認します。

このようにパケットをテストすることによって、ポリシーの結果を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。設定の確認に加えて、トレーサを使用して許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。

手順

ステップ 1 このコマンドは複雑なため、複数の部分に分けて説明します。トレース用のインターフェイスとプロトコルを選択することから始めます。

packet-tracer input *ifc_name* [**vlan-id***vlan_id*] {**icmp** | **tcp** | **udp** | **rawip** | **sctp**} [**inline-tag** *tag*] ...

それぞれの説明は次のとおりです。

- **input** *ifc_name*：トレースを開始するインターフェイスの名前。ブリッジ グループの場合、ブリッジ グループ メンバー インターフェイスの名前を指定します。
- **vlan-id** *vlan_id*：（オプション）。パケット トレーサが（あとでサブインターフェイスにリダイレクトされる）親インターフェイスに入る仮想 LAN。VLAN ID は、入力インターフェイスがサブインターフェイスでない場合にのみ使用可能です。有効な値の範囲は 1 ～ 4096 です。
- **icmp**、**tcp**、**udp**、**rawip**、**sctp**：使用するプロトコル。「rawip」は未加工の IP、つまり、TCP/UDP 以外の IP パケットです。
- **inline-tag** *tag*：（オプション）。レイヤ 2 CMD ヘッダーに埋め込まれたセキュリティ グループ タグの値。有効な値の範囲は 0 ～ 65533 です。

ステップ 2 次に、送信元アドレスとプロトコル基準を入力します。

...{*src_ip* | **user** *username* | **security-group** {**name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*}...

それぞれの説明は次のとおりです。

- *src_ip*：パケット トレース用の送信元 IPv4 または IPv6 アドレス。

- **user** *username*：domain\user の形式のユーザー ID。ユーザーに対して最後にマッピングされたアドレス（複数ある場合）がトレースに使用されます。
- **security-group**{**name***name* | **tag***tag*}：TrustSec の IP-SGT 参照に基づく送信元セキュリティ グループ。セキュリティ グループの名前またはタグ番号を指定できます。
- **fqdn** *fqdn-string*：送信元ホストの完全修飾ドメイン名、IPv4 のみ。

ステップ 3 次に、プロトコルの特性を入力します。

- [ICMP]：ICMP タイプ（1 ～ 255）、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。各変数に対応する数字（エコーに対応する 8 など）を使用する必要があります。

  type code... [*ident*]*...*
- TCP/UDP/SCTP：送信元ポート番号を入力します。

  ...src_port ...
- [Raw IP]：プロトコル番号（0 ～ 255）を入力します。

  ...protocol ...

ステップ 4 最後に、宛先アドレス基準、TCP/UDP トレース用の宛先ポート、およびオプションのキーワードを入力して、**Enter** キーを押します。

...dmac {*dst_ip* | **security-group** { **name** *name* | **tag** *tag*} | **fqdn** *fqdn-string*} *dst_port* [**detailed**] [**xml**]

それぞれの説明は次のとおりです。

- *dst_ip*：パケット トレース用の宛先 IPv4 または IPv6 アドレス。
- **security-group** {**name** *name* **|** **tag** *tag*}：TrustSec の IP-SGT 参照に基づく宛先セキュリティ グループ。セキュリティ グループの名前またはタグ番号を指定できます。
- **fqdn** *fqdn-string*：宛先ホストの完全修飾ドメイン名、IPv4 のみ。
- *dst_port*：TCP/UDP/SCTP トレース用の宛先ポート。ICMP または未加工 IP トレースの場合はこの値を含めないでください。
- *dmac*：（トランスペアレント モード）宛先 MAC アドレス。
- **detailed**：標準出力に加えて詳細なトレース結果情報を提供します。
- **xml**：トレース結果を XML 形式で表示します。

ステップ 5 クラスタ ユニット全体でパケットをデバッグするには、パケット トレーサの **persist** オプションを入力します。

- **transmit** オプションを使用すると、シミュレートされたパケットが ASA から出られるようにすることができます。
- ACL、VPN フィルタ、IPsec スプーフィング、uRPF などのセキュリティ チェックをスキップするには、**bypass-checks** オプションを使用します。

- **decrypted** オプションを使用すると、復号化されたパケットを VPN トンネルに注入し、さらに、VPN トンネルを経由して到着するパケットをシミュレートすることもできます。

ステップ 6 特定のパケットをクラスタ ユニットで追跡するには、**id** と **origin** を入力します。

- **id**：トレースを開始するユニットによって割り当てられた識別番号。
- **origin**：トレースを開始するクラスタ ユニットを示します。

例

次に、HTTP ポート 10.100.10.10 から 10.100.11.11 への TCP パケットをトレースする例を示します。暗黙の拒否アクセス ルールによってパケットがドロップされることを示す結果が表示されます。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10 80
10.100.11.11 80

Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside

Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:

Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

接続のモニタリング

送信元、宛先、プロトコルなどに関する情報を含む現在の接続を表示するには、**show conn all detail** コマンドを使用します。

テストおよびトラブルシューティングの履歴

機能名	プラットフォーム リリース	説明
tracerouteの IPv6 サポート	9.7(1)	**traceroute** コマンドが変更され、IPv6 アドレれられるようになりました。 次のコマンドが変更されました。**traceroute**
ブリッジ グループ メンバー インターフェイス用のパケット トレーサのサポート	9.7(1)	ブリッジ グループ メンバー インターフェイト トレーサを使用できるようになりました。 **packet-tracer** コマンドに次の 2 つのオプションれました。**vlan-id** および **dmac**
手動によるパケット キャプチャの開始と停止	9.7(1)	キャプチャを手動で停止および開始できるようした。 追加/変更されたコマンド： **capture stop**
強化されたパケット トレーサおよびパケット キャプチャ機能	9.9(1)	パケット トレーサは次の機能で強化されま • パケットがクラスタ ユニット間を通過すケットを追跡します。 • シミュレートされたパケットが ASA かようにします。 • シミュレートされたパケットのセキュリクをバイパスします。 • シミュレートされたパケットを IPsec/SSされたパケットとして扱います。 パケット キャプチャは次の機能で強化され • パケットを復号化した後にキャプチャし • トレースをキャプチャし、永続リストにす。 新規または変更されたコマンド：**cluster exe trace include-decrypted**、**cluster exec capture persist**、**cluster exec clear packet-tracer**、**clus packet-tracer id**、**cluster exec show packet-tr packet-tracer persist**、**packet-tracer transmit packet-tracer decrypted**、**packet-tracer bypa**

機能名	プラットフォーム リリース	説明
ACL を使用せず IPv6 トラフィックを一致させるためのパケット キャプチャのサポート	9.10(1)	**capture** コマンドの **match** キーワードを使 **any** キーワードは IPv4 トラフィックのみ IPv4 または IPv6 トラフィックをキャプチ **any4** と **any6** キーワードを指定できるよう **any** キーワードでは、引き続き IPv4 トラ 合されます。 新規/変更されたコマンド：**capture matc**
Forepower 9300/4100 の新しい **debug telemetry** コマンド	9.14(1)	**debug telemetry** コマンドを使用すると、 連するデバッグメッセージが表示されま グは、テレメトリレポートの生成時にエ 定するために役立ちます。 新規/変更されたコマンド：**[no] debug t** **debug telemetry**
ping コマンドの変更	9.18(2)	ループバック インターフェイスの ping を ために、**ping** コマンドの動作が変更され ドでインターフェイスを指定する場合、 スは指定されたインターフェイスの IP ア ますが、実際の出力インターフェイスは ティングテーブルを使用したルートルッ て決定されます。 新規/変更されたコマンド： **ping**
スイッチのパケットキャプチャ	9.20(1)	スイッチの出力および入力トラフィック プチャするように設定できるようになり プションは、Secure Firewall 4200 モデル てのみ使用できます。 新しい/変更されたコマンド： **capture** *capture_name* **switch interface** *inte* **direction** { **both** | **egress** | **ingress** }]

第 VIII 部

モニタリング

- ロギング （1655 ページ）
- SNMP （1689 ページ）
- Cisco Success Network とテレメトリデータ （1733 ページ）
- Anonymous Reporting および Smart Call Home （1745 ページ）

第 46 章

ロギング

この章では、システム メッセージを記録して、トラブルシューティングに使用する方法について説明します。

- ロギングの概要 （1655 ページ）
- ロギングのガイドライン （1663 ページ）
- ロギングの設定 （1665 ページ）
- ログのモニタリング （1682 ページ）
- ロギングの例 （1683 ページ）
- ロギングの履歴 （1684 ページ）

ロギングの概要

システム ロギングは、デバイスから syslog デーモンを実行するサーバへのメッセージを収集する方法です。中央syslogサーバへロギングは、ログおよびアラートの集約に役立ちます。シスコ デバイスでは、これらのログ メッセージを UNIX スタイルの syslog サービスに送信できます。syslogサービスは、簡単なコンフィギュレーション ファイルに従って、メッセージを受信してファイルに保存するか、出力します。この形式のロギングは、保護された長期的な保存場所をログに提供します。ログは、ルーチンのトラブルシューティングおよびインシデント処理の両方で役立ちます。

ASA のシステムログにより、ASA のモニタリングおよびトラブルシューティングに必要な情報が得られます。ロギング機能を使用して、次の操作を実行できます。

- ログに記録する syslog メッセージを指定する。
- syslog メッセージの重大度を無効化または変更する。
- 次のような syslog メッセージ送信先を 1 つ以上指定する。
  - 内部バッファ
  - 1 台以上の syslog サーバ
  - ASDM
  - SNMP 管理ステーション

- 指定の電子メール アドレス
- コンソール
- Telnet および SSH セッション。

- 重大度レベルやメッセージ クラスなどによる、グループ内での syslog メッセージを設定および管理する。
- syslog の生成にレート制限を適用するかどうかを指定する。
- 内部ログ バッファがいっぱいになった場合に、その内容に対して実行する処理（バッファを上書きする、バッファの内容を FTP サーバに送信する、または内容を内部フラッシュ メモリに保存する）を指定する。
- 場所、重大度レベル、クラス、またはカスタム メッセージ リストにより、syslog メッセージをフィルタリングする。

マルチ コンテキスト モードでのロギング

それぞれのセキュリティ コンテキストには、独自のロギング コンフィギュレーションが含まれており、独自のメッセージが生成されます。システム コンテキストまたは管理コンテキストにログインし、別のコンテキストに変更した場合、セッションで表示されるメッセージは現在のコンテキストに関連するメッセージに限定されます。

システム実行スペースで生成されるフェールオーバー メッセージなどの syslog メッセージは、管理コンテキストで生成されるメッセージとともに管理コンテキストで表示できます。システム実行スペースでは、ロギングの設定やロギング情報の表示はできません。

ASA は、各メッセージとともにコンテキスト名を含めるように設定できます。これによって、単一の syslog サーバーに送信されるコンテキストメッセージを区別できます。この機能は、管理コンテキストから送信されたメッセージとシステムから送信されたメッセージの判別にも役立ちます。これが可能なのは、送信元がシステム実行スペースであるメッセージでは**システム**のデバイス ID が使用され、管理コンテキストが送信元であるメッセージではデバイス ID として管理コンテキストの名前が使用されるからです。

syslog メッセージ分析

次に、さまざまな syslog メッセージを確認することで取得できる情報タイプの例を示します。

- ASA セキュリティ ポリシーで許可された接続。これらのメッセージは、セキュリティ ポリシーで開いたままのホールを発見するのに役立ちます。
- ASA セキュリティ ポリシーで拒否された接続。これらのメッセージは、セキュアな内部ネットワークに転送されているアクティビティのタイプを示します。
- ACE 拒否率ロギング機能を使用すると、使用している ASA に対して発生している攻撃が表示されます。

- IDS アクティビティ メッセージには、発生した攻撃が示されます。
- ユーザー認証とコマンドの使用により、セキュリティ ポリシーの変更を監査証跡することができます。
- 帯域幅使用状況メッセージには、確立および切断された各接続のほか、使用された時間とトラフィック量が示されます。
- プロトコル使用状況メッセージには、各接続で使用されたプロトコルとポート番号が示されます。
- アドレス変換監査証跡メッセージは、確立または切断されている NAT または PAT 接続を記録します。この情報は、内部ネットワークから外部に送信される悪意のあるアクティビティのレポートを受信した場合に役立ちます。

syslog メッセージ形式

syslog メッセージは、次のように構造化されています。

`[<PRI>]: [Timestamp] [Device-ID] : %ASA-Level-Message_number: Message_text`

次の表に、フィールドの説明を示します。

<PRI>	プライオリティ値。ロギング EMBLEM が有効になっている場合は、この値が syslog メッセージに表示されます。ロギング EMBLEM は、TCP ではなく UDP と互換性があります。
Timestamp	イベントの日時が表示されます。タイムスタンプのロギングが有効になっており、そのタイムスタンプが RFC 5424 形式になるように設定されている場合は、syslog メッセージのすべてのタイムスタンプで、RFC 5424 標準規格に従って UTC の時刻が表示されます。
Device-ID	ユーザーインターフェイスを介して logging device-id オプションを有効にするときに設定されたデバイス識別子文字列。イネーブルにすると、EMBLEM 形式の syslog メッセージにデバイス ID は表示されません。
ASA	ASA が生成するメッセージの syslog メッセージ ファシリティ コード。この値は常に `ASA` です。
Level	0 ～ 7。レベルは、syslog メッセージに記述されている状況の重大度を示します。値が低いほどその状況の重大度は高くなります。
Message_number	syslog メッセージを特定する 6 桁の固有の番号。
Message_text	状況を説明するテキスト文字列。syslog メッセージのこの部分には、IP アドレス、ポート番号、またはユーザー名が含まれていることがあります。

デバイスによって生成されるすべての syslog メッセージは、『Cisco Secure Firewall ASA Series Syslog Messages』ガイドに記載されています。

EMBLEM syslog フォーマットは、RFC 3164 および RFC 5424 の標準に基づいて構築されたシスコ固有の規則です。したがって、EMBLEM が有効になっている場合、syslog メッセージは、<PRI> フィールドの後にコロン（:）を出力します。

ロギング EMBLEM、logging timestamp rfc5424、および device-id が有効になっている syslog メッセージの例。次のコロン（:）に注意してください<PRI>フィールド (<*166*>)。

```
<<166>:2018-06-27T12:17:46Z: %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

logging timestamp rfc5424 と device-id が有効になっている syslog メッセージの例。タイムスタンプの前にコロン（:）が表示されません。

```
2018-06-27T12:17:46Z ASA : %ASA-6-110002: Failed to locate egress interface for protocol
from src interface :src IP/src port to dest IP/dest port
```

重要度レベル

次の表に、syslog メッセージのシビラティ（重大度）の一覧を示します。それぞれのシビラティ（重大度）にカスタム カラーを割り当て、ASDM ログ ビューアでシビラティ（重大度）を識別しやすくできます。syslog メッセージの色設定を行うには、[ツール（Tools）] > [設定（Preferences）] > [Syslog] タブを選択するか、またはログ ビューア自体のツールバーで [色の設定（Color Settings）] をクリックします。

表 *61 : Syslog*メッセージのシビラティ（重大度）

レベル番号	重要度	説明
0	**致命的**	システムが使用不可能です。
1	**Alert（警告）**	すぐに措置する必要があります。
2	**深刻**	深刻な状況です。
3	**エラー**	エラー状態です。
4	**warning**	注意状態。
5	**Notification（通告）**	正常ですが、注意を必要とする状況です。
6	**情報**	情報メッセージです。
7	**デバッグ**	デバッグメッセージ。 問題をデバッグするときに、このレベルで一時的にのみログに記録します。このログレベルでは、非常に多くのメッセージが生成される可能性があるため、システムパフォーマンスに影響を与える可能性があります。

（注） ASA および は、重大度 0（緊急）の syslog メッセージを生成しません。

syslog メッセージ フィルタリング

生成される syslog メッセージは、特定の syslog メッセージだけが特定の出力先に送信されるようにフィルタリングできます。たとえば、ASA を設定して、すべての syslog メッセージを 1 つの出力先に送信し、それらの syslog メッセージのサブセットを別の出力先に送信することができます。

具体的には、syslog メッセージが次の基準に従って出力先に転送されるようにできます。

- syslog メッセージの ID 番号
- syslog メッセージの重大度
- syslog メッセージ クラス（機能エリアと同等）

これらの基準は、出力先を設定するときに指定可能なメッセージ リストを作成して、カスタマイズできます。あるいは、メッセージ リストとは無関係に、特定のメッセージ クラスを各タイプの出力先に送信するように ASA を設定することもできます。

syslog メッセージ クラス

syslog メッセージのクラスは次の 2 つの方法で使用できます。

- syslog メッセージのカテゴリ全体の出力場所を指定します。**logging class** コマンドを使用します。
- メッセージ クラスを指定するメッセージ リストを作成します。**logging list** コマンドを使用します。

syslog メッセージ クラスは、デバイスの特徴または機能と同等のタイプによって syslog メッセージを分類する方法を提供します。たとえば、RIP クラスは RIP ルーティングを示します。

特定のクラスに属する syslog メッセージの ID 番号はすべて、最初の 3 桁が同じです。たとえば、611 で始まるすべての syslog メッセージ ID は、vpnc（VPN クライアント）クラスに関連付けられています。VPN クライアント機能に関連付けられている syslog メッセージの範囲は、611101 ～ 611323 です。

また、ほとんどの ISAKMP syslog メッセージには先頭に付加されたオブジェクトの共通セットが含まれているため、トンネルを識別するのに役立ちます。これらのオブジェクトは、使用可能なときに、syslog メッセージの説明テキストの前に付加されます。syslog メッセージ生成時にオブジェクトが不明な場合、特定の heading = value の組み合わせは表示されません。

オブジェクトは次のように先頭に付加されます。

Group = *groupname*, Username = *user*, IP = *IP_address*

Group はトンネル グループ、Username はローカル データベースまたは AAA サーバから取得したユーザ名、IP アドレスはリモート アクセス クライアントまたはレイヤ 2 ピアのパブリック IP アドレスです。

次の表に、メッセージ クラスと各クラスのメッセージ ID の範囲をリストします。

表 *62 : syslog* メッセージのクラスおよび関連付けられているメッセージ *ID* 番号

クラス	定義	Syslog メッセージ ID 番号
auth	ユーザ認証	109、113
—	アクセス リスト	106
—	アプリケーション ファイアウォール	415
—	ボットネット トラフィック フィルタ	338
bridge	トランスペアレント ファイアウォール	110、220
ca	PKI 証明機関	717
citrix	Citrix クライアント	723
—	クラスタリング	747
—	カード管理	323
config	コマンド インターフェイス	111、112、208、308
csd	セキュアなデスクトップ	724
cts	Cisco TrustSec	776
dap	ダイナミック アクセス ポリシー	734
eap、eapoudp	ネットワーク アドミッション コントロール用の EAP または EAPoUDP	333、334
eigrp	EIGRP ルーティング	336
email	電子メール プロキシ	719
—	環境モニタリング	735
ha	フェールオーバー	101、102、103、104、105、210、311、709
—	Identity-Based ファイアウォール	746
ids	侵入検知システム	400、733
—	IKEv2 ツールキット	750、751、752

クラス	定義	Syslog メッセージ ID 番号
ip	IP スタック	209、215、313、317、408
ipaa	IP アドレスの割り当て	735
ips	侵入防御システム	400、401、420
—	IPv6	325
—	ライセンシング	444
mdm-proxy	MDM プロキシ	802
nac	ネットワーク アドミッション コントロール	731、732
nacpolicy	NAC ポリシー	731
nacsettings	NAC ポリシーを適用するための NAC 設定	732
—	NAT および PAT	305
—	ネットワーク アクセス ポイント	713
np	ネットワーク プロセッサ	319
—	NP SSL	725
ospf	OSPF ルーティング	318、409、503、613
—	パスワードの暗号化	742
—	Phone Proxy	337
rip	RIP ルーティング	107、312
rm	Resource Manager	321
—	Smart Call Home	120
session	ユーザ セッション	106、108、201、202、204、302、303、304、305、314、405、406、407、500、502、607、608、609、616、620、703、710
snmp	SNMP	212
—	ScanSafe	775
ssl	SSL スタック	725

クラス	定義	Syslog メッセージ ID 番号
svc	SSL VPN クライアント	722
sys	システム	199、211、214、216、306、307、315、414、604、605、606、610、612、614、615、701、711、741
—	脅威の検出	733
tag-switching	サービス タグ スイッチング	779
transactional-rule-engine-tre	トランザクション ルール エンジン	780
uc-ims	UC-IMS	339
vm	VLAN マッピング	730
vpdn	PPTP および L2TP セッション	213、403、603
vpn	IKE および IPsec	316、320、402、404、501、602、702、713、714、715
vpnc	VPN クライアント	611
vpnfo	VPN フェールオーバー	720
vpnlb	VPN ロード バランシング	718
—	VXLAN	778
webfo	WebVPN フェールオーバー	721
webvpn	WebVPN と セキュアクライアント	716

カスタム メッセージ リスト

カスタム メッセージ リストを作成して、送信する syslog メッセージとその出力先を柔軟に制御できます。カスタム syslog メッセージのリストで、次の条件のいずれかまたはすべてを使用して syslog メッセージのグループを指定します。

- 重大度
- メッセージ ID
- syslog メッセージ ID の範囲
- メッセージ クラス

たとえば、メッセージ リストを使用して次の操作を実行できます。

- 重大度が 1 および 2 の syslog メッセージを選択し、1 つ以上の電子メール アドレスに送信する。
- メッセージ クラス（「ha」など）に関連付けられたすべての syslog メッセージを選択し、内部バッファに保存する。

メッセージ リストには、メッセージを選択するための複数の基準を含めることができます。ただし、メッセージ選択基準の追加は、それぞれ個別のコマンドエントリで行う必要があります。重複したメッセージ選択基準を含むメッセージ リストが作成される可能性もあります。メッセージリストの 2 つの基準によって同じメッセージが選択される場合、そのメッセージは一度だけログに記録されます。

クラスタ

syslog メッセージは、クラスタリング環境でのアカウンティング、モニタリング、およびトラブルシューティングのための非常に重要なツールです。クラスタ内の各 ASA ユニット（最大 8 ユニットを使用できます）は、syslog メッセージを個別に生成します。特定の **logging** コマンドを使用すると、タイム スタンプおよびデバイス ID を含むヘッダー フィールドを制御できます。syslog サーバーは、syslog ジェネレータを識別するためにデバイス ID を使用します。**logging device-id** コマンドを使用すると、同一または異なるデバイス ID 付きで syslog メッセージを生成することができ、クラスタ内の同一または異なるユニットからのメッセージのように見せることができます。

ロギングのガイドライン

この項では、ロギングを設定する前に確認する必要のある制限事項とガイドラインについて説明します。

IPv6 のガイドライン

- IPv6 がサポートされます。Syslog は、TCP または UDP を使用して送信できます。
- syslog 送信用に設定されたインターフェイスが有効であること、IPv6 対応であること、および syslog サーバが指定インターフェイス経由で到達できることを確認します。
- IPv6 上でのセキュア ロギングはサポートされません。

その他のガイドライン

- syslog サーバでは、syslogd というサーバ プログラムを実行する必要があります。Windows では、オペレーティング システムの一部として syslog サーバを提供しています。
- syslog サーバーは、ファイアウォールシステムの syslog-ng プロセスに基づいて動作します。SecureWorks の *scwx.conf* ファイルなどの外部設定ファイルは使用しないでください。このようなファイルは、デバイスと互換性がありません。これらを使用すると、解析エラーが発生し、最終的に syslog-ng プロセスが失敗します。

- ASAが生成したログを表示するには、ロギングの出力先を指定する必要があります。ロギングの出力先を指定せずにロギングをイネーブルにすると、ASAはメッセージを生成しますが、それらのメッセージは後で表示できる場所に保存されません。各ロギングの出力先は個別に指定する必要があります。たとえば、出力先として複数のsyslogサーバを指定するには、新しいコマンドを入力し、で、個別のエントリを指定します。
- スタンドバイ デバイスでは、TCP 上での syslog の送信はサポートされません。
- トランスポートプロトコルとして TCP を使用する場合、メッセージが失われないように syslog サーバーへの接続が 4 つ開きます。syslog サーバーを使用して非常に多数のデバイスからメッセージを収集する場合、接続オーバーヘッドの合計がサーバーに対して大きすぎる場合は、代わりに UDP を使用します。
- 2 つの異なるリストまたはクラスを、異なる syslog サーバーまたは同じロケーションに割り当てることはできません。
- 最大 16 台の syslog サーバを設定できます。ただし、マルチ コンテキスト モードでは、コンテキストごとに 4 サーバに制限されています。
- syslog サーバは、ASA 経由で到達できなければなりません。syslog サーバが到達できるインターフェイス上で、デバイスがICMP到達不能メッセージを拒否し、同じサーバにsyslogを送信するように設定する必要があります。すべてのシビラティ（重大度）に対してロギングがイネーブルであることを確認します。syslog サーバーがクラッシュしないようにするため、syslog 313001、 313004、および 313005 の生成を抑制します。
- syslogのUDP接続の数は、ハードウェア プラットフォームのCPUの数と、設定するsyslogサーバの数に直接関連しています。可能な UDP syslog 接続の数は常に、CPU の数と設定するsyslogサーバの数を乗算した値と同じになります。これは予期されている動作です。グローバル UDP 接続アイドル タイムアウトはこれらのセッションに適用され、デフォルトは2分であることに注意してください。これらのセッションをこれよりも短い時間で閉じる場合にはこの設定を調整できますが、タイムアウトはsyslogだけでなくすべてのUDP接続に適用されます。
- アクセス リストのヒット数だけを照合するためにカスタム メッセージ リストを使用すると、ロギングシビラティ（重大度）がデバッグ（レベル 7）のアクセス リストに対しては、アクセスリストのログは生成されません。**logging list** コマンドのロギングシビラティ（重大度）のデフォルトは、6 に設定されています。このデフォルト動作は設計によるものです。アクセス リスト コンフィギュレーションのロギングシビラティ（重大度）をデバッグに明示的に変更する場合は、ロギング コンフィギュレーション自体も変更する必要があります。

  ロギングシビラティ（重大度）がデバッグに変更されたため、アクセスリストのヒットが含まれていない **show running-config logging** コマンドの出力例を次に示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging list test message 106100
logging buffered test
```

次に、アクセス リスト ヒットを含む **show running-config logging** コマンドの出力例を示します。

```
ciscoasa# show running-config logging
logging enable
logging timestamp
logging buffered debugging
```

この場合、アクセス リスト コンフィギュレーションは変更せず、アクセス リスト ヒット数が次の例のように表示されます。

```
ciscoasa(config)# access-list global line 1 extended
permit icmp any host 4.2.2.2 log debugging interval 1 (hitcnt=7) 0xf36b5386
ciscoasa(config)# access-list global line 2 extended
permit tcp host 10.1.1.2 any eq www log informational interval 1 (hitcnt=18) 0xe7e7c3b8
ciscoasa(config)# access-list global line 3 extended
permit ip any any (hitcnt=543) 0x25f9e609
```

- ASA が TCP 経由で syslog を送信すると、syslogd サービスの再起動後、接続の開始に約 1 分かかります。
- TCP ロギングホストがダウンすると、接続ステータスが *[*接続済み（*Connected*）*]* から *[*接続されていない（*Not connected*）*]* に変わるまで約 6 分かかります。ロギングは TCP を使用してチャネルステートを検出します。それまでは、ロギングはチャネルを介してログを送信します。この間に、 **show log**を実行すると、出力に TCP ロギングホストが接続済みであると表示されます。TCP チャネルが閉じられると、TCP ロギング ホストの状態は *[*接続されていません（*Not connected*）*]* に更新されます。
- syslog サーバーから受信したサーバー証明書は、[Extended Key Usage] フィールドに「ServAuth」を含める必要があります。このチェックは、自己署名証明書以外の証明書にのみ実行されます。自己署名証明書の場合、このフィールドに値は表示されません。

ロギングの設定

ここでは、ロギングの設定方法について説明します。

ロギングの有効化

ロギングをイネーブルにするには、次の手順を実行します。

手順

ロギングをイネーブルにします。

logging enable

例：

```
ciscoasa(config)# logging enable
```

出力先の設定

トラブルシューティングおよびパフォーマンスのモニタリング用にsyslogメッセージの使用状況を最適化するには、syslog メッセージの送信先（内部ログ バッファ、1 つまたは複数の外部 syslog サーバー、ASDM、SNMP 管理ステーション、コンソール ポート、指定した電子メール アドレス、または Telnet および SSH セッションなど）を 1 つまたは複数指定することをお勧めします。

管理専用アクセスが有効になっているインターフェイスで syslog ロギングを設定した場合、データプレーン関連のログ（syslog ID 302015、302014、106023、および 304001）はドロップされて syslog サーバーに到達しません。これらの syslog メッセージがドロップされるのは、データパス ルーティング テーブルに管理インターフェイスのルーティングがないためです。したがって、設定するインターフェイスで管理専用アクセスが無効になっていることを確認してください。

外部 syslog サーバーへの syslog メッセージの送信

外部syslogサーバーで利用可能なディスク領域に応じてメッセージをアーカイブし、その保存後、ロギング データを操作できます。たとえば、特定タイプの syslog メッセージがログに記録されたときに特別なアクションが実行されるように指定したり、ログからデータを抽出してレポート用の別のファイルにその記録を保存したり、サイト固有のスクリプトを使用して統計情報を追跡したりできます。

外部 syslog サーバーに syslog メッセージを送信するには、次の手順を実行します。

手順

ステップ 1 syslog サーバーにメッセージを送信するために ASA を設定します。

IPv4 または IPv6 syslog サーバーにメッセージを送信するよう ASA を設定できます。

logging host *interface_name syslog_ip* [**tcp**[/*port*] | **udp** [/*port*] [**format emblem**]]

例：

```
ciscoasa(config)# logging host dmz1 192.168.1.5 udp/1026
ciscoasa(config)# logging host dmz1 2002::1:1 udp/2020
```

format emblem キーワードは、UDP 限定で syslog サーバーでの EMBLEM 形式ロギングを有効にします。*interface_name* 引数には、syslog サーバーにアクセスするときのインターフェイスを指定します。*syslog_ip* 引数には、syslog サーバーの IP アドレスを指定します。**tcp**[/*port*] ま

たは **udp**[*/port*] キーワードと引数のペアは、syslog サーバーに syslog メッセージを送信するために ASA で TCP を使用するか、UDP を使用するかを指定します。

UDP または TCP のいずれかを使用して syslog サーバーにデータを送信するように ASA を設定することはできますが、両方を使用するように設定することはできません。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

警告
TCP を指定すると、ASA は syslog サーバーの障害を検出したときに、セキュリティ上の理由で ASA を経由する新しい接続をブロックします。TCP syslog サーバーへの接続に関係なく新しい接続を許可するには、手順 3 を参照してください。

UDP を指定すると、ASA は、syslog サーバーが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

ステップ 2 syslog サーバに送信する syslog メッセージを指定します。

logging trap {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging trap errors
```

重大度として、値（1 ～ 7）または名前を指定できます。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。syslog サーバーに送信する syslog メッセージを特定したカスタム メッセージ リストを指定することもできます。

ステップ 3 （オプション）TCP 接続された syslog サーバーがダウンした場合、新しい接続をブロックする機能をディセーブルにします。

logging permit-hostdown

例：

```
ciscoasa(config)# logging permit-hostdown
```

ASA が syslog メッセージを TCP ベースの syslog サーバーに送信するように設定されている場合、および syslog サーバーがダウンしているか、ログキューがいっぱいの場合、ASA への新しい接続はブロックされます。新しい接続は、syslog サーバーがバック アップされ、ログ キューがいっぱいでなくなった後に再度許可されます。このコマンドを使用すると、syslog サーバーが動作していない場合でも新しい接続を許可できます。

ステップ 4 （オプション）ロギング ファシリティを 20 以外の値に設定します。これは、ほとんどの UNIX システムで想定されています。

logging facility *number*

例：

```
ciscoasa(config)# logging facility 21
```

セキュア ロギングの有効化

手順

logging host コマンドで **secure** キーワードを指定して、セキュア ロギングを有効にします。また、必要に応じて **reference-identity** を入力します。

logging host *interface_name syslog_ip* [**tcp**/*port* | **udp**/*port*] [**format emblem**] [**secure**[**reference-identity** *reference_identity_name*]]

それぞれの説明は次のとおりです。

- **logging host***interface_name syslog_ip* には、syslog サーバーが常駐するインターフェイスと syslog サーバーの IP アドレスを指定します。
- [**tcp**/*port* | **udp**/*port*] には、syslog サーバーが syslog メッセージをリスンするポート（TCP または UDP）を指定します。**tcp** キーワードは、ASA が TCP を使用して syslog メッセージを syslog サーバーに送信することを指定します。**udp** キーワードは、ASA が UDP を使用して syslog メッセージを syslog サーバーに送信することを指定します。
- **format emblem** キーワードは、syslog サーバーに対して EMBLEM 形式のロギングを有効にします。
- **secure** キーワードは、リモート ロギング ホストへの接続で、TCP の場合にだけ SSL/TLS を使用するように指定します。セキュア ロギングでは UDP をサポートしていないため、このプロトコルを使用しようとするとエラーが発生します。
- [**reference-identity** *reference_identity_name*] は、以前に設定された参照アイデンティティ オブジェクトに基づく証明書での RFC 6125 参照アイデンティティ検査を有効にします。参照 ID オブジェクトについて詳しくは、参照 ID の設定 （1091 ページ）を参照してください。

例：

```
ciscoasa(config)# logging host inside 10.0.0.1 TCP/1500 secure  reference-identity
syslogServer
```

syslog サーバーに送信する EMBLEM 形式の syslog メッセージの生成

syslog サーバーへの EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

EMBLEM 形式の syslog メッセージを、UDP のポート 514 を使用して syslog サーバーに送信します。

logging host *interface_name ip_address*{**tcp** [/*port*] | **udp** [/ *port*]] [**format emblem**]

例：

```
ciscoasa(config)# logging host interface_1 127.0.0.1 udp format emblem
ciscoasa(config)# logging host interface_1 2001::1 udp format emblem
```

IPv4 または IPv6 の Syslog サーバを設定できます。

format emblem キーワードは、syslog サーバーでの EMBLEM 形式ロギングを有効にします（UDP 限定）。*interface_name* 引数には、syslog サーバーにアクセスするときのインターフェイスを指定します。*ip_address* 引数には、syslog サーバーの IP アドレスを指定します。 **tcp**[/*port*] または **udp**[/*port*] キーワードと引数のペアは、syslog サーバーに syslog メッセージを送信するために ASA で TCP を使用するか、UDP を使用するかを指定します。

UDP または TCP のいずれかを使用して syslog サーバーにデータを送信するように ASA を設定することができます。プロトコルを指定しない場合、デフォルトのプロトコルは UDP です。

複数の **logging host** コマンドを使用して、syslog メッセージを受信するすべての追加サーバーを指定できます。2 つ以上のロギング サーバーを設定する場合は、必ず、すべてのロギング サーバーにおいて、ロギングの重大度の上限を warnings にしてください。

警告
TCP を指定すると、ASA は syslog サーバーの障害を検出したときに、セキュリティ上の理由で ASA を経由する新しい接続をブロックします。syslog サーバーに障害が発生しても新しい接続を許可するには、外部 syslog サーバーへの syslog メッセージの送信 （1666 ページ）のステップ 3 を参照してください。

UDP を指定すると、ASA は、syslog サーバーが動作しているかどうかに関係なく新しい接続を許可し続けます。有効なポート値は、どちらのプロトコルでも 1025 ～ 65535 です。デフォルトの UDP ポートは 514 です。デフォルトの TCP ポートは 1470 です。

（注）
TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

他の出力先への EMBLEM 形式の syslog メッセージの生成

他の出力先への EMBLEM 形式の syslog メッセージを生成するには、次の手順を実行します。

手順

syslog サーバー以外の出力先（たとえば Telnet または SSH セッション）に EMBLEM 形式の syslog メッセージを送信します。

logging emblem

例：

```
ciscoasa(config)# logging emblem
```

内部ログ バッファへの syslog メッセージの送信

一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定する必要があります。新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。

syslog メッセージを内部ログ バッファに送信するには、次の手順を実行します。

手順

ステップ 1 一時的な保存場所となる内部ログ バッファに送信する syslog メッセージを指定します。

logging buffered {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging buffered critical
ciscoasa(config)# logging buffered level 2
ciscoasa(config)# logging buffered notif-list
```

新しいメッセージは、リストの最後に追加されます。バッファがいっぱいになったとき、つまりバッファラップが発生した場合、ASA がいっぱいになったバッファを別の場所に保存するように設定されていない限り、古いメッセージは生成される新しいメッセージによって上書きされます。内部ログ バッファを空にするには、**clear logging buffer** コマンドを入力します。

ステップ 2 内部ログ バッファのサイズを変更します。デフォルトのバッファ サイズは 4 KB です。

logging buffer-size *bytes*

例：

```
ciscoasa(config)# logging buffer-size 16384
```

ステップ 3 次のいずれかのオプションを選択します。

- 新しいメッセージを内部ログ バッファに保存し、いっぱいになったログ バッファの内容を内部フラッシュ メモリに保存します。

  logging flash-bufferwrap

  例：

  ```
  ciscoasa(config)# logging flash-bufferwrap
  ```

  （注）
  バッファ サイズが 2 MB を超えている場合、このコマンドは警告なしでフラッシュへのデータの書き込みを停止します。

- 新しいメッセージを内部ログ バッファに保存し、いっぱいになったログ バッファの内容を FTP サーバーに保存します。

  logging ftp-bufferwrap

  例：

  ```
  ciscoasa(config)# logging ftp-bufferwrap
  ```

  バッファの内容を別の場所に保存するとき、ASAは、次のタイムスタンプ形式を使用する名前でログ ファイルを作成します。

  ```
  LOG-YYYY-MM-DD-HHMMSS.TXT
  ```

  *YYYY*は年、*MM*は月、*DD*は日付、*HHMMSS*は時間、分、および秒で示された時刻です。

- ログ バッファの内容を保存する FTP サーバーを指定します。

  logging ftp-server *server pathusername password*

  例：

  ```
  ciscoasa(config)# logging ftp-server 10.1.1.1 /syslogs logsupervisor 1luvMy10gs
  ```

  *server*引数には、外部FTPサーバーのIPアドレスを指定します。*path*引数には、ログ バッファのデータを保存するFTPサーバーへのディレクトリ パスを指定します。このパスは、FTP ルート ディレクトリに対する相対パスです。*username* 引数には、FTP サーバーへのロギングで有効なユーザー名を指定します。*password*引数は、指定したユーザー名に対するパスワードを示します。

- 現在のログ バッファの内容を内部フラッシュ メモリに保存します。

  logging savelog [*savefile*]

  例：

```
ciscoasa(config)# logging savelog latest-logfile.txt
```

ログの記録で使用可能な内部フラッシュ メモリの容量の変更

ログの記録で使用可能な内部フラッシュ メモリの容量を変更するには、次の手順を実行します。

手順

ステップ 1 ログ ファイルの保存で使用可能な内部フラッシュ メモリの最大容量を指定します。

logging flash-maximum-allocation *kbytes*

例：

```
ciscoasa(config)# logging flash-maximum-allocation 1200
```

デフォルトで ASA は、内部フラッシュ メモリの最大 50 MB をログ データに使用できます。ASA でログデータを保存するために必要な内部フラッシュメモリの最小空き容量は 3 MB です。flash-maximum-allocation 値の上限は 2 GB です。

内部フラッシュメモリに保存されているログファイルにより、内部フラッシュメモリの空き容量が設定された最小限の容量を下回ってしまう場合、ASA は最も古いログファイルを削除し、新しいログファイルの保存後も最小限の容量が確保されるようにします。削除するファイルがない場合、または古いファイルをすべて削除しても空きメモリの容量が最小限の容量を下回っている場合、ASA はその新しいログファイルを保存できません。

ステップ 2 ASA でログファイルを保存するために必要な内部フラッシュメモリの最小空き容量を指定します。

logging flash-minimum-free *kbytes*

例：

```
ciscoasa(config)# logging flash-minimum-free 4000
```

電子メール アドレスへの syslog メッセージの送信

syslog メッセージを電子メール アドレスに送信するには、次の手順を実行します。

手順

ステップ 1 電子メール アドレスに送信する syslog メッセージを指定します。

logging mail {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging mail high-priority
```

電子メールで送信される場合、syslogメッセージは電子メールメッセージの件名行に表示されます。このため、このオプションでは、critical、alert、および emergency など、重大度の高い syslog メッセージを管理者に通知するように設定することをお勧めします。

ステップ 2 電子メール アドレスに syslog メッセージを送信するときに使用する送信元電子メール アドレスを指定します。

logging from-address *email_address*

例：

```
ciscoasa(config)# logging from-address xxx-001@example.com
```

ステップ 3 電子メール アドレスに syslog メッセージを送信するときに使用する宛先の電子メール アドレスを指定します。

logging recipient-address *e-mail_address*[*severity_level*]

例：

```
ciscoasa(config)# logging recipient-address admin@example.com
```

ステップ 4 電子メール アドレスに syslog メッセージを送信するときに使用する SMTP サーバーを指定します。プライマリおよびセカンダリサーバーのアドレスを提供して、失敗したログメッセージングサービスを確保することができます。必要に応じて、インターフェイスをサーバーに関連付けて、ロギングに使用するルーティングテーブルを識別することもできます。インターフェイスが指定されていない場合、ASA は管理ルーティング テーブルを参照し、ルート エントリが存在しない場合は、データ ルーティング テーブルを参照します。

smtp-server [*primary-interface*] *primary-smpt-server-ip-address* [[*backup-interface*]*backup-smpt-server-ip-address*]

例：

```
ciscoasa(config)# smtp-server 10.1.1.24 10.1.1.34
ciscoasa(config)# smtp-server 10.1.1.24
ciscoasa(config)# smtp-server management 10.1.1.24 outside 10.1.1.34
```

```
ciscoasa(config)# smtp-server management 10.1.1.24
```

ASDM への syslog メッセージの送信

syslog メッセージを ASDM に送信するには、次の手順を実行します。

手順

ステップ 1 ASDM に送信する syslog メッセージを指定します。

logging asdm {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging asdm 2
```

ASA は、ASDM への送信を待機している syslog メッセージのバッファ領域を確保し、メッセージが生成されるとバッファに保存します。ASDM ログ バッファは、内部ログ バッファとは別のバッファです。ASDM のログバッファがいっぱいになると、ASA は最も古い syslog メッセージを削除し、新しい syslog メッセージのバッファ領域を確保します。最も古い syslog メッセージを削除して新しい syslog メッセージのためのスペースを確保するのは、ASDM のデフォルト設定です。ASDM ログ バッファに保持される syslog メッセージの数を制御するために、バッファのサイズを変更できます。

ステップ 2 ASDM ログ バッファに保持される syslog メッセージの数を指定します。

logging asdm-buffer-size *num_of_msgs*

例：

```
ciscoasa(config)# logging asdm-buffer-size 200
```

ASDM ログ バッファの現在の内容を空にするには、**clear logging asdm** コマンドを入力します。

ロギング キューの設定

ロギング キューを設定するには、次の手順を実行します。

手順

設定された出力先に送信されるまでの間、ASA がそのキューに保持できる syslog メッセージの数を指定します。

logging queue *message_count*

例：

```
ciscoasa(config)# logging queue 300
```

ASA のメモリ内には、設定された出力先への送信を待機している syslog メッセージをバッファするために割り当てられる、一定数のブロックがあります。必要なブロックの数は、syslog メッセージ キューの長さと、指定した syslog サーバーの数によって異なります。デフォルトのキューのサイズは 512 syslog メッセージです。キューのサイズは、使用可能なブロック メモリのサイズが上限です。有効値は 0 ～ 8192 メッセージです。値はプラットフォームによって異なります。ロギング キューをゼロに設定した場合、そのキューは設定可能な最大サイズ（8192 メッセージ）になります。

コンソール ポートへの syslog メッセージの送信

syslog メッセージをコンソール ポートに送信するには、次の手順を実行します。

手順

コンソール ポートに送信する syslog メッセージを指定します。

logging console { *severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging console errors
```

SNMP サーバーへの syslog メッセージの送信

SNMP サーバーへのロギングをイネーブルにするには、次の手順を実行します。

手順

SNMP ロギングをイネーブルにし、SNMP サーバーに送信するメッセージを指定します。

logging history [**rate-limit** *number interval* | **level** *level* | *logging_list* | *level*]

logging rate-limit コマンドを使用してグローバル レート制限を設定した場合、そのコマンドは、このコマンドの **rate-limit** キーワードよりも優先されます。

例：

```
ciscoasa(config)# logging history errors

ciscoasa(config)# logging history rate-limit 15 15 level critical
```

Telnet または SSH セッションへの syslog メッセージの送信

syslog メッセージを Telnet または SSH セッションに送信するには、次の手順を実行します。

手順

ステップ 1 Telnet または SSH セッションに送信する syslog メッセージを指定します。

logging monitor {*severity_level* | *message_list*}

例：

```
ciscoasa(config)# logging monitor 6
```

ステップ 2 現在のセッションへのロギングだけをイネーブルにします。

terminal monitor

例：

```
ciscoasa(config)# terminal monitor
```

一度ログアウトして再びログインする場合は、このコマンドを再入力する必要があります。現在のセッションへのロギングを無効にするには、**terminal no monitor** コマンドを入力します。

syslog メッセージの設定

Syslog での無効なユーザー名の表示または非表示

ログイン試行に失敗した場合の無効なユーザー名をsyslogメッセージに表示または非表示にできます。デフォルト設定では、ユーザー名が無効な場合、または有効かどうか不明な場合、ユーザー名は非表示です。たとえば、ユーザーが誤ってユーザー名の代わりにパスワードを入力した場合、結果として生成されるsyslogメッセージで「ユーザー名」を隠すのが安全です。ログインに関するトラブルシューティングに役立てるために、無効なユーザー名を表示することもできます。

手順

ステップ 1 無効なユーザー名を表示するには、次のようにします。

no logging hide username

ステップ 2 無効なユーザー名を非表示にするには、次のようにします。

logging hide username

syslog メッセージに日付と時刻を含める

syslog メッセージに日付と時刻を含めるには、次の手順を実行します。

手順

syslog メッセージにメッセージが生成された日付と時刻が含まれるように指定します。

logging timestamp

例：

```
ciscoasa(config)# logging timestamp
LOG-2008-10-24-081856.TXT
```

syslog メッセージから日付と時刻を削除するには、**no logging timestamp** コマンドを入力します。

syslog メッセージの無効化

指定した syslog メッセージをディセーブルにするには、次の手順を実行します。

手順

ASA が特定の syslog メッセージを生成しないように指定します。

no logging message *syslog_id*

例：

```
ciscoasa(config)# no logging message 113019
```

無効にした syslog メッセージを再び有効にするには、**logging message** *syslog_id* コマンドを入力します（例：**logging message 113019**）。無効にしたすべての syslog メッセージのロギングを再び有効にするには、**clear configure logging disabled** コマンドを入力します。

syslog メッセージの重大度の変更

syslog メッセージの重大度を変更するには、次の手順を実行します。

手順

syslog メッセージの重大度を指定します。

logging message *syslog_id* **level** *severity_level*

例：

```
ciscoasa(config)# logging message 113019 level 5
```

syslog メッセージの重大度をその設定にリセットするには、**no logging message** *syslog_id* **level** *severity_level* コマンド（**no logging message 113019 level 5** など）を入力します。変更されたすべての syslog メッセージの重大度をそれぞれの設定にリセットするには、**clear configure logging level** コマンドを入力します。

スタンバイ装置の syslog メッセージのブロック

手順

スタンバイユニットで特定の syslog メッセージが生成されないようにブロックするには、次のコマンドを使用します。

no logging message *syslog-id* **standby**

例：

```
ciscoasa(config)# no logging message 403503 standby
```

フェールオーバー発生時にフェールオーバースタンバイ ASA の syslog メッセージの同期が継続されるようにするには、特定の syslog メッセージのブロックを解除します。スタンバイユニットでの生成を以前にブロックした特定の syslog メッセージのブロックを解除するには、**logging standby** コマンドを使用します。

（注）

安定状態のときは、アクティブとスタンバイの両方の ASA でロギングを行うと、syslog サーバー、SNMP サーバー、FTP サーバーなどの共有ロギング先でのトラフィックは 2 倍になります。ただし、フェールオーバー発生時のスイッチオーバーフェーズでは、スイッチオーバーによるアクティブユニットの侵入イベントや接続イベントなど、スタンバイ ASA でより多くのイベントが生成されます。

非 EMBLEM 形式の syslog メッセージにデバイス ID を含める

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるには、次の手順を実行します。

手順

デバイス ID を非 EMBLEM 形式の syslog メッセージに含めるように ASA を設定します。syslog メッセージに対して指定できるデバイス ID のタイプは 1 つだけです。

logging device-id {**cluster-id** | **context-name** | **hostname** | **ipaddress** *interface_name* [**system**] | **string** *text*}

例：

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# logging device-id context-name
```

context-name キーワードは、現在のコンテキストの名前をデバイス ID として使用することを示します（マルチ コンテキスト モードにだけ適用されます）。マルチ コンテキスト モードの管理コンテキストでデバイス ID のロギングをイネーブルにすると、そのシステム実行スペースで生成されるメッセージは**system**のデバイス ID を使用し、管理コンテキストで生成されるメッセージは管理コンテキストの名前をデバイス ID として使用します。

（注）
ASA クラスタでは、選択したインターフェイスの制御ユニットの IP アドレスを常に使用します。

cluster-id キーワードは、デバイス ID として、クラスタの個別の ASA ユニットのブート設定に一意の名前を指定します。**hostname** キーワードは、ASA のホスト名をデバイス ID として使用するように指定します。**ipaddress** *interface_name* キーワード引数のペアは、*interface_name* として指定されたインターフェイスの IP アドレスをデバイス ID として使用することを指定します。**ipaddress** キーワードを使用すると、syslog メッセージの送信元となるインターフェイスに関係なく、そのデバイス ID は指定された ASA のインターフェイス IP アドレスとなります。クラスタ環境では、**system** キーワードは、デバイス ID がインターフェイスのシステム IP アドレスとなることを指定します。このキーワードにより、デバイスから送信されるすべての syslog メッセージに単一の一貫したデバイス ID を指定できます。**string** *text* キーワード引数のペアは、テキスト文字列をデバイス ID として使用することを指定します。文字列の長さは、最大で 16 文字です。

空白スペースを入れたり、次の文字を使用したりすることはできません。

- &（アンパサンド）
- '（一重引用符）
- "（二重引用符）
- <（小なり記号）
- >（大なり記号）
- ?（疑問符）

（注）
イネーブルにすると、EMBLEM 形式の syslog メッセージや SNMP トラップにデバイス ID は表示されません。

カスタム イベント リストの作成

イベント リストの定義には、次の 3 つの基準を使用します。

- イベント クラス
- 重大度
- メッセージ ID

特定のロギングの宛先（SNMP サーバーなど）に送信するカスタム イベント リストを作成するには、次の手順を実行します。

手順

ステップ 1 内部ログ バッファに保存されるメッセージの選択基準を指定します。たとえば重大度を 3 に設定すると、ASA は、重大度が 3、2、および 1 の syslog メッセージを送信します。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

例：

```
ciscoasa(config)# logging list list-notif level 3
```

name 引数には、リストの名前を指定します。**level** *level* キーワードと引数のペアは、重大度を指定します。**class** *message_class* キーワードと引数のペアは、特定のメッセージ クラスを指定します。**message** *start_id* [*-end_id*] キーワードと引数のペアは、個々の syslog メッセージ番号または番号の範囲を指定します。

（注）

重大度の名前を syslog メッセージ リストの名前として使用しないでください。使用禁止の名前には、emergencies、alert、critical、error、warning、notification、informational、および debugging が含まれます。同様に、イベントリスト名の先頭にこれらの単語の最初の 3 文字は使用しないでください。たとえば、「err」で始まるイベント リスト名は使用しないでください。

ステップ 2 （オプション）リストにメッセージの選択基準をさらに追加します。

logging list *name* {**level** *level* [**class** *message_class*] | **message** *start_id*[*-end_id*]}

例：

```
ciscoasa(config)# logging list list-notif message 104024-105999
ciscoasa(config)# logging list list-notif level critical
ciscoasa(config)# logging list list-notif level warning class ha
```

前回の手順で使用したものと同じコマンドを入力し、既存のメッセージリストの名前と追加基準を指定します。リストに追加する基準ごとに、新しいコマンドを入力します。たとえば、リストに追加される syslog メッセージの基準として、次の基準を指定できます。

- ID が 104024 ～ 105999 の範囲の syslog メッセージ。
- 重大度が critical 以上（emergency、alert、または critical）のすべての syslog メッセージ。
- 重大度が warning 以上（emergency、alert、critical、error、または warning）のすべての ha クラスの syslog メッセージ。

（注）
syslog メッセージは、これらの条件のいずれかを満たす場合にログに記録されます。syslog メッセージが複数の条件を満たす場合、そのメッセージは一度だけログに記録されます。

ロギング フィルタの設定

指定した出力先へのクラス内のすべての syslog メッセージの送信

クラス内のすべての syslog メッセージを指定した出力先に送信するには、次の手順を実行します。

手順

指定した出力先コマンドでコンフィギュレーションを上書きします。たとえば、重大度 7 のメッセージが内部ログ バッファに送信されるように指定し、重大度 3 の ha クラスのメッセージが内部ログバッファに送信されるように指定すると、後のコンフィギュレーションが優先されます。

logging class*message_class* {**buffered** |**console** |**history** |**mail** |**monitor** |**trap**} [*severity_level*]

例：

```
ciscoasa(config)# logging class ha buffered alerts
```

buffered、**history**、**mail**、**monitor**、および **trap** キーワードは、このクラスの syslog メッセージの出力先を指定します。**history** キーワードは、SNMP でのロギングを有効にします。**monitor** キーワードは、Telnet および SSH でのロギングを有効にします。**trap** キーワードは、syslog サーバーでのロギングを有効にします。コマンドライン エントリあたり 1 つの出力先を指定します。1 つのクラスが複数の出力先に送信されるように指定する場合は、出力先ごとに新しいコマンドを入力します。

syslog メッセージの生成レートの制限

syslog メッセージの生成レートを制限するには、次の手順を実行します。

手順

指定された重大度（1 ～ 7）を、指定の時間内でメッセージセットまたは個々のメッセージ（出力先ではない）に適用します。

logging rate-limit {**unlimited** | {*num* [*interval*]}} **message** *syslog_id* | **level** *severity_level*

例：

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

レート制限は、すべての設定された出力先に送信されるメッセージの量に影響します。ロギング レート制限をデフォルト値にリセットするには、**clear running-config logging rate-limit** コマンドを入力します。ロギング レート制限をリセットするには、**clear configure logging rate-limit** コマンドを入力します。

ログのモニタリング

ロギング ステータスの監視については、次のコマンドを参照してください。

- **show logging**

  このコマンドは、重大度を含む syslog メッセージを表示します。

（注）

- 表示できる syslog メッセージの最大数は、1000 です。これはデフォルト設定です。表示できる syslog メッセージの最大数は、2000 です。
- **show logging** の出力にホスト TX カウンタが表示される場合、**clear logging counters all** コマンドを実行した後でも表示されます。

- **show logging message**

  このコマンドは、変更された重大度とディセーブルにされた syslog メッセージを含む syslog メッセージのリストを示します。

- **show logging message** *message_ID*

  このコマンドは、特定の syslog メッセージの重大度を示します。

- **show logging queue**

  このコマンドは、ロギング キューとキュー統計情報を示します。

- **show running-config logging rate-limit**

  このコマンドは、現在のロギング レート制限の設定を表示します。

- **[設定（Configuration）] > [Firewall] > [アクセス ルール（Access Rules）]**

  このペインでは、検索条件（Rule Hex Id）に基づいて、特定のログに対するロギングのライブビューアをフィルタリングできます。結果を表示するには、ルールを選択して、**[ログの表示（Show Log）]**をクリックします。

ロギングの例

次の例は、**show logging** コマンドで表示されるロギング情報を示しています。

```
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

```
ciscoasa (config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: enabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 330272 messages logged
    Trap logging: level debugging, facility 20, 325464 messages logged
        Logging to inside 2001:164:5:1::123
    Permit-hostdown logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

次の例は、syslog メッセージをイネーブルにするかどうかを制御する方法と、指定した syslog メッセージの重大度を制御する方法を示しています。

```
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)

ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (disabled)

ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors, current-level alerts (enabled)

ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: -level errors (enabled)
```

ロギングの履歴

表 *63*：ロギングの履歴

機能名	プラットフォーム リリース	説明
Logging	7.0(1)	さまざまな出力先を経由して ASA ネットワーク ロギング情報を提供します。ログ ファイルを表示して保存するオプションも含まれています。

機能名	プラットフォーム リリース	説明
レート制限	7.0(4)	syslog メッセージが生成されるレートを制限します。 **logging rate-limit** コマンドが導入されました。
ロギング リスト	7.2(1)	さまざまな基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するために他のコマンドで使用されるロギング リストを作成します。 次のコマンドが導入されました。**logging list**
セキュア ロギング	8.0(2)	リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 **logging host** コマンドが変更されました。
ロギング クラス	8.0(4)、8.1(1)	ロギング メッセージの ipaa イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。
ロギング クラスと保存されたロギング バッファ	8.2(1)	ロギング メッセージの dap イベント クラスに対するサポートが追加されました。 **logging class** コマンドが変更されました。 保存されたロギング バッファ（ASDM、内部、FTP、およびフラッシュ）をクリアする追加サポート。 **clear logging queue bufferwrap** コマンドが導入されました。
パスワードの暗号化	8.3(1)	パスワードの暗号化に対するサポートが追加されました。 **logging ftp server** コマンドが変更されました。
ログ ビューア	8.3(1)	送信元 IP アドレスおよび宛先 IP アドレスがログ ビューアに追加されました。

機能名	プラットフォーム リリース	説明
拡張ロギングと接続ブロック	8.3(2)	TCP を使用するように syslog サーバーを設定すると、syslog サーバーを使用できない場合、ASA はサーバーが再び使用可能になるまで syslog メッセージを生成する新しい接続をブロックします（たとえば、VPN、ファイアウォール、カットスルー プロキシ接続）。この機能は、ASA のロギング キューがいっぱいのときにも新しい接続をブロックするように拡張されました。接続は、ロギング キューがクリアされると再開されます。 この機能は、Common Criteria EAL4+ への準拠のために追加されました。必要でない限り、syslog メッセージを送受信できない場合でも接続を許可することを推奨します。接続を許可するには、**logging permit-hostdown** コマンドを使用します。 414005、414006、414007、414008 の各 syslog メッセージが導入されました。 **show logging** コマンドが変更されました。
syslog メッセージのフィルタリングとソート	8.4(1)	次のサポートが追加されました。 • さまざまなカラムに対応する複数のテキスト文字列に基づく syslog メッセージ フィルタリング。 • カスタム フィルタの作成。 • メッセージのカラムによるソート。詳細については、『ASDM 構成ガイド』を参照してください。 この機能は、すべての ASA バージョンと相互運用性があります。
クラスタ	9.0(1)	ASA 5580 および 5585-X のクラスタリング環境での syslog メッセージ生成のサポートが追加されました。 **logging device-id** コマンドが変更されました。
スタンバイ装置の syslog のブロック	9.4(1)	フェールオーバー コンフィギュレーションのスタンバイ装置で特定の syslog メッセージの生成をブロックするためのサポートを追加しました。 **logging message** *syslog-id* **standby** コマンドが導入されました。
syslog サーバーのセキュアな接続のための参照 ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 検証は、syslog サーバー サーバーへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のコマンドが追加または変更されました。**[no] crypto ca reference-identity**、**logging host**。

機能名	プラットフォーム リリース	説明
syslog サーバーでの IPv6 アドレスのサポート	9.7(1)	TCP と UDP 経由で syslog を記録、送信、受信するために、syslog サーバーを IPv6 アドレスで設定できるようになりました。 次のコマンドが変更されました。**logging host**
ロギング クラス	9.12(1)	ロギングメッセージの BFD、BGP、インターフェイス、IPv6、マルチキャスト、Object-Group-Search、PBR、ルーティング、SLA クラスのサポートが追加されました。 **logging class** コマンドが変更されました。
syslog のループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、syslog に使用できるようになりました。 新規/変更されたコマンド：**interface loopback**、**logging host**
SNMP syslog のレート制限	9.20(1)	システム全体のレート制限を設定しない場合、SNMP サーバーに送信される syslog に対して個別にレート制限を設定できるようになりました。 新規/変更されたコマンド： **logging history rate-limit**

第 47 章

SNMP

この章では、Simple Network Management Protocol（SNMP）に ASA をモニターさせるための設定方法について説明します。

- SNMP について （1689 ページ）
- SNMP のガイドライン （1708 ページ）
- SNMP の構成 （1712 ページ）
- SNMP モニタリング （1723 ページ）
- SNMP の例 （1724 ページ）
- SNMP の履歴 （1725 ページ）

SNMP について

SNMPは、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルで、TCP/IP プロトコル スイートの一部です。ASAは SNMP バージョン 1、2c、および 3 を使用したネットワーク監視に対するサポートを提供し、3 つのバージョンの同時使用をサポートします。ASA のインターフェイス上で動作する SNMP エージェントを使用すると、HP OpenView などのネットワーク管理システム（NMS）を使用してネットワーク デバイスをモニターできます。ASAは GET 要求の発行を通じて SNMP 読み取り専用アクセスをサポートします。SNMP 書き込みアクセスは許可されていないため、SNMP を使用して変更することはできません。さらに、SNMP SET 要求はサポートされていません。

NMS（ネットワーク管理システム）に特定のイベント（イベント通知）を送信するために、管理対象デバイスから管理ステーションへの要求外のメッセージであるトラップを送信するように ASA を設定したり、NMS を使用してセキュリティ デバイス上で管理情報ベース（MIB）を検索できます。MIBは定義の集合であり、ASAは各定義に対応する値のデータベースを保持しています。MIB をブラウズすることは、NMS から MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して値を決定することを意味します。

（注） 集中的なワークロードでは、10 を超える NMS を展開すると、デバイスのパフォーマンスに影響を与える可能性があります。デバイスの安定性と応答性を確保するために、SNMP ウォークポーリングの実行とトラップトラフィックの管理には NMS を慎重に利用することを推奨します。

ASA には SNMP エージェントが含まれています。このエージェントは、通知を必要とすることが事前に定義されているイベント（たとえば、ネットワーク内のリンクがアップ状態またはダウン状態になる）が発生すると、指定した管理ステーションに通知します。このエージェントが送信する通知には、管理ステーションに対して自身を識別する SNMP OID が含まれています。ASA エージェントは、管理ステーションが情報を要求した場合にも応答します。

SNMP の用語

次の表に、SNMP で頻繁に使用される用語を示します。

表 *64 : SNMP* の用語

用語	説明
エージェント	ASAで稼働する SNMP サーバー。SNMP エージェントは、次の機能を搭載しています。 • ネットワーク管理ステーションからの情報の要求およびアクションに応答する。 • 管理情報ベース（SNMP マネージャが表示または変更できるオブジェクトの集合）へのアクセスを制御する。 • SET 操作を許可しない。
ブラウジング	デバイス上の SNMP エージェントから必要な情報をポーリングすることによって、ネットワーク管理ステーションからデバイスのヘルスをモニターすること。このアクティビティには、ネットワーク管理ステーションから MIB ツリーの一連の GET-NEXT または GET-BULK 要求を発行して、値を決定することが含まれる場合があります。
管理情報ベース（MIB）	パケット、接続、バッファ、フェールオーバーなどに関する情報を収集するための標準化されたデータ構造。MIB は、大部分のネットワークデバイスで使用される製品、プロトコル、およびハードウェア標準によって定義されます。SNMP ネットワーク管理ステーションは、MIB をブラウズし、特定のデータまたはイベントの発生時にこれらを要求できます。
ネットワーク管理ステーション（NMS）	SNMPイベントのモニターやASAなどのデバイスの管理用に設定されている、PC またはワークステーション。
オブジェクト ID（OID）	NMS に対してデバイスを識別し、モニターおよび表示される情報の源をユーザーに示すシステム。

用語	説明
Trap	SNMP エージェントから NMS へのメッセージを生成する、事前定義済みのイベント。イベントには、リンクアップ、リンクダウン、コールドスタート、ウォームスタート、認証、syslog メッセージなどのアラーム状態が含まれます。

MIB およびトラップ

MIB は、標準またはエンタープライズ固有です。標準 MIB はインターネット技術特別調査委員会（IETF）によって作成され、さまざまな Request for Comment（RFC）に記載されています。トラップは、ネットワークデバイスで発生する重要なイベント（多くの場合、エラーまたは障害）を報告します。SNMP トラップは、標準またはエンタープライズ固有の MIB のいずれかで定義されます。標準トラップは IETF によって作成され、さまざまな RFC に記載されています。SNMP トラップは、ASA ソフトウェアにコンパイルされています。

必要に応じて、次の場所から RFC、標準 MIB、および標準トラップをダウンロードすることもできます。

http://www.ietf.org/

次の場所から Cisco MIB、トラップ、および OID の完全なリストを参照してください。

https://github.com/cisco/cisco-mibs/blob/main/supportlists/asa/asa-supportlist.html

また、Cisco OID を次の場所から FTP でダウンロードしてください。

https://github.com/cisco/cisco-mibs/tree/main/oid

（注） ソフトウェア バージョン 7.2(1)、8.0(2) 以降では、SNMP を介してアクセスされるインターフェイス情報は 5 秒ごとにリフレッシュされます。そのため、連続するポーリングの間に少なくとも 5 秒間は待機することをお勧めします。

MIB のすべての OID がサポートされているわけではありません。特定の ASA に対してサポートされている SNMP MIB および OID のリストを取得するには、次のコマンドを入力します。

```
ciscoasa(config)# show snmp-server oidlist
```

（注） **oidlist** キーワードは **show snmp-server** コマンドのヘルプのオプション リストには表示されませんが、使用できます。ただし、このコマンドは Cisco TAC でのみ使用されます。このコマンドを使用する前に TAC にお問い合わせください。

次に、**show snmp-server oidlist** コマンドの出力例を示します。

```
ciscoasa(config)# show snmp-server oidlist
[0]     1.3.6.1.2.1.1.1.        sysDescr
```

```
[1]     1.3.6.1.2.1.1.2.        sysObjectID
[2]     1.3.6.1.2.1.1.3.        sysUpTime
[3]     1.3.6.1.2.1.1.4.        sysContact
[4]     1.3.6.1.2.1.1.5.        sysName
[5]     1.3.6.1.2.1.1.6.        sysLocation
[6]     1.3.6.1.2.1.1.7.        sysServices
[7]     1.3.6.1.2.1.2.1.        ifNumber
[8]     1.3.6.1.2.1.2.2.1.1.    ifIndex
[9]     1.3.6.1.2.1.2.2.1.2.    ifDescr
[10]    1.3.6.1.2.1.2.2.1.3.    ifType
[11]    1.3.6.1.2.1.2.2.1.4.    ifMtu
[12]    1.3.6.1.2.1.2.2.1.5.    ifSpeed
[13]    1.3.6.1.2.1.2.2.1.6.    ifPhysAddress
[14]    1.3.6.1.2.1.2.2.1.7.    ifAdminStatus
[15]    1.3.6.1.2.1.2.2.1.8.    ifOperStatus
[16]    1.3.6.1.2.1.2.2.1.9.    ifLastChange
[17]    1.3.6.1.2.1.2.2.1.10.   ifInOctets
[18]    1.3.6.1.2.1.2.2.1.11.   ifInUcastPkts
[19]    1.3.6.1.2.1.2.2.1.12.   ifInNUcastPkts
[20]    1.3.6.1.2.1.2.2.1.13.   ifInDiscards
[21]    1.3.6.1.2.1.2.2.1.14.   ifInErrors
[22]    1.3.6.1.2.1.2.2.1.16.   ifOutOctets
[23]    1.3.6.1.2.1.2.2.1.17.   ifOutUcastPkts
[24]    1.3.6.1.2.1.2.2.1.18.   ifOutNUcastPkts
[25]    1.3.6.1.2.1.2.2.1.19.   ifOutDiscards
[26]    1.3.6.1.2.1.2.2.1.20.   ifOutErrors
[27]    1.3.6.1.2.1.2.2.1.21.   ifOutQLen
[28]    1.3.6.1.2.1.2.2.1.22.   ifSpecific
[29]    1.3.6.1.2.1.4.1.        ipForwarding
[30]    1.3.6.1.2.1.4.20.1.1.   ipAdEntAddr
[31]    1.3.6.1.2.1.4.20.1.2.   ipAdEntIfIndex
[32]    1.3.6.1.2.1.4.20.1.3.   ipAdEntNetMask
[33]    1.3.6.1.2.1.4.20.1.4.   ipAdEntBcastAddr
[34]    1.3.6.1.2.1.4.20.1.5.   ipAdEntReasmMaxSize
[35]    1.3.6.1.2.1.11.1.       snmpInPkts
[36]    1.3.6.1.2.1.11.2.       snmpOutPkts
[37]    1.3.6.1.2.1.11.3.       snmpInBadVersions
[38]    1.3.6.1.2.1.11.4.       snmpInBadCommunityNames
[39]    1.3.6.1.2.1.11.5.       snmpInBadCommunityUses
[40]    1.3.6.1.2.1.11.6.       snmpInASNParseErrs
[41]    1.3.6.1.2.1.11.8.       snmpInTooBigs
[42]    1.3.6.1.2.1.11.9.       snmpInNoSuchNames
[43]    1.3.6.1.2.1.11.10.      snmpInBadValues
[44]    1.3.6.1.2.1.11.11.      snmpInReadOnlys
[45]    1.3.6.1.2.1.11.12.      snmpInGenErrs
[46]    1.3.6.1.2.1.11.13.      snmpInTotalReqVars
[47]    1.3.6.1.2.1.11.14.      snmpInTotalSetVars
[48]    1.3.6.1.2.1.11.15.      snmpInGetRequests
[49]    1.3.6.1.2.1.11.16.      snmpInGetNexts
[50]    1.3.6.1.2.1.11.17.      snmpInSetRequests
[51]    1.3.6.1.2.1.11.18.      snmpInGetResponses
[52]    1.3.6.1.2.1.11.19.      snmpInTraps
[53]    1.3.6.1.2.1.11.20.      snmpOutTooBigs
[54]    1.3.6.1.2.1.11.21.      snmpOutNoSuchNames
[55]    1.3.6.1.2.1.11.22.      snmpOutBadValues
[56]    1.3.6.1.2.1.11.24.      snmpOutGenErrs
[57]    1.3.6.1.2.1.11.25.      snmpOutGetRequests
[58]    1.3.6.1.2.1.11.26.      snmpOutGetNexts
[59]    1.3.6.1.2.1.11.27.      snmpOutSetRequests
[60]    1.3.6.1.2.1.11.28.      snmpOutGetResponses
[61]    1.3.6.1.2.1.11.29.      snmpOutTraps
[62]    1.3.6.1.2.1.11.30.      snmpEnableAuthenTraps
[63]    1.3.6.1.2.1.11.31.      snmpSilentDrops
[64]    1.3.6.1.2.1.11.32.      snmpProxyDrops
```

```
[65]    1.3.6.1.2.1.31.1.1.1.1. ifName
[66]    1.3.6.1.2.1.31.1.1.1.2. ifInMulticastPkts
[67]    1.3.6.1.2.1.31.1.1.1.3. ifInBroadcastPkts
[68]    1.3.6.1.2.1.31.1.1.1.4. ifOutMulticastPkts
[69]    1.3.6.1.2.1.31.1.1.1.5. ifOutBroadcastPkts
[70]    1.3.6.1.2.1.31.1.1.1.6. ifHCInOctets
--More--
```

SNMP オブジェクト識別子

シスコのシステムレベルの各製品には、MIB-II の sysObjectID として使用される SNMP オブジェクト ID（OID）があります。CISCO-PRODUCTS-MIB と CISCO-ENTITY-VENDORTYPE-OID-MIB は、SNMPv2-MIB、Entity Sensor MIB および Entity Sensor Threshold Ext MIB の sysObjectID オブジェクト内で報告できる OID が含まれています。モデル タイプを識別するためにこの値を使用できます。次の表に、ASA および ISA モデルの sysObjectID OID を示します。

表 *65 : SNMP* オブジェクト識別子

製品 ID	sysObjectID	モデル番号
ASA 仮想	ciscoASAv（ciscoProducts 1902）	Cisco 適応型セキュリティ仮想アプライアンス（ASA 仮想）
ASA 仮想 システム コンテキスト	ciscoASAvsy（ciscoProducts 1903）	Cisco 適応型セキュリティ仮想アプライアンス（ASA 仮想）のシステム コンテキスト
ASA 仮想 セキュリティ コンテキスト	ciscoASAvsc（ciscoProducts 1904）	Cisco 適応型セキュリティ仮想アプライアンス（ASA 仮想）のセキュリティ コンテキスト。
Cisco Secure Firewall 1200	ciscoCsf1210ce（ciscoProducts 3303） ciscoCsf1210cp（ciscoProducts 3304） ciscoCsf1220cx（ciscoProducts 3305）	CSF1210CE、CSF1210CP、CSF1220CX
Cisco Secure Firewall 4200	ciscoFpr4215td（ciscoProducts 3043） ciscoFpr4225td（ciscoProducts 3042） ciscoFpr4245td（ciscoProducts 3041）	FPR4215、FPR4225、FPR4245
ISA 30004C 産業用セキュリティ アプライアンス	ciscoProducts 2268	ciscoISA30004C
CISCO ISA30004C（4 GE Copper セキュリティ コンテキスト）	ciscoProducts 2139	ciscoISA30004Csc

製品 ID	sysObjectID	モデル番号
CISCO ISA30004C（4 GE Copper システム コンテキスト）	ciscoProducts 2140	ciscoISA30004Csy
ISA 30002C2F 産業用セキュリティ アプライアンス	ciscoProducts 2267	ciscoISA30002C2F
CISCO ISA30002C2F（2 GE 銅線ポート、2 GE 光ファイバ セキュリティ コンテキスト）	ciscoProducts 2142	ciscoISA30002C2Fsc
CISCO ISA30002C2F（2 GE 銅線ポート、2 GE 光ファイバ システム コンテキスト）	ciscoProducts 2143	ciscoISA30002C2Fsy
Cisco 産業用セキュリティ アプライアンス（ISA）30004C シャーシ	cevChassis 1677	cevChassisISA30004C
Cisco 産業用セキュリティ アプライアンス（ISA）30002C2F シャーシ	cevChassis 1678	cevChassisISA30002C2F
ISA30004C Copper SKU 向け中央演算処理装置温度センサー	cevSensor 187	cevSensorISA30004CCpuTempSensor
ISA30002C2F 光ファイバ向け中央演算処理装置温度センサー	cevSensor 189	cevSensorISA30002C2FCpuTempSensor
ISA30004C Copper SKU 向けプロセッサ カード温度センサー	cevSensor 192	cevSensorISA30004CPTS
ISA30002C2F Fiber SKU 向けプロセッサ カード温度センサー	cevSensor 193	cevSensorISA30002C2FPTS
ISA30004C Copper SKU 向けパワー カード温度センサー	cevSensor 197	cevSensorISA30004CPowercardTS
ISA30002C2F Fiber SKU 向けパワー カード温度センサー	cevSensor 198	cevSensorISA30002C2FPowercardTS
ISA30004C 向けポート カード温度センサー	cevSensor 199	cevSensorISA30004CPortcardTS
ISA30002C2F 向けポート カード温度センサー	cevSensor 200	cevSensorISA30002C2FPortcardTS
ISA30004C Copper SKU 向け中央演算処理装置	cevModuleCpuType 329	cevCpuISA30004C

製品 ID	sysObjectID	モデル番号
ISA30002C2F 光ファイバ SKU 向け中央演算処理装置	cevModuleCpuType 330	cevCpuISA30002C2F
モジュール ISA30004C、ISA30002C2F	cevModule 111	cevModuleISA3000Type
30004C 産業用セキュリティ アプライアンス ソリッド ステート ドライブ	cevModuleISA3000Type 1	cevModuleISA30004CSSD64
30002C2F 産業用セキュリティ アプライアンス ソリッド ステート ドライブ	cevModuleISA3000Type 2	cevModuleISA30002C2FSSD64
Cisco ISA30004C/ISA30002C2F ハードウェア バイパス	cevModuleISA3000Type 5	cevModuleISA3000HardwareBypass
Cisco Secure Firewall 1210CE	cevChassis 2580	cevChassisCsf1210ce
Secure Firewall 1210CP Chassis	cevChassis 2581	cevChassisCsf 1210cp
Secure Firewall 1220CX Chassis	cevChassis 2582	cevChassisCsf1220cx
Secure Firewall 1200 シリーズ ファン	cevFan 468	cevFanCsf1200
Cisco Secure Firewall 1220CX 向け中央演算処理装置	cevModuleCpuType 380	cevCpuCsf1220cx
Cisco Secure Firewall 1210CP 向け中央演算処理装置	cevModuleCpuType 381	cevCpuCsf1210cp
Cisco Secure Firewall 1210CE 向け中央演算処理装置	cevModuleCpuType 382	`cevCpuCsf 1210ce`
FirePOWER 4140 セキュリティ アプライアンス、1U（組み込みセキュリティ モジュール 36）	ciscoFpr4140K9（ciscoProducts 2293）	FirePOWER 4140
FirePOWER 4120 セキュリティ アプライアンス、1U（組み込みセキュリティ モジュール 24）	ciscoFpr4120K9（ciscoProducts 2294）	FirePOWER 4120
FirePOWER 4K ファン ベイ	cevContainer 363	cevContainerFPR4KFanBay
FirePOWER 4K 電源ベイ	cevContainer 364	cevContainerFPR4KPowerSupplyBay
Cisco Secure Firewall Threat Defense Virtual、VMware	cevChassis 1795	cevChassisCiscoFTDVVMW
Cisco Firewall Threat Defense Virtual、AWS	cevChassis 1796	cevChassisCiscoFTDVAWS

物理ベンダー タイプ値

シスコの各シャーシまたはスタンドアロン システムには、SNMP で使用する一意のタイプ番号があります。entPhysicalVendorType OID は CISCO-ENTITY-VENDORTYPE-OID-MIB で定義されます。この値は、ASA、ASA 仮想、または ASASM の SNMP エージェントから entPhysicalVendorType オブジェクトで返されます。この値を使用してコンポーネントのタイプ（モジュール、電源装置、ファン、センサー、CPU など）を識別できます。次の表に、ASA モデルの物理ベンダータイプ値を示します。

表 *66 :* 物理ベンダー タイプ値

項目	**entPhysicalVendorType OID** の説明
ギガビット イーサネット ポート	cevPortGe（cevPort 109）
Cisco 適応型セキュリティ仮想アプライアンス	cevChassisASAv（cevChassis 1451）
Cisco Secure Firewall 4200-X（FPR4215/FPR4225/FPR4245）	cevFPRNM4X200Gng および cevFPRNM2X100Gng（デュアル EPM 2X100G および 4X200G がスロット 2 およびスロット 3 に追加された場合）

MIB でサポートされるテーブルおよびオブジェクト

次の表 に、指定された MIB でサポートされるテーブルおよびオブジェクトを示します。

マルチコンテキストモードでは、これらのテーブルとオブジェクトは単一のコンテキストに関する情報を提供します。コンテキスト全体のデータが必要な場合は、それらを合計する必要があります。たとえば、全体的なメモリ使用量を取得するには、各コンテキストの cempMemPoolHCUsed 値を合計します。

表 *67 : MIB* でサポートされるテーブルおよびオブジェクト

MIB 名と **OID**	サポートされているテーブルとオブジェクト
ENTITY-MIB。OID：1.3.6.1.2.1.47	entPhysicalTable、entPhysicalDescr、entPhysicalVendorType、entPhysicalName

MIB 名と OID	サポートされているテーブルとオブジェクト
CISCO-ENHANCED-MEMPOOL-MIB、OID:1.3.6.1.4.1.9.9.221	cempMemPoolTable、cempMemPoolIndex、cempMemPoolType、cempMemPoolName、cempMemPoolAlternate、cempMemPoolValid 32 ビットメモリシステムの場合は、32 ビットメモリカウンタを使用してポーリング：cempMemPoolUsed、cempMemPoolFree、cempMemPoolUsedOvrflw、cempMemPoolFreeOvrflw、cempMemPoolLargestFree、cempMemPoolLowestFree、cempMemPoolUsedLowWaterMark、cempMemPoolAllocHit、cempMemPoolAllocMiss、cempMemPoolFreeHit、cempMemPoolFreeMiss、cempMemPoolLargestFreeOvrflw、cempMemPoolLowestFreeOvrflw、cempMemPoolUsedLowWaterMarkOvrflw、cempMemPoolSharedOvrflw 64 ビットメモリシステムの場合は、64 ビットメモリカウンタを使用してポーリング：cempMemPoolHCUsed、cempMemPoolHCFree、cempMemPoolHCLargestFree、cempMemPoolHCLowestFree、cempMemPoolHCUsedLowWaterMark、cempMemPoolHCShared
CISCO-REMOTE-ACCESS-MONITOR-MIB、OID:1.3.6.1.4.1.9.9.392 （注） これら 3 つの MIB OID を使用して、リモートアクセス接続が失敗する理由を追跡できます。	crasNumTotalFailures、crasNumSetupFailInsufResources、crasNumAbortedSessions
CISCO-ENTITY-SENSOR-EXT-MIB、OID:1.3.6.1.4.1.9.9.745	ceSensorExtThresholdTable
CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、OID:1.3.6.1.4.1.9.9.480	ciscoL4L7ResourceLimitTable
CISCO-TRUSTSEC-SXP-MIB、OID:1.3.6.1.4.1.9.9.720 （注） ASA 仮想 ではサポートされていません。	ctsxSxpGlobalObjects、ctsxSxpConnectionObjects、ctsxSxpSgtObjects
DISMAN-EVENT-MIB、OID:1.3.6.1.2.1.88	mteTriggerTable、mteTriggerThresholdTable、mteObjectsTable、mteEventTable、mteEventNotificationTable
DISMAN-EXPRESSION-MIB、OID:1.3.6.1.2.1.90	expExpressionTable、expObjectTable、expValueTable
ENTITY-SENSOR-MIB、OID: 1.3.6.1.2.1.99 （注） シャーシの温度、ファン RPM、電源電圧などの物理センサーに関連する情報を提供します。ASA 仮想プラットフォームではサポートされません。	entPhySensorTable

MIB 名と OID	サポートされているテーブルとオブジェクト
NAT-MIB、OID:1.3.6.1.2.1.123	natAddrMapTable、natAddrMapIndex、natAddrMapName、natAddrMapGlobalAddrType、natAddrMapGlobalAddrFrom、natAddrMapGlobalAddrTo、natAddrMapGlobalPortFrom、natAddrMapGlobalPortTo、natAddrMapProtocol、natAddrMapAddrUsed、natAddrMapRowStatus
CISCO-PTP-MIB、OID:1.3.6.1.4.1.9.9.760 （注） E2E トランスペアレント クロック モードに対応する MIB のみがサポートされます。	ciscoPtpMIBSystemInfo、cPtpClockDefaultDSTable、cPtpClockTransDefaultDSTable、cPtpClockPortTransDSTable
CISCO-PROCESS-MIB; 1.3.6.1.4.1.9.9.109.1.1.1.1.7.1 1.3.6.1.4.1.9.9.109.1.1.1.1.7.2 ～ 1.3.6.1.4.1.9.9.109.1.1.1.1.7.(n+1)	cpmCPUTotal1minRev cpmCPUTotal1minRev の関連パラメータと値 例： • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+2) - 集約システム CPU 使用率（この値は、シングルコンテキストモードの .3.6.1.4.1.9.9.109.1.1.1.1.7.1 のシステム CPU 使用率と同じです）。 • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+3) - Snort 平均 CPU 使用率（すべての snort インスタンスの合計値） • .3.6.1.4.1.9.9.109.1.1.1.1.7.(n+4) - システムプロセス平均 %（「Sysproc」コアの平均）

サポートされるトラップ（通知）

次の表 に、サポートされているトラップ（通知）および関連する MIB を示します。

表 *68 :* サポートされるトラップ（通知）

トラップおよび **MIB** 名	変数バインド リスト	説明
authenticationFailure （SNMPv2-MIB）	—	SNMP バージョン 1 または 2 の場合は、SNMP 要求で指定されたコミュニティ ストリングが正しくありません。SNMP バージョン 3 では、auth または priv パスワードまたはユーザ名が間違っている場合、レポート PDU がトラップの代わりに生成されます。 **snmp-server enable traps snmp authentication** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
bgpBackwardTransition	bgpPeerLastError、bgpPeerState	**snmp-server enable traps peer-flap** コマンドは、BGP ピアフラップに関連するトラップの送信をイネーブルにするために使用されます。
ccmCLIRunningConfigChanged （CISCO-CONFIG-MAN-MIB）	ccmHistoryRunningLastChanged、ccmHistoryEventTerminalType	**snmp-server enable traps config** コマンドは、このトラップの送信をイネーブルにするために使用されます。
cefcFRUInserted (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-insert** コマンドはこの通知をイネーブルにするために使用されます。
cefcFRURemoved (CISCO-ENTITY-FRU-CONTROL-MIB)	entPhysicalContainedIn	**snmp-server enable traps entity fru-remove** コマンドはこの通知をイネーブルにするために使用されます。

トラップおよび **MIB** 名	変数バインド リスト	説明
ceSensorExtThresholdNotification (CISCO-ENTITY-SENSOR-EXT-MIB)	entPhysicalName、 entPhysicalDescr、 entPhySensorValue、 entPhySensorType、 ceSensorExtThresholdValue	**snmp-server enable traps entity** [**power-supply-failure** | **fan-failure** | **cpu-temperature**] コマンドは、エンティティしきい値通知の伝送をイネーブルにするために使用されます。この通知は、電源障害に対して送信されます。送信されるオブジェクトは、ファンおよび CPU の温度を指定します。 **snmp-server enable traps entity fan-failure** コマンドは、ファン障害トラップの送信をイネーブルにするために使用されます。このトラップは、Firepower 2100 シリーズには適用されません。 **snmp-server enable traps entity power-supply-failure** コマンドは、電源障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity chassis-fan-failure** コマンドは、シャーシファン障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity cpu-temperature** コマンドは、高 CPU 温度トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity power-supply-presence** コマンドは、電源プレゼンス障害トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity power-supply-temperature** コマンドは、電源温度しきい値トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity chassis-temperature** コマンドは、シャーシ周囲温度トラップの送信をイネーブルにするために使用されます。 **snmp-server enable traps entity accelerator-temperature** コマンドは、シャーシアクセラレータ温度トラップの送信をイネーブルにするために使用されます。

トラップおよび MIB 名	変数バインド リスト	説明
cikeTunnelStart （CISCO-IPSEC-FLOW-MONITOR-MIB）	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunLifeTime	**snmp-server enable traps ikev2 start** コマンドは、ikev2 start トラップの送信をイネーブルにするために使用されます。
cikeTunnelStop （CISCO-IPSEC-FLOW-MONITOR-MIB）	cikePeerLocalAddr、 cikePeerRemoteAddr、 cikeTunActiveTime	**snmp-server enable traps ikev2 stop** コマンドは、ikev2 stop トラップの送信をイネーブルにするために使用されます。
cipSecTunnelStart (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunLifeTime、 cipSecTunLifeSize	**snmp-server enable traps ipsec start** コマンドは、このトラップの送信をイネーブルにするために使用されます。
cipSecTunnelStop (CISCO-IPSEC-FLOW-MONITOR-MIB)	cipSecTunActiveTime	**snmp-server enable traps ipsec stop** コマンドは、このトラップの送信をイネーブルにするために使用されます。
ciscoConfigManEvent （CISCO-CONFIG-MAN-MIB）	ccmHistoryEventCommandSource、 ccmHistoryEventConfigSource、 ccmHistoryEventConfigDestination	**snmp-server enable traps config** コマンドは、このトラップの送信をイネーブルにするために使用されます。
ciscoRasTooManySessions (CISCO-REMOTE-ACCESS-MONITOR-MIB)	crasNumSessions、 crasNumUsers、 crasMaxSessionsSupportable、 crasMaxUsersSupportable、 crasThrMaxSessions	**snmp-server enable traps remote-access session-threshold-exceeded** コマンドは、これらのトラップの送信をイネーブルにするために使用されます。
ciscoUFwFailoverStateChanged （CISCO-UNIFIED-FIREWALL-MIB）	gid、FOStatus	**snmp-server enable traps failover-state** コマンドは、failover-state トラップの送信をイネーブルにするために使用されます。
clogMessageGenerated （CISCO-SYSLOG-MIB）	clogHistFacility、 clogHistSeverity、 clogHistMsgName、 clogHistMsgText、 clogHistTimestamp	syslog メッセージが生成されます。 clogMaxSeverity オブジェクトの値は、トラップとして送信する syslog メッセージを決定するために使用されます。 **snmp-server enable traps syslog** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
clrResourceLimitReached (CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB)	crlResourceLimitValueType、 crlResourceLimitMax、 clogOriginIDType、clogOriginID	**snmp-server enable traps connection-limit-reached** コマンドは、この connection-limit-reached 通知の伝送を有効にするために使用されます。clogOriginID オブジェクトには、トラップを発信したコンテキスト名が含まれています。

トラップおよび **MIB** 名	変数バインド リスト	説明
coldStart （SNMPv2-MIB）	—	SNMP の設定後に SNMP エージェントが起動するときに発生する ColdStart トラップ。このトラップは、システムの再起動後にエージェントが起動したときにも発生します。 （注） クラスタノードと HA ノードの場合、リロード後、インターフェイスのリブート時間が 5 分（プリセットしきい値）を超えると、トラップはドロップされます。クラスタおよびHA ノードが正常に再起動すると、他のすべてのトラップが想定どおりに送信されます。 **snmp-server enable traps snmp coldstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
cpmCPURisingThreshold （CISCO-PROCESS-MIB）	cpmCPURisingThresholdValue、cpmCPUTotalMonIntervalValue、cpmCPUInterruptMonIntervalValue、cpmCPURisingThresholdPeriod、cpmProcessTimeCreated、cpmProcExtUtil5SecRev	**snmp-server enable traps cpu threshold rising** コマンドは、CPU threshold rising 通知の伝送を有効にするために使用されます。cpmCPURisingThresholdPeriod オブジェクトは、他のオブジェクトとともに送信されます。
cufwClusterStateChanged （CISCO-UNIFIED-FIREWALL-MIB）	status	**snmp-server enable traps cluster-state** コマンドは、cluster-state トラップの送信をイネーブルにするために使用されます。
entConfigChange （ENTITY-MIB）	—	**snmp-server enable traps entity config-change fru-insert fru-remove** コマンドは、この通知をイネーブルにするために使用されます。 （注） この通知は、セキュリティ コンテキストが作成または削除された場合にマルチ モードでのみ送信されます。
linkDown （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクダウン トラップ。 **snmp-server enable traps snmp linkdown** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

トラップおよび **MIB** 名	変数バインド リスト	説明
linkUp （IF-MIB）	ifIndex、ifAdminStatus、ifOperStatus	インターフェイスのリンクアップ トラップ。 **snmp-server enable traps snmp linkup** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。
mteTriggerFired （DISMAN-EVENT-MIB）	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、cempMemPoolName、cempMemPoolHCUsed	**snmp-server enable traps memory-threshold** コマンドは、memory threshold 通知を有効にするために使用されてます。mteHotOID が cempMemPoolHCUsed に設定されます。cempMemPoolName および cempMemPoolHCUsed オブジェクトは、他のオブジェクトとともに送信されます。
mteTriggerFired （DISMAN-EVENT-MIB）	mteHotTrigger、mteHotTargetName、mteHotContextName、mteHotOID、mteHotValue、ifHCInOctets、ifHCOutOctets、ifHighSpeed、entPhysicalName	**snmp-server enable traps interface-threshold** コマンドは、interface threshold 通知を有効にするために使用されます。entPhysicalName オブジェクトは、他のオブジェクトと共に送信されます。
natPacketDiscard （NAT-MIB）	ifIndex	**snmp-server enable traps nat packet-discard** コマンドは、NAT packet discard 通知を有効にするために使用されます。この通知は、マッピング スペースを使用できないため、5 分間にレート制限され、IP パケットが NAT により廃棄された場合に生成されます。ifIndex は、マッピング インターフェイスの ID を提供します。
ospfNbrStateChange	ospfRouterId、ospfNbrIpAddr、ospfNbrAddressLessIndex、ospfNbrRtrId、ospfNbrState	**snmp-server enable traps peer-flap** コマンドは、OSPF peer-flap に関連するトラップの送信をイネーブルにするために使用されます。 （注） ASA5585 モデルの場合、netsnmp バージョン 5.8 ライブラリを使用するように SNMP エンジンが変更されており、次の OID はライブラリで使用できません。 • ospfIfStateChange 1.3.6.1.2.1.14.16.2.16 • ospfVirtIfStateChange 1.3.6.1.2.1.14.16.2.1 • ospfVirtNbrStateChange 1.3.6.1.2.1.14.16.2.3

トラップおよび MIB 名	変数バインド リスト	説明
warmStart （SNMPv2-MIB）	—	SNMP エージェントが初めて再起動したときに発生するwarmStartトラップ。このトラップは、SNMP 設定の変更後にエージェントが再起動した場合にも発生し、すべてのSNMPホスト設定が削除され、新しいSNMP設定が行われます。 **snmp-server enable traps snmp warmstart** コマンドは、これらのトラップの伝送をイネーブルおよびディセーブルにするために使用されます。

インターフェイスの種類と例

SNMP トラフィック統計情報を生成するインターフェイスの種類には次のものがあります。

- 論理：物理統計情報のサブセットであり、ソフトウェア ドライバによって収集される統計情報。
- 物理：ハードウェア ドライバによって収集される統計情報。物理的な名前の付いた各インターフェイスは、それに関連付けられている論理統計情報と物理統計情報のセットを1つ持っています。各物理インターフェイスは、関連付けられている VLAN インターフェイスを複数持っている場合があります。VLANインターフェイスは論理統計情報だけを持っています。

（注） 複数の VLAN インターフェイスが関連付けられている物理インターフェイスでは、ifInOctets と ifOutoctets の OID の SNMP カウンタがその物理インターフェイスの集約トラフィック カウンタと一致していることに注意してください。

- VLAN-only：SNMP は ifInOctets と ifOutOctets に対して論理統計情報を使用します。

次の表の例で、SNMP トラフィック統計情報における差異を示します。例 1 では、**show interface** コマンドと **show traffic** コマンドの物理出力統計情報と論理出力統計情報の差異を示します。例 2 では、**show interface** コマンドと **show traffic** コマンドの VLAN だけのインターフェイスに対する出力統計情報を示します。この例は、統計情報が **show traffic** コマンドに対して表示される出力に近いことを示しています。

表 *69 :* 物理インターフェイスと *VLAN* インターフェイスの *SNMP* トラフィック統計情報

例 1	例 2
ciscoasa# **show interface GigabitEthernet3/2** interface GigabitEthernet3/2 description fullt-mgmt nameif mgmt security-level 10 ip address 10.7.14.201 255.255.255.0 management-only ciscoasa# **show traffic** (Condensed output) Physical Statistics GigabitEthernet3/2: received (in 121.760 secs) **36 packets 3428 bytes** 0 pkts/sec 28 bytes/sec Logical Statistics mgmt: received (in 117.780 secs) **36 packets 2780 bytes** 0 pkts/sec 23 bytes/sec 次の例は、管理インターフェイスと物理インターフェイスの SNMP 出力統計情報を示しています。ifInOctets 値は、**show traffic** コマンド出力で表示される物理統計情報出力に近くなりますが、論理統計情報出力には近くなりません。 mgmt インターフェイスの ifIndex： IF_MIB::ifDescr.6 = Adaptive Security Appliance 'mgmt' interface 物理インターフェイス統計情報に対応する物理インターフェイス統計： **IF-MIB::ifInOctets.6 = Counter32:3246**	ciscoasa# **show interface GigabitEthernet** interface GigabitEthernet0/0.100 vlan 100 nameif inside security-level 100 ip address 10.7.1.101 255.255.255.0 stan ciscoasa# **show traffic** inside received (in 9921.450 secs) **1977 packets 126528 bytes** 0 pkts/sec 12 bytes/sec transmitted (in 9921.450 secs) **1978 packets 126556 bytes** 0 pkts/sec 12 bytes/sec 内部の VLAN の ifIndex： IF-MIB::ifDescr.9 = Adaptive Security Ap **IF-MIB::ifInOctets.9 = Counter32: 126318**

SNMP バージョン 3 の概要

SNMP バージョン 3 は SNMP バージョン 1 またはバージョン 2c では使用できなかったセキュリティ拡張機能を提供します。SNMP バージョン 1 とバージョン 2c は SNMP サーバーと SNMP エージェント間でデータをクリアテキストで転送します。SNMP バージョン 3 は認証とプライバシー オプションを追加してプロトコル オペレーションをセキュリティ保護します。また、このバージョンはユーザーベース セキュリティ モデル（USM）とビューベース アクセス コントロール モデル（VACM）を通して SNMP エージェントと MIB オブジェクトへのアクセスをコントロールします。ASA は、SNMP グループとユーザーの作成、およびセキュアな SNMP 通信の転送の認証と暗号化を有効にするために必要なホストの作成もサポートします。

セキュリティ モデル

設定上の目的のために、認証とプライバシーのオプションはセキュリティモデルにまとめられます。セキュリティモデルはユーザーとグループに適用され、次の3つのタイプに分けられます。

- NoAuthPriv：認証もプライバシーもありません。メッセージにどのようなセキュリティも適用されないことを意味します。
- AuthNoPriv：認証はありますがプライバシーはありません。メッセージが認証されることを意味します。
- AuthPriv：認証とプライバシーがあります。メッセージが認証および暗号化されることを意味します。

SNMP グループ

SNMP グループはユーザーを追加できるアクセス コントロール ポリシーです。各 SNMP グループはセキュリティ モデルを使用して設定され、SNMP ビューに関連付けられます。SNMP グループ内のユーザーは、SNMP グループのセキュリティ モデルに一致する必要があります。これらのパラメータは、SNMP グループ内のユーザがどのタイプの認証とプライバシーを使用するかを指定します。各 SNMP グループ名とセキュリティ モデルのペアは固有である必要があります。

SNMP ユーザー

SNMP ユーザーは、指定されたユーザー名、ユーザーが属するグループ、認証パスワード、暗号化パスワード、および使用する認証アルゴリズムと暗号化アルゴリズムを持ちます。認証アルゴリズムのオプションは SHA-1、SHA-224、SHA-256 HMAC および SHA-384 です。暗号化アルゴリズムのオプションは、3DES および AES（128、192、および 256 バージョンで使用可能）です。ユーザーを作成した場合は、それを SNMP グループに関連付ける必要があります。その後、そのユーザーはグループのセキュリティ モデルを継承します。

（注） SNMP v3 ユーザーアカウントを設定するときは、認証アルゴリズムの長さが暗号化アルゴリズムの長さ以上であることを確認してください。

SNMP ホスト

SNMP ホストは SNMP 通知とトラップの送信先となる IP アドレスです。トラップは設定されたユーザーだけに送信されるため、ターゲット IP アドレスとともに SNMP バージョン 3 のホストを設定するには、ユーザー名を設定する必要があります。SNMP ターゲット IP アドレスとターゲットパラメータ名は ASA で一意である必要があります。各 SNMP ホストはそれぞれに関連付けられているユーザ名を 1 つだけ持つことができます。SNMP トラップを受信するには、**snmp-server host** コマンドを追加した後に、NMS のユーザー クレデンシャルが ASA のクレデンシャルと一致するように設定してください。

（注） 最大 8,192 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。

ASA と Cisco IOS ソフトウェアの実装の相違点

ASA での SNMP バージョン 3 の実装は、Cisco IOS ソフトウェアでの SNMP バージョン 3 の実装とは次の点で異なります。

- ローカル エンジン ID とリモート エンジン ID は設定できません。ローカルエンジン ID は、ASA が起動されたとき、またはコンテキストが作成されたときに生成されます。
- ビューベースのアクセス コントロールに対するサポートはないため、結果として MIB のブラウジングは無制限になります。
- サポートは、USM、VACM、FRAMEWORK、および TARGET という MIB に制限されます。
- 正しいセキュリティ モデルを使用してユーザーとグループを作成する必要があります。
- 正しい順序でユーザー、グループ、およびホストを削除する必要があります。
- snmp-server host コマンドを使用すると、着信 SNMP トラフィックを許可する ASA ルールが作成されます。

SNMP syslog メッセージ

SNMP では、212*nnn* という番号が付いた詳細な syslog メッセージが生成されます。syslog メッセージは、ASA または ASASM から、SNMP 要求、SNMP トラップ、SNMP チャネルのステータスを、指定のインターフェイスの指定のホストに表示します。

syslog メッセージの詳細については、syslog メッセージガイドを参照してください。

（注） SNMP syslog メッセージがレート制限（毎秒約 4000）を超えた場合、SNMP ポーリングは失敗します。

アプリケーション サービスとサードパーティ ツール

SNMP サポートについては、次の URL を参照してください。

http://www.cisco.com/en/US/tech/tk648/tk362/tk605/tsd_technology_support_sub-protocol_home.html

SNMP バージョン 3 MIB をウォークするためのサードパーティ ツールの使い方については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa83/snmp/snmpv3_tools.html

SNMP のガイドライン

この項では、SNMP を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

フェールオーバーとクラスタリングのガイドライン

- クラスタリングまたはフェールオーバーで SNMPv3 を使用する場合、最初のクラスタ形成後に新しいクラスタユニットを追加するか、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットに複製されません。ユーザを新しいユニットに強制的に複製するには、SNMPv3 ユーザを制御またはアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます（SNMPv3 ユーザおよびグループは、クラスタデータユニットで設定コマンドを入力できないというルールの例外です）。制御ユニットまたはアクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してデータユニットまたはスタンバイユニットに直接入力することにより、各ユーザを再設定します。

IPv6 ガイドライン（すべての ASA モデル）

SNMP を IPv6 転送上で設定できるため、IPv6 ホストは SNMP クエリを実行でき、IPv6 ソフトウェアを実行するデバイスから SNMP 通知を受信できます。SNMP エージェントおよび関連する MIB が拡張され、IPv6 アドレッシングがサポートされるようになりました。

その他のガイドライン

- アプライアンスモードで動作しているシステムでは、電源トラップは発行されません。
- アプライアンス モードの Firepower 2100 では、ハードウェアモデルとシリアルをポーリングできません。ASA では、これらの詳細についてトラップは生成されません。そのため、ASA インスタンスのインターフェイスではなくシャーシ管理 IP をポーリングするように FXOS またはシャーシ マネージャの SNMP を設定します。
- SNMP トラップを受信するか MIB をブラウズするには、CiscoWorks for Windows か別の SNMP MIB-II 互換ブラウザを持っている必要があります。
- VPN トンネル経由の管理アクセスは、SNMP（**management-access** コマンド）ではサポートされません。VPN 経由の SNMP の場合、ループバック インターフェイスで SNMP を有効にすることをお勧めします。ループバック インターフェイスで SNMP を使用するために、管理アクセス機能を有効にする必要はありません。ループバックは SSH でも機能します。
- ビューベースのアクセス コントロールはサポートされませんが、ブラウジングに VACM MIB を使用してデフォルトのビュー設定を決定できます。
- ENTITY-MIB は管理外コンテキストでは使用できません。代わりに IF-MIB を使用して、管理外コンテキストでクエリーを実行します。

- ENTITY-MIB は Firepower 9300 では使用できません。代わりに、CISCO-FIREPOWER-EQUIPMENT-MIB および CISCO-FIREPOWER-SM-MIB を使用します。
- 一部のデバイスでは、**snmpwalk** の出力に表示されるインターフェイスの順序（ifDescr）が再起動後に変わることが確認されています。ASA では、アルゴリズムを使用して SNMP が照会する ifIndex テーブルを決定します。ASA の起動時、ASA による設定の読み取りでロードされる順序でインターフェイスが ifIndex テーブルに追加されます。ASA に新しいインターフェイスが追加されると、ifIndex テーブルのインターフェイスのリストに追加されていきます。インターフェイスの追加、削除、または名前変更により、再起動時にインターフェイスの順序が変わることがあります。
- **snmpwalk** コマンドで OID を指定すると、snmpwalk ツールは、指定された OID の下にあるサブツリー内のすべての変数をクエリし、その値を表示します。そのため、デバイス上のオブジェクトの包括的な出力を表示するには、**snmpwalk** コマンドで OID を指定してください。
- AIP SSM または AIP SSC では、SNMP バージョン 3 はサポートされません。
- SNMP デバッグはサポートされません。
- ARP 情報の取得はサポートされません。
- SNMP SET コマンドはサポートされません。
- NET-SNMP バージョン 5.4.2.1 を使用する場合、暗号化アルゴリズム バージョン AES128 だけがサポートされます。暗号化アルゴリズム バージョンの AES256 または AES192 はサポートされません。
- 結果として SNMP 機能の整合性が取れない状態になる場合、既存の設定への変更は拒否されます。
- SNMP バージョン 3 の設定は、グループ、ユーザー、ホストの順に行う必要があります。
- SecureFirewall モデルの場合、**snmpwalk** コマンドは、管理のコンテキストからのみ FXOS MIB をポーリングします。
- グループを削除する前に、そのグループに関連付けられているすべてのユーザーが削除されていることを確認する必要があります。
- ユーザーを削除する前に、そのユーザー名に関連付けられているホストが設定されていないことを確認する必要があります。
- 特定のセキュリティ モデルを使用して特定のグループに属するようにユーザーが設定されている場合にそのグループのセキュリティ レベルを変更する場合は、次の順に操作を実行する必要があります。
  - そのグループからユーザを削除します。
  - グループのセキュリティ レベルを変更します。
  - 新しいグループに属するユーザーを追加します。

- MIB オブジェクトのサブセットへのユーザー アクセスを制限するためのカスタム ビューの作成はサポートされていません。
- すべての要求とトラップは、デフォルトの読み取り/通知ビューだけで使用できます。
- connection-limit-reached トラップは管理コンテキストで生成されます。このトラップを生成するには、接続制限に達したユーザー コンテキストで設定された SNMP サーバー ホストが少なくとも 1 つ必要です。
- 最大 4000 個までホストを追加できます。ただし、トラップの対象として設定できるのはそのうちの 128 個だけです。
- サポートされるアクティブなポーリング先の総数は 128 個です。
- ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。
- 1 つのホストに複数のユーザを関連付けることができます。
- ネットワーク オブジェクトは、別の **host-group** コマンドと重複して指定することができます。異なるネットワーク オブジェクトの共通のホストに対しては、最後のホスト グループに指定した値が適用されます。
- ホスト グループや他のホスト グループと重複するホストを削除すると、設定済みのホスト グループで指定されている値を使用してホストが再設定されます。
- ホストで取得される値は、コマンドの実行に使用するように指定したシーケンスによって異なります。
- SNMP で送信できるメッセージのサイズは 1472 バイトまでです。
- ASA では、コンテキストごとに SNMP サーバーのトラップ ホスト数の制限がありません。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。

トラブルシューティングのヒント

- NMS からの着信パケットを受信する SNMP プロセスが実行されていることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# show process | grep snmp
```

- SNMP からの syslog メッセージをキャプチャし、ASA コンソールに表示するには、次のコマンドを入力します。

```
ciscoasa(config)# logging list snmp message 212001-212015
ciscoasa(config)# logging console snmp
```

- SNMP プロセスがパケットを送受信していることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# clear snmp-server statistics
ciscoasa(config)# show snmp-server statistics
```

出力は SNMPv2-MIB の SNMP グループに基づきます。

- SNMP パケットが ASA を通過し、SNMP プロセスに送信されていることを確認するには、次のコマンドを入力します。

```
ciscoasa(config)# clear asp drop
ciscoasa(config)# show asp drop
```

- NMS が正常にオブジェクトを要求できない場合、または ASA からの着信トラップを処理していない場合は、次のコマンドを入力し、パケットキャプチャを使用して問題を切り離します。

```
ciscoasa (config)# access-list snmp permit udp any eq snmptrap any
ciscoasa (config)# access-list snmp permit udp any any eq snmp
ciscoasa (config)# capture snmp type raw-data access-list snmp interface mgmt
ciscoasa (config)# copy /pcap capture:snmp tftp://192.0.2.5/exampledir/snmp.pcap
```

- ASA が期待どおりに動作していない場合は、次の操作を実行して、ネットワークトポロジとトラフィックに関する情報を取得します。
  - NMS の設定について、次の情報を取得します。

    タイムアウトの回数

    リトライ回数

    エンジン ID キャッシング

    使用されるユーザー名とパスワード

  - 次のコマンドを発行します。

    show block

    show interface

    show process

    show cpu

    show vm

- 重大エラーが発生した場合は、エラーの再現を支援するために、Cisco TAC にトレースバック ファイルと **show tech-support** コマンドの出力を送信します。
- SNMP トラフィックが ASA インターフェイスを通過できない場合、**icmp permit** コマンドを使用して、リモート SNMP サーバーから ICMP トラフィックを許可する必要がある場合があります。
- **snmp-server enable oid** でデバイスを設定している場合、SNMP ウォークの操作を実行すると、ASA は MEMPOOL_DMA プールと MEMPOOL_GLOBAL_SHARED プールからメモリ

情報を照会します。これにより、SNMP 関連の CPU ホグ状態になり、パケットがドロップされることがあります。この問題を軽減するには、 **no snmp-server enable oid** コマンドを使用して、グローバル共有プールに関連する OID をポーリングしないようにしてください。無効にすると、mempool OID は 0 バイトを返します。

- ASP ドロップカウンタをポーリングするための単一の要求で多数の OID を指定して SNMPGET を使用する場合、ASP ドロップカウンタのポーリングを繰り返す必要があり、CPU 使用率が高くなります。そのため、モニターする重要なカウンタを特定し、カウンタごとに SNMPGET を使用してそれらの値を取得することで、CPU への影響を限定的なものにすることをお勧めします。
- マルチコンテキスト ASA の複数のコンテキストで SNMP が設定されている場合は、コンテキストを順番にポーリングし、snmpwalk ではなく SNMPBULKGET を使用してプラットフォームへの接続数を減らします。このアプローチにより、多数のコンテキストが同時にポーリングされている場合に、SNMP による遅延やタイムアウトを回避できます。
- ASA は、SNMP BULKGET などの SNMP get-response メッセージで SNMP ポーリングに応答する場合は、Don't Fragment（DF）ビットを常に設定します。この場合、ネットワークパス全体が、ASA で設定されている最大伝送ユニット（MTU）をサポートする必要があります。ネットワーク パスで設定された MTU の値を小さくすると、他のデバイスからフラグメンテーションを要求する ICMP パケットが送信されることがあります。ただし、DF ビットが設定されているため、ASA は応答せず、パケットをフラグメント化しません。その結果、ASA からの応答は失われます。

  この問題に対処するには、ASA またはネットワークパス全体で MTU を変更するか、SNMPBULKGET の代わりに複数の get 要求を使用するか、または SNMPBULKGET 要求のバルク サイズを小さくします。

- トラブルシューティングの追加情報については、次の URL を参照してください。
  http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/116423-troubleshoot-asa-snmp.html

SNMP の構成

ここでは、SNMP の設定方法について説明します。

手順

ステップ 1 SNMP エージェントおよび SNMP サーバーをイネーブルにします。

ステップ 2 SNMP トラップを設定します。

ステップ 3 SNMP バージョン 1 および 2c のパラメータまたは SNMP バージョン 3 のパラメータを設定します。

SNMP エージェントおよび SNMP サーバーの有効化

SNMPエージェントおよびSNMPサーバーをイネーブルにするには、次の手順を実行します。

手順

ASA で SNMP エージェントおよび SNMP サーバーを有効にします。デフォルトでは、SNMP サーバーはイネーブルになっています。

snmp-server enable

例：

```
ciscoasa(config)# snmp-server enable
```

SNMP トラップの設定

SNMP エージェントが生成するトラップ、およびそのトラップを収集し、NMS に送信する方法を指定するには、次の手順を実行します。

（注） すべてのSNMPトラップまたはsyslogトラップを有効にすると、SNMPプロセスがエージェントとネットワーク内で過剰にリソースを消費し、システムがハングアップする可能性があります。システムの遅延、未完了の要求、またはタイムアウトが発生した場合は、SNMPトラップとsyslogトラップを選択して有効にすることができます。たとえば、情報syslogトラップのシビラティ（重大度）レベルをスキップできます。

手順

個別のトラップ、トラップのセット、またはすべてのトラップを NMS に送信します。

snmp-server enable traps [**all** | **syslog** | **snmp** [**authentication** | **linkup** | **linkdown** | **coldstart** | **warmstart**] | **config** | **entity** [**config-change** | **fru-insert** | **fru-remove** | **fan-failure** | **cpu-temperature** | **chassis-fan-failure** | **power-supply**] | **chassis-temperature** | **power-supply-presence** | **power-supply-temperature l1-bypass-status**] | **ikev2** [**start** | **stop**] | **cluster-state** | **failover-state** | **peer-flap** | **ipsec** [**start** | **stop**] | **remote-access** [**session-threshold-exceeded**] | **connection-limit-reached** | **cpu threshold rising** | **interface-threshold** | **memory-threshold** | **nat** [**packet-discard**]

例：

```
ciscoasa(config)# snmp-server enable traps snmp authentication
linkup linkdown coldstart warmstart
```

このコマンドでは、トラップとして NMS に送信する syslog メッセージをイネーブルにしています。デフォルトコンフィギュレーションでは、例に示すように、すべての SNMP 標準トラップがイネーブルになっています。このトラップを無効にするには、**no snmp-server enable traps snmp** コマンドを使用します。

このコマンドを入力するときにトラップ タイプを指定しない場合、デフォルトでは **syslog** トラップになります。デフォルトでは、**syslog** トラップはイネーブルになっています。デフォルトの SNMP トラップは、**syslog** トラップとともにイネーブルの状態を続けます。

syslog MIB からのトラップを生成するには、**logging history** コマンドと **snmp-server enable traps syslog** コマンドの両方を設定する必要があります。

SNMP トラップがイネーブルにされたデフォルトの状態を復元するには、**clear configure snmp-server** コマンドを使用します。デフォルトでは他のトラップはすべてディセーブルです。

管理コンテキストでのみ使用できるトラップ：

- **connection-limit-reached**
- **entity**
- **memory-threshold**

システム コンテキストの物理的に接続されたインターフェイスに対してだけ管理コンテキストを介して生成されたトラップ：

- **interface-threshold**

その他すべてのトラップは、シングル モードの管理およびユーザー コンテキストで使用できます。

config トラップを指定すると、ciscoConfigManEvent 通知と ccmCLIRunningConfigChanged 通知がイネーブルになります。これらの通知は、コンフィギュレーション モードを終了した後に生成されます。

CPU 使用率が、設定されたモニタリング期間に設定済みしきい値を超えると、**cpu threshold rising** トラップが生成されます。

使用されたシステム コンテキストのメモリが総システム メモリの 80 % に達すると、**memory-threshold** トラップが管理コンテキストから生成されます。他のすべてのユーザー コンテキストでは、このトラップは使用メモリが特定のコンテキストの総システム メモリの 80 % に到達した場合に生成されます。

一部のトラップは、特定のハードウェア モデルに適用できません。トラップキーワードの代わりに ? を使用すると、デバイスで使用可能なトラップを確認できます。次に例を示します。

- Firepower 1000 シリーズ は、次のエンティティトラップのみをサポートします：**chassis-temperature**、**config-change**、および **cpu-temperature**。

（注）
SNMP は電圧センサーをモニターしません。

CPU 使用率のしきい値の設定

CPU 使用率のしきい値を設定するには、次の手順を実行します。

手順

高 CPU しきい値の値とモニタリング期間を設定します。

snmp cpu threshold rising *threshold_value monitoring_period*

例：

```
ciscoasa(config)# snmp cpu threshold rising 75% 30 minutes
```

CPU 使用率のしきい値およびモニタリング期間をクリアするには、このコマンドの **no** 形式を使用します。**snmp cpu threshold rising** コマンドが設定されていない場合、上限しきい値レベルのデフォルトは 70 % を超え、クリティカルしきい値レベルのデフォルトは 95 % を超えます。デフォルトのモニタリング期間は 1 分に設定されます。

CPU のクリティカルしきい値レベルは設定できません。この値は 95 % に固定されています。高 CPU しきい値の有効値の範囲は 10 ～ 94 % です。モニタリング期間の有効値は 1～60 分です。

物理インターフェイスのしきい値の設定

物理インターフェイスのしきい値を設定するには、次の手順を実行します。

手順

SNMP 物理インターフェイスのしきい値を設定します。

snmp interface threshold *threshold_value*

例：

```
ciscoasa(config)# snmp interface threshold 75%
```

SNMP 物理インターフェイスのしきい値をクリアするには、このコマンドの **no** 形式を使用します。しきい値は、インターフェイス帯域幅利用率の割合として定義されます。有効なしきい値の範囲は 30～99 % です。デフォルト値は 70 % です。

snmp interface threshold コマンドを使用できるのは、管理コンテキストのみです。

物理インターフェイスの使用状況はシングル モードおよびマルチ モードでモニターされ、システム コンテキストの物理インターフェイスのトラップは管理コンテキストを通して送信されます。物理インターフェイスだけがしきい値の使用状況を計算するために使用されます。

SNMP バージョン 1 または 2c のパラメータの設定

SNMP バージョン 1 または 2c のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 SNMP通知の受信者を指定し、トラップの送信元のインターフェイスを指定し、ASAに接続できる NMS または SNMP マネージャの名前および IP アドレスを指定します。

snmp-server host{*interface hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1 2c**| *username*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 2c
ciscoasa(config)# snmp-server host corp 172.18.154.159 community public

ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 2c
```

trap キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルトのコミュニティ ストリングは public です。ASA では、このキーを使用して着信 SNMP 要求が有効かどうかを判別します。たとえば、コミュニティ ストリングを使用してサイトを指定し、同じストリングを使って ASA と管理ステーションを設定できます。ASA は指定されたストリングを使用し、無効なコミュニティ ストリングを使用した要求には応答しません。ただし、SNMP モニタリングが診断インターフェイスではなく管理インターフェイスを介している場合、ASA がコミュニティ文字列を検証せずにポーリングが実行されます。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリア テキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

version キーワードは、トラップと要求（ポーリング）に使用される SNMP のバージョンを指定します。サーバとの通信は、選択したバージョンのみを使用して許可されます。

トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA で設定されたクレデンシャルと同じクレデンシャルを使用して NMS でユーザーを確実に設定するようにします。

ステップ 2 SNMP バージョン 1 または 2c だけで使用するコミュニティ ストリングを設定します。

snmp-server community *community-string*

例：

```
ciscoasa(config)# snmp-server community onceuponatime
```

（注）
コミュニティストリングでは特殊文字（!、@、#、$、%、^、&、*、\）を使用しないでください。一般に、オペレーティングシステムで使用される関数用に予約されている特殊文字を使用すると、予期しない結果が生じる可能性があります。たとえば、バックスラッシュ（\）はエスケープ文字と解釈されるため、コミュニティストリングでは使用できません。

ステップ 3 SNMP サーバーの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 4 SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different
port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

SNMP バージョン 3 のパラメータの設定

SNMP バージョン 3 のパラメータを設定するには、次の手順を実行します。

手順

ステップ 1 SNMP バージョン 3 だけで使用する、新しい SNMP グループを指定します。

snmp-server group *group-name* **v3** [**auth** | **noauth** | **priv**]

例：

```
ciscoasa(config)# snmp-server group testgroup1 v3 auth
```

コミュニティ ストリングが設定されている場合は、コミュニティ ストリングに一致する名前を持つ 2 つの追加グループが自動生成されます。1 つはバージョン 1 のセキュリティ モデルのグループであり、もう 1 つはバージョン 2 のセキュリティ モデルのグループです。**auth** キーワードは、パケット認証を有効にします。**noauth** キーワードは、パケット認証や暗号化が使用されていないことを示します。**priv** キーワードは、パケット暗号化と認証を有効にします。**auth** または **priv** キーワードには、デフォルト値がありません。

ステップ 2 SNMP バージョン 3 だけで使用する、SNMP グループの新しいユーザーを設定します。

snmp-server user *username group_name* **v3** [**engineID** *engineID*] [**encrypted**] [**auth** {**sha** | **sha224** | **sha256** | **sha384**} *auth_password* [**priv** {**3des** | **aes** {**128** | **192** | **256**}} *priv_password*]]

例：

```
ciscoasa(config)# snmp-server user testuser1 testgroup1 v3 auth md5 testpassword
aes 128 mypassword
ciscoasa(config)# snmp-server user testuser1 public v3 encrypted auth md5
00:11:22:33:44:55:66:77:88:99:AA:BB:CC:DD:EE:FF
```

username 引数は、SNMP エージェントに属するホスト上のユーザーの名前です。ユーザー名を 32 文字までで入力します。名前の先頭は文字である必要があります。有効な文字は、文字、数字、_（アンダースコア）です。.（ピリオド）、@（アットマーク）、-（ハイフン）も指定できます。

group-name 引数は、ユーザーが属するグループの名前です。**v3** キーワードは、SNMP バージョン 3 のセキュリティ モデルを使用することを指定し、**encrypted**、**priv**、および **auth** キーワードの使用を有効化します。**engineID** キーワードはオプションで、ユーザーの認証と暗号化の情報をローカライズするために使用される ASA のエンジン ID を指定します。engineID 引数には、有効な ASA エンジン ID を指定する必要があります。

encrypted キーワードは、暗号化された形式でパスワードを指定します。暗号化されたパスワードは、次の要件を満たしている必要があります。

- 16 進数形式。
- 8 ～ 80 文字を含む。
- 文字、数字、および ~`!@#%^&*()_-+{}[]|\:;"'<,>./ のみを含む。
- 次の記号を含まない。$（ドル記号）、?（疑問符）、「=」（等号）。

- 5 つ以上の異なる文字を含める必要があります。
- 連続するインクリメントまたはデクリメントの数字または文字をたくさん含めないでください。たとえば、「12345」は 4 つ、「ZYXW」は 3 つ文字列が続いています。このような文字の合計数が特定の制限を超えると（通常は約 4 ～ 6 回発生）、簡素化チェックに失敗します。

（注）
連続するインクリメントまたはデクリメント文字列の間に連続しないインクリメントまたはデクリメント文字列が含まれても、文字数はリセットされません。たとえば、abcd&!21 はパスワード チェックに失敗しますが、abcd&!25 は失敗しません。

auth キーワードは、使用する認証レベル（**sha**、**sha224**、**sha256**、または **sha384**）を指定します。**priv** キーワードは、暗号化レベルを指定します。**auth** または **priv** キーワードのデフォルト値はありません。また、デフォルト パスワードもありません。

暗号化アルゴリズムには、**3des** または **aes** キーワードを指定できます。使用する AES 暗号化アルゴリズムのバージョンとして、**128**、**192**、**256** のいずれかを指定することもできます。auth-password 引数は、認証ユーザー パスワードを指定します。priv-password 引数は、暗号化ユーザー パスワードを指定します。

パスワードを忘れた場合は、回復できないため、ユーザーを再設定する必要があります。プレーンテキストのパスワードまたはローカライズされたダイジェストを指定できます。ローカライズされたダイジェストは、ユーザに対して選択した認証アルゴリズム（SHA、SHA-224、SHA-256、または SHA-384）に一致する必要があります。ユーザー設定がコンソールに表示される場合、またはファイル（スタートアップ コンフィギュレーション ファイルなど）に書き込まれる場合、ローカライズされた認証ダイジェストとプライバシー ダイジェストが常にプレーンテキストのパスワードの代わりに表示されます（2 番目の例を参照してください）。パスワードの最小長は、英数字 1 文字です。ただし、セキュリティを確保するために 8 文字以上の英数字を使用することを推奨します。

クラスタリングまたはフェールオーバーで SNMPv3 を使用する場合、最初のクラスタ形成後に新しいクラスタユニットを追加するか、フェールオーバーユニットを交換すると、SNMPv3 ユーザは新しいユニットに複製されません。ユーザを新しいユニットに強制的に複製するには、SNMPv3 ユーザを制御またはアクティブユニットに再度追加する必要があります。または、新しいユニットにユーザを直接追加できます（SNMPv3 ユーザおよびグループは、クラスタデータユニットで設定コマンドを入力できないというルールの例外です）。制御ユニットまたはアクティブユニットで **snmp-server user** *username group-name* **v3** コマンドを入力するか、暗号化されていない形式の *priv-password* オプションと *auth-password* オプションを使用してデータユニットまたはスタンバイユニットに直接入力することにより、各ユーザを再設定します。

制御ユニットまたはアクティブユニットで **encrypted** キーワードを使用してユーザを入力すると、SNMPv3 ユーザコマンドがレプリケートされないことを通知するエラーメッセージが表示されます。この動作は、既存の SNMPv3 ユーザおよびグループコマンドがレプリケーション中にクリアされないことも意味します。

たとえば、暗号化されたキーで入力されたコマンドを使用する制御ユニットまたはアクティブユニットは次のようになります。

```
ciscoasa(config)# snmp-server user defe abc v3 encrypted auth sha
c0:e7:08:50:47:eb:2e:e4:3f:a3:bc:45:f6:dd:c3:46:25:a0:22:9a
priv aes 256 cf:ad:85:5b:e9:14:26:ae:8f:92:51:12:91:16:a3:ed:de:91:6b:f7:
f6:86:cf:18:c0:f0:47:d6:94:e5:da:01
ERROR: This command cannot be replicated because it contains localized keys.
```

クラスタ複製時のデータユニットの場合の例（**snmp-server user** コマンドが設定にある場合にのみ表示されます）：

```
ciscoasa(cfg-cluster)#
Detected Cluster Master.
Beginning configuration replication from Master.
WARNING: existing snmp-server user CLI will not be cleared.
```

ステップ 3 SNMP通知の受信者を指定します。トラップの送信元となるインターフェイスを指定します。ASA に接続できる NMS または SNMP マネージャの名前と IP アドレスを指定します。

snmp-server host *interface* {*hostname* | *ip_address*} [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** *username*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host mgmt 10.7.14.90 version 3 testuser1
ciscoasa(config)# snmp-server host mgmt 10.7.26.5 version 3 testuser2
ciscoasa(config)# snmp-server host mgmt 12:ab:56:ce::11 version 3 testuser3
```

trap キーワードは、NMS をトラップの受信だけに制限します。**poll** キーワードは、NMS を要求の送信（ポーリング）だけに制限します。デフォルトでは、SNMP トラップはイネーブルになっています。デフォルトでは、UDP ポートは 162 です。コミュニティ ストリングは、ASA と NMS の間の共有秘密キーです。キーは、大文字と小文字が区別される最大 32 文字の英数字の値です。スペースは使用できません。デフォルト コミュニティ ストリングは public です。ASA は、このキーを使用して、着信 SNMP 要求が有効かどうかを判断します。たとえば、コミュニティストリングを使用してサイトを指定すると、ASA と NMS を同じストリングを使用して設定できます。ASA は指定されたストリングを使用し、無効なコミュニティストリングを使用した要求には応答しません。暗号化されたコミュニティ ストリングを使用した後は、暗号化された形式だけがすべてのシステム（CLI、ASDM、CSM など）に表示されます。クリアテキストのパスワードは表示されません。暗号化されたコミュニティ ストリングは常に ASA によって生成されます。通常は、クリア テキストの形式で入力します。

version キーワードは、トラップと要求（ポーリング）に使用される SNMP のバージョンを指定します。サーバとの通信は、選択したバージョンのみを使用して許可されます。

SNMP バージョン 3 のホストを ASA に設定する場合は、ユーザーをそのホストに関連付ける必要があります。

トラップを受信するには、**snmp-server host** コマンドを追加した後に、ASA で設定されたクレデンシャルと同じクレデンシャルを使用してNMSでユーザーを確実に設定するようにします。

ステップ 4 SNMP サーバーの場所または担当者情報を設定します。

snmp-server [**contact** | **location**] *text*

例：

```
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
```

text 引数には、担当者または ASA システム管理者の名前を指定します。名前は大文字と小文字が区別され、最大 127 文字です。スペースを使用できますが、複数のスペースを入力しても 1 つのスペースになります。

ステップ 5 SNMP 要求のリスニング ポートを設定します。

snmp-server listen-port *lport*

例：

```
ciscoasa(config)# snmp-server lport 192
```

lport 引数には、着信要求を受け取るポートを指定します。デフォルトのリスニング ポートは 161 です。**snmp-server listen-port** コマンドは管理コンテキストでのみ使用でき、システム コンテキストでは使用できません。現在使用中のポートで **snmp-server listen-port** コマンドを設定すると、次のメッセージが表示されます。

```
The UDP port port is in use by another feature. SNMP requests to the device
will fail until the snmp-server listen-port command is configured to use a different
port.
```

既存の SNMP スレッドはポートが使用可能になるまで 60 秒ごとにポーリングを続け、ポートがまだ使用中の場合は syslog メッセージ %ASA-1-212001 を発行します。

ユーザーのグループの設定

指定したユーザーのグループからなる SNMP ユーザー リストを設定するには、次の手順を実行します。

手順

SNMP ユーザー リストを設定します。

snmp-server user-list *list_name* **username** *user_name*

例：

```
ciscoasa(config)# snmp-server user-list engineering username user1
```

listname 引数には、ユーザー リストの名前を指定します。最大 33 文字まで指定できます。**username** *user_name* のキーワードと引数のペアで、ユーザー リストに設定するユーザーを指定します。ユーザー リストのユーザーは、**snmp-server user** *username* コマンドで設定します。

このコマンドは、SNMP バージョン 3 を使用している場合にのみ使用できます。ユーザー リストには複数のユーザーを含める必要があり、ホスト名または IP アドレスの範囲に関連付けることができます。

ネットワーク オブジェクトへのユーザーの関連付け

ユーザー リストの単一のユーザーまたはユーザーのグループをネットワーク オブジェクトに関連付けるには、次の手順を実行します。

手順

ユーザー リストの単一のユーザーまたはユーザーのグループをネットワーク オブジェクトに関連付けます。

snmp-server host-group *net_obj_name* [**trap**| **poll**] [**community** *community-string*] [**version** {**1** | **2c** | **3** {*username* | **user-list** *list_name*}] [**udp-port** *port*]

例：

```
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 1
ciscoasa(config)# snmp-server host-group inside net1 trap community public version 2c
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user1
ciscoasa(config)# snmp-server host-group inside net1 trap version 3 user-list engineering
```

net_obj_name 引数は、ユーザーまたはユーザー グループを関連付けるインターフェイスのネットワーク オブジェクト名を指定します。

trap キーワードは、トラップの送信のみが可能であり、このホストはブラウズ（ポーリング）できないことを指定します。SNMP トラップはデフォルトでイネーブルになっています。

poll キーワードは、ホストでブラウズ（ポーリング）が可能であるものの、トラップの送信はできないことを指定します。

community キーワードは、NMS からの要求に対して、または NMS に送信されるトラップを生成するときに、デフォルト以外のストリングが必要であることを指定します。このキーワードは、SNMP バージョン 1 または 2c でのみ使用できます。*community-string* 引数には、通知または NMS からの要求で送信されるコミュニティ ストリングを指定します。コミュニティ ストリングはパスワードのような役割を果たします。このコミュニティ ストリングは最大 32 文字です。

version キーワードは、トラップの送信と要求の受け入れ（ポーリング）に使用する SNMP 通知のバージョン（バージョン 1、2c、または 3）を設定します。デフォルトのバージョンは 1 です。

username 引数には、SNMP バージョン 3 を使用する場合にユーザーの名前を指定します。

user-list キーワードと *list_name* 引数で、ユーザー リストの名前を指定します。

udp-port *port* のキーワードと引数の組み合わせは、NMS ホストへの SNMP トラップの送信にデフォルト以外のポートを使用する場合に、NMS ホストの UDP ポート番号を設定します。デフォルトの UDP ポートは 162 です。

SNMP モニタリング

次の SNMP モニタリング用のコマンドを参照してください。

- **show running-config snmp-server** [**default**]

  すべての SNMP サーバーのコンフィギュレーション情報を表示します。

- **show running-config snmp-server group**

  SNMP グループのコンフィギュレーション設定を表示します。

- **show running-config snmp-server host**

  リモート ホストに送信されるメッセージと通知を制御するために SNMP によって使用されているコンフィギュレーション設定を表示します。

- **show running-config snmp-server host-group**

  SNMP ホスト グループのコンフィギュレーションを表示します。

- **show running-config snmp-server user**

  SNMP ユーザーベースのコンフィギュレーション設定を表示します。

- **show running-config snmp-server user-list**

  SNMP ユーザー リストのコンフィギュレーションを表示します。

- **show snmp-server engineid**

  設定されている SNMP エンジンの ID を表示します。

- **show snmp-server group**

  設定されている SNMP グループの名前を表示します。コミュニティ ストリングがすでに設定されている場合、デフォルトでは 2 つの別のグループが出力に表示されます。この動作は通常のものです。

- **show snmp-server statistics**

  SNMP サーバーの設定済み特性を表示します。すべての SNMP カウンタをゼロにリセットするには、**clear snmp-server statistics** コマンドを使用します。

- **show snmp-server user**

  ユーザーの設定済み特性を表示します。

例

次の例は、SNMP サーバーの統計情報を表示する方法を示しています。

```
ciscoasa(config)# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

次の例は、SNMP サーバーの実行コンフィギュレーションを表示する方法を示しています。

```
ciscoasa(config)# show running-config snmp-server
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
```

SNMP の例

次の項では、すべての SNMP バージョンの参考として使用できる例を示します。

SNMP バージョン 1 および 2c

次の例は、どのホストにも SNMP syslog 要求を送信せずに、ASA が内部インターフェイスでホスト 192.0.2.5 からの SNMP 要求を受信する方法を示しています。

```
ciscoasa(config)# snmp-server host 192.0.2.5
ciscoasa(config)# snmp-server location building 42
ciscoasa(config)# snmp-server contact EmployeeA
ciscoasa(config)# snmp-server community ohwhatakeyisthee
```

SNMP バージョン 3

次の例は、ASA が SNMP バージョン 3 のセキュリティ モデルを使用して SNMP 要求を受信する方法を示しています。このモデルでは、グループ、ユーザー、ホストという一定の順序で設定する必要があります。

```
ciscoasa(config)# snmp-server group v3 vpn-group priv
ciscoasa(config)# snmp-server user admin vpn group v3 auth sha letmein priv 3des cisco123
ciscoasa(config)# snmp-server host mgmt 10.0.0.1 version 3 priv admin
```

SNMP の履歴

表 *70 : SNMP* の履歴

機能名	バージョン	説明
SNMP バージョン 1 および 2c	7.0(1)	クリアテキストのコミュニティストリングを使用した SNMP サーバーと SNMP エージェント間のデータ送信によって、ASA ネットワークのモニタリングおよびイベント情報を提供します。
SNMP バージョン 3	8.2(1)	3DES または AES 暗号化、およびサポートされているセキュリティ モデルの中で最もセキュアな形式である SNMP バージョン 3 のサポートを提供します。このバージョンでは、USM を使用して、ユーザー、グループ、ホスト、および認証の特性を設定できます。さらに、このバージョンでは、エージェントと MIB オブジェクトへのアクセス コントロールが許可され、追加の MIB サポートが含まれます。 次のコマンドが導入または変更されました。**show snmp-server engineid**、**show snmp-server group**、**show snmp-server user**、**snmp-server group**, **snmp-server user**、**snmp-server host**
パスワードの暗号化	8.3(1)	パスワードの暗号化がサポートされます。 **snmp-server community**、**snmp-server host** コマンドが変更されました。

機能名	バージョン	説明
SNMP トラップと MIB	8.4(1)	追加のキーワードとして、**connection-limit-reached**、**cpu threshold rising**、**entity cpu-temperature**、**entity fan-failure**、**entity power-supply**、**ikev2 stop | start**、**interface-threshold**、**memory-threshold**、**nat packet-discard**、**warmstart** をサポートします。 entPhysicalTable によって、センサー、ファン、電源、および関連コンポーネントのエントリがレポートされます。 追加の MIB として、CISCO-ENTITY-SENSOR-EXT-MIB、CISCO-ENTITY-FRU-CONTROL-MIB、CISCO-PROCESS-MIB、CISCO-ENHANCED-MEMPOOL-MIB、CISCO-L4L7MODULE-RESOURCE-LIMIT-MIB、DISMAN-EVENT-MIB、DISMAN-EXPRESSION-MIB、ENTITY-SENSOR-MIB、NAT-MIB をサポートします。 さらに ceSensorExtThresholdNotification、clrResourceLimitReached、cpmCPURisingThreshold、mteTriggerFired、natPacketDiscard、warmStart トラップをサポートしています。 **snmp cpu threshold rising**、**snmp interface threshold**、**snmp-server enable traps** コマンドが導入または変更されました。
IF-MIB ifAlias OID のサポート	8.2(5) / 8.4(2)	ASA は、ifAlias OID をサポートするようになりました。IF-MIB をブラウズする際、fAlias OID はインターフェイスの記述に設定済みの値に設定されます。

機能名	バージョン	説明
ASA サービス モジュール（ASASM）	8.5(1)	ASASM は、次を除く 8.4(1) にあるすべての MIB およびトラップをサポートします。 8.5(1) のサポートされていない MIB： • CISCO-ENTITY-SENSOR-EXT-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • ENTITY-SENSOR-MIB（entPhySensorTable グループのオブジェクトだけがサポートされます）。 • DISMAN-EXPRESSION-MIB（expExpressionTable、expObjectTable、および expValueTable グループのオブジェクトだけがサポートされます）。 8.5(1) のサポートされていないトラップ： • ceSensorExtThresholdNotification（CISCO-ENTITY-SENSOR-EXT-MIB）。このトラップは、電源障害、ファン障害および高 CPU 温度のイベントだけに使用されます。 • InterfacesBandwidthUtilization。
SNMP トラップ	8.6(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X の追加のキーワードとして、**entity power-supply-presence**、**entity power-supply-failure**、**entity chassis-temperature**、**entity chassis-fan-failure, entity power-supply-temperature** をサポートします。 次のコマンドが変更されました。**snmp-server enable traps**。
VPN-related MIB	9.0(1)	CISCO-IPSEC-FLOW-MONITOR-MIB.my MIB の更新バージョンが、次世代の暗号化機能をサポートするために実装されました。 ASASM では、次の MIB が有効になりました。 • ALTIGA-GLOBAL-REG.my • ALTIGA-LBSSF-STATS-MIB.my • ALTIGA-MIB.my • ALTIGA-SSL-STATS-MIB.my • CISCO-IPSEC-FLOW-MONITOR-MIB.my • CISCO-REMOTE-ACCESS-MONITOR-MIB.my
Cisco TrustSec MIB	9.0(1)	CISCO-TRUSTSEC-SXP-MIB のサポートが追加されました。

機能名	バージョン	説明
SNMP OID	9.1(1)	ASA 5512-X、5515-X、5525-X、5545-X、および 5555-X をサポートするために 5 つの新しい SNMP 物理ベンダー タイプ OID が追加されました。
NAT MIB	9.1(2)	cnatAddrBindNumberOfEntries および cnatAddrBindSessionCount OID が、xlate_count および max_xlate_count エントリをサポートするようになりました。これは、**show xlate count** コマンドを使用したポーリングの許可と同等です。
SNMP のホスト、ホスト グループ、ユーザー リスト	9.1(5)	最大 4000 個までホストを追加できるようになりました。サポートされるアクティブなポーリング先の数は 128 個です。ホスト グループとして追加する個々のホストを示すためにネットワーク オブジェクトを指定できます。1 つのホストに複数のユーザを関連付けることができます。 **snmp-server host-group**、**snmp-server user-list**、**show running-config snmp-server**、**clear configure snmp-server** の各コマンドが導入または変更されました。
SNMP メッセージのサイズ	9.2(1)	SNMP で送信できるメッセージのサイズが 1472 バイトまでに増えました。
SNMP の MIB および OID	9.2(1)	ASA は、cpmCPUTotal5minRev OID をサポートするようになりました。 SNMP の sysObjectID OID および entPhysicalVendorType OID に、新しい製品として ASA 仮想 が追加されました。 新しいプラットフォームである ASA 仮想 をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 VPN 共有ライセンスの使用状況をモニターするための新しい SNMP MIB が追加されました。
SNMP の MIB および OID	9.3(1)	ASASM 用に CISCO-REMOTE-ACCESS-MONITOR-MIB（OID 1.3.6.1.4.1.9.9.392）のサポートが追加されました。

機能名	バージョン	説明
SNMP の MIB およびトラップ	9.3(2)	ASA 5506-X をサポートするように CISCO-PRODUCTS-MIB および CISCO-ENTITY-VENDORTYPE-OID-MIB が更新されました。 SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506-X が追加されました。 ASA で CISCO-CONFIG-MAN-MIB がサポートされるようになりました。以下が可能です。 • 特定のコンフィギュレーションについて入力されたコマンドを確認する。 • 実行コンフィギュレーションに変更が発生したときに NMS に通知する。 • 実行コンフィギュレーションが最後に変更または保存されたときのタイム スタンプを追跡する。 • 端末の詳細やコマンドのソースなど、コマンドに対するその他の変更を追跡する。 次のコマンドが変更されました。**snmp-server enable traps**。
SNMP の MIB およびトラップ	9.4(1)	SNMP の sysObjectID OID および entPhysicalVendorType OID のテーブルに、新しい製品として ASA 5506W-X、ASA 5506H-X、ASA 5508-X、および ASA 5516-X が追加されました。
コンテキストごとに無制限の SNMP サーバー トラップ ホスト	9.4(1)	ASA は、コンテキストごとに無制限の SNMP サーバー トラップ ホストをサポートします。**show snmp-server host** コマンドの出力には ASA をポーリングしているアクティブなホストと、静的に設定されたホストのみが表示されます。 **show snmp-server host** コマンドが変更されました。
ISA 3000 のサポートが追加されました。	9.4(1.225)	ISA 3000 製品ファミリーで SNMP がサポートされました。このプラットフォームに新しい OID が追加されました。**snmp-server enable traps entity** コマンドが変更され、新しい変数 *l1-bypass-status* が追加されました。これにより、ハードウェアのバイパス状態の変更が可能になりました。 次のコマンドが変更されました。**snmp-server enable traps entity**

機能名	バージョン	説明
CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable のサポート	9.6(1)	CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable がサポートされました。これは、管理型システムのすべての物理エンティティのメモリプール モニタリング エントリのテーブルです。 （注） CISCO-ENHANCED-MEMPOOL-MIB は 64 ビットのカウンタを使用して、プラットフォーム上の 4 GB 以上のメモリのレポーティングをサポートします。
Precision Time Protocol（PTP）の E2E トランスペアレント クロック モード MIB のサポート	9.7(1)	E2E トランスペアレント クロック モードに対応する MIB がサポートされます。 （注） SNMP の bulkget、getnext、walk 機能のみがサポートされています。
SNMP over IPv6	9.9(2)	ASA は、IPv6 経由での SNMP サーバーとの通信、IPv6 経由でのクエリとトラップの実行許可、既存の MIB に対する IPv6 アドレスのサポートなど、SNMP over IPv6 をサポートするようになりました。RFC 8096 で説明されているように、次の新しい SNMP IPv6 MIB オブジェクトが追加されました。 • ipv6InterfaceTable（OID：1.3.6.1.2.1.4.30）：インターフェイスごとの IPv6 固有の情報が含まれています。 • ipAddressPrefixTable（OID：1.3.6.1.2.1.4.32）：このエンティティによって学習されたすべてのプレフィックスが含まれています。 • ipAddressTable（OID：1.3.6.1.2.1.4.34）：エンティティのインターフェイスに関連するアドレッシング情報が含まれています。 • ipNetToPhysicalTable（OID：1.3.6.1.2.1.4.35）：IP アドレスから物理アドレスへのマッピングが含まれています。 新規または変更されたコマンド：**snmp-server host** （注） **snmp-server host-group** コマンドは IPv6 をサポートしていません。
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.10(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 新規/変更されたコマンド：**snmp-server enable oid**

機能名	バージョン	説明
SNMP ウォーク操作中の空きメモリおよび使用済みメモリの統計情報の結果を有効または無効にするためのサポート	9.12(1)	CPU リソースが過剰に使用されないようにするには、SNMP ウォーク操作によって収集された空きメモリと使用済みメモリの統計情報のクエリを有効または無効にすることができます。 変更されたコマンドはありません。
SNMPv3 認証	9.14(1)	ユーザー認証に SHA-256 HMAC を使用できるようになりました。 新規/変更されたコマンド：**snmp-server user**
9.14(1) 以降のフェールオーバーペアの場合、ASA は SNMP クライアントエンジンデータをピアと共有しません。	9.14(1)	ASA は、SNMP クライアントのエンジンデータをピアと共有しなくなりました。
サイト間 VPN 経由の SNMP ポーリング	9.14(2)	サイト間 VPN 経由のセキュアな SNMP ポーリングの場合、VPN 設定の一部として外部インターフェイスの IP アドレスを暗号マップアクセスリストに含めます。
CISCO-MEMORY-POOL-MIB OID のサポートの廃止	9.15(1)	64 ビットカウンタを使用するシステムの CISCO-MEMORY-POOL-MIB OID（ciscoMemoryPoolUsed、ciscoMemoryPoolFree）が廃止されました。 64 ビットカウンタを使用するシステムのメモリ プール モニタリング エントリは、CISCO-ENHANCED-MEMPOOL-MIB の cempMemPoolTable で提供されます。
SNMPv3 認証	9.16(1)	ユーザー認証に SHA-224 および SHA-384 を使用できるようになりました。ユーザー認証に MD5 を使用できなくなりました。 暗号化に DES を使用できなくなりました。 新規/変更されたコマンド：**snmp-server user**
SNMP over IPv6	9.17(1)	**snmp-server host-group** コマンドは、IPv6 ホスト、範囲、およびサブネットオブジェクトをサポートするようになりました。
SNMP のループバック インターフェイス サポート	9.18(2)	ループバック インターフェイスを追加して、SNMP に使用できるようになりました。 新規/変更されたコマンド：**interface loopback**、**snmp-server host**
SNMP の MIB およびトラップ	9.20(1)	Cisco Secure Firewall 4200 モデルデバイス（FPR4215、FPR4225、FPR4245）が、SNMP の sysObjectID OID および entPhysicalVendorType OID の表に、新しい製品として追加されました。これらの Cisco Secure Firewall 4200 シリーズデバイスの 2 つの EPM カード（4X200G および 2X100G）の SNMP サポートが追加されました。

第 48 章

Cisco Success Network とテレメトリデータ

この章では、Cisco Success Network についてと、Cisco Success Network を ASA で有効にする方法について説明します。また、Security Service Engine（SSE）クラウドに送信されるテレメトリデータポイントも示します。

- Cisco Success Network について （1733 ページ）
- Cisco Success Networkの有効化または無効化 （1734 ページ）
- ASA テレメトリデータの表示 （1735 ページ）
- Cisco Success Network - テレメトリデータ （1736 ページ）
- デバッグテレメトリデータ （1742 ページ）

Cisco Success Network について

Cisco Success Network は、ASA の使用率情報と統計情報をストリーミングする Security Service Exchange（SSE）クラウドとのセキュアな接続を確立するユーザーが有効なクラウドサービスです。テレメトリをストリーミングすることによって、ASA使用率とその他の詳細を構造化形式（JSON）でリモートの管理ステーションに送信するメカニズムが提供されるため、次のメリットが得られます。

- 製品に利用可能な、追加のテクニカルサポートサービスとモニタリングについて通知します。
- シスコ製品の改善に役立ちます。

デフォルトでは、Cisco Success Network は、（ブレードレベルで）ASA デバイスをホストする Firepower 4100/9300 プラットフォームで有効になっています。ただし、テレメトリデータを送信するには、シャーシレベルで FXOS の設定を有効にするか（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』を参照）、シャーシマネージャで Cisco Success Network を有効にする必要があります（『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide』を参照）。

ASAデバイスで収集されるテレメトリデータには、CPU、メモリ、ディスク、または帯域幅、ライセンスの使用状況、設定されている機能リスト、クラスタ/フェールオーバー情報などが含まれます。「Cisco Success Network - テレメトリデータ （1736 ページ）」を参照してください。

サポートされるプラットフォームと必要な設定

- ASA バージョン 9.13.1 以降を実行している FP9300/4100 プラットフォームでサポートされます。
- クラウドに接続するには、FXOS バージョン2.7.1 以降が必要です。
- FXOS の SSE コネクタは、SSE クラウドに接続されている必要があります。この接続は、スマートライセンスバックエンドでスマートライセンスを有効にして登録することによって確立されます。FXOS の SSE コネクタは、スマートライセンスを登録することによって、SSE クラウドに自動的に登録されます。
- Cisco Success Network の設定は、シャーシマネージャで有効にする必要があります。
- テレメトリ設定は、ASA で有効にする必要があります。

ASA テレメトリデータが SSE クラウドに到達する仕組み

Cisco Success Network は、ASA 9.13(1) の Firepower 4100/9300 プラットフォームでデフォルトでサポートされています。FXOS サービスマネージャは、そのプラットフォームで実行されている ASA アプリケーションにテレメトリ要求を毎日送信します。ASA エンジンは、設定および接続ステータスに基づいて、スタンドアロンモードまたはクラスタモードのいずれかでテレメトリデータを FXOS に送信します。つまり、テレメトリのサポートが ASA で有効になっていて、SSE コネクタのステータスが接続済みの場合、テレメトリスレッドは、システムやプラットフォーム、またはデバイス API、ライセンス API、CPU API、メモリ API、ディスク API、Smart Call Home 機能の API などさまざまなソースから必要な情報を取得します。ただし、テレメトリのサポートが ASA で無効になっているか、または SSE コネクタのステータスが切断である場合、ASA は、テレメトリの設定ステータスを示す応答を FXOS（appAgent）に送信し、テレメトリデータは送信しません。

FXOS では、1 つの SSE コネクタインスタンスのみが実行されます。これが SSE クラウドに登録されると、1 つのデバイスと見なされ、SSE インフラでは FXOS に 1 つのデバイス ID が割り当てられます。SSE コネクタを介して送信されるテレメトリレポートは、同じデバイス ID で分類されます。したがって、FXOS は、各 ASA からのテレメトリレポートを 1 つのレポートに集約します。スマート ライセンス アカウント情報などのその他の内容が、レポートに追加されます。その後、FXOS は、最終的なレポートを SSE クラウドに送信します。テレメトリデータは、SSE データ交換（DEX）に保存され、シスコの IT チームで使用できるようになります。

Cisco Success Networkの有効化または無効化

始める前に

- FXOS でスマートライセンスを有効にして登録します。
- シャーシレベルで FXOS のテレメトリサポートを有効にするか（『Cisco Firepower 4100/9300 FXOS CLI Configuration Guide』』を参照）、シャーシマネージャで Cisco Success Network

を有効にします（『Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide』を参照）。

手順

ASA でテレメトリサービスを有効にするには、グローバルコンフィギュレーションモードで、次のコマンドを入力します。テレメトリサービスを無効にするには、このコマンドの no 形式を使用します。

[no] service telemetry

例：

```
ciscoasa(config)# service telemetry
ciscoasa(config)# no service telemetry
```

次のタスク

- テレメトリの設定とアクティビティのログまたはテレメトリデータを表示できます。「ASA テレメトリデータの表示 （1735 ページ）」を参照してください
- テレメトリデータおよびデータフィールドのサンプルを表示するには、次を参照してください。 Cisco Success Network - テレメトリデータ （1736 ページ）

ASA テレメトリデータの表示

始める前に

- ASA でテレメトリサービスを有効にします。「Cisco Success Networkの有効化または無効化 （1734 ページ）」を参照してください

手順

ネットワークの ASA デバイスのテレメトリデータを表示するには、特権 EXEC モードで次のコマンドを入力します。

show telemetry [history | last-report | sample]

例：

```
ciscoasa# show telemetry history
17:38:24 PDT Apr 30 2019: Telemetry support on the blade: enabled
17:38:03 PDT Apr 30 2019: Telemetry support on the blade: disabled
11:49:47 PDT Apr 29 2019: msgId 3. Telemetry support on the chassis: disabled
```

```
11:48:47 PDT Apr 29 2019: msgId 2. Telemetry request from the chassis received. SSE
connector status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent
11:47:47 PDT Apr 29 2019: msgId 1. Telemetry request from the chassis received. SSE
connector status: enabled. Telemetry config on the blade: enabled. Telemetry data Sent.
```

テレメトリの設定とアクティビティに関連する過去 100 のイベントを表示するには **history**、FXOS に送信された最新のテレメトリデータを JSON 形式で表示するには **last-report**、即座に生成されたテレメトリデータを JSON 形式で表示するには **sample** を使用します。

Cisco Success Network - テレメトリデータ

Cisco Success Network は、Firepower 4100/9300 プラットフォームでデフォルトでサポートされています。FXOS サービスマネージャは、このプラットフォームで実行されている ASA エンジンにテレメトリ要求を毎日送信します。ASAエンジンは、要求を受信すると、接続ステータスに基づいて、スタンドアロンモードまたはクラスタモードのいずれかでテレメトリデータを FXOS に送信します。次の表に、テレメトリデータポイント、その説明、およびサンプル値を示します。

表 *71 : Device Info*

データ ポイント	説明	値の例
Device Model	デバイス モデル	Cisco Adaptive Security Appliance
シリアル番号	デバイスのシリアル番号	FCH183771EZ
System Time	システムの動作期間	11658000
プラットフォーム	ハードウェア	FPR9K-SM-24
構成モード	展開タイプ	Native
セキュリティ コンテキスト モード	単一/複数	シングル

表 *72 :* バージョン情報

データ ポイント	説明	値の例
バージョングローバル変数	ASA のバージョン	9.13.1.5
デバイスマネージャのバージョン	デバイスマネージャのバージョン	7.10.1

表 *73*：ライセンス情報

データ ポイント	説明	値の例
スマートライセンスのグローバル変数	有効化されているライセンス	regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION、1.0_555507e9-85f8-4e41-96de-860b59f10bbe

表 *74*：プラットフォームに関する情報

データ ポイント	説明	値の例
CPU	過去 5 分間の CPU 使用率	fiveSecondsPercentage：0.2000000、 oneMinutePercentage：0、 fiveMinutesPercentage：0
メモリ	メモリ使用量	freeMemoryInBytes：225854966384、 usedMemoryInBytes：17798281616、 totalMemoryInBytes：243653248000
ディスク	ディスク使用量	freeGB：21.237285、 usedGB：0.238805、 totalGB：21.476090
Bandwidth	帯域幅の使用方法	receivedPktsPerSec：3、 receivedBytesPerSec：212、 transmittedPktsPerSec：3、 transmittedBytesPerSec：399

表 *75*：機能情報

データ ポイント	説明	値の例
機能リスト	有効な機能リスト	name：cluster status：enabled

表 *76 :* クラスタ情報

データ ポイント	説明	値の例
クラスタ情報	クラスタ情報	clusterGroupName：ssp-cluster interfaceMode：spanned unitName：unit-3-3 unitState：SLAVE otherMembers： items： memberName：unit-2-1 memberState：MASTER memberSerialNum：FCH183771BA

表 *77 :* フェールオーバー情報

データ ポイント	説明	値の例
フェールオーバー	フェールオーバー情報	myRole：Primary、 peerRole：Secondary、 myState：active、 peerState：standby、 peerSerialNum：FCH183770EZ

表 *78 :* ログイン情報

データ ポイント	説明	値の例
ログイン	ログイン履歴	loginTimes：2 times in last 2 days、 lastSuccessfulLogin：12:25:36 PDT Mar 11 2019

ASA テレメトリデータの例

次に、JSON 形式で ASA から送信されるテレメトリデータの例を示します。サービスマネージャは、この入力を受信すると、すべての ASA のデータを集約し、SSE コネクタに送信する前に必要なヘッダー/フィールドを追加します。ヘッダー/フィールドには、“version”、“metadata”、“payload”（“recordedAt”、“recordType”、 “recordVersion” 、および ASA テレメトリ

データの "smartLicenseProductInstanceIdentifier"、"smartLicenseVirtualAccountName" などを含む）があります。


```
{
  "version": "1.0",
  "metadata": {
    "topic": "ASA.telemetry",
    "contentType": "application/json"
  },
  "payload": {
    "recordType": "CST_ASA",
    "recordVersion": "1.0",
    "recordedAt": 1557363423705,
    "SSP": {
      "SSPdeviceInfo": {
        "deviceModel": "Cisco Firepower FP9300 Security Appliance",
        "serialNumber": "JMX2235L01J",
        "smartLicenseProductInstanceIdentifier": "f85a5bb0-xxxx-xxxx-xxxx-xxxxxxxxx",
        "smartLicenseVirtualAccountName": "SSP-general",
        "systemUptime": 198599,
        "udiProductIdentifier": "FPR-C9300-AC"
      },
      "versions": {
        "items": [
          {
            "type": "package_version",
            "version": "92.7(1.342g)"
          }
        ]
      }
    },
    "asaDevices": {
      "items": [
        {
    "deviceInfo": {
        "deviceModel": "Cisco Adaptive Security Appliance",
        "serialNumber": "AANNNXXX",
        "systemUptime": 285,
        "udiProductIdentifier": "FPR9K-SM-36",
        "deploymentType": "Native",
        "securityContextMode": "Single"
    },
    "versions": {
        "items": [
            {
                "type": "asa_version",
                "version": "201.4(1)82"
            },
            {
                "type": "device_mgr_version",
                "version": "7.12(1)44"
            }
        ]
    },
    "licenseActivated": {
        "items": [
            {
                "type": "Strong encryption",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-STRONG-ENCRYPTION,1.0_xxxxxxx-xxxx-xxxx-96de-860b59f10bbe",

                "count": 1
            },
            {
```

```
                "type": "Carrier",
                "tag":
"regid.2015-01.com.cisco.ASA-SSP-MOBILE-SP,1.0_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx",
                "count": 1
            }
        ]
    },
    "CPUUsage": {
        "fiveSecondsPercentage": 0,
        "oneMinutePercentage": 0,
        "fiveMinutesPercentage": 0
    },
    "memoryUsage": {
        "freeMemoryInBytes": 99545662064,
        "usedMemoryInBytes": 20545378704,
        "totalMemoryInBytes": 120091040768
    },
    "diskUsage": {
        "freeGB": 21.237027,
        "usedGB": 0.239063,
        "totalGB": 21.476090
    },
    "bandwidthUsage": {
        "receivedPktsPerSec": 3,
        "receivedBytesPerSec": 268,
        "transmittedPktsPerSec": 4,
        "transmittedBytesPerSec": 461
    },
    "featureStatus": {
        "items": [
            {
                "name": "call-home",
                "status": "enabled"
            },
            {
                "name": "cluster",
                "status": "enabled"
            },
            {
                "name": "firewall_user_authentication",
                "status": "enabled"
            },
            {
                "name": "inspection-dns",
                "status": "enabled"
            },
            {
                "name": "inspection-esmtp",
                "status": "enabled"
            },
            {
                "name": "inspection-ftp",
                "status": "enabled"
            },
            {
                "name": "inspection-netbios",
                "status": "enabled"
            },
            {
                "name": "inspection-rsh",
                "status": "enabled"
            },
            {
                "name": "inspection-sip",
```

```
                "status": "enabled"
            },
            {
                "name": "inspection-sqlnet",
                "status": "enabled"
            },
            {
                "name": "inspection-sunrpc",
                "status": "enabled"
            },
            {
                "name": "inspection-tftp",
                "status": "enabled"
            },
            {
                "name": "inspection-xdmcp",
                "status": "enabled"
            },
            {
                "name": "logging-console",
                "status": "informational"
            },
            {
                "name": "management-mode",
                "status": "normal"
            },
            {
                "name": "sctp-engine",
                "status": "enabled"
            },
            {
                "name": "threat_detection_basic_threat",
                "status": "enabled"
            },
            {
                "name": "threat_detection_stat_access_list",
                "status": "enabled"
            },
            {
                "name": "webvpn-activex-relay",
                "status": "enabled"
            },
            {
                "name": "webvpn-dtls",
                "status": "enabled"
            }
        ]
    },
    "clusterInfo": {
        "clusterGroupName": "ssp-cluster",
        "interfaceMode": "spanned",
        "unitName": "unit-3-3",
        "unitState": "SLAVE",
        "otherMembers": {
            "items": [
                {
                    "memberName": "unit-2-1",
                    "memberState": "MASTER",
                    "memberSerialNum": "FCH183771BA"
                },
                {
                    "memberName": "unit-2-3",
                    "memberState": "SLAVE",
                    "memberSerialNum": "FLM1949C6JR"
```

```
                },
                {
                    "memberName": "unit-2-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-2",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                },
                {
                    "memberName": "unit-3-1",
                    "memberState": "SLAVE",
                    "memberSerialNum": "xxxxxxxx"
                }
            ]
        }
    },
    "loginHistory": {
        "loginTimes": "1 times in last 1 days",
        "lastSuccessfulLogin": "12:25:36 PDT Mar 11 2019"
    }
}
```


デバッグテレメトリデータ

始める前に

- ASA でテレメトリサービスを有効にします。「Cisco Success Networkの有効化または無効化 （1734 ページ）」を参照してください

手順

ステップ 1 テレメトリに関連するデバッグメッセージを表示するには、特権EXECモードで次のコマンドを使用してデバッグテレメトリサービスを有効にします。

debug telemetry<*1-255*>

例：

```
asa# debug telemetry ?
   <1-255>  Specify an optional debug level (default is 1)
```

デバッグテレメトリサービスを無効にするには、このコマンドの **no** 形式を使用します。

ステップ 2 選択したデバッグレベルのデバッグテレメトリメッセージを表示するには、次のコマンドを使用します。

show debug telemetry

例：

```
asa# show debug telemetry
debug telemetry  enabled at level 1

[telemetry_collect_device_info]: telemetry successfully collected device info
[telemetry_collect_versions]: telemetry successfully collected version info
[telemetry_collect_licenses]: no smart-lic entitlement in use
[telemetry_collect_cpu]: telemetry successfully collected cpu info
[telemetry_collect_memory]: telemetry successfully collected mem info
[telemetry_collect_disk_usage]: telemetry successfully collected disk info
[telemetry_collect_bandwidth_usage]: telemetry successfully collected bandwidth usage
info
[telemetry_collect_enabled_feature_status]: telemetry successfully collected enabled
feature info
[telemetry_collect_cluster_info]: telemetry successfully collected cluster info
[telemetry_collect_failover_info]: ha is not configured
[telemetry_get_user_login_hist]: telemetry successfully collected login history
[telemetry_collect_blocks]: telemetry successfully collected block info
[telemetry_collect_perfmon]: telemetry successfully collected perfmon stats
[telemetry_collect_resource_usage]: telemetry successfully collected res usage
[telemetry_collect_process_cpu_usage]: telemetry successfully collected res usage
[telemetry_collect_crashinfo]: telemetry successfully collected crashinfo
[telemetry_collect]: the serialized string is generated
[telemetry_collect]: successfully allocated mem for serialized string
[telemetry_history_add_record]: telemetry has a new history record: 16:23:29 PDT Oct 22
 2019: Telemetry support on the blade: enabled
[telemetry_history_add_record]: telemetry has a new history record: 16:24:01 PDT Oct 22
 2019: Telemetry support on the blade: disabled
```

第 49 章

Anonymous Reporting および Smart Call Home

この章では、Anonymous Reporting および Smart Call Home サービスを設定する方法について説明します。

- Anonymous Reporting について （1745 ページ）
- Smart Call Home の概要 （1746 ページ）
- Anonymous Reporting および Smart Call Home のガイドライン （1753 ページ）
- Anonymous Reporting および Smart Call Home の設定 （1754 ページ）
- Anonymous Reporting および Smart Call Home のモニタリング （1767 ページ）
- Smart Call Home の例 （1768 ページ）
- Anonymous Reporting および Smart Call Home の履歴 （1769 ページ）

Anonymous Reporting について

Anonymous Reporting をイネーブルにして ASA プラットフォームを強化することができます。Anonymous Reporting により、エラーと正常性に関する最小限の情報をデバイスからシスコに安全に送信できます。この機能をイネーブルにした場合、お客様のアイデンティティは匿名のままとなり、識別情報は送信されません。

Anonymous Reporting をイネーブルにすると、トラスト ポイントが作成され、証明書がインストールされます。CA 証明書は、ASA でメッセージを安全に送信できるように、Smart Call Home Web サーバー上のサーバー証明書を検証して、HTTPS セッションを形成するために必要です。ソフトウェアに事前定義済みの証明書が、シスコによってインポートされます。Anonymous Reporting をイネーブルにする場合は、ハードコードされたトラスト ポイント名の _SmartCallHome_ServerCA で証明書が ASA にインストールされます。Anonymous Reporting をイネーブルにすると、このトラスト ポイントが作成され、適切な証明書がインストールされて、このアクションに関するメッセージが表示されます。これで、証明書が設定の中に存在するようになります。

Anonymous Reporting をイネーブルにしたときに、適切な証明書がすでに設定に存在する場合、トラスト ポイントは作成されず、証明書はインストールされません。

（注） Anonymous Reporting をイネーブルにすると、指定されたデータをシスコまたはシスコの代わりに運用するベンダー（米国以外の国を含む）に転送することに同意することになります。シスコでは、すべてのお客様のプライバシーを保護しています。シスコの個人情報の取り扱いに関する詳細については、次の URL にあるシスコのプライバシー声明を参照してください。
http://www.cisco.com/web/siteassets/legal/privacy.html

ASA はバックグラウンドで Smart Call Home 匿名レポートを設定するときに、Call Home サーバー証明書を発行する CA の証明書を含むトラストポイントを自動生成します。ASA は、サーバー証明書の発行階層が変更された場合に証明書の検証をサポートするようになりました。カスタマーが証明書階層を変更する必要はありません。また、手動介入なしに ASA が証明書階層を更新できるよう、トラストプールの証明書を自動的にインポートすることもできます。

ASA 9.14（2.14）をアップグレードすると、トラストポイントの設定が CallHome_ServerCA から CallHome_ServerCA2 に自動的に変更されます。

DNS 要件

ASA が Cisco Smart Call Home サーバーに到達してシスコにメッセージを送信できるように DNS サーバーを正しく設定する必要があります。ASA をプライベート ネットワークに配置し、パブリック ネットワークにはアクセスできないようにすることが可能なため、シスコでは DNS 設定を検証し、必要な場合には次の手順を実行して、ユーザーの代わりにこれを設定します。

1. 設定されているすべての DNS サーバーに対して DNS ルックアップを実行します。
2. 最もセキュリティレベルの高いインターフェイスで DHCPINFORM メッセージを送信して、DHCP サーバーから DNS サーバーを取得します。
3. ルックアップにシスコの DNS サーバーを使用します。
4. tools.cisco.com に対してランダムに静的 IP アドレスを使用します。

これらの作業は、現在の設定を変更せずに実行されます。（たとえば、DHCP から学習された DNS サーバーは設定には追加されません）。

設定されている DNS サーバーがなく、ASA が Cisco Smart Call Home サーバーに到達できない場合は、各 Smart Call Home メッセージに対して、重大度「warning」の syslog メッセージが生成されます。これは、DNS を適切に設定するようお願いするためです。

syslog メッセージについては、syslog メッセージガイドを参照してください。

Smart Call Home の概要

完全に設定が終わると、Smart Call Home は設置場所での問題を検出し、多くの場合はそのような問題があることにユーザーが気付く前に、シスコにレポートを返すか、別のユーザー定義のチャネル（ユーザー宛の電子メールまたはユーザーに直接など）を使用してレポートを返します。シスコでは、これらの問題の重大度に応じて次のサービスを提供することにより、システ

ムコンフィギュレーションの問題、製品ライフサイクル終了通知の発表、セキュリティ勧告問題などに対応します。

- 継続的モニタリング、リアルタイムの予防的なアラート、および詳細な診断により、問題を迅速に識別する。
- サービス要求が開かれ、すべての診断データが添付された Smart Call Home 通知を使用して、潜在的な問題をユーザーに認識させる。
- Cisco TAC の専門家に自動的に直接アクセスすることにより、重大な問題を迅速に解決する。
- トラブルシューティングに必要な時間を短縮することにより、スタッフ リソースを効率よく使用する。
- Cisco TAC へのサービス リクエストを自動的に生成し（サービス契約がある場合）、適切なサポート チームに提出する。問題解決の時間を短縮する、詳細な診断情報を提供します。

Smart Call Home ポータルを使用すると必要な情報に迅速にアクセスできるため、以下の事項が実現されます。

- すべての Smart Call Home メッセージ、診断、および推奨事項を一箇所で確認する。
- サービス リクエスト ステータスを確認する。
- すべての Smart Call Home 対応デバイスに関する最新のインベントリ情報およびコンフィギュレーション情報を表示する。

アラート グループへの登録

アラート グループは、ASA でサポートされる Smart Call Home アラートの定義済みサブセットです。Smart Call Home アラートにはさまざまなタイプがあり、タイプに応じてさまざまなアラート グループにグループ化されます。各アラート グループは、特定の CLI の出力を報告します。サポートされる Smart Call Home アラート グループは次のとおりです。

- syslog
- diagnostic
- 環境
- インベントリ
- 設定
- 脅威
- snapshot
- telemetry
- テスト

アラート グループの属性

アラート グループには次の属性があります。

- イベントはまず 1 個のアラート グループに登録します。
- 1 個のグループを、複数のイベントに関連付けることができます。
- 個々のアラート グループに登録できます。
- 個々のアラート グループをイネーブルまたはディセーブルにできます。デフォルト設定では、すべてのアラート グループに対してイネーブルです。
- 診断および環境アラート グループは定期的なメッセージのサブスクリプションをサポートします。
- syslog アラート グループは、メッセージ ID ベースのサブスクリプションをサポートします。
- 環境アラート グループの CPU とメモリの使用率のしきい値を設定できます。特定のパラメータが定義済みしきい値を超えると、メッセージが送信されます。しきい値のほとんどは、プラットフォームによって決まっており、変更できません。
- 指定する CLI 出力を送信するようスナップショット アラート グループを設定します。

アラート グループによって Cisco に送信されるメッセージ

メッセージは、定期的に、および ASA がリロードされるたびにシスコに送信されます。これらのメッセージは、アラート グループによって分類されます。

インベントリ アラートは、次のコマンドによる出力で構成されます。

- **show version**：ASA ソフトウェア バージョン、ハードウェア構成、ライセンス キー、および関連するデバイスの稼働時間を表示します。
- **show inventory—**ネットワーキング デバイスにインストールされている各 Cisco 製品のインベントリ情報を取得および表示します。各製品は UDI と呼ばれる一意のデバイス情報で識別されます。UDI は、製品 ID（PID）、バージョン ID（VID）、およびシリアル番号（SN）の 3 つの異なるデータ要素の組み合わせです。
- **show failover state**：フェールオーバー ペアの両方のユニットのフェールオーバー状態を表示します。表示される情報は、ユニットのプライマリまたはセカンダリ ステータス、ユニットのアクティブ/スタンバイ ステータス、最後にレポートされたフェールオーバーの理由などがあります。
- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。

コンフィギュレーション アラートは、次のコマンドによる出力で構成されます。

- **show context**：割り当てられているインターフェイスと設定ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting を有効にしている場合には、すべてのコンテキストのリストを表示します。
- **show call-home registered-module status**：登録されたモジュールのステータスを表示します。システム コンフィギュレーション モードを使用している場合、コマンドによって、コンテキストごとではなく、デバイス全体に基づくシステムモジュールのステータスが表示されます。
- **show running-config**：ASA で現在実行されている設定を表示します。
- **show startup-config**：スタートアップ コンフィギュレーションを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。

診断アラートは、次のコマンドによる出力で構成されます。

- **show failover**：ユニットのフェールオーバー ステータスに関する情報を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show cluster info**：クラスタ情報を表示します。
- **show cluster history**：クラスタの履歴を表示します。
- **show crashinfo**（切り捨て）：予期しないソフトウェアのリロード後に、デバイスは、変更されたクラッシュ情報ファイルをファイルのトレースバック セクションだけを含めて送信します。したがって、ファンクション コール、レジスタ値、およびスタック ダンプだけがシスコに報告されます。
- **show tech-support no-config**：テクニカル サポート アナリストによる診断に使用される情報を表示します。

環境アラートは、次のコマンドによる出力で構成されます。

- **show environment**：シャーシ、ドライバ、ファン、および電源のハードウェア動作ステータスや、温度ステータス、電圧、CPU 使用率などの、ASA システム コンポーネントのシステム環境情報を表示します。
- **show cpu usage**：CPU 使用率情報を表示します。
- **show memory detail**：空きおよび割り当て済みのシステム メモリの詳細情報を表示します。

脅威アラートは、次のコマンドによる出力で構成されます。

- **show threat-detection rate**：脅威検出統計情報を表示します。
- **show threat-detection shun**：現在排除されているホストを表示します。
- **show shun**：排除情報を表示します。

- **show dynamic-filter reports top**：ボットネット トラフィック フィルタによって分類された上位 10 のマルウェア サイト、ポート、および感染ホストのレポートを生成します。

スナップショット アラートは、次のコマンドによる出力で構成されます。

- **show conn count**：アクティブな接続の数を表示します。
- **show asp drop**：高速セキュリティ パスでドロップされたパケットまたは接続を表示します。

テレメトリ アラートは、次のコマンドによる出力で構成されます。

- **show perfmon detail**：ASA パフォーマンスの詳細を表示します。
- **show traffic**：インターフェイスの送受信アクティビティを表示します。
- **show conn count**：アクティブな接続の数を表示します。
- **show vpn-sessiondb summary**：VPN セッションのサマリー情報を表示します。
- **show vpn load-balancing**：VPN ロードバランシングの仮想クラスタ コンフィギュレーションの実行時統計情報を表示します。
- **show local-host | include interface**：ローカル ホストのネットワーク状態を表示します。
- **show memory**：物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
- **show context**：割り当てられているインターフェイスと設定ファイルの URL、設定済みコンテキストの数を表示します。または、システム実行スペースで Anonymous Reporting を有効にしている場合には、すべてのコンテキストのリストを表示します。
- **show access-list | include elements**：アクセス リストのヒット カウンタおよびタイム スタンプ値を表示します。
- **show interface**：インターフェイス統計情報を表示します。
- **show threat-detection statistics protocol**：IP プロトコルの統計情報を表示します。
- **show phone-proxy media-sessions count**：電話プロキシによって保存されている、対応するメディア セッションの数を表示します。
- **show phone-proxy secure-phones count**：データベースに保存されているセキュア モード対応の電話機の数を表示します。
- **show route**：ルーティング テーブルを表示します。
- **show xlate count**：NAT セッション（xlates）の数を表示します。

メッセージ重大度しきい値

特定のアラートグループに宛先プロファイルを登録すると、メッセージの重大度に基づいてアラート グループ メッセージを送信するしきい値を設定できます。宛先プロファイルに指定したしきい値より低い値のメッセージは、宛先に送信されません。

次の表にメッセージの重大度と syslog の重大度のマッピングを示します。

表 *79 :* メッセージの重大度と *syslog* レベルのマッピング

レベル	メメッセージ重大度レベル	Syslog 重大度レベル	説明
9	Catastrophic	該当なし	ネットワーク全体に壊滅的な障害が発生しています。
8	Disaster	該当なし	ネットワークに重大な影響が及びます。
7	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	0	緊急事態。システムが使用不可能な状態。
6	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	1	アラート。クリティカルな状態。ただちに注意が必要。
5	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	2	Critical 重大な状態。
4	指定された CLI キーワードによって決定： **subscribe-to-alert-group** *name of alert group* **severity** *severity level*	3	エラー。軽微な状態。
3	警告	4	警告状態。
2	通知	5	基本的な通知および情報メッセージです。他と関係しない、重要性の低い障害です。
1	標準	6	Information。通常のイベント。通常の状態に戻ることを意味します。

レベル	メメッセージ重大度レベル	Syslog 重大度レベル	説明
0	Debugging	7	デバッグ メッセージ（デフォルト設定）。

サブスクリプション プロファイル

サブスクリプションプロファイルを使用すると宛先受信者と関心のあるグループを関連付けることができます。プロファイルにあるサブスクライブされたグループに登録されているイベントがトリガーされると、イベントに関連付けられたメッセージが設定された受信者に送信されます。サブスクリプション プロファイルには次の属性があります。

- 複数のプロファイルを作成および設定できます。
- 1 個のプロファイルに複数の電子メールまたは HTTPS の受信者を設定できます。
- 1 個のプロファイルで、指定した重大度に複数のグループを登録できます。
- 1 個のプロファイルで、3 種類のメッセージ フォーマット（ショート テキスト、ロング テキスト、XML）をサポートします。
- 特定のプロファイルをイネーブルまたはディセーブルにできます。デフォルトでは、プロファイルはディセーブルです。
- 最大メッセージ サイズを指定できます。デフォルトは 3 MB です。

デフォルト プロファイル「Cisco TAC」が提供されました。デフォルト プロファイルには、事前定義されたモニタ対象グループ（診断、環境、インベントリ、コンフィギュレーション、テレメトリ）のセットと、事前定義された宛先電子メールおよび HTTPS URL があります。デフォルト プロファイルは、Smart Call Home を初めて設定するときに自動的に作成されます。宛先電子メールは callhome@cisco.com で、宛先 URL は https://tools.cisco.com/its/service/oddce/services/DDCEService です。

（注） デフォルト プロファイルの宛先電子メールと宛先 URL は変更できません。

コンフィギュレーション、インベントリ、テレメトリ、またはスナップショット アラート グループに宛先プロファイルを登録すると、アラート グループ メッセージを非同期に、または定期的に指定の時間に受信するよう選択できます。

次の表に、デフォルトのアラート グループと重大度のサブスクリプションおよび期間（該当する場合）のマッピングを示します。

表 *80 :* アラート グループと重大度のサブスクリプションのマッピング

アラート グループ	重大度	Period
設定（Configuration）	Informational	Monthly

アラート グループ	重大度	Period
診断	Informational 以上	該当なし
環境	Notification 以上	該当なし
インベントリ	Informational	Monthly
Snapshot	Informational	該当なし
Syslog	同等の syslog	該当なし
Telemetry	Informational	Daily
Test	N/A	なし
Threat	通知	N/A

Anonymous Reporting および Smart Call Home のガイドライン

この項では、Anonymous Reporting と Smart Call Home を設定する前に考慮する必要のあるガイドラインおよび制限事項について説明します。

Anonymous Reporting のガイドライン

- DNS が設定されていること。
- Anonymous Reporting のメッセージを最初の試行で送信できなかった場合、ASA はメッセージをドロップする前にさらに 2 回試行します。
- Anonymous Reporting は、既存の設定を変更せずに、他の Smart Call Home 設定と共存させることができます。たとえば、Anonymous Reporting をイネーブルにする前に Smart Call Home がディセーブルになっている場合、Anonymous Reporting をイネーブルにした後でも、ディセーブルのままです。
- Anonymous Reporting をイネーブルにしている場合、トラスト ポイントを削除することはできません。また、Anonymous Reporting をディセーブルにした場合、トラスト ポイントはそのまま残ります。Anonymous Reporting がディセーブルの場合は、トラスト ポイントを削除できますが、Anonymous Reporting をディセーブルにしてもトラスト ポイントは削除されません。
- マルチ コンテキスト モード設定を使用している場合は、**dns**、**interface**、**trustpoint** コマンドは管理コンテキストにあり、**call-home** コマンドはシステム コンテキストにあります。
- CA サーバーの自己署名証明書が変更された場合に、Smart Call Home がアクティブな状態を維持できるように、定期的な trustpool バンドルの更新を自動化できます。このトラストプール自動更新機能は、マルチ コンテキストの導入ではサポートされません。

Smart Call Home のガイドライン

- マルチ コンテキスト モードでは、subscribe-to-alert-group snapshot periodic コマンドは、システム コンフィギュレーションから情報を取得するコマンドと、ユーザ コンテキストから情報を取得するコマンドの 2 つのコマンドに分割されます。
- Smart Call Home のバックエンド サーバーは、XML 書式のメッセージのみ受け取ることができます。
- Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタ イベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次のイベントに対してのみ送信されます。
  - ユニットがクラスタに参加したとき
  - ユニットがクラスタから脱退したとき
  - クラスタユニットがクラスタ制御ユニットになったとき
  - クラスタのセカンダリ ユニットが故障したとき

  送信される各メッセージには次の情報が含まれています。
  - アクティブ クラスタのメンバ数
  - クラスタ制御ユニットでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力

Anonymous Reporting および Smart Call Home の設定

Anonymous Reporting は Smart Call Home サービスの一部であり、これを使用すると、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに匿名で送信できます。一方、Smart Call Home サービスは、システム ヘルスのサポートをカスタマイズする機能です。Cisco TAC がお客様のデバイスをモニタして、問題があるときにケースを開くことができるようになります。多くの場合は、お客様がその問題に気付く前に発見できます。

両方のサービスをシステム上で同時に設定できますが、Smart Call Home サービスを設定すれば、Anonymous Reporting と同じ機能に加えて、カスタマイズされたサービスも使用できるようになります。

コンフィギュレーション モードに入ると、次のガイドラインに従って Anonymous Reporting および Smart Call Home サービスをイネーブルにすることを要求するプロンプトが出ます。

- このプロンプトで、[Y]es、[N]o、または [A]sk later を選択できます。[[A]sk later] を選択した場合、7 日後または ASA をリロードしたときに再度通知されます。[[A]sk later] を連続で選択すると、さらに ASA で 7 日ごとに 2 回プロンプトが表示されたのち、[[N]o] という答えだと見なされて再度表示されることはなくなります。

- プロンプトが表示されない場合は、Anonymous Reporting の設定 （1755 ページ）またはSmart Call Home の設定 （1755 ページ）の手順を実行して、Anonymous Reporting または Smart Call Home をイネーブルにすることができます。

Anonymous Reporting の設定

Anonymous Reporting を設定するには、次の手順を実行します。

手順

ステップ 1 Anonymous Reporting 機能をイネーブルにし、新しい匿名のプロファイルを作成します。

call-home reporting anonymous

例：

```
ciscoasa(config)# call-home reporting anonymous
```

このコマンドを入力すると、トラスト ポイントが作成され、シスコの Web サーバーの識別情報を検証するために使用する証明書がインストールされます。

ステップ 2 （オプション）このサーバーへの接続があり、システムがメッセージを送信できることを確認します。

call-home test reporting anonymous

例：

```
ciscoasa(config)# call-home test reporting anonymous

INFO: Sending test message to
https://tools.cisco.com/its/service/oddce/services/DDCEService...

INFO: Succeeded
```

成功またはエラー メッセージは、テスト結果を返します。

Smart Call Home の設定

ASA で Smart Call Home サービスを設定するには、次のタスクを実行します。

手順

ステップ 1 Smart Call Home サービスをイネーブルにします。Smart Call Home のイネーブル化 （1756 ページ）を参照してください。

ステップ 2 Smart Call Home メッセージがサブスクライバに配信される際に通過するメール サーバーを設定します。メール サーバーの設定 （1761 ページ）を参照してください。

ステップ 3 Smart Call Home メッセージの連絡先情報を設定します。顧客連絡先情報の設定 （1760 ページ）を参照してください。

ステップ 4 処理できるイベントの最大レートなどのアラート処理パラメータを定義します。アラート グループ サブスクリプションの設定 （1758 ページ）を参照してください。

ステップ 5 アラート サブスクリプション プロファイルを設定します。宛先プロファイルの設定 （1764 ページ）を参照してください。

個々のアラート サブスクリプション プロファイルによって、次の内容が特定されます。

- シスコの Smart Call Home サーバーや電子メール受信者のリストなど、Smart Call Home メッセージの送信先となるサブスクライバ。
- コンフィギュレーション情報またはインベントリ情報など、受信するアラートの情報カテゴリ。

Smart Call Home のイネーブル化

Smart Call Home をイネーブルにして、Call Home プロファイルをアクティブにするには、次の手順を実行します。

手順

ステップ 1 Smart Call Home サービスをイネーブルにします。

service call-home

例：

```
ciscoasa(config)# service call-home
```

ステップ 2 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call home
```

認証局のトラスト ポイントの宣言および認証

HTTPS 経由で Web サーバーにメッセージを送信するように Smart Call Home が設定されている場合、Web サーバーの証明書または証明書を発行した認証局（CA）の証明書を信頼するように ASA を設定する必要があります。Cisco Smart Call Home 実稼働サーバー証明書は、Verisign によって発行されます。Cisco Smart Call Home Staging サーバーの証明書は Digital Signature Trust Company によって発行されます。

（注） VPN 検証に使用されないために、no client-types および no validation-usage 用のトラスト ポイントを設定する必要があります。

Cisco サーバー セキュリティの証明書を宣言および認証し、Smart Call Home サービス用に Cisco HTTPS サーバーとの通信を確立するには、次の手順を実行します。

手順

ステップ 1 （マルチ コンテキスト モードのみ）管理コンテキストで証明書をインストールします。

changeto context *admincontext*

例：

```
ciscoasa(config)# changeto context contextA
```

ステップ 2 トラスト ポイントを設定し、証明書登録の準備を整えます。

crypto ca trustpoint *trustpoint-name*

例：

```
ciscoasa(config)# crypto ca trustpoint cisco
```

（注）
転送方法として HTTP を使用する場合は、セキュリティ証明書をトラスト ポイント経由でインストールする必要があります。HTTPS には、これが必須です。次の URL で、インストールする指定の証明書を探します。

http://www.cisco.com/en/US/docs/switches/lan/smart_call_home/SCH31_Ch6.html#wp1035380

ステップ 3 証明書登録に、手動でのカットアンドペースト方式を指定します。

enroll terminal

例：

```
ciscoasa(ca-trustpoint)# enroll terminal
```

ステップ 4 指定した CA を認証します。CA の名前は、**crypto ca trustpoint** コマンドで指定したトラストポイント名と一致している必要があります。プロンプトで、セキュリティ証明書のテキストを貼り付けます。

crypto ca authenticate trustpoint

例：

```
ciscoasa(ca-trustpoint)# crypto ca authenticate cisco
```

ステップ 5 セキュリティ証明書のテキストの終わりを指定し、入力されたセキュリティ証明書の受け入れを確認します。

quit

例：

```
ciscoasa(ca-trustpoint)# quit
%Do you accept this certificate [yes/no]:
yes
```

環境およびスナップショット アラート グループの設定

環境およびスナップショット アラート グループを設定するには、次の手順を実行します。

手順

アラート グループ コンフィギュレーション モードを開始します。

alert-group-config {**environment** | **snapshot**}

例：

```
ciscoasa(config)# alert-group-config environment
```

アラート グループ サブスクリプションの設定

宛先プロファイルをアラート グループに登録するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 指定した Smart Call Home アラート グループをイネーブルにします。

alert-group {**all** |**configuration** |**diagnostic** |**environment** |**inventory** |**syslog**}

例：

```
ciscoasa(cfg-call-home)# alert-group syslog
```

すべてのアラート グループをイネーブルにするには、**all** キーワードを使用します。デフォルトでは、すべてのアラート グループがイネーブルになります。

ステップ 3 指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile CiscoTAC-1
```

ステップ 4 使用可能なすべてのアラート グループに登録します。

subscribe-to-alert-group all

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group all
```

ステップ 5 この宛先プロファイルをコンフィギュレーション アラート グループに登録します。

subscribe-to-alert-group configuration periodic {**daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm*}

例：

```
ciscoasa(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
 Wednesday 23:30
```

periodic キーワードを指定すると、定期的に通知するようにコンフィギュレーション アラート グループが設定されます。デフォルトの間隔は daily です。

daily キーワードでは、送信する時刻を 24 時間制の *hh:mm* 形式（例：14:30）で指定します。

weekly キーワードでは、曜日と時刻を *day hh:mm* 形式で指定します。曜日は英語で記述します（例：Monday）。

monthly キーワードでは、1 ～ 31 の日付と時刻を *date hh:mm* 形式で指定します。

顧客連絡先情報の設定

顧客連絡先情報を設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 顧客電話番号を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

phone-number *phone-number-string*

例：

```
ciscoasa(cfg-call-home)# phone-number 8005551122
```

ステップ 3 顧客の住所（自由形式の文字列、最長 255 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

street-address *street-address*

例：

```
ciscoasa(cfg-call-home)# street-address “1234 Any Street, Any city, Any state, 12345”
```

ステップ 4 顧客名（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contact-name *contact-name*

例：

```
ciscoasa(cfg-call-home)# contact-name contactname1234
```

ステップ 5 シスコ カスタマー ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

customer-id *customer-id-string*

例：

```
ciscoasa(cfg-call-home)# customer-id customer1234
```

ステップ 6 顧客サイト ID（最長 64 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

site-id *site-id-string*

例：

```
ciscoasa(cfg-call-home)# site-id site1234
```

ステップ 7 顧客連絡先 ID（最長 128 文字）を指定します。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

contract-id *contract-id-string*

例：

```
ciscoasa(cfg-call-home)# contract-id contract1234
```

例

次に、連絡先情報を設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# contact-email-addr username@example.com
ciscoasa(cfg-call-home)# phone-number 8005551122
ciscoasa(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
ciscoasa(cfg-call-home)# contact-name contactname1234
ciscoasa(cfg-call-home)# customer-id customer1234
ciscoasa(cfg-call-home)# site-id site1234
ciscoasa(cfg-call-home)# contract-id contract1234
```

メール サーバーの設定

メッセージの転送には、最もセキュアなHTTPSを使用することをお勧めします。ただし、Smart Call Home宛ての電子メールを設定し、電子メール メッセージ転送を使用するようメール サーバーを設定できます。

電子メール サーバーを設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 SMTP メール サーバーを指定します。

mail-server*ip-address* **name priority** [**1-100**] [**all**]

例：

```
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 smtp.example.com priority 1
```

最大 5 つのメール サーバーを指定できます。その場合は、コマンドを 5 回実行します。Smart Call Home メッセージの電子メール転送を使用するには、最低 1 つのメール サーバーを設定する必要があります。

番号が小さいほどメール サーバーの優先順位が高くなります。

ip-address 引数には、IPv4 と IPv6 のどちらのメール サーバー アドレスも指定できます。

例

次に、プライマリ メール サーバー（smtp.example.com）および IP アドレス 10.10.1.1 にあるセカンダリ メール サーバーを設定する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# mail-server smtp.example.com priority 1
ciscoasa(cfg-call-home)# mail-server 10.10.1.1 priority 2
ciscoasa(cfg-call-home)# exit
ciscoasa(config)#
```

トラフィック レートの制限の設定

トラフィック レートの制限を設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 Smart Call Home が 1 分間に送信できるメッセージの数を指定します。デフォルト値は、1 分間に 10 のメッセージです。

rate-limit *msg-count*

例：

```
ciscoasa(cfg-call-home)# rate-limit 5
```

Smart Call Home 通信の送信

特定の Smart Call Home 通信を送信するには、次の手順を実行します。

手順

次のいずれかのオプションを選択します。

- オプション 1：プロファイル コンフィギュレーションを使用して、テスト メッセージを送信します。

  call-home test [*test-message*] **profile** *profile-name*

  例：

  ```
  ciscoasa# call-home test [testing123] profile CiscoTAC-1
  ```

- オプション 2：アラート グループ メッセージを 1 つの宛先プロファイルに送信します（指定されている場合）。プロファイルが指定されていない場合は、インベントリ、コンフィギュレーション、スナップショット、またはテレメトリ アラート グループの通知を受け取るように設定されたすべてのプロファイルにメッセージが送信されます。

  call-home send alert-group inventory { | **configuration** | **snapshot** | **telemetry**} [**profile** *profile-name*]

  例：

  ```
  ciscoasa# call-home send alert-group inventory
  ```

- オプション 3：コマンド出力を電子メールアドレスに送信します。指定する CLI コマンドは、どのようなコマンドでもかまいません。これには、すべての登録済みモジュールのコマンドも含まれます。

  call-home send*cli command* [**email** *email*]

例：

```
ciscoasa# call-home send cli destination email username@example.com
```

電子メールアドレスを指定した場合、コマンド出力はそのアドレスに送信されます。電子メール アドレスを指定していない場合、出力は Cisco TAC に送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ログテキスト形式で送信されます。

電子メール アドレスを指定しない場合、または Cisco TAC 電子メール アドレスを指定した場合に限り、サービス番号が必要になります。

宛先プロファイルの設定

電子メールまたは HTTP の宛先プロファイルを設定するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 指定された宛先プロファイルに対するプロファイル コンフィギュレーション モードを開始します。指定された宛先プロファイルが存在しない場合、作成されます。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

最大10個のアクティブプロファイルを作成できます。デフォルトプロファイルは、Cisco TACに報告するように設定されています。Call Home情報を別の場所（たとえば、自社のサーバー）に送信するには、別のプロファイルを設定します。

ステップ 3 宛先、メッセージのサイズ、メッセージの形式、および Smart Call Home メッセージ受信者への転送方法を設定します。デフォルトのメッセージ形式は XML です。デフォルトでイネーブルになっている転送方法は、電子メールです。

destination address { **email** *address* | **http** *url*[**reference-identity** *ref-id-name*]} |**message-size-limit** *size* | **preferred-msg-format** {**long-text** | **short-text** | **xml**} **transport-method** {**email** | **http**}}

例：

```
ciscoasa(cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService reference-identity
 ExampleService
ciscoasa(cfg-call-home-profile)# destination address email username@example.com
ciscoasa(cfg-call-home-profile)# destination preferred-msg-format long-text
```

reference-identity オプションは、受信したサーバー証明書に対する RFC 6125 参照 ID チェックを有効にします。このチェックは、HTTP アドレスが設定されている宛先にのみ適用されます。ID チェックは設定済みの参照 ID オブジェクトに基づいて行われます。参照 ID オブジェクトについて詳しくは、参照 ID の設定 （1091 ページ）を参照してください。

電子メール アドレスは、Smart Call Home のメッセージを受け取る電子メール アドレスです（最長 100 文字）。デフォルトの最大 URL サイズは 5 MB です。

モバイル デバイスでメッセージを送信し、読み取るにはショート テキスト形式を使用し、コンピュータでメッセージを送信し、読み取るにはロング テキスト形式を使用します。

メッセージの受信者が Smart Call Home バックエンド サーバーの場合、バックエンド サーバーは XML 形式のメッセージのみ受け入れられるため **preferred-msg-format** の値が XML であることを確認します。

電子メールの転送方式をメールに戻すには、このコマンドを使用します。

宛先プロファイルのコピー

既存の宛先プロファイルをコピーして新しい宛先プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 コピーするプロファイルを指定します。

profile *profile-name*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3 既存のプロファイルの内容を新しいプロファイルにコピーします。

copy profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# copy profile newprofile profile1
```

既存のプロファイル（*src-profile-name*）と新しいプロファイル（*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルをコピーする例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# copy profile newprofile profile1
```

宛先プロファイルの名前の変更

既存のプロファイルの名前を変更するには、次の手順を実行します。

手順

ステップ 1 Call Home コンフィギュレーション モードを開始します。

call-home

例：

```
ciscoasa(config)# call-home
```

ステップ 2 名前を変更するプロファイルを指定します。

profile *profilename*

例：

```
ciscoasa(cfg-call-home)# profile newprofile
```

ステップ 3 既存のプロファイルの名前を変更します。

rename profile *src-profile-name dest-profile-name*

例：

```
ciscoasa(cfg-call-home)# rename profile newprofile profile1
```

既存のプロファイル（*src-profile-name*) と新しいプロファイル (*dest-profile-name*）は最大 23 文字です。

例

次に、既存のプロファイルの名前を変更する例を示します。

```
ciscoasa(config)# call-home
ciscoasa(cfg-call-home)# profile newprofile
ciscoasa(cfg-call-home-profile)# rename profile newprofile profile1
```

Anonymous Reporting および Smart Call Home のモニタリング

Anonymous Reporting および Smart Call Home サービスのモニタリングについては、次のコマンドを参照してください。

- **show call-home detail**

  このコマンドは、現在の Smart Call Home の詳細設定を表示します。

- **show call-home mail-server status**

  このコマンドは、現在のメール サーバーのステータスを表示します。

- **show call-home profile** {profile name | **all**}

  このコマンドは、Smart Call Home プロファイルのコンフィギュレーションを表示します。

- **show call-home registered-module status** [**all**]

  このコマンドは、登録されているモジュールのステータスを表示します。

- **show call-home statistics**

  このコマンドは、Call Home の詳細ステータスを表示します。

- **show call-home**

  このコマンドは、現在の Smart Call Home のコンフィギュレーションを表示します。

- **show running-config call-home**

  このコマンドは、現在の Smart Call Home の実行コンフィギュレーションを表示します。

- **show smart-call-home alert-group**

  このコマンドは、Smart Call Home アラート グループの現在のステータスを表示します。

- **show running-config all**

このコマンドは、Anonymous Reportingユーザープロファイルに関する詳細を表示します。

Smart Call Home の例

次の例は、Smart Call Home サービスを設定する方法を示しています。

```
ciscoasa (config)# service call-home
ciscoasa (config)# call-home
ciscoasa (cfg-call-home)# contact-email-addr customer@example.com
ciscoasa (cfg-call-home)# profile CiscoTAC-1
ciscoasa (cfg-call-home-profile)# destination address http
https://example.cisco.com/its/service/example/services/ExampleService
ciscoasa (cfg-call-home-profile)# destination address email callhome@example.com
ciscoasa (cfg-call-home-profile)# destination transport-method http
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group configuration periodic weekly
 Wednesday 23:30
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group environment
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group diagnostic
ciscoasa (cfg-call-home-profile)# subscribe-to-alert-group telemetry periodic weekly
Monday 23:30
```

Anonymous Reporting および Smart Call Home の履歴

表 *81 : Anonymous Reporting* および *Smart Call Home* の履歴

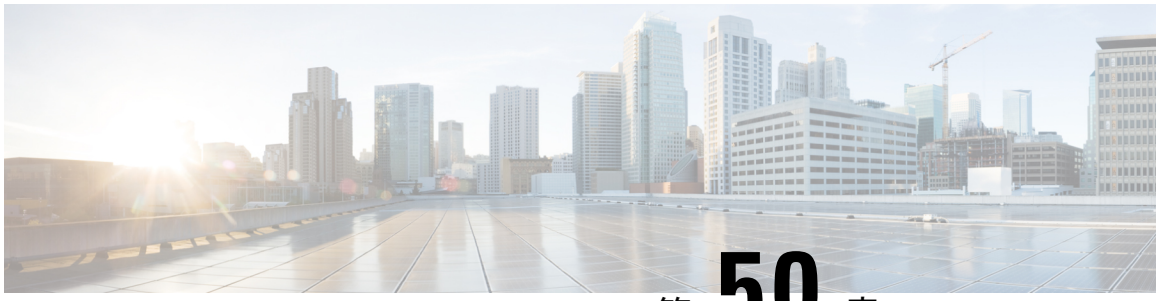
機能名	プラットフォーム リリース	説明
Smart Call Home	8.2(2)	Smart Call Home サービスは、ASA に関するプロアクティブ診断およびリアルタイム アラートを提供し、ネットワークの可用性と運用効率を向上させます。 次のコマンドを導入または変更しました。 **active (call home)**、**call-home**、**call-home send alert-group**、**call-home test**、**contact-email-addr**、**customer-id (call home)**、**destination (call home)**、**profile**、**rename profile**、**service call-home**、**show call-home**、**show call-home detail**、**show smart-call-home alert-group**、**show call-home profile**、**show call-home statistics**、**show call-home mail-server status**、**show running-config call-home**、**show call-home registered-module status all**、**site-id**、**street-address**、**subscribe-to-alert-group all**、**alert-group-config**、**subscribe-to-alert-group configuration**、**subscribe-to-alert-group diagnostic**、**subscribe-to-alert-group environment**、**subscribe-to-alert-group inventory periodic**、**subscribe-to-alert-group snapshot periodic**、**subscribe-to-alert-group syslog**、**subscribe-to-alert-group telemetry periodic**。
Anonymous Reporting	9.0(1)	Anonymous Reporting をイネーブルにして、ASA プラットフォームを強化することができます。Anonymous Reportingにより、エラーおよびヘルスに関する最小限の情報をデバイスからシスコに安全に送信できます。 **call-home reporting anonymous**、**call-home test reporting anonymous** コマンドが導入されました。
Smart Call Home	9.1(2)	テレメトリ アラート グループ レポートのための **show local-host** コマンドは、**show local-host | include interface** コマンドに変更になりました。

機能名	プラットフォーム リリース	説明
Smart Call Home	9.1(3)	Smart Call Home メッセージは、クラスタリングをイネーブルにしており、クリティカルな重大度を持つ診断アラート グループに登録するように Smart Call Home を設定してある場合に、重要なクラスタイベントをレポートするためにシスコに送信されます。Smart Call Home クラスタリング メッセージは、次の 3 種類のイベントに対してのみ送信されます。 • ユニットがクラスタに参加したとき • ユニットがクラスタから脱退したとき • クラスタユニットがクラスタ制御ユニットになったとき 送信される各メッセージには次の情報が含まれています。 • アクティブ クラスタのメンバ数 • クラスタ制御ユニットでの **show cluster info** コマンドおよび **show cluster history** コマンドの出力
セキュアな Smart Call Home サーバー接続のリファレンス ID	9.6(2)	TLS クライアント処理は、RFC 6125 のセクション 6 に定義されるサーバー ID の検証ルールをサポートするようになりました。ID 検証は、Smart Call Home サーバーへの TLS 接続の PKI 確認中に実行されます。提示された ID が設定されたリファレンス ID と一致しない場合、接続を確立できません。 次のコマンドが追加または変更されました。**[no] crypto ca reference-identity**、**call home profile destination address http**。

第 IX 部

参照先

- コマンドライン インターフェイスの使用 （1773 ページ）
- アドレス、プロトコル、およびポート （1785 ページ）



第 50 章

コマンドライン インターフェイスの使用

この章では、ASA での CLI の使用方法について説明します。

（注） CLI は、Cisco IOS CLI と類似したシンタックスや他の規則を使用しますが、ASA オペレーティング システムは Cisco IOS ソフトウェアのバージョンではありません。Cisco IOS CLI コマンドが、ASA の機能で動作したり、ASA と同じ機能を有しているものだと思わないでください。

- ファイアウォール モードとセキュリティ コンテキスト モード （1773 ページ）
- コマンドのモードとプロンプト （1774 ページ）
- 構文の書式 （1775 ページ）
- コマンドの短縮形 （1776 ページ）
- コマンドラインの編集 （1776 ページ）
- コマンドの補完 （1777 ページ）
- コマンドのヘルプ （1777 ページ）
- 実行コンフィギュレーションの確認 （1777 ページ）
- show コマンドおよび more コマンドの出力のフィルタリング （1778 ページ）
- show コマンド出力のリダイレクトと追加 （1779 ページ）
- show コマンド出力の行数の取得 （1780 ページ）
- コマンド出力のページング （1780 ページ）
- コメントの追加 （1781 ページ）
- テキスト コンフィギュレーション ファイル （1781 ページ）
- サポートされている文字セット （1783 ページ）

ファイアウォール モードとセキュリティ コンテキスト モード

ASA は、次のモードの組み合わせで動作します。

- トランスペアレント ファイアウォール モードまたはルーテッド ファイアウォール モード

ファイアウォール モードは、ASA がレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールとして動作するかどうかを決定します。

- マルチ コンテキスト モードまたはシングル コンテキスト モード

  セキュリティ コンテキスト モードは、ASA が単一のデバイスとして動作するか、またはマルチ セキュリティ コンテキストとして動作する（仮想デバイスのように動作する）かを決定します。

特定のモードでしか使用できないコマンドもあります。

コマンドのモードとプロンプト

ASA の CLI にはコマンド モードが含まれています。特定のモードでしか入力できないコマンドもあります。たとえば、機密情報を表示するコマンドを入力するには、パスワードを入力して特権モードに入る必要があります。次に、コンフィギュレーション変更が誤って入力されないようにするために、コンフィギュレーション モードに入る必要があります。下位のコマンドはすべて、高位のモードで入力できます。たとえば、グローバル コンフィギュレーション モードで特権 EXEC コマンドを入力することができます。

（注） さまざまなタイプのプロンプトはすべてデフォルトで、別々のプロンプトとして設定できます。

- システム コンフィギュレーション モードまたはシングル コンテキスト モードに入っている場合、プロンプトはホスト名で始まります。

  ```
  ciscoasa
  ```

- プロンプト文字列を表示するときに、プロンプト コンフィギュレーションが解析され、設定されたキーワード値が prompt コマンドで設定された順に表示されます。キーワード引数は、ホスト名、ドメイン、コンテキスト、プライオリティ、状態のいずれかで、任意の順になります。

  prompt hostname context priority state

- コンテキスト内では、プロンプトはホスト名の後にコンテキスト名が表示されます。

  ```
  ciscoasa/context
  ```

プロンプトは、アクセス モードに応じて変化します。

- ユーザ EXEC モード

  ユーザー EXEC モードでは、最小限の ASA 設定が表示されます。ユーザー EXEC モードのプロンプトは、初めて ASA にアクセスしたときに次のように表示されます。

```
ciscoasa>

ciscoasa/context>
```

- 特権 EXEC モード

  特権EXECモードでは、ユーザの特権レベルまでの現在の設定がすべて表示されます。すべてのユーザEXECモードコマンドは、特権EXECモードで動作します。特権EXECモードを開始するには、ユーザー EXEC モードで **enable** コマンドを入力します。これにはパスワードが必要です。プロンプトにはシャープ記号（#）が含まれています。

```
ciscoasa#

ciscoasa/context#
```

- グローバル コンフィギュレーション モード

  グローバル コンフィギュレーション モードでは、ASA コンフィギュレーションを変更できます。このモードでは、ユーザー EXEC、特権 EXEC、およびグローバルの各コンフィギュレーション コマンドをすべて使用できます。グローバルコンフィギュレーションモードを開始するには、特権 EXEC モードで **configure terminal** コマンドを入力します。プロンプトが次のように変化します。

```
ciscoasa(config)#

ciscoasa/context(config)#
```

- コマンド固有のコンフィギュレーション モード

  いくつかのコマンドは、グローバル コンフィギュレーション モードから、コマンド固有のコンフィギュレーション モードに移行します。このモードでは、ユーザ EXEC、特権 EXEC、グローバルの各コンフィギュレーション コマンド、およびコマンド固有のコンフィギュレーション コマンドをすべて使用できます。たとえば、**interface** コマンドを使用すると、インターフェイス コンフィギュレーション モードに移行します。プロンプトが次のように変化します。

```
ciscoasa(config-if)#

ciscoasa/context(config-if)#
```

構文の書式

コマンド構文の説明では、次の表に記載されている表記法を使用します。

表 *82 :* 構文の表記法

表記法	説明
bold	記載されているとおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
|	省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの短縮形

ほとんどのコマンドは、コマンドに固有の最小文字数まで短縮できます。たとえば、設定を表示するには完全なコマンド **write terminal** を入力する代わりに **wr t** と入力できます。また、特権モードを開始するには **en**、設定モードを開始するには **conf t** と入力できます。さらに、**0** を入力して **0.0.0.0** を表すこともできます。

コマンドラインの編集

ASA では、Cisco IOS ソフトウェアと同じコマンドライン編集ルールが使用されます。以前に入力したすべてのコマンドを表示するには、**show history** コマンドを使用します。個々のコマンドを表示するには、上矢印キーまたは **^p** コマンドを使用します。前に入力したコマンドを確認したら、下矢印や **^n** コマンドでリスト内を前に進むことができます。再利用するコマンドに到達したら、そのコマンドを編集することも、**Enter** キーを押して実行することもできます。**^w** を使用してカーソルの左側にある単語を削除することも、**^u** を使用して行を消去することもできます。

ASA では、1 つのコマンドに 512 文字まで入力できます。512 文字を超えて入力した文字は無視されます。

コマンドの補完

部分的な文字列を入力してからコマンドまたはキーワードを完成させるには、**Tab** キーを押します。ASA は、部分的な文字列がコマンドまたはキーワード 1 つだけと一致する場合に限り、コマンドまたはキーワードを完成させます。たとえば、**s** と入力して Tab キーを押した場合は、一致するコマンドが複数あるため、ASA はコマンドを完成させません。一方、**dis** と入力して [Tab] キーを押した場合、**disable** コマンドが完成します。

コマンドのヘルプ

次のコマンドを入力すると、コマンドラインからヘルプ情報を利用できます。

- **help** *command_name*

  特定のコマンドのヘルプを表示します。

- *command_name* **?**

  使用可能な引数のリストを表示します。

- *string***?**（スペースなし）

  その文字列で始まるコマンドをリストします。

- **?** および **+?**

  使用できるすべてのコマンドをリストします。**?** と入力すると、ASA は現在のモードで使用できるコマンドだけを表示します。下位モードのコマンドも含め、使用できるすべてのコマンドを表示するには、**+?** と入力します。

（注） コマンド文字列に疑問符（?）を組み込む場合は、誤って CLI ヘルプを起動しないよう、疑問符を入力する前に Ctrl+V を押す必要があります。

実行コンフィギュレーションの確認

実行コンフィギュレーションを確認するには、次のいずれかのコマンドを使用します。

- **show running-config** [**all**] [*command*]

  all を指定すると、すべてのデフォルト設定も表示されます。*Command* を指定すると、関連するコマンドだけが出力に含まれます。

（注） 多くのパスワードは ***** として表示されます。パスワードをプレーン テキストまたは暗号化された形式（マスター パスフレーズを有効にしている場合）で表示するには、**more** コマンドを使用します。

- **more system:running-config**

show コマンドおよび more コマンドの出力のフィルタリング

縦棒（|）はどの **show** コマンドでも使用できます。これには、フィルタ オプションとフィルタリング式を組み込むことができます。フィルタリングは、Cisco IOS ソフトウェアと同様に、各出力行を正規表現と照合することによって行われます。選択するフィルタ オプションによって、正規表現に一致するすべての出力を含めたり除外したりできます。また、正規表現に一致する行で始まるすべての出力を表示することもできます。

show コマンドでフィルタリング オプションを使用する場合の構文は、次のとおりです。

show *command* | {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

または

more system:running-config| {**include**| **exclude** | **begin** | **grep** [**-v**]} *regexp*

（注） **more** コマンドを入力すると、実行コンフィギュレーションだけでなく、任意のファイルの内容を表示できます。詳細については、コマンド リファレンスを参照してください。

このコマンド文字列の最初の縦棒（|）は演算子であり、コマンド内に含める必要があります。この演算子は、**show** コマンドの出力をフィルタに組み込みます。構文内に含まれるその他の縦棒（|）は代替オプションを示すものであり、コマンドの一部ではありません。

include オプションを指定すると、正規表現に一致するすべての出力行が表示されます。**-v** を付けずに **grep** オプションを使用する場合も、同じ結果となります。**exclude** オプションを指定すると、正規表現に一致するすべての出力行が除外されます。**-v** を付けて **grep** オプションを使用する場合も、同じ結果となります。**begin** オプションを指定すると、正規表現に一致する行で始まるすべての出力行が表示されます。

regexp には、Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、メタ文字と呼ばれるキーボード文字は、正規表現で使用されると特別な意味を持ちます。

疑問符（?）やタブなど、CLI の特殊文字をすべてエスケープするには、**Ctrl+V** を使用します。たとえば、コンフィギュレーションで **d?g** と入力するには、**d[Ctrl+V]?g** とキー入力します。

show コマンド出力のリダイレクトと追加

表示する出力が多い場合、コマンドの完了に時間がかかることがあります。たとえば、100 万のアクセス制御エントリや非常に大きい ASP テーブルを表示しようとすると、システムが停止したと思うかもしれません。

show コマンドの出力を画面に表示するのではなく、デバイス上またはリモート ロケーション内のファイルにリダイレクトすることができます。デバイス上のファイルへのリダイレクトの場合は、ファイルにコマンド出力を追加することもできます。

show *command* | {**append | redirect**} *url*

- **append** *url* により、出力が既存のファイルに追加されます。次のいずれかを使ってファイルを指定します。
  - **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
  - **disk1:/**[[*path/*]*filename*]：外部メモリを意味します。
- **redirect** *url* により、指定されたファイルが作成されます。または、ファイルがすでに存在している場合は、上書きされます。
  - **disk0:/**[[*path/*]*filename*] または **flash:/**[[*path/*]*filename*]：**flash** と **disk0** はどちらも内部フラッシュ メモリを示します。どちらのオプションを使用してもかまいません。
  - **disk1:/**[[*path/*]*filename*]：外部メモリを意味します。
  - **smb:/**[[*path/*]*filename*]：サーバー メッセージ ブロック、UNIX サーバーのローカル ファイル システムを示します。
  - **ftp://**[[*user*[**:***password*]@] *server*[:*port*]/[*path/*] *filename*[**;type=***xx*]]：SCP サーバーを示します。**type** には次のいずれかのキーワードを使用できます。**ap**（ASCII パッシブ モード）、**an**（ASCII 通常モード）、**ip**（デフォルト：バイナリ パッシブ モード）、**in**（バイナリ通常モード）。
  - **scp://**[[*user*[:*password*]@] *server*[/*path*]/*filename*[**;int=***interface_name*]]：**;int=***interface* オプションを指定すると、ルート ルックアップがバイパスされ、常に指定したインターフェイスを使用してセキュア コピー（SCP）サーバーに接続するようになります。
  - **tftp://**[[*user*[**:***password*]@] *server*[:*port*] /[*path/*]*filename*[**;int=***interface_name*]]：TFTP サーバーを示します。パス名にスペースを含めることはできません。**;int=***interface* オプションを指定すると、ルートルックアップをバイパスし、常に指定したインターフェイスを使用して TFTP サーバーに接続するようになります。

show コマンド出力の行数の取得

実際の **show** コマンド出力を表示するのではなく、出力の行数のみを確認したり、正規表現に一致する行数のみを確認したりすることもできます。それにより、行数を以前のコマンド入力時の数と簡単に比較することができます。この方法は、設定に変更を加えたときの簡易チェックとして使用できます。**count** キーワードを使用するか、grep キーワードに **-c** を追加できます。

show *command* | **count** [*regular_expression*]

show *command* | **grep -c** [*regular_expression*]

regular_expression の箇所は、任意の Cisco IOS 正規表現と置き換えます。正規表現は一重引用符または二重引用符で囲まれていません。したがって、末尾の空白スペースが正規表現の一部と解釈されるため、末尾の空白スペースに注意してください。正規表現はオプションです。正規表現を含めない場合に返されるカウントは、フィルタリングされていない出力の合計行数となります。

正規表現を作成する場合は、照合する任意の文字または数字を使用できます。また、メタ文字と呼ばれる特定のキーボード文字は、正規表現で使用されると、特別な意味を持ちます。CLI で疑問符（?）やタブなどの特殊文字をエスケープするには、いずれの特殊文字の場合も、Ctrl+V を使用します。たとえば、設定で **d?g** と入力するには、**d[Ctrl+V]?g** と入力します。

たとえば、**show running-config** の出力のすべての行数を表示するには、以下のように行います。

```
ciscoasa# show running-config | count
Number of lines which match regexp = 271
```

下記の例は、稼働中のインターフェイスの数をすばやく確認できる方法を示しています。最初の例は、正規表現で **grep** キーワードを使用することにより、稼動状態を示す行のみに絞り込む方法です。次の例は、**-c** オプションを追加することにより、実際の出力行ではなくその数だけを表示する方法です。

```
ciscoasa# show interface | grep is up
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
Interface GigabitEthernet0/1 "inside", is up, line protocol is up

ciscoasa# show interface | grep -c is up
Number of lines which match regexp = 2
```

コマンド出力のページング

help や **?**、**show**、**show xlate** など、長いリストが出力されるコマンドでは、1 画面分ずつ表示して停止させるか、リストの最後まで表示させるかを決めることができます。**pager** コマンドを使用すると、画面上に表示する行数を選択してから More プロンプトを表示するようにできます。

ページングがイネーブルになっているときには、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトの構文は、UNIX の **more** コマンドと似ています。

- 次の 1 画面を表示するには、Space バーを押します。
- 次の行を表示するには、Enter キーを押します。
- コマンド ラインに戻るには、q キーを押します。

コメントの追加

行の先頭にコロン（:）を置いて、コメントを作成できます。しかし、コメントが表示されるのはコマンド ヒストリ バッファだけで、コンフィギュレーションには表示されません。したがって、コメントは、**show history** コマンドを使用するか、矢印キーを押して前のコマンドを取得することによって表示できますが、コンフィギュレーションには含まれないので、**write terminal** コマンドでは表示できません。

テキスト コンフィギュレーション ファイル

この項では、ASA にダウンロードできるテキスト コンフィギュレーション ファイルをフォーマットする方法について説明します。

テキスト ファイルでコマンドと行が対応する仕組み

テキスト コンフィギュレーション ファイルには、このガイドで説明するコマンドに対応する行が含まれています。

例では、コマンドの前に CLI プロンプトがあります。次の例でのプロンプトは「ciscoasa(config)#」です。

```
ciscoasa(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンドの入力を求めるプロンプトが表示されないので、プロンプトは省略されています。

```
context a
```

コマンド固有のコンフィギュレーション モード コマンド

コマンド固有のコンフィギュレーション モード コマンドは、コマンドラインで入力されたときに、メイン コマンドの下に字下げして表示されます。テキスト ファイルの行は、コマンドがメイン コマンドのすぐ後に表示される限り、字下げする必要はありません。たとえば、次のテキストは字下げされていませんが、字下げしたテキストと同じように読み取られます。

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自動テキスト入力

コンフィギュレーションを ASA にダウンロードすると、それにより一部の行が自動的に挿入されます。たとえば、ASA は、デフォルト設定のため、またはコンフィギュレーションが変更されたときのための行を挿入します。テキスト ファイルを作成するときは、これらの自動入力を行う必要はありません。

行の順序

ほとんどの場合、コマンドはファイル内で任意の順序に置くことができます。ただし、ACE などいくつかの行は表示された順に処理されるので、順序がアクセス リストの機能に影響する場合があります。その他のコマンドでも、順序の要件がある場合があります。たとえば、あるインターフェイスの名前を多数の後続コマンドが使用する場合は、そのインターフェイスの **nameif** コマンドをまず入力する必要があります。また、コマンド固有のコンフィギュレーション モードのコマンドは、メイン コマンドの直後に置く必要があります。

テキスト コンフィギュレーションに含まれないコマンド

いくつかのコマンドは、コンフィギュレーションに行を挿入しません。たとえば、**show running-config** などのランタイム コマンドは、テキスト ファイル内に対応する行がありません。

パスワード

ログイン パスワード、イネーブル パスワード、およびユーザ パスワードは、コンフィギュレーションに保存される前に自動的に暗号化されます。たとえば、パスワード「cisco」の暗号化された形式は jMorNbK0514fadBh のようになります。コンフィギュレーション パスワードは暗号化された形式で別の ASA にコピーできますが、そのパスワードの暗号を解読することはできません。

暗号化されていないパスワードをテキスト ファイルに入力した場合、コンフィギュレーションを ASA にコピーしても、ASA は自動的にパスワードを暗号化しません。ASA がパスワードを

暗号化するのは、**copy running-config startup-config** または **write memory** コマンドを使用して、コマンドラインから実行コンフィギュレーションを保存した場合のみです。

マルチセキュリティ コンテキスト ファイル

マルチ セキュリティ コンテキストの場合、コンフィギュレーション全体は次に示す複数の部分で構成されます。

- セキュリティ コンテキスト コンフィギュレーション
- コンテキストのリストなど、ASA の基本設定を示すシステム コンフィギュレーション
- システム コンフィギュレーション用のネットワーク インターフェイスを提供する管理コンテキスト

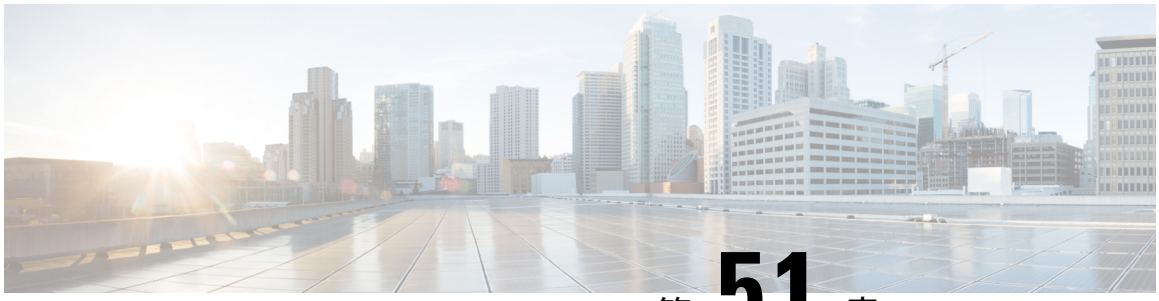
  システムコンフィギュレーションには、それ自体のインターフェイスまたはネットワーク設定は含まれていません。代わりに、システムは、ネットワーク リソースにアクセスする必要があるときに（サーバからコンテキストをダウンロードするときなど）、管理コンテキストとして指定されたコンテキストを使用します。

各コンテキストは、シングル コンテキスト モード コンフィギュレーションに似ています。システム コンフィギュレーションにはシステム限定のコマンド（全コンテキストのリストなど）が含まれており、その他の一般的なコマンド（多数のインターフェイス パラメータなど）は存在しない点で、システム コンフィギュレーションは、コンテキスト コンフィギュレーションとは異なっています。

サポートされている文字セット

ASA CLI は、現在 UTF-8 の符号化方式だけをサポートしています。UTF-8 は Unicode 文字の特定の符号化スキームであり、ASCII 文字のサブセットと互換性を持つように設計されています。ASCII 文字は UTF-8 で 1 バイト文字として表現されます。その他のすべての文字は、UTF-8 でマルチバイト文字として表現されます。

ASCII の印刷可能文字（0x20 ～ 0x7e）はすべてサポートされています。印刷可能な ASCII 文字は、ISO 8859-1 の文字と同じです。UTF-8 は ISO 8859-1 のスーパーセットであるため、最初の 256 文字（0 ～ 255）は ISO 8859-1 の文字と同じになります。ASA CLI は、ISO 8859-1 の文字を 255 文字（マルチバイト文字）までサポートしています。



第 51 章

アドレス、プロトコル、およびポート

この章では、IP アドレス、プロトコル、およびアプリケーションのクイック リファレンスを提供します。

- IPv4 アドレスとサブネット マスク （1785 ページ）
- IPv6 アドレス （1789 ページ）
- プロトコルとアプリケーション （1796 ページ）
- TCP ポートおよび UDP ポート （1797 ページ）
- ローカル ポートとプロトコル （1801 ページ）
- ICMP タイプ （1802 ページ）

IPv4 アドレスとサブネット マスク

この項では、ASA で IPv4 アドレスを使用する方法について説明します。IPv4 アドレスはドット付き 10 進数表記の 32 ビットの数値であり、バイナリから 10 進数に変換されドットで区切られた 4 つの 8 ビット フィールド（オクテット）で構成されます。IP アドレスの最初の部分はホストが常駐するネットワークを示し、2 番目の部分は所定のネットワーク上の特定のホストを示します。ネットワーク番号フィールドは、ネットワーク プレフィックスと呼ばれます。所定のネットワーク上のホストはすべて、同じネットワーク プレフィックスを共有しますが、固有のホスト番号を持つ必要があります。クラスフル IP では、アドレスのクラスがネットワーク プレフィックスとホスト番号の間の境界を決定します。

クラス

IP ホスト アドレスは、Class A、Class B、Class C の 3 つの異なるアドレス クラスに分かれています。各クラスは、32 ビット アドレス内の異なるポイントで、ネットワーク プレフィックスとホスト番号の間の境界を決定します。Class D アドレスは、マルチキャスト IP 用に予約されています。

- Class A アドレス（1.xxx.xxx.xxx ～ 126.xxx.xxx.xxx）は、最初のオクテットのみをネットワーク プレフィックスとして使用します。

- Class B アドレス（128.0.xxx.xxx ～ 191.255.xxx.xxx）は、最初の 2 つのオクテットをネットワーク プレフィックスとして使用します。
- Class C アドレス（192.0.0.xxx ～ 223.255.255.xxx）は、最初の 3 つのオクテットをネットワーク プレフィックスとして使用します。

Class A アドレスには 16,777,214 個のホスト アドレス、Class B アドレスには 65,534 個のホストがあるので、サブネットマスクを使用してこれらの膨大なネットワークを小さいサブネットに分割することができます。

プライベート ネットワーク

ネットワーク上に多数のアドレスが必要な場合、それらをインターネットでルーティングする必要がないときは、インターネット割り当て番号局（IANA）が推奨するプライベート IP アドレスを使用できます（RFC 1918 を参照）。次のアドレス範囲が、アドバタイズされないプライベート ネットワークとして指定されています。

- 10.0.0.0 ～ 10.255.255.255
- 172.16.0.0 ～ 172.31.255.255
- 192.168.0.0 ～ 192.168.255.255

サブネット マスク

サブネット マスクを使用すると、単一の Class A、B、または C ネットワークを複数のネットワークに変換できます。サブネット マスクを使用して、ホスト番号からネットワーク プレフィックスにビットを追加する拡張ネットワーク プレフィックスを作成することができます。たとえば、Class C ネットワーク プレフィックスは常に、IP アドレスの最初の 3 つのオクテットで構成されます。一方、Class C 拡張ネットワーク プレフィックスは、4 番目のオクテットの一部も使用します。

ドット付き 10 進数の代わりにバイナリ表記を使用している場合は、サブネット マスクを容易に理解できます。サブネット マスク内のビットには、インターネット アドレスとの 1 対 1 の対応関係があります。

- IP アドレス内の対応するビットが拡張ネットワーク プレフィックスの一部である場合、ビットは 1 に設定されます。
- ビットがホスト番号の一部である場合、ビットは 0 に設定されます。

例 1：Class B アドレスが 129.10.0.0 の場合に 3 番目のオクテット全体をホスト番号ではなく拡張ネットワーク プレフィックスの一部として使用するには、サブネット マスクとして 11111111.11111111.11111111.00000000 を指定する必要があります。このサブネット マスクによって、Class B アドレスは、ホスト番号が最後のオクテットだけで構成される Class C アドレスに相当するものに変換されます。

例 2：3 番目のオクテットの一部だけを拡張ネットワーク プレフィックスに使用する場合は、11111111.11111111.11111000.00000000 のようなサブネット マスクを指定する必要があります。ここでは、3 番目のオクテットのうち 5 ビットだけが拡張ネットワーク プレフィックスに使用されます。

サブネット マスクは、ドット付き 10 進数マスクまたは /ビット（「スラッシュ ビット」）マスクとして記述できます。例 1 では、ドット付き 10 進数マスクに対して、各バイナリ オクテットを 10 進数の 255.255.255.0 に変換します。/ビット マスクの場合は、1s: /24 の数値を追加します。例 2 では、10 進数は 255.255.248.0 で、/ビットは /21 です。

3 番目のオクテットの一部を拡張ネットワーク プレフィックスに使用して、複数の Class C ネットワークを大規模なネットワークにスーパーネット化することもできます。たとえば、192.168.0.0/20 です。

サブネットマスクの決定

必要なホストの数に基づいてサブネットマスクを決定するには、次の表を参照してください。

（注） 単一のホストを示す /32 を除き、サブネットの最初と最後の数は予約されています。

表 *83*：ホスト、ビット、ドット区切りの *10* 進数マスク

ホスト	/ビットマスク	ドット付き 10 進数マスク
16,777,216	/8	255.0.0.0 Class A ネットワーク
65,536	/16	255.255.0.0 Class B ネットワーク
32,768	/17	255.255.128.0
16,384	/18	255.255.192.0
8192	/19	255.255.224.0
4096	/20	255.255.240.0
2048	/21	255.255.248.0
1024	/22	255.255.252.0
512	/23	255.255.254.0
256	/24	255.255.255.0 Class C ネットワーク
128	/25	255.255.255.128
64	/26	255.255.255.192
32	/27	255.255.255.224
16	/28	255.255.255.240

ホスト	/ビットマスク	ドット付き 10 進数マスク
8	/29	255.255.255.248
4	/30	255.255.255.252
使用不可	/31	255.255.255.254
1	/32	255.255.255.255 単一ホスト アドレス

サブネットマスクに使用するアドレスの決定

次の各項では、Class C サイズおよび Class B サイズのネットワークに対してサブネット マスクで使用するネットワーク アドレスを判別する方法について説明します。

クラス C 規模ネットワーク アドレス

2 ～ 254 のホストを持つネットワークの場合、4 番目のオクテットは、0 から始まるホスト アドレスの数の倍数になります。例として、次の表に 8 個のホストを持つサブネット（/29）、192.168.0.x を示します。

（注） サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、192.168.0.0 と 192.168.0.7 は使用できません。

表 *84 :* クラス *C* 規模ネットワーク アドレス

マスク /29（255.255.255.248）でのサブネット	アドレス範囲
192.168.0.0	192.168.0.0 ～ 192.168.0.7
192.168.0.8	192.168.0.8 ～ 192.168.0.15
192.168.0.16	192.168.0.16 ～ 192.168.0.31
—	—
192.168.0.248	192.168.0.248 ～ 192.168.0.255

クラス B 規模ネットワーク アドレス

254 ～ 65,534 のホストを持つネットワークのサブネット マスクで使用するネットワーク アドレスを判別するには、可能な拡張ネットワーク プレフィックスそれぞれについて 3 番目のオクテットの値を判別する必要があります。たとえば、10.1.*x*.0 のようなアドレスをサブネット化することができます。ここで、最初の 2 つのオクテットは拡張ネットワーク プレフィックスで使用されるため固定されています。4 番目のオクテットは、すべてのビットがホスト番号に使用されるため、0 です。

3 番目のオクテットの値を判別するには、次の手順を実行します。

1. 65,536（3 番目と 4 番目のオクテットを使用するアドレスの合計）を必要なホスト アドレスの数で割って、ネットワークから作成できるサブネットの数を計算します。

   たとえば、65,536 を 4096 のホストで割ると、16 になります。したがって、Class B サイズのネットワークでは、それぞれ 4096 個のアドレスを持つサブネットが 16 個できます。

2. 256（3 番目のオクテットの値の数）をサブネットの数で割って、3 番目のオクテット値の倍数を判別します。

   この例では、256/16 = 16 です。

   3 番目のオクテットは、0 から始まる 16 の倍数になります。

次の表に、ネットワーク 10.1 の 16 個のサブネットを示します。

（注） サブネットの最初と最後のアドレスは予約されています。最初のサブネットの例では、10.1.0.0 と 10.1.15.255 は使用できません。

表 *85* : ネットワークのサブネット

マスク /20（255.255.240.0）でのサブネット	アドレス範囲
10.1.0.0	10.1.0.0 ～ 10.1.15.255
10.1.16.0	10.1.16.0 ～ 10.1.31.255
10.1.32.0	10.1.32.0 ～ 10.1.47.255
—	—
10.1.240.0	10.1.240.0 ～ 10.1.255.255

IPv6 アドレス

IPv6は、IPv4後の次世代インターネットプロトコルです。これにより、アドレス空間の拡張、ヘッダー形式の簡略化、拡張子とオプションのサポートの向上、フローラベル機能、および認証とプライバシーの機能が提供されます。IPv6についてはRFC 2460で説明されています。IPv6 アドレッシング アーキテクチャについては RFC 3513 で説明されています。

この項では、IPv6 のアドレス形式とアーキテクチャについて説明します。

IPv6 アドレスの形式

IPv6 アドレスは、x:x:x:x:x:x:x:x のように、コロン（:）で区切られた 8 つの一連の 16 ビット 16 進数フィールドとして表されます。次に、IPv6 アドレスの例を 2 つ示します。

- 2001:0DB8:7654:3210:FEDC:BA98:7654:3210
- 2001:0DB8:0000:0000:0008:0800:200C:417A

（注） IPv6 アドレスの 16 進文字は大文字と小文字が区別されません。

アドレスの個々のフィールドに先行ゼロを入れる必要はありませんが、各フィールドに 1 個以上の桁が含まれている必要があります。したがって、例のアドレス 2001:0DB8:0000:0000:0008:0800:200C:417A は、左から 3 番目～ 6 番目のフィールドから先行ゼロを削除して、2001:0DB8:0:0:8:800:200C:417A のように短縮することができます。ゼロだけを含むフィールド（左から 3 番目と 4 番目のフィールド）は、単一のゼロに短縮されています。左から 5 番目のフィールドでは、3 つの先行ゼロが削除され、単一の 8 がフィールドに残されています。左から 6 番目のフィールドでは、1 つの先行ゼロが削除され、800 がフィールドに残されています。

IPv6 アドレスには、ゼロの 16 進数フィールドがいくつか連続して含まれていることがよくあります。IPv6 アドレスの先頭、中間、または末尾で 2 つのコロン（::）を使用して、ゼロの連続フィールドを圧縮することができます（コロンは、ゼロの 16 進数フィールドが連続していることを表します）。次の表に、さまざまなタイプの IPv6 アドレスでのアドレス圧縮の例をいくつか示します。

表 *86 : IPv6* アドレスの圧縮例

アドレスタイプ	標準形式	圧縮形式
ユニキャスト	2001:0DB8:0:0:0:BA98:0:3210	2001:0DB8::BA98:0:3210
マルチキャスト	FF01:0:0:0:0:0:0:101	FF01::101
ループバック	0:0:0:0:0:0:0:1	::1
未指定	0:0:0:0:0:0:0:0	::

（注） ゼロのフィールドが連続することを表す 2 つのコロン（::）は、IPv6 アドレスの中で一度だけ使用できます。

IPv4 アドレスと IPv6 アドレスの両方を含む環境に対処するため、別の IPv6 形式がよく使用されます。その形式は x:x:x:x:x:x:y.y.y.y です。ここで、x は IPv6 アドレスの 6 つの高次の部分の 16 進数値を表し、y はアドレスの 32 ビット IPv4 部分（IPv6 アドレスの残りの 2 つの 16 ビット部分を占める）の 10 進数値を表します。たとえば、IPv4 アドレス 192.168.1.1 は、IPv6 アドレス 0:0:0:0:0:0:FFFF:192.168.1.1 または ::FFFF:192.168.1.1 として表すことができます。

IPv6 アドレス タイプ

次に、IPv6 アドレスの 3 つの主なタイプを示します。

- **ユニキャスト**：ユニキャストアドレスは、単一インターフェイスの識別子です。ユニキャストアドレスに送信されたパケットは、そのアドレスで示されたインターフェイスに送信されます。1つのインターフェイスに複数のユニキャストアドレスが割り当てられている場合もあります。
- **マルチキャスト**：マルチキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスに送信されたパケットは、そのアドレスで示されたすべてのアドレスに送信されます。
- **エニーキャスト**：エニーキャストアドレスは、インターフェイスのセットを表す識別子です。マルチキャストアドレスと違い、エニーキャストアドレスに送信されたパケットは、ルーティングプロトコルの距離測定によって判別された「最も近い」インターフェイスにだけ送信されます。

（注） IPv6 にはブロードキャスト アドレスはありません。マルチキャスト アドレスにブロードキャスト機能があります。

ユニキャスト アドレス

この項では、IPv6ユニキャストアドレスについて説明します。ユニキャストアドレスは、ネットワーク ノード上のインターフェイスを識別します。

グローバル アドレス

IPv6 グローバル ユニキャスト アドレスの一般的な形式では、グローバル ルーティング プレフィックス、サブネット ID、インターフェイス ID の順に並んでいます。グローバル ルーティングプレフィックスは、別の IPv6 アドレス タイプによって予約されていない任意のプレフィックスです。

バイナリ 000 で始まるものを除くすべてのグローバル ユニキャスト アドレスが、Modified EUI-64 形式で 64 ビットのインターフェイス ID を持っています。

バイナリ 000 で始まるグローバル ユニキャスト アドレスには、アドレスのインターフェイス ID部分のサイズまたは構造に対する制約がありません。このタイプのアドレスの一例として、IPv4 アドレスが埋め込まれた IPv6 アドレスがあります。

サイトローカル アドレス

サイトローカルアドレスは、サイト内のアドレッシングに使用されます。このアドレスを使用すると、グローバルで一意のプレフィックスを使用せずにサイト全体をアドレッシングすることができます。サイトローカルアドレスでは、プレフィックス FEC0::/10、54 ビット サブネット ID、64 ビット インターフェイス ID（Modified EUI-64 形式）の順に並んでいます。

サイトローカル ルータは、サイト外の送信元または宛先にサイトローカル アドレスを持つパケットを転送しません。したがって、サイトローカル アドレスは、プライベート アドレスと見なされます。

リンクローカル アドレス

すべてのインターフェイスに、少なくとも 1 つのリンクローカル アドレスが必要です。インターフェイスごとに複数の IPv6 アドレスを設定できますが、設定できるリンクローカル アドレスは 1 つだけです。

リンクローカル アドレスは、Modified EUI-64 形式でリンクローカル プレフィックス FE80::/10 とインターフェイス識別子を使用して任意のインターフェイスで自動的に設定できる IPv6 ユニキャスト アドレスです。リンクローカル アドレスは、ネイバー探索プロトコルとステートレス自動設定プロセスで使用されます。リンクローカルアドレスを持つノードは、通信が可能です。これらのノードは通信にサイトローカルアドレスまたはグローバルに固有なアドレスを必要としません。

ルータは、送信元または宛先にリンクローカルアドレスを持つパケットを送信しません。したがって、リンクローカル アドレスは、プライベート アドレスと見なされます。

IPv4 互換 IPv6 アドレス

IPv4 アドレスを組み込むことができる IPv6 アドレスのタイプは 2 つあります。

最初のタイプは、IPv4 互換 IPv6 アドレスです。IPv6 移行メカニズムには、IPv4 ルーティング インフラストラクチャ上で IPv6 パケットを動的にトンネリングさせるためのホストおよびルータの技術が実装されています。この技術を使用する IPv6 ノードには、低次 32 ビットでグローバル IPv4 アドレスを伝送する特別な IPv6 ユニキャスト アドレスが割り当てられます。このタイプのアドレスは「IPv4 互換 IPv6 アドレス」と呼ばれ、形式は ::y.y.y.y です。この y.y.y.y は IPv4 ユニキャスト アドレスになります。

（注） 「IPv4 互換 IPv6 アドレス」で使用する IPv4 アドレスは、グローバルに固有な IPv4 ユニキャスト アドレスである必要があります。

2 つ目のタイプの IPv6 アドレスは、IPv4 アドレスが埋め込まれたもので、「IPv4 マッピング IPv6 アドレス」と呼ばれます。このアドレス タイプは、IPv4 ノードのアドレスを IPv6 アドレスとして表すために使用されます。このタイプのアドレス形式は ::FFFF:y.y.y.y です。ここで、y.y.y.y は IPv4 ユニキャスト アドレスです。

未指定アドレス

未指定アドレス 0:0:0:0:0:0:0:0 は、IPv6 アドレスがないことを示しています。たとえば、IPv6 ネットワーク上で新しく初期化されたノードは、IPv6 アドレスを受信するまで、パケットで未指定アドレスを送信元アドレスとして使用できます。

（注） IPv6 未指定アドレスは、インターフェイスに割り当てることができません。未指定 IPv6 アドレスを IPv6 パケットまたは IPv6 ルーティング ヘッダーで宛先アドレスとして使用することはできません。

ループバック アドレス

ループバック アドレス 0:0:0:0:0:0:0:1 は、ノードが IPv6 パケットをそれ自体に送信するために使用できます。IPv6 のループバック アドレスは、IPv4 のループバック アドレス（127.0.0.1）と同じように機能します。

（注） IPv6 ループバック アドレスは、物理インターフェイスに割り当てることができません。IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットは、そのパケットを作成したノード内に留まっている必要があります。IPv6 ルータは、IPv6 ループバック アドレスを送信元アドレスまたは宛先アドレスとするパケットを転送しません。

インターフェイス識別子

IPv6 ユニキャスト アドレス内のインターフェイス識別子は、リンク上でインターフェイスを識別するために使用されます。これらの識別子は、サブネットプレフィックス内で固有である必要があります。多くの場合、インターフェイス識別子はインターフェイス リンク層アドレスから導出されます。各インターフェイスが異なるサブネットに接続されていれば、単一ノードの複数のインターフェイスで同一のインターフェイス識別子を使用することもできます。

バイナリ 000 で始まるものを除くすべてのユニキャストアドレスで、インターフェイス識別子は、64 ビットの長さで Modified EUI-64 形式で構築されている必要があります。Modified EUI-64 形式は、アドレス内のユニバーサル/ローカル ビットを逆にし、MAC アドレスの上の 3 つのバイトと下の 3 つのバイトの間に 16 進数 FFFE を挿入することによって、48 ビット MAC アドレスから作成されます。

たとえば、MAC アドレスが 00E0.b601.3B7A のインターフェイスの場合、64 ビット インターフェイス ID は 02E0:B6FF:FE01:3B7A になります。

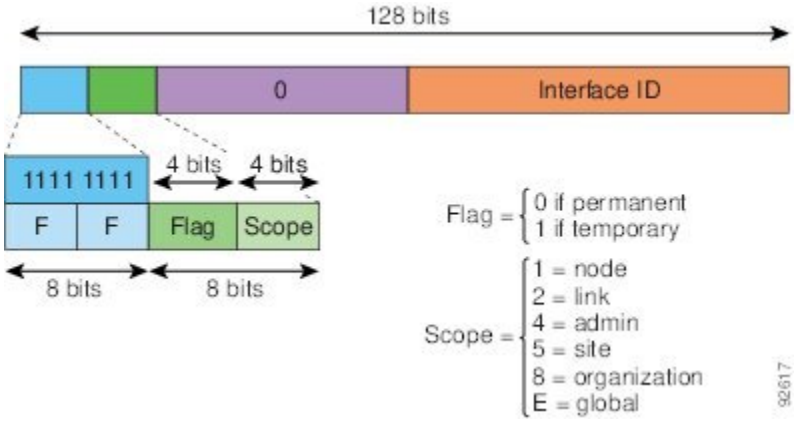
マルチキャスト アドレス

IPv6 マルチキャスト アドレスは、通常は異なるノード上にある、インターフェイスのグループの識別子です。マルチキャスト アドレスに送信されたパケットは、マルチキャスト アドレスが示すすべてのインターフェイスに配信されます。1 つのインターフェイスが任意の数のマルチキャスト グループに属すことができます。

IPv6 マルチキャスト アドレスのプレフィックスは FF00::/8（1111 1111）です。オクテットとそれに続くプレフィックスは、マルチキャストアドレスのタイプとスコープを定義します。永続的に割り当てられた（周知の）マルチキャストアドレスには、0 に等しいフラグ パラメータがあり、一時的な（過渡）マルチキャスト アドレスには 1 に等しいフラグ パラメータがあります。ノード、リンク、サイト、組織のスコープ、またはグローバル スコープを持つマルチ

キャスト アドレスのスコープ パラメータは、それぞれ 1、2、5、8、または E です。たとえば、プレフィックスが FF02::/16 のマルチキャスト アドレスは、リンク スコープを持つ永続マルチキャスト アドレスです。次の図に、IPv6 マルチキャスト アドレスの形式を示します。

図 *95 : IPv6* マルチキャスト アドレス形式



IPv6 ノード（ホストとルータ）は、次のマルチキャスト グループに参加する必要があります。

- All Nodes マルチキャスト アドレス：
  - FF01::（インターフェイスローカル）
  - FF02::（リンクローカル）
- ノード FF02:0:0:0:0:1:FFXX:XXXX/104 上の各 IPv6 ユニキャスト アドレスおよびエニーキャスト アドレスの送信要求ノード アドレス。ここで、XX:XXXX は低次 24 ビットのユニキャスト アドレスまたはエニーキャスト アドレスです。

（注） 送信要求ノードアドレスは、ネイバー送信要求メッセージで使用されます。

IPv6 ルータは、次のマルチキャスト グループに参加する必要があります。

- FF01::2（インターフェイスローカル）
- FF02::2（リンクローカル）
- FF05::2（サイトローカル）

マルチキャスト アドレスは、IPv6 パケットで送信元アドレスとして使用できません。

（注） IPv6 にはブロードキャスト アドレスはありません。ブロードキャスト アドレスの代わりに IPv6 マルチキャスト アドレスが使用されます。

エニーキャスト アドレス

IPv6 エニーキャスト アドレスは、複数のインターフェイス（通常は異なるノードに属す）に割り当てられたユニキャスト アドレスです。エニーキャスト アドレスにルーティングされたパケットは、そのアドレスを持ち、有効なルーティング プロトコルによって最も近いと判別されたインターフェイスにルーティングされます。

エニーキャスト アドレスは、ユニキャスト アドレス空間から割り当てられます。エニーキャスト アドレスは、複数のインターフェイスに割り当てられたユニキャスト アドレスにすぎません。インターフェイスは、アドレスをエニーキャストアドレスとして認識するように設定されている必要があります。

エニーキャスト アドレスには次の制限が適用されます。

- エニーキャスト アドレスは、IPv6 パケットの送信元アドレスとして使用できません。
- エニーキャスト アドレスは、IPv6 ホストに割り当てることはできません。IPv6 ルータにだけ割り当てるこができます。

（注） ASA では、エニーキャスト アドレスをサポートされていません。

必須アドレス

IPv6 ホストには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 各インターフェイスのリンクローカル アドレス
- ループバック アドレス
- All-Nodes マルチキャスト アドレス
- 各ユニキャスト アドレスまたはエニーキャスト アドレスの送信要求ノード マルチキャスト アドレス

IPv6 ルータには、少なくとも次のアドレスが（自動または手動で）設定されている必要があります。

- 必須ホスト アドレス
- このルータがルータとして動作するように設定されているすべてのインターフェイスのサブネットルータ エニーキャスト アドレス
- All-Routers マルチキャスト アドレス

IPv6 アドレス プレフィックス

IPv6 アドレス プレフィックスは、ipv6-prefix/prefix-length の形式で、アドレス空間全体のビット連続ブロックを表すために使用できます。IPv6-prefix は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。プレフィックス長は、アドレスの高次の連続ビットのうち、何個がプレフィックス（アドレスのネットワーク部分）を構成しているかを指定する 10 進数値です。たとえば、2001:0DB8:8086:6502::/32 は有効な IPv6 プレフィックスです。

IPv6 プレフィックスは、IPv6 アドレスのタイプを特定します。次の表に、各 IPv6 アドレス タイプのプレフィックスを示します。

表 *87 : IPv6* アドレス タイプのプレフィックス

アドレスタイプ	バイナリ プレフィックス	IPv6 表記
未指定	000...0（128 ビット）	::/128
ループバック	000...1（128 ビット）	::1/128
マルチキャスト	11111111	FF00::/8
リンクローカル（ユニキャスト）	1111111010	FE80::/10
サイトローカル（ユニキャスト）	1111111111	FEC0::/10
グローバル（ユニキャスト）	その他すべてのアドレス。	
エニーキャスト	ユニキャスト アドレス空間から取得。	

プロトコルとアプリケーション

次の表に、プロトコルのリテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。

表 *88 :* プロトコルのリテラル値

リテラル	値	説明
ah	51	IPv6 の認証ヘッダー（RFC 1826）。
eigrp	88	Enhanced Interior Gateway Routing Protocol（Enhanced IGRP）。
esp	50	IPv6 の暗号ペイロード（RFC 1827）。
gre	47	総称ルーティング カプセル化。

リテラル	値	説明
icmp	1	インターネット制御メッセージ プロトコル（RPC 792）。
icmp6	58	IPv6 のインターネット制御メッセージ プロトコル（RFC 2463）。
igmp	2	インターネット グループ管理プロトコル（RFC 1112）。
igrp	9	Interior Gateway Routing Protocol。
ip	0	インターネット プロトコル。
ipinip	4	IP-in-IP カプセル化。
ipsec	50	IP セキュリティ。ipsec プロトコル リテラルを入力すると、esp プロトコル リテラルを入力した場合と同じ結果が得られます。
nos	94	ネットワーク オペレーティング システム（Novell の NetWare）。
ospf	89	OSPF ルーティング プロトコル（RFC 1247）。
pcp	108	ペイロード圧縮プロトコル。
pim	103	プロトコル独立型マルチキャスト。
pptp	47	ポイントツーポイント トンネリング プロトコル。pptp プロトコル リテラルを入力すると、gre プロトコル リテラルを入力した場合と同じ結果が得られます。
snp	109	Sitara Networks Protocol。
tcp	6	伝送制御プロトコル（RFC 793）。
udp	17	ユーザー データグラム プロトコル（RFC 768）。

IANA の Web サイトでオンラインでプロトコル番号を確認できます。

http://www.iana.org/assignments/protocol-numbers

TCP ポートおよび UDP ポート

次の表に、リテラル値とポート番号を示します。いずれも ASA のコマンドで入力できます。次の警告を参照してください。

- ASA は、SQL*Net 用にポート 1521 を使用します。これは、Oracle が SQL*Net に使用するデフォルトのポートです。ただし、この値は IANA ポート割り当てとは一致しません。
- ASA は、ポート 1645 と 1646 で RADIUS をリッスンしています。RADIUS サーバーが標準ポート 1812 と 1813 を使用している場合は、**authentication-port** コマンドと **accounting-port** コマンドを使用して、それらのポートでリッスンするように ASA を設定できます。

- DNSアクセスにポートを割り当てるには、**dns**ではなく**domain**リテラル値を使用します。**dns** を使用した場合、ASA では、**dnsix** リテラル値を使用すると見なされます。

IANA の Web サイトでオンラインでポート番号を確認できます。

http://www.iana.org/assignments/port-numbers

表 *89*：ポートのリテラル値

リテラル	**TCP** または **UDP**	値	説明
aol	TCP	5190	America Online
bgp	TCP	179	ボーダー ゲートウェイ プロトコル（RFC 1163）
biff	UDP	512	新しいメールの受信をユーザーに通知するために、メール システムが使用
bootpc	UDP	68	ブートストラップ プロトコル クライアント
bootps	UDP	67	ブートストラップ プロトコル サーバー
chargen	TCP	19	キャラクタ ジェネレータ
cifs	TCP、UDP	3020	Common Internet File System
citrix-ica	TCP	1494	Citrix Independent Computing Architecture（ICA）プロトコル
cmd	TCP	514	cmd は自動認証機能がある点を除いて、exec と同様。
ctiqbe	TCP	2748	Computer Telephony Interface Quick Buffer Encoding
daytime	TCP	13	Day time（日時）（RFC 867）
discard	TCP、UDP	9	廃棄
dnsix	UDP	195	DNSIX Session Management Module Audit Redirector
domain	TCP、UDP	53	DNS
echo	TCP、UDP	7	Echo
exec	TCP	512	リモート プロセスの実行
finger	TCP	79	Finger
ftp	TCP	21	ファイル転送プロトコル（コンソールポート）

リテラル	TCP または UDP	値	説明
ftp-data	TCP	20	ファイル転送プロトコル（データ ポート）
gopher	TCP	70	Gopher
h323	TCP	1720	H.323 発呼信号
hostname	TCP	101	NIC ホスト ネーム サーバー
http	TCP、UDP	80	World Wide Web HTTP
https	TCP	443	HTTP over SSL
ident	TCP	113	ID 認証サービス
imap4	TCP	143	Internet Message Access Protocol バージョン 4
irc	TCP	194	インターネット リレー チャット プロトコル
isakmp	UDP	500	Internet Security Association and Key Management Protocol
klogin	TCP	543	KLOGIN
kshell	TCP	544	Korn シェル
ldap	TCP	389	Lightweight Directory Access Protocol。
ldaps	TCP	636	ライトウェイトディレクトリ アクセス プロトコル（SSL）
login	TCP	513	リモート ログイン
lotusnotes	TCP	1352	IBM Lotus Notes
lpd	TCP	515	ライン プリンタ デーモン（プリンタ スプーラー）
mobile-ip	UDP	434	モバイル IP-Agent
nameserver	UDP	42	ホスト ネーム サーバー
netbios-dgm	UDP	138	NetBIOS データグラム サービス
netbios-ns	UDP	137	NetBIOS ネーム サービス
netbios-ssn	TCP	139	NetBIOS セッション サービス
nfs	TCP、UDP	2049	ネットワーク ファイル システム（Sun Microsystems）

リテラル	TCP または UDP	値	説明
nntp	TCP	119	Network News Transfer Protocol
ntp	UDP	123	ネットワーク タイム プロトコル
pcanywhere-data	TCP	5631	pcAnywhere データ
pcanywhere-status	UDP	5632	pcAnywhere ステータス
pim-auto-rp	TCP、UDP	496	Protocol Independent Multicast、逆パス フラッド、デンス モード
pop2	TCP	109	Post Office Protocol（POP）Version 2
pop3	TCP	110	Post Office Protocol - Version 3
pptp	TCP	1723	ポイントツーポイント トンネリング プロトコル
radius	UDP	1645	リモート認証ダイヤルイン ユーザー サービス
radius-acct	UDP	1646	リモート認証ダイヤルイン ユーザー サービス（アカウンティング）
rip	UDP	520	ルーティング情報プロトコル
rsh	TCP	514	リモート シェル
rtsp	TCP	554	Real Time Streaming Protocol
secureid-udp	UDP	5510	SecureID over UDP
sip	TCP、UDP	5060	Session Initiation Protocol
smtp	TCP	25	シンプル メール転送プロトコル
snmp	UDP	161	簡易ネットワーク管理プロトコル
snmptrap	UDP	162	簡易ネットワーク管理プロトコル（トラップ）
sqlnet	[TCP]	1521	構造化照会言語ネットワーク
ssh	TCP	22	セキュア シェル
sunrpc	TCP、UDP	111	Sun Remote Procedure Call
syslog	UDP	514	システム ログ
tacacs	TCP、UDP	49	Terminal Access Controller Access Control System Plus

リテラル	TCP または UDP	値	説明
talk	TCP、UDP	517	Talk
Telnet	TCP	23	Telnet（RFC 854）
tftp	UDP	69	『Trivial File Transfer Protocol』
time	UDP	37	時刻
uucp	TCP	540	UNIX 間コピー プログラム
vxlan	UDP	4789	Virtual eXtensible Local Area Network（VXLAN）
who	UDP	513	Who
whois	TCP	43	Who Is
www	TCP、UDP	80	ワールドワイド ウェブ
xdmcp	UDP	177	X Display Manager Control Protocol

ローカル ポートとプロトコル

次の表に、ASA に向かうトラフィックを処理するために ASA が開くプロトコル、TCP ポート、および UDP ポートを示します。この表に記載されている機能とサービスをイネーブルにしない限り、ASA は、TCP または UDP ポートでローカル プロトコルを開きません。ASA がデフォルトのリスニング プロトコルまたはポートを開くように機能またはサービスを設定する必要があります。多くの場合、機能またはサービスをイネーブルにすると、デフォルト ポート以外のポートを設定できます。

表 *90*：機能とサービスによって開かれるプロトコルとポート

機能またはサービス	プロトコル	ポート番号	注
DHCP	UDP	67、68	—
フェールオーバー制御	105	なし	—
HTTP	TCP	80	—
HTTPS	TCP	443	—
ICMP	1	なし	—

機能またはサービス	プロトコル	ポート番号	注
IGMP	2	該当なし	プロトコルは宛先 IP アドレス 224.0.0.1 でだけ開かれます
ISAKMP/IKE	UDP	500	設定可能。
IPsec（ESP）	50	該当なし	—
IPsec over UDP（NAT-T）	UDP	4500	—
IPsec over TCP（CTCP）	TCP	—	デフォルト ポートは使用されません。IPsec over TCP の設定時にポート番号を指定する必要があります。
NTP	UDP	123	—
OSPF	89	該当なし	プロトコルは宛先 IP アドレス 224.0.0.5 および 224.0.0.6 でだけ開かれます
PIM	103	該当なし	プロトコルは宛先 IP アドレス 224.0.0.13 でだけ開かれます
RIP	UDP	520	—
RIPv2	UDP	520	ポートは宛先 IP アドレス 224.0.0.9 でだけ開かれます
SNMP	UDP	161	設定可能。
SSH	TCP	22	—
ステートフルアップデート	8（ノンセキュア）9（セキュア）	なし	—
Telnet	TCP	23	—
VPN ロードバランシング	UDP	9023	設定可能。
VPN 個別ユーザー認証プロキシ	UDP	1645、1646	ポートは VPN トンネルでだけアクセスできます。

ICMP タイプ

次の表に、ASA のコマンドで入力できる ICMP タイプの番号と名前を示します。

表 *91 : ICMP* タイプ

ICMP 番号	ICMP 名
0	echo-reply
3	unreachable
4	ソース クエンチ（始点抑制要求）
5	redirect
6	代替アドレス
8	echo
9	ルータ アドバタイズメント
10	ルータ要求
11	time-exceeded
12	パラメータ問題
13	timestamp-request
14	タイムスタンプ応答
15	情報要求
16	情報応答
17	マスク要求
18	mask-reply
30	traceroute
31	変換エラー
32	mobile-redirect

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。